SOPHOS
Cybersecurity evolved.

Il Team Di IT Security: Nel 2021 Ed Oltre

I risultati di un sondaggio condotto tra 5.400 responsabili IT in 30 paesi

Whitepaper Sophos. Giugno 2021

Nella maggior parte delle organizzazioni il personale IT ha dovuto affrontare numerosi attacchi informatici durante la pandemia. I team IT hanno svolto un ruolo diretto ed essenziale nel permettere alle organizzazioni di continuare a lavorare, nonostante le restrizioni e le limitazioni imposte dal COVID-19. Grazie all'impegno assiduo di personale tecnico in tutto il mondo, molte organizzazioni sono riuscite a rimanere operative durante la pandemia. Il personale IT ha aiutato le scuole e le università ad implementare la didattica a distanza, ha permesso ai commercianti di vendere online e ha fatto in modo che gli enti pubblici potessero continuare a erogare servizi essenziali, per citare solo alcuni esempi.

Il report, basato sul feedback diretto di 5.400 responsabili IT in 30 paesi, mette in luce le realtà affrontate dai team tecnici negli ultimi 12 mesi. Rivela i cambiamenti che i team IT hanno affrontato nel corso del 2020, focalizzandosi principalmente sulla cybersecurity e sull'impatto che ha avuto sul personale IT. Il documento analizza ciò che i team di IT security dovranno affrontare in futuro, ed aiuta le organizzazioni nell'iniziare a creare oggi il proprio team IT di domani.

I risultati più salienti

Come sono cambiate le esperienze dei team IT durante il 2020

- **Aumento del carico di lavoro informatico e di cybersecurity:** il 63% degli intervistati ha osservato un incremento nel carico di lavoro non legato alla sicurezza, mentre il 69% ha riscontrato un aumento del carico di lavoro dell'IT security
- **Aumento della prevalenza degli attacchi informatici:** il 61% degli intervistati ha riportato un incremento nel numero di attacchi informatici che hanno preso di mira la propria organizzazione
- **I team IT sono stati in grado di migliorare le proprie competenze di cybersecurity:** il 70% del personale IT intervistato ha dichiarato di aver incrementato le proprie conoscenze e competenze di cybersecurity in questo periodo
- **Le avversità hanno favorito lo spirito di squadra:** il 52% dei partecipanti al sondaggio afferma di aver notato un morale più alto durante l'anno. Questo fenomeno è stato più prominente nelle organizzazioni che hanno subito un attacco ransomware, rispetto a quelle che non ne sono state colpite (60% vs 47%)

Lo stato attuale

- **I team IT hanno bisogno di aiuto quando devono affrontare attacchi complessi:** Il 54% degli intervistati ammette che gli attacchi informatici sono ora troppo avanzati per essere affrontati dal team tecnico interno, senza un aiuto esterno
- **I team IT si sentono adeguatamente preparati per le sfide future:** l'82% sostiene di avere gli strumenti e le conoscenze necessari per svolgere indagini esaustive sulle attività sospette

Il team IT del futuro

- **Ci sarà un aumento del personale nei team di IT security**
  - Il 68% si attende un incremento del personale IT interno entro il 2023, mentre il 76% lo attende entro il 2026
  - Il 56% prevede un incremento del personale IT esterno entro il 2023 mentre il 64% lo prevede entro il 2026
- **Le tecnologie basate su intelligenza artificiale sono uno strumento essenziale per le strategie di sicurezza del futuro**
  - Il 92% ritiene che l'intelligenza artificiale aiuterà ad affrontare la maggiore quantità e complessità delle minacce

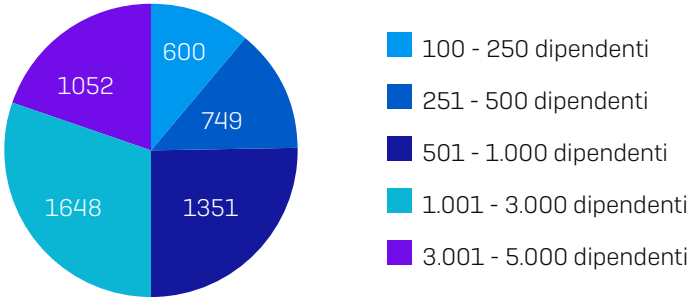
Informazioni sul sondaggio

Sophos ha affidato a Vanson Bourne, un'azienda di ricerca indipendente, l'incarico di intervistare 5.400 decision maker dell'IT in 30 paesi. Il sondaggio è stato svolto tra gennaio e febbraio 2021.

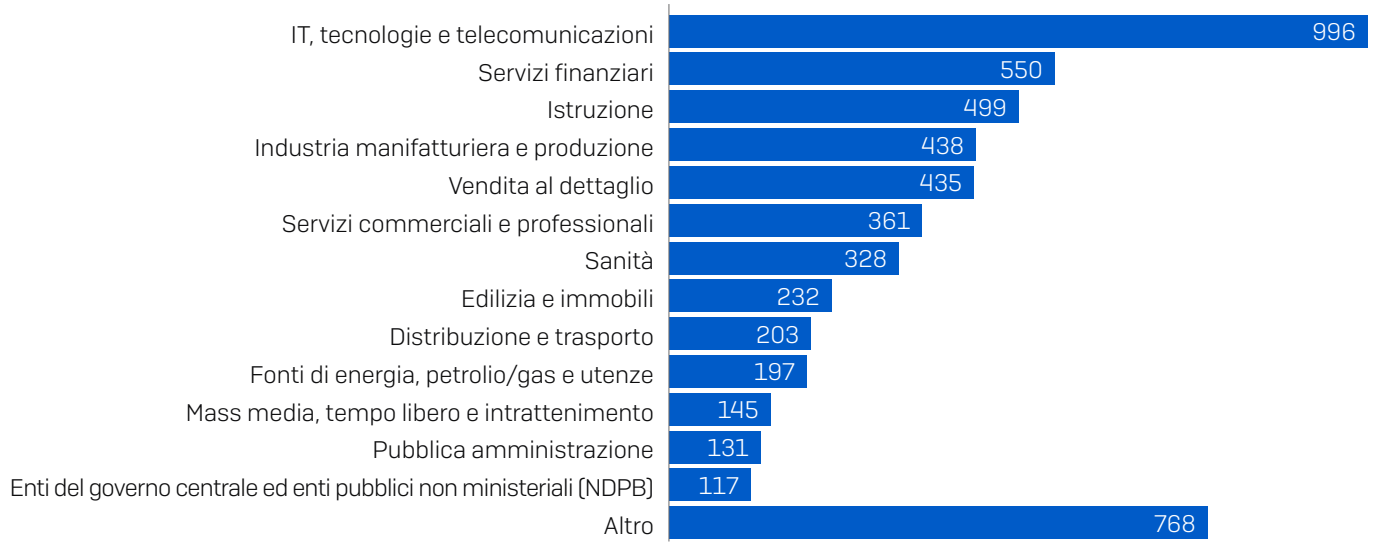
Paese	Num. partecipanti	Paese	Num. partecipanti	Paese	Num. partecipanti
Australia	250	India	300	Arabia Saudita	100
Austria	100	Israele	100	Singapore	150
Belgio	100	Italia	200	Sud Africa	200
Brasile	200	Giappone	300	Spagna	150
Canada	200	Malaysia	150	Svezia	100
Cile	200	Messico	200	Svizzera	100
Colombia	200	Paesi Bassi	150	Turchia	100
Repubblica Ceca	100	Nigeria	100	EAU	100
Francia	200	Filippine	150	Regno Unito	300
Germania	300	Polonia	100	Stati Uniti	500

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 partecipanti appartenevano a settori diversi.

