Il valore aggiunto dei Managed Service Provider: sfide e opportunità in uno scenario di sicurezza IT in costante evoluzione

kaspersky

Sommario

Introduzione

Il mercato dei Managed Service Provider (MSP) rappresenta un business molto importante. Ciò che agli inizi era essenzialmente un ruolo di rivenditore IT, per la fornitura, installazione e gestione di una specifica applicazione, ha conosciuto una profonda evoluzione: gli MSP sono ormai divenuti parte integrante della rete di supporto e approvvigionamento IT al servizio delle aziende. Per molte imprese, un MSP rappresenta la naturale estensione del proprio team IT (in alcuni casi costituisce di fatto il team IT a cui si affida l'azienda): spesso colma le lacune in termini di competenze e risorse interne, per garantire che le operazioni IT procedano agevolmente e con successo.

In particolare le PMI affidano agli MSP il ruolo di "trusted advisor" nell'ambito del variegato e mutevole panorama IT, quando le insufficienti competenze interne e i budget limitati impediscono di stare al passo con i tempi. La continua crescita dei servizi cloud, già ampiamente prevista, rappresenta uno dei numerosi esempi in cui si evidenzia l'importante ruolo svolto dagli MSP nell'aiutare le piccole imprese a trarre vantaggio dalle applicazioni cloud-based.

Secondo le previsioni di Gartner, nel 2019 il mercato mondiale dei servizi di cloud pubblico farà segnare una crescita del 17,5%, per totalizzare l'imponente cifra di 214,3 miliardi di dollari USD; vi sono quindi grandi opportunità, per gli MSP, nell'affiancare le aziende per realizzare con successo tali progetti. Di fatto, da qui al 2022, Gartner proietta l'entità e la crescita del mercato relativo al settore dei servizi cloud su cifre superiori di quasi tre volte rispetto alla crescita prevista per i servizi IT di carattere generale.

Non costituisce quindi motivo di particolare sorpresa il fatto che, secondo i dati recenti, si preveda una sensibile crescita del mercato dei servizi IT gestiti, dagli attuali 180,5 miliardi di dollari USD ai 282 miliardi attesi entro il 2023. Questo è in gran parte dovuto al fatto che le organizzazioni si affidano agli MSP per "massimizzare la produttività aziendale e soddisfare la crescente richiesta di servizi gestiti cloud-based". Un altro fattore chiave in relazione a questo improvviso incremento è costituito dall'effettivo valore associato all'outsourcing in termini di servizi IT e gestione della sicurezza.

Senza ombra di dubbio i cyberattacchi nei confronti delle aziende sono in costante aumento: questo fa sì che si accresca di continuo il livello di consapevolezza, all'interno delle imprese, riguardo ai rischi e alle conseguenze prodotti da eventuali data breach o da attacchi ransomware diretti alle attività di business. Molti dei casi pubblicamente noti riguardano i data breach subiti dalle aziende Enterprise. Tuttavia, le società di minori dimensioni, al pari di quelle facenti parte della supply chain, risultano altrettanto vulnerabili: in entrambi i casi vi sono serie conseguenze.

La tecnologia, di fatto, è l'asse portante di ogni azienda, indipendentemente dalle dimensioni o dal settore in cui opera l'impresa: sulla base di tale presupposto mantenere il passo con le applicazioni più innovative e con la rapida evoluzione delle minacce informatiche può di sicuro rappresentare una seria sfida. Ciò è vero in particolar modo per le società che non hanno budget o risorse paragonabili, per entità, alle effettive disponibilità delle aziende Enterprise. In effetti, una recente ricerca condotta da Kaspersky ha evidenziato come le aziende con meno di 500 dipendenti siano più inclini a rivolgersi ai fornitori di servizi in outsourcing, al fine di assicurare un'efficace gestione e una solida protezione delle proprie infrastrutture IT. Il 40% ricorre all'outsourcing per quanto riguarda la gestione dei sistemi IT, mentre il 33% esternalizza a una terza parte l'implementazione di una valida soluzione di sicurezza IT.

Percentuali così elevate suggeriscono che, in presenza di budget e risorse limitati, le aziende sono solite adottare quale migliore soluzione il ricorso a uno o più esperti esterni. Simili circostanze generano enormi opportunità per gli MSP, largamente evidenziate dalle elevate stime di crescita del mercato globale; tuttavia, presentano al tempo stesso sfide particolarmente delicate per i provider, sempre oggetto di enormi aspettative quando si tratta di colmare il divario in termini di competenze specifiche; a tutto questo si aggiunge il fattore della cattiva reputazione che questi ultimi possono acquisire nel caso in cui intervengano violazioni dei sistemi informatici aziendali o imprevisti tempi di inattività.

Al fine di aiutare a comprendere la reale portata delle attuali sfide e opportunità che attendono gli MSP di tutta Europa, il presente report esamina con la dovuta attenzione sia le dinamiche di un mercato in continua evoluzione, sia l'impatto generato sul settore MSP dalle mutevoli esigenze della clientela. Il documento cerca di fornire consigli e raccomandazioni per gli MSP, per far sì che i provider di servizi gestiti possano trarre vantaggio da tali opportunità, mantenendo relazioni a lungo termine con i clienti indipendentemente dalle sfide da affrontare.

