Cisco
Report annuale sulla cybersecurity 2017

cisco

Sommario

PANORAMICA GENERALE E RISULTATI PRINCIPALI 3
INTRODUZIONE 8
L'ESPANSIONE DELLA SUPERFICIE DI ATTACCO 10
COMPORTAMENTO DEGLI HACKER 13
La fase di ricognizione 13
Metodi di attacco tramite Web: le minacce con la " coda corta" consentono ai criminali informatici di porre le basi per le campagne 13
La fase di adescamento 15
Vettori di attacco Web: Flash perde importanza, ma gli utenti devono rimanere vigili 15
Sicurezza delle applicazioni: come gestire il rischio delle connessioni OAuth in seguito al boom delle app 16
La fase di dirottamento 20
La scomparsa dei principali exploit kit offre opportunità per entità minori e nuovi arrivi 20
Malvertising: gli hacker utilizzano intermediari per aumentare velocità e agilità 22
L'indagine ha rilevato che il 75% delle aziende è interessata da infezioni adware 23
La quantità complessiva di spam è in aumento, così come la percentuale degli allegati dannosi 25
La fase di installazione 30
Metodi di attacco Web: una panoramica sulla "coda lunga" svela le minacce che gli utenti possono evitare con facilità 30
Tutti i settori rischiano di venire a contatto con il malware: gli hacker vedono valore ovunque 31
Panoramica dell'attività di blocco del Web in base alle aree geografiche 32
Tempi di rilevamento: una metrica essenziale per misurare i progressi degli addetti alla sicurezza 33
Tempo di evoluzione: per alcune minacce, il cambiamento è costante 34
COMPORTAMENTO DEGLI ADDETTI ALLA SICUREZZA 42
Vulnerabilità in declino nel 2016 42
Middleware: gli hacker individuano opportunità nel software privo di patch 44
Tempo per le patch: azzerare il tempo per il ripristino 45
STUDIO COMPARATIVO DI CISCO DELLE INFRASTRUTTURE DI SICUREZZA DEL 2017 49
Opinioni: gli esperti della sicurezza hanno fiducia negli strumenti, ma non sono certi di usarli in modo efficace 49
Limiti: tempo, risorse qualificate e fondi incidono sulla capacità di rispondere alle minacce 51
Risultato: un maggior numero di aziende subisce perdite in conseguenza di violazioni 55
Risultati: un controllo più minuzioso contribuirà al miglioramento della sicurezza 58
Affidabilità o costi: che cosa determina gli acquisti di soluzioni di sicurezza? 61
Riepilogo: risultati emersi dallo studio comparativo 62
SETTORE 64
Sicurezza della catena del valore: il successo nel mondo digitale dipende dalla mitigazione del rischio di terze parti 64
Aggiornamento geopolitico: crittografia, affidabilità e una richiesta di trasparenza 65
Crittografia ad alta velocità: una soluzione scalabile per proteggere i dati in transito 66
Prestazioni e adozione di rete contro maturità della sicurezza 67
CONCLUSIONI 71
Per una superficie di attacco in rapida espansione serve un approccio alla sicurezza integrato e interconnesso 71
L'obiettivo chiave: ridurre lo spazio operativo degli hacker 73
INFORMAZIONI SU CISCO 74
Contributi al report annuale di Cisco sulla cybersecurity 2017 75
APPENDICE 78

Sintesi

Via via che la superficie di attacco si amplia, gli addetti alla sicurezza devono concentrarsi sull'obiettivo più importante: ridurre lo spazio operativo degli hacker.

I criminali informatici non hanno mai avuto a disposizione così tanti strumenti. Oltretutto sono capaci di usarli nel momento più opportuno per ottenere il massimo effetto. L'enorme crescita degli endpoint mobili e del traffico online va a loro favore, poiché hanno più spazio in cui agire e una gamma più ampia di obiettivi e approcci tra cui scegliere.

I responsabili della sicurezza possono avvalersi di una varietà di strategie per affrontare le sfide di un panorama delle minacce in continua espansione. Possono acquistare le soluzioni più all'avanguardia che funzionano singolarmente per fornire informazioni e protezione. Possono inoltre competere per il personale in un mercato in cui le competenze scarseggiano e i budget sono limitati.

Ma è pressoché impossibile bloccare tutti gli attacchi. Si può, però, ridurre al minimo il rischio e l'impatto delle minacce limitando lo spazio operativo degli hacker e, quindi, la loro capacità di compromettere le risorse. Una misura che si può adottare è quella di semplificare l'insieme degli strumenti di sicurezza riunendoli in un'architettura di sicurezza integrata e interconnessa.

Gli strumenti di sicurezza integrata che interagiscono in un'architettura automatizzata possono semplificare il processo di rilevamento e di mitigazione delle minacce, consentendo quindi di avere tempo per risolvere problemi più complessi e incalzanti. Molte aziende utilizzano una media di cinque di soluzioni di altrettanti fornitori (pagina 53). In molti casi i team di sicurezza riescono ad analizzare solo la metà degli avvisi di sicurezza che ricevono su base giornaliera.

Il Report annuale di Cisco sulla cybersecurity 2017 riunisce le ricerche, le analisi e le opinioni di Cisco Security Research. Evidenziamo l'inarrestabile tira e molla tra hacker che cercano di guadagnare più tempo per agire e addetti alla sicurezza che lavorano per bloccare le opportunità che i criminali informatici cercano di sfruttare. Analizziamo i dati stilati dai ricercatori sulle minacce di Cisco e di altri esperti. La nostra ricerca e la nostra analisi sono concepite per aiutare le aziende a rispondere in modo efficace alle minacce sofisticate e in rapida evoluzione di oggi.

Questo report è suddiviso nelle seguenti sezioni:

Comportamento degli hacker

In questa sezione esaminiamo le modalità in cui gli hacker perlustrano le reti vulnerabili e diffondono il malware. Viene spiegato come vengono sfruttati strumenti come e-mail, applicazioni cloud di terze parti e adware. Vengono inoltre illustrati i metodi che i criminali informatici utilizzano durante la fase di installazione di un attacco. Questa sezione introduce inoltre la nostra ricerca sul "tempo di evoluzione" (TTE, Time To Evolve) che mostra come gli hacker mantengono aggiornate le loro tattiche ed eludono il rilevamento. Sono inoltre riportati gli aggiornamenti sugli sforzi volti a ridurre la mediana dei tempi di rilevamento (TTD). Inoltre, sono presentati gli studi più recenti di Cisco sul rischio di malware per diversi settori e aree geografiche.

Comportamento degli addetti alla sicurezza

In questa sezione sono riportati gli aggiornamenti sulle vulnerabilità. Innanzitutto si pone l'accento sui punti deboli emergenti nelle librerie del middleware che per gli hacker si concretizzano nell'opportunità di utilizzare gli stessi strumenti in molte applicazioni diverse, riducendo così i tempi e i costi necessari per compromettere i computer degli utenti. Inoltre viene illustrata la ricerca sulle tendenze relative al patching. Viene evidenziato il vantaggio di offrire agli utenti aggiornamenti con una frequenza periodica per favorire l'adozione di versioni più sicure delle soluzioni di produttività e dei browser Web più diffusi.

Studio comparativo di Cisco delle infrastrutture di sicurezza del 2017

Questa sezione analizza i risultati del nostro terzo studio comparativo delle infrastrutture di sicurezza. Lo studio si basa sulle opinioni degli esperti della sicurezza in relazione all'infrastruttura di sicurezza delle aziende in cui essi operano. Quest'anno gli esperti della sicurezza evidenziano una certa fiducia degli strumenti che hanno a disposizione, ma non sono certi del fatto che tali risorse possano aiutarli a ridurre lo spazio operativo degli hacker. Lo studio indica anche che le violazioni della sicurezza di dominio pubblico hanno un impatto nefasto ma misurabile sulle opportunità, il fatturato e i clienti. Allo stesso tempo, a causa delle violazioni, le aziende sono spinte a migliorare tecnologie e processi.

Per un'analisi più approfondita sullo stato della sicurezza nelle aziende, vedere pag. 49.

Settore

In questa sezione viene evidenziato quanto sia importante garantire la sicurezza della catena del valore. Viene analizzato il danno potenziale che viene inferto ai governi che non divulgano informazioni su vulnerabilità ed exploit zero-day, riscontrati nei prodotti dei fornitori. Inoltre, è stato valutato l'utilizzo della crittografia rapida come soluzione per la protezione dei dati in ambienti ad alta velocità. Infine, vengono delineate le sfide di sicurezza aziendale a fronte della crescita del traffico Internet globale e della superficie di attacco.

Conclusioni

Nelle conclusioni si consiglia agli addetti alla sicurezza di adeguare le proprie procedure di sicurezza in modo da affrontare meglio le sfide tipiche di questo ambito in tutta la catena delle fasi dell'attacco, riducendo quindi lo spazio operativo dei criminali informatici. Questa sezione offre indicazioni specifiche sulla creazione di un approccio integrato e semplificato alla sicurezza: un approccio atto a collegare i dirigenti operativi, policy, protocolli e strumenti per prevenire, rilevare e mitigare le minacce.

Risultati principali

- Nel 2016 tre fra i principali exploit kit (Angler, Nuclear e Neutrino) sono improvvisamente scomparsi dalla scena, consentendo ad attori nuovi o più piccoli di farsi strada.
- Secondo lo studio comparativo di Cisco delle infrastrutture di sicurezza del 2017, la maggior parte delle aziende utilizza più di cinque fornitori di sicurezza e più di cinque prodotti di sicurezza nel proprio ambiente. Il 55% degli esperti della sicurezza utilizza almeno 6 fornitori rispetto al 45% che ne usa da 1 a 5. Il 65% invece utilizza almeno 6 prodotti.
- Secondo lo studio comparativo, i vincoli principali all'adozione di prodotti e soluzioni di sicurezza avanzata sono: budget (citato dal 35% degli intervistati), compatibilità dei prodotti (28%), certificazioni (25%) e competenze (25%).
- Lo studio comparativo di Cisco delle infrastrutture di sicurezza del 2017 ha rilevato che, a causa dei diversi vincoli, le aziende possono analizzare solo il 56% degli avvisi di sicurezza che ricevono quotidianamente. Di questi, la metà (28%) è ritenuta affidabile ma viene posto rimedio a meno della metà (46%) degli avvisi legittimi. Inoltre, il 44% dei direttori delle operazioni di sicurezza riceve oltre 5000 avvisi di sicurezza al giorno.
- Nel 2016 il 27% delle applicazioni cloud connesse di terze parti introdotte dai dipendenti negli ambienti aziendali ha comportato un elevato rischio per la sicurezza. Le connessioni tramite autenticazione aperta (OAuth) intervengono sull'infrastruttura aziendale e possono comunicare liberamente con il cloud e con le piattaforme SaaS (Software-as-a-Service) aziendali dopo che gli utenti consentono l'accesso.
- Da una ricerca condotta da Cisco su 130 aziende di tutti i settori è emerso che il 75% di tali aziende è interessata da infezioni adware. Gli hacker possono potenzialmente utilizzare queste infezioni per facilitare altri attacchi malware.
- I criminali che lanciano le campagne di malvertising utilizzano sempre più intermediari (detti anche "gate") che consentono loro di muoversi più velocemente, di mantenere il proprio spazio operativo e di eludere il rilevamento. Questi link intermedi consentono agli autori degli attacchi di passare rapidamente da un server dannoso a un altro senza modificare il reindirizzamento iniziale.
- Lo spam rappresenta circa i due terzi (65%) del volume complessivo di e-mail e la nostra ricerca indica che il volume globale sta crescendo a causa di grandi e prospere botnet specifiche per l'invio di spam. Secondo i ricercatori sulle minacce di Cisco, una percentuale variabile dall'8 al 10% circa di spam globale rilevata nel 2016 potrebbe essere classificata come dannosa. Inoltre, la percentuale di spam con allegati e-mail dannosi è in aumento e sembra che gli hacker stiano sperimentando un'ampia gamma di tipi di file per garantire che le proprie campagne vadano a buon fine.
- Secondo lo Studio comparativo delle infrastrutture di sicurezza, le aziende che non hanno ancora subito una violazione della sicurezza potrebbero credere che le proprie reti siano protette. Probabilmente questa fiducia non è del tutto fondata, considerando che il 49% degli esperti della sicurezza intervistati ha dichiarato che le rispettive aziende si sono ritrovate esposte al clamore pubblico in seguito a una violazione della sicurezza.

- Inoltre, dallo Studio comparativo di Cisco delle infrastrutture di sicurezza del 2017 emerge che circa un quarto delle aziende che hanno subito un attacco ha perso opportunità di business. Quattro su 10 hanno indicato che tali perdite sono ingenti. Un'azienda su cinque ha perso clienti a causa di un attacco e quasi il 30% ha subito perdite di fatturato.
- Secondo gli intervistati dello studio comparativo, in caso di violazioni gli ambiti con più probabilità di subire ricadute negative sono stati operazioni e finanze (36 e 30% rispettivamente), seguiti dalla reputazione del marchio e dalla fidelizzazione dei clienti (entrambi al 26%).
- Le interruzioni di rete causate dalle violazioni della sicurezza spesso possono avere un impatto duraturo. Secondo lo studio comparativo, il 45% delle interruzioni è durato da 1 a 8 ore, il 15% dalle 9 alle 16 ore e l'11% si è protratto tra le 17 e le 24 ore. Il 41% (vedere pagina 55) di queste interruzioni ha interessato tra l'11 e il 30% dei sistemi.
- Le vulnerabilità nel middleware, un software che funge da ponte o connettore tra piattaforme o applicazioni, diventano sempre più evidenti, suscitando quindi la preoccupazione che il middleware stia diventando un vettore di minaccia diffuso. Molte aziende si affidano al middleware, quindi la minaccia potrebbe colpire ogni settore. Nel corso di un progetto Cisco®, i ricercatori delle minacce hanno scoperto che la gran parte delle nuove vulnerabilità analizzate era riconducibile all'utilizzo del middleware.
- La frequenza degli aggiornamenti software può influire sul comportamento degli utenti quando si tratta di installare patch e aggiornamenti. Secondo i nostri ricercatori, la pianificazione periodica e prevedibile degli aggiornamenti porta gli utenti ad aggiornare prima il software, riducendo il lasso di tempo in cui i criminali informatici hanno la possibilità di sfruttare le vulnerabilità.
- Dallo Studio comparativo di Cisco delle infrastrutture di sicurezza del 2017 emerge che la maggior parte delle aziende affida almeno il 20% della propria sicurezza a fornitori terzi e coloro che si affidano di più a queste risorse sono più propensi ad avvalersene maggiormente.

Introduzione

Introduzione

Gli hacker sfruttano un'ampia e diversificata gamma di tecniche per accedere alle risorse aziendali e per garantirsi un tempo illimitato per agire. Le loro strategie riguardano tutti gli elementi basilari, tra cui:

- Sfruttare gli intervalli nell'applicazione di patch e aggiornamenti
- Attirare gli utenti in trappole create con il social engineering
- Inserire malware in contenuti online apparentemente legittimi come la pubblicità

Hanno anche molte altre capacità, dallo sfruttamento delle vulnerabilità del middleware alla diffusione di spam dannoso. Una volta raggiunti i loro obiettivi, possono tranquillamente terminare le proprie operazioni.

I criminali informatici lavorano ininterrottamente per sviluppare le minacce, si muovono a una velocità ancora maggiore e trovano modi per ampliare il proprio spazio operativo. La crescita vertiginosa del traffico Internet, dovuta soprattutto alla maggiore velocità di Internet mobile e alla proliferazione dei dispositivi online, va a loro favore perché contribuisce ad ampliare la superficie di attacco. Di conseguenza, si accresce il rischio per le aziende. Lo studio comparativo di Cisco delle infrastrutture di sicurezza del 2017 mostra che un terzo delle aziende che hanno subito un attacco ha perso almeno il 20% di fatturato. Il 49% degli intervistati ha indicato che la propria azienda si è ritrovata sotto i riflettori in seguito a una violazione della sicurezza.

Quante aziende possono subire questo tipo di perdite di profitti e non risentirne? Gli addetti alla sicurezza devono concentrare le proprie risorse sulla riduzione dello spazio operativo degli hacker che così avranno enormi difficoltà a ottenere l'accesso a importanti risorse aziendali e a svolgere le proprie attività senza essere individuati.

L'automazione è essenziale per centrare questo obiettivo. Aiuta a capire quale sia l'attività normale nell'ambiente di rete, in modo da poter concentrare risorse ridotte sull'analisi e la risoluzione delle minacce reali. Semplificando le operazioni di sicurezza, si incrementa anche la sicurezza delle operazioni volte a eliminare l'illimitato spazio operativo dei criminali informatici. Tuttavia, lo studio comparativo indica che la maggior parte delle aziende utilizza più di 5 soluzioni di oltre cinque fornitori (pagina 53).

Un tale groviglio di prodotti tecnologici e l'enorme quantità di avvisi di sicurezza comporta inequivocabilmente meno protezione, non la intensifica di certo. Assumere personale qualificato nell'ambito della sicurezza può senz'altro aiutare, perché, secondo logica, più sono gli esperti in squadra, più l'azienda ha migliori capacità di gestire la tecnologia e ottenere migliori risultati. Però, tale eventualità è poco probabile vista la scarsità di risorse qualificate e i limitati budget per la sicurezza. Anzi, la maggior parte delle aziende deve cavarsela con gli esperti che ha già a disposizione. In genere le aziende si affidano a professionisti esterni per rafforzare i propri team di sicurezza e per non sforare i limiti del budget.

La risposta reale per affrontare queste sfide, come verrà spiegato più avanti nel report, è quella di far lavorare persone, processi e tecnologie in modo integrato. Per adottare un approccio operativo alla sicurezza, bisogna identificare realisticamente le risorse che l'azienda deve proteggere e quali misure devono essere utilizzate per metterle al sicuro.

Il report annuale di Cisco sulla cybersecurity 2017 presenta gli ultimi progressi nel settore della sicurezza, volti ad aiutare le aziende e gli utenti a difendersi dagli attacchi. Inoltre esaminiamo le tecniche e le strategie che gli hacker utilizzano per aggirare le difese. Nel report vengono inoltre illustrati i risultati principali dello Studio comparativo di Cisco delle infrastrutture di sicurezza del 2017, che analizza la postura di sicurezza delle aziende e la percezione sulla propria rapidità di intervento nella difesa dagli attacchi.

L’espansione della superficie di attacco

L'espansione della superficie di attacco

Dispositivi mobili. Cloud pubblico. Infrastruttura cloud. Comportamento degli utenti. Gli esperti della sicurezza che hanno partecipato al terzo Studio comparativo delle infrastrutture di sicurezza hanno indicato tutti questi elementi come fonti principali di preoccupazione quando si pensa al rischio di esposizione a un attacco informatico per la propria azienda (**figura 1**). Ciò è comprensibile: la proliferazione di dispositivi mobili fa aumentare il numero di endpoint da proteggere. Il cloud sta ampliando il perimetro di sicurezza e gli utenti sono, e saranno sempre, un anello debole della catena di sicurezza.

Con le aziende che adottano la digitalizzazione, e Internet of Everything (IoE)[1] che inizia a prendere forma, le preoccupazioni degli addetti alla sicurezza aumenteranno sempre più. La superficie di attacco potrà solamente aumentare, offrendo ai criminali informatici più spazio per agire.

Da oltre un decennio, il Cisco® Visual Networking Index (VNI) fornisce previsioni sul traffico IP globale e analizza i fattori dinamici che facilitano la crescita della rete. Si considerino queste statistiche dell'ultimo report, *The Zettabyte Era—Trends and Analysis*:[2]

- Il traffico IP globale annuo supererà la soglia dello zettabyte (ZB) entro la fine del 2016 e raggiungerà i 2,3 ZB annuali entro il 2020. (Uno zettabyte equivale a 1000 exabyte o a 1 miliardo di terabyte). Ciò significa che il traffico IP globale triplicherà nei prossimi 5 anni.
- Entro il 2020 due terzi (66%) del traffico IP totale saranno generati da dispositivi Wi-Fi e mobili mentre i dispositivi cablati rappresenteranno solo il 34%.
- Tra il 2015 e il 2020 si assisterà quasi al raddoppio della velocità media della banda larga.
- Entro il 2020 l'82% di tutto il traffico Internet consumer a livello globale sarà rappresentato dal traffico video IP, che arriverà al 70% nel 2015.

Figura 1 Le principali fonti di preoccupazione degli esperti della sicurezza in merito agli attacchi informatici

Dispositivi mobili	Dati nel cloud pubblico	Infrastruttura cloud	Comportamento dell'utente (che, ad esempio, fa clic su link dannosi nelle e-mail o nei siti Web)
58%	57%	57%	57%

Percentuale di esperti della sicurezza che ritiene queste categorie molto o estremamente impegnative

Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Scaricare il grafico del 2017 al link seguente: **www.cisco.com/go/acr2017graphics**

[1] "Internet of Everything FAQ", Cisco: http://ioeassessment.cisco.com/learn/ioe-faq.
[2] *The Zettabyte Era—Trends and Analysis*, Cisco VNI, 2016: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html.

Inoltre, il white paper Cisco *VNI™ Forecast and Methodology, 2015–2020*[3] prevede che il volume di traffico Internet globale nel 2020 sarà di 95 volte superiore rispetto al 2005.

Naturalmente, anche gli opportunisti criminali informatici prestano estrema attenzione a queste tendenze. Alcuni di quelli che agiscono nell'economia sommersa stanno già intraprendendo iniziative per diventare più agili in questo ambiente in continua evoluzione. Stanno creando attacchi molto mirati e diversificati, progettati appositamente per andare a buon fine nella superficie di attacco in espansione. Nel frattempo, i team di sicurezza sono continuamente in stato di allerta, subissati dagli avvisi. Devono affidarsi a una serie di prodotti di sicurezza nell'ambiente di rete che servono solo ad aggiungere complessità e possono anche aumentare la suscettibilità alle minacce di un'azienda.

Le aziende devono:

- Integrare le tecnologie di sicurezza
- Semplificare le operazioni di sicurezza
- Affidarsi maggiormente all'automazione

Questo approccio consentirà di ridurre le spese operative, diminuire il carico di lavoro del personale addetto alla sicurezza e migliorare i risultati di sicurezza. Soprattutto, conferirà agli addetti alla sicurezza la possibilità di dedicare più tempo all'abolizione dello spazio incontrollato in cui gli hacker possono agire al momento.

[3] *Cisco VNI Forecast and Methodology, 2015–2020*, Cisco VNI, 2016: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html.

Comportamento degli hacker

Comportamento degli hacker

Ricognizione | Adescamento | Dirottamento | Installazione

Gli hacker cercano, identificano e selezionano gli obiettivi.

Metodi di attacco tramite Web: le minacce con la "coda corta" consentono ai criminali informatici di gettare le basi per le campagne

La ricognizione è, ovviamente, una fase fondamentale del lancio di attacchi informatici, durante la quale gli autori vanno alla ricerca di infrastrutture Internet vulnerabili o di punti deboli delle reti che consentano loro di ottenere l'accesso ai computer degli utenti e, in ultima analisi, di infiltrarsi nelle aziende.

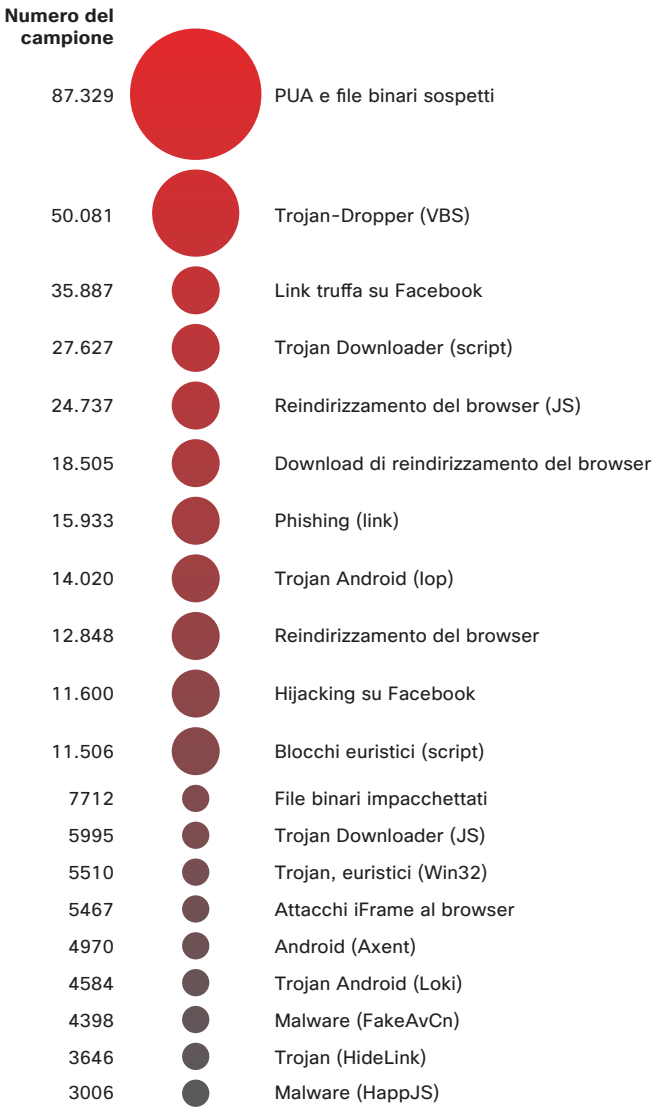
I file binari di Windows sospetti e le applicazioni potenzialmente indesiderate (PUA) si stagliano inequivocabilmente in cima alla classifica dei metodi di attacco tramite Web per il 2016 (**vedere la figura 2**). I file binari di Windows sospetti veicolano minacce quali spyware e adware, mentre le estensioni dannose per i browser sono un esempio di PUA.

Le truffe su Facebook, costituite da false offerte e contenuti multimediali associati a finti sondaggi si sono classificati al terzo posto. La costante prevalenza delle truffe su Facebook nelle nostre classifiche annuali e semestrali relative ai casi di malware osservati più di frequente evidenzia il ruolo fondamentale del social engineering in molti attacchi informatici. Facebook dispone di circa 1,8 miliardi di utenti attivi al mese in tutto il mondo[4] ed è il terreno di caccia ideale per i criminali informatici e altri attori intenzionati a truffare gli utenti. Una notizia positiva è costituita dal recente annuncio dell'azienda di provvedimenti che verranno assunti per eliminare le notizie false e gli hoax. I critici ipotizzano che questi contenuti possano avere influito sul voto in occasione delle elezioni presidenziali del 2016 negli Stati Uniti.[5]

[4] Statistiche di Facebook, settembre 2016: http://newsroom.fb.com/company-info/.