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



In quale settore opera la vostra organizzazione? [5.400]



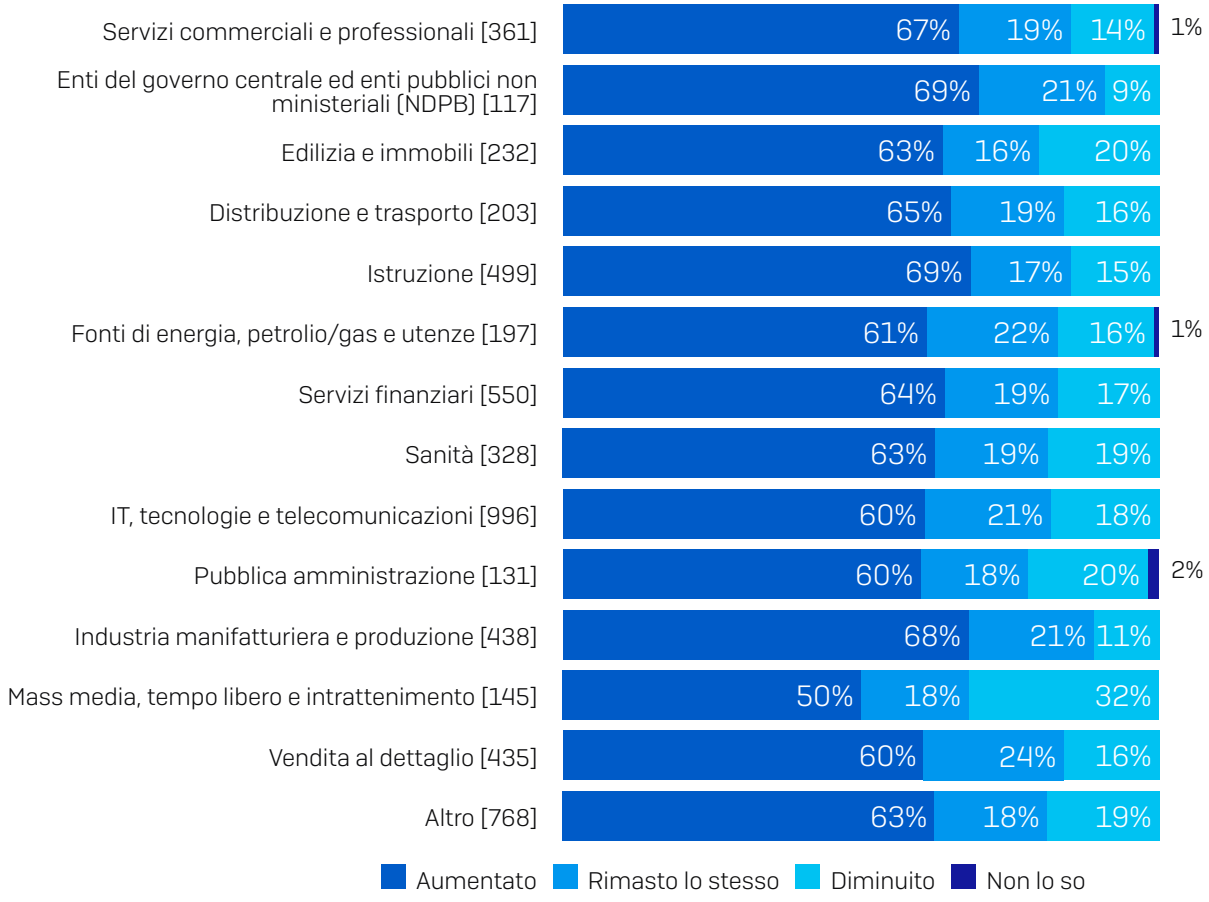
Il 2020: un anno di grandi cambiamenti

Il 2020 è stato un anno come nessun altro e i team IT si sono trovati in prima linea nel dovere abilitare le proprie organizzazioni a rispondere in modo proattivo alla pandemia. Non sorprende, pertanto, che tutto ciò abbia avuto un impatto notevole sul carico di lavoro.

Il carico di lavoro non legato alla sicurezza ha subito un incremento...

Il 2020 ha introdotto moltissimo nuovo lavoro per i team IT: il 63% dei responsabili IT sostiene di aver notato un aumento del carico di lavoro non legato alla sicurezza nel 2020 e solo il 17% ha dichiarato di averne vista una riduzione. Gli intervistati in Turchia (84%), Austria (81%) e USA (75%) sono quelli che hanno riportato un maggiore aumento nel carico di lavoro.

Com'è cambiato il carico di lavoro (non legato alla sicurezza) dei team IT nel 2020



Nel 2020 il nostro carico di lavoro (non legato alla sicurezza) è aumentato/diminuito/rimasto lo stesso [base di partecipanti indicata nel grafico], suddivisione in base al settore

Osservando i dati per i vari settori, si nota che i team IT negli **Enti del governo centrale ed enti pubblici non ministeriali (NDPB)** e nel settore dell'**Istruzione** sono quelli che hanno subito l'impatto più significativo, con il 69% degli intervistati che dichiara di aver riscontrato un incremento nel carico di lavoro durante l'anno. Probabilmente, questo è dovuto al ruolo fondamentale svolto dagli enti governativi e dagli istituti di istruzione nella risposta alla pandemia. **Mass media, tempo libero e intrattenimento** è invece il settore in cui si nota la percentuale più alta di intervistati che dichiarano di aver notato una riduzione (32%). Questa statistica è probabilmente attribuibile al fatto che molte strutture di questo settore hanno dovuto limitare i propri servizi.