Risultati principali

- L'outsourcing IT, e in particolar modo l'esternalizzazione della sicurezza informatica, rappresenta un fenomeno in evidente espansione. In Europa un terzo (33%) delle aziende con meno di 500 dipendenti sta attualmente ricorrendo all'outsourcing per quanto riguarda la gestione della propria sicurezza IT; il 21% prevede invece di farlo nel corso dei prossimi 12 mesi.
- Il trend a esternalizzare è in gran parte dovuto alla carenza di competenze interne e al fatto che le aziende desiderano sfruttare al massimo i budget IT disponibili. La metà (51%) si avvale dell'outsourcing per integrare le competenze interne, mentre il 52% ritiene che lavorare in base a tale schema contribuisca in modo significativo a ridurre i costi relativi alla sicurezza.
- Quando si riducono i budget IT le aziende si orientano naturalmente verso l'outsourcing, da esse considerato il modo più efficiente, in termini di costi, per garantire valore di business e supportare le future esigenze di gestione in materia di sicurezza IT.
- Tre quarti (75%) degli MSP ammettono che soddisfare le esigenze dei clienti è una sfida fondamentale; i due terzi (68%) incontrano difficoltà nel mantenere la redditività nelle relazioni con i clienti a causa di un eccesso di risorse atte ad affrontare i problemi di sicurezza degli utenti.
- Godere di ottima reputazione sul mercato è la chiave per attrarre e fidelizzare i clienti: l'83% degli MSP fa quindi affidamento sul passaparola e sui consigli ricevuti; inoltre, per aumentare la propria base di clienti, il 50% conta sulla forza vendita che mantiene un rapporto diretto con i clienti, mentre il 48% ricorre alla sponsorizzazione di eventi.
- Lo stesso avviene quando gli MSP selezionano un partner specializzato in sicurezza IT: il 92% effettua la scelta in base alla reputazione e ai prezzi offerti. Come con i propri clienti, per aggiungere valore all'offerta commerciale gli MSP devono necessariamente collaborare con un partner che non solo dispone delle soluzioni e competenze necessarie per supportarli, ma sia ugualmente in grado di offrire tutto questo al miglior prezzo possibile.
- La principale qualità di cui i clienti hanno bisogno (84%), in termini di aspettative nutrite nei confronti degli attuali MSP, è che i provider di servizi gestiti siano realmente esperti di infrastrutture cloud e on-premise. Sono in cima alla lista anche le specifiche competenze in materia di Cybersecurity; il 74% dei clienti considera tale elemento una caratteristica chiave in relazione al proprio partner MSP.
- L'affrontare situazioni impreviste può ripercuotersi in modo negativo sulle relazioni con i clienti e comportare un impatto finanziario: in simili circostanze si può rivelare più difficile, per gli MSP, mantenere la crescita a livello di fatturato. I tre quarti (78%) dei clienti si aspettano che gli MSP gestiscano eventuali problematiche al di fuori dei termini del contratto stipulato, mentre il 65% degli MSP si trova ad affrontare problemi di sicurezza generati da errori degli utenti, anziché correlati ai servizi gestiti.
- Questo può far sì che gli MSP siano spesso incolpati per incidenti di sicurezza non dovuti a loro negligenze. Il 43% delle aziende vittime di un data breach ha addossato la responsabilità al proprio MSP; il 27%, infine, ha imputato tutto ciò alla mancanza di un'adeguata conoscenza della sicurezza IT da parte del proprio fornitore di servizi.

Metodologia

Le conclusioni illustrate nel report derivano da due diverse fonti di dati:

- Interviste telefoniche condotte nei mesi di luglio e agosto 2019 con 101 dipendenti di provider MSP situati nel Regno Unito, in Francia, Germania, Spagna, Italia, Austria, Svezia e Danimarca.
- "Corporate IT Security and Risks Survey 2019", indagine annuale online sui rischi per la sicurezza informatica delle imprese condotta da Kaspersky nel mese di giugno 2019 in 23 Paesi diversi, consultando i responsabili delle decisioni IT all'interno dell'azienda. Il presente report si focalizza sulle risposte fornite dagli addetti che operano in società europee con meno di 500 dipendenti.

L'outsourcing IT e le mutevoli dinamiche del mercato MSP

Prospettive in Europa

Il ruolo svolto dall'MSP nell'ambito della collaborazione con le aziende clienti sta progressivamente cambiando: da semplice fornitore di soluzioni, il provider di servizi gestiti diviene in misura sempre maggiore un consulente di fiducia e un vero e proprio riferimento per il successo operativo dell'impresa. Di conseguenza, l'IT in outsourcing sta divenendo un nuovo standard a tutti gli effetti, visto che le aziende si rivolgono sempre di più agli esperti del settore per la gestione di complesse infrastrutture IT e per tutto quanto è correlato a tali sistemi.

Attualmente il 40% delle aziende europee con meno di 500 dipendenti esternalizza la gestione IT a terze parti. Un terzo (33%) ricorre all'outsourcing anche per la gestione della sicurezza IT. Ciò suggerisce che si tratta indubbiamente di un'area chiave nell'ambito del supporto IT: adesso le aziende si affidano ai provider esterni anche per coprire le loro esigenze in materia di Cybersecurity.

È ormai un tema comune in tutta Europa, con i Paesi Bassi decisamente all'avanguardia nell'esternalizzazione della sicurezza informatica (45%). Seguono, a ruota, Svezia (39%) e Italia (39%). Altri Paesi stanno tuttavia accelerando il passo: si prevede che, nel corso dei prossimi 12 mesi, Polonia (35%), Repubblica Ceca (24%), Francia (22%) e Spagna (22%) mostreranno il tasso di crescita più elevato per ciò che riguarda l'outsourcing in termini di gestione della sicurezza IT.

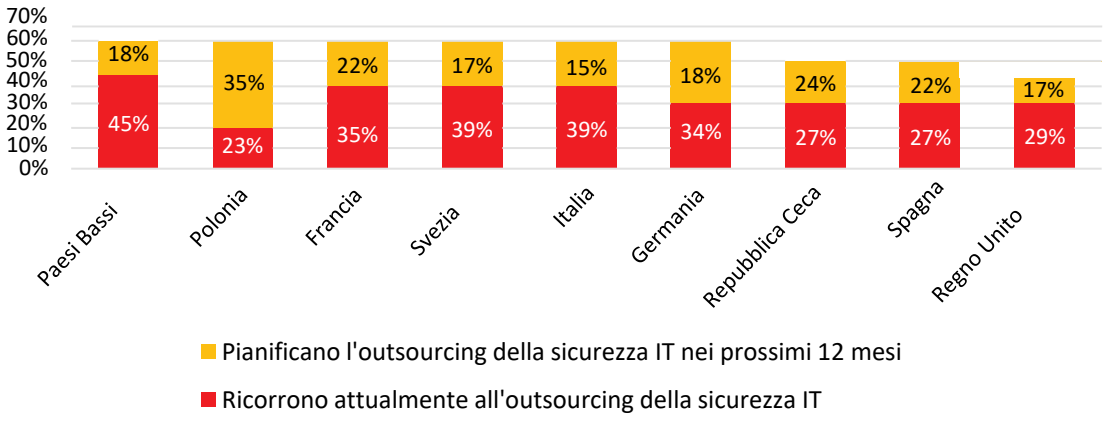

Figura 1. Quote percentuali relative agli attuali livelli e alle previsioni di crescita nei prossimi 12 mesi in termini di outsourcing della sicurezza IT

Nelle aziende che adottano un approccio favorevole all'outsourcing, il modello di impegno può assumere forme diverse, a seconda delle specifiche esigenze dell'impresa. La maggior parte degli MSP rivela che i clienti desiderano instaurare una partnership, ossia un approccio misto (51%), al fine di integrare le competenze interne con quelle derivanti dalla scelta di outsourcing, per un perfetto equilibrio nella gestione della sicurezza IT. Tuttavia, quasi un terzo (29%) degli MSP ritiene che le aziende preferiscano esternalizzare l'intera funzione IT, compresa la sicurezza IT.