[5] "Zuckerberg Vows to Weed Out Facebook 'Fake News'", di Jessica Guynn e Kevin McCoy, *USA Today*, 14 novembre 2016: http://www.usatoday.com/story/tech/2016/11/13/zuckerberg-vows-weed-out-facebook-fake-news/93770512/.

Figura 2 Malware più comuni



Fonte: Cisco Security Research

Il malware per il reindirizzamento dei browser completa l'elenco delle prime cinque tipologie di malware rilevate più frequentemente nel 2016. Come illustrato nel *Report semestrale di Cisco sulla cybersecurity 2016*,[6] le infezioni dei browser possono esporre gli utenti alla pubblicità dannosa (malvertising), che gli autori degli attacchi utilizzano per diffondere il ransomware e altre campagne di malware. Gli esperti di minacce di Cisco sostengono che la pubblicità dannosa, costituita da ad injector, hijacker delle impostazioni del browser, utility e downloader rappresenti un problema in costante espansione. Infatti, nell'ambito della nostra recente ricerca sul problema dell'adware, abbiamo rilevato infezioni di questo tipo nel 75% delle aziende esaminate. (Per ulteriori informazioni su questo argomento, vedere "L'indagine ha rilevato che il 75% delle aziende è interessata da infezioni adware" a pagina 23).

Altri tipi di malware elencati nella **figura 3**, come quello che abusa di JavaScript o di iFrame, sono progettati per agevolare le infezioni dei browser. I trojan (dropper e downloader) figurano tra i primi cinque tipi di malware rilevati più frequentemente, il che dimostra come essi siano tuttora strumenti molto diffusi per ottenere l'accesso iniziale ai computer degli utenti e, in seguito, alle reti aziendali.

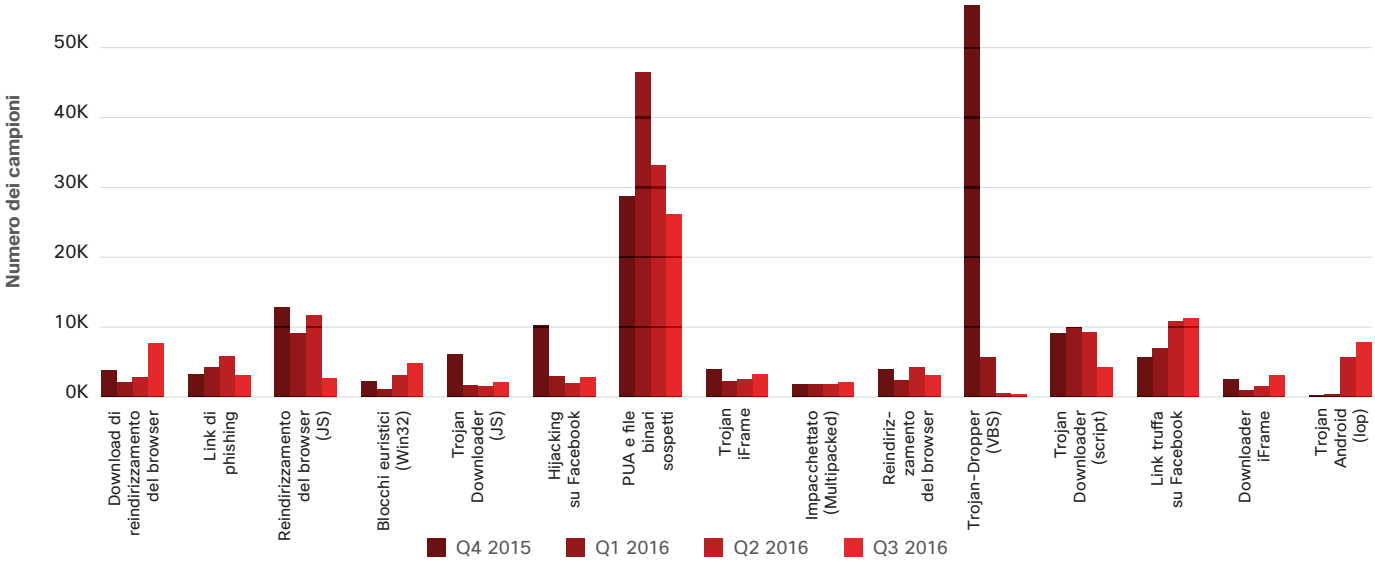
Un'altra tendenza da tenere sotto controllo è l'uso costantemente elevato di malware che ha per obiettivo gli utenti di Android. Negli ultimi 2 anni, i trojan per Android hanno scalato in modo continuo la classifica e, nel 2016, si sono posizionati tra i 10 tipi di malware più rilevati.

Il malware Loki, visualizzato all'estremità del grafico mostrato nella **figura 2** (vedere la pagina precedente), è particolarmente problematico, poiché può replicarsi e infettare altri file e programmi.

La **figura 3** illustra le tendenze in fatto di malware che i ricercatori di Cisco hanno osservato dalla fine del 2015 e mostra come gli hacker abbiano impresso una decisa svolta alla fase di ricognizione degli attacchi Web, giacché ora più minacce hanno per obiettivo browser e plug-in vulnerabili. Questo cambiamento si deve al fatto che gli autori degli attacchi si affidano in misura sempre maggiore al malvertising, dal momento che sta diventando sempre più difficile accedere a un gran numero di utenti attraverso i tradizionali vettori di attacco Web. (Vedere la sezione successiva, "Vettori di attacco Web: Flash perde importanza, ma gli utenti devono rimanere vigili" a pagina 15).

Il messaggio per gli utenti, gli esperti della sicurezza e le aziende è chiaro: è indispensabile assicurarsi che i browser siano sicuri e disattivare o rimuovere i plug-in per i browser non necessari può contribuire in modo significativo alla prevenzione delle infezioni da malware che, come le campagne di ransomware, possono dare origine ad attacchi più imponenti, dannosi e costosi. Questi semplici provvedimenti riducono notevolmente l'esposizione alle più diffuse minacce basate sul Web e possono impedire agli hacker di individuare lo spazio operativo necessario per attuare la fase successiva della catena delle fasi dell'attacco: l'adescamento.

Figura 3 Il malware più comune, Q4 2015–Q3 2016



Fonte: Cisco Security Research

[6] *Report semestrale di Cisco sulla cybersecurity 2016*: http://www.cisco.com/c/m/en_us/offers/sc04/2016-midyear-cybersecurity-report/index.html.

Ricognizione | **Adescamento** | Dirottamento | Installazione

Gli hacker abbinano il malware di accesso remoto agli exploit in payload veicolabili.

Vettori di attacco Web: Flash perde importanza, ma gli utenti devono rimanere vigili

Adobe Flash è stato per lungo tempo un interessante vettore di attacco Web per i criminali informatici intenzionati ad attaccare e compromettere i sistemi. Tuttavia, la continua diminuzione dei contenuti Adobe Flash nel Web e la crescente consapevolezza circa le vulnerabilità di Flash, rendono sempre più difficile per i criminali informatici condurre attacchi contro gli utenti su larga scala come, invece, avveniva in passato.

Adobe stessa sta abbandonando lo sviluppo e il supporto completo della piattaforma software e ha incoraggiato gli sviluppatori ad adottare standard più recenti, come HTML5[7] e anche i provider dei browser Web più diffusi stanno assumendo posizioni molto precise sull'uso di Flash. Ad esempio, nel 2016 Google ha annunciato che eliminerà dal proprio browser, Chrome, il supporto per Adobe Flash.[8] Firefox, invece, continua a supportare i contenuti Flash esistenti, ma ha deciso di bloccare "alcuni contenuti Flash non indispensabili per l'esperienza utente".[9]

Flash starà anche perdendo importanza, ma gli sviluppatori di exploit kit contribuiscono alla sua sopravvivenza come vettore di attacco. Tuttavia, alcuni segnali sembrano indicare che la situazione sta cambiando. Dopo l'improvvisa sparizione, nel 2016, dal panorama delle minacce di tre fra i principali exploit kit (Angler, Nuclear e Neutrino), i nostri ricercatori hanno osservato una diminuzione significativa del traffico Internet collegato a Flash. (Vedere "La scomparsa dei principali exploit kit offre opportunità per entità minori e nuovi arrivi" a pagina 20). Gli autori dell'exploit kit Angler si sono concentrati sulle vulnerabilità di Flash per compromettere gli utenti. Anche Nuclear si avvaleva in modo particolare di Flash, mentre Neutrino sfruttava i file Flash per diffondere gli exploit.

Per questo motivo, gli utenti devono continuare a essere prudenti e devono rimuovere Flash, a meno che quest'ultimo sia necessario per motivi aziendali e, in questo caso, devono eseguire tutti gli aggiornamenti previsti. L'uso di browser Web dotati di funzionalità di patching automatico può essere utile. Come osservato in "Metodi di attacco tramite Web: le minacce 'con la coda corta' consentono ai criminali informatici di porre le basi per le campagne" a pagina 13, l'uso di browser sicuri, unitamente alla disabilitazione o alla rimozione dei plug-in non necessari, riduce in misura notevole l'esposizione alle minacce basate sul Web.

Java, PDF e Silverlight

Nel 2016, il traffico Internet correlato a Java e ai file PDF ha mostrato un decremento significativo, mentre il traffico legato a Silverlight ha già raggiunto un livello tale per cui i ricercatori non ritengono produttivo controllarlo regolarmente.

Java, un tempo il vettore di attacco Web predominante, negli ultimi anni ha migliorato notevolmente il proprio assetto in termini di sicurezza. La decisione di Oracle, assunta all'inizio del 2016, di eliminare i plug-in Java per i browser ha contribuito a rendere Java stesso un vettore di attacco Web molto meno interessante e, a loro volta, gli attacchi tramite PDF sono sempre più rari. Per questo motivo, essi possono essere identificati più facilmente e ciò giustifica il loro impiego meno frequente da parte degli hacker.

Tuttavia, come nel caso di Flash, i criminali informatici utilizzano ancora Java, PDF e Silverlight per attaccare gli utenti e, pertanto, i singoli utenti, le aziende e gli esperti della sicurezza devono essere consapevoli dell'esistenza di queste possibili vie di attacco. Per ridurre il rischio di esposizione a queste minacce, essi devono:

- Scaricare patch
- Utilizzare tecnologie Web aggiornate
- Evitare contenuti Web che possono presentare rischi

[7] "Flash, HTML5 and Open Web Standards", Adobe News, novembre 2015: https://blogs.adobe.com/conversations/2015/11/flash-html5-and-open-web-standards.html.
[8] "Flash and Chrome", di Anthony LaForge, blog The Keyword, Google, 9 agosto 2016: https://blog.google/products/chrome/flash-and-chrome/.
[9] "Reducing Adobe Flash Usage in Firefox", di Benjamin Smedberg, blog Future Release, Mozilla, 20 luglio 2016: https://blog.mozilla.org/futurereleases/2016/07/20/reducing-adobe-flash-usage-in-firefox/.

Sicurezza delle applicazioni: come gestire il rischio delle connessioni OAuth in seguito al boom delle app

Quando le aziende passano al cloud, il loro perimetro di sicurezza si allarga al mondo virtuale. Tuttavia, quel perimetro di sicurezza si dissolve rapidamente a causa di ciascuna applicazione cloud connessa di terze parti che i dipendenti introducono nell'ambiente.

I dipendenti, infatti, desiderano aumentare la propria produttività e rimanere connessi mentre sono al lavoro, ma queste applicazioni IT fantasma costituiscono un pericolo per le aziende, poiché intervengono sull'infrastruttura aziendale e, non appena gli utenti concedono loro l'accesso tramite l'autenticazione aperta (OAuth), possono comunicare liberamente con il cloud e con le piattaforme SaaS (Software-as-a-Service) aziendali. Queste applicazioni possono presentare amplissime e, talvolta, eccessive prerogative in materia di accesso e, pertanto, devono essere gestite con attenzione, poiché possono visualizzare, eliminare, inviare all'esterno e memorizzare dati aziendali e, addirittura, agire per conto degli utenti.

CloudLock, provider di servizi di sicurezza cloud ora parte di Cisco, ha monitorato la crescita delle applicazioni cloud connesse di terze parti all'interno di un campione di 900 aziende che rappresentano un'ampia gamma di settori. Come mostrato nella **figura 4**, all'inizio del 2016 sono state censite circa 129.000 applicazioni diverse che, alla fine di ottobre, sono diventate 222.000.

Il numero di applicazioni è aumentato di circa 11 volte dal 2014. (Vedere la **figura 5**).

Classificazione delle applicazioni più rischiose

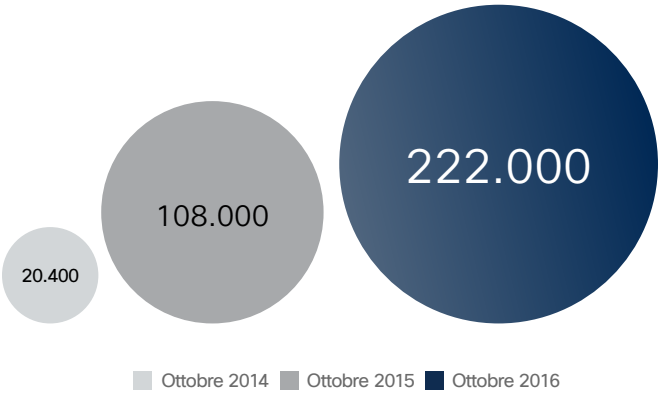
Per aiutare i team di sicurezza a comprendere come l'introduzione negli ambienti di applicazioni cloud connesse di terze parti comporti un grave pericolo per la sicurezza delle reti, CloudLock ha messo a punto l'indice CARI (Cloud Application Risk Index, indice di rischio delle applicazioni cloud). Il processo si basa su vari livelli di valutazione:

- **Requisiti per l'accesso ai dati:** le aziende rispondono, tra l'altro, alle seguenti domande: "Quali permessi sono necessari per autorizzare l'applicazione?" "Concedere l'accesso ai dati significa che l'applicazione può accedere in modalità di programmazione (API) alle piattaforme SaaS aziendali avvalendosi di connessioni OAuth?" "L'applicazione (e, per estensione, il suo fornitore) è in grado di agire per conto degli utenti e di intervenire sui dati aziendali, ad esempio visualizzandoli e/o eliminandoli?"
- **Valutazione dell'affidabilità da parte delle community:** considera le valutazioni collettive condotte tra pari.
- **Intelligence sulle minacce rappresentate dalle applicazioni:** questo controllo esaustivo eseguito dagli esperti di cybersecurity si basa su vari attributi di sicurezza delle applicazioni come certificazioni, violazioni subite in passato e recensioni degli analisti.

Figura 4 Crescita esponenziale delle applicazioni cloud connesse di terze parti nel 2016

Fonte: Cisco CloudLock

Figura 5 Confronto anno per anno della crescita delle applicazioni cloud di terze parti



Fonte: Cisco CloudLock

Scaricare il grafico del 2017 al link seguente: **www.cisco.com/go/acr2017graphics**

Punteggi ed esempi di rischio

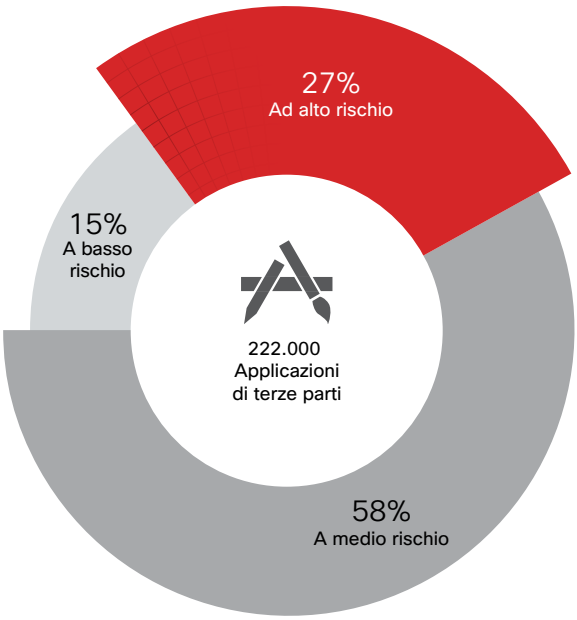
Dopo aver categorizzato le applicazioni cloud di terze parti utilizzando l'indice CARI, CloudLock assegna un punteggio di rischio per ogni app su una scala da 1 (rischio minimo) a 5 (rischio massimo).

Un'app con un punteggio pari a 1 su questa scala potrebbe avere, ad esempio, autorizzazioni di accesso minime (può visualizzare solo le e-mail), un indice di affidabilità da parte delle community pari al 100 per cento e nessun precedente di violazioni.

Un'app con un punteggio pari a 5 su questa scala potrebbe avere un accesso completo all'account (può visualizzare tutte le e-mail, i documenti, la cronologia di navigazione, il calendario e molto altro), un indice di affidabilità pari all'8 per cento (il che significa che solo l'8 per cento degli amministratori la ritengono affidabile) e nessuna certificazione di sicurezza.

CloudLock ha impiegato l'indice CARI per valutare le 222.000 applicazioni identificate nelle 900 aziende del campione. Sul totale, il 27% delle applicazioni è stato valutato come altamente pericoloso, mentre la maggior parte è stata classificata come mediamente pericolosa. (Vedere la figura 6). La metà delle aziende presentava connessioni OAuth a una diffusa applicazione di gioco rilasciata nell'estate 2016.

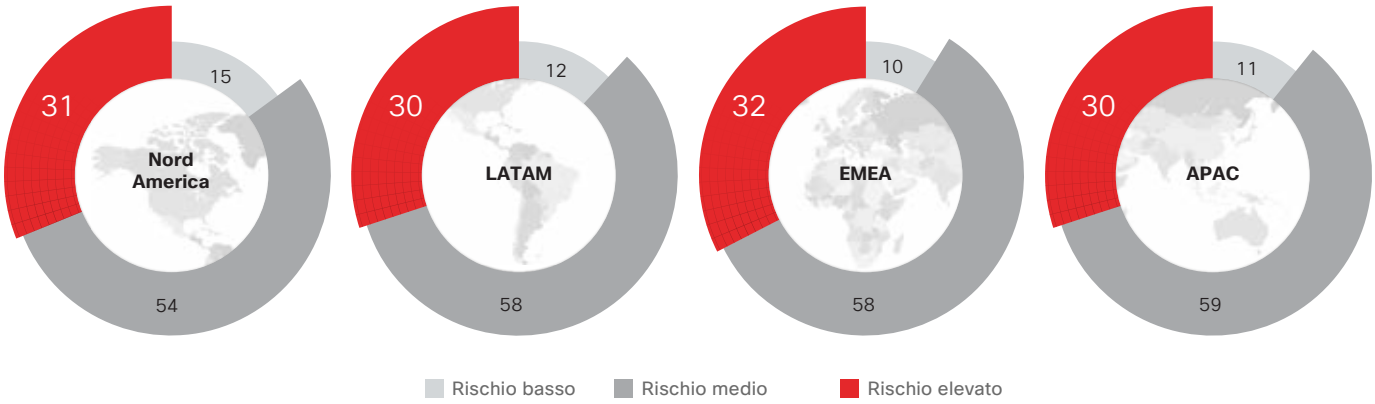
Figura 6 Applicazioni di terze parti classificate ad alto rischio



Fonte: Cisco CloudLock

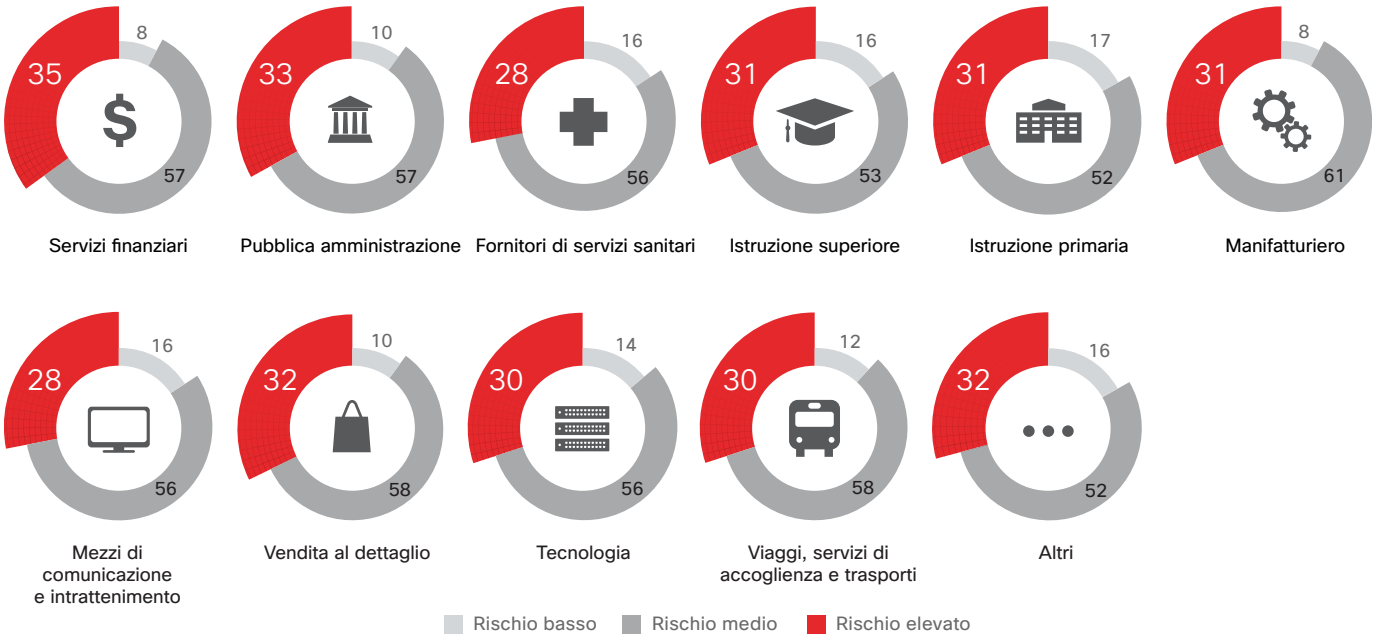
Con la nostra analisi abbiamo scoperto che tutte le aziende, indipendentemente da dimensioni, settore o area geografica di appartenenza, presentano una quantità relativamente uniforme di applicazioni a basso, medio e alto rischio (figure 7 e 8).

Figura 7 Distribuzione di applicazioni a basso, medio e alto rischio per area



Fonte: Cisco CloudLock

Figura 8 Distribuzione di applicazioni a basso, medio e alto rischio per settore



Fonte: Cisco CloudLock

Scaricare il grafico del 2017 al link seguente: **www.cisco.com/go/acr2017graphics**

Orientarsi nel rumore

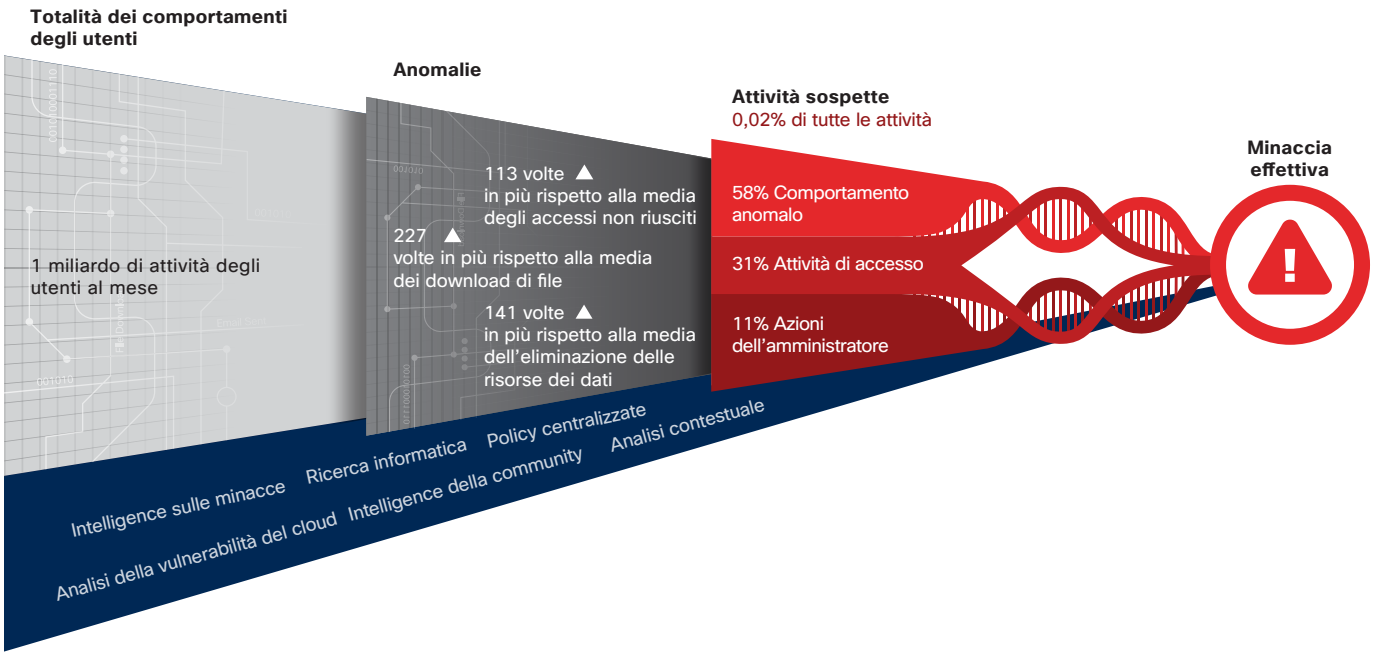
Per identificare il comportamento sospetto di utenti ed entità all'interno delle piattaforme SaaS aziendali, comprese le applicazioni cloud di terze parti, i team responsabili della sicurezza devono analizzare miliardi di attività per definire modelli di comportamento normale all'interno di ciascun ambiente e, successivamente, andare alla ricerca di anomalie che esulano dai modelli attesi. In seguito, devono porre in relazione le attività sospette per determinare che cosa potrebbe rappresentare una minaccia reale che richiede un'analisi approfondita.

