Situazione del mercato

Il nuovo panorama delle minacce

Il futuro della sicurezza degli MSP

N-ABLE™

Un report indipendente commissionato da N-able

Adattarsi a un ambiente in continua evoluzione

I provider di servizi IT gestiti (MSP) hanno affrontato sfide uniche durante la pandemia. In molti casi, si sono accollati la responsabilità di garantire che i clienti fossero in grado di continuare a lavorare in una situazione incerta e in continua evoluzione. Al contempo, hanno dovuto anche adattarsi per continuare a operare e sopravvivere.

I criminali informatici hanno immediatamente sfruttato il momento come una succulenta opportunità e, infatti, da inizio pandemia, è stato registrato l'aumento degli attacchi informatici. Gli MSP si sono trovati a essere sempre più spesso i principali bersagli di tali attacchi, poiché i criminali hanno tentato di sfruttare il loro rapporto con i clienti per infiltrarsi nei sistemi e sottrarre dati sensibili.

In risposta a tale ambiente in continua evoluzione, N-able ha pubblicato un report annuale di valutazione (in associazione con Coleman Parkes Research), nel tentativo di illustrare il ruolo degli MSP e il contributo fondamentale che offrono nel proteggere le aziende dei clienti. Il documento, inoltre, spiega come gli MSP saranno interessati in modo diretto dalle minacce per la sicurezza, illustra le tendenze nel settore della sicurezza informatica da conoscere e spiega su cosa dovranno concentrarsi gli MSP quando implementano le necessarie tecnologie informatiche per tenere al sicuro le proprie aziende e quelle dei relativi clienti.

In realtà, a prescindere dal settore in cui operano, le aziende non sono più soltanto aziende ormai, ma componenti fondamentali dell'infrastruttura e della supply chain globali. Questo le rende tutte bersagli ideali. Sono tutte sulla stessa barca.

RIEPILOGO ESECUTIVO DEI RISULTATI DEL REPORT:[1]

- Gli MSP stanno rapidamente diventando i bersagli principali degli attacchi informatici
- Quasi tutti gli MSP sono stati vittime di un attacco informatico andato a buon fine negli ultimi 18 mesi e il 90% di loro ha registrato l'aumento degli attacchi da inizio pandemia
- L'82% dei clienti degli MSP ha registrato l'aumento dei tentativi di attacco informatico
- Gli MSP stanno incrementando i budget per la sicurezza in media del 5%. Basterà?
- L'automazione delle funzioni chiave è fondamentale per tenere alla larga i criminali informatici
- Sebbene il servizio di backup sia essenziale, solo il 40% degli MSP sottopone a backup le workstation ogni 48 ore o meno e questo dato deve migliorare
- Con solo il 40% che ha implementato l'autenticazione a due fattori sui propri sistemi, gli MSP devono ancora concentrarsi sugli aspetti di base
- I budget per la sicurezza delle aziende di piccole e medie dimensioni stanno aumentando, il che consente agli MSP di vendere di più e di erogare servizi avanzati