Quali sono i fattori trainanti a livello decisionale?

Così come avviene di solito per molte decisioni prese in ambito aziendale, il costo rappresenta il principale fattore trainante in merito alla necessità di esternalizzare la gestione della sicurezza IT. Oltre la metà delle aziende che stanno pianificando l'outsourcing della sicurezza informatica (52%) ritiene che operare in tal modo contribuisca a ridurre i costi relativi alla sicurezza; ne consegue che oltre un terzo (38%) intende esternalizzare a terze parti tutto l'IT, sicurezza inclusa. È di particolare interesse notare come un terzo (33%) delle aziende consideri l'outsourcing della sicurezza IT un valido modo per "spuntare" la casella relativa a SLA (Service Level Agreements) e responsabilità operative. Più o meno la stessa percentuale di imprese (32%) ammette semplicemente di non disporre di risorse o competenze interne atte a fornire i livelli di sicurezza necessari per garantire l'operatività del business aziendale.

Dall'altro lato, esistono ugualmente ragioni per le quali le imprese scelgono di non esternalizzare la gestione della loro sicurezza IT; gli MSP ne debbono tener conto, nel momento in cui mirano ad aumentare la propria offerta e costruire relazioni durature con i clienti. Nonostante il fattore competenze venga spesso citato quale ragione principale per avviare una collaborazione con terze parti, il 40% delle aziende contrarie all'outsourcing della sicurezza IT, da noi consultate, ha dichiarato di sentirsi sufficientemente competente, grazie a risorse interne, riguardo alla gestione della sicurezza informatica. Un altro motivo di preoccupazione, per un terzo delle imprese (33%) è rappresentato dalla percezione di costi elevati in relazione all'eventuale outsourcing della sicurezza IT.

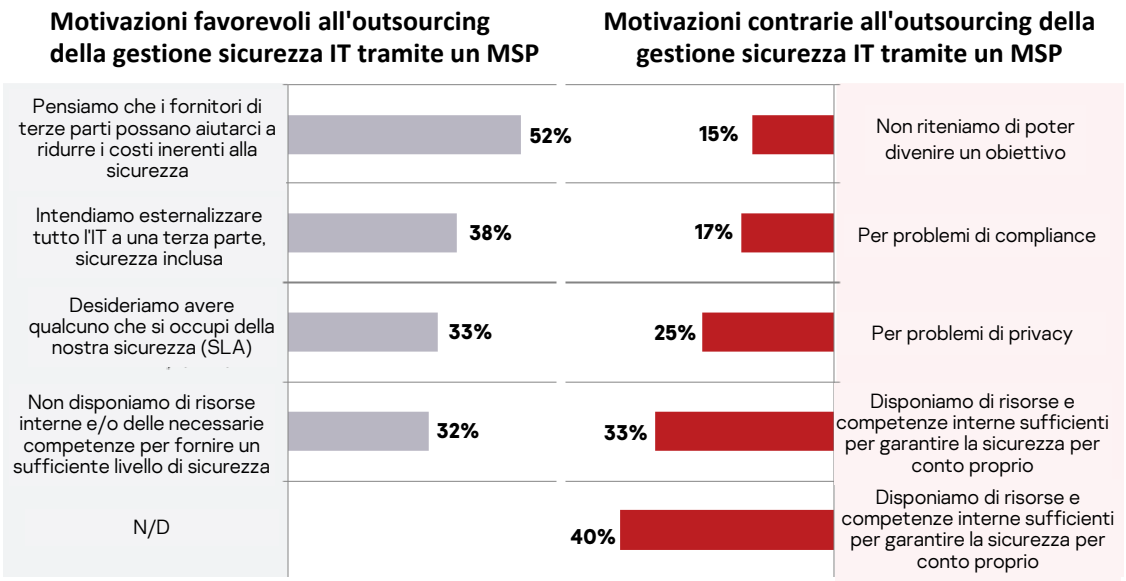

Figura 2. Pro e contro riguardo all'esternalizzazione a un provider MSP della gestione sicurezza IT

Un'analisi più approfondita dei processi decisionali in atto all'interno di vari settori evidenzia come esistano vari fattori motivanti in relazione all'outsourcing. Per la maggior parte dei settori produttivi il fattore trainante è rappresentato dal risparmio sui costi; il settore sanitario evidenzia invece i problemi di privacy quale ragione principale per evitare il ricorso all'outsourcing; quello dell'istruzione, infine, ritiene che il prezzo delle soluzioni fornite da terze parti sia troppo elevato.

L'eterno rompicapo costo vs. budget è di sicuro una sfida particolarmente impegnativa sia per gli MSP, sia per le aziende che intendono avvalersi di servizi IT gestiti. È interessante rilevare come le imprese che si attendono un innalzamento dei propri budget dedicati alla sicurezza IT abbiano l'intenzione di effettuare investimenti nel rafforzamento del personale IT interno specializzato. Per contro, una riduzione del budget disponibile favorisce la tendenza, da parte delle aziende, ad orientarsi verso i servizi MSP per la futura gestione della sicurezza IT; è logico pensare che, in presenza di budget limitati, le imprese intravedano un maggior valore nell'operare in base a tale schema.