Un esempio di attività sospetta è il numero eccessivo di accessi da più paesi in un breve arco di tempo. Supponiamo che, in una determinata azienda, il comportamento normale da parte degli utenti implichi l'accesso a una particolare applicazione da non più di uno o due paesi alla settimana. Se un utente inizia ad accedere a quell'applicazione da 68 paesi nell'arco di una settimana, il team addetto alla sicurezza dovrà analizzare quest'attività per accertarsi che sia legittima.

Secondo la nostra analisi, solo 1 attività utente su 5000, pari allo 0,02%, associate ad applicazioni cloud connesse di terze parti è sospetta e la sfida posta ai team di sicurezza, ovviamente, è identificare esattamente quell'attività.

Solo l'automazione può aiutare gli addetti a orientarsi nel "rumore" degli avvisi di sicurezza e a concentrare le risorse disponibili sull'analisi delle minacce reali. Il processo, articolato su più livelli, di identificazione delle attività normali e potenzialmente sospette descritto in precedenza e illustrato nella figura 9, si fonda sull'uso dell'automazione e di algoritmi impiegati a ciascun livello.

Figura 9 Identificazione dei modelli di comportamento degli utenti attraverso l'automazione (processo)



Fonte: Cisco CloudLockW

Ricognizione | Adescamento | **Dirottamento** | Installazione

Con l'utilizzo dannoso di e-mail, allegati di file, siti Web e altri strumenti, gli hacker trasmettono le armi informatiche ai loro obiettivi.

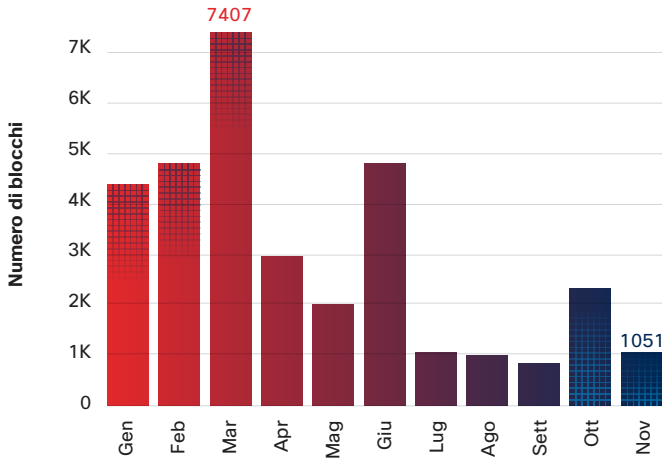
La scomparsa dei principali exploit kit offre opportunità per entità minori e nuovi arrivi

Il 2016 ha visto un cambiamento radicale in materia di exploit kit. All'inizio dell'anno, Angler, Nuclear, Neutrino e RIG erano di gran lunga gli exploit kit più usati. A novembre, RIG era l'unico ancora attivo. Come mostra la **figura 10**, le attività degli exploit kit si sono ridotte sensibilmente intorno a giugno.

Nuclear è stato il primo a scomparire, cessando improvvisamente il proprio funzionamento a maggio e la ragione per cui i suoi autori l'hanno abbandonato è un mistero. L'exploit kit Neutrino, che ha anch'esso abbandonato la scena nel 2016, sfruttava i file Flash per diffondere vulnerabilità. (Vedere la **figura 11** alla pagina successiva per l'elenco delle vulnerabilità principali contenute negli exploit kit noti al 2016).

Flash rimane un interessante vettore di attacco Web per gli hacker, ma è probabile che, con il passare del tempo, perda questa caratteristica, poiché sempre meno siti e browser supportano Flash e vi è una consapevolezza generalmente superiore delle vulnerabilità che esso comporta. (Per ulteriori approfondimenti su questo tema, vedere la sezione "Vettori di attacco Web: Flash perde importanza, ma gli utenti devono rimanere vigili" a pagina 15).

Figura 10 Blocchi delle pagine di destinazione degli exploit kit, gennaio – novembre 2016



Fonte: Cisco Security Research

Scaricare il grafico del 2017 al link seguente: **www.cisco.com/go/acr2017graphics**

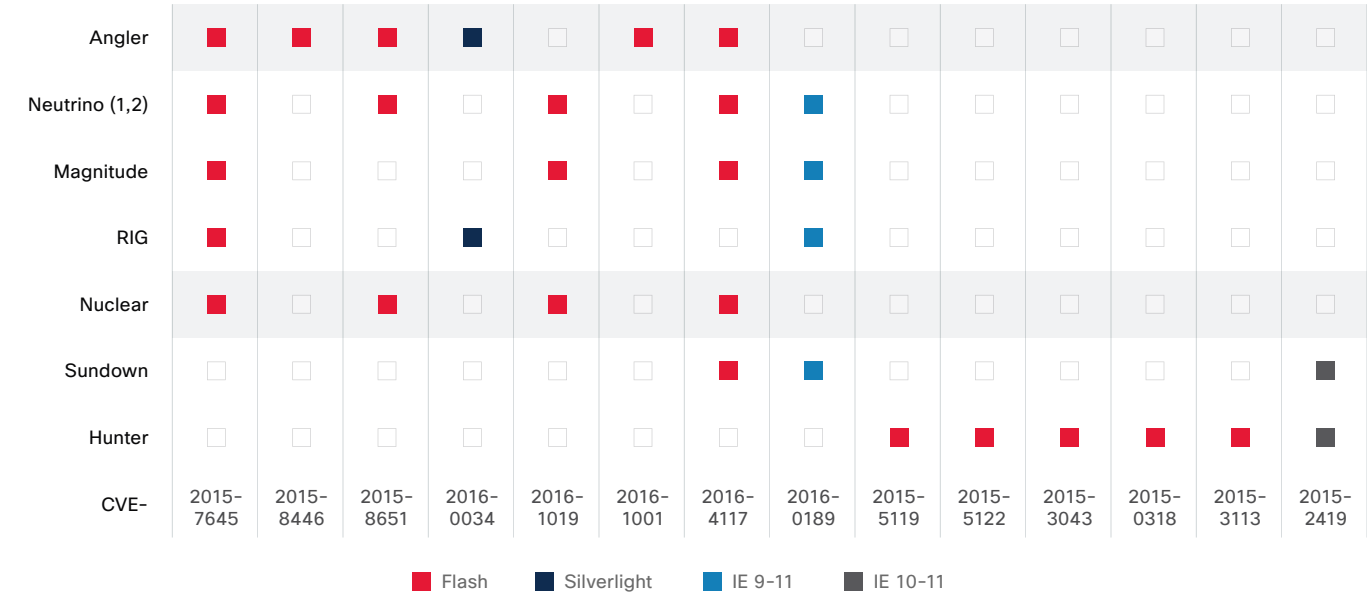
Un gigante ridotto al silenzio

Anche Angler, l'exploit kit più evoluto e di dimensioni maggiori, aveva per obiettivo le vulnerabilità di Flash ed era collegato a numerose campagne di malvertising e ransomware di alto profilo. Tuttavia, a differenza di Neutrino e Nuclear, la scomparsa di Angler nel 2016 non è affatto un mistero.

Nella tarda primavera, infatti, in Russia sono stati arrestati circa 50 hacker e criminali informatici: il gruppo era collegato al malware Lurk, un trojan bancario che prendeva di mira in modo specifico gli istituti di credito russi.[10] I ricercatori di Cisco hanno individuato con chiarezza collegamenti tra Lurk e Angler, compreso il fatto che, molto frequentemente, Lurk veniva distribuito in Russia attraverso Angler. In seguito agli arresti, Angler è sparito dal repertorio degli exploit kit.[11]

Ora che tre dei principali exploit kit sono stati eliminati, le entità di dimensioni minori e i nuovi arrivati hanno la possibilità di ampliare le rispettive quote di mercato e stanno diventando sempre più sofisticati e agili. Gli exploit kit che nel 2016 sembravano destinati a crescere erano Sundown, Sweet Orange e Magnitude che, come RIG, sfruttano notoriamente le vulnerabilità di Flash, Silverlight e Microsoft Internet Explorer. (Vedere la **figura 11**). La disinstallazione di Flash e la disattivazione o la rimozione dei plug-in dei browser non necessari aiuta gli utenti a diminuire il rischio di essere compromessi da una di queste minacce.

Figura 11 Vulnerabilità principali degli exploit kit



Fonte: Cisco Security Research

CONDIVIDI

[10] "Russian Hacker Gang Arrested Over $25M Theft," BBC News, 2 giugno 2016: http://www.bbc.com/news/technology-36434104.
[11] Per ulteriori informazioni su questo argomento, vedere il post del blog di Cisco Talos di luglio 2016, Connecting the Dots Reveals Crimeware Shake-Up.

Malvertising: gli hacker utilizzano intermediari per aumentare velocità e agilità

Gli utenti vengono reindirizzati verso gli exploit kit in due modi principali: tramite siti Web compromessi e il malvertising. Gli hacker mettono un link a una pagina di destinazione di un exploit kit all'interno di un annuncio pubblicitario dannoso o di un sito Web compromesso, oppure utilizzano un link che fa da intermediario, detto anche "broker". (Questi link, che si trovano a metà tra i siti Web compromessi e i server degli exploit kit, vengono anche chiamati "gate"). Il broker funge da intermediario tra il reindirizzamento iniziale e l'exploit kit reale che trasmette il payload del malware agli utenti.

Quest'ultima tattica è sempre più diffusa poiché gli hacker hanno capito di doversi muovere più rapidamente per mantenere il proprio spazio operativo e per eludere il rilevamento. Gli intermediari consentono agli hacker di passare rapidamente da un server dannoso a un altro senza modificare il reindirizzamento iniziale. E visto che non devono modificare costantemente i siti Web o gli annunci dannosi per avviare la catena di infezione, gli autori degli exploit kit possono attuare campagne più lunghe.

ShadowGate: una campagna conveniente

Siccome diventa più difficile compromettere molti utenti solo attraverso i vettori di attacco tradizionali (vedere pagina 15), gli hacker si affidano sempre più al malvertising per esporre gli utenti agli exploit kit. I nostri ricercatori hanno denominato una recente campagna di malvertising "ShadowGate". Questa campagna illustra come gli annunci dannosi stanno offrendo agli autori degli attacchi maggiore flessibilità e opportunità di mirare a utenti in aree geografiche diverse e su larga scala.

ShadowGate ha coinvolto siti Web di ogni tipo: dalla cultura di massa al commercio al dettaglio, dalla pornografia alle notizie. Ha interessato potenzialmente milioni di utenti in Nord America, Europa, nell'area Asia-Pacifico e in Medio Oriente. La portata globale della campagna e l'utilizzo di molte lingue sono notevoli.

ShadowGate, che utilizza il domain shadowing, è stata individuata per la prima volta all'inizio del 2015. Talvolta rimaneva dormiente e poi si riattivava in modo casuale per indirizzare il traffico verso le pagine di destinazione dell'exploit kit. Inizialmente, ShadowGate veniva utilizzata per indirizzare gli utenti solo verso l'exploit kit Angler. Ma dopo la scomparsa di Angler nell'estate del 2016, gli utenti sono stati indirizzati all'exploit kit di Neutrino, finché non è scomparso anch'esso alcuni mesi più tardi. (Per ulteriori informazioni su questa vicenda, vedere la sezione "La scomparsa dei principali exploit kit offre opportunità per entità minori e nuovi arrivi" a pagina 20).

Sebbene ShadowGate avesse registrato un grande volume di traffico Web, solo una frazione minuscola di interazioni aveva indirizzato gli utenti verso un exploit kit. Gli annunci dannosi erano prevalentemente imitazioni, annunci che vengono rappresentati sulla pagina ma che non richiedono l'interazione dell'utente. Questo modello di pubblicità online ha consentito agli autori di ShadowGate di attuare la campagna in modo più conveniente.

La nostra ricerca su ShadowGate ha portato a uno sforzo congiunto con un'importante azienda di Web hosting. Abbiamo lavorato insieme per mitigare la minaccia risanando gli account degli iscritti che gli hacker avevano utilizzato come host dell'attività. Quindi abbiamo rimosso tutti i sottodomini relativi.

Per ulteriori informazioni sulla campagna di ShadowGate, vedere il post del blog di Cisco Talos di settembre 2016, Talos ShadowGate Take Down: Global Malvertising Campaign Thwarted.

L'indagine ha rilevato che il 75% delle aziende è interessata da infezioni adware

L'adware, se utilizzato per scopi legittimi, è un tipo di software che scarica o visualizza pubblicità tramite reindirizzamenti, popup e inserimenti di annunci che producono guadagni per i rispettivi creatori. Tuttavia, i criminali informatici stanno utilizzando l'adware anche come strumento volto ad aumentare il flusso delle proprie entrate. Essi impiegano adware dannoso non solo per trarre profitto dall'inserimento di pubblicità, ma anche come primo passo per facilitare altre campagne di malware, come DNSChanger. L'adware dannoso viene distribuito attraverso pacchetti software costituiti da un programma di installazione di un'applicazione legittima unito a decine di applicazioni adware dannose.

I criminali utilizzano l'adware per:

- Inserire pubblicità, il che può causare ulteriori infezioni o l'esposizione a exploit kit
- Modificare le impostazioni di browser e sistemi operativi per indebolire la sicurezza
- Violare antivirus o altri prodotti per la sicurezza
- Acquisire il controllo totale dell'host allo scopo di installare atro software dannoso
- Tracciare gli utenti in base a posizione, identità, servizi utilizzati e siti normalmente visualizzati
- Estrapolare informazioni quali dati personali, credenziali e informazioni sull'infrastruttura (ad esempio, le pagine interne dell'ufficio vendite di un'azienda)

Per valutare la portata dei problemi che l'adware pone alle aziende, i ricercatori di Cisco hanno esaminato 80 versioni diverse di questo fenomeno. Nella ricerca, condotta tra novembre 2015 e novembre 2016, sono state coinvolte circa 130 aziende di vari settori.

In base al comportamento principale di ciascun componente, l'adware è stato suddiviso in quattro gruppi:

- **Ad injector:** questo adware risiede solitamente nel browser e può influire su tutti i sistemi operativi.
- **Hijacker delle impostazioni del browser:** questo componente può modificare le impostazioni del computer allo scopo di rendere il browser meno sicuro.
- **Utility:** si tratta di una categoria di adware ampia e in espansione. Le utility sono applicazioni Web che offrono servizi utili agli utenti, come l'ottimizzazione dei PC. Queste applicazioni possono inserire pubblicità, ma il loro scopo primario è indurre gli utenti a pagare per il servizio. Tuttavia, in molti casi, le utility non sono nient'altro che truffe e non offrono alcun vantaggio agli utenti.
- **Downloader:** questo adware può veicolare altro software, come una barra degli strumenti.

Abbiamo stabilito che il 75% delle aziende oggetto dello studio erano affette da infezioni adware.

Figura 12 Percentuale di aziende colpite da infezioni da adware

Fonte: Cisco Security Research

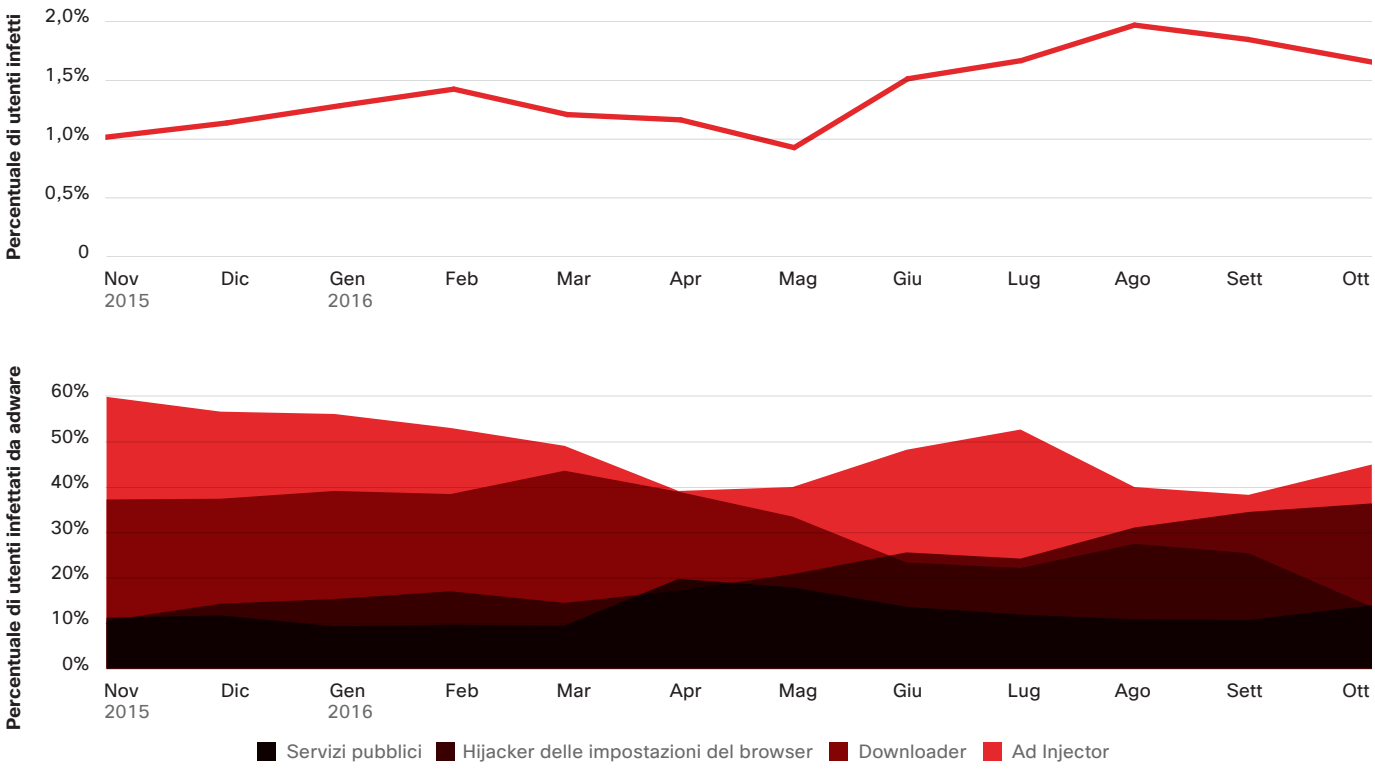
CONDIVIDI

La figura 13 mostra i tipi di incidenti che abbiamo osservato nelle aziende incluse nella nostra ricerca. Gli iniettori di pubblicità sono la fonte principale delle infezioni. Questo dato indica che la maggior parte di queste applicazioni indesiderate prende di mira i browser Web. Inoltre, negli ultimi anni abbiamo registrato un aumento delle infezioni basate su browser, il che suggerisce che gli hacker stiano avendo successo nella loro strategia di compromissione degli utenti.

Tutte i componenti adware che abbiamo identificato nel corso della nostra ricerca possono esporre gli utenti e le aziende al rischio di attività dannose e i team di sicurezza devono riconoscere la minaccia rappresentata dalle infezioni da adware e accertarsi che gli utenti all'interno delle aziende siano pienamente consapevoli del rischio.

Per ulteriori informazioni su questo argomento, vedere il post di febbraio 2016 del blog di Cisco Security, DNSChanger Outbreak Linked to Adware Install Base.

Figura 13 Analisi dettagliata degli incidenti totali in base al componente adware



Fonte: Cisco Security Research

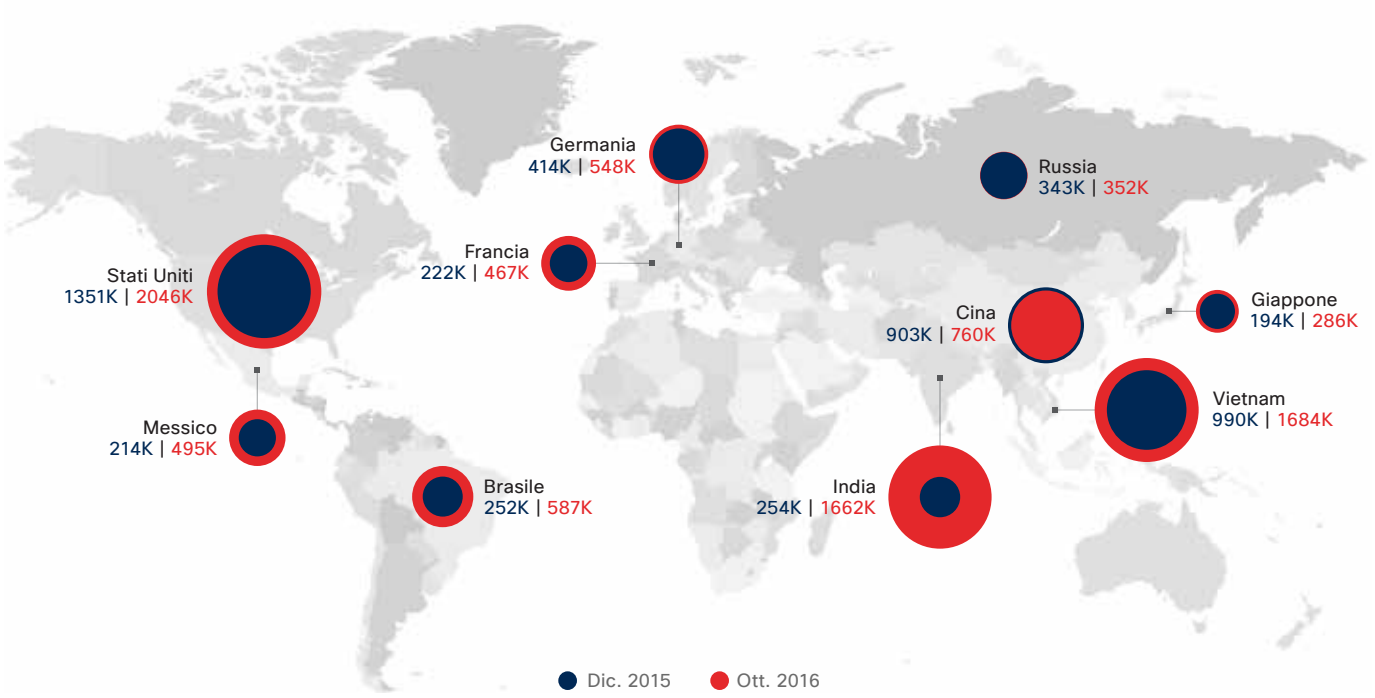
Scaricare il grafico del 2017 al link seguente: **www.cisco.com/go/acr2017graphics**

La quantità complessiva di spam è in aumento, così come la percentuale degli allegati dannosi

Nel 2016, gli esperti di minacce di Cisco hanno condotto due studi nei quali hanno utilizzato la telemetria nei confronti di clienti consenzienti per determinare la percentuale di spam veicolato attraverso le e-mail. Abbiamo scoperto che lo spam rappresenta circa due terzi (65%) del volume complessivo di e-mail. La nostra ricerca indica anche che il volume complessivo dello spam è in aumento, principalmente a causa di botnet efficaci e di grandi dimensioni come Necurs. Inoltre, grazie a questo studio abbiamo determinato che tra l'8 e il 10% di tutto lo spam osservato nel 2016 può essere considerato dannoso.

Da agosto a ottobre 2016, si è verificato un aumento significativo del numero di blocchi delle connessioni IP (**figura 14**).[12] Questa tendenza può essere attribuita a un aumento generale del volume dello spam, nonché all'adattamento dei sistemi per la gestione della reputazione alle informazioni relative ai generatori di spam.

Figura 14 Blocchi IP per paese, dicembre 2015 – novembre 2016



Fonte: Cisco Security Research

CONDIVIDI

[12] I blocchi delle connessioni IP sono messaggi spam che vengono bloccati immediatamente dalla tecnologia di rilevamento dello spam perché il mittente ha un punteggio negativo in relazione alla reputazione. Si tratta ad esempio di messaggi che derivano da botnet conosciute perché inviano spam o da reti compromesse note per la partecipazione agli attacchi spam.

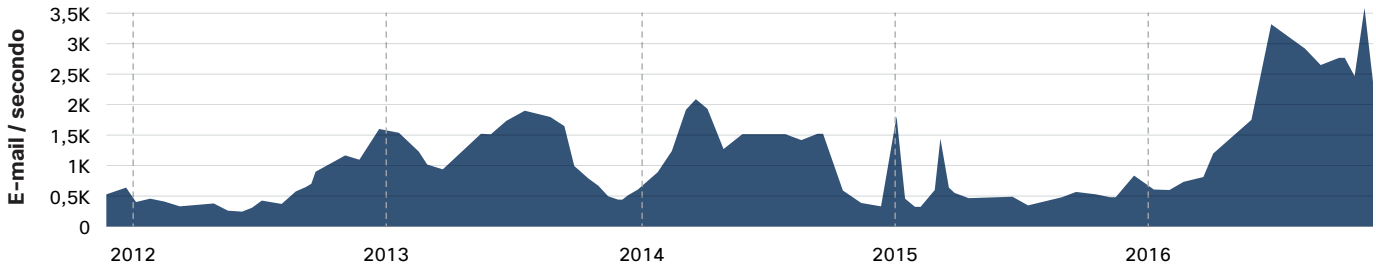
Anche il grafico, elaborato su un arco temporale di cinque anni, relativo all'elenco CBL (Composite Blocking List), una "blackhole list" basata su DNS di infezioni informatiche sospettate di inviare spam,[13] mostra un notevole aumento del volume di spam nel 2016 (**figura 15**).

L'esame dei dati relativi a un decennio provenienti da CBL (non mostrati) indica che il volume di spam registrato nel 2016 è prossimo ai livelli record raggiunti nel 2010. Negli ultimi anni le nuove tecnologie antispam e la neutralizzazione di botnet collegate allo spam hanno contribuito a mantenere bassi i livelli di quest'ultimo e i nostri ricercatori attribuiscono il recente aumento del volume complessivo dello spam alla botnet Necurs, uno dei principali vettori del ransomware Locky che, inoltre, distribuisce minacce come il trojan bancario Dridex.

La **figura 16** è un grafico interno generato dal servizio SpamCop di Cisco e illustra la variazione del volume dello spam rilevato nel 2016. Questo grafico mostra le dimensioni complessive di SCBL (SpamCop Block List) tra novembre 2015 e novembre 2016. Ogni riga di SCBL rappresenta un diverso indirizzo IP.

