REPORT SPECIALE SULLA CYBERSECURITY

PMI E IMPRESE MEDIO-GRANDI

Piccole e forti

Ecco come PMI e imprese medio-grandi possono rafforzare le proprie difese contro le minacce odierne

CISCO

Il 53% delle imprese medio-grandi ha subito una violazione

Fino a

5000

avvisi di sicurezza in media

Le imprese medio-grandi analizzano il 55,6% degli avvisi di sicurezza

Il 29% delle imprese medio-grandi afferma che le violazioni costano loro meno di 100 mila dollari. Il 20% afferma che il costo varia tra $ 1.000.000 e $ 2.499.999

Molte PMI e imprese medio-grandi aspirano ad avere procedure di cybersecurity più efficaci proprio come le aziende più grandi. Le PMI sono dinamiche: sono la colonna portante dell'innovazione e il simbolo della tenacia. Operano a ritmi più serrati e pesanti rispetto alle grandi aziende. E sono esposte alle stesse minacce informatiche.

Nel panorama attuale delle minacce informatiche, ogni azienda, grande o piccola, corre il rischio di subire attacchi. Ma le PMI e le imprese medio-grandi sono sempre più spesso l'obiettivo di attacchi[1] e di frequente fungono da trampolino di lancio o veicolo per campagne più ampie. Per gli hacker le PMI e le imprese medio-grandi sono bersagli deboli perché usano procedure e infrastrutture di sicurezza meno sofisticate e hanno poche risorse interne specializzate in grado di gestire le minacce e intervenire in caso di attacchi.[1]

Molte PMI e imprese medio-grandi iniziano a rendersi conto di essere un bersaglio molto ambito per i criminali informatici. Spesso se ne rendono conto troppo tardi: dopo un attacco. A seconda della tipologia e della portata dell'attacco subito, ripristinare la situazione normale per queste aziende può essere difficile e costoso, a volte addirittura impossibile. Questo report analizza i rischi che le aziende più piccole devono affrontare, confronta il livello di sicurezza di imprese di diverse dimensioni e presenta alcune linee guida per il 2018 e il futuro.

Si consideri questo dato dello Studio comparativo di Cisco delle infrastrutture di sicurezza del 2018: più della metà (54%) degli attacchi informatici ha causato danni finanziari superiori a 500.000 dollari, comprese, tra l'altro, perdite di entrate, clienti, opportunità e costi vivi. Una cifra del genere è sufficiente per costringere una PMI o impresa medio-grande impreparata a chiudere definitivamente.

Un recente studio del Better Business Bureau (BBB)[2] sottolinea ulteriormente come le PMI e le imprese medio-grandi possono avere grosse difficoltà a livello finanziario per sopravvivere dopo un attacco informatico grave. Il BBB ha chiesto a proprietari di piccole imprese del Nord America: " Per quanto tempo potrebbe sopravvivere la tua azienda se perdessi l'accesso a dati essenziali in modo permanente?" Solo circa un terzo (il 35 per cento) ha dichiarato che le proprie aziende sarebbero potute rimanere redditizie per più di tre mesi. Oltre la metà ha affermato che le rispettive aziende non sarebbero più state redditizie in meno di un mese.

Consideriamo PMI le aziende con meno di 250 dipendenti e imprese medio-grandi quelle che hanno da 250 a 499 dipendenti. Entrambi i segmenti vengono trattati in questo report.

Nel nostro Studio comparativo delle infrastrutture di sicurezza del 2018 (che chiameremo semplicemente Studio comparativo), analizziamo i risultati delle interviste alle PMI e alle imprese medio-grandi. Lo studio offre informazioni dettagliate sulle procedure di sicurezza attualmente in uso e confronta i risultati completi degli ultimi tre anni.

I nostri dati su PMI e imprese medio-grandi includono 1816 intervistati in 26 paesi.

1 Cyberthreats and Solutions for Small and Midsize Businesses, Vistage Research Center, 2018. Sviluppato in collaborazione con Cisco e The National Center for the Middle Market. Disponibile all'indirizzo: https://www.vistage.com/research-center/business-operations/risk-management/20180503-22912/.

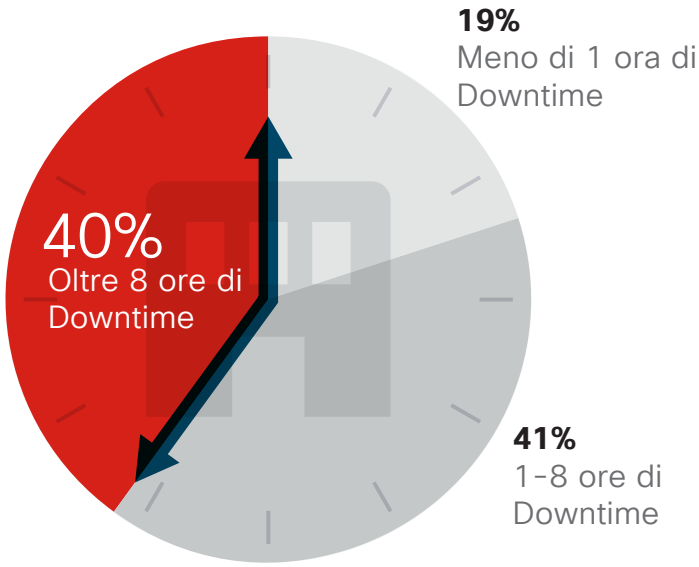
2 2017 State of Cybersecurity Among Small Businesses in North America, BBB, 2017: https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf.

