SOPHOS

CYBERSECURITY: THE HUMAN CHALLENGE

I risultati di un sondaggio indipendente a cui hanno partecipato 5.000 responsabili IT in 26 paesi

Whitepaper Sophos Ottobre 2020

Introduzione

Viviamo in un periodo in cui il ruolo dei professionisti di cybersecurity non è mai stato così importante. Sebbene i progressi compiuti nell'ambito di automazione e tecnologia abbiano svolto un ruolo importante nel rafforzare le difese informatiche delle organizzazioni, per essere veramente efficaci i programmi di sicurezza richiedono pur sempre l'inclusione di competenze tecniche umane.

La sempre maggiore importanza che ha assunto il ruolo del professionista della sicurezza deriva principalmente dall'evoluzione degli attacchi informatici. Dietro a ogni minaccia informatica si trova un cybercriminale e al giorno d'oggi gli attacchi più avanzati sono spesso basati sulla combinazione tra tecnologie all'avanguardia e azioni pratiche di hacking svolte in tempo reale. Per proteggere i sistemi da questi attacchi coordinati da una mente umana, occorrono le competenze tecniche di altre menti umane.

Questo studio offre nuovi approfondimenti sulla situazione attuale delle competenze tecniche e delle risorse di cybersecurity in tutto il mondo. Rivela qual è la realtà vissuta dal personale informatico dedicato alla gestione della cybersecurity coordinata da una mente umana ed esplora qual è la risposta delle organizzazioni ai problemi affrontati.

Lo studio offre anche approfondimenti esclusivi sulla correlazione tra un incidente causato da un attacco ransomware e le best pratice di cybersecurity implementate dall'organizzazione che ne è caduta vittima.

Informazioni sul sondaggio

Sophos ha incaricato l'azienda Vanson Bourne, specializzata nelle ricerca, di intervistare 5.000 responsabili IT di 26 paesi, in un sondaggio che è stato condotto nei mesi di gennaio e febbraio 2020. Sophos non è intervenuta in alcun modo nella selezione dei partecipanti e tutte le risposte sono state fornite in maniera anonima.

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

PAESE	NUM. PARTECIPANTI
India	300
Italia	200
Giappone	200
Malaysia	100
Messico	200
Paesi Bassi	200
Nigeria	100
Filippine	100
Polonia	100

PAESE	NUM. PARTECIPANTI
Singapore	200
Sud Africa	200
Spagna	200
Svezia	100
Turchia	100
EAU	100
Regno Unito	300
Stati Uniti	500

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

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

Riepilogo

Il personale IT fa progressi in molte delle battaglie sulla sicurezza

- **Il personale informatico applica tempestivamente le patch.** In tre quarti dei casi, il personale informatico applica patch a desktop, server, applicazioni e risorse con connessione Internet entro una settimana dal rilascio. I server e le risorse con connessione Internet ricevono le patch più rapidamente, entro 24 ore per il 39% dei partecipanti.
- **Viene attribuita massima priorità alla prevenzione.** In media, il personale informatico dedica quasi metà del proprio tempo (45%) alla prevenzione, mentre investe il 30% del tempo nel rilevamento e il restante 25% nella risposta.
- **I responsabili IT tengono il passo con l'evoluzione della cybersecurity.** La maggior parte dei responsabili IT sostiene che sia loro (72%) che i loro team (72%) stanno tenendo il passo con le minacce di cybersecurity o che si trovano persino in vantaggio. Solo l'11% dei partecipanti dichiara di trovarsi significativamente indietro.

Per migliorare la cybersecurity occorre personale esperto, che non è facile da trovare

- **Il threat hunting con supervisione dell'operatore umano è un requisito tanto essenziale quanto urgente.** Il 48% degli intervistati ha già integrato attività di threat hunting svolta attraverso la supervisione dell'operatore umano nelle proprie procedure di sicurezza e un ulteriore 48% ha in programma di implementarle entro un anno.
- **La mancanza di competenze tecniche in materia di cybersecurity sta avendo un impatto diretto sulla protezione.** Più di un quarto (27%) dei responsabili IT ha confessato che il maggiore ostacolo al garantire un'IT security efficace è l'impossibilità di inserire e mantenere nell'organico professionisti di IT security con le giuste competenze tecniche, mentre nel 54% dei casi questa sfida è stata comunque elencata tra i problemi principali.

Le organizzazioni stanno cambiando la strategia di implementazione della sicurezza

- **L'outsourcing dell'IT security è in rapido aumento.** Attualmente, il 65% dei partecipanti utilizza servizi esterni per alcuni ambiti o l'intera gestione dell'IT security. Si prevede che questa percentuale raggiungerà il 72% entro il 2022. La percentuale delle organizzazioni che si affida esclusivamente a personale interno calerà dal 34% al 26%.
- **Migliorare l'efficienza operativa è una delle priorità principali.** Quattro partecipanti su dieci (39%) collocano il miglioramento dell'efficienza operativa e della scalabilità tra le principali priorità di quest'anno per il proprio team IT.

Le vittime di attacchi ransomware mostrano comportamenti e attitudini diversi rispetto alle organizzazioni che non sono mai state colpite

- **Le vittime del ransomware sono maggiormente esposte a infezioni provenienti da terze parti.** Il 29% delle organizzazioni colpite dal ransomware negli ultimi dodici mesi consente a cinque o più fornitori di connettersi direttamente alla propria rete, a differenza del 13% delle organizzazioni che non sono mai state colpite.
- **Il ransomware danneggia la fiducia nelle proprie capacità professionali.** I responsabili IT delle organizzazioni colpite dal ransomware hanno una probabilità quasi tre volte superiore di sentirsi "significativamente indietro" rispetto alle minacce informatiche, se messi a confronto con le organizzazioni che non sono state colpite (rispettivamente il 17% e il 6%).
- **Diventare vittima di un attacco accelera l'implementazione del threat hunting con supervisione dell'operatore umano.** Il 43% delle vittime del ransomware ha in programma di implementare il threat hunting con supervisione dell'operatore umano entro sei mesi, a differenza del 33% per le organizzazioni che non hanno subito un attacco.
- **Le vittime hanno compreso l'importanza dei professionisti di sicurezza dotati di competenze tecniche avanzate.** Più di un terzo (35%) delle vittime del ransomware confessa che inserire e mantenere nell'organico professionisti con elevate competenze di IT security rappresenta per loro il principale problema di cybersecurity, rispetto a solamente il 19% delle organizzazioni che non sono state colpite.

Il personale IT fa progressi in molte delle battaglie sulla sicurezza

Cominciamo con la buona notizia: il personale informatico riesce a tenere il passo con diversi aspetti della cybersecurity. I team IT hanno tanta carne al fuoco, ma riescono comunque a proteggere le proprie organizzazioni da moltissime minacce.