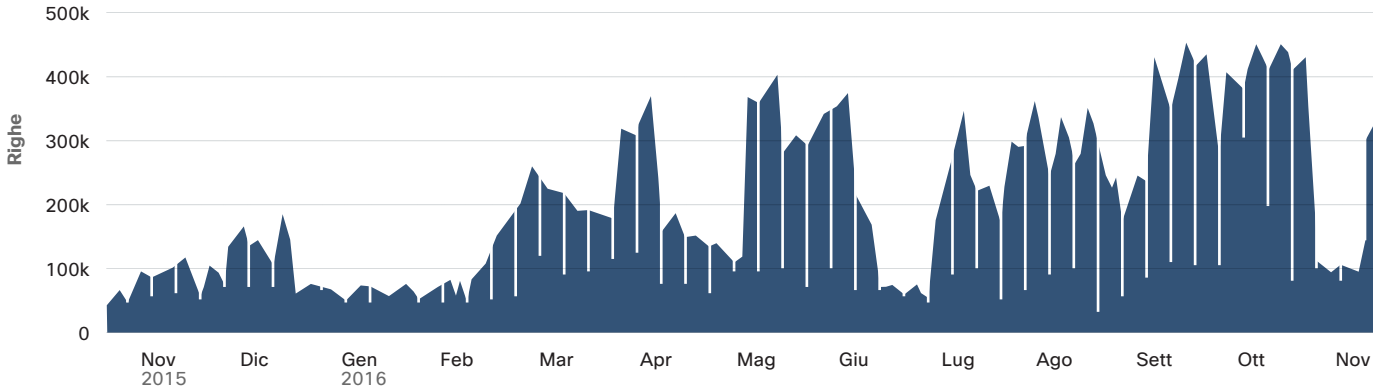
Fra novembre 2015 e febbraio 2016 SCBL conteneva meno di 200.000 indirizzi IP, mentre a settembre e ottobre gli indirizzi erano passati a oltre 400.000 prima di diminuire bruscamente, circostanza che i nostri ricercatori attribuiscono al semplice fatto che gli operatori di Necurs sembrano essersi presi una pausa. Degno di nota è anche il declino significativo a giugno. Alla fine di maggio in Russia sono stati eseguiti arresti in relazione al trojan bancario Lurk (**vedere a** pagina 21). In seguito a questo evento, diverse minacce di alto profilo, compreso Necurs, hanno smesso di operare. Tuttavia, 3 settimane più tardi Necurs è tornato in azione aggiungendo più di 200.000 indirizzi IP a SCBL in meno di 2 ore.

Figura 15 Volume totale di spam



Fonte: CBL

Figura 16 Volume complessivo di SCBL



Fonte: SpamCop

CONDIVIDI

[13] Per ulteriori informazioni su CBL, visitare http://www.abuseat.org/.

Molti IP degli host che inviano spam Necurs sono infetti da oltre 2 anni. Per mantenere nascosta l'intera portata della botnet, Necurs invierà spam solo da un sottoinsieme degli host infettati, ciascuno dei quali potrebbe essere usato per 2-3 giorni e, quindi, rimanere inattivo per 2 o 3 settimane. Questo comportamento complica il compito del personale addetto alla sicurezza che deve reagire agli attacchi di spam, poiché gli addetti possono credere di avere individuato e pulito un host infetto, ma i criminali che lavorano dietro le quinte di Necurs potrebbero essere semplicemente in attesa di lanciare un altro attacco.

Il 75% dello spam rilevato in ottobre 2016 conteneva allegati dannosi e la maggior parte è stata inviata dal botnet Necurs. (Vedere la **figura 17**). Necurs invia allegati .zip dannosi che contengono file eseguibili integrati come downloader JavaScript, .hta, .wsf e VBScript. Nel calcolo della percentuale di spam che contiene allegati dannosi abbiamo considerato sia il "contenitore" (.zip), sia i "figli" al suo interno (come i file JavaScript) come singoli allegati dannosi.

Gli autori utilizzano vari tipi di allegati per rendere sempre nuove le campagne di spam dannoso

I nostri ricercatori hanno esaminato il modo in cui i criminali informatici impiegano diversi tipi di allegati per ostacolare la rilevazione dello spam dannoso e hanno scoperto che essi evolvono continuamente le strategie adottate, avvalendosi di un'ampia gamma di tipi di file e cambiando velocemente tattica quando non hanno successo.

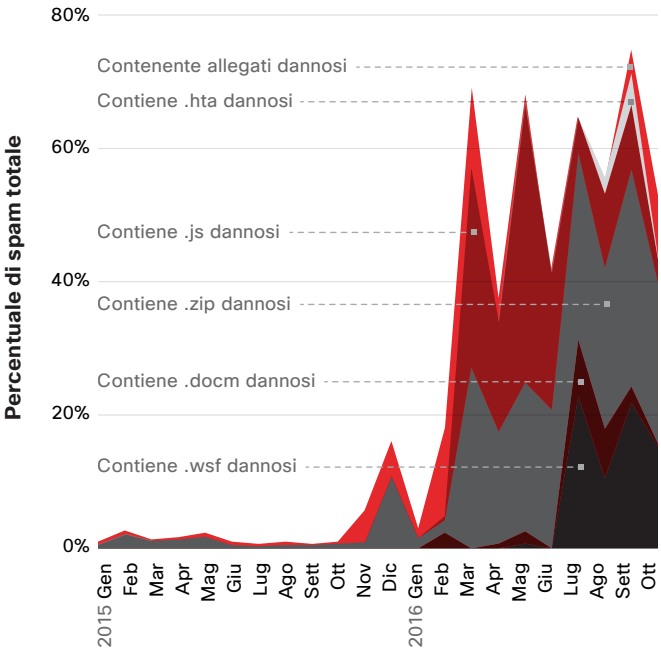
La **figura 17** mostra come, durante il periodo di osservazione, i creatori di spam abbiano usato file .docm, JavaScript, .wsf e .hta. Come rilevato in precedenza, molti di questi tipi di file sono associati allo spam inviato dalla botnet Necurs. (Per la ricerca relativa ad altri tipi di file esaminati, vedere l'Appendice a pagina 78).

I valori relativi a ciascun tipo di file in un determinato mese sono ricavati a partire dalla percentuale di spam che conteneva gli allegati dannosi rilevati nel mese. Quindi, ad esempio, a luglio 2016 i file .docm rappresentavano l'8% del totale di allegati dannosi osservati.

I modelli d'uso dei file .wsf durante il 2016 (vedere la **figura 17**) forniscono un esempio di come gli hacker, nel tempo, cambiano le tattiche di spam impiegate. Prima di febbraio 2016, questo tipo di file era usato raramente come allegato dannoso, ma, a mano a mano che Necurs è diventato più attivo, anche l'utilizzo di questo tipo di file si è fatto più frequente ed entro luglio, i file .wsf rappresentavano il 22% di tutti gli allegati spam dannosi. Questo fenomeno è avvenuto all'incirca quando l'attività di spam globale è aumentata notevolmente (vedere la sezione precedente) a causa dell'attività della botnet Necurs.

In agosto, settembre e ottobre abbiamo registrato oscillazioni nella percentuale dei file .wsf, il che indica che gli hacker si ritiravano quando questo tipo di file veniva rilevato più spesso.

Figura 17 Percentuale di spam totale contenente allegati dannosi



Fonte: Cisco Security Research

CONDIVIDI

Hailstorm e snowshoe

Due tipi di attacchi spam dannosi sono particolarmente problematici per gli addetti alla sicurezza: hailstorm e snowshoe. Entrambi sfruttano la velocità e la capacità di individuare gli obiettivi ed entrambi sono molto efficaci.

Gli attacchi hailstorm hanno per obiettivo i sistemi antispam e i loro ideatori sfruttano la finestra di tempo, estremamente limitata, tra il lancio di una campagna di spam e il momento in cui i sistemi antispam la rilevano ed estendono la propria copertura. In generale, gli autori degli attacchi dispongono di pochi secondi o minuti per agire prima che le loro campagne vengano rilevate e bloccate.

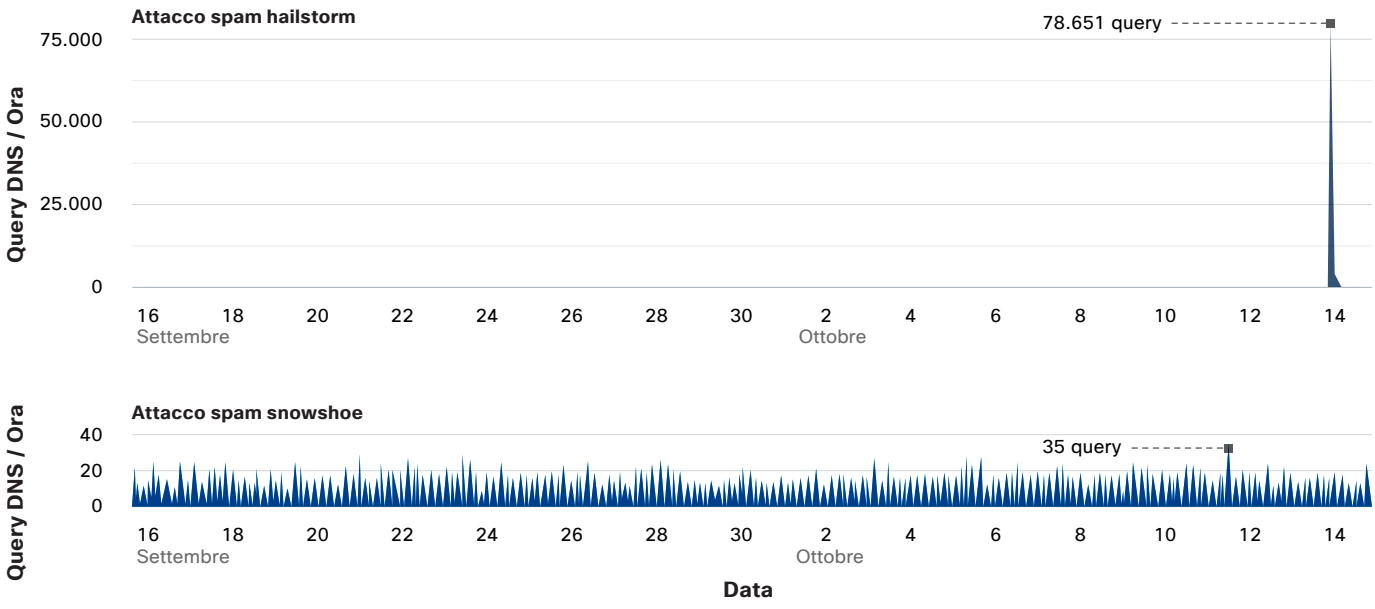
Il picco nella figura 18 è un attacco hailstorm. L'attività è indicata nell'interfaccia di Cisco Investigate. Immediatamente prima dell'attacco, nessuno risolveva gli indirizzi IP. Quindi, improvvisamente, il numero di computer che risolvevano il dominio attraverso DNS è balzato a oltre 78.000 per poi tornare a zero.

Confrontiamo l'attacco hailstorm con una campagna di spam snowshoe, anch'essa mostrata nella figura 18, nel corso della quale gli autori degli attacchi tentano di volare al di sotto del radar messo in campo dalle soluzioni per il rilevamento basate sui volumi. Il numero di ricerche DNS è costante, ma vi sono solo 25 interrogazioni all'ora. Questi attacchi basati su bassi volumi consentono agli autori di distribuire silenziosamente spam da un ampio parco di indirizzi IP.

Anche se questi attacchi spam funzionano in modo diverso, essi presentano alcune caratteristiche in comune. Con l'uno o l'altro approccio, gli autori degli attacchi possono:

- Eludere una cattiva reputazione eseguendo gli invii da IP e domini "puliti"
- Emulare le e-mail di marketing con contenuti professionali e sistemi per la gestione degli abbonamenti
- Utilizzare sistemi di e-mail ben configurati invece di script o spam bot di scarso livello
- Impostare correttamente la tecnica FCrDNS (forward-confirmed reverse DNS) e i record SPF (Send Policy Framework)

Figura 18 Confronto tra gli attacchi spam hailstorm e snowshoe



Fonte: Cisco Investigate

CONDIVIDI

Gli hacker possono anche rendere inefficace il rilevamento dei contenuti cambiando il testo e passando da un tipo di file all'altro. (Per ulteriori informazioni su come i criminali informatici modificano le minacce per eludere le protezioni, vedere la sezione "Tempo di evoluzione" a pagina 34). Per ulteriori informazioni su come essi utilizzino vari file dannosi come allegati ai messaggi di spam, vedere la sezione precedente.

La **figura 19** mostra i principali avvisi relativi agli attacchi e offre una panoramica circa i messaggi spam e di phishing che, in base alle nostre osservazioni, gli hacker hanno modificato spesso nel 2016 allo scopo di aggirare i controlli e le regole volti ad assicurare la sicurezza delle e-mail. È importante sapere quali siano i tipi di minacce e-mail più diffusi, in modo da evitare di essere tratti in inganno.

Figura 19 Avvisi principali di minaccia

Versione	Identificativo di pubblicazione	Nome e URL di pubblicazione	Riepilogo del messaggio	Tipo di file dell'allegato	Lingua	Ultima data di pubblicazione
96	35656	RuleID4626	Fattura, Pagamento	.zip	Tedesco, inglese	25/04/16
87	34577	RuleID10277	Ordine di acquisto	.zip	Tedesco, inglese	02/06/16
82	36916	RuleID4400KVR	Ordine di acquisto	.zip	Inglese	01/02/16
74	38971	RuleID15448	Ordine di acquisto, Pagamento, Ricezione	.zip, .gz	Inglese	08/08/16
72	41513	RuleID18688	Ordine, Pagamento, Seminario	.zip	Inglese	01/09/16
70	40056	RuleID6396	Ordine di acquisto, Pagamento, Ricezione	.rar	Inglese	07/06/16
66	34796	RuleID5118	Ordine prodotto, Pagamento	.zip	Tedesco, inglese	29/09/16
64	39317	RuleID4626 (cont)	Fattura, Pagamento, Spedizione	.zip	Inglese, tedesco, spagnolo	28/01/16
64	36917	RuleID4961KVR	Conferma, Pagamento/ Trasferimento, Ordine, Spedizione	.zip	Inglese	08/07/16
63	37179	RuleID13288	Avviso di consegna, Comparizione in tribunale, Fattura biglietto	.zip	Inglese, spagnolo	21/07/16
61	38095	RuleID858KVR	Spedizione, Preventivo, Pagamento	.zip	Inglese	01/08/16
58	39150	RuleID4961KVR	Richiesta Preventivo, Ordine prodotto	.zip	Inglese, tedesco, Più lingue	25/01/16
47	41886	RuleID4961	Trasferimento, Spedizione, Fattura	.zip	Inglese, tedesco, spagnolo	22/02/16

Fonte: Cisco Security Research

Scaricare il grafico del 2017 al link seguente: **www.cisco.com/go/acr2017graphics**

Ricognizione | Adescamento | Dirottamento | **Installazione**

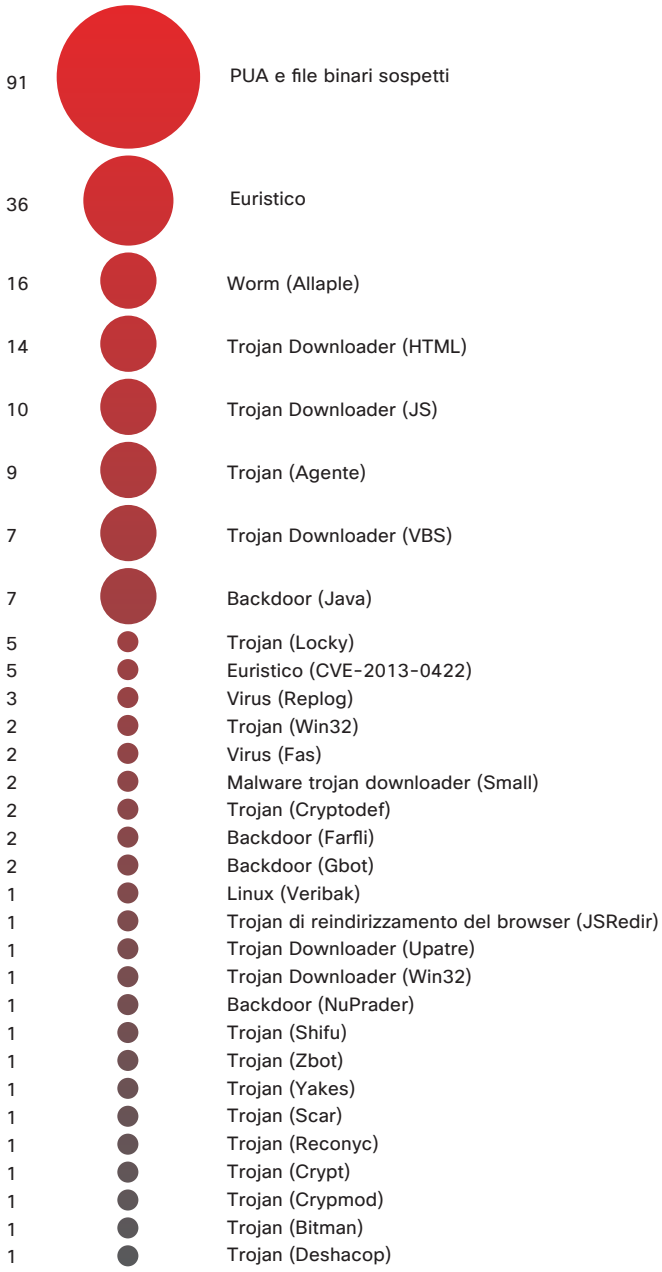
Una volta posizionatasi, la minaccia installa una backdoor sul sistema dell'obiettivo, fornendo agli hacker un accesso costante.

Metodi di attacco Web: una panoramica sulla "coda lunga" svela le minacce che gli utenti possono evitare con facilità

La cosiddetta coda lunga del panorama dei metodi di attacco Web (**figura 20**) presenta una raccolta di malware che generano volumi inferiori impiegati in una fase successiva della catena di attacco: l'installazione. In questa fase, la minaccia che è giunta a destinazione (un trojan bancario, un virus, un downloader o un exploit di altro tipo) installa una backdoor nel sistema oggetto di attacco, garantendo agli hacker un accesso permanente e, insieme, l'opportunità di esfiltrare dati, lanciare attacchi ransomware e compiere altri misfatti.

Le minacce elencate nella **figura 20** sono esempi di firme individuate nei 50 tipi di malware osservati più di frequente. La coda lunga dei metodi di attacco Web è, sostanzialmente, un'istantanea delle minacce che lavorano silenziosamente all'interno dei computer e dei sistemi in seguito a un attacco condotto con successo. Molte di queste infezioni sono state diffuse inizialmente dall'incontro con adware dannoso o dall'esposizione a una truffa basata sul phishing ben architettata: queste sono situazioni che gli utenti spesso possono evitare facilmente o correggere rapidamente.

Figura 20 Campione di malware a più basso volume osservato



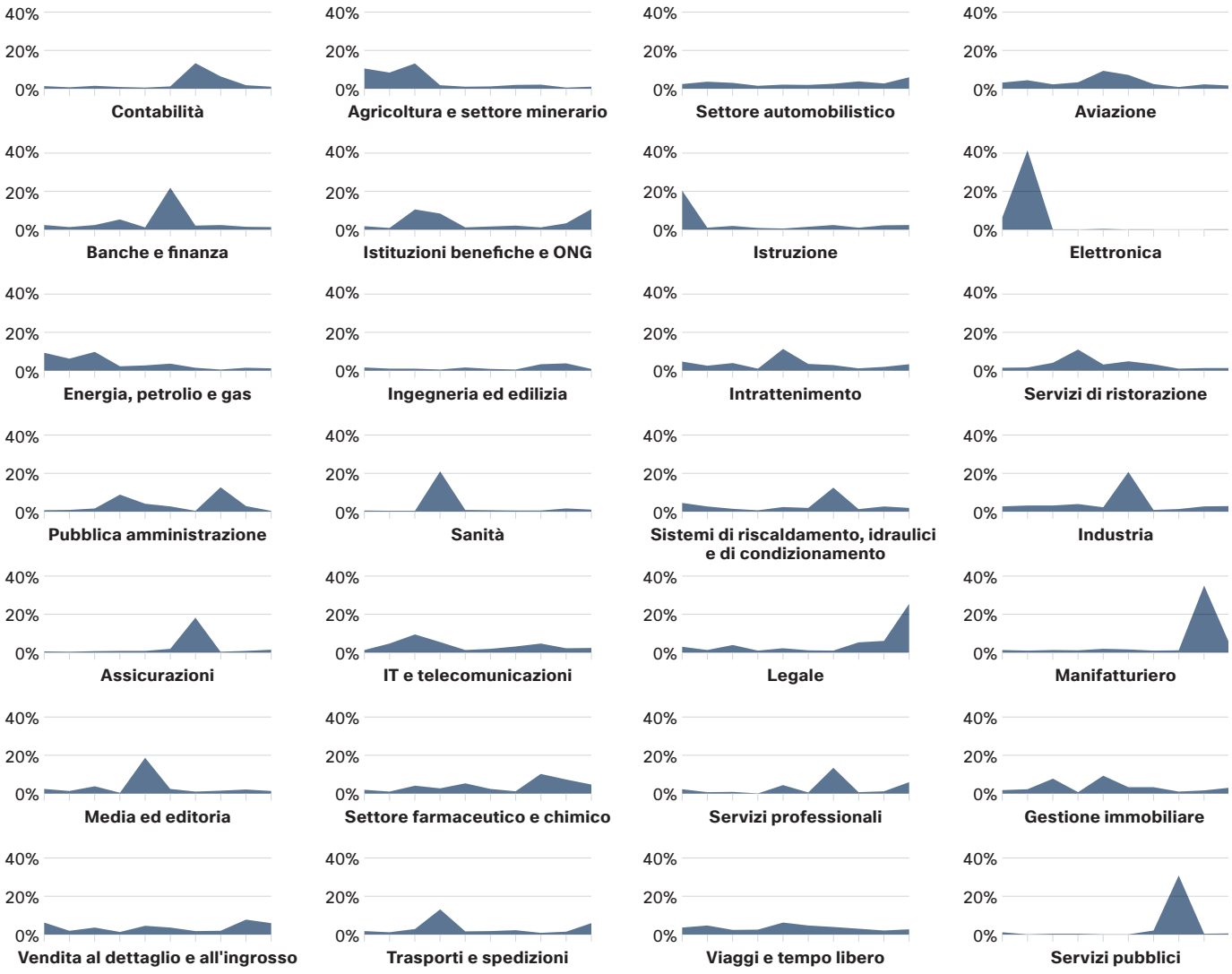
Fonte: Cisco Security Research

Tutti i settori rischiano di venire a contatto con il malware: gli hacker vedono valore ovunque

Uno dei messaggi chiave sui rischi del malware del *Report semestrale di Cisco sulla cybersecurity 2016* era "nessun settore è al sicuro" e, a giudicare dall'analisi periodica condotta dai nostri ricercatori sul traffico di attacco ("tassi di blocco") e su quello "normale" o previsto in relazione al settore, questo messaggio è rimasto vero anche nella seconda metà dell'anno.

Esaminando i settori verticali e i relativi tassi di blocco rilevati nel tempo (figura 21), si osserva che, in qualche momento nell'arco di più mesi, ogni settore è stato soggetto a traffico di attacco a vari livelli. È evidente che le oscillazioni rilevate mostrano come gli attacchi colpiscano settori diversi in momenti diversi, ma nessuno è stato risparmiato.

Figura 21 Percentuale di tassi di blocco mensili per settore



Fonte: Cisco Security Research

Panoramica dell'attività di blocco del Web in base alle aree geografiche

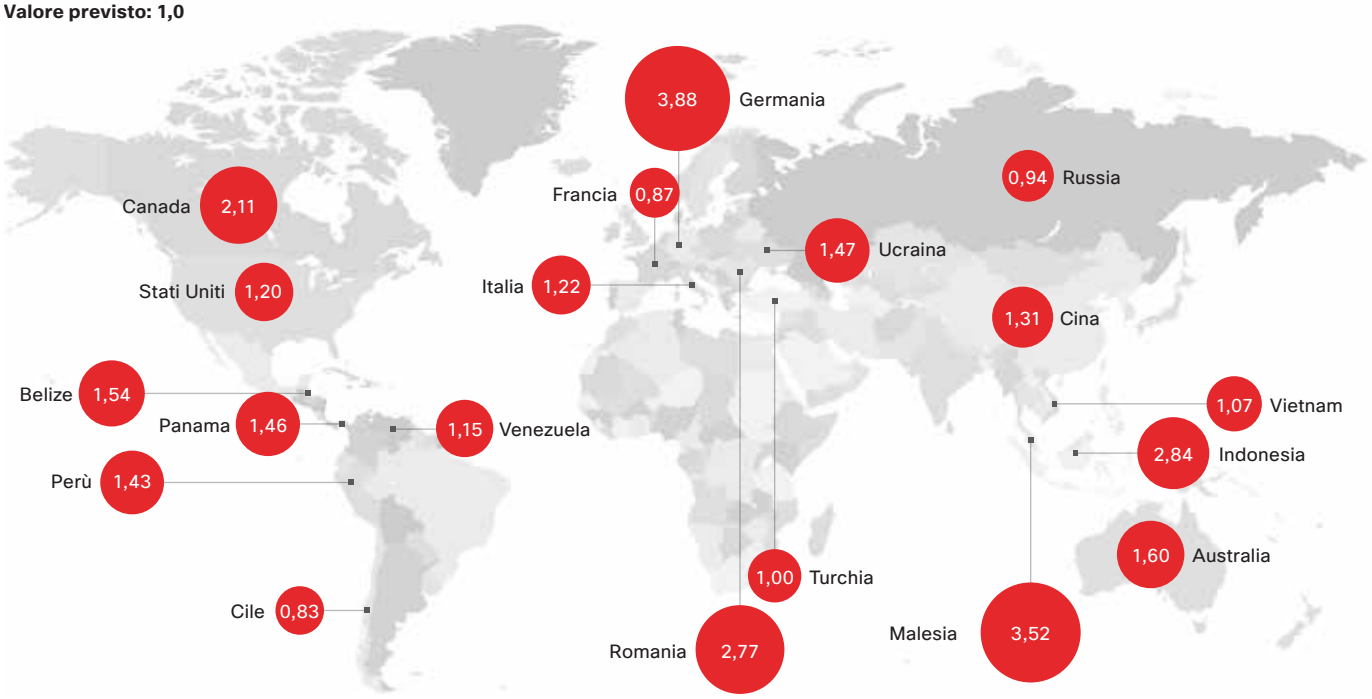
I criminali informatici frequentemente trasferiscono la propria base operativa, cercando infrastrutture deboli dalle quali lanciare le campagne di attacchi. Grazie all'analisi complessiva del volume di traffico Internet e delle attività di blocco, i ricercatori Cisco possono offrire informazioni approfondite sulle origini del malware.