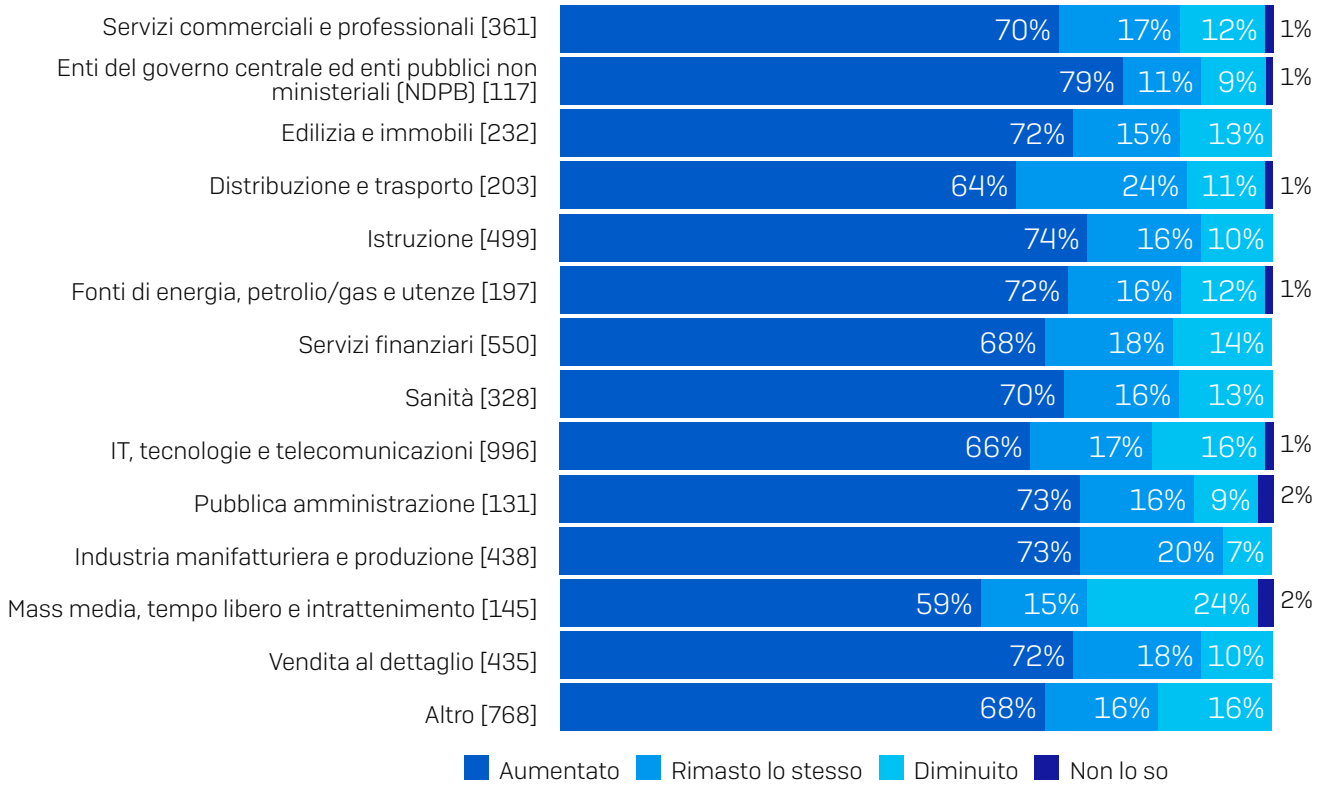
...e il carico di lavoro di cybersecurity è aumentato ancora di più

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], la risposta "Non lo so" è stata omessa

Il 69% degli intervistati ha osservato un aumento nel proprio carico di lavoro per la cybersecurity rispetto all'anno precedente, il 13% ha notato una riduzione e il 17% ha dichiarato di avere lo stesso carico di lavoro. Ancora una volta, la Turchia (82%) ha riportato il livello più alto di incremento, seguita da Svezia (80%), Israele e Brasile (entrambi 78%). All'estremo opposto, i partecipanti al sondaggio negli EAU sono quelli che hanno registrato la maggiore probabilità di una diminuzione del carico di lavoro di cybersecurity (26%), seguiti da Svizzera (22%), e Nigeria e Filippine (entrambi 19%).

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

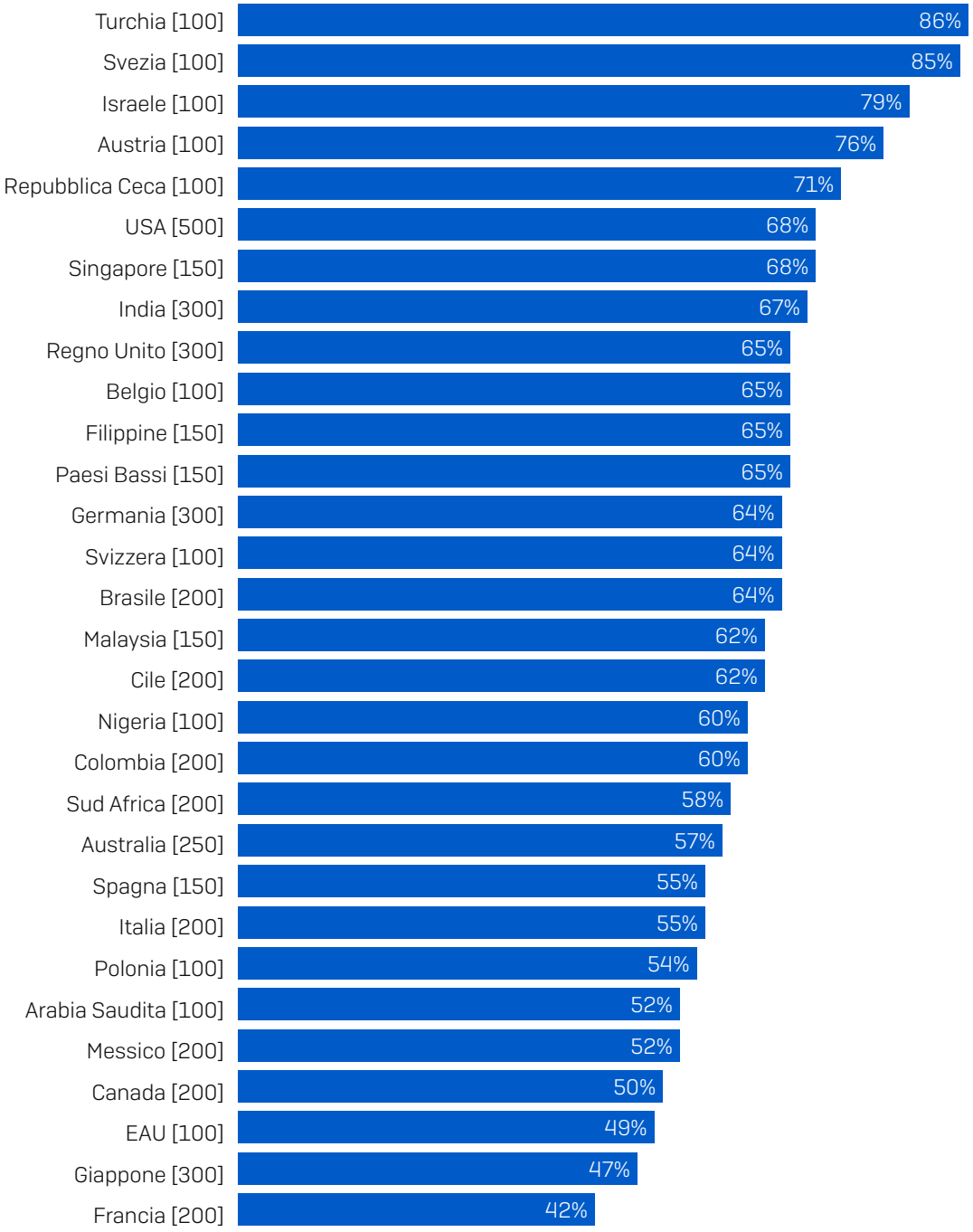
Seguendo le tendenze in base al settore osservate prima, i responsabili IT negli **Enti del governo centrale ed enti pubblici non ministeriali (NDPB)** (79%) e nel settore dell'**Istruzione** (74%) sono quelli con la maggiore probabilità di riscontrare un incremento del carico di lavoro di cybersecurity rispetto all'anno precedente, mentre gli intervistati nel settore **Mass media, tempo libero e intrattenimento** sono quelli con la più elevata probabilità di notare una diminuzione (24%). Anche in questo caso, è molto probabile che il motivo sia il fatto che questi settori hanno subito maggiormente l'impatto della pandemia, seppur in modi diversi.