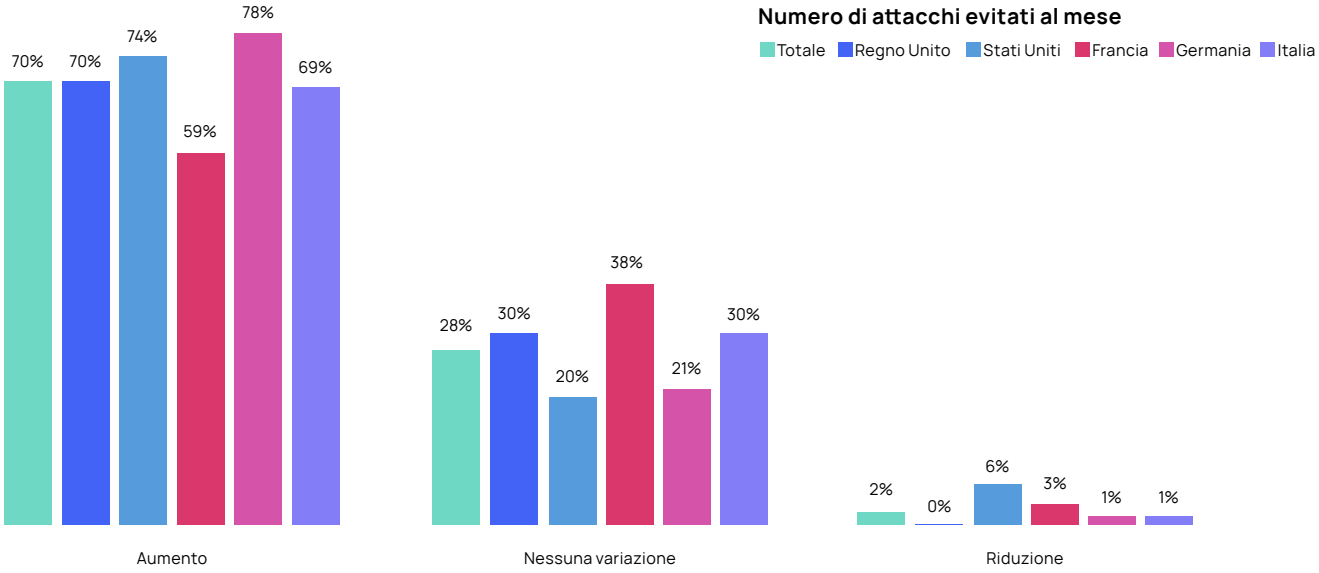
[1]Tutte le statistiche presenti nel documento si basano sui risultati di una ricerca indipendente commissionata da N-able.

Le piccole e medie imprese stanno incrementando i budget per la sicurezza

Prima di esaminare come dovrebbe cambiare la loro strategia per la sicurezza, gli MSP devono considerare come verranno pagati per i loro servizi. Molte aziende, infatti, hanno vissuto due anni incredibilmente duri e, sebbene tutti sappiano quanto sia importante una strategia di sicurezza avanzata, al momento potrebbe essere un investimento impraticabile per molte PMI.

Ma c'è una buona notizia. Secondo il nostro report, la maggioranza delle PMI (il 70%) sta pensando di incrementare il budget destinato alla sicurezza. L'unica eccezione è la Francia, ma anche lì la percentuale di PMI che intendono aumentare il budget è pari al 60%.

Delle restanti aziende, la maggioranza destinerà alla sicurezza lo stesso importo, mentre il 2% pensa di ridurlo. Gli aumenti sono sostanziali, in media del 7%. Date le circostanze recenti, si tratta di un investimento consistente finalizzato alla sicurezza.



Per gli MSP, questo significa una grande opportunità. Non dovranno, infatti, impegnarsi molto per convincere la maggior parte dei clienti che la sicurezza è importante e che richiede investimenti; piuttosto, la conversazione dovrà riguardare come utilizzare questi investimenti e come sfruttarli al massimo.

Le PMI sono desiderose di investire questo budget maggiore nella sicurezza dei dati e nella sicurezza su cloud, mentre l'accesso tramite identità è più in fondo nella lista di priorità. Gli MSP devono sicuramente basarsi sull'input dei clienti quando propongono loro servizi aggiuntivi e avanzati, ma devono anche ricordare che sono loro gli esperti.

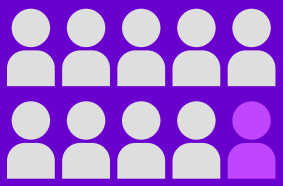
- Sicurezza dei dati
- Sicurezza su cloud
- Protezione delle infrastrutture
- Servizi di sicurezza
- Attrezzature per la sicurezza di rete
- Sicurezza delle applicazioni
- Sicurezza integrata per i rischi
- Sicurezza per l'accesso tramite identità

Gli attacchi ai danni degli MSP sono in aumento

Gli attacchi informatici occupano le prime pagine dei giornali. Sono stati registrati imponenti attacchi ransomware che hanno paralizzato supply chain e utenze pubbliche in tutto il mondo.