In fondo una giornata persa non è un grosso problema...

Non lo direbbe nessun amministratore IT. L'interruzione dell'operatività dei sistemi, che compromette produttività e redditività, è un problema significativo che le aziende devono affrontare in seguito a un attacco informatico. In base alla ricerca dello Studio comparativo, nel corso dell'ultimo anno il 40% degli intervistati (250-499 dipendenti) ha subito un'interruzione dell'operatività dei sistemi per almeno otto ore a causa di una grave violazione della sicurezza (Figura 1). Cisco ha rilevato risultati simili per aziende più grandi del campione dello studio (quelle con minimo 500 dipendenti). La differenza, però, è che le aziende più grandi tendono a essere più resilienti dopo un attacco rispetto alle PMI e alle imprese medio-grandi, perché hanno più risorse da dedicare a risposta e ripristino.

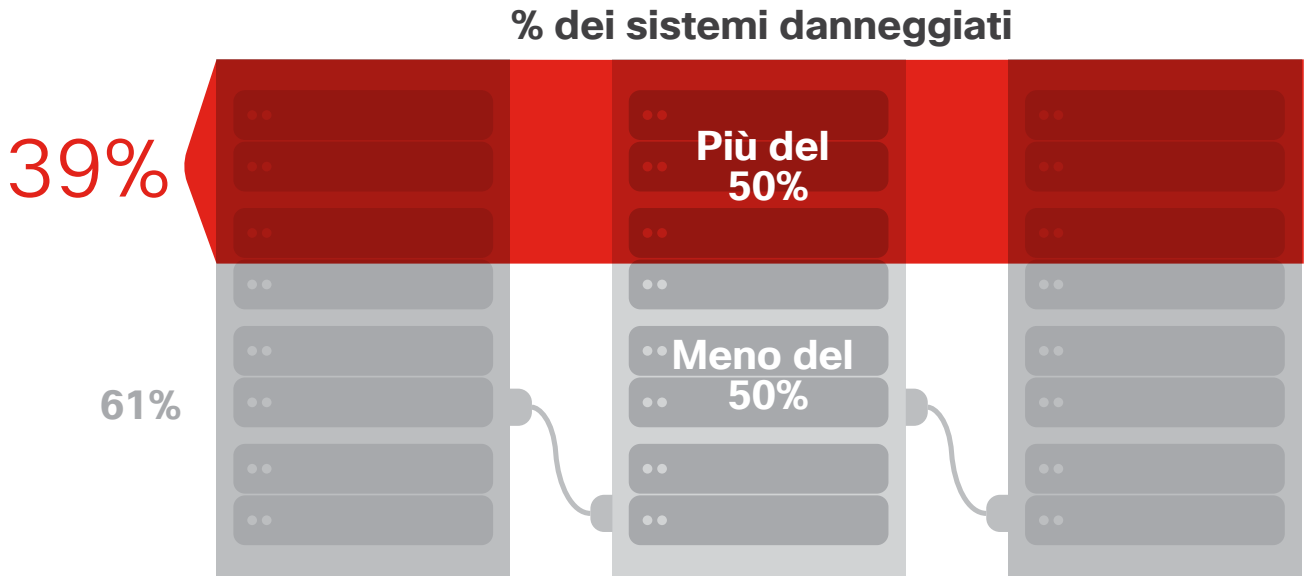
Inoltre, il 39% degli intervistati ha dichiarato che almeno la metà dei loro sistemi era stata colpita da una violazione grave (Figura 2). È meno probabile che le aziende più piccole abbiano sedi o segmenti di business diversi e i loro sistemi di base in genere sono più interconnessi. Quando queste aziende subiscono un attacco, la minaccia può diffondersi rapidamente e con facilità dalla rete ad altri sistemi.