Come mostrato nella **figura 22**, il traffico dagli Stati Uniti è leggermente superiore ai tassi di blocco rilevati nel *Report semestrale di Cisco sulla cybersecurity 2016*. Gli Stati Uniti hanno subito in assoluto la maggior parte dei blocchi, ma questo dipende dall'enorme quota di traffico online che ha luogo entro i loro confini. Inoltre, essi sono uno dei principali obiettivi al mondo di attacchi malware.

Conclusioni per gli esperti della sicurezza: analogamente alle attività di blocco Web relative ai settori, quelle regionali mostrano che il traffico malware è un problema globale.

Figura 22 Blocchi Web per paese

Valore previsto: 1,0



Fonte: Cisco Security Research

CONDIVIDI

Tempi di rilevamento: una metrica essenziale per misurare i progressi degli addetti alla sicurezza

Cisco affina costantemente il proprio approccio alla misurazione del TTD, allo scopo di effettuare e registrare stime sempre più precise delle mediane. Le recenti modifiche in questo approccio hanno migliorato la visibilità nella categoria di file classificati come "sconosciuti" alla prima comparsa sulla scena e, in seguito ad analisi continue e osservazioni globali, identificati come "notoriamente dannosi". Grazie a una visione dei dati più olistica, siamo maggiormente in grado di determinare il momento in cui è apparsa una minaccia e quanto tempo è stato necessario perché i team responsabili della sicurezza potessero identificarla in quanto tale.

Queste nuove informazioni ci hanno aiutato a calcolare la mediana TTD relativa a novembre 2015, pari a 39 ore. (Vedere la **figura 23**). Entro gennaio 2016, abbiamo ridotto la mediana TTD a 6,9. Dopo avere raccolto e analizzato i dati relativi a ottobre 2016, i nostri ricercatori esperti di minacce hanno determinato che i prodotti Cisco avevano conseguito una mediana TTD di 14 ore nel periodo compreso tra novembre 2015 e ottobre 2016. (Nota: il valore della mediana TTD per il 2016 è la media dei valori rilevati nell'arco di tempo in esame).

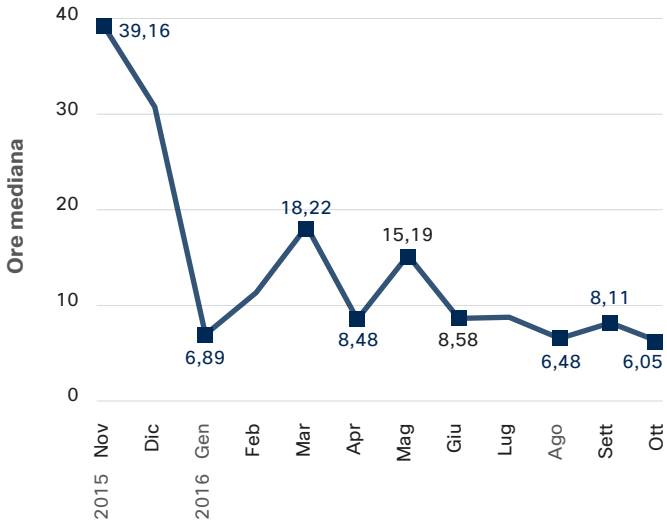
Durante tutto il 2016 la mediana TTD ha oscillato, ma nel complesso ha presentato una tendenza decrescente. Gli incrementi della mediana TTD indicano i momenti in cui gli hacker hanno lanciato un'ondata di nuove minacce. Le diminuzioni successive corrispondono ai periodi in cui gli addetti alla difesa hanno ripreso il controllo della situazione e hanno identificato rapidamente le minacce note.

La **figura 23** indica inoltre che, entro la fine di aprile 2016, la mediana TTD era di circa 15 ore, un valore superiore alle 13 ore registrate nel *Report semestrale di Cisco sulla cybersecurity 2016*.[14] Il valore pari a 15 ore si basa sui dati raccolti tra novembre 2015 e aprile 2016 e non è stato ricavato analizzando, in modo retrospettivo e per mezzo nel nuovo approccio, le informazioni più dettagliate sui file. Utilizzando il nuovo valore TTD semestrale, possiamo rilevare come il TTD sia diminuito a circa 9 ore nel periodo compreso tra maggio e ottobre 2016.

L'esame retrospettivo dei dati è importante, non solo per misurare in modo più preciso la mediana TTD, ma anche per studiare in che modo le minacce si evolvano nel tempo. Molte di esse, infatti, sono particolarmente sfuggenti e può essere necessario molto tempo per identificarle, sebbene esse siano note alla comunità degli esperti di sicurezza.

Gli hacker modificheranno alcune famiglie di malware per impedirne il rilevamento e aumentare il lasso di tempo in cui esse possono agire. Questa tattica ostacola i progressi degli addetti alla sicurezza nel conseguire, e poi mantenere, un vantaggio nel rilevamento di molti tipi di minacce conosciute. (Per ulteriori informazioni su questo argomento, vedere "Tempo di evoluzione: per alcune minacce, il cambiamento è costante" a pagina 34). Tuttavia, il fatto che i criminali informatici stiano modificando spesso e rapidamente le minacce indica che essi stanno incontrando difficoltà, elevate e costanti, nel trovare nuovi modi per mantenere le minacce operative e redditizie.

Figura 23 Mediana mensile del TTD



Fonte: Cisco Security Research

Usiamo il termine tecnico "time to detection" o "TTD" per indicare il periodo di tempo che intercorre fra una compromissione e il rilevamento della minaccia. Questo lasso di tempo viene determinato utilizzando dati telemetrici di sicurezza opt-in, raccolti da prodotti di sicurezza Cisco distribuiti in tutto il mondo. Sfruttando la nostra visibilità globale e un modello di analisi continua, siamo in grado di misurare il tempo che intercorre dal momento in cui un codice dannoso è eseguito in un endpoint al momento in cui si determina che si tratta di una minaccia; per ogni codice dannoso che risultava non classificato al momento del rilevamento.

[14] *Report semestrale di Cisco sulla cybersecurity 2016*: **http://www.cisco.com/c/m/en_us/offers/sc04/2016-midyear-cybersecurity-report/index.html**.

Tempo di evoluzione: per alcune minacce, il cambiamento è costante

I criminali informatici impiegano varie tecniche di mimetizzazione per mantenere il proprio malware operativo e redditizio: due metodi molto diffusi consistono nella modifica delle modalità di distribuzione del payload e nella generazione di nuovi file in rapida sequenza (il che rende inefficaci le tecniche di rilevamento esclusivamente hash). I nostri ricercatori hanno esaminato attentamente il modo in cui gli hacker hanno usato queste due strategie per consentire a sei note famiglie di malware (Locky, Cerber, Nemucod, Adwind RAT, Kryptik e Dridex) di eludere il rilevamento e continuare a compromettere utenti e sistemi.

Con il nostro studio abbiamo cercato di misurare il "tempo di evoluzione" (TTE), ossia il tempo che gli hacker impiegano a modificare il modo in cui un determinato malware viene distribuito e l'intervallo tra un cambio di tattica e il successivo. Abbiamo analizzato i dati degli attacchi Web provenienti da varie fonti Cisco, in particolare, dati dei proxy Web, prodotti malware avanzati di tipo cloud ed endpoint nonché vari motori antimalware.

I nostri ricercatori sono andati alla ricerca di differenze nelle estensioni dei file che trasportavano il malware e nel tipo di contenuto dei file (MIME) così come definito dai sistemi degli utenti e hanno stabilito che ciascuna famiglia di malware presenta un percorso evolutivo unico. Per ognuna di esse, abbiamo esaminato i percorsi sia nei metodi di distribuzione basati sul Web, sia in quelli basati sulle e-mail. Abbiamo anche tracciato l'età degli hash univoci associati a ogni famiglia di malware per determinare la rapidità con la quale gli hacker creano nuovi file (e, di conseguenza, nuovi hash).

Nel corso della ricerca, abbiamo imparato che:

- Le famiglie di ransomware sembrano presentare uno schema comune di rotazione dei nuovi file binari. Tuttavia, Locky utilizza più estensioni di file e combinazioni MIME per veicolare il proprio payload.
- Alcune famiglie di malware usano solo alcuni metodi per la trasmissione dei file, mentre altre ne impiegano 10 o più. Gli hacker tendono a utilizzare i file binari efficaci per lunghi periodi. In altri casi, i file appaiono e scompaiono rapidamente, il che indica che gli autori del malware hanno la necessità di cambiare tattica rapidamente.
- Le famiglie di malware di Adwind RAT e Kryptik presentano una mediana TTD più elevata. (Per ulteriori informazioni sul TTD, vedere a pagina 33). Inoltre, abbiamo osservato che queste famiglie presentano età dei file diversificate, il che suggerisce che i criminali informatici riutilizzano i file binari efficaci che sanno essere più difficili da individuare.
- Considerando le età dei file della famiglia di malware di Dridex, sembra che l'economia sommersa stia abbandonando questo trojan bancario una volta molto diffuso. Alla fine del 2016 il volume di rilevamenti per Dridex è diminuito, così come lo sviluppo di nuovi file binari per la distribuzione di questo malware. Questa tendenza suggerisce che gli autori di malware non trovano più interessante curare l'evoluzione di questa minaccia oppure che hanno trovato un nuovo modo per confezionare il malware che lo rende più difficile da individuare.

TTE e TTD

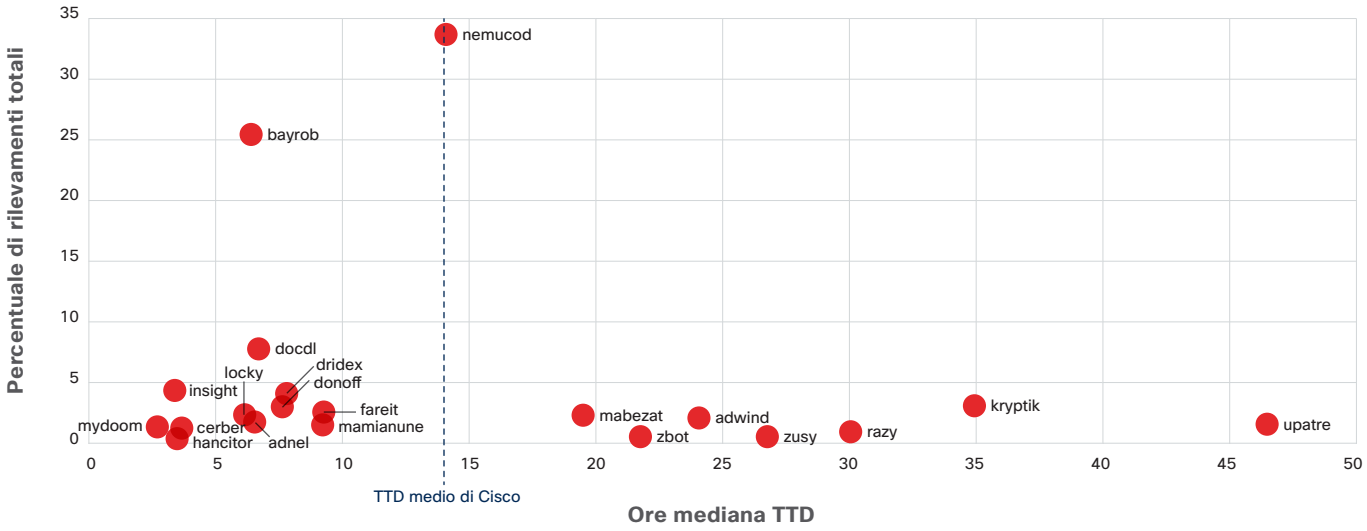
Le sei famiglie di malware analizzate nel nostro studio sul TTE sono elencate nella **figura 24**. Il grafico mostra la mediana TTD per le prime 20 famiglie di malware (ordinate in base al numero di rilevamenti) registrata dai nostri ricercatori tra novembre 2015 e novembre 2016. Il nostro valore medio per la mediana TTD relativa a questo periodo è pari a 14 ore. (Per informazioni sulla modalità di calcolo del TTD, vedere a pagina 33).

Molte delle famiglie di malware che i prodotti Cisco stanno rilevando all'interno della mediana TTD sono minacce industrializzate che si diffondono rapidamente e, quindi, risultano predominanti. Cerber e Locky, entrambi ransomware, ne sono due esempi.

Al di sotto della mediana TTD vengono normalmente rilevate minacce vecchie e pervasive che gli hacker non si preoccupano di far evolvere molto. Gli esempi includono famiglie di malware come Bayrob (malware botnet), Mydoom (un worm per computer che agisce su Microsoft Windows) e Dridex (un trojan bancario).

Nelle sezioni che seguono, presentiamo i principali risultati della ricerca su TTE e TTD per le famiglie di malware di Locky, Nemucod, Adwind RAT e Kryptik. I risultati dettagliati per Cerber e Dridex sono riportati nell'Appendice a pagina 78.

Figura 24 Le mediane del TTD delle principali famiglie di malware (le 20 famiglie principali in base al numero di rilevamenti)



Fonte: Cisco Security Research

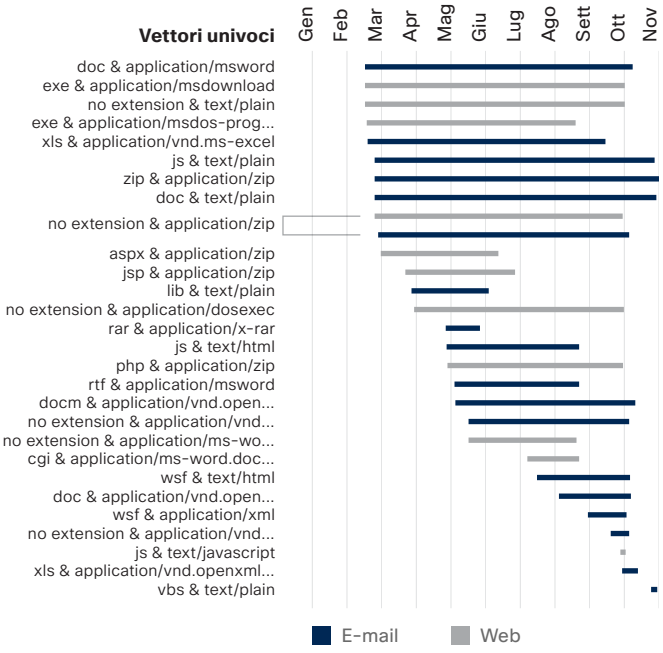
Analisi del TTE: Locky

Grazie alla nostra ricerca sul TTE abbiamo appreso che Locky e Cerber impiegano un numero limitato di estensioni di file e combinazioni MIME per diffondere malware attraverso il Web o i messaggi e-mail. (Vedere la **figura 25**). Abbiamo osservato varie combinazioni che comprendevano tipi di contenuti di file correlati a Microsoft Word (msdownload, ms-word). Tuttavia, le estensioni dei file associate (.exe e .cgi) non rimandavano a un file Word. Abbiamo inoltre identificato tipi di contenuti che facevano riferimento a file .zip dannosi.

Sembra altresì che sia Locky che Cerber utilizzino entrambi nuovi file binari con una certa frequenza nel tentativo di eludere il rilevamento basato su file. Le età dei file relativi alla famiglia di malware di Locky sono riportate nella **figura 26**. La metà superiore del grafico mostra le età dei file osservati durante un determinato mese, mentre la parte inferiore mostra le variazioni mensili nel volume degli hash collegati a Locky (sia i file nuovi, sia quelli osservati in precedenza).

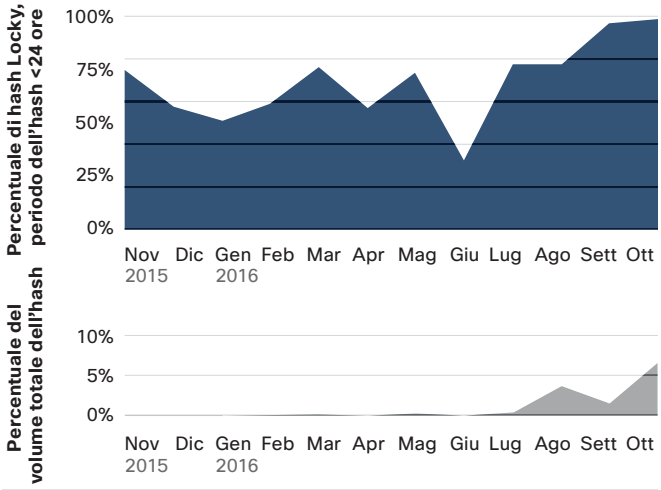
Nella **figura 26** si osserva anche la diminuzione dei volumi a giugno nonché la distribuzione delle età dei file. La botnet di Necurs, che era nota per trasmettere Locky, è stato disattivata a giugno. Questa circostanza ha probabilmente reso marginali gli sforzi degli autori di malware per tenere aggiornato il malware nel corso del mese. Tuttavia, è chiaro che essi abbiano recuperato terreno rapidamente. Entro luglio, il malware era tornato alla sua più normale combinazione di età dei file, la maggior parte dei quali (74%) era meno vecchia di un giorno quando è stata rilevata per la prima volta.

Figura 25 Estensioni di file e combinazioni MIME per la famiglia di minacce e gli indicatori che rimandano al payload Locky e lo contengono (vettori e-mail e Web)



Fonte: Cisco Security Research

Figura 26 Età degli hash per la famiglia di malware Locky e percentuale del volume hash totale osservato mensilmente



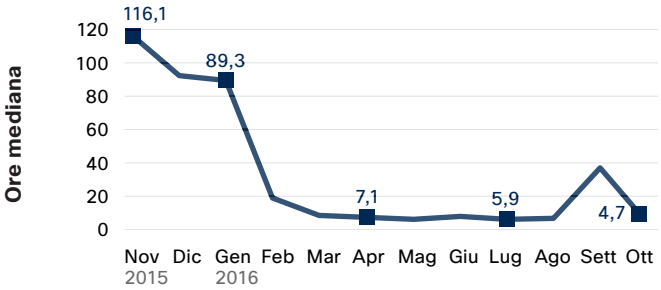
Fonte: Cisco Security Research

CONDIVIDI

La rapida rotazione di file binari per questo tipo di ransomware non sorprende. Istanze di Locky e di Cerber sono spesso rilevate nello stesso giorno in cui vengono introdotte oppure entro 1 o 2 giorni successivi, imponendo ai criminali informatici di modificare continuamente queste minacce se vogliono che rimangano attive ed efficaci. (La figura 24, illustrata in precedenza, mostra che i prodotti Cisco hanno rilevato sia Locky, sia Cerber entro la mediana del TTD per il 2016).

La figura 27 mostra la mediana TTD per il ransomware Locky, che è diminuita notevolmente da circa 116 ore di novembre 2015 a meno di 5 a ottobre 2016.

Figura 27 TTD per la famiglia di malware Locky



Fonte: Cisco Security Research

Analisi del TTE: Nemucod

Nel 2016 Nemucod è stato il malware rilevato più spesso nell'ambito delle 20 principali famiglie mostrate nella figura 24. Gli autori degli attacchi utilizzano questo dowloader per distribuire ransomware e altre minacce come trojan backdoor che facilitano gli attacchi basati sui clic fraudolenti. Alcune varianti di Nemucod agiscono anche come motori per la distribuzione del payload dannoso di Nemucod.

Figura 28 Estensioni di file e combinazioni MIME per Nemucod (vettori e-mail e Web)

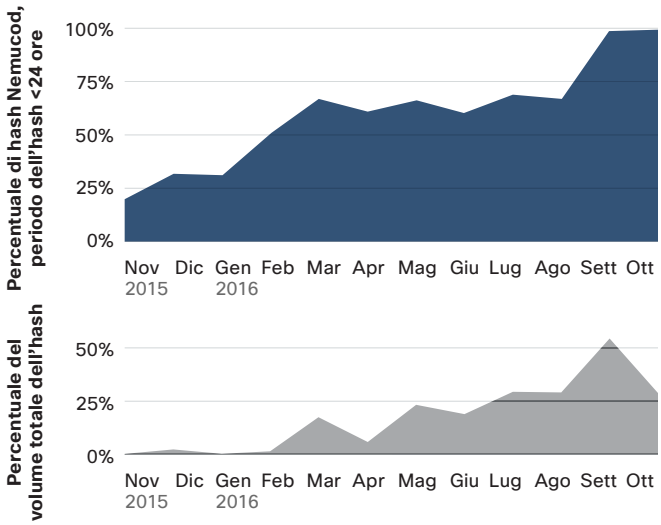
Fonte: Cisco Security Research

Secondo i nostri ricercatori, una delle ragioni per cui Nemucod è stato così preponderante nel 2016 è che i suoi autori hanno modificato spesso questa minaccia. Cisco ha identificato oltre 15 estensioni di file e combinazioni MIME associate alla famiglia di Nemucod utilizzate per trasmettere malware attraverso il Web mentre un numero ancora maggiore di combinazioni è stato impiegato per inviare la minaccia agli utenti per mezzo dei messaggi e-mail (figura 28).

Diverse estensioni di file e combinazioni MIME (Web ed e-mail) sono state progettate per indirizzare gli utenti verso file .zip o archivi dannosi. Inoltre, gli hacker hanno riutilizzato molte combinazioni nei mesi oggetto dell'osservazione.

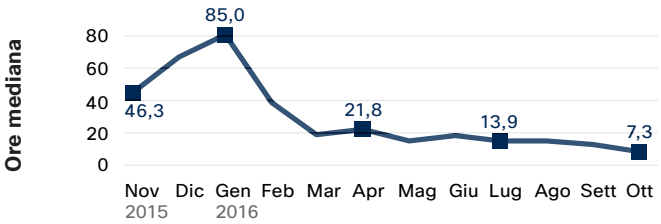
Come illustrato nella figura 29, molti hash di Nemucod hanno meno di 2 giorni quando vengono rilevati. A settembre e ottobre 2016, quasi ogni file binario bloccato collegato alla famiglia di Nemucod aveva meno di un giorno di vita.

Figura 29 Età degli hash per la famiglia di malware Nemucod e percentuale del volume hash totale osservato mensilmente



Fonte: Cisco Security Research

Figura 30 TTD per la famiglia di malware Nemucod



Fonte: Cisco Security Research

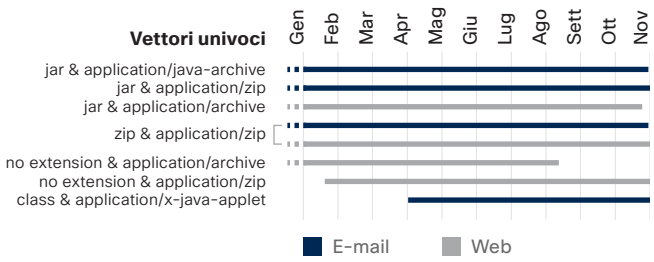
Analisi del TTE: Adwind RAT

Gli esperti di minacce di Cisco hanno scoperto che il malware Adwind RAT (un trojan per l'accesso remoto) viene distribuito per mezzo di estensioni di file e combinazioni MIME che comprendono i file .zip o .jar, indipendentemente dal fatto che il malware venga trasmesso attraverso un vettore di attacco e-mail o Web. (Vedere la **figura 31**).

Durante la maggior parte del periodo osservato nel 2016 Adwind RAT ha utilizzato un'ampia gamma di età degli hash, fatta eccezione per i mesi di settembre e ottobre, quando i file erano per lo più vecchi di 1 o 2 giorni (**figura 32**).

Inoltre, abbiamo scoperto che la mediana TTD di Adwind RAT è costantemente superiore a quella delle altre famiglie di malware analizzate (**figura 33**). Per garantire il successo di Adwind RAT, gli autori del malware sembrano avere sviluppato meccanismi di trasmissione difficili da identificare. Di conseguenza, non hanno bisogno di cambiare hash così spesso o così rapidamente come gli attori dietro ad altre famiglie di malware. Il trojan Adwind è noto anche con altri nomi, come JSocket e AlienSpy.