Impatto delle modifiche ai budget dedicati alla sicurezza IT sulla futura gestione della sicurezza informatica aziendale

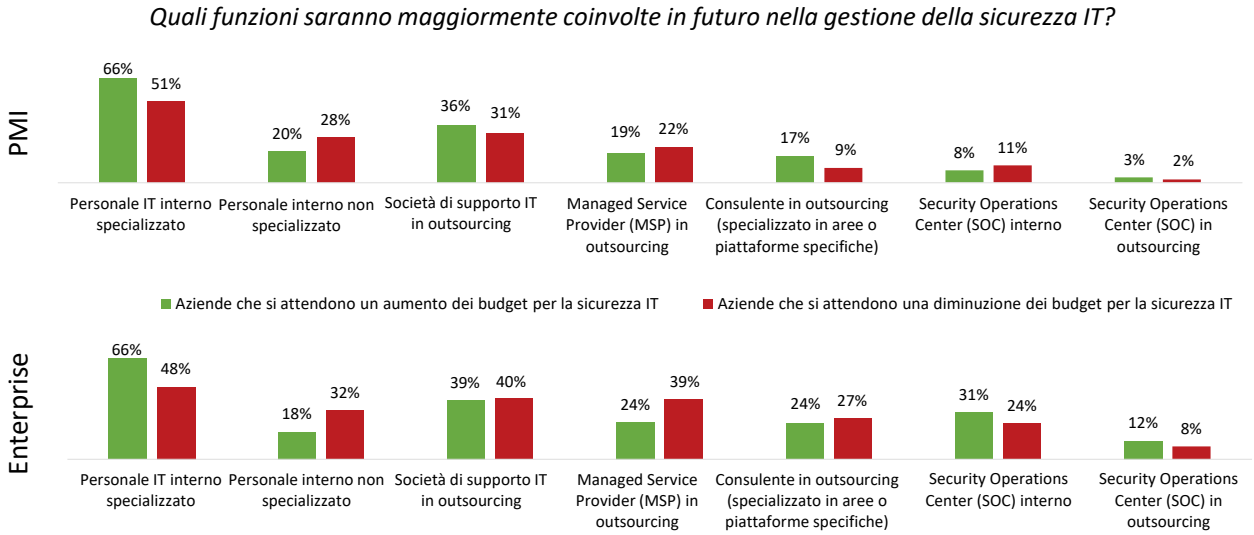

Figura 3. Impatto delle modifiche ai budget dedicati alla sicurezza IT sulla futura gestione della sicurezza informatica aziendale

La crescita del modello di business MSP è indubbiamente trainata e alimentata da due fattori fondamentali: la necessità di sfruttare al massimo il budget disponibile e il bisogno di garantire l'implementazione di risorse e misure di protezione adeguate. Tuttavia per molte aziende, in numerosi settori produttivi, gli stessi fattori motivanti possono paradossalmente rappresentare un potenziale deterrente nei confronti di investimenti mirati al supporto esterno.

Il panorama MSP in Europa: sfide e priorità

Un "tipico" MSP

Abbiamo già appurato come il ruolo e le responsabilità degli MSP stiano progressivamente cambiando: è quindi opportuno ridefinire l'effettivo posizionamento della maggior parte dei provider di servizi gestiti nel quadro dell'attuale panorama, al fine di valutare correttamente le specifiche opportunità e le sfide che questi ultimi devono affrontare.

La maggior parte (57%) degli MSP da noi interpellati presenta tra i due e i 20 dipendenti; tuttavia, pur nella veste di aziende di piccole dimensioni, un terzo (32%) degli stessi fornisce assistenza a clienti con oltre 300 addetti. Il 50% degli MSP opera con una gamma di clienti notevolmente diversificata, in vari settori produttivi; un terzo (35%) si focalizza sul supporto alle PMI.

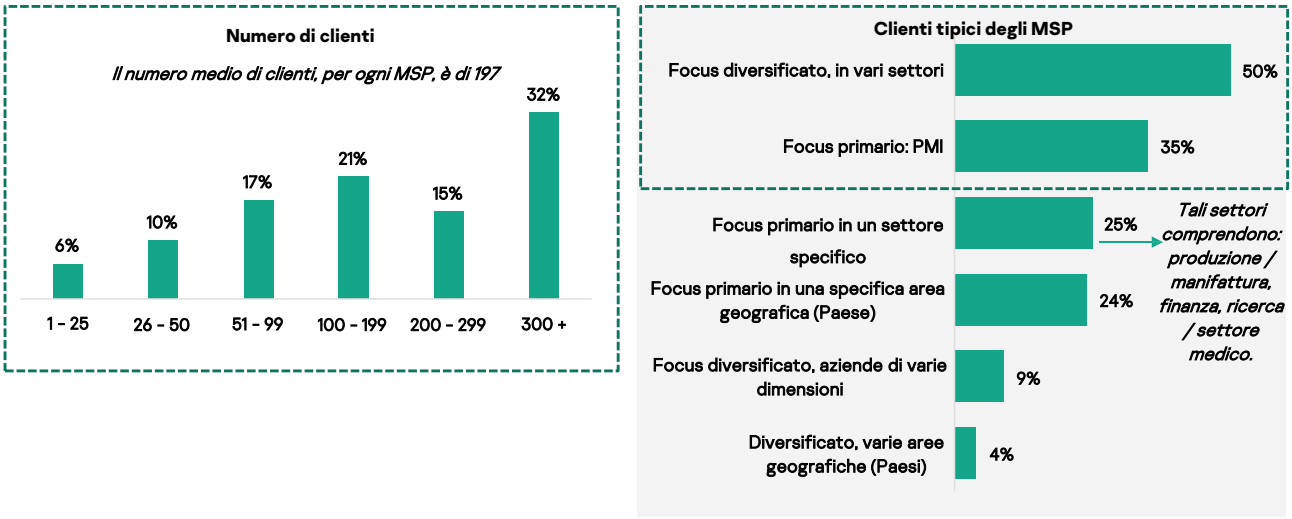

Figura 4. Numero di clienti / clienti tipici degli MSP

Una base di clienti così ampia può rappresentare un'ardua sfida per gli MSP, visto che tali provider devono necessariamente dimostrare di comprendere alla perfezione e supportare adeguatamente sia le complesse diversità che contraddistinguono ogni settore, sia gli specifici punti deboli dell'azienda. Pertanto, gli MSP devono essere in grado di offrire una vasta gamma di servizi per soddisfare al meglio le esigenze dei propri clienti: ciò significa possedere competenze specifiche e conoscenze approfondite in svariati settori.