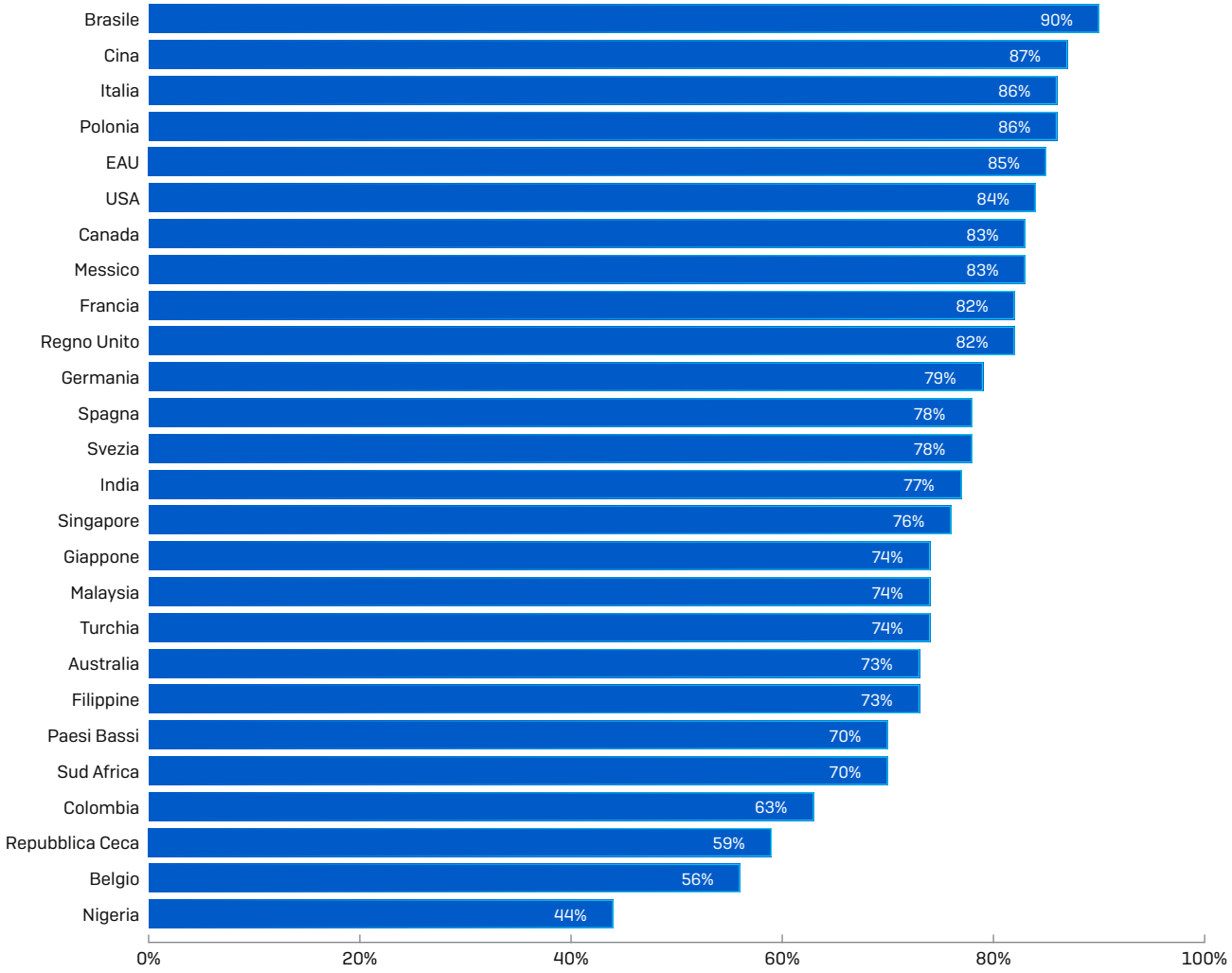
Il personale informatico applica le patch

"Applicare le patch presto, spesso e volentieri" è un tema ricorrente tra gli esperti di sicurezza e questo motto è stato adottato e applicato dal personale IT. Gli intervistati si sono dimostrati coscienti dell'importanza di applicare rapidamente le patch. Infatti, molti le applicano entro 24 ore dal rilascio e tre quarti entro una settimana. I server e le risorse con connessione Internet ricevono le patch più rapidamente, entro 24 ore per il 39% dei partecipanti.

	PATCH APPLICATE ENTRO 24 ORE	PATCH APPLICATE ENTRO UNA SETTIMANA	PATCH APPLICATE ENTRO UN MESE
Desktop	36%	41%	14%
Server	39%	38%	14%
Applicazioni	36%	40%	15%
Risorse con connessione internet	39%	38%	14%

Tuttavia, il 22% ammette di applicare le patch ai desktop dopo più di una settimana; le tempistiche più lunghe si osservano in Nigeria, Belgio e Repubblica Ceca.

Percentuale di intervistati che applica patch ai desktop entro una settimana dal rilascio

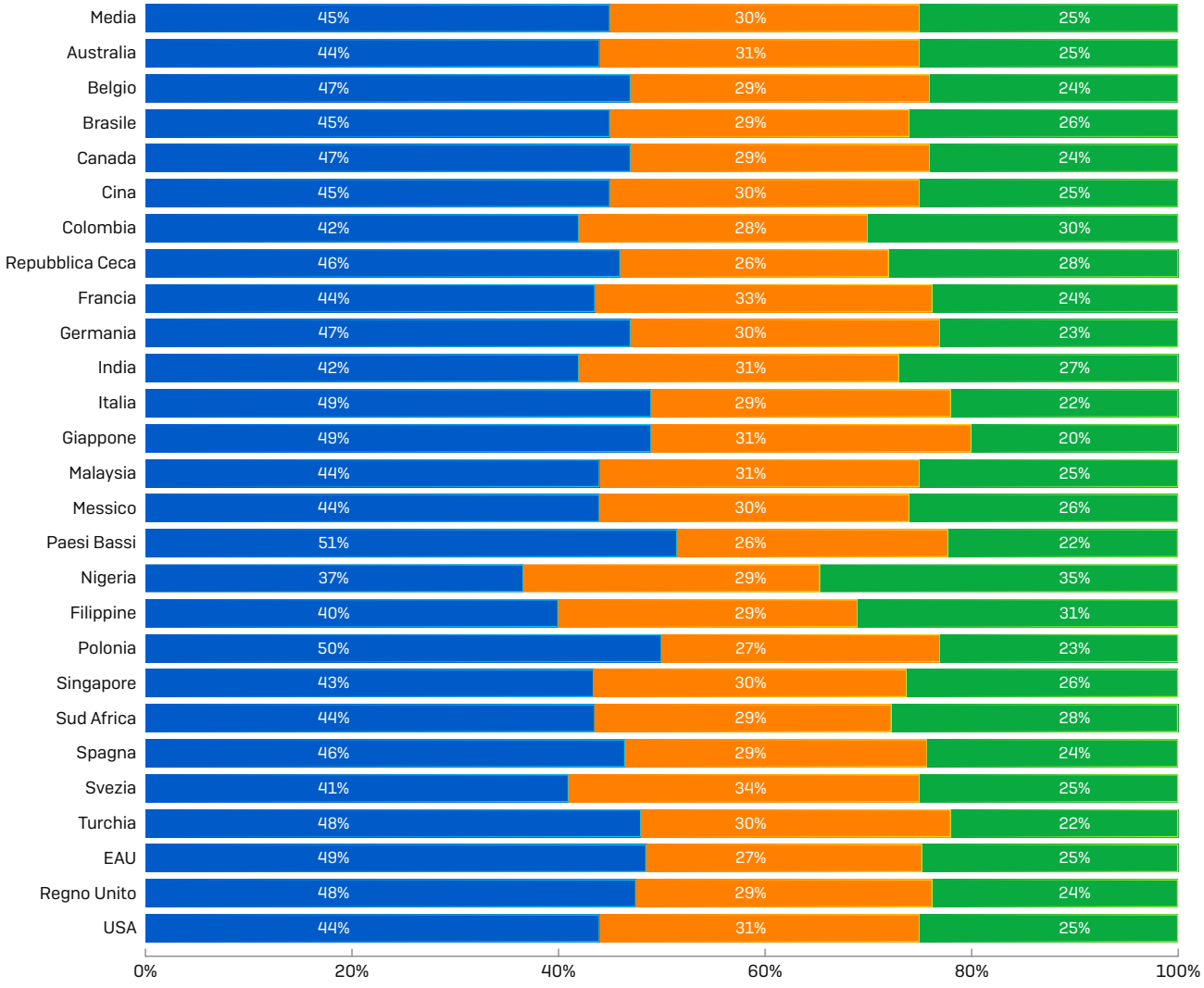


Massima priorità alla prevenzione

In media, il personale informatico dedica quasi metà del proprio tempo (45%) alla prevenzione, mentre investe il 30% del tempo nel rilevamento e il restante 25% nella risposta agli incidenti di sicurezza. Dai dati emergono alcune variazioni geografiche: tra i paesi degli intervistati, il personale IT nei Paesi bassi dichiara di investire più tempo nella prevenzione (51%), in Svezia il personale IT dedica più tempo al rilevamento (34%), mentre le organizzazioni in Nigeria registrano la percentuale più alta di tempo investito nelle attività di risposta (35%).