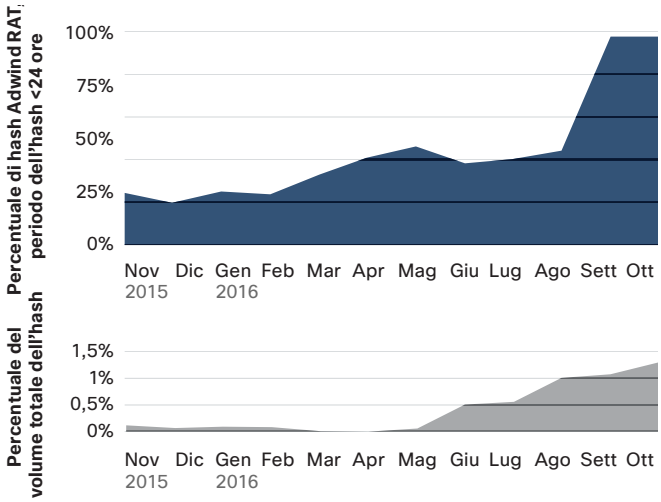
Figura 31 Estensioni di file e combinazioni MIME per Adwind RAT (vettori e-mail e Web)



Fonte: Cisco Security Research

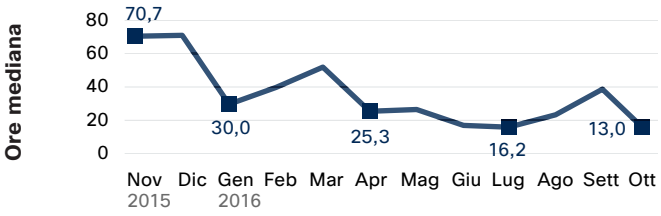
Scaricare il grafico del 2017 al link seguente: **www.cisco.com/go/acr2017graphics**

Figura 32 Età degli hash per la famiglia di malware Adwind RAT e percentuale del volume hash totale osservato mensilmente



Fonte: Cisco Security Research

Figura 33 TTD per la famiglia di malware Adwind RAT



Fonte: Cisco Security Research

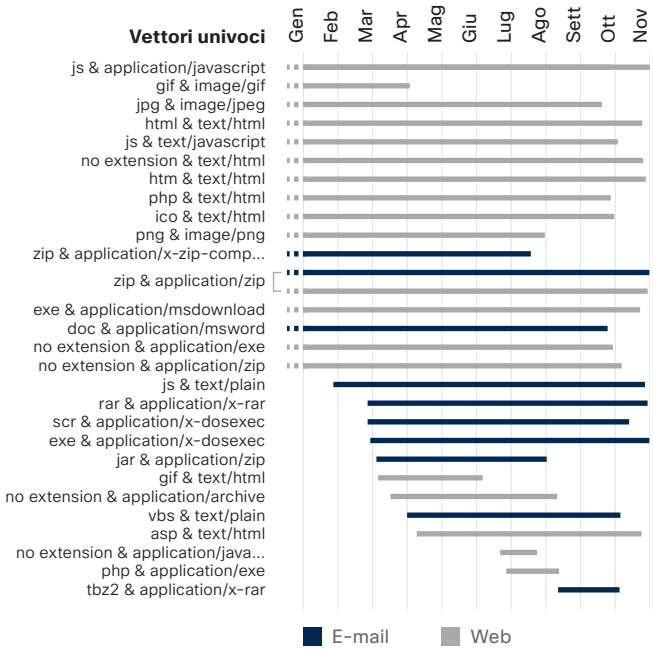
Analisi del TTE: Kryptik

Kryptik, come il malware Adwind RAT, aveva una mediana TTD costantemente superiore (pari a circa 20 ore) a quella delle altre famiglie di malware analizzate da Cisco per lo studio sul TTE condotto tra novembre 2015 e ottobre 2016 (figura 36). Tuttavia, entro ottobre i prodotti Cisco avevano ridotto la finestra relativa alla mediana TTD di Kryptik a meno di 9 ore (figura 36).

La famiglia di malware di Kryptik, inoltre, impiegava una gamma di età degli hash più ampia rispetto alle altre famiglie di malware analizzate, specialmente durante la prima metà del 2016. La capacità degli autori di Kryptik di avvalersi di hash vecchi per un tempo così lungo indica che gli addetti alla sicurezza hanno incontrato difficoltà nell'identificazione di questo tipo di malware.

Durante il periodo sotto osservazione, gli autori di Kryptik hanno utilizzato un'ampia gamma di metodi per la consegna del payload basati sui vettori di attacco Web. Essi hanno impiegato file JavaScript e file di archiviazione come i file .zip in estensioni di file e combinazioni MIME tanto per il Web, quanto per le e-mail. (Vedere la figura 34). Alcune delle combinazioni risalgono al 2011.

Figura 34 Estensioni di file e combinazioni MIME per Kryptik (vettori e-mail e Web)

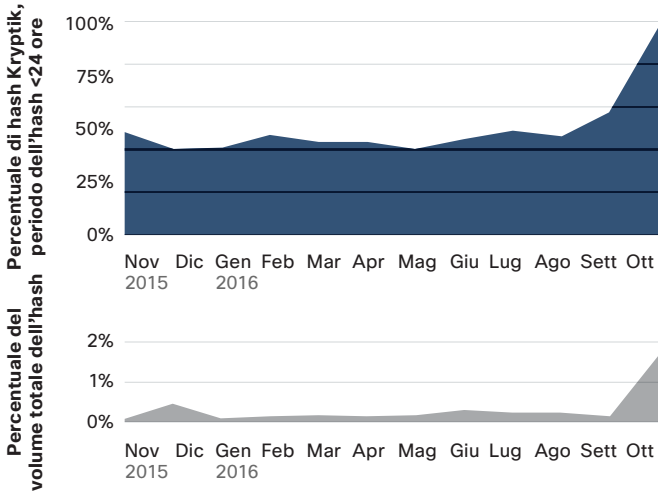


Fonte: Cisco Security Research

Nell'analisi che abbiamo condotto sulle sei famiglie di malware abbiamo scoperto che gli hacker devono cambiare spesso tattica per sfruttare la limitata finestra di tempo durante la quale le minacce possono operare con successo. Queste modifiche indicano che gli addetti alla sicurezza sono sempre più bravi nell'individuare rapidamente il malware conosciuto, anche quando una minaccia si è evoluta. Gli hacker sono quindi costretti a trovare nuovi modi per evitare il rilevamento e mantenere la redditività delle loro campagne.

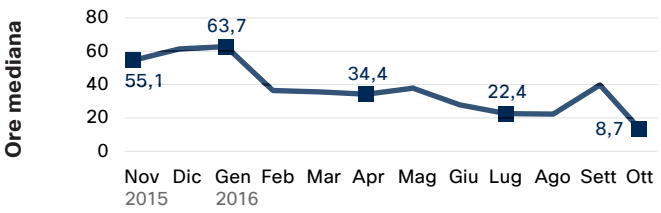
In questo panorama complesso fatto di rapide trasformazioni, dove tutte le famiglie di malware si comportano in modo diverso, esperienza umana e soluzioni puntuali non sono sufficienti per identificare le minacce e reagire rapidamente. Un'architettura di sicurezza integrata che fornisce informazioni in tempo reale sulle minacce, insieme a rilevamento e difesa automatici, è essenziale per migliorare il TTD e garantire un rimedio rapido quando si verificano infezioni.

Figura 35 Età degli hash per la famiglia di malware Kryptik e percentuale del volume hash totale osservato mensilmente



Fonte: Cisco Security Research

Figura 36 TTD per la famiglia di malware Kryptik



Fonte: Cisco Security Research

Comportamento degli addetti alla sicurezza

Comportamento degli addetti alla sicurezza

Vulnerabilità in declino nel 2016

Secondo la nostra ricerca, nella seconda metà del 2016 le vulnerabilità rivelate dai produttori sono diminuite significativamente rispetto al 2015 (**figura 37**) e il National Vulnerability Database mostra un declino simile, ma le ragioni di questa circostanza non sono del tutto chiare.

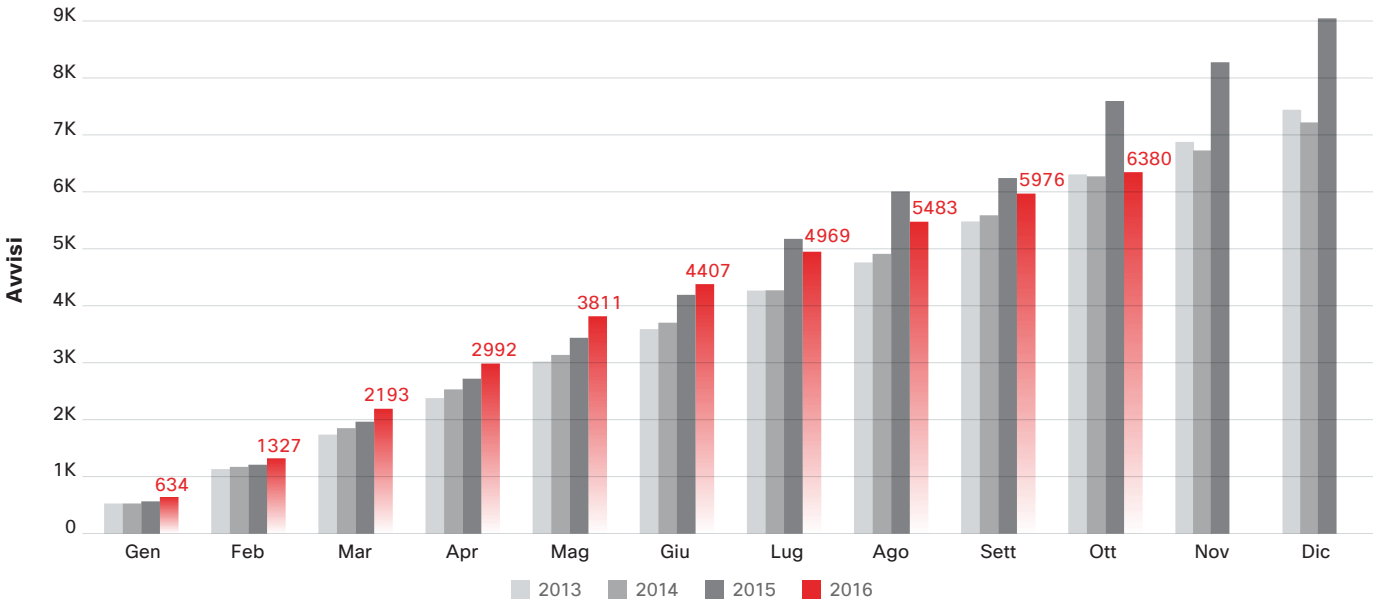
Va notato che il 2015 è stato un anno particolarmente attivo per quanto riguarda le vulnerabilità e, quindi, i numeri del 2016 potrebbero essere quelli relativi a un ritmo normale. Da gennaio a ottobre 2015 il numero complessivo di avvisi ha raggiunto quota 7602. Nello stesso periodo del 2016, il numero totale degli avvisi era pari a 6380, mentre nel 2014 era 6272.

Questo numero elevato di report sulla vulnerabilità del 2015 potrebbe indicare che i produttori hanno esaminato più attentamente i prodotti e il codice esistenti e implementato con maggiore rigore le pratiche SDL (Secure Development Lifecycle, ciclo di vita dello sviluppo sicuro), identificando e correggendo le vulnerabilità. La riduzione delle vulnerabilità segnalate potrebbe significare che questi sforzi vengono ripagati, ossia, che i produttori si stanno concentrando sull'identificazione delle vulnerabilità e sulla loro eliminazione prima che i prodotti raggiungano il mercato.

Nel 2016 Apple è stata il fornitore che ha mostrato la diminuzione più drastica in materia di vulnerabilità: 324 rispetto alle 705 segnalate dall'azienda nel 2015, con una diminuzione del 54%. Analogamente, Cisco ha riferito 488 vulnerabilità nel 2015 e 310 nel 2016 (con una riduzione del 36%).

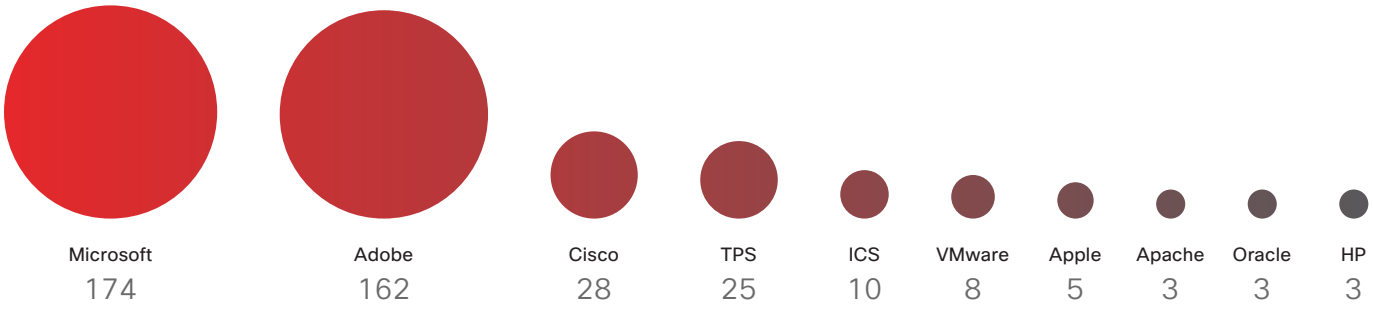
Una preoccupazione tra i ricercatori della sicurezza è che tra gli esperti della sicurezza si stia diffondendo una sorta di "stress da vulnerabilità". Negli ultimi mesi, infatti, non vi è stato alcun annuncio relativo a vulnerabilità importanti che abbia sconvolto il settore come fece Heartbleed nel 2014. Infatti, il clamore attorno a vulnerabilità "famose" come Heartbleed e l'aumento del 2015 hanno, con tutta probabilità, contribuito al livello di stress o, per lo meno, hanno prodotto un minore interesse a segnalare vulnerabilità.

Figura 37 Totale cumulativo annuo degli avvisi



Fonte: Cisco Security Research

Figura 38 Avvisi di vulnerabilità critiche in base a fornitore e tipo



Fonte: National Vulnerability Database (NVD)

Cisco ora utilizza valutazioni basate su gravità/impatto (SIR, severity/impact rating) in cui i livelli di valutazione sono: "critico", "elevato", "medio" e "basso". Le valutazioni riflettono una classificazione semplificata dei punteggi del Common Vulnerability Scoring System (CVSS). Inoltre, Cisco ha adottato CVSS v3.0, il successore di CVSS v2.0. A causa di questo cambiamento, alcune vulnerabilità possono avere punteggi più alti rispetto a prima, quindi gli esperti della sicurezza potrebbero notare un piccolo incremento delle vulnerabilità classificate come "critiche" ed "elevate" invece che "medie" o "basse". Per ulteriori informazioni sul cambiamento nel sistema di punteggi, leggere il post del blog di Cisco Security,The Evolution of Scoring Security Vulnerabilities: The Sequel.

Nello Studio comparativo di Cisco delle infrastrutture di sicurezza del 2017 (pagina 49), gli esperti della sicurezza hanno descritto una leggera diminuzione del loro consenso in materia di attuazione della sicurezza. Questa diminuzione può essere collegato allo "stress" dovuto alla necessità di implementare aggiornamenti e patch a ciclo continuo. Ad esempio, nel 2016 il 53% degli esperti della sicurezza ha affermato di condividere pienamente la necessità di rivedere e migliorare le procedure di sicurezza in modo regolare, formale e strategico mentre nel 2014 e nel 2015 la percentuale era pari al 56%.

Naturalmente, la diminuzione delle vulnerabilità non deve generare un eccesso di fiducia circa il panorama delle minacce e in nessun caso si può pensare di diminuire l'attenzione alle minacce, anche in assenza di vulnerabilità di alto profilo.

Come abbiamo consigliato nei report precedenti, gli esperti della sicurezza devono porre in atto uno sforzo programmato per determinare la priorità delle patch e, se la mancanza di personale o di altre risorse impedisce l'installazione di tutte quelle disponibili, valutare quali siano quelle indispensabili per la sicurezza della rete e porle in cima all'elenco delle cose da fare.

Scaricare il grafico del 2017 al link seguente: **www.cisco.com/go/acr2017graphics**

Figura 39 Avvisi di vulnerabilità critiche selezionate

Titolo dell'avviso	Data del rilascio
Vulnerabilità nell'esecuzione del codice di corruzione della memoria di Adobe Acrobat e Adobe Reader	28 luglio 2016
Vulnerabilità nell'esecuzione del codice remoto di corruzione della memoria di Adobe Acrobat e Adobe Reader	28 luglio 2016
Vulnerabilità di corruzione della memoria di Adobe Acrobat e Adobe Reader	21 luglio 2016
Vulnerabilità dell'intero overflow di Adobe Acrobat e Adobe Reader	23 maggio 2016
Vulnerabilità nell'esecuzione del codice remoto di corruzione della memoria di Adobe Acrobat e Adobe Reader	8 febbraio 2016
Vulnerabilità di corruzione della memoria di Adobe Acrobat e Adobe Reader	28 luglio 2016
Vulnerabilità di corruzione della memoria di Adobe Acrobat e Adobe Reader	18 luglio 2016
Vulnerabilità di corruzione della memoria di Adobe Acrobat e Adobe Reader	23 giugno 2016
Vulnerabilità di corruzione della memoria di Adobe Acrobat e Adobe Reader	24 maggio 2016
Vulnerabilità di corruzione della memoria di Adobe Acrobat e Adobe Reader	23 maggio 2016

Fonte: Cisco Security Research

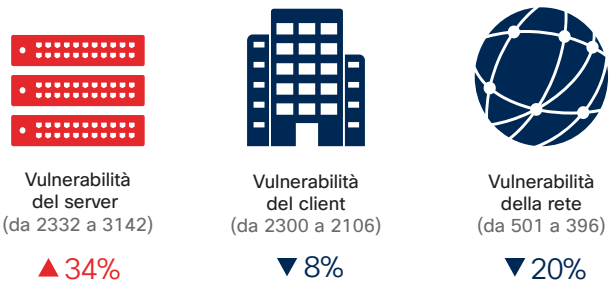
Gli avvisi elencati sopra corrispondono a vulnerabilità selezionate classificate come critiche nel 2016. Inoltre fonti diverse hanno segnalato la presenza di codice exploit disponibile pubblicamente o da sfruttare attivamente in rete.

Vulnerabilità dei server e dei client

Come illustrato nel *Report semestrale di Cisco sulla cybersecurity 2016*, gli hacker trovano spazio e tempo per operare anche con soluzioni lato server. Lanciando attacchi ai software dei server, essi possono potenzialmente acquisire il controllo di più risorse di rete oppure spostarsi su soluzioni di importanza fondamentale per le aziende.

I ricercatori di Cisco hanno tracciato le vulnerabilità di client e server per ciascun fornitore (**figura 40**).

Figura 40 Analisi dettagliata delle vulnerabilità client-server, 2015-2016



Fonte: National Vulnerability Database

Middleware: gli hacker individuano opportunità nel software privo di patch

Nel *Report semestrale di Cisco sulla cybersecurity 2016* abbiamo mostrato i dati relativi agli attacchi condotti contro sistemi lato server. Riteniamo che, nel 2017, il middleware, che collega le piattaforme o le applicazioni, attirerà l'attenzione di hacker in cerca di spazi operativi nei quali gli addetti alla sicurezza siano lenti a reagire o a riconoscere le minacce.

Mentre erano alla ricerca di vulnerabilità nei software di terze parti, i ricercatori di Cisco hanno individuato una media di 14 nuovi problemi al mese, la maggior parte dei quali (62) erano attribuibili all'uso di middleware. Di queste 62 vulnerabilità, 20 sono state trovate nel codice che gestisce i file PDF; 12 nel codice che gestisce le immagini; 10 nel codice di diffuse soluzioni per la produttività individuale; nove nel codice dei software di compressione e 11 in altre librerie (**figura 41**).

Le vulnerabilità del middleware rappresentano una minaccia alla sicurezza del tutto unica, poiché le librerie normalmente non sono aggiornate così rapidamente come il software destinato ai client, ossia quello con cui gli utenti interagiscono direttamente ogni giorno come le soluzioni per la produttività individuale. Le librerie del middleware potrebbero venire escluse dai controlli sul software e, di conseguenza, le vulnerabilità possono permanere.

Figura 41 Vulnerabilità riscontrate nelle librerie del middleware

Fonte: Cisco Security Research

CONDIVIDI

Le aziende possono assumere che il middleware sia sicuro e porre maggiore attenzione all'aggiornamento delle soluzioni di alto profilo, ma devono anche dare per scontato che gli hacker tenteranno di accedere alle loro reti attraverso queste vie poco presidiate. Il middleware diventa così un punto cieco in fatto di sicurezza per gli addetti alla difesa e un'opportunità per i criminali informatici.

La difficoltà nell'aggiornamento delle librerie del middleware è strettamente collegata al problema del software open source (affrontato nel *Report semestrale di Cisco sulla sicurezza 2015*), poiché molte soluzioni middleware sono prodotte da sviluppatori open source. (Tuttavia, il problema esistente può riguardare gli sviluppatori di middleware sia open source, sia proprietario). Di conseguenza, le librerie del middleware possono disporre di molti sviluppatori che le mantengano aggiornate. Nell'elenco dei compiti di un team di sicurezza o IT oberato, gli aggiornamenti delle librerie del middleware possono non occupare le prime posizioni, ma è indubbio che essi dovrebbero ricevere maggiore attenzione.

Qual è l'impatto potenziale di una vulnerabilità del middleware sfruttata dagli hacker? Grazie alle connessioni tra il middleware e altri sistemi chiave, quali le applicazioni e-mail o per la messaggistica, gli hacker potrebbero spostarsi all'interno di questi ultimi e utilizzarli per inviare messaggi di phishing o spam oppure spacciarsi per utenti autorizzati e avvalersi in modo fraudolento dei rapporti di fiducia esistenti per ampliare le possibilità di accesso.

Per evitare di diventare vittime di un attacco lanciato per mezzo di una vulnerabilità del middleware, è necessario:

- Mantenere attivamente un elenco delle dipendenze note e delle librerie delle applicazioni utilizzate
- Monitorare attivamente la sicurezza di queste applicazioni e ridurre il più possibile i rischi
- Inserire un Service Level Agreement nei contratti con i fornitori di software che obblighi questi ultimi a fornire patch in modo tempestivo
- Verificare e riesaminare regolarmente le dipendenze tra software e l'uso delle librerie
- Chiedere ai fornitori di software informazioni dettagliate sulle procedure in essere per la manutenzione e il test dei loro prodotti

In sintesi: i ritardi nell'installazione delle patch aumentano il margine operativo a favore degli hacker e consentono loro di disporre di più tempo per acquisire il controllo di sistemi di importanza fondamentale. Nella sezione successiva, analizzeremo questo aspetto e le tendenze nell'applicazione di patch a soluzioni per la produttività molto diffuse come i browser Web.

Tempo per le patch: azzerare il tempo per il ripristino

Molti utenti non scaricano né installano tempestivamente le patch e gli hacker possono sfruttare le vulnerabilità non risolte da patch per accedere alle reti. Nell'ultima ricerca abbiamo osservato che la chiave per incoraggiare gli utenti a scaricare e installare le patch potrebbe consistere nella frequenza degli aggiornamenti software da parte dei fornitori.

Il rilascio di una patch di sicurezza è un chiaro segnale, a favore degli hacker, dell'esistenza di una vulnerabilità che può essere sfruttata proficuamente. Sebbene sia probabile che gli hacker di alto livello abbiano già trovato il modo di approfittarne, l'annuncio di una patch apre a tutti la stagione di caccia per le versioni precedenti del software.

Quando i fornitori di software rilasciano nuove versioni in base a un programma regolare, gli utenti sono condizionati a scaricare e installare gli aggiornamenti. Al contrario, se questi ultimi vengono rilasciati in modo sporadico e imprevedibile, è meno probabile che gli utenti li installino, continuando a utilizzare soluzioni obsolete che possono contenere vulnerabilità sfruttabili.

Altri aspetti che influiscono sul ciclo di aggiornamento sono:

- La quantità di disturbo provocata dal promemoria
- La facilità di uscita dal programma di aggiornamento
- La frequenza con la quale il software viene utilizzato

Vi sono varie finestre temporali nelle quali è più alta la probabilità che gli utenti installino un aggiornamento rilasciato da un fornitore. I nostri ricercatori hanno preso in esame le installazioni di software negli endpoint utilizzati dai nostri clienti e le hanno classificate in tre categorie:

- **Nuove versioni:** nell'endpoint è eseguita la versione software più recente disponibile
- **Versioni recenti:** nell'endpoint è eseguita una delle tre versioni precedenti del software, ma non la più recente
- **Vecchie versioni:** nell'endpoint è eseguito un software più vecchio delle tre versioni precedenti a quella attuale

Ad esempio, se un fornitore software rilascia la versione 28 l'1 gennaio 2017, questa è la versione nuova; la versione 26 è recente e la versione 23 è vecchia. (Le figure mostrate nella pagina seguente contengono didascalie relative alla settimana in cui è avvenuto il rilascio di una o più versioni del software).

Esaminando gli utenti di Adobe Flash (**figura 42**), abbiamo scoperto che, entro la prima settimana dal rilascio di un aggiornamento, quasi l'80% degli utenti aveva installato l'ultima versione del software. In altri termini, è sufficiente una sola settimana circa affinché la popolazione di utenti acquisisca la versione più recente. Questo periodo di "ripristino" pari a una settimana costituisce la finestra nella quale gli hacker hanno l'opportunità di agire.

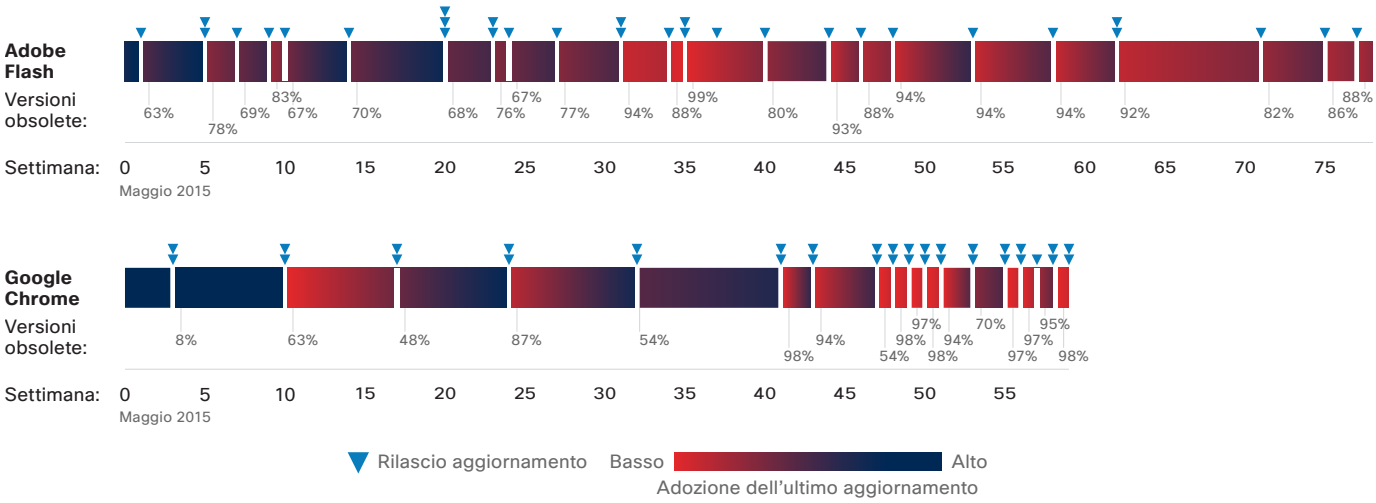
Se consideriamo l'ultima parte del IV trimestre 2015 del grafico relativo ad Adobe Flash, osserviamo una brusca diminuzione del numero di utenti che disponevano della versione più recente della soluzione. Nell'arco temporale oggetto di esame, Adobe ha rilasciato in rapida successione cinque versioni di Flash contenenti una combinazione di ulteriori funzionalità, correzioni dei bug e aggiornamenti di sicurezza. Un simile turbine di aggiornamenti può confondere gli utenti, che potrebbero chiedersi per quale motivo debbano scaricare così tanti aggiornamenti, sentirsi a disagio a causa del numero elevato di notifiche e pensare di avere già scaricato un aggiornamento essenziale e, quindi, ignorare i nuovi avvisi. Indipendentemente dal motivo alla base della mancanza di interesse nell'installazione di un aggiornamento, questa è una cattiva notizia per gli addetti alla difesa.