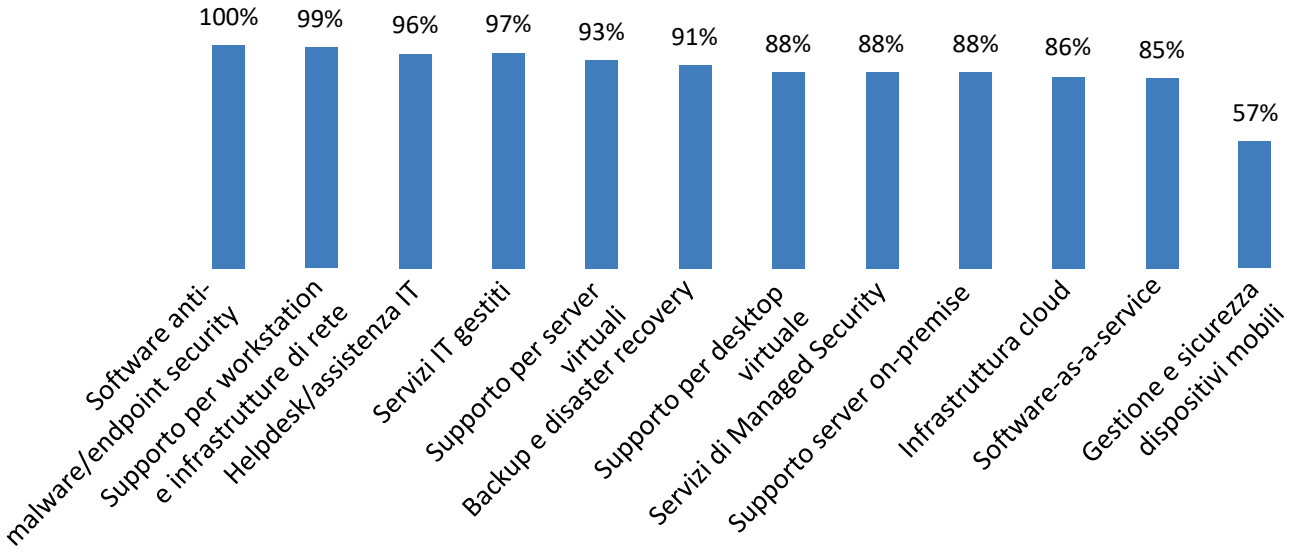

Figura 5. Panoramica dei principali "servizi gestiti" offerti ai clienti

Nonostante l'elevato numero di clienti, quando si tratta dell'effettiva quantità di dispositivi abitualmente gestiti dagli MSP si evince che un quarto dei provider (23%) gestisce solo un numero di dispositivi compreso tra le 10 e le 25 unità per cliente. Per il 48% degli MSP tali cifre si riducono addirittura a meno di dieci "nodi" per cliente.

Punti di forza e di debolezza

Una base di clienti in espansione può costituire, per gli MSP, un'arma a doppio taglio. In effetti, nonostante le aziende chiedano a gran voce i loro servizi, una simile situazione genera un significativo aumento del livello concorrenziale all'interno del mercato: questo rende i clienti più esigenti che mai nei confronti del proprio MSP. Ciò vale per i tre quarti (75%) degli MSP, i quali ammettono che la crescente presenza di clienti e utenti con particolari esigenze rappresenta una sfida chiave. Più o meno lo stesso numero (78%) considera ugualmente difficile trovare nuovi clienti, mentre i due terzi (68%) dei provider MSP lottano per mantenere la redditività.

Il problema del fatturato viene posto in evidenza quando si prendono in considerazione due aspetti fondamentali: l'ampia varietà di servizi che gli MSP devono fornire e il basso numero di nodi effettivamente gestiti per ogni singolo cliente. Per rafforzare il loro valore di mercato nei confronti della clientela e avere maggiori opportunità di guadagno, gli MSP potrebbero offrire un deal basato su appositi sconti sul software di sicurezza, allo scopo di rendere il modello di business in outsourcing ancor più conveniente in termini di costi e fidelizzare quindi i clienti a lungo termine.

La soddisfazione del cliente occupa una posizione di primo piano nell'ambito della strategia commerciale attuata da numerosi provider MSP; non sorprende pertanto il fatto che le cifre relative al livello di fidelizzazione rappresentino il principale indice di successo per il 43% degli MSP, mentre il 41% dei provider in questione si affida ai sondaggi sul grado di soddisfazione dei clienti per valutare l'effettiva performance del proprio business. Per contro, gli indici percentuali che misurano il valore offerto dagli MSP ai propri clienti in termini di redditività (33%) ed efficienza (20%) si situano a livelli inferiori.

Quanto alle strategie messe in atto per attrarre nuova clientela, occorre dire che la stragrande maggioranza (83%) degli MSP si basa di fatto sul passaparola o sulla raccomandazione diretta per accrescere la propria base di clienti: la gestione del livello reputazionale diviene quindi un asset chiave utilizzato dai provider per acquisire nuovi clienti.

Nonostante le complesse sfide che si presentano, gli MSP di tutta Europa prevedono una significativa crescita del proprio business nel corso dei prossimi due anni; il 63% degli stessi si attende persino un forte aumento delle entrate (fino al 20%). Tutto questo riflette in pieno l'attuale trend del mercato globale e avvalora le stime relative al tasso di crescita annuale, previsto al 9,3%.