Aumento della frequenza degli attacchi informatici

Il maggiore carico di lavoro per la cybersecurity osservato nel 2020 è in parte dovuto all'aumento degli attacchi informatici: più di sei intervistati su dieci (61%) hanno riportato un incremento nel numero di attacchi subiti dalla propria organizzazione l'anno scorso. Solo il 19% sostiene di aver notato una diminuzione.

Questo aumento è stato osservato in tutti i settori e la differenza tra i settori che lo hanno dichiarato maggiormente **(Enti del governo centrale ed enti pubblici non ministeriali, NDPB)** e in maniera minore **(Tecnologie IT e telecomunicazioni** e **Mass media, tempo libero e intrattenimento)** è di soli 16 punti percentuali (74% vs 58%).

Percentuale delle organizzazioni degli intervistati che hanno riscontrato un aumento degli attacchi informatici nel 2020

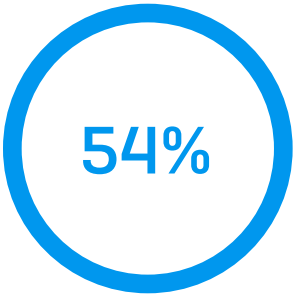


Nel 2020 gli attacchi informatici sono aumentati [base di partecipanti indicata nel grafico], alcune risposte sono state omesse, suddivisione in base al settore

Tuttavia, osservando i dati in base ai paesi, si nota una maggiore variazione in termini di esperienza, con il doppio dei partecipanti in Turchia che segnalano un aumento negli attacchi, rispetto a quelli in Francia (86% vs 42%). Ci sono percentuali molto elevate anche in Svezia (85%), Israele (79%) e Austria (76%) per i partecipanti che hanno dichiarato di aver notato un aumento degli attacchi informatici contro la propria organizzazione nel 2020. In Francia, Giappone e negli EAU, invece, meno della metà degli intervistati ha dichiarato di avere osservato un aumento.

Gli attacchi stanno diventando più difficili da bloccare

Gli attacchi informatici avanzati sono caratterizzati da una struttura complessa e si svolgono in fasi multiple. I loro autori utilizzano varie Tattiche, Tecniche e Procedure (TTP) nel corso dell'incidente. Affrontare questi tipi di attacchi è problematico e per più della metà dei partecipanti al sondaggio (54%), gli attacchi sono ora troppo avanzati per essere risolti dal loro team IT senza un aiuto esterno.

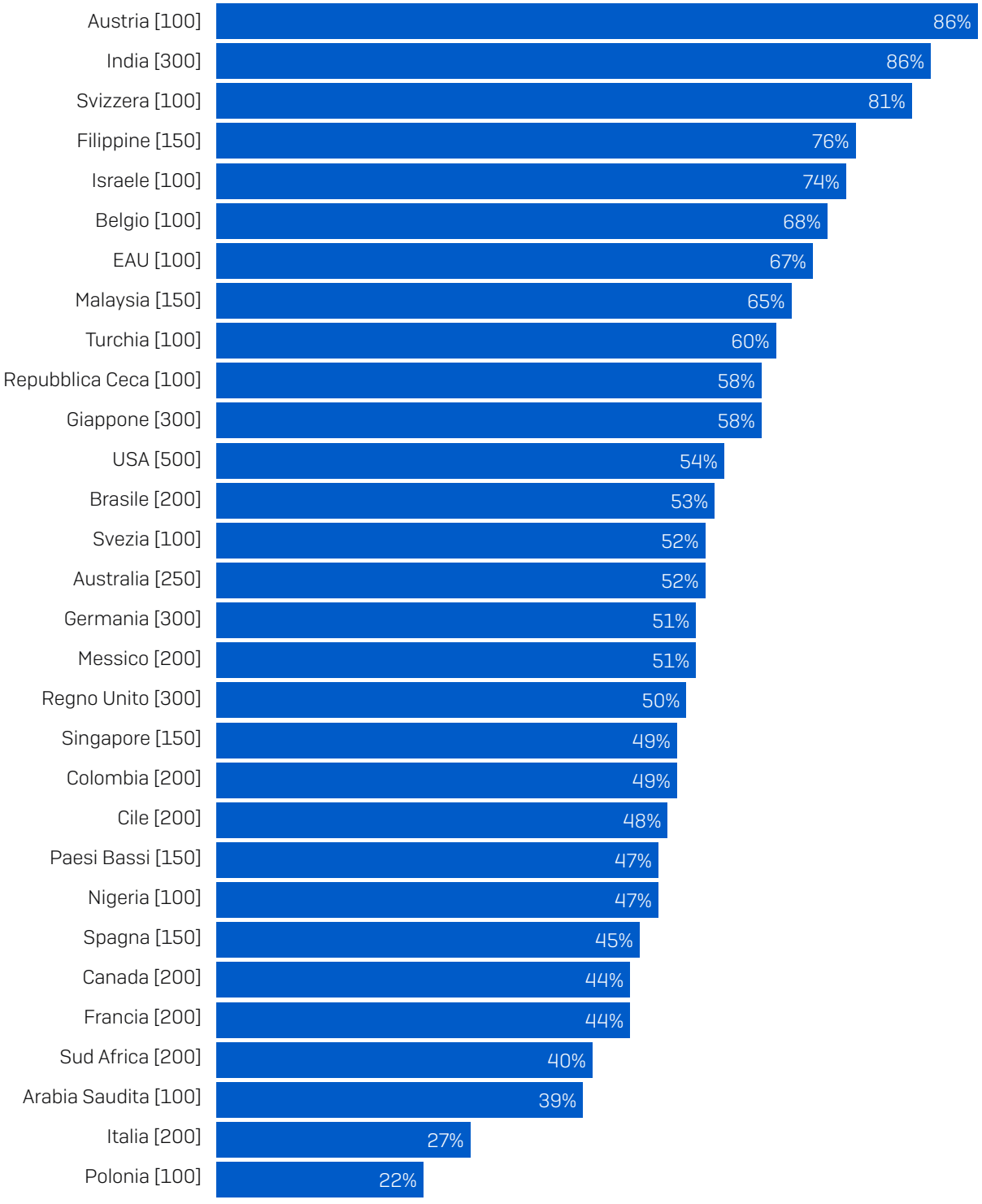


Percentuale che sostiene che gli attacchi informatici sono ora troppo avanzati per essere affrontati dal team IT dell'organizzazione, senza un aiuto esterno

Questa sfida è particolarmente sentita nel settore dei **Servizi commerciali e professionali**, dove il 63% degli intervistati ritiene di non essere più in grado di affrontare gli attacchi informatici senza un aiuto esterno, seguono a distanza ravvicinata gli **Enti del governo centrale ed enti pubblici non ministeriali (NDPB)** (62%) e la **Sanità** (60%). Una tendenza diversa si osserva invece nei settori **Edilizia e immobili** e **Pubblica amministrazione**, con una minore propensione a concordare con questa dichiarazione (47%). Il risultato della Pubblica amministrazione è particolarmente sorprendente, in quanto, come indicato nel rapporto La Vera Storia Del Ransomware 2021, in questo settore è più probabile che gli attacchi ransomware riescano a cifrare i dati.

Trai paesi che hanno partecipato al sondaggio, si nota una variazione significativa nei livelli di fiducia nelle proprie abilità durante un attacco complesso.