Esaminando gli aggiornamenti del browser Web Google Chrome, abbiamo osservato uno schema differente che riflette la regolarità degli aggiornamenti nonché una policy forte di uscita dal programma di aggiornamento che rende difficile per gli utenti ignorare le notifiche. Come mostrato nella **figura 42**, il numero di endpoint che eseguono la nuova versione è rimasto relativamente stabile nell'arco di più settimane.

I dati di Chrome indicano che gli utenti recuperano in tempi relativamente brevi e che, nel caso di aggiornamenti regolari, il tempo necessario è pari a circa una settimana. Nell'arco di 9 settimane comprese tra il secondo e il terzo trimestre del 2016, tuttavia, ci sono stati sette aggiornamenti. In questo intervallo la popolazione ha effettuato il ripristino, ma lo stress da aggiornamento ha iniziato a manifestarsi e la percentuale di utenti che hanno mantenuto una vecchia versione è aumentato costantemente, malgrado la maggioranza abbia compiuto le operazioni prescritte.

Anche il browser Mozilla Firefox propone aggiornamenti con cadenza regolare, ma il periodo di ripristino successivo a ciascun rilascio sembra essere pari a un mese. In altri termini, gli utenti non scaricano e non installano gli aggiornamenti con la stessa frequenza degli utenti di Chrome. Uno dei possibili motivi è che alcuni potrebbero non utilizzare il browser regolarmente e, pertanto, non visualizzano e non scaricano gli aggiornamenti. (Vedere la **figura 43** alla pagina successiva).

Figura 42 Tempo per le patch per Adobe Flash e Google Chrome



Fonte: Cisco Security Research

Abbiamo scoperto che Firefox eseguiva l'aggiornamento delle versioni a settimane alterne, con un aumento della frequenza nel corso del periodo osservato. Questo incremento della frequenza si manifesta nell'aumento delle versioni vecchie di Firefox nella popolazione. Il tempo di ripristino è di circa 1,5 settimane, ma i tempi si sovrappongono e la popolazione che tenta di rimanere aggiornata è appena il 30% della base di utenti. A un certo punto, due terzi degli utenti si sono limitati a eseguire un browser di quattro versioni più vecchio rispetto a quella corrente. Quindi, sebbene Firefox stia affrontando e risolvendo rapidamente gli errori, la base degli utenti non effettua gli aggiornamenti con la stessa frequenza.

Nel caso del software, il livello di utilizzo sembra essere anche un indicatore della sua vulnerabilità, giacché, quando gli utenti non vi accedono spesso e, di conseguenza, non sono consapevoli della necessità di applicare patch e di aggiornarlo, il software ignorato offre agli hacker margini in termini di spazio e di tempo per operare.

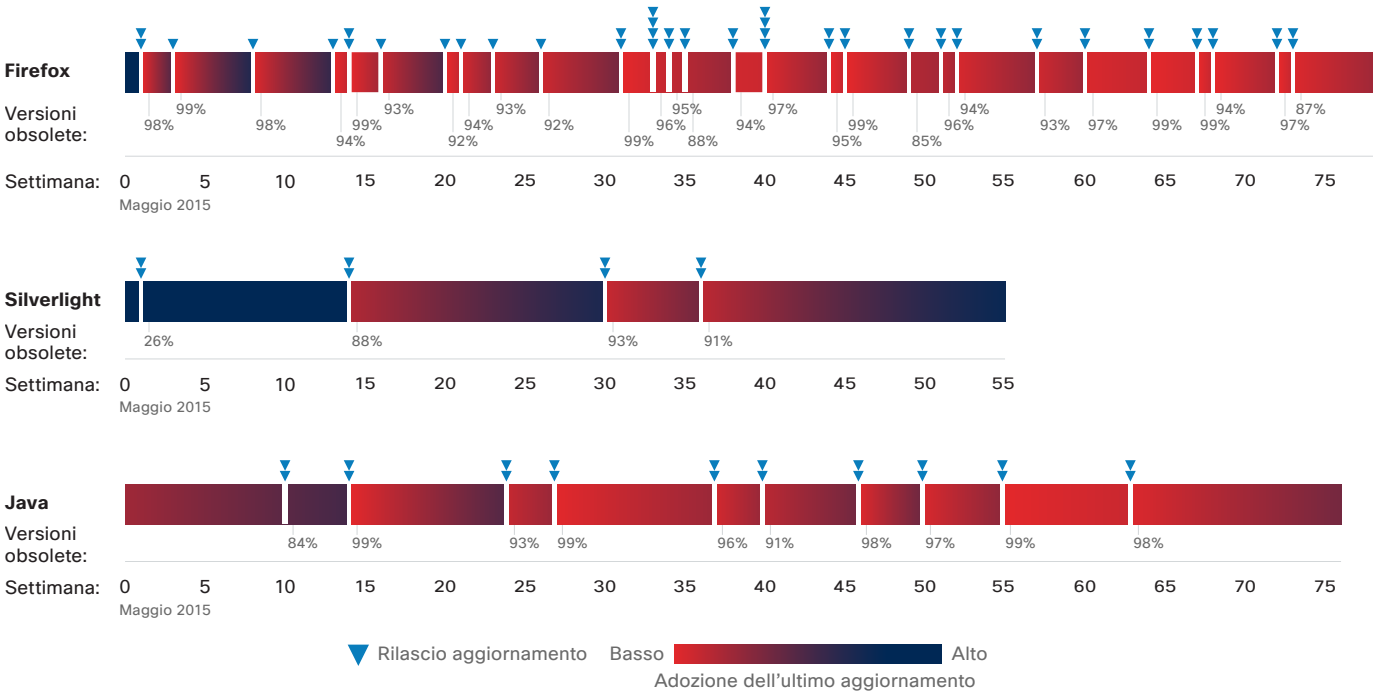
Questo aspetto appare palese nella ricerca su Microsoft Silverlight, che mostra un periodo di ripristino di 2 mesi dopo ogni rilascio. A un certo punto, in 5 settimane sono state pubblicate due release che hanno influito sulla popolazione degli utenti per oltre 3 mesi, come si può osservare tra il IV trimestre 2015 e il I trimestre 2016.

Sebbene Microsoft abbia annunciato la fine del ciclo di vita di Silverlight nel 2012, sta ancora rilasciando patch e correzioni dei bug. Tuttavia, questo comportamento pone lo stesso problema di Internet Explorer, poiché il software obsoleto e privo di patch invita gli hacker ad approfittare delle proprie vulnerabilità.

Il periodo di ripristino degli utenti di Java indica che la maggior parte di essi utilizza versioni di software da una a tre versioni più vecchio della release più recente. Il tempo di ripristino è di circa 3 settimane. Un aspetto insolito di Java è che la parte predominante della popolazione utilizza versioni recenti, mentre il ciclo di aggiornamento è pari a 1-2 mesi.

L'insegnamento generale che possiamo trarre dall'osservazione dei cicli di pubblicazione delle patch è che gli schemi di rilascio degli aggiornamenti sono un fattore determinante della postura degli utenti in materia di sicurezza che può mettere in pericolo le reti.

Figura 43 Tempo per le patch per Firefox, Silverlight e Java



Fonte: Cisco Security Research

Scaricare il grafico del 2017 al link seguente: **www.cisco.com/go/acr2017graphics**

Studio comparativo di Cisco delle infrastrutture di sicurezza del 2017

Studio comparativo di Cisco delle infrastrutture di sicurezza del 2017

Per valutare le opinioni degli esperti della sicurezza relativamente allo stato della sicurezza aziendale, Cisco ha chiesto a CSO (Chief Security Officer) e manager delle operazioni di sicurezza (SecOps), in diversi paesi e in aziende di varie dimensioni, cosa pensano delle risorse e delle procedure di sicurezza di cui dispongono. Lo studio comparativo di Cisco delle infrastrutture di sicurezza del 2017 offre informazioni dettagliate sul livello di maturità delle operazioni e delle procedure di sicurezza attualmente in uso, e una comparazione di questi risultati con quelli riportati negli studi del 2015 e 2016. Lo studio è stato condotto in 13 paesi, tra più di 2900 intervistati.

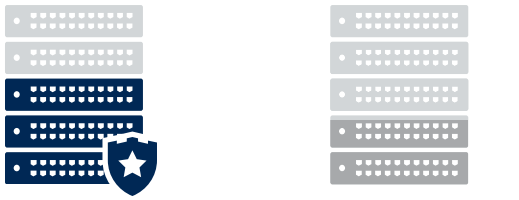
Gli esperti della sicurezza vogliono rendere le proprie aziende più sicure, ma in modo tale da rispondere alla complessità del panorama delle minacce e agli sforzi dei criminali per espandere lo spazio operativo a loro disposizione. Molte aziende si affidano a una molteplicità di soluzioni di fornitori diversi. Questa tattica rende più complessi e confusi gli sforzi di protezione della rete, via via che Internet continua a crescere in termini di velocità, dispositivi connessi e traffico. Per proteggersi efficacemente le aziende devono puntare su semplicità e integrazione.

Opinioni: gli esperti della sicurezza hanno fiducia negli strumenti, ma non sono certi di usarli in modo efficace

La maggior parte degli esperti della sicurezza ritiene di disporre di soluzioni adeguate e di un'infrastruttura di sicurezza aggiornata. Tuttavia, secondo il nostro studio, questa fiducia si accompagna a una dose di incertezza. Non sempre i professionisti intervistati hanno la certezza di disporre del budget e delle competenze umane necessari per sfruttare al meglio le tecnologie disponibili.

Le minacce contro le aziende provengono da tutte le direzioni. Gli autori degli attacchi agiscono in modo rapido e creativo, e sono in grado di aggirare le difese. Nonostante questo ambiente poco rassicurante, la maggior parte degli addetti si dice certa di disporre di un'infrastruttura di sicurezza aggiornata, anche se tale certezza appare lievemente in declino rispetto agli anni scorsi. Nel 2016 il 58% degli intervistati dichiarava di disporre di un'infrastruttura di sicurezza moderna e continuamente aggiornata con le tecnologie più recenti. Il 37% ha affermato di sostituire o aggiornare regolarmente le tecnologie di sicurezza, ma di non disporre degli strumenti più moderni e avanzati (figura 44).

Figura 44 Percentuali di esperti della sicurezza che ritengono che la propria infrastruttura di sicurezza sia aggiornata



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Peraltro, più dei due terzi degli intervistati ritiene molto o estremamente efficaci gli strumenti utilizzati. Il 74%, ad esempio, ritiene gli strumenti molto o estremamente efficaci per bloccare le minacce note, mentre il 71% ritiene gli strumenti efficaci per rilevare le anomalie di rete e proteggere dinamicamente l'ambiente rispetto all'evoluzione delle minacce adattive (figura 45).

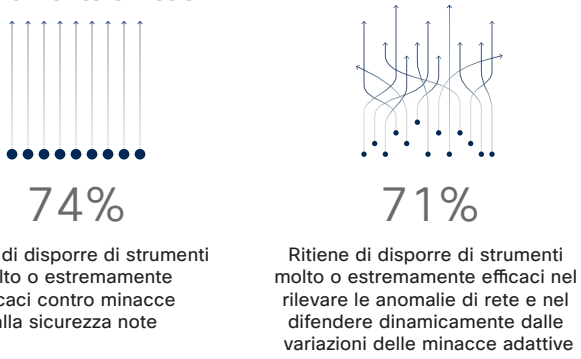
Il problema è che la fiducia negli strumenti non si traduce necessariamente in una protezione efficace. Lo studio evidenzia infatti che i reparti di sicurezza sono impegnati a giostrarsi tra una varietà di strumenti complessi di diversi fornitori e la mancanza di risorse interne competenti. Ciò significa che esiste un problema di percezione, tra quelle che sono le intenzioni e quella che è la realtà. Gli esperti della sicurezza vogliono strumenti semplici ed efficaci, ma non dispongono dell'approccio integrato necessario per concretizzare questa visione.

La sicurezza resta una priorità importante per gli alti dirigenti di molte aziende. E gli esperti stessi ritengono che la sicurezza sia una delle prime priorità per i livelli esecutivi. La sfida, naturalmente, sta nell'ottenere il sostegno dei livelli esecutivi per poter adottare le risorse e le tecnologie effettivamente in grado di influenzare i risultati della sicurezza.

La quota di esperti della sicurezza fermamente convinti che questa rappresenti un'alta priorità per i vertici esecutivi nel 2016 è risultata pari al 59%, poco più bassa del 61% del 2015 e del 63% del 2014 (figura 46). Nel 2016 il 55% degli esperti della sicurezza ha indicato che i ruoli e le responsabilità in quest'area sono chiaramente definiti dal team dirigente; nel 2014 e 2015 la quota era del 58%.

Per riassumere, gli esperti della sicurezza hanno fiducia negli strumenti che utilizzano, e paiono godere dell'attenzione della leadership aziendale per quanto riguarda la risposta alle problematiche in questa area. Tuttavia il grado di fiducia appare lievemente in declino. Gli addetti iniziano a prendere atto degli attacchi andati a segno, e delle difficoltà che sorgono quando si deve gestire una superficie di attacco in continua espansione.

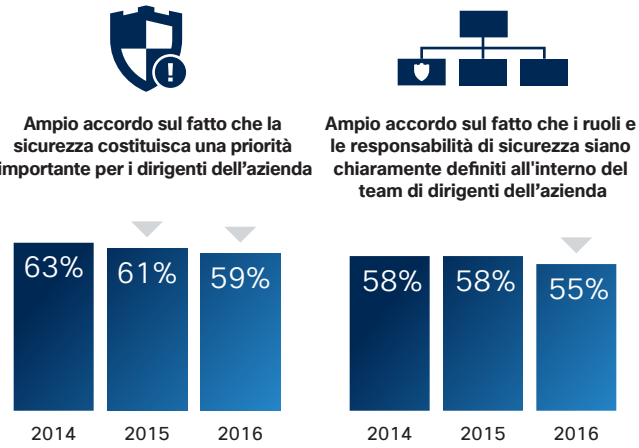
Figura 45 Percentuali di esperti della sicurezza che giudicano diversi strumenti di sicurezza estremamente efficaci



2016 (n=2912)

Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 46 Percentuali di esperti della sicurezza che ritengono che la sicurezza sia di massima priorità a livello dirigenziale, 2014-2016



2014 (n=1738), 2015 (n=2432), 2016 (n=2912)

Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

CONDIVIDI

Limiti: tempo, risorse qualificate e fondi incidono sulla capacità di rispondere alle minacce

Se gli esperti della sicurezza appaiono relativamente certi di disporre degli strumenti necessari per rilevare le minacce e mitigare i danni, essi tuttavia riconoscono che il raggiungimento dei loro obiettivi è ostacolato da alcuni vincoli strutturali. I limiti di budget rappresentano una difficoltà perenne. Tuttavia altri fattori che limitano la protezione efficace rimandano al problema di semplificare e automatizzare la sicurezza.

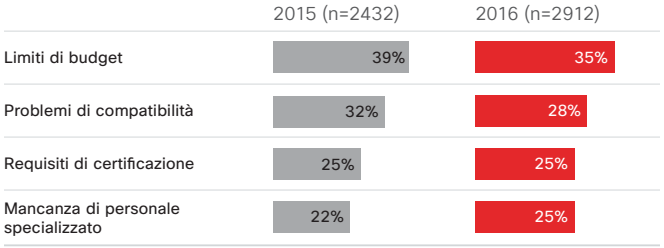
Nel 2016 il 35% degli esperti di sicurezza ha affermato che il maggiore ostacolo all'adozione di processi e tecnologie avanzate in quest'area è stato il budget (in lieve calo rispetto al 39% che vedeva nel budget il primo ostacolo nel 2015), come illustrato alla **figura 47**. Come nel 2015, il secondo ostacolo più comune è stato individuato nei problemi di compatibilità con i sistemi legacy: nel 2016 secondo il 28% degli intervistati, contro il 32% del 2015.

I fondi rappresentano solo una parte della questione. I problemi di compatibilità, per esempio, rinviano al problema dei sistemi disconnessi che non si possono integrare. E la questione della mancanza di risorse qualificate rimanda al fatto che anche quando si dispone degli strumenti, non si hanno le competenze necessarie per comprendere cosa accade realmente nell'ambiente di sicurezza.

La difficoltà di reperire talenti rappresenta una preoccupazione, se si considerano le competenze e le capacità decisionali necessarie per contrastare gli attacchi mirati e la continua trasformazione delle tattiche degli hacker. Un team di sicurezza IT esperto e ben costituito, dotato degli strumenti giusti, consente di far lavorare in sinergia tecnologie e policy, per ottenere risultati di sicurezza migliori.

Il numero medio di esperti della sicurezza nelle aziende intervistate è pari a 33 elementi, rispetto ai 25 del 2015. Nel 2016 il 19% delle aziende utilizzava da 50 a 99 esperti dedicati, il 9% da 100 a 199, e il 12% 200 o più (**figura 48**).

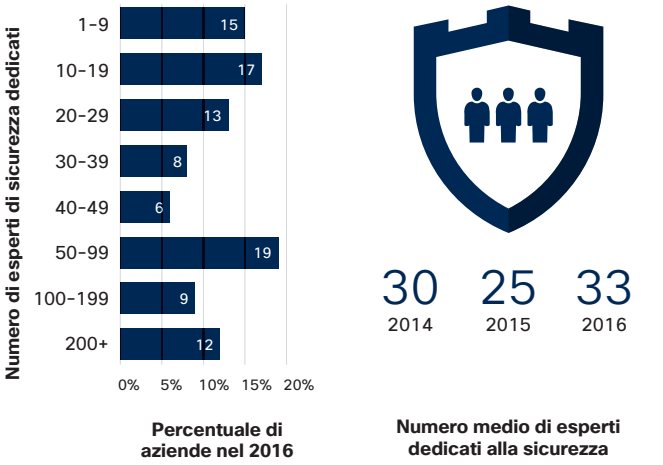
Figura 47 Maggiori ostacoli alla sicurezza



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

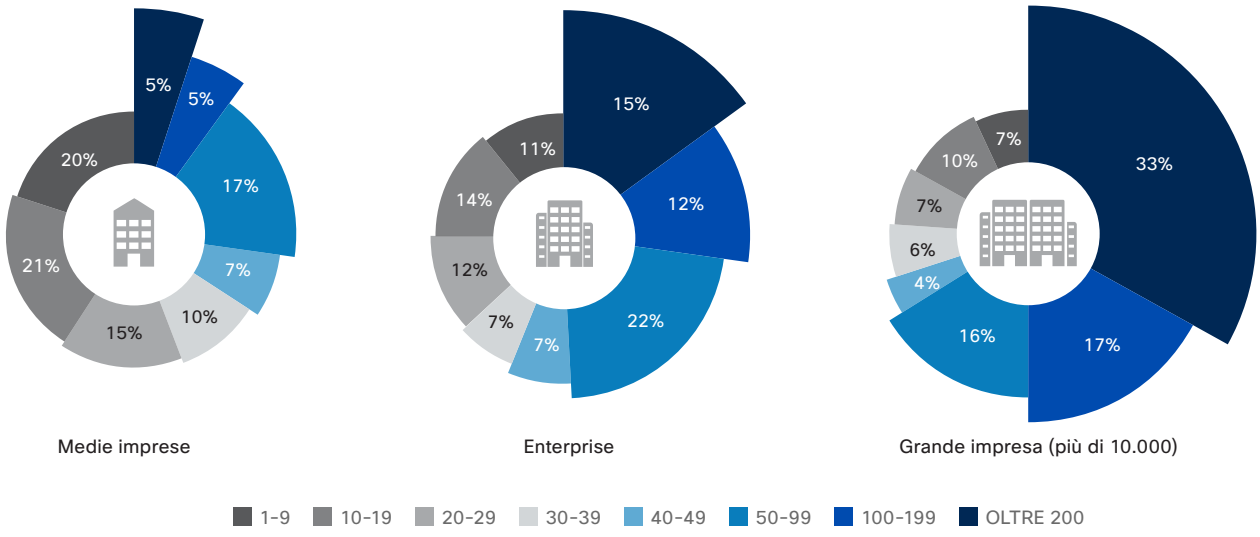
CONDIVIDI

Figura 48 Numero di esperti della sicurezza assunti dalle aziende



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 49 Numero di esperti della sicurezza in base alle dimensioni dell'azienda



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

CONDIVIDI

Il numero di esperti della sicurezza varia a seconda delle dimensioni dell'azienda. Come illustrato nella figura 49, il 33% delle grandi aziende con più di 10.000 dipendenti aveva almeno 200 addetti.

Quali che siano i limiti, è necessario che gli esperti della sicurezza si pongano una serie di domande molto concrete sulle barriere che ostacolano la capacità di fronteggiare le minacce in ingresso.

Per esempio, per quanto riguarda il budget, qual è la somma effettivamente sufficiente? Come hanno spiegato gli intervistati, i team di sicurezza devono fare a gara con molte altre priorità aziendali, perfino all'interno della stessa organizzazione IT. E quando non riescono a ottenere fondi per aggiungere strumenti, devono per forza sfruttare maggiormente il budget disponibile. L'automazione, per esempio, permette di bilanciare la disponibilità limitata di personale.

Le stesse domande andranno fatte anche riguardo il problema della compatibilità tra hardware e software. Via via che i problemi di compatibilità si moltiplicano, quante diverse versioni del software e dell'hardware è necessario gestire (posto che la maggior parte di queste probabilmente non funziona in modo efficace)? E come faranno i team di sicurezza a gestire le diverse esigenze in fatto di certificazioni?

Esternalizzazione e cloud consentono di sfruttare meglio i budget

Molti esperti della sicurezza che hanno partecipato allo studio comparativo hanno indicato di non avere abbastanza fondi per acquistare soluzioni di sicurezza. Sono riusciti a rientrare nel budget esternalizzando alcune attività o utilizzando le soluzioni cloud. Si sono anche affidati all'automazione.

A parte questi limiti, gli esperti della sicurezza oggi sembrano dare un po' meno importanza anche all'operazionalizzazione della sicurezza stessa. Questa tendenza potrebbe far temere che gli esperti stiano implementando infrastrutture di sicurezza meno che ottimali. I segnali di una diminuita concentrazione sull'operazionalizzazione possono indicare che l'azienda non è preparata per difendersi da un panorama di minacce in espansione.

Per fare un esempio, nel 2016 il 53% degli intervistati ha affermato di condividere pienamente la necessità di rivedere e migliorare le procedure di sicurezza in modo regolare, formale e strategico; nel 2014 e 2015 questa quota ammontava al 56%. Analogamente, nel 2016 il 53% degli intervistati ha dichiarato di essere fermamente convinto di aver proceduto ad analizzare in modo regolare e sistematico gli incidenti di sicurezza, contro il 55% del 2014 e il 56% del 2015 (figura 50).

Se gli esperti della sicurezza scivolano sui loro stessi obiettivi di operativizzazione, non può sorprendere che non riescano a implementare efficacemente gli strumenti di cui dispongono, figuriamoci aggiungerne di nuovi. Se gli intervistati, come hanno sostenuto loro stessi, non riescono a utilizzare le tecnologie di cui dispongono già, allora occorrono strumenti più semplici e razionali capaci di automatizzare i processi di sicurezza. Questi strumenti peraltro devono fornire una visione olistica di ciò che accade nell'ambiente di rete.

La mancata integrazione della sicurezza può aprire falle in termini di tempo e di spazio: falle che i criminali possono utilizzare per lanciare attacchi. Di fronte alla tendenza degli addetti ai lavori a giostrarsi tra più soluzioni e piattaforme di fornitori diversi, risulta più difficile mettere insieme una difesa priva di discontinuità. Come si vede nella figura 51, la maggior parte delle aziende nel proprio ambiente utilizza più di cinque fornitori e più di cinque prodotti di sicurezza. Il 55% degli esperti della sicurezza utilizza come minimo sei fornitori; il 45% da uno a cinque fornitori; e il 65% sei o più prodotti.