Gli MSP sono da sempre considerati un potenziale vettore di attacco poiché costituiscono un comodo punto di ingresso nella supply chain, il che consente ai criminali informatici di compromettere i relativi sistemi e di avere accesso a dati sensibili e sistemi dei clienti. Il valore degli MSP è aumentato significativamente agli occhi dei criminali informatici, grazie agli effetti della pandemia e alla possibilità di utilizzare come arma i software di monitoraggio e gestione da remoto per sferrare un'ampia gamma di attacchi, ad esempio la compromissione delle e-mail aziendali e gli attacchi ransomware. Questo cambio di rotta da parte dei criminali informatici persisterà anche in futuro.

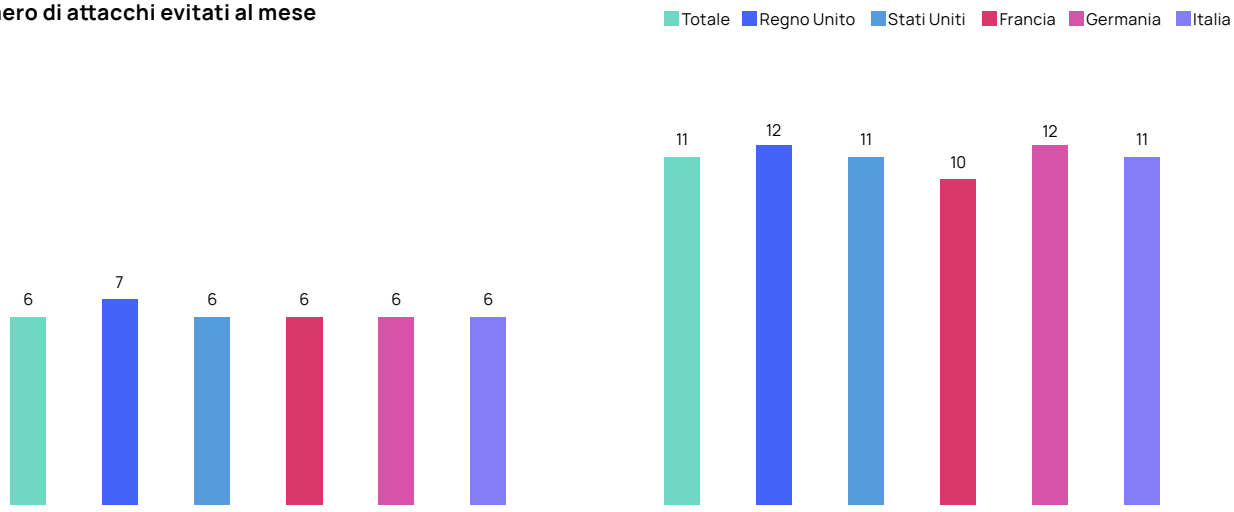
Una ragione per cui gli MSP continuano a essere considerati come veri e propri vettori di attacco è che ormai troppi attacchi vanno a buon fine. Secondo il report, quasi tutti gli MSP sono stati vittime di un attacco informatico andato a buon fine negli ultimi 18 mesi e il 90% di loro ha registrato l'aumento degli attacchi da inizio pandemia. Per giunta, un terzo degli MSP solo nell'ultimo trimestre è stato vittima di un attacco andato a buon fine. È anche importante notare che il numero di attacchi che questi MSP stanno evitando è quasi raddoppiato, da 6 a 11.



9 persone su 10

Il 90% dei partecipanti ha registrato un aumento del numero di attacchi da inizio pandemia.