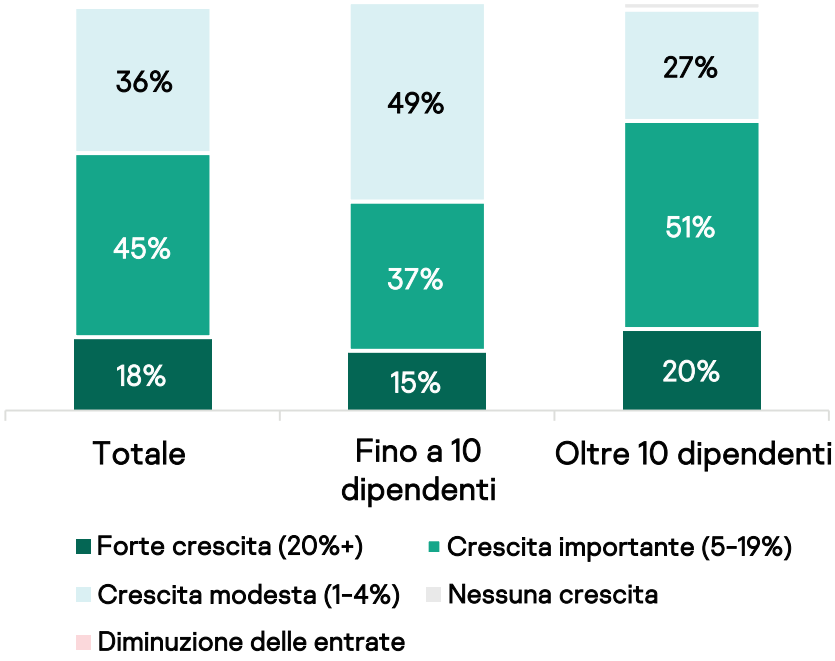

Figura 6. Percentuali di crescita previste per il modello di business MSP

Un partner perfetto per la sicurezza IT

L'outsourcing inerente alla gestione della sicurezza IT occupa un posto di assoluto rilievo nell'agenda dell'impresa: in che modo gli MSP possono continuare a soddisfare al meglio questa esigenza, garantendo che le soluzioni e i servizi forniti siano davvero all'altezza? Nel momento in cui cerca di instaurare una proficua collaborazione con un vendor di soluzioni di sicurezza IT, il 92% dei provider di servizi gestiti effettua la propria scelta sulla base di due elementi essenziali: reputazione e prezzo. Seguono, a pochi punti percentuali di distanza, ulteriori fattori di particolare rilievo quali semplicità di gestione, possibilità di integrazione e modalità di acquisto delle licenze (88%).

La procedura attraverso la quale gli MSP provvedono ad acquistare le licenze influisce anche in termini di rischi assunti e relativa ricompensa, visto che può contribuire in maniera significativa ad accelerare e semplificare la fornitura di servizi ai clienti. A livello di licensing gli MSP preferiscono la massima flessibilità: in effetti, quasi la metà (47%) degli stessi dichiara di preferire l'acquisto di singole licenze per ciascun cliente. Altri provider MSP (44%) hanno invece scelto di pagare software e servizi di sicurezza IT forniti dai relativi vendor attraverso un modello di acquisto basato sulla subscription mensile. Entrambe le opzioni consentono agli MSP sia di proteggersi adeguatamente, nel caso in cui un cliente intenda rivolgersi altrove, sia di gestire le proprie licenze in modo più efficiente.

Gli MSP preferiscono ugualmente utilizzare modalità di gestione e ordine delle licenze improntate a criteri di semplicità; tale fattore esercita una considerevole influenza nel momento in cui si orienta la scelta verso una determinata soluzione di sicurezza o uno specifico vendor. Di fatto, oltre la metà (56%) ha dichiarato che, per ottenere le licenze, è solita ricorrere all'utilizzo del portale appositamente creato dal vendor per la gestione del licensing. Gli MSP traggono inoltre importanti vantaggi sia dagli strumenti RMM (Remote Monitoring and Management) e PSA (Professional Service Automation) integrati con il software di sicurezza (per quanto riguarda le procedure centralizzate di gestione e monitoraggio), sia dall'automazione dei task di routine quotidiani.

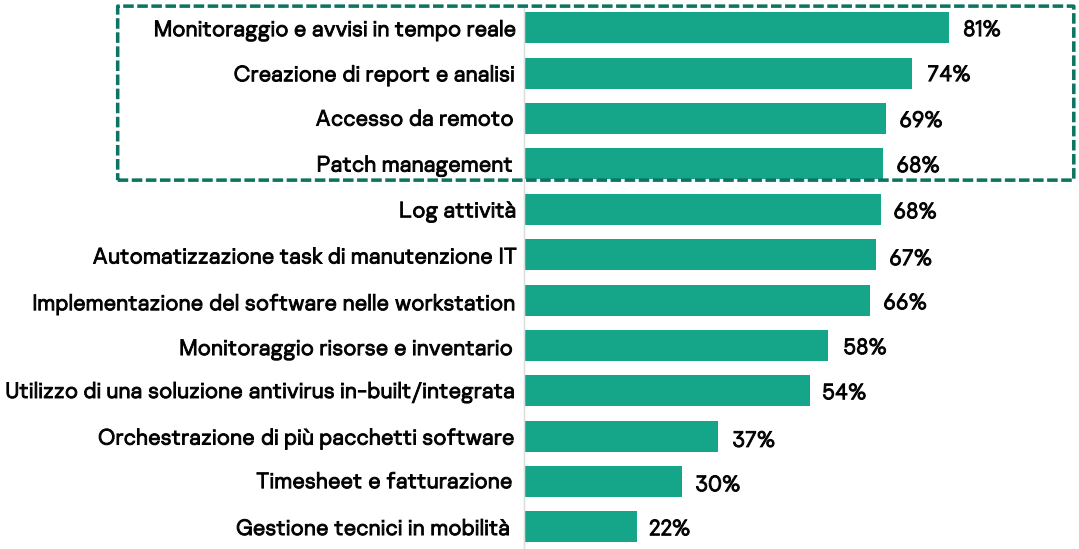

Figura 7. Principali utilizzi delle piattaforme RMM da parte degli MSP

Gestione delle difficoltà nelle relazioni con la clientela

Qualità e sfide

Così come avviene in qualsiasi tipo di relazione, entrambe le parti hanno elevate aspettative; tuttavia, lungo il cammino si presentano inevitabilmente sfide e ostacoli da superare. Per quanto riguarda le aspettative dei clienti nei confronti degli attuali MSP, la qualità principale ricercata dai primi è indubbiamente il fatto di trovare dei veri esperti (84%), sia a livello di soluzioni on-premise, sia per le soluzioni inerenti alle infrastrutture cloud. Gli MSP devono essere ugualmente in grado di fornire aiuto in materia di compliance e normative (82%), dare risposte rapide e attenersi a SLA di livello elevato (80%).