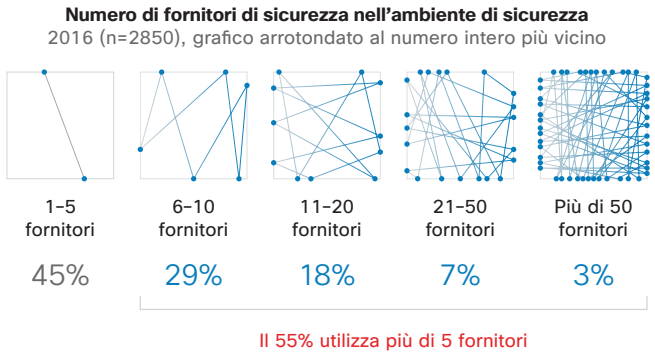
Scaricare il grafico del 2017 al link seguente: **www.cisco.com/go/acr2017graphics**

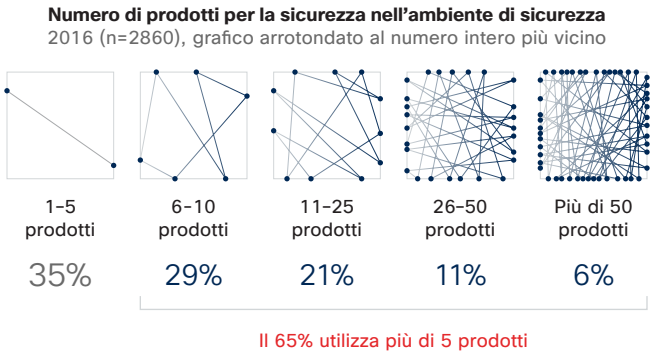
Figura 50 Percentuali di intervistati che si dichiarano decisamente d'accordo con le affermazioni sulla gestione operativa della sicurezza

2014 (n=1738), 2015 (n=2432), 2016 (n=2912)

Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

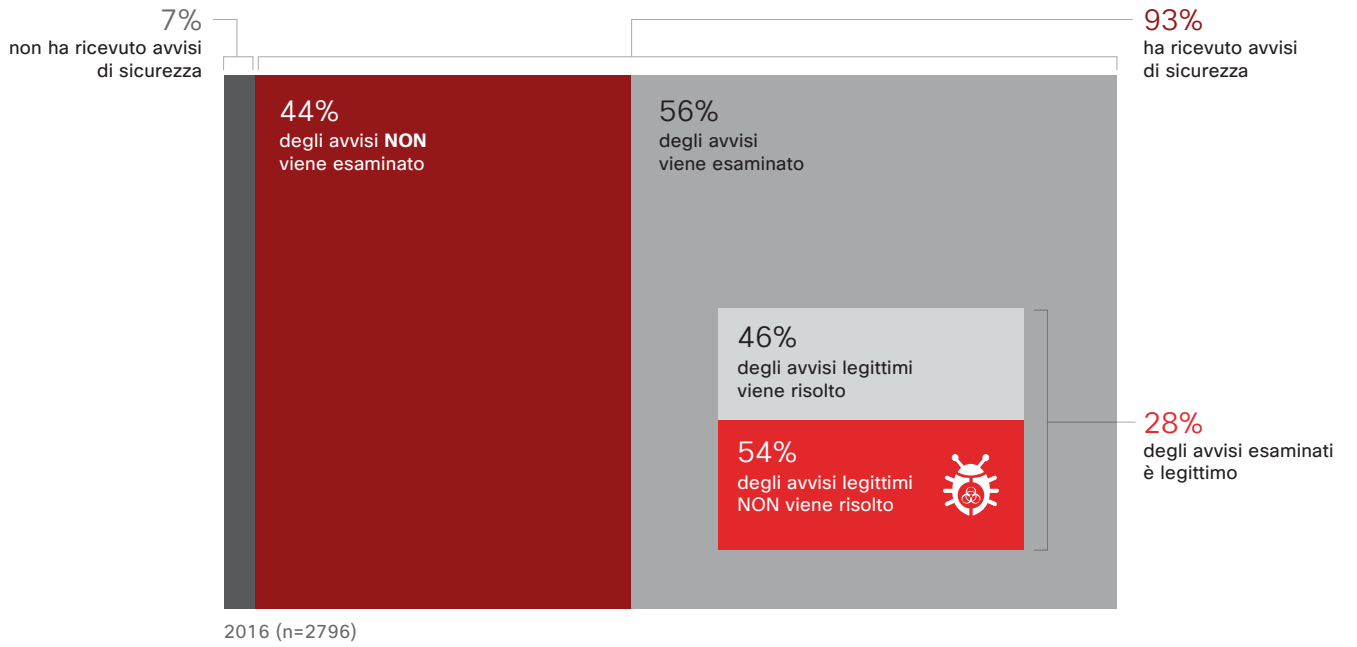
Figura 51 Numero di fornitori e prodotti di sicurezza utilizzati dalle aziende





Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 52 Percentuali di avvisi di sicurezza che non vengono analizzati o corretti



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Se gli obiettivi di operazionalizzazione sfuggono, se gli strumenti non vengono utilizzati al massimo della loro efficacia e se il personale non è valido, la sicurezza non può che vacillare. Il team si vede costretto a rinunciare all'investigazione degli avvisi perché non dispone degli addetti, degli strumenti o delle soluzioni automatizzate per stabilire quali sono critici e come mai si sono verificati.

Probabilmente a causa di diversi fattori, quale la mancanza di un sistema di difesa integrato e di tempo del personale, le aziende riescono a condurre indagini su poco più della metà degli avvisi di sicurezza ricevuti in un dato giorno. Come illustrato nella **figura 52**, il 56% degli avvisi è oggetto di indagini, e il 44% no; tra gli avvisi che vengono indagati, il 28% è giudicato come legittimo. Il 46% degli avvisi legittimi viene quindi corretto.

Per riportare il problema in termini più concreti, ciò significa che se in un giorno un'azienda registra 5000 avvisi:

- 2800 avvisi (56%) vengono indagati, mentre 2200 (44%) no
- Tra gli avvisi investigati, 784 (28%) risultano legittimi, 2016 (72%) no
- Tra gli avvisi legittimi, 360 (46%) vengono risolti, 424 (54%) no

Il fatto che quasi la metà degli avvisi non sia sottoposto a indagini dovrebbe sollevare inquietudini. Da cosa è costituito il gruppo di avvisi che non vengono risolti: si tratta di minacce di basso livello che potrebbero appena distribuire spam, o potrebbero condurre a un attacco ransomware o alla paralisi di una rete? Per poter indagare e comprendere una quota più grande delle minacce che articolano il panorama, le aziende devono adottare l'automazione e soluzioni adeguatamente integrate. L'automazione consente di sfruttare di più e meglio le risorse e di alleggerire il team dalle attività di rilevamento e indagine.

L'impossibilità di visionare un numero così elevato di avvisi solleva dubbi riguardo l'impatto che questi hanno sul successo complessivo dell'azienda. Cosa potrebbero comportare questi avvisi non indagati in termini di produttività, soddisfazione dei clienti e fiducia nell'azienda? Come indicato dagli intervistati, le interruzioni o violazioni della sicurezza di rete, per quanto minime, possono avere effetti a lungo termine sugli utili. Anche quando le perdite sono relativamente secondarie e i sistemi colpiti facili da identificare e isolare, le violazioni restano comunque significative agli occhi dei responsabili della sicurezza, per via dello stress che comportano per l'azienda.

Lo stress può avere una molteplicità di effetti sull'azienda. I team di sicurezza sono costretti a sacrificare del tempo per gestire gli errori di rete che si verificano dopo una violazione. Circa la metà di queste interruzioni è durata per ben 8 ore. Il 45% delle interruzioni è durato da 1 a 8 ore (figura 53); il 15% da 9 a 16 ore; e l'11% da 17 a 24 ore. Il 41% di queste interruzioni ha interessato tra l'11 e il 30% dei sistemi aziendali.

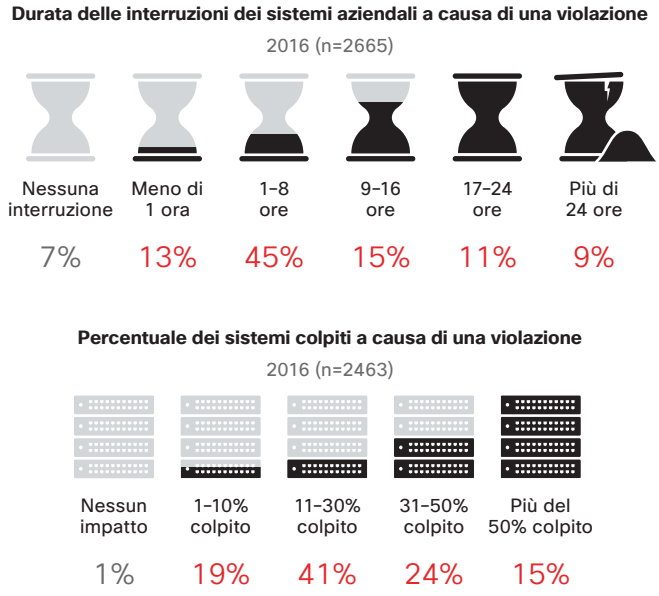
Risultato: un maggior numero di aziende subisce perdite in conseguenza di violazioni

Gli effetti delle violazioni non si limitano alle interruzioni. Le violazioni comportano anche una perdita di denaro, tempo e danni alla reputazione. I team di sicurezza che credono di riuscire a evitare questo rischio ignorano la realtà dei dati. Come dimostra il nostro studio, quasi la metà delle aziende, in conseguenza di una violazione della sicurezza, ha dovuto rendere conto pubblicamente del suo operato. Considerata la varietà di abilità e tattiche messe in campo degli autori degli attacchi, la domanda da farsi non è se possa verificarsi una violazione, ma quando.

Come mostra lo studio comparativo, quando le violazioni si verificano, gli esperti della sicurezza sono bruscamente riportati alla realtà. Spesso cambiano strategie di sicurezza o rafforzano le difese. Le aziende che non hanno ancora subito una violazione della rete potrebbero pensare di essere riuscite a sfuggire. Ma questa fiducia probabilmente è mal riposta.

Il 49% degli esperti della sicurezza intervistati ha risposto che l'azienda si è trovata a dover rendere conto pubblicamente di una violazione della sicurezza. In queste aziende, nel 49% dei casi la violazione è stata rivelata volontariamente, mentre nel 31% questa è stata denunciata da terzi (figura 54). In altre parole, quasi un terzo delle aziende intervistate è stato costretto a fronteggiare la divulgazione involontaria di una violazione. È evidente che l'epoca in cui una violazione poteva essere gestita con discrezione è finita da un pezzo. Ormai ci sono troppe autorità normative, troppi mezzi di comunicazione e troppi utenti di social media pronti a divulgare la notizia.

Figura 53 Durata e dimensioni delle interruzioni causate da violazioni della sicurezza



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 54 Percentuale di aziende che hanno subito una violazione di dominio pubblico

Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 55 Funzioni maggiormente a rischio di essere interessate da una violazione di dominio pubblico

Fonte: Cisco Security Research

Il danno per l'azienda va molto al di là dello spreco di tempo necessario per risolvere una violazione o un guasto. Vi sono conseguenze reali e concrete che le aziende devono cercare in tutti i modi di evitare.

Come mostrato nella figura 55, il 36% degli esperti della sicurezza sostiene che la funzione che più probabilmente risulta interessata sono le operazioni. Ciò significa che i sistemi di base che supportano la produttività, utilizzati in una varietà di settori, dal trasporto alla sanità, al manifatturiero, possono rallentare o persino interrompersi.

L'altra funzione più probabilmente interessata dopo le operazioni sono le finanze (citata dal 30% degli intervistati), seguita da reputazione del marchio e fidelizzazione dei clienti (entrambe al 26%).

Nessuna azienda intenzionata a crescere e a raggiungere il successo desidera che gli effetti delle violazioni della sicurezza possano ripercuotersi sui suoi reparti critici. Nel considerare i risultati del sondaggio, gli addetti alla sicurezza dovrebbero pensare alla propria azienda, e domandarsi: "se subissimo una perdita del genere a causa di una violazione, quali sarebbero le conseguenze per il business, andando avanti?"

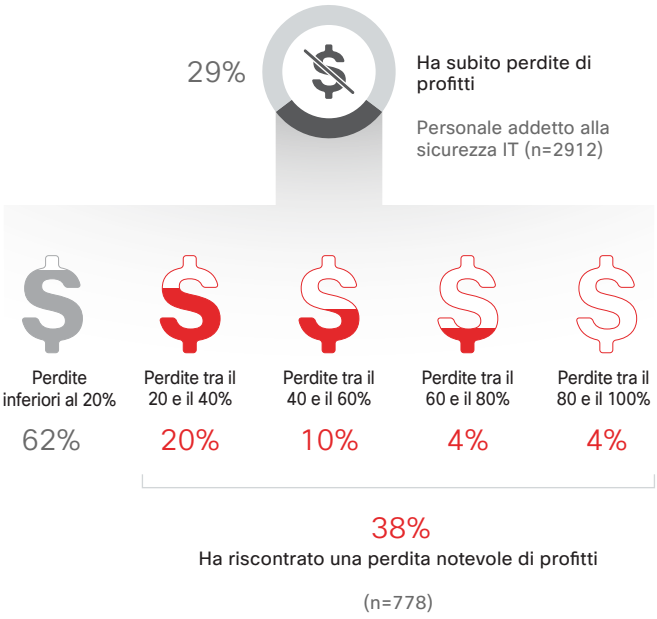
Il costo, in termini di opportunità perse, per le aziende che subiscono attacchi online è esorbitante. Il 23% degli esperti della sicurezza intervistati ha detto che nel 2016 la propria azienda ha perso delle opportunità in conseguenza di attacchi (**figura 56**). Di questo gruppo, il 58% ha detto che le opportunità perse in totale sono state inferiori al 20%; per il 25% sono state pari al 20 – 40% e per il 9% dal 40 al 60%.

Molte aziende sono in grado di quantificare le perdite di fatturato imputabili a pubbliche violazioni. Come illustrato nella **figura 57**, il 29% degli esperti ha indicato che la propria azienda ha subito perdite di fatturato in conseguenza di attacchi. Di questo gruppo, il 38% ritiene che la perdita di fatturato sia stata pari o superiore al 20%.

Gli attacchi online portano come conseguenza anche una riduzione dei clienti. Come mostrato nella **figura 58**, il 22% delle aziende ha risposto di aver perso dei clienti in conseguenza degli attacchi. Di questo gruppo, il 39% riferisce una quota di clienti persi pari almeno al 20%.

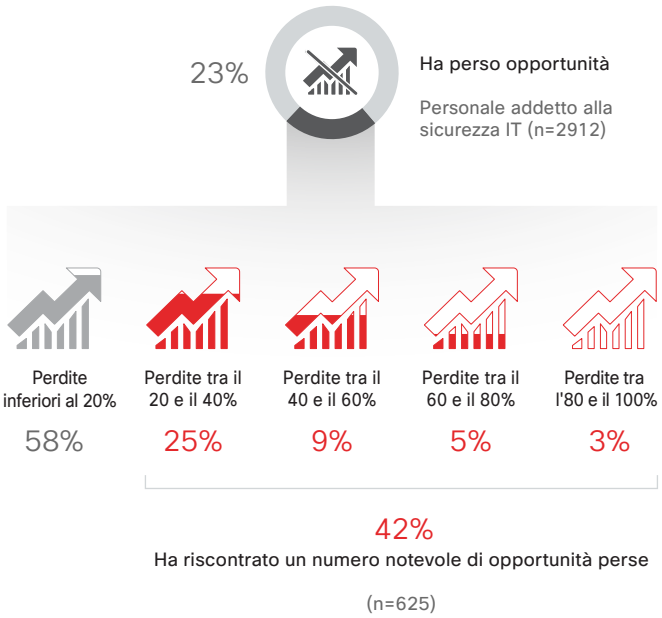
Scaricare il grafico del 2017 al link seguente: **www.cisco.com/go/acr2017graphics**

Figura 57 Percentuale di profitti aziendali persi a causa di un attacco



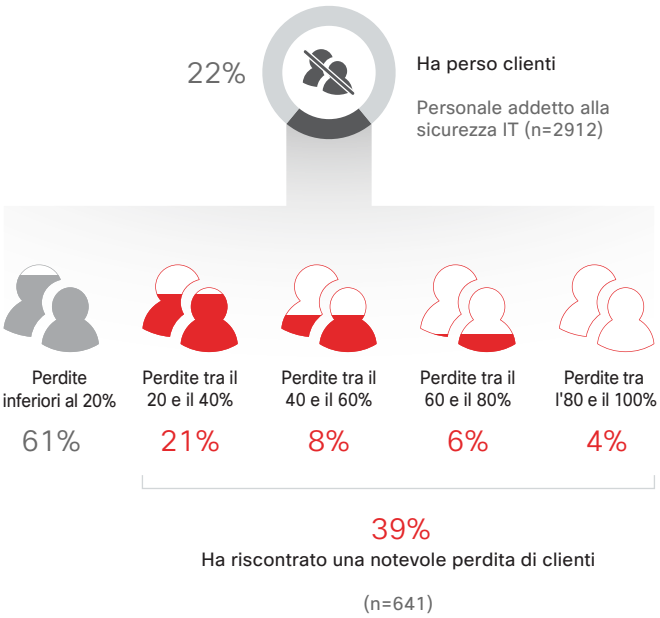
Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 56 Percentuale di opportunità di business perse a causa di un attacco



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 58 Percentuale di clienti persi dalle aziende a causa degli attacchi



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Risultati: un controllo più minuzioso contribuirà al miglioramento della sicurezza

Come mostrano i risultati del sondaggio, l'impatto delle violazioni può essere esteso e duraturo. Quando si parte dal presupposto che l'azienda prima o poi sarà interessata da una violazione, la domanda da farsi è: che succederà, a quel punto? Su cosa deve spostare attenzione e risorse il management, per ridurre le probabilità che si verifichino violazioni?

L'indomani di una violazione rappresenta un'opportunità di apprendimento, un'esperienza che non dovrebbe andare sprecata, per investire in approcci migliori.

Il 90% degli esperti della sicurezza ha segnalato che in conseguenza di una violazione sono stati apportati miglioramenti a livello di tecnologie e processi di difesa dalle minacce, come mostrato nella **figura 59**. Di queste aziende, il 38% segnala di aver risposto separando il team di sicurezza dal reparto IT; il 38% di aver migliorato la formazione dei dipendenti rispetto alla sicurezza e il 37% di essersi maggiormente focalizzata sull'analisi e la mitigazione del rischio.

Figura 59 In che modo le violazioni della sicurezza possono generare dei miglioramenti

Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Le aziende riconoscono che è necessario un esercizio di creatività per superare i limiti in termini di risorse qualificate, problemi di compatibilità tecnologica e budget. Una strategia sta nell'utilizzare risorse qualificate in outsourcing, per rafforzare il budget e avere la possibilità di sfruttare talenti magari non reperibili internamente.

Nel 2016, il 51% degli addetti alla sicurezza ha utilizzato esperti e consulenti esterni, mentre il 45% ha esternalizzato la risposta agli incidenti (**figura 60**). Il 52% ha sostenuto di utilizzare servizi esterni per risparmiare sui costi, mentre il 48% per ottenere informazioni imparziali.

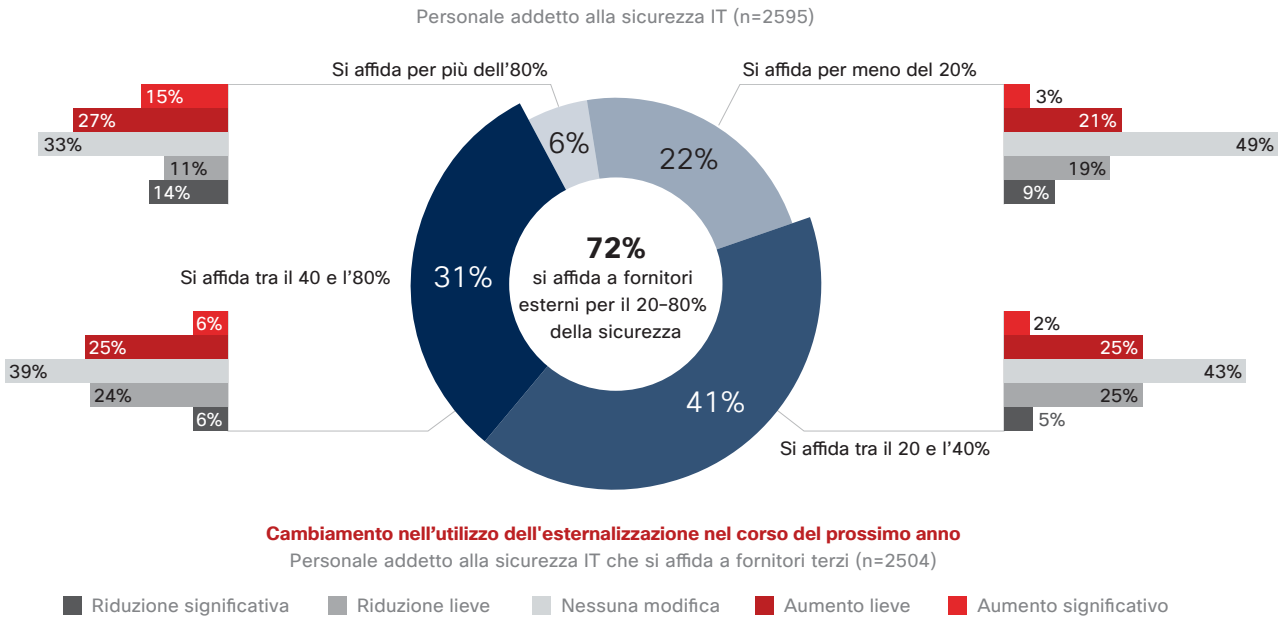
Come per l'outsourcing, le aziende si affidano a fornitori terzi anche per potenziare le strategie di difesa. L'ecosistema della sicurezza offre vari modi per condividere questa responsabilità.

Il 72% degli esperti della sicurezza ha detto di utilizzare fornitori terzi per il 20 – 80% delle risorse di protezione aziendali, come illustrato nella **figura 61**. Le aziende che si affidano più largamente a un aiuto esterno in materia di sicurezza sono anche quelle che tendenzialmente dichiarano che in futuro intensificheranno il ricorso a fornitori terzi.

Figura 60 Le aziende si affidano all'esternalizzazione

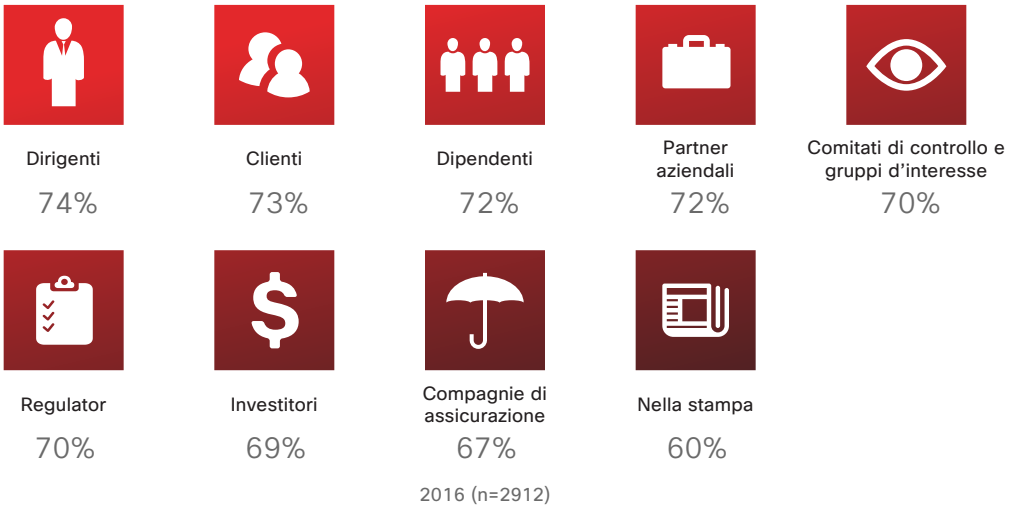
Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 61 Percentuale con cui le aziende si affidano all'esternalizzazione



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 62 Fonti di maggiori controlli

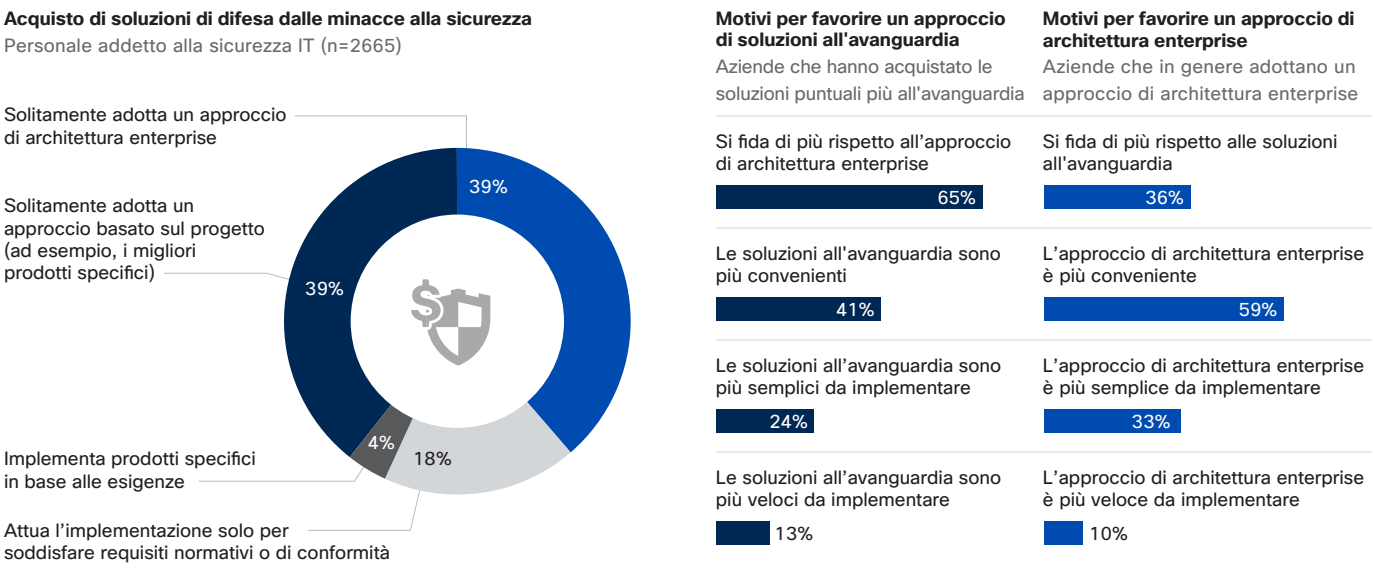


Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Via via che l'azienda adotta misure volte a rafforzare la postura di sicurezza, è prevedibile che gli sforzi fatti inizieranno a richiamare più attenzione. Questo controllo sarà esercitato da soggetti influenti, per cui non può essere ignorato. Il modo di rispondere alle preoccupazioni espresse da tali soggetti può avere un impatto notevole sulla capacità dell'azienda di difendersi.

Il 74% degli esperti della sicurezza si aspetta che questo controllo sarà esercitato dai dirigenti; il 73% da utenti e clienti e il 72% dai dipendenti, come mostrato nella figura 62.

Figura 63 In che modo l'affidabilità e la convenienza influenzano le decisioni di sicurezza



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Affidabilità o costi: che cosa determina gli acquisti di soluzioni di sicurezza?

Gli esperti della sicurezza vogliono soluzioni migliori per proteggere le aziende, ma le loro opinioni su come creare l'ambiente di sicurezza ideale sono differenti. Acquistano soluzioni innovative da diversi fornitori perché confidano nel fatto che queste soluzioni risolveranno molti problemi differenti? Oppure ricorrono a un'architettura integrata, poiché ritengono che questo approccio sia più