Numero di attacchi evitati al mese



Numero medio di attacchi al mese **PRIMA** della pandemia

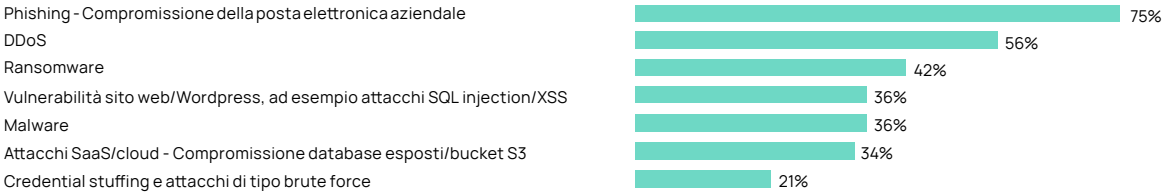
Numero medio di attacchi al mese **DALLA** pandemia

Risposta singola

Base: partecipanti al sondaggio che hanno registrato un aumento degli attacchi informatici (451) Regno Unito (86) Stati Uniti (85) Francia (92) Germania (90) Italia (98)

Attacchi e vettori di attacco

Tipi di attacchi più di frequente mirati



Gli MSP che hanno partecipato al sondaggio hanno segnalato la proliferazione degli attacchi in queste tre aree principali (con alcune variazioni in base all'area geografica):

1. PHISHING

Il phishing è il più comune vettore di attacco, con Italia (86%) e Francia (82%) che registrano il maggior numero di attacchi in quest'area.

2. DDOS

Gli attacchi DDoS rappresentano un vettore sempre più popolare negli Stati Uniti, con il 65%.

3. RANSOMWARE

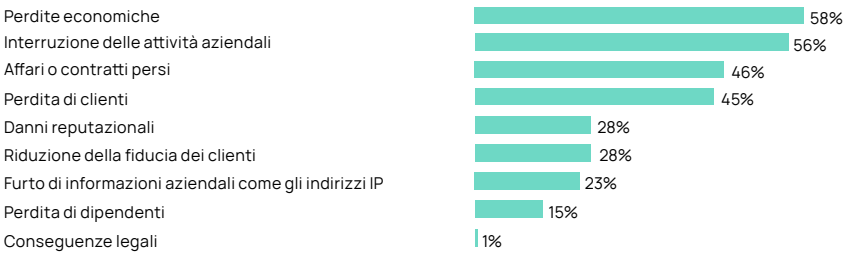
In linea con l'elevato numero di incidenti informatici registrati quest'anno, il 55% degli MSP statunitensi dichiara di essere spesso bersaglio di attacchi ransomware rispetto al solo 34% degli MSP del Regno Unito.

Costo della protezione dei clienti

Gli MSP dichiarano che l'82% dei loro clienti ha registrato l'aumento dei tentativi di attacco informatico. Se da un lato è aumentato il numero dei tentati attacchi informatici, la tendenza è la stessa anche per il numero medio di quelli sventati da inizio pandemia: 14 al mese rispetto agli 8 al mese prima del Covid.

Questi attacchi hanno un impatto devastante su MSP e utenti finali, poiché comportano la perdita di clienti, perdite economiche e l'interruzione delle attività aziendali.