È di particolare interesse notare come le competenze di Cybersecurity siano state evidenziate in qualità di attributo chiave, per gli MSP, da quasi tre quarti (74%) dei clienti intenzionati ad avvalersi di un supporto per la gestione IT. Il fatto che tale requisito occupi una posizione di assoluto rilievo nell'elenco delle specifiche esigenze aziendali è indubbiamente la prova di come la capacità di mantenersi al passo nel mutevole panorama della Cybersecurity rappresenti un elemento per il quale le imprese necessitano di ulteriore supporto.

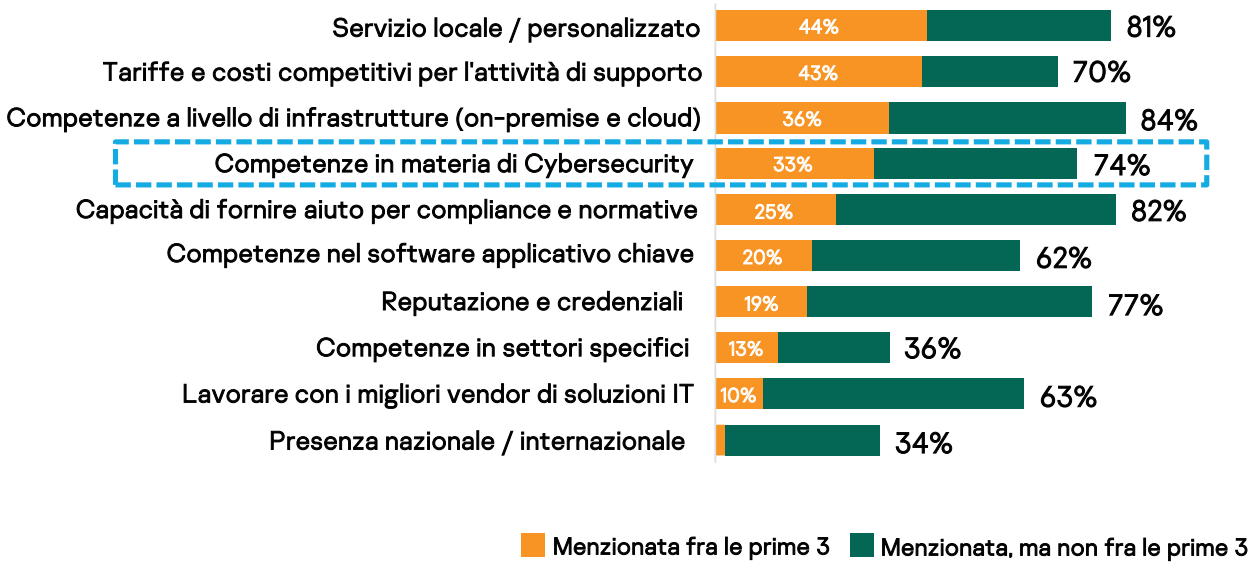

Figura 8. Caratteristiche maggiormente richieste dai clienti degli MSP

Oltre a tali specifici requisiti, espressamente dichiarati, si richiede ugualmente agli MSP la capacità di affrontare situazioni impreviste. Purtroppo, il fatto di essere un provider fidato ed esperto comporta ulteriori sfide. Tre quarti (78%) dei clienti si aspettano che gli MSP siano in grado di gestire eventuali problematiche al di fuori dei termini del contratto stipulato. Per altri, sono i problemi creati dagli stessi utenti a generare una maggior mole di lavoro (65%); inoltre l'incapacità di seguire correttamente i processi di helpdesk (59%) aggiunge task non necessari all'elenco delle cose da fare.

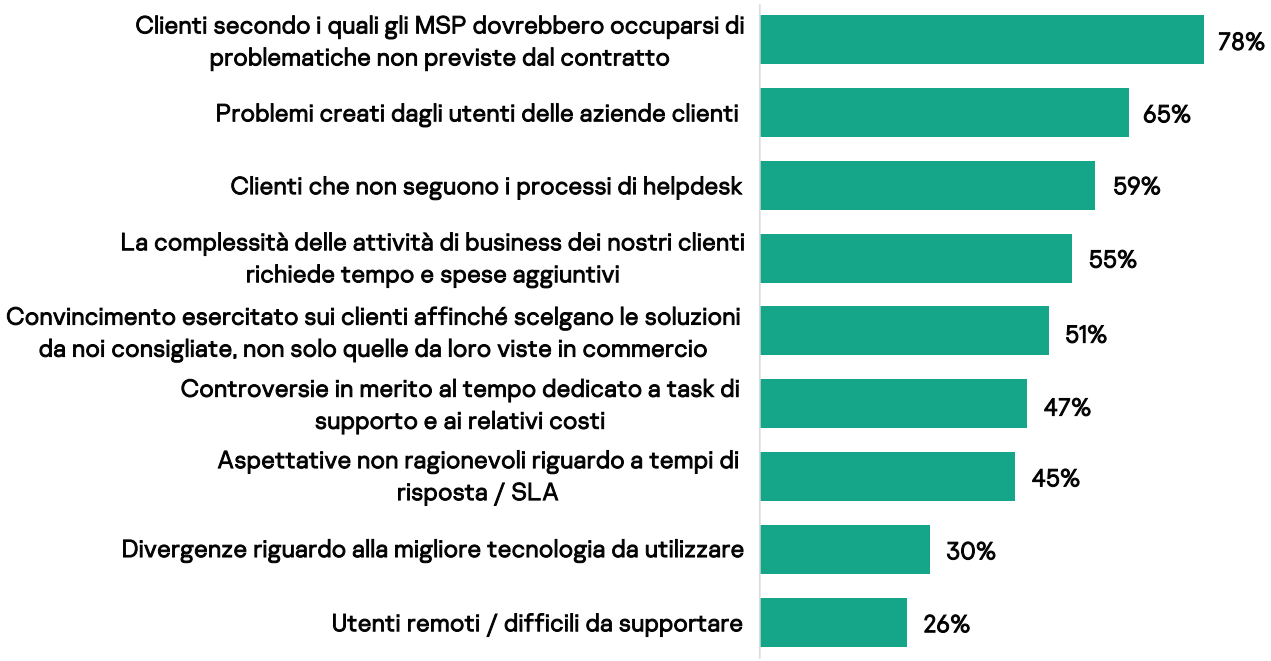

Figura 9. Situazioni critiche incontrate dagli MSP nelle relazioni con i clienti

La maggiore sfida che si trovano ad affrontare gli MSP è senza dubbio rappresentata dal notevole volume di cyberattacchi e infezioni da malware in grado di causare tempi di inattività per i loro clienti (72%); seguono, a breve distanza, gli attacchi ransomware (65%). Non sono in ogni caso solo le minacce esterne a creare problemi agli MSP: il fattore umano genera ancora serie problematiche. Il 69% degli MSP vede negli errori degli utenti e nel fatto di non seguire i criteri di sicurezza le minacce chiave per la sicurezza dei clienti.