Se l'approccio più logico alla cybersecurity prevede un buon equilibrio tra prevenzione e rilevamento, un'elevata percentuale di tempo dedicato alla risposta agli incidenti di sicurezza indica l'impossibilità di arrestare gli incidenti. Punteggi alti per la risposta indicano un'elevata quantità di incidenti, un rilevamento tardivo, o ambedue i casi.

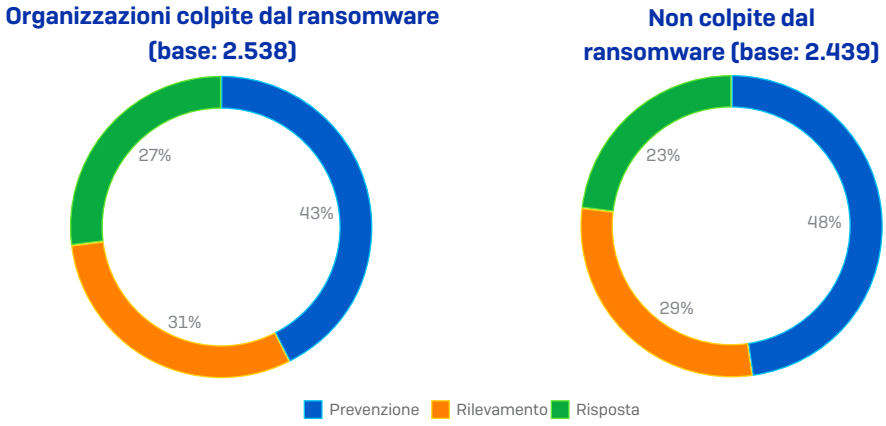
Suddivisione del tempo dedicato a prevenzione, rilevamento e risposta agli incidenti di sicurezza



Ci sono occasioni in cui la somma dei totali non è del 100%, questo è dovuto agli arrotondamenti applicati

Le vittime di un attacco ransomware dedicano meno tempo alla prevenzione e più tempo alla risposta agli incidenti

Il 51% dei partecipanti al sondaggio ha ammesso che la propria organizzazione aveva subito un attacco ransomware nei dodici mesi precedenti. Le organizzazioni colpite dal ransomware si focalizzano maggiormente sul rilevamento e sulla risposta, a differenza di quelle che non hanno subito incidenti. Le organizzazioni che invece non sono state colpite dal ransomware dedicano più tempo alla prevenzione, rispetto alle organizzazioni che hanno subito attacchi.



Un'ipotesi è che questo particolare impegno verso la prevenzione abbia aiutato le organizzazioni non colpite a prevenire gli attacchi: la strategia di difesa più efficace comincia sempre con la migliore protezione. Allo stesso tempo, è probabile che le vittime del ransomware siano maggiormente consce della complessità e delle varie sfaccettature degli attacchi avanzati e che pertanto investano maggiormente nel rilevamento e nella risposta ai segnali di un attacco imminente.

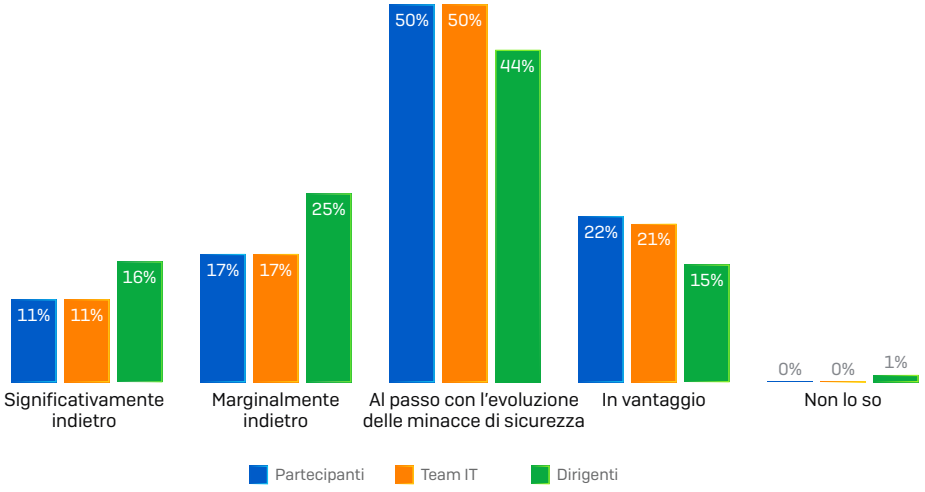
Per maggiori informazioni su come identificare il rischio di essere nell'occhio del mirino di un hacker che attacca utilizzando il ransomware, leggere l'articolo dei SophosLabs Cinque segnali che indicano che si sta per subire un attacco.

I responsabili IT tengono il passo con l'evoluzione della cybersecurity

Nonostante la mutevole natura delle minacce di cybersecurity, i professionisti dell'IT security ritengono di riuscire a tenere il passo con le minacce informatiche. La maggior parte dei responsabili IT sostiene che sia loro (72%) che i loro team (72%) stanno tenendo il passo con le minacce di cybersecurity o che si trovano persino in vantaggio. Del 28% dei responsabili IT che ritiene di essere rimasto indietro, il 17% si sente marginalmente indietro e solo l'11% si sente significativamente indietro.

Dietro queste percentuali si celano variazioni geografiche rilevanti: gli intervistati situati in Polonia, Messico e Turchia sono quelli che dichiarano maggiormente di sentirsi in vantaggio rispetto alle minacce di sicurezza (rispettivamente con il 39%, 34% e 31%), mentre le organizzazioni in Nigeria (60%), Svezia (57%) e Germania (49%) sono quelle che dichiarano più frequentemente di sentirsi indietro. Si noti che questi dati rappresentano la percezione dei partecipanti (ed è quindi probabile che vi sia un'influenza culturale) e non l'effettivo stato di preparazione.

Percezione dei partecipanti sulla preparazione dei dipendenti della propria organizzazione in materia di minacce di cybersecurity



Sebbene siano generalmente sicuri della loro preparazione e di quella del proprio team, il 41% dei responsabili IT ritiene che i dirigenti della propria organizzazione si trovino indietro (25% marginalmente, 16% significativamente indietro). Sotto molti punti di vista, questa differenza è comprensibile: normalmente i dirigenti non sono specialisti di cybersecurity. Tuttavia la situazione mette in evidenza la sfida che deve affrontare il personale informatico nel sensibilizzare i dirigenti sui rischi di cybersecurity, per convincerli ad acconsentire alle richieste di investimento in questo ambito.

Gli attacchi ransomware incidono sulla fiducia nelle proprie capacità dei professionisti dell'IT

Analizzando i dati in maniera approfondita, si nota che, per i responsabili IT e i loro team, gli attacchi ransomware infliggono danni notevoli alla fiducia nelle proprie capacità. Questo fattore va ad aggiungersi all'impatto sull'organizzazione.

La percentuale dei responsabili IT di organizzazioni colpite dal ransomware ha una probabilità quasi tre volte superiore di sentirsi "significativamente indietro" rispetto alle minacce informatiche, se paragonata a quella dei responsabili IT delle organizzazioni non attaccate (rispettivamente 17% e 6%). Questa diminuzione della fiducia nelle proprie capacità si estende anche alla percezione che i responsabili IT hanno del proprio team IT e dei dirigenti, come indica la tabella che segue.