Figura 1 Interruzione dell'operatività dei sistemi in seguito a una grave violazione



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

Figura 2 Percentuale di sistemi colpiti da una grave violazione



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

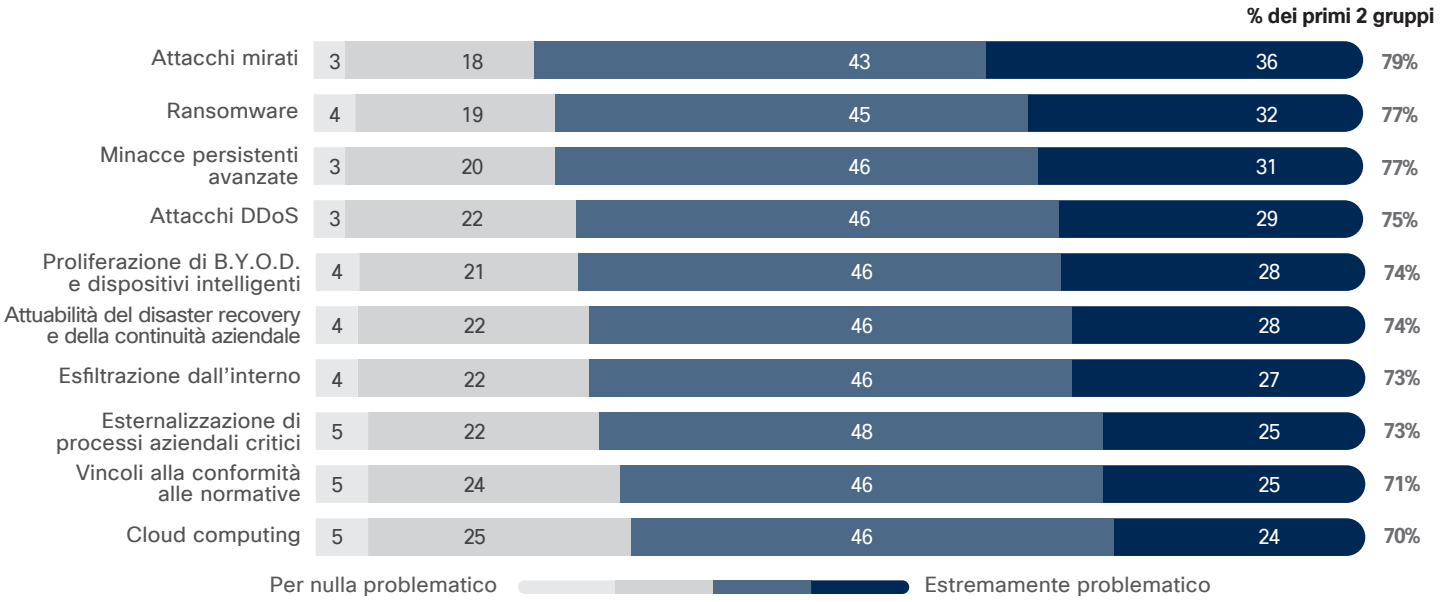
Le preoccupazioni del team della sicurezza

Per quanto riguarda la domanda sulle principali sfide di sicurezza che devono affrontare, gli intervistati hanno indicato tre principali motivi di preoccupazione:

- Attacchi mirati contro i dipendenti (ad esempio phishing ben architettato)
- Minacce persistenti avanzate (malware avanzato mai visto prima)
- Ransomware

Il ransomware (che non è stato citato fra le tre principali preoccupazioni delle grandi imprese, cosa molto interessante) è, come ormai saprai sicuramente, un malware che cripta i dati, di solito fino a quando gli utenti colpiti non pagano un riscatto. Può creare gravi turbative e interruzioni dell'operatività dei sistemi di PMI e imprese medio-grandi. Il ransomware è anche costoso per queste aziende ma in modo diverso: gli esperti di sicurezza Cisco spiegano che le PMI e le imprese medio-grandi sono più inclini a pagare il riscatto agli autori degli attacchi in modo da poter riprendere in fretta le normali operazioni. Semplicemente non possono permettersi l'interruzione dell'operatività e la mancanza di accesso ai dati importanti, tra cui quelli sui clienti. (Vedere la figura 3).

Figura 3 Principali preoccupazioni relative alla sicurezza per le imprese medio-grandi[5]



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

Altre minacce che le PMI non possono ignorare

Nonostante le preoccupazioni per il ransomware, gli esperti di sicurezza Cisco ritengono che la portata di questo tipo di minaccia sia in diminuzione poiché un numero maggiore di hacker sta spostando la propria attenzione sul mining di criptovaluta illegale (" cryptomining"). L'attrattiva di questa attività è triplice: può essere estremamente redditizia, i pagamenti non possono essere tracciati e gli hacker possono preoccuparsi meno per la potenziale responsabilità penale delle loro azioni. Ad esempio, non c'è rischio che i pazienti vengano privati dell'assistenza sanitaria di base perché i sistemi e i dati essenziali di un ospedale sono bloccati dal ransomware. Gli hacker possono anche distribuire software di mining ("miner") attraverso diversi metodi, tra cui le campagne di spam basate su e-mail e gli exploit kit.[3]

3 Ransom Where? Malicious Cryptocurrency Miners Takeover, Generating Millions", blog di Cisco Talos, 31 gennaio 2018: https://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html.