Cosa significa tutto questo per gli MSP

L'impatto di qualsiasi incidente di sicurezza può avere conseguenze di vasta portata non solo per il cliente, ma anche per l'MSP coinvolto nella situazione critica. Il recente data breach scoperto da Capital One, che ha riguardato oltre 100 milioni di utenti, è stato causato dalla "errata configurazione del firewall di un'applicazione web su Amazon Web Services". Tuttavia, nonostante fosse presa di mira, la piattaforma AWS non è stata hackerata; il problema occorso è stato imputato a un cliente che non era riuscito a configurare in modo corretto il firewall cloud.

Questo è solo un esempio lampante di come una terza parte possa di fatto trovarsi in prima linea nel momento in cui un cliente subisce un data breach; di sicuro non sarà l'ultimo esempio del genere. In sostanza, il 43% dei clienti MSP intervistati vittime di un data breach ha attribuito la colpa di quanto avvenuto al proprio MSP; solo il 41% degli stessi ha ammesso che la responsabilità della violazione informatica era dovuta a errori commessi dai dipendenti dell'azienda. Ciò che sorprende di più, tuttavia, è il fatto che un quarto (27%) di coloro che hanno subito un data breach ha imputato tale violazione a una mancanza di conoscenze in materia di sicurezza IT da parte del proprio fornitore di servizi.

Inoltre, gli errori dei clienti riguardo alla sicurezza IT possono ugualmente produrre un impatto sul provider MSP in termini di tempo impiegato da quest'ultimo per risolvere il problema (il 67% concorda); un terzo (38%) ha addirittura perso denaro risolvendo problemi non dovuti alla propria negligenza o mancanza di competenze.

Conclusioni

È del tutto evidente come la riduzione dei costi e l'ottimizzazione dei budget IT disponibili siano i principali fattori trainanti a livello decisionale per le aziende che intendono ricorrere all'outsourcing per quanto riguarda la gestione dei propri sistemi IT. Se a tutto questo si aggiunge la carenza di risorse interne e specifiche competenze in tema di sicurezza informatica, emerge ugualmente in tutta evidenza la chiara opportunità, per gli MSP, di divenire esperti di Cybersecurity e colmare in tal modo le lacune in termini di gestione della sicurezza per le aziende di tutta Europa.

Si rivela pertanto di vitale importanza, per i Managed Service Provider, essere pienamente in grado di offrire un simile livello di servizio e soddisfare quindi la crescente domanda di servizi di sicurezza in outsourcing. Per attrarre nuovi clienti e aumentare le entrate, gli MSP debbono necessariamente ampliare l'elenco dei servizi offerti e focalizzarsi sia sul proprio posizionamento di mercato, sia sulla gestione del livello reputazionale, al fine di prevalere sulla concorrenza.

Dal proprio MSP i clienti si attendono un'efficace protezione in termini di sicurezza IT, così come elevate competenze in materia di Cybersecurity. La mancanza di specifiche competenze in tale settore può comportare la perdita di clienti e far venir meno l'ambizioso proposito di diventare consulente e partner di fiducia. Per gli MSP si rivela in effetti indispensabile costruire un rapporto con la clientela basato su fiducia e fidelizzazione: ciò si può realizzare solo avendo a disposizione gli strumenti e le competenze più adeguati per supportare i clienti in ogni step del delicato processo.

La reputazione costituisce senza dubbio l'elemento chiave: un solo passo falso può determinare spiacevoli conseguenze a lungo termine, nel momento in cui si intende attrarre e successivamente conservare il cliente. Disporre di una gamma completa di servizi di sicurezza, supportati da un partner di Cybersecurity solido e affidabile, consentirà agli MSP di realizzare la prevista crescita sul mercato, favorendo i profitti e la stabilità a lungo termine del business.

Da parte loro, i vendor svolgono un ruolo di primaria importanza e possono fornire un supporto davvero vitale per gli MPS. Gli MSP aumenteranno, nei prossimi anni, la gamma dei servizi di Cybersecurity da loro offerti; dall'altro lato, i vendor in grado di fornire soluzioni di sicurezza a livello di assessment, incident response, e-mail o web gateway, sembrano pronti a beneficiare della crescente domanda.

I vendor di soluzioni di sicurezza IT possono trasferire importanti competenze e conoscenze in materia di Cybersecurity, nonché fornire un prezioso supporto per il marketing e le vendite. La partnership di Kaspersky con i Managed Service Provider offre prodotti di Cybersecurity dedicati allo specifico uso da parte degli MSP, assieme a corsi di formazione, materiali didattici ed eventi altamente focalizzati sulla sicurezza IT. Kaspersky dispone di un ampio portfolio appositamente pensato per gli MSP, che consente ai provider di servizi gestiti di implementare efficaci soluzioni on-premise o cloud-based, dalla protezione endpoint alla hybrid cloud security, compresa la protezione dei sistemi e-mail e dell'accesso web. Tali soluzioni si possono integrare con piattaforme RMM (Remote Monitoring and Management) e PSA (Professional Service Automation), per far sì che i fornitori di servizi IT gestiti possano automatizzare i task di routine. Il Partner Program comprende altresì i benefit a livello finanziario e di marketing riservati a tutti i partner Kaspersky.

Ulteriori informazioni sul programma di partnership Kaspersky dedicato ai Managed Service Provider sono disponibili sul sito web di Kaspersky.