	SI TROVA SIGNIFICATIVAMENTE INDIETRO RISPETTO ALLE MINACCE INFORMATICHE (%)	TIENE IL PASSO CON LE MINACCE INFORMATICHE (%)
Responsabili IT (intervistati)		
Colpiti dal ransomware	17%	43%
Non colpiti dal ransomware	6%	57%
Team IT (percezione degli intervistati)		
Colpiti dal ransomware	15%	43%
Non colpiti dal ransomware	6%	58%
Dirigenti (percezione degli intervistati)		
Colpiti dal ransomware	20%	39%
Non colpiti dal ransomware	11%	49%

Anche in questo caso è importante ricordare che queste risposte rappresentano la percezione dei partecipanti al sondaggio e non offrono un'indicazione della loro preparazione effettiva. Un'ipotesi è che cadere vittima del ransomware costringa maggiormente ad affrontare la realtà e di conseguenza le vittime di un attacco ransomware, basandosi sulle proprie esperienze, riescono a capire meglio la situazione.

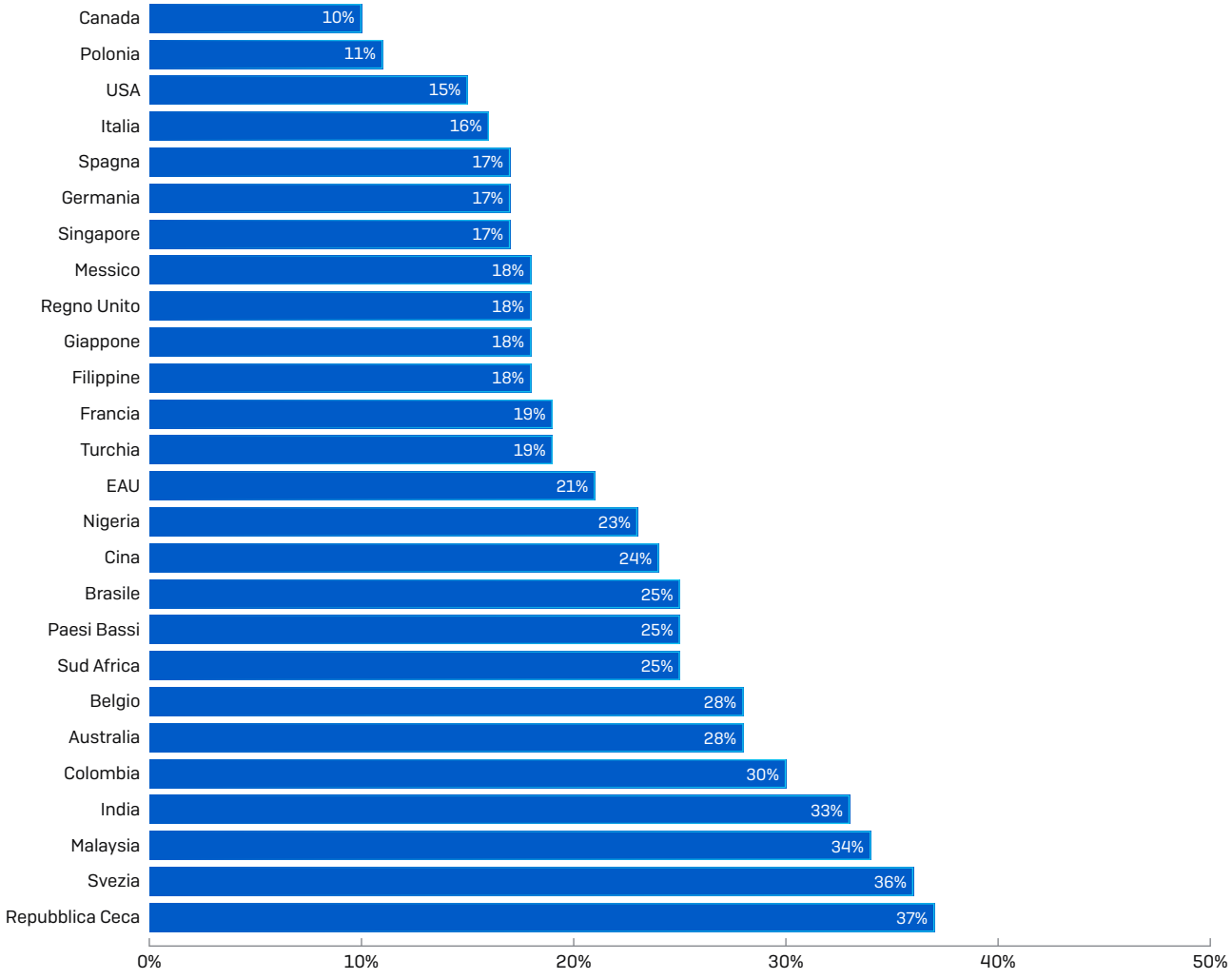
Per migliorare la cybersecurity occorre personale esperto, che non è facile da trovare

Sebbene il personale IT abbia vinto molte battaglie, la guerra è ancora in corso. Nonostante l'impegno dei responsabili IT e dei loro team, le minacce informatiche rimangono un problema attuale, al punto che più di metà degli intervistati (51%) dichiara che ridurre il rischio di un attacco informatico costituisce una delle principali aree di focalizzazione delle loro organizzazioni per i prossimi 12 mesi. I motivi di queste statistiche sono evidenti, se si osserva la varietà dei problemi di sicurezza affrontati dai responsabili IT.

Il personale IT è costantemente travolto da un'enorme quantità di attacchi informatici, con minacce che giungono da varie direzioni e che attaccano bersagli diversi. Come già accennato, il 51% dei partecipanti è stato colpito dal ransomware negli ultimi dodici mesi e i cybercriminali sono riusciti a cifrare i dati nel 73% di questi attacchi*. Anche la protezione del cloud rappresenta una sfida: l'anno scorso, il 70% delle organizzazioni che ospitano dati o workload sul cloud pubblico è stata vittima di un incidente di sicurezza**.

Un'altra sfida per il personale IT è la protezione di terze parti che sono in grado di connettersi direttamente alla rete dell'organizzazione, ad esempio per fornire servizi informatici o di contabilità. Gli intervistati hanno segnalato una media di tre fornitori autorizzati a connettersi ai propri sistemi. Tuttavia, per un partecipante al sondaggio su cinque (21%) sono cinque o più i fornitori autorizzati a connettersi alla rete, una statistica che sale a un terzo (o più) in Repubblica Ceca, India, Malaysia e Svezia. In Canada e in Polonia, invece, solamente un partecipante su dieci dichiara di autorizzare l'accesso da remoto a cinque o più fornitori.

Percentuale delle organizzazioni che consente a cinque o più fornitori di connettersi direttamente alla propria rete



Naturalmente, oltre a fornire vantaggi a livello organizzativo, autorizzare la connessione alla propria rete a terze parti introduce un ulteriore rischio di sicurezza. Più sono i fornitori che possono connettersi, maggiori saranno le sfide in termini di sicurezza e il carico di lavoro per il personale IT.

Le vittime del ransomware sono maggiormente esposte a infezioni provenienti da terze parti

Tra le organizzazioni colpite dal ransomware negli ultimi dodici mesi, il 29% consente a cinque o più fornitori di connettersi direttamente alla propria rete, a differenza del 13% delle organizzazioni che non sono mai state colpite. Le terze parti, menzionate come metodo di ingresso delle minacce dal 9% delle vittime, sono evidentemente uno dei principali vettori di attacco.

Sebbene esistano molti validi motivi commerciali per autorizzare organizzazioni esterne a connettersi alla rete interna, è lampante che proteggere la catena di distribuzione deve essere una delle priorità principali per chiunque adotti questo approccio. Disporre di un sistema di cybersecurity efficace deve essere un criterio essenziale per chiunque desideri connettersi alla rete interna.