I ricercatori sulle minacce di Cisco spiegano che gli hacker che utilizzando il nuovo modello di business di cryptomining illecito " non puniscono più le vittime perché aprono un allegato o eseguono uno script dannoso prendendo in ostaggio i sistemi e richiedendo un riscatto. Ora sfruttano attivamente le risorse dei sistemi infetti" .[4] Per le PMI e imprese medio-grandi che favoriscono involontariamente le operazioni illecite di cryptomining, l'unico segnale di compromissione potrebbero essere le prestazioni rallentate dei sistemi, a meno che non dispongano della giusta tecnologia in grado di rilevare attività di cryptomining.

Il rischio interno dello 0,5% è comunque troppo alto?

Le aziende degli intervistati spostano sul cloud un numero sempre maggiore di dati e processi, ma devono anche adottare misure per gestire un'altra potenziale minaccia: i criminali infiltrati. Senza gli strumenti per rilevare le attività sospette (ad esempio il download di informazioni sensibili dei clienti), rischiano di perdere la proprietà intellettuale e dati finanziari o informazioni sensibili sui clienti attraverso i sistemi cloud aziendali.

Una recente indagine condotta dai ricercatori sulle minacce di Cisco evidenzia il rischio: da gennaio a giugno 2017 hanno esaminato le tendenze di esfiltrazione dei dati utilizzando il machine learning per profilare 150.000 utenti di 34 paesi che usavano il cloud. Nel corso di 1,5 mesi, i ricercatori hanno scoperto che lo 0,5% degli utenti era responsabile di download sospetti. Lo 0,5% non sembra male, no? Detto in altri termini, significa che in un'azienda con 400 persone ben due dipendenti costituivano una minaccia interna. Perciò questa cifra è il 100% troppo alta. In particolare, tali utenti hanno scaricato, in totale, più di 3,9 milioni di documenti dai sistemi cloud aziendali. Si tratta di una media di 5200 documenti per utente nel corso di 1,5 mesi.[5]

Studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

Questo report speciale presenta risultati selezionati dello Studio comparativo di Cisco delle infrastrutture di sicurezza del 2018. La ricerca ha coinvolto più di 3600 intervistati in 26 paesi. Per ulteriori informazioni sulle procedure di sicurezza attualmente in uso presso le aziende di tutte le dimensioni e per un confronto con i risultati di studi precedenti di Cisco, scarica il *Report annuale di Cisco sulla cybersecurity 2018* disponibile all'indirizzo: https://www.cisco.com/c/en/us/products/security/security-reports.html.

4 Ibid.

5 Per ulteriori informazioni, consulta "Minacce interne attraverso il cloud" nel Report annuale di Cisco sulla cybersecurity 2018, disponibile all'indirizzo: https://www.cisco.com/c/en/us/products/security/security-reports.html.

Sfide

La migliore difesa contro le minacce descritte prima è data dal coordinamento e dall'orchestrazione delle risorse IT. Tali risorse sono in genere le persone, i processi e la tecnologia che le aziende possono raccogliere per scoraggiare gli attacchi.

Tuttavia, ancor più che le grandi aziende, le imprese più piccole faticano a coordinare queste risorse in modo che diano informazioni approfondite sulle minacce e blocchino o mitighino gli attacchi prima che possano causare danni. La costante mancanza di esperti di sicurezza che caratterizza le grandi aziende è ancora più significativa per quelle più piccole.

Tendenze tecnologiche di sicurezza delle PMI

Andando avanti, le aziende più piccole cercano di affrontare le sfide di cybersecurity che minacciano le loro aziende con nuovi strumenti in grado di bloccare le minacce.

Gli intervistati dello Studio comparativo hanno affermato che, se avessero a disposizione il personale adeguato, sarebbero più propensi a:

- Aggiornare la sicurezza degli endpoint con Advanced Malware Protection/EDR più sofisticati (questa è stata la risposta più comune con una percentuale del 19 per cento).
- Prendere in considerazione una migliore sicurezza delle applicazioni Web per la difesa dagli attacchi Web (18 per cento)
- Implementare la prevenzione delle intrusioni, che è considerata ancora come una tecnologia fondamentale per bloccare gli attacchi di rete e i tentativi di exploit (17 per cento). (Vedere la figura 5).

Quando le aziende valutano nuove tecnologie, un problema è quello di determinare come interagiscono i prodotti in uso al fine di garantire la protezione delle aziende stesse. Non bisogna sottovalutare le difficoltà di gestione quando si tratta di spulciare tra diverse console per rispondere alle minacce o agli incidenti di sicurezza.