Intervistati che ritengono che gli attacchi informatici sono ora troppo avanzati per essere affrontati dal proprio team IT, senza un aiuto esterno



Intervistati che confermano che gli attacchi informatici sono ora troppo avanzati per essere affrontati dal proprio team IT, senza un aiuto esterno [base di partecipanti indicata nel grafico], alcune risposte sono state omesse, suddivisione in base al settore

I partecipanti al sondaggio situati in Austria e in India sono quelli con minore fiducia nelle proprie capacità durante un attacco, con l'86% degli intervistati che dichiara che gli attacchi sono ora troppo complessi per essere affrontati dal proprio team senza un aiuto esterno, seguiti dagli intervistati in Svizzera (81%), nelle Filippine (76%) e in Israele (74%).

Riconoscere la complessità degli attacchi e identificare quando occorre richiedere assistenza esterna è un passo fondamentale nella strategia di difesa contro i moderni attacchi avanzati. I SophosLabs e il team Sophos Managed Threat Response hanno osservato un aumento costante nel numero di attacchi basati sulla combinazione tra automazione e attività di hacking manuale in tempo reale, nel tentativo di aggirare le difese dell'organizzazione. Per bloccare questi attacchi sofisticati occorre la presenza di responsabili della protezione estremamente abili e le organizzazioni fanno sicuramente bene a riconoscere quando non possono contare su queste competenze internamente e devono chiedere un aiuto esterno.

All'estremo opposto del grafico troviamo la Polonia, che dichiara in meno occasioni la difficoltà di gestire internamente gli attacchi informatici: solo il 22% degli intervistati sostiene infatti che gli attacchi sono troppo avanzati per essere gestiti dal proprio team interno, segue a breve distanza l'Italia, con il 27%. Questa fiducia nelle proprie capacità nonostante un numero in costante crescita di attacchi potrebbe essere dovuta all'investimento nell'assumere e nel formare professionisti con competenze tecniche adeguate per far fronte agli hacker. Tuttavia, potrebbe anche indicare un'eccessiva spavalderia di fronte ai moderni attacchi avanzati. Con cybercriminali che adottano approcci sempre più evoluti, è importante essere realistici sulle competenze necessarie per fermarli.

I tempi di risposta sono peggiorati

Visto l'incremento del carico di lavoro, sentito in maniera diffusa nel 2020, e considerando le sfide derivate dal doversi adattare alla pandemia, probabilmente non sorprende che gran parte dei partecipanti al sondaggio (61%) abbia riportato un aumento nei tempi di risposta ai casi IT in questo periodo. Il 20% dichiara di aver notato una diminuzione dei tempi di risposta, mentre per il 19% degli intervistati i tempi sono rimasti uguali.

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 [5.400], la risposta "Non lo so" è stata omessa

L'aumento dei tempi di risposta è un fenomeno maggiormente diffuso nel settore dell'**Istruzione**, dove il 65% degli intervistati ha riportato di aver notato un incremento. Gli istituti di istruzione in molti paesi sono dovuti passare alla didattica a distanza nel 2020 e questo ha generato una mole di lavoro non indifferente per i team IT. L'impatto è stato particolarmente sentito nella loro capacità di rispondere rapidamente alle richieste di supporto.

Mass media, tempo libero e intrattenimento è stato il settore che ha riportato maggiormente una diminuzione nei tempi di risposta, con quasi un terzo (32%) degli intervistati che dichiara di aver risposto più rapidamente alle richieste di supporto. Anche in questo caso, è probabile che uno dei principali fattori determinanti sia stata la pandemia: con meno attività di produzione, il team IT ha avuto più tempo per rispondere con maggiore rapidità.

L'impatto del 2020 sui team IT

Ma non ci sono solo cattive notizie. Osservando i team IT, si notano anche molti dati incoraggianti. Il 70% dei responsabili IT sostiene che le capacità del proprio team di sviluppare competenze e conoscenze di cybersecurity è aumentata nel 2020. Solo il 12% degli intervistati dichiara di aver notato una diminuzione.

Cambiamenti nella capacità di sviluppare ulteriormente competenze e conoscenze di cybersecurity nel 2020

Nel 2020, la capacità di sviluppare ulteriormente le nostre competenze e conoscenze di cybersecurity è aumentata/diminuita/rimasta la stessa [5.400], la risposta "Non lo so" è stata omessa

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

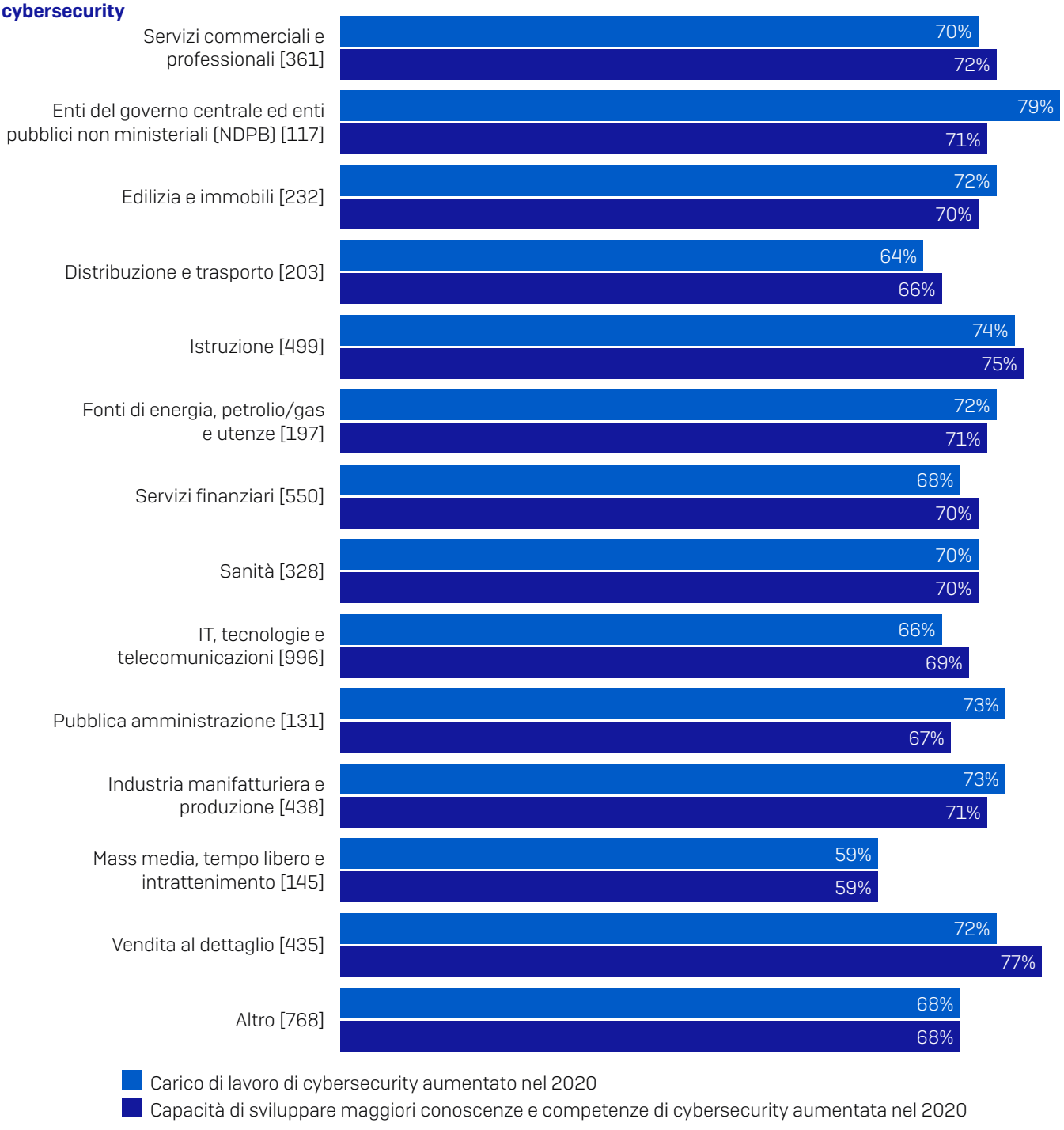
È interessante notare come diversi settori particolarmente colpiti dalla pandemia abbiano vissuto esperienze contrastanti:

- La **Vendita al dettaglio** è stato il settore che ha maggiormente accresciuto le proprie competenze e conoscenze di cybersecurity (77%). Molto probabilmente, il passaggio alla vendita online durante il lockdown è stato significativo nel generare nuove sfide ma anche nuove opportunità di crescita per i team IT di questo settore.
- L'**Istruzione** si trova al secondo posto in termini di aumento delle competenze e conoscenze di cybersecurity (75%). Anche questo è un settore che ha subito trasformazioni notevoli l'anno scorso. Sebbene adottare la didattica a distanza abbia indubbiamente rappresentato una sfida significativa per i team IT, ha anche generato un'enorme opportunità di sviluppo.
- **Mass media, tempo libero e intrattenimento** hanno segnalato la percentuale minore di sviluppo delle competenze (59%). Poiché questo settore ha anche riportato la percentuale più elevata di intervistati che hanno osservato una diminuzione del carico di lavoro (di cybersecurity e non), è molto probabile che i bassi livelli di attività abbiano anche limitato le opportunità di sviluppo.

L'aumento del carico di lavoro ha portato da uno sviluppo delle conoscenze e delle competenze

Complessivamente, i dati hanno rivelato una correlazione diretta tra l'aumento del carico di lavoro di cybersecurity e lo sviluppo di maggiori conoscenze e competenze di cybersecurity in tutti i settori.

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

Tra i partecipanti che hanno notato un incremento del carico di lavoro di cybersecurity nel 2020, l'84% ha anche dichiarato di aver sviluppato maggiormente le proprie competenze e conoscenze di cybersecurity. Analogamente, più di otto intervistati su dieci (82%) tra quelli che sostengono di aver osservato un aumento degli attacchi informatici contro la propria organizzazione hanno anche registrato un aumento delle proprie capacità di sviluppare competenze e conoscenze di cybersecurity. Sembra esserci un nesso logico: se da un lato l'aumento del carico di lavoro e degli attacchi informatici mette i team sotto pressione, dall'altro offre anche ottime opportunità di sviluppo di nuove competenze.

Il morale dei team è più alto

Più della metà dei responsabili IT intervistati (52%) sostiene che nel 2020 il morale del proprio team è migliorato. Il 26% ha dichiarato che è peggiorato e il 22% che è rimasto uguale.

Cambiamenti nel morale dei team nel 2020

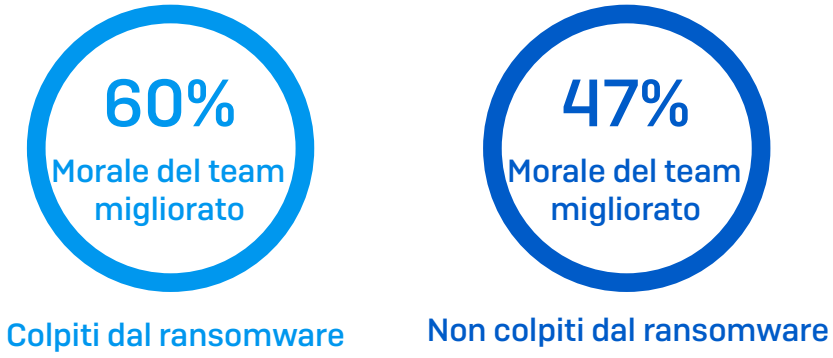
Nel 2020 il morale del nostro team è migliorato/peggiorato/rimasto lo stesso [5.400], la risposta "Non lo so" è stata omessa

Geograficamente, il morale è migliorato maggiormente in Turchia (75%), Austria (71%) e India e Sud Africa (entrambe 69%). All'estremo opposto della classifica, i team IT in Israele (26%), Francia (31%), Italia (33%) e Polonia (36%) sono quelli con la minore probabilità di osservare un miglioramento nel morale dei team.

Si noti che molti dei paesi messi in evidenza in questo paragrafo sono stati protagonisti anche in sezioni precedenti di questo documento. Turchia e Austria, che hanno la percentuale più elevata di intervistati che sostengono di aver notato un miglioramento nel morale del proprio team, erano tra i quattro paesi che hanno registrato un aumento del numero di attacchi informatici. Analogamente, la Francia si trova al penultimo posto tra le percentuali di partecipanti che hanno osservato un miglioramento del morale, ed è anche il paese con il minore aumento di attacchi informatici. La correlazione tra le esperienze di attacco informatico e il morale dei team è uno dei risultati più salienti emersi dal sondaggio.

A ulteriore dimostrazione di questo punto, il 60% degli intervistati provenienti da organizzazioni colpite da un attacco di ransomware nei 12 mesi precedenti ha osservato un miglioramento del morale del proprio team. Si confronti questo dato con il 47% delle organizzazioni non colpite da un attacco.

Cambiamenti nel morale dei team nel 2020

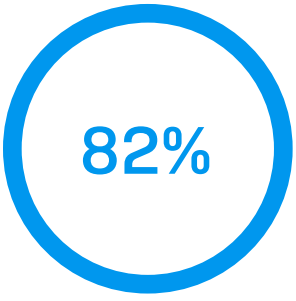


Nel 2020 il morale del nostro team è migliorato/peggiorato/rimasto lo stesso [5.400], alcune risposte sono state omesse, suddivisione in base ai partecipanti provenienti da organizzazioni colpite dal ransomware l'anno scorso

I potenziali fattori alla base di questa correlazione sono diversi. Spesso le avversità, in questo caso gli attacchi informatici, offrono l'opportunità di stringere rapporti più stretti e di lavorare insieme verso un unico obiettivo, contribuendo così al miglioramento del morale. Inoltre, essere in grado di fornire sostegno all'organizzazione di fronte a un maggiore rischio di attacco produce un senso di soddisfazione.La percentuale più elevata di miglioramento del morale è stata registrata nei due settori che hanno subito maggiormente l'impatto della pandemia, con l'**Istruzione** al primo posto (58%), seguita a distanza ravvicinata dalla **Sanità** (57%).

Allo stesso tempo, il ruolo fondamentale svolto dai team IT nel mantenere la continuità del business durante la pandemia potrebbe aver contribuito ad aumentare la consapevolezza e la stima verso il loro lavoro, un altro fattore che mantiene alto il morale. Se in passato il valore dei team IT è stato sottovalutato, ora è il momento di riconoscerne l'importanza.

I team IT si sentono adeguatamente preparati per le sfide future



Percentuale che sostiene di avere gli strumenti e le conoscenze necessari per svolgere indagini esaustive sulle attività sospette

Intervistati che, se vengono rilevate attività sospette nell'organizzazione, concordano di avere gli strumenti e le conoscenze necessari per svolgere indagini esaustive [5.400], alcune risposte sono state omesse

Di fronte all'aumento del carico di lavoro e della frequenza degli attacchi informatici nel 2020, un dato incoraggiante è che l'82% dei responsabili IT sostiene di avere gli strumenti e le conoscenze necessari per svolgere indagini esaustive sulle attività sospette, se dovessero essere rilevate all'interno dell'organizzazione. Le opportunità di sviluppare competenze e conoscenze nel 2020 hanno dotato i team delle giuste risorse per affrontare le sfide future. Continuare a investire in strumenti e formazione è essenziale per fare in modo che i team IT possano far fronte alla costante evoluzione degli attacchi informatici.

Tuttavia, osservando la risposta a questa domanda in base al settore, emergono due eccezioni: **Enti del governo centrale ed enti pubblici non ministeriali (NDPB)** (67%) e **Pubblica amministrazione** (64%). Gli enti governativi in tutto il mondo sono stati pesantemente colpiti dagli effetti della pandemia. Hanno dovuto garantire la continuità di servizi essenziali per un periodo esteso di disagio, e allo stesso tempo erano tenuti a fornire maggiore assistenza sia ai cittadini che alle organizzazioni. Allo stesso tempo, il problema della mancanza di fondi per il settore pubblico è una sfida che dura da anni in molti paesi ed è un fattore che potrebbe limitare le risorse disponibili. Poiché i cybercriminali che sferrano attacchi di ransomware puntano molto sugli enti governativi, è essenziale che questi ultimi dispongano delle risorse e delle competenze necessarie per svolgere indagini adeguate sulle attività sospette.

Il futuro dei team di IT security

Come abbiamo visto, l'anno scorso è stato un anno particolarmente difficile per molti professionisti dell'IT. Tuttavia, i tecnici IT hanno raccolto e superato la sfida del 2020 in modo encomiabile, migliorando come risultato sia le proprie competenze che il morale del team. Queste esperienze, insieme ai grandi cambiamenti nel panorama informatico (come ad esempio l'incremento delle modalità di lavoro flessibili e l'utilizzo del cloud), avranno un impatto diretto sul team di IT security del futuro.

Ci sarà un aumento del personale nei team di IT security e sarà rapido

Di fronte alle sempre più pressanti richieste rivolte ai team IT, gli intervistati prevedono un aumento significativo del personale di IT security interno ed esterno, soprattutto nei prossimi due anni:

- Il 68% si attende un incremento del personale interno nei prossimi due anni, mentre il 76% lo attende nei prossimi cinque anni
- Il 56% prevede un incremento del personale IT esterno nei prossimi due anni, mentre il 64% prevede un aumento nei prossimi cinque anni
- Solo l'8% ritiene che il personale diminuirà nei prossimi cinque anni

Risorse di IT security	Cambiamento previsto	Entro il 2023	Entro il 2026
Personale di IT security interno	Incremento	68%	76%
	Diminuzione	11%	8%
Personale di IT security esterno	Incremento	56%	64%
	Diminuzione	14%	10%

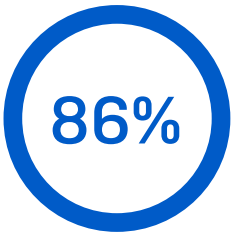
Quali cambiamenti prevedete per le dimensioni del team di IT security della vostra organizzazione entro il 2023 ed entro il 2026? [5.400], alcune risposte sono state escluse

È interessante notare come la crescita del personale IT esterno non influisce sui team interni. Quasi la metà (46%) degli intervistati si attende un incremento sia del personale di IT security interno che esterno entro il 2023, e la percentuale raggiunge il 55% per le previsioni per il 2026.

Complessivamente, il 77% dei partecipanti al sondaggio si aspetta una crescita in almeno uno degli ambiti delle risorse di IT security (personale interno o esterno) nei prossimi due anni, e questa statistica sale al 85% per il 2026.

L'intelligenza artificiale è un fattore essenziale

Percentuale che prevede che l'intelligenza artificiale aiuterà a gestire l'incremento della quantità di attacchi



Percentuale che prevede che l'intelligenza artificiale aiuterà ad affrontare la maggiore complessità degli attacchi

Intervistati che confermano di prevedere che le tecnologie di intelligenza artificiale aiuteranno a gestire l'incremento della quantità di attacchi e/o ad affrontare la maggiore complessità degli attacchi [5.400], alcune risposte sono state omesse

Quasi universalmente, i team IT si affidano alle tecnologie di intelligenza artificiale per contrastare minacce informatiche sempre più numerose. L'86% degli intervistati prevede che le tecnologie di intelligenza artificiale aiuteranno a gestire l'incremento della quantità di attacchi e la stessa percentuale prevede che le tecnologie di intelligenza artificiale aiuteranno ad affrontare la maggiore complessità degli attacchi. Il 92% degli intervistati ha selezionato almeno una di queste opzioni.

Cominciare oggi a creare il team di IT security di domani

Per creare il team IT di domani, occorre cominciare subito. Consigliamo alle organizzazioni di utilizzare questi approfondimenti provenienti da esperti che lavorano in prima linea per predisporsi al successo in ambito di cybersecurity nel 2023 e in futuro. Prendendo spunto da ciò che abbiamo appreso in questo rapporto, Sophos offre cinque raccomandazioni:

1. Implementare strumenti e approcci che riducano il carico di lavoro degli amministratori IT

L'aumento del carico di lavoro correlato o meno alla sicurezza osservato l'anno scorso è evidente. Consigliamo alle organizzazioni di cercare di implementare strumenti e approcci che riducano il carico di lavoro dell'IT security, per concedere ai team più tempo da dedicare ad altre attività.

- **Automazione.** Approfittare dell'automazione può aiutare a ridurre la mole di lavoro delle normali operazioni quotidiane, che sottraggono tempo prezioso ed energia ai professionisti dell'IT, i quali non possono pertanto dedicarsi a progetti strategici. I computer sono immancabilmente più rapidi degli operatori umani. Inoltre, aiutano ad accelerare i tempi di risposta eD a diminuire l'esposizione ai rischi.
- **Unione.** Le mansioni amministrative quotidiane possono essere semplificate gestendo tutte le soluzioni di cybersecurity da un'unica console unificata. Poter controllare tutti i componenti da un'unica schermata permette di eliminare il bisogno di passare da una console all'altra per gestire la sicurezza e correlare i dati tra sistemi diversi. Questa strategia aiuta i team IT a risparmiare tempo e fatica. Inoltre, unificare l'IT security consente di risparmiare sui costi di gestione di più vendor.
- **Integrazione.** Le soluzioni ideali sono quelle dotate di capacità di integrazione e progettate per interagire reciprocamente. Optando per questi tipi di soluzioni, è possibile incrementare sia la capacità di automatizzare le operazioni semplificando le indagini su più prodotti, sia la compilazione di analisi approfondite sullo stato di sicurezza generale.

2. Investire in strumenti e formazione che permettano ai team IT di utilizzare le nuove competenze acquisite

L'anno scorso, si è osservato uno sviluppo significativo delle competenze e delle conoscenze dei team IT. Alle organizzazioni consigliamo di investire in strumenti e corsi di formazione che permettano a questi dipendenti di utilizzare le nuove competenze acquisite e di continuare ad apprendere. Queste risorse aiutano anche a trovare nuovi talenti da inserire nel team.

3. Utilizzare una combinazione di competenze tecniche interne ed esterne

Le minacce informatiche sono già troppo complesse per più della metà dei responsabili IT, che sostengono di non poterle affrontare senza un aiuto esterno. E in futuro non faranno altro che diventare più complicate. Unendo alle abilità dei propri team di sicurezza interni le competenze di professionisti esterni, è possibile usufruire di vantaggi su entrambi i fronti: da un lato professionisti specializzati nel combattere le minacce e dall'altro esperti che conoscono bene l'organizzazione da proteggere. Questa struttura combinata facilita anche le capacità di adattamento e risposta ai cambiamenti, per fare in modo che ogni situazione venga gestita dalle persone più appropriate. Consigliamo alle organizzazioni di rivolgersi a Partner di IT security in grado di svolgere il ruolo di "estensione" del team tecnico, fornendo competenze che non sono disponibili internamente. Questi Partner devono avere la flessibilità di adattarsi al modello operativo scelto dall'organizzazione.

4. Predisporsi per attirare i migliori talenti a livello globale

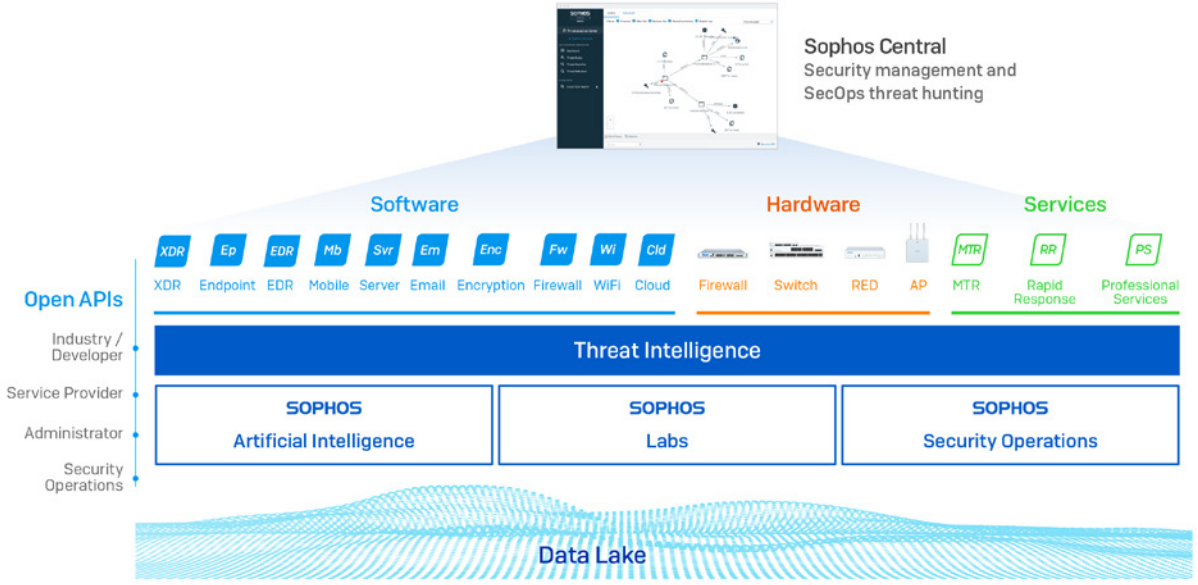
Visto che la maggior parte delle organizzazioni cerca personale da inserire nei propri team IT, c'è molta competizione per assumere i migliori talenti. L'adozione di tecnologie innovative che possono essere gestite da qualsiasi luogo aiuta a estendere il pool di talenti da cui attingere. La pandemia ha dimostrato che quasi tutti i ruoli IT possono essere svolti da remoto, se necessario. In più, la disponibilità di strumenti di elevata qualità renderà l'organizzazione un posto di lavoro molto più attraente per i candidati più abili.

5. Impostare una pipeline per il team di IT security interno

I talenti nel mondo dell'IT security sono limitati. Oltre ad impegnarsi per estendere il pool di talenti da cui attingere, le organizzazioni devono anche impostare una pipeline con programmi interni volti alla formazione e allo sviluppo del proprio team IT, come ad esempio apprendistati e tirocini supervisionati. Sebbene l'immagine di un giovane che indossa una felpa con cappuccio, chinato sul computer in camera sua non sia che uno stereotipo, è bene ricordare che molte persone riescono a sviluppare competenze informatiche avanzate in ambiti diversi dalle tradizionali carriere professionali.

Sophos vi può aiutare, ecco come

Sophos assiste i team IT in più di 500.000 organizzazioni e 150 paesi, per aiutarli a difendere le proprie organizzazioni contro le minacce informatiche.



Sophos Adaptive Cybersecurity Ecosystem (ACE)

- Offriamo una gamma completa di **soluzioni di ultima generazione** con tecnologie di **intelligenza artificiale.** I nostri prodotti sono realizzati per interagire in maniera ottimale, nonché per automatizzare le operazioni manuali e limitare l'esposizione alle minacce. Questo sistema prende il nome di Synchronized Security. I clienti che utilizzano la nostra protezione endpoint e firewall riportano una riduzione di almeno il 50% nelle attività di gestione quotidiana, oltre a una minore quantità di incidenti di sicurezza.
- **Sophos Extended Detection and Response (XDR)** e **Sophos Endpoint Detection and Response (EDR)** offrono ai team IT gli strumenti necessari per identificare rapidamente e porre rimedio alle minacce e ai problemi di integrità del sistema informatico. Sophos EDR è la prima soluzione EDR progettata per gli analisti di sicurezza e gli amministratori IT, che permette ai team IT di incrementare le proprie competenze senza dover assumere altro personale.
- Tutte le tecnologie Sophos Next-Gen sono gestite dalla piattaforma di sicurezza **Sophos Central**, uno strumento basato sul web che consente alle organizzazioni di poter contare sui migliori talenti di cybersecurity, indipendentemente da dove si trovino.
- I team **Sophos Managed Threat Response (MTR)** e **Sophos Rapid Response** mettono a disposizione competenze avanzate di threat hunting e risposta agli incidenti, per aiutare i team interni, il servizio viene fornito in modalità completamente gestita. Le organizzazioni mantengono pieno controllo su come e quando effettuare l'escalation dei potenziali incidenti e su quali azioni di risposta desiderano da noi (sempre che le vogliano intraprendere).
- Il nostro sistema di protezione è basato sui dati collettivi di intelligence sulle minacce raccolti dai **SophosLabs, dai team Sophos Security Operations** e **Sophos Ai** e dal **Sophos Data Lake**.
- Le **API aperte** permettono a tutti i clienti di usufruire dei dati e della telemetria dei nostri Partner in tutto il mondo.

Per scoprire di più su come funzionano i nostri sistemi e servizi e per discutere delle sfide affrontate dal vostro team, visitate il nostro sito web o rivolgetevi a un rappresentante Sophos.

Per scoprire di più su come funzionano i nostri sistemi e servizi e per parlare delle sfide affrontate dal vostro team, visitate il nostro sito web o rivolgetevi a un rappresentante Sophos.

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.

25/06/2021 (WP-NP)

SOPHOS