Il threat hunting con supervisione dell'operatore umano è un requisito essenziale e urgente

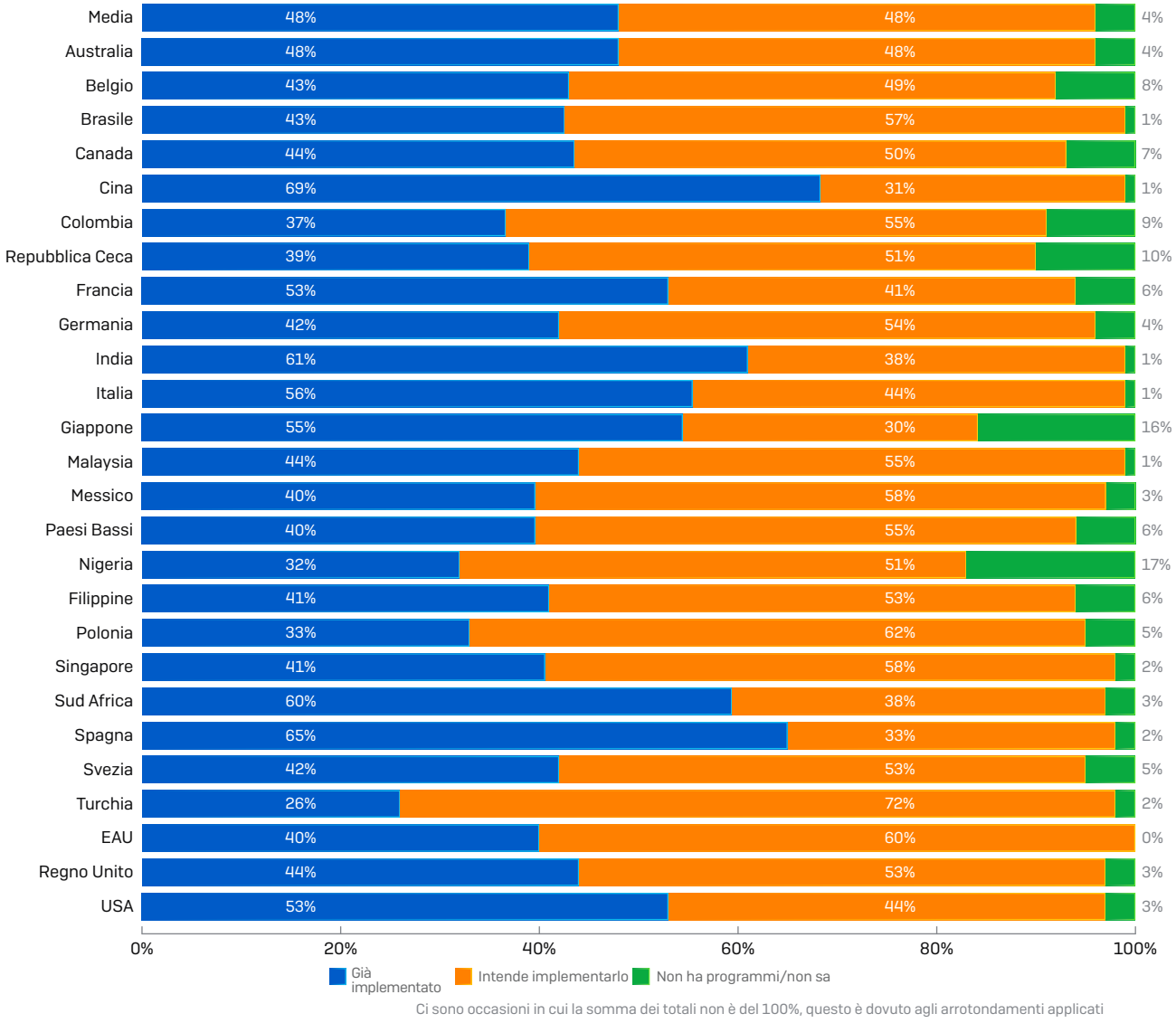
Le minacce informatiche più distruttive sono generalmente coordinate da menti umane e sovente si servono di strumenti legittimi, come PowerShell. L'hacking in tempo reale permette ai cybercriminali di modificare le proprie tattiche, tecniche e procedure (TTP) all'istante, per bypassare prodotti e protocolli di sicurezza. Una volta infiltratisi nella rete della vittima, gli hacker possono muoversi lateralmente, esfiltrare dati, installare malware e backdoor per attacchi futuri e distribuire ransomware.

Anche se le tecnologie, in particolar modo quelle automatizzate e basate su intelligenza artificiale, svolgono un ruolo importante, le competenze di operatori esperti rimangono indispensabili. Per bloccare attacchi coordinati da una mente umana, occorre un threat hunting con supervisione umana.

Quasi tutti i partecipanti al sondaggio sono consci di quanto sia essenziale questo approccio:il 48% ha già integrato il threat hunting con supervisione dell'operatore umano nelle proprie procedure di sicurezza, per identificare le attività di hacking che potrebbero sfuggire agli strumenti di sicurezza (ad es. SIEM, protezione endpoint, firewall ecc.). Un ulteriore 48% ha intenzione di implementarlo. Gli intervistati sono anche consapevoli dell'urgenza con cui occorre adottare un sistema di threat hunting con supervisione dell'operatore umano, con la quasi totalità (99,6%) degli intervistati che dichiara di volerlo implementare entro i prossimi dodici mesi.

Lo stato di implementazione del threat hunting con supervisione dell'operatore umano varia notevolmente a seconda della posizione geografica. Il 69% degli intervistati che si trovano in Cina hanno già adottato questo approccio, seguiti subito dopo da Spagna (65%), India (61%) e Sud Africa (60%). La Turchia, invece, si è dimostrata la nazione meno pronta ad adottare il threat hunting con supervisione umana, con solamente il 26% dei partecipanti che dichiara di averlo già implementato. Seguono Nigeria (32%) e Polonia (33%) a distanza ravvicinata.

Programmi di integrare attività di threat hunting con supervisione dell'operatore umano