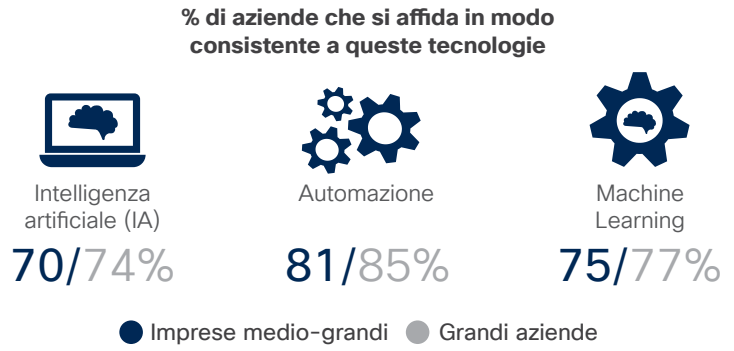
" Molte persone pensano che un approccio multivendor con soluzioni all'avanguardia li proteggerà meglio" , afferma Ben M. Johnson, CEO di Cisco Partner Liberty Technology a Griffin, Georgia. " Ma a noi risulta sia più difficile da gestire, più costoso e nel complesso meno efficiente a livello di sicurezza" .

Machine learning: un aiuto effettivo per la sicurezza o una moda?

Tutti abbiamo sentito parlare di machine learning vista la recente risonanza di cui gode. È emerso che più o meno lo stesso numero di imprese medio-grandi e grandi aziende si affida a soluzioni di sicurezza per l'analisi comportamentale in grado di rilevare in modo efficace gli attacchi. Le soluzioni basate su automazione e machine learning vengono sfruttate un po' meno dalle imprese medio-grandi rispetto alle aziende con più di 1000 dipendenti (Figura 4).

Il machine learning è più efficace quando consiste in un livello aggiuntivo di rilevamento in un prodotto già implementato rispetto all'acquisto di un prodotto separato con l'unico scopo di attuare il " machine learning" . In questo modo i team hanno il vantaggio di poter sfruttare il machine learning per rilevare le anomalie e le minacce a una velocità di macchina senza ulteriori incarichi gravosi per il team.

Figura 4 Le imprese medio-grandi fanno meno affidamento su strumenti di automazione e IA



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

Le imprese medio-grandi e la tecnologia mobile

Le aziende si rendono anche conto che i loro approcci alla sicurezza devono soddisfare le esigenze dell'ambiente di lavoro moderno, in particolare, il passaggio alla mobilità e l'adozione di dispositivi mobili. Il 56% degli intervistati ritiene che difendere i dispositivi mobili dagli attacchi informatici sia molto o estremamente difficile.

Le imprese medio-grandi e il cloud

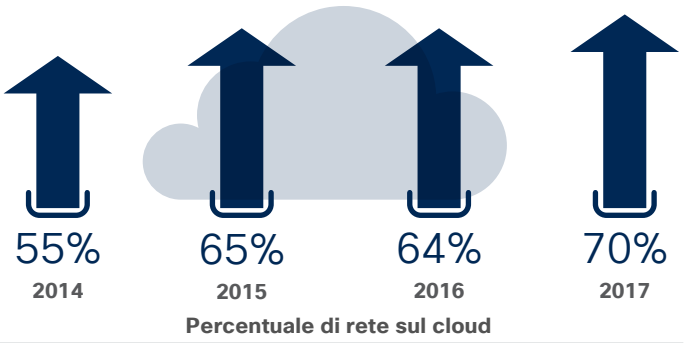
Essendo consapevoli delle sfide di sicurezza che devono affrontare, molti intervistati puntano al cloud per rafforzare le difese senza aggiungere personale o mettere a dura prova le risorse esistenti. Il dilemma è se spostare la sicurezza sul cloud sia una strategia sufficiente per respingere gli attacchi. Inoltre, le aziende non possono semplicemente scaricare la responsabilità della sicurezza trasferendo i dati nel cloud. Devono comunque essere informate sui controlli di sicurezza imposti dai provider di servizi cloud e su come le potenziali violazioni nel cloud potrebbero avere un impatto sulle risorse on-premise.

In base alla ricerca di Cisco, l'adozione dei servizi cloud tra le imprese medio-grandi è nettamente in crescita. Nel 2014, il 55% di queste aziende dichiarava di ospitare alcune delle reti tramite una qualche forma di cloud; nel 2017, la percentuale è salita al 70% (Figura 5).

Molti intervistati ritengono che il cloud possa aiutare a colmare alcune lacune nelle proprie difese, nonché a risolvere alcune manchevolezze della propria infrastruttura e delle capacità del personale. Infatti, secondo la ricerca di Cisco, il motivo principale che spinge le imprese medio-grandi a ospitare le reti nel cloud è la convinzione che questo offra una migliore sicurezza dei dati (68 per cento); il secondo motivo più comune è che l'azienda non dispone di abbastanza addetti IT interni (49 per cento). (Vedere la figura 6).

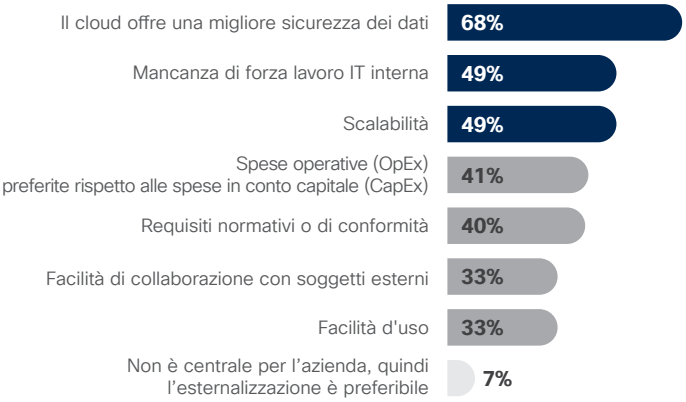
Le imprese medio-grandi apprezzano il cloud anche per la sua scalabilità (il che significa ridurre la dipendenza dell'azienda dalle proprie risorse interne) e perché consente di passare in modo flessibile alle spese operative anziché quelle in conto capitale (Figura 6).

Figura 5 Si rileva un aumento costante nell'adozione del cloud da parte delle imprese medio-grandi



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

Figura 6 Le imprese medio-grandi scelgono il cloud per la sicurezza e l'efficienza



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

Persone: trovare il personale per rafforzare la sicurezza

La buona notizia rivelata dallo Studio comparativo è che il 92% delle imprese medio-grandi ha un dirigente incaricato e responsabile della sicurezza. (Vedere la figura 7).

Se avessero un ampio personale, le imprese medio-grandi aggiungerebbero volentieri più strumenti di sicurezza come misure di protezione avanzata degli endpoint e firewall per app Web.

Le imprese medio-grandi hanno qualcosa in comune con le aziende più grandi: una carenza di personale IT che intralcia la capacità di armare le difese. Secondo la ricerca di Cisco, semplicemente non c'è abbastanza personale interno per gestire gli strumenti che potrebbero migliorare la sicurezza.

Per questo motivo molte PMI e imprese medio-grandi si rivolgono all'assistenza esterna per disporre degli esperti di cui hanno bisogno per aumentare le loro conoscenze delle minacce, risparmiare e rispondere più rapidamente alle violazioni. Il desiderio di analisi imparziali è stato indicato dalle imprese medio-grandi come il motivo più comune per esternalizzare le attività di sicurezza (Figura 8), seguito dalla convenienza e dalla necessità di reagire prontamente agli incidenti di sicurezza.

Esternalizzare l'assistenza è un'ottima opzione, perché permette alle aziende di sfruttare al meglio risorse limitate. Ma queste aziende possono incontrare difficoltà se presumono che un provider esterno o un partner cloud forniranno tutte le funzionalità di cui non dispongono internamente.

Chad Paalman, CEO di NuWave Technology Partners a Kalamazoo, Michigan, un partner Cisco, ritiene che molte PMI e imprese medio-grandi non siano consapevoli della misura di analisi e monitoraggio che i provider di sicurezza in outsourcing offrono esattamente.

Figura 7 Dirigenti incaricati e responsabili della sicurezza nelle imprese medio-grandi

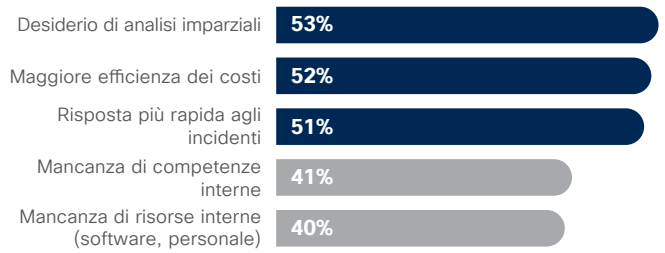
92%
Ha un dirigente responsabile della sicurezza

Qualifica del dirigente responsabile della sicurezza

42%	(CISO) Chief Information Security Officer
24%	(CSO) Chief Security Officer
10%	(CEO) Chief Executive Officer
8%	(CIO) Chief Information Officer
3%	(COO) Chief Operating Officer
5%	(CTO) Chief Technology Officer
6%	(SVP o VP) Vicepresidente senior o Vicepresidente del reparto IT
2%	(CRO o CCO) Chief Risk Officer o Chief Compliance Officer

Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

Figura 8 Le imprese medio-grandi utilizzano aiuti esterni per superare il problema della mancanza di risorse interne



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

"Molti vertici aziendali non conoscono le loro reti. Presumono che, avendo un firewall, hanno un lucchetto alla porta che impedisce a chiunque di entrare. Presumono anche che, se la sicurezza delle loro aziende è stata esternalizzata a un provider di servizi gestiti (MSP), venga effettuato anche il monitoraggio dei log oppure che il servizio includa il rilevamento delle intrusioni".

Chad Paalman, CEO di NuWave Technology Partners

Comunque, in conclusione, le PMI e le imprese medio-grandi contano sul fatto che i partner esterni offrano:

- Servizi di consulenza in outsourcing (57 per cento),
- Reazione agli incidenti (54 per cento),
- Monitoraggio della sicurezza (51 per cento).

Tuttavia, sono meno inclini a esternalizzare attività come l'intelligence sulle minacce (39 per cento). (Vedere la figura 9).

La buona notizia è che sembra che le imprese medio-grandi stiano accantonando alcune delle loro limitate risorse per comprendere e rispondere alle minacce, ad esempio per attività come l'intelligence sulle minacce e la reazione agli incidenti.

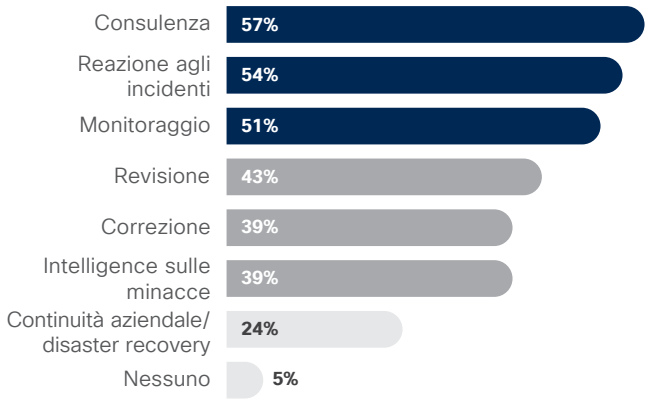
Processi: controlli regolari per gestire la sicurezza

Processi di sicurezza completi e regolari, ad esempio i controlli per le risorse di alto valore e le revisioni delle procedure di sicurezza, aiutano le aziende a identificare i punti deboli delle loro difese. Tali processi non sono diffusi nelle PMI e nelle imprese medio-grandi quanto dovrebbero esserlo, forse a causa della mancanza di personale.

Ad esempio, secondo lo Studio comparativo di Cisco delle infrastrutture di sicurezza del 2018, è meno probabile che le imprese medio-grandi, rispetto a quelle più grandi, affermino di rivedere le procedure di sicurezza regolarmente, di disporre di strumenti in grado di rivedere le funzionalità di sicurezza e di analizzare gli incidenti di sicurezza abitualmente (Figura 10).

Una nota positiva è che il 91% delle imprese medio-grandi ha dichiarato di effettuare esercitazioni per testare i piani di reazione agli incidenti almeno una volta all'anno. Tuttavia, come per la loro dipendenza da cloud e da partner in outsourcing, il dubbio è se tali piani di reazione agli incidenti siano adeguati per respingere hacker sempre più sofisticati.

Figura 9 Le imprese medio-grandi esternalizzano i servizi di consulenza e di reazione agli incidenti



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

Figura 10 È meno probabile che le imprese medio-grandi siano concordi sull'uso dei processi operativi

Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

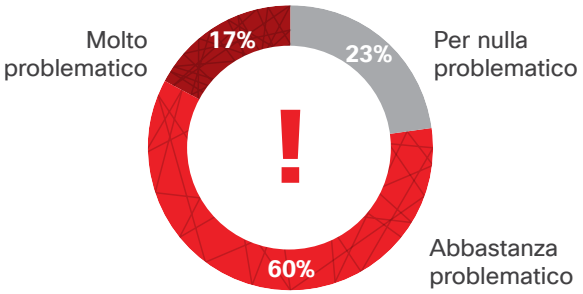
Connettere persone, processi e tecnologia: la sfida dell'orchestrazione

Se le PMI e le imprese medio-grandi aggiungessero più prodotti per la sicurezza e fornitori alle loro difese e dedicassero risorse IT a gestire questi prodotti, le loro aziende gestirebbero meglio la sicurezza? Potrebbe essere vero anche il contrario, almeno in termini di comprensione e orchestrazione degli avvisi di sicurezza.

La maggior parte delle PMI e delle imprese medio-grandi oggi riconosce che creando un ambiente più complesso con diversi prodotti e fornitori, aumentano anche le loro responsabilità. Ad esempio, il 77% delle imprese medio-grandi ha trovato abbastanza o molto problematico orchestrare gli avvisi di così tante soluzioni (Figura 11).

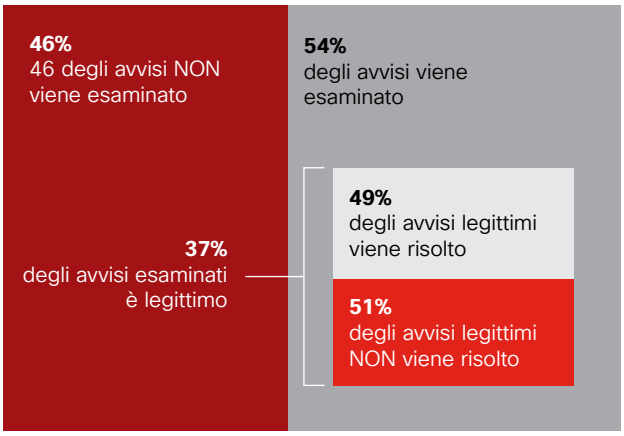
Quando le aziende cercano di analizzare questi avvisi, la combinazione delle problematiche di personale, processi e tecnologia può comportare che molti avvisi non vengano indagati, come emerge dallo Studio comparativo (Figura 12):

Figura 11 È meno probabile che le imprese medio-grandi siano concordi sull'uso dei processi operativi



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

Figura 12 Percentuale di avvisi di sicurezza che non vengono analizzati o risolti



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2018

Suggerimenti per il futuro

Tecnologia

Idealmente, quando le aziende valutano nuovi strumenti, possono evitare di aumentare il numero di fornitori che gestiscono e degli avvisi a cui devono rispondere.

Tenendo presente questo, i prodotti sono costruiti considerando l'apertura? Come si integreranno con gli altri in termini di condivisione dei dati e intelligence sulle minacce? Le console di gestione sono integrate?

Se un fornitore dice che i prodotti sono progettati per integrarsi e funzionare con gli altri, si tratta di prodotti già pronti per l'uso o l'acquirente dovrà fare un lavoro considerevole relativo alle API?

Il machine learning, seppur circondato da molte aspettative, ha un ruolo non indifferente nell'ambito della sicurezza. Tuttavia, cerca di adottare un machine learning presente come livello di rilevamento all'interno di prodotti già implementati rispetto a un prodotto stand-alone di un altro fornitore, perché sarebbe solo un altro prodotto da gestire.

Persone e processi

Per farla breve, sviluppa una strategia che migliori la cybersecurity. Solo il 38% delle PMI e delle imprese medio-grandi dispone di una strategia di valutazione dei rischi informatici attiva, secondo il Vistage Research Center, un centro risorse per vertici aziendali.[6]

La pianificazione prevede che gli utenti finali ricevano una formazione adeguata? Le polizze assicurative coprono il calo degli affari in seguito a un attacco informatico? Perché non creare piani di comunicazione di crisi e continuità aziendale per consentire un recupero più rapido e prevenire i danni alla reputazione?

Inoltre, i responsabili IT devono spiegare in termini chiari ciò che i dirigenti aziendali vogliono davvero sapere per quanto riguarda le violazioni:

- Qual è l'impatto per l'azienda?
- Quali misure sta adottando il team di sicurezza per contenere e analizzare la minaccia. Quanto tempo ci vorrà per riprendere le normali operazioni?[7]

"Adottando una serie di piattaforme e strumenti di sicurezza che interagiscono, anziché elementi eterogenei che possono effettivamente entrare in conflitto tra loro, si amplifica l'efficacia della sicurezza e si semplifica la gestione".

Ben M. Johnson, CEO di Liberty Technology

"Le PMI e le imprese medio-grandi devono valutare questi rischi e sviluppare piani di risposta prima di una violazione, non dopo".

Chad Paalman, NuWave Technology Partners

6 Cyberthreats and Solutions for Small and Midsize Businesses, Vistage Research Center, 2018. Sviluppato in collaborazione con Cisco e The National Center for the Middle Market. Disponibile all'indirizzo: https://www.vistage.com/research-center/business-operations/risk-management/20180503-22912/.

7 Report semestrale di Cisco sulla cybersecurity 2017: https://www.cisco.com/c/dam/global/es_mx/solutions/security/pdf/cisco-2017-midyear-cybersecurity-report.pdf. 13 Ibid.

Conclusioni

Un consiglio finale per le PMI e le imprese medio-grandi che desiderano apportare miglioramenti alla cybersecurity è rendersi conto che un cambiamento incrementale è meglio di nessun cambiamento. In breve, non devono lasciare che il desiderio di un approccio alla sicurezza " perfetto" impedisca di farlo diventare " migliore" . La perfezione, come in tutte le cose, non esiste.

Le PMI e le imprese medio-grandi devono anche comprendere che non esiste alcuna soluzione tecnologica definitiva per risolvere tutte le loro sfide di cybersecurity. Il panorama delle minacce è troppo complesso e dinamico. La superficie di attacco è in continua espansione ed evoluzione. E, in risposta, le strategie e tecnologie per la sicurezza devono continuamente evolversi di pari passo.

Per ulteriori informazioni sull'approccio alla sicurezza incentrato sulle minacce di Cisco, visita il sito cisco.com/go/security.

Sede centrale Americhe
Cisco Systems, Inc.
San Jose, California (USA)

Sede centrale Asia e Pacifico
Cisco Systems (USA) Pte. Ltd.
Singapore

Sede centrale Europa
Cisco Systems International BV Amsterdam,
Paesi Bassi

Le sedi Cisco nel mondo sono oltre 200. Gli indirizzi e i numeri di telefono e di fax delle sedi italiane sono disponibili nel sito Web Cisco all'indirizzo https://www.cisco.com/c/it_it/about/local-offices.html.

Pubblicato nel luglio 2018