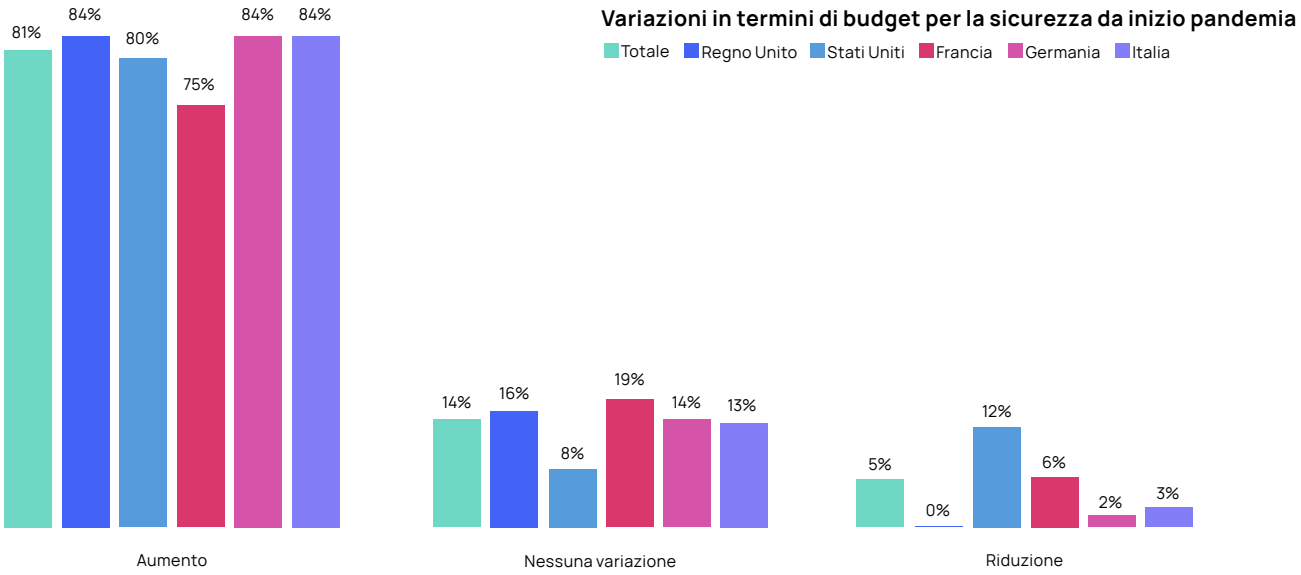
Impatto degli attacchi informatici sulle aziende



Secondo la nostra ricerca, la perdita di clienti ha rappresentato un problema significativo in Francia e Stati Uniti, mentre gli MSP italiani hanno registrato la perdita di fiducia da parte dei clienti. Gli MSP tedeschi e britannici hanno registrato la più seria perdita di dipendenti a causa di un attacco (il 26% per entrambe le aree geografiche).

Gli MSP fanno quello che possono in un momento molto delicato

La situazione è insostenibile, ma gli MSP stanno facendo il massimo. Quattro su cinque MSP che hanno partecipato al sondaggio stanno incrementando il proprio budget di sicurezza (in Francia, solo 3 su 4). L'aumento medio è pari al 5%; **in Francia la percentuale è di poco inferiore, mentre in Germania di poco superiore.** Sarà sufficiente per sventare gli attacchi diretti agli MSP, ormai quasi raddoppiati?



L'81% degli MSP ha incrementato il budget per la sicurezza a seguito della pandemia rispetto al 70% dei clienti che hanno fatto lo stesso. Poiché i clienti degli MSP investono una cifra maggiore (7%), gli MSP possono permettersi di spendere di più per stare al passo?

In che ambito investono gli MSP?

I più comuni strumenti di sicurezza su cui investono gli MSP includono la sicurezza dei dati, la sicurezza su cloud e la protezione delle infrastrutture. L'accesso tramite identità, invece, rappresenta l'investimento meno frequente. I set di strumenti che gli MSP stanno implementando includono crittografia dei dati, antivirus e autenticazione a più fattori. Abbiamo rilevato spunti interessanti anche per quanto riguarda le variazioni per le diverse aree geografiche: gli MSP francesi investono somme ingenti nelle VPN, mentre in Regno Unito e Germania si investe nelle soluzioni di filtri per le e-mail.