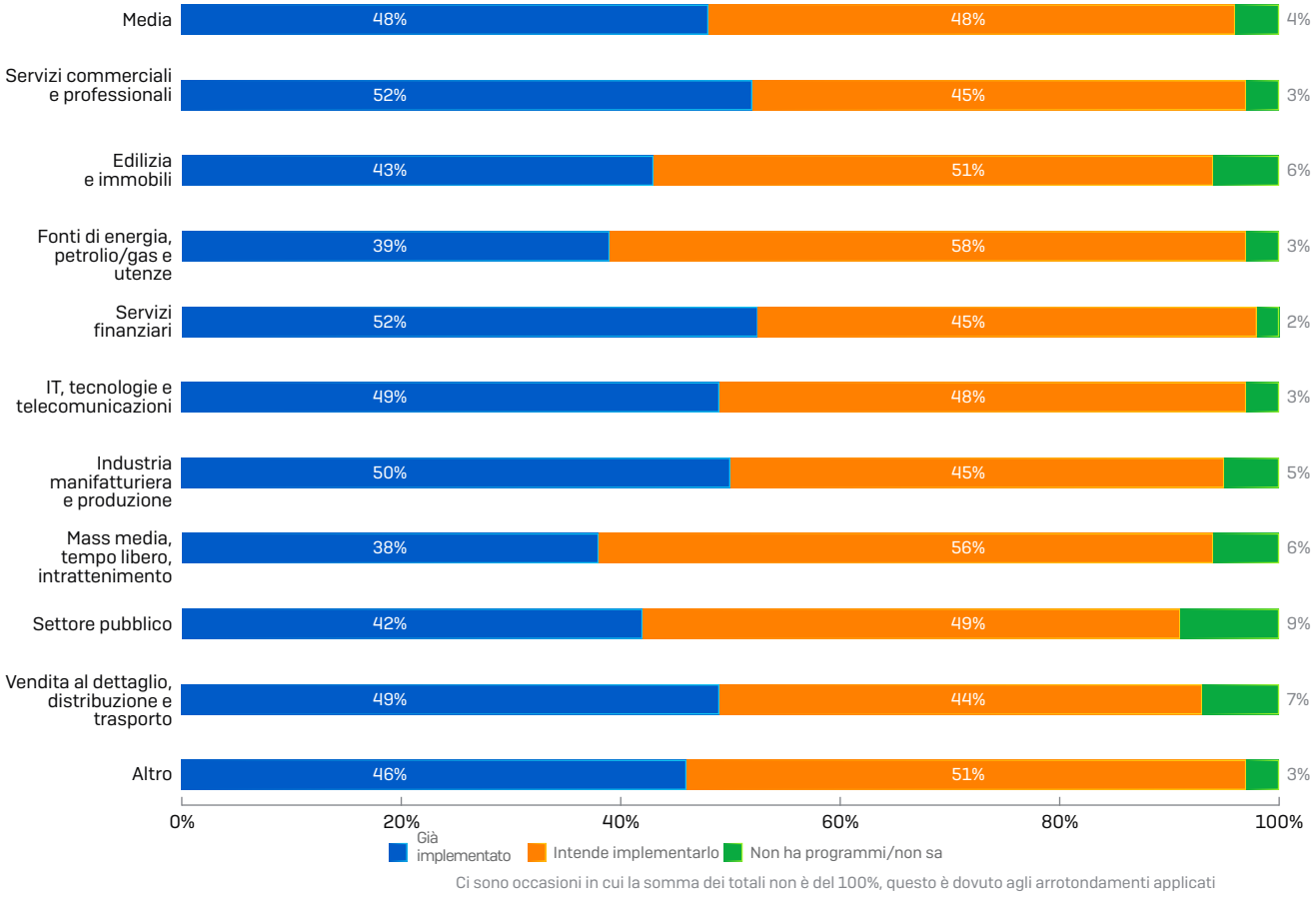


Ci sono occasioni in cui la somma dei totali non è del 100%, questo è dovuto agli arrotondamenti applicati

Dal sondaggio sono anche emersi livelli differenti di apertura a tale possibilità, in base al settore. I servizi commerciali, professionali e finanziari si dimostrano maggiormente propensi all'implementazione del threat hunting con supervisione umana, con il 52% degli intervistati in ciascuno di questi settori che dichiara di utilizzare già questo approccio.

La risposta è diversa per i settori che riguardano mass media, tempo libero e intrattenimento (38%) e fonti di energia, petrolio/gas e utenze (39%), che mostrano una minore probabilità di implementazione di attività di threat hunting con supervisione umana. Considerando che il settore delle fonti di energia rappresenta un bersaglio potenziale per gli attacchi contro i governi, questa vulnerabilità alle minacce coordinate da menti umane è preoccupante.

Programmi di integrare attività di threat hunting con supervisione dell'operatore umano a seconda del settore

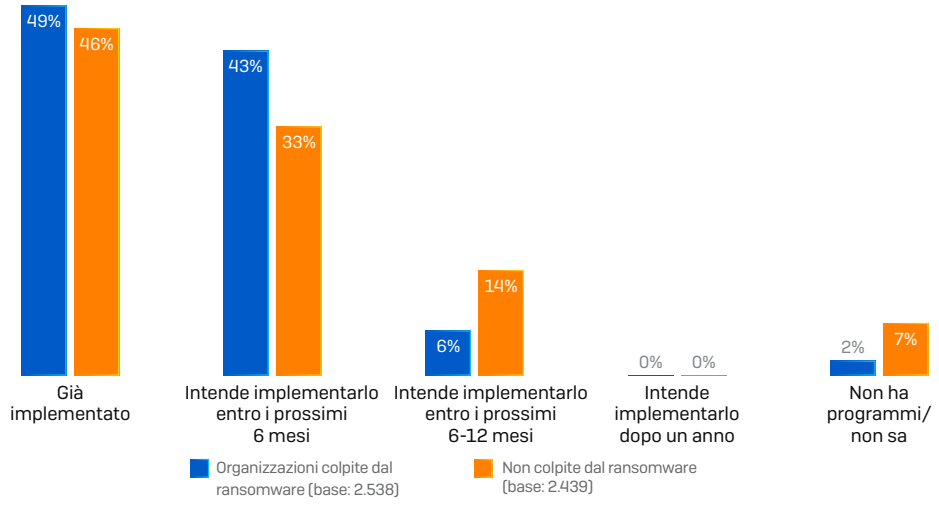


Ci sono occasioni in cui la somma dei totali non è del 100%, questo è dovuto agli arrotondamenti applicati

Cadere vittima del ransomware accelera l'implementazione del threat hunting con supervisione dell'operatore umano

Diventare vittima del ransomware ha un impatto complessivo trascurabile sul desiderio di un'organizzazione di integrare il threat hunting con supervisione umana, tuttavia incrementa il senso di urgenza per l'implementazione. Il 43% delle vittime del ransomware ha in programma di implementare il threat hunting con supervisione dell'operatore umano entro sei mesi, a differenza del 33% per le organizzazioni che non hanno subito un attacco. Queste statistiche indicano che le vittime del ransomware sono altamente motivate a evitare che un incidente si ripeta.

Impatto di un'esperienza recente di ransomware sull'implementazione del threat hunting con supervisione dell'operatore umano



La mancanza di competenze tecniche in materia di cybersecurity sta avendo un impatto diretto sulla protezione

L'81% dei partecipanti al sondaggio dichiara che trovare professionisti esperti in ambito di IT security è uno dei problemi principali della propria organizzazione nell'ambito dell'implementazione di una strategia di IT security efficace: il 54% identifica questa difficoltà come uno dei problemi più gravi, mentre più di un quarto (27%) come il problema principale.

Tutti i paesi hanno segnalato difficoltà nel trovare personale informatico dotato delle giuste competenze. In Italia (94%), India (93%) e Brasile e Colombia (entrambi con il 92%), più di nove intervistati su dieci afferma che l'impossibilità di trovare personale dotato delle giuste competenze rappresenta uno dei principali ostacoli alla protezione delle organizzazioni contro le minacce informatiche.

Anche in Sud Africa, il paese che registra una percentuale minore di difficoltà nell'assumere personale esperto di cybersecurity, le risorse umane costituiscono una sfida, e sei intervistati su dieci (62%) sostiene che questo sta causando problemi gravi alla propria organizzazione.

Classificazione dell'impatto sull'IT security della difficoltà di inserire e mantenere nell'organico professionisti esperti di IT security

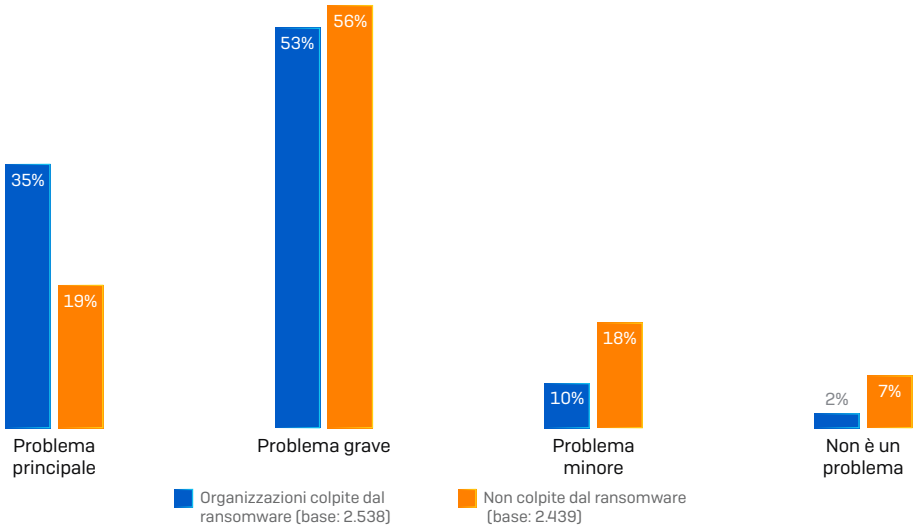
PAESE	È IL NOSTRO PROBLEMA PRINCIPALE	È UN PROBLEMA GRAVE, MA NON QUELLO PRINCIPALE	È UN PROBLEMA MINORE	NON È UN PROBLEMA	NON LO SO
Media	27%	54%	14%	4%	0%
Australia	17%	57%	22%	5%	0%
Belgio	24%	52%	24%	0%	0%
Brasile	45%	47%	6%	3%	1%
Canada	19%	55%	18%	7%	2%
Cina	24%	54%	18%	4%	0%
Colombia	29%	63%	8%	1%	0%
Repubblica Ceca	33%	47%	18%	1%	1%
Francia	23%	62%	11%	4%	0%
Germania	19%	63%	14%	5%	0%
India	58%	35%	6%	1%	0%
Italia	28%	67%	5%	2%	0%
Giappone	35%	44%	17%	4%	1%
Malaysia	26%	54%	16%	4%	0%
Messico	27%	62%	6%	6%	0%
Paesi Bassi	26%	49%	25%	0%	1%
Nigeria	32%	51%	16%	1%	0%
Filippine	40%	49%	8%	2%	1%
Polonia	9%	59%	20%	12%	0%
Singapore	17%	72%	10%	2%	0%
Sud Africa	22%	40%	19%	19%	0%
Spagna	17%	58%	17%	8%	1%
Svezia	44%	41%	13%	1%	1%
Turchia	30%	52%	9%	8%	1%
EAU	22%	62%	15%	1%	0%
Regno Unito	14%	64%	20%	2%	0%
USA	26%	49%	17%	8%	0%

Le vittime del ransomware hanno compreso a caro prezzo l'importanza del ruolo dei professionisti di sicurezza dotati di competenze tecniche avanzate

Cadere vittima di un attacco informatico ha un impatto significativo sull'attitudine verso le risorse umane esperte di cybersecurity. Più di un terzo (35%) degli intervistati che erano stati colpiti dal ransomware negli ultimi dodici mesi ha confessato che inserire e mantenere nell'organico professionisti esperti di IT security è il loro problema principale in termini di cybersecurity, mentre un ulteriore 53% lo definisce un problema grave.

Delle organizzazioni che, invece, non erano state colpite dal ransomware negli ultimi dodici mesi, solo il 19% dichiara che il problema principale è inserire e mantenere nell'organico personale esperto, con una differenza di ben 16 punti percentuali.

L'impatto sull'IT security della difficoltà di inserire e mantenere nell'organico professionisti esperti di IT security



Con molta probabilità, la differenza di attitudine è dovuta a diversi fattori. In primo luogo, le conseguenze della mancanza di competenze di sicurezza avanzate sono ancora fresche nelle menti di chi ha recentemente pagato il prezzo in termini finanziari, operativi e di reputazione di un attacco ransomware.

Inoltre, le vittime del ransomware avranno indagato sull'origine dell'attacco. Durante il processo, avranno individuato le lacune nella propria strategia di difesa che hanno permesso agli hacker di infiltrarsi nell'organizzazione e accedere ai dati. Probabilmente, molti avranno identificato nella carenza di personale qualificato uno dei fattori che hanno contribuito alla loro vulnerabilità all'attacco.

Assumere professionisti dotati delle giuste competenze è la priorità principale per i responsabili IT

Questa mancanza di personale dotato delle giuste competenze tecniche si riflette nel fatto che inserire e mantenere nell'organico personale competente ha assunto il primo posto nell'elenco di priorità dei responsabili IT. Il 55% degli intervistati dichiara che si tratta di una delle loro aree di focalizzazione per i prossimi 12 mesi, mentre al secondo posto si trova la riduzione del rischio di un attacco informatico. (nota: gli intervistati potevano selezionare più di una risposta per questa domanda).

Le organizzazioni stanno cambiando la strategia di implementazione della sicurezza

Probabilmente la difficoltà di trovare personale adeguato non coglie di sorpresa i professionisti dell'informatica. Le risorse umane nell'ambito della cybersecurity sono da diversi anni una sfida costante e, sebbene sia incoraggiante che i responsabili IT vi attribuiscano la massima priorità, l'entità del problema suggerisce che la soluzione non sarà semplice.

In quest'ottica, i cambiamenti che i responsabili IT stanno introducendo nella strategia di implementazione della sicurezza e la loro focalizzazione sul migliorare l'efficienza e la scalabilità possono essere considerate una risposta diretta al problema delle risorse umane.

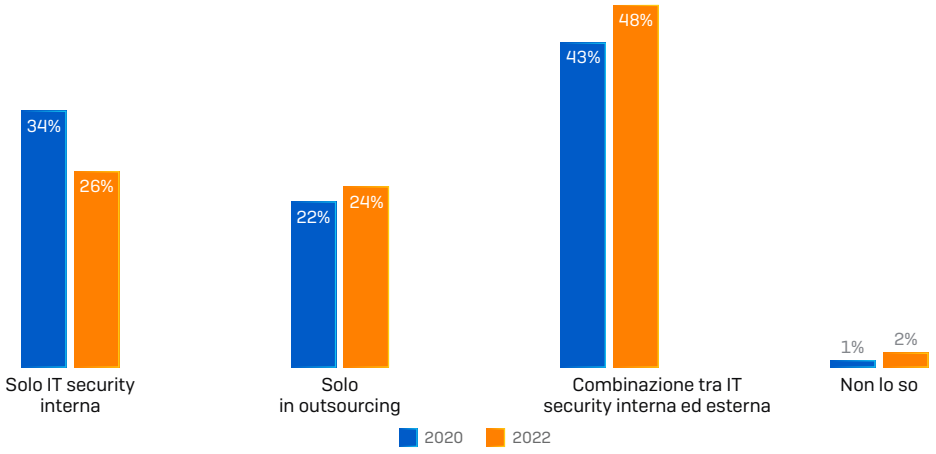
L'outsourcing è in rapido aumento

L'outsourcing della cybersecurity permette alle organizzazioni di usufruire di tutti i vantaggi delle competenze tecniche dei professionisti di sicurezza, senza doverli assumere direttamente. Inoltre, consente di accedere a livelli di competenza più elevati rispetto a quanto sarebbe possibile internamente per un'organizzazione, grazie alla capacità dei fornitori di servizi di sicurezza di continuare il proprio percorso formativo e sviluppare competenze specializzate.

L'outsourcing dell'IT security è già un processo consolidato, applicato in modalità diverse dal 65% degli intervistati: il 43% utilizza una combinazione tra risorse interne ed esterne, mentre il 22% si affida interamente all'outsourcing per la propria IT security. Dal sondaggio sono emerse variazioni di natura geografica. In cima all'elenco per l'outsourcing si trovano Cina (76%), EAU (74%) e Malaysia e Singapore (entrambi con il 73%), paesi nei quali circa tre quarti degli intervistati include già l'outsourcing nella propria strategia di IT security. In fondo alla classifica, si trovano Belgio (52%), Francia (54%) e Nigeria (54%), dove più della metà degli intervistati ricorre a fornitori di servizi di sicurezza esterni.

Come tendenza globale, si prevede un aumento dell'outsourcing nei prossimi due anni, quando dovrebbe passare dall'attuale 65% a quasi tre quarti (72%) nel 2022. Il cambiamento principale si riscontrerà nella percentuale delle organizzazioni che si affiderà esclusivamente a personale interno: è previsto un calo dal 34% al 26%. Ci sarà un incremento delle percentuali sia per le organizzazioni che si affidano completamente a fornitori esterni per l'IT security, sia per quelle che utilizzano una combinazione tra esperti interni ed esterni.

La strategia di implementazione dell'IT security adottata dalle organizzazioni



Dietro a queste percentuali, si nascondono delle interessanti variazioni in base alla posizione geografica:

- Gli intervistati in Spagna e India intendono incrementare la gestione dell'IT security interna. Sebbene le statistiche siano relativamente basse (dal 34% al 37% in Spagna e dal 33% al 34% in India), è interessante osservare come l'intenzione in questi paesi sia opposta rispetto alla tendenza globale
- Nelle Filippine, quasi la metà (48%) degli intervistati intende affidarsi interamente all'outsourcing per l'IT security nel 2022: un incremento molto elevato rispetto all'attuale 30%. Altri paesi che intendono implementare l'approccio di solo outsourcing con una percentuale superiore alla media sono Repubblica Ceca, Nigeria e Svezia (tutte con il 35%) e Australia (34%)
- Più di sei partecipanti al sondaggio su dieci intendono adottare un approccio combinato tra risorse interne ed esterne in Cina (67%) e Messico (62%)

I responsabili IT sono focalizzati sul miglioramento dell'efficienza e della scalabilità

Un'altra risposta alla carenza di esperti di IT security è ricorrere a modi alternativi di utilizzare le risorse disponibili. Quattro partecipanti su dieci (39%) collocano il miglioramento dell'efficienza operativa e della scalabilità tra le principali priorità di quest'anno per il proprio team IT. Gli intervistati europei e giapponesi hanno contribuito ad abbassare la media, mentre in Cina, Malaysia e Sud Africa metà dei partecipanti al sondaggio include questo fattore nel proprio elenco di priorità.

Conclusione

Questi approfondimenti, con statistiche tratte da 5.000 responsabili IT in 26 paesi, hanno rivelato i problemi di sicurezza del personale IT in termini di gestione e implementazione dell'IT security. Sebbene il personale informatico stia vincendo molte battaglie (specialmente applicando patch e mantenendosi aggiornato sulle minacce di sicurezza), la guerra è ancora in corso. I professionisti dell'IT security affrontano sfide su tutti i fronti: da ransomware e cloud security, alla gestione di fornitori di terze parti in grado di connettersi alla rete interna.

Di fronte all'aumento degli attacchi coordinati da esseri umani, la maggior parte delle organizzazioni si sta sempre più affidando al threat hunting con supervisione dell'operatore umano: il 95% degli intervistati ha espresso il desiderio di implementarlo, in modalità diverse, entro la fine del 2020. Allo stesso tempo, le difficoltà riscontrate nell'inserire e mantenere nell'organico professionisti esperti di cybersecurity costituiscono un fattore limitante per gran parte delle organizzazioni. Le organizzazioni che sono recentemente cadute vittima del ransomware sono particolarmente consce dell'impatto di questa mancanza di risorse umane sulla propria capacità di implementare una cybersecurity efficace.

È emersa una correlazione diretta tra le esperienze in termini di ransomware e i comportamenti in ambito informatico. Le vittime del ransomware sono maggiormente esposte alle infezioni provenienti da terze parti, rispetto alle organizzazioni che non hanno subito attacchi; inoltre, dedicano più tempo alle attività di risposta, il che indica che devono risolvere un maggior numero di incidenti. Allo stesso tempo, le esperienze affrontate da queste organizzazioni hanno contribuito a sensibilizzarle maggiormente sull'importanza del ruolo dei professionisti esperti di cybersecurity, suscitando maggiore urgenza nell'implementazione del threat hunting con supervisione umana.

Alla luce di queste sfide, è incoraggiante osservare l'evoluzione degli approcci adottati dal personale IT. Si prevede un ulteriore incremento dell'utilizzo di personale esperto in outsourcing nei prossimi due anni, in quanto entro il 2022 quasi tre quarti delle organizzazioni si affideranno, in modalità diverse, all'outsourcing per la propria IT security. Cresce inoltre la focalizzazione sull'incremento dell'efficienza operativa e della scalabilità in varie aree geografiche, per permettere al personale IT di sfruttare maggiormente le competenze dei professionisti attualmente disponibili.

La cybersecurity non si ferma mai. Il personale IT merita di essere elogiato per essere riuscito a tenere il passo con diversi aspetti della sicurezza. Considerando l'attuale mancanza di personale dotato di competenze di cybersecurity, il personale IT dovrà trovare modi alternativi per ampliare e potenziare il proprio sistema di difesa, al fine di contrastare la costante evoluzione delle minacce, tenendo presente soprattutto l'aumento degli attacchi coordinati da menti umane.

Sophos vi può aiutare, ecco come

Indipendentemente da come desideriate gestire la vostra IT security, noi possiamo aiutarvi.

Servizio di threat hunting con supervisione umana 24/7

Con Sophos Managed Threat Response (MTR), la vostra organizzazione può usufruire di una protezione disponibile 24/7 a cura di un team selezionato di esperti di threat hunting e risposta alle minacce, in grado di individuare proattivamente e neutralizzare le minacce per conto vostro. Questi professionisti di sicurezza altamente qualificati sono in grado di rilevare e bloccare gli attacchi coordinati da esseri umani prima che possano lasciare un segno nella vostra organizzazione.

Maggiori informazioni e Guida all'acquisto di soluzioni MDR.

Servizio di risposta agli incidenti in tempo reale

Qualsiasi organizzazione che si trovi ad affrontare un incidente attivo può affidarsi al nostro servizio **Rapid Response**. Il nostro team di esperti in ambito di risposta agli incidenti identificherà e neutralizzerà rapidamente la minaccia attiva. Che si tratti di un'infezione, di un tentativo di compromissione o di un accesso non autorizzato che cerca di eludere i controlli di sicurezza, abbiamo già visto e bloccato di tutto.

Maggiori informazioni

Protezione avanzata delle strutture informatiche e strumenti per il threat hunting

Se preferite svolgere attività di threat hunting in maniera indipendente, Sophos Endpoint Detection and Response (EDR) offre tutti gli strumenti necessari per implementare una strategia avanzata di threat hunting e protezione dell'integrità delle IT security operation. Le potenti opzioni di ricerca permettono al personale di identificare e reagire proattivamente ai problemi di integrità delle strutture informatiche, incrementando il livello di protezione.

Maggiori informazioni e prova gratuita.

Sistema di cybersecurity next-gen

Le organizzazioni che implementano un sistema di cybersecurity next-gen Sophos mostrano una tendenza costante a una riduzione del 50% nei costi di gestione delle strutture informatiche. Utilizzando le nostre soluzioni endpoint e firewall leader di mercato e gestendo tutti i sistemi con la piattaforma Sophos Central, il personale IT dimezza il tempo da investire nella gestione della cybersecurity, migliorando allo stesso tempo l'efficacia della sicurezza.

Maggiori informazioni e testimonianze dei clienti.

Approfondimenti sul ransomware

I SophosLabs e il team Sophos MTR pubblicano regolarmente i risultati delle loro ricerche sulle più recenti tecniche di attacco del ransomware. Potete scoprire di più sul blog di Sophos.

* La vera storia del ransomware. Un sondaggio globale condotto tra 5.000 responsabili IT, sponsorizzato da Sophos e condotto da Vanson Bourne.

** La Cloud Security nel 2020. Un sondaggio globale condotto tra 3.521 responsabili IT, sponsorizzato da Sophos e condotto da Vanson Bourne.

Informazioni su Vanson Bourne

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

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

05/10/20 WPEN (DD)

SOPHOS