È fondamentale implementare un approccio di base

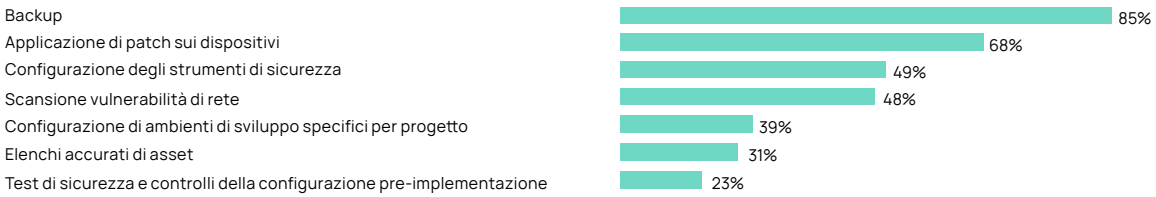
Affinché gli MSP proteggano al meglio i loro clienti, sono diversi gli aspetti di base che vanno implementati, ma che invece in alcuni casi vengono ignorati del tutto.

1. L'AUTOMAZIONE È FONDAMENTALE

Poiché gli attacchi aumentano sia per quanto riguarda il volume che la complessità, la gestione manuale delle difese è impossibile; per questo motivo, implementare maggiori livelli di automazione è essenziale per tenere al sicuro le attività dei clienti. Ecco cosa abbiamo registrato nel settore:

- **L'automazione dei backup** rappresenta la più comune forma di automazione impiegata dagli MSP per tenere al sicuro le attività dei clienti. Viene utilizzata dall'85% dei partecipanti al sondaggio, con oltre il 90% in Francia e Italia.

Automazione per tenere al sicuro le aziende dei clienti



- **Applicazione automatica di patch**: l'80% degli MSP applica le patch in modo automatico.
- **Filtri web**: il 90% degli MSP fornisce filtri web automatizzati, molti dei quali basati su URL. Solo il 10% impiega invece i più sicuri filtri DNS.
- **Test di sicurezza e controlli automatici della configurazione delle nuove implementazioni** vengono impiegati da meno di un quarto degli MSP.

2. IL BACKUP È UNA PROCEDURA FONDAMENTALE, MA BISOGNA MODIFICARNE LA FREQUENZA

Il backup è essenziale come ultima linea di difesa in ogni attacco: gli MSP devono poter ripristinare dati e sistemi dei clienti, a prescindere da quel che succede. In generale, il backup viene fornito alla maggior parte dei clienti, ma il problema principale è che solo il 40% delle aziende sottopone a backup le workstation ogni 48 ore o meno. La situazione è più rosea in Francia, dove questa percentuale aumenta al 60%. Va meglio, invece, per i server che vengono sottoposti a backup più di frequente: ogni 48 ore o meno dal 74% dei partecipanti al sondaggio.

Soprattutto, con un numero sempre maggiore di aziende che trasferiscono le procedure operative su cloud, il backup per Microsoft 365™ viene messo a disposizione dalla maggior parte degli MSP, ma anche qui sono presenti differenze a seconda dell'area geografica: tutti gli MSP offrono questo servizio negli Stati Uniti, ma solo l'87% in Germania.

> "Backup per Microsoft 365 viene messo a disposizione dalla maggioranza degli MSP"

3. L'AUTENTICAZIONE A PIÙ FATTORI VIENE IGNORATA

Se da un lato quasi tutti gli MSP offrono l'autenticazione a due fattori ai clienti, solo il 40% di essi la implementa nella propria attività. E, nonostante venga messa a disposizione, solo un terzo dei clienti la utilizza al momento. Tuttavia, gli MSP segnalano di avere in programma la migrazione del 95% dei clienti all'autenticazione a due fattori entro i prossimi cinque anni, anche se la maggioranza mira a completare l'operazione entro i prossimi due anni.

MSP e relativi clienti sembrano non dare più alcuna priorità alla gestione delle identità. Se da un lato gli MSP devono accontentare in un certo modo i clienti, dovranno affrontare l'argomento di assegnare la priorità a questo componente essenziale di qualsiasi approccio alla sicurezza.

> "Solo un terzo dei clienti utilizza al momento l'autenticazione a due fattori"

PROGRAMMI DI MIGRAZIONE

2021 **2026**

33% → **95%**

La sicurezza informatica degli MSP è nei piani dei governi

Aspetto molto importante per gli MSP, nel contesto dello scenario delineato dal nostro sondaggio, il panorama di sicurezza globale sta cambiando. L'accordo tra i governi francese e statunitense sulla sicurezza informatica sarà esteso a livello internazionale, con una crescente collaborazione tra fornitori di tecnologie, provider di servizi IT ed enti governativi a seguito degli attacchi ad alto profilo delle supply chain nel 2021.

Infatti, l'entità della minaccia degli attacchi alle supply chain che hanno coinvolto gli MSP nel 2021 ha portato diversi governi a intervenire per tentare di mitigare il problema. Ad esempio, il governo britannico sta procedendo con la proposta di un framework di sicurezza informatica per gli MSP. Sostiene che sia necessario adottare "un approccio più interventista per aumentare la resilienza delle supply chain, con la normativa considerata 'molto efficace' da più parti interessate rispetto a qualsiasi altro intervento".[2]

Gli interventi inseriti tra le priorità del governo includono lavori legislativi per garantire che gli MSP adottino " misure di sicurezza informatica ragionevoli e proporzionate".

Questi potrebbero imporre agli MSP di aderire a una serie di principi di sicurezza informatica, ad esempio implementando criteri per proteggere dispositivi e impedire gli accessi non autorizzati. Li obbligheranno anche ad assicurarsi che i dati siano protetti sia in transito sia a riposo. Sostengono inoltre la necessità di mantenere backup dei dati sicuri e accessibili, di formare opportunamente il personale e di favorire l'adozione di una cultura positiva per la sicurezza informatica.

[2]https://www.gov.uk/government/publications/government-response-on-supply-chain-cyber-security

Conclusioni

È il momento per gli eroi rimasti dietro le quinte durante la pandemia di ottimizzare l'approccio alla sicurezza

In molti casi gli MSP si sono occupati di garantire l'operatività delle aziende dei clienti durante la pandemia e di garantire che riuscissero a gestire il passaggio al lavoro da remoto. Pertanto, hanno dimostrato il proprio valore più e più volte, diventando estensioni molto apprezzate dei team IT interni, in particolare quando gli addetti alla sicurezza interni sono stati riallocati per supportare gli addetti all'assistenza che lavoravano da casa.[3]

Proprio per questo motivo, gli MSP non possono permettersi di perdere la fiducia conquistata nell'era del Covid a causa della mancata messa in sicurezza dei propri sistemi. La realtà è che sono un bersaglio di attacco da parte degli hacker molto più frequentemente dei loro clienti, con le stesse modalità. Di certo molti MSP rispondono incrementando i budget destinati alla sicurezza e investendo in nuovi strumenti, ma gli aumenti sono comunque ridotti e potrebbero non essere sufficienti per tenere a bada il maggior numero di attacchi.

Occuparsi delle basi di un'opportuna igiene informatica è essenziale, soprattutto con le normative ufficiali all'orizzonte. Se da un lato è vero che molti MSP possono occuparsi di questo aspetto con i clienti, allo stesso tempo è importante che si espongano in prima linea, implementando le medesime tecnologie utilizzate dai clienti per le proprie attività. Le aree più critiche messe in luce dal sondaggio sono l'uso dell'autenticazione a più fattori, oltre a backup più regolari e all'automazione.

La buona notizia è che molti clienti degli MSP non andranno persuasi circa la necessità di investire in ambito sicurezza, poiché stanno già incrementando i budget e hanno già stabilito le priorità circa gli investimenti che intendono fare. Gli MSP devono continuare a investire sulla sicurezza e collaborare con i clienti per fornire l'approccio alla sicurezza necessario per le proprie attività e per i clienti.

[3](ISC)² Survey Finds Cybersecurity Professionals Being Repurposed During COVID-19 Pandemic (isc2.org)

Nota: tutte le statistiche presenti nel documento si basano sui risultati di una ricerca indipendente commissionata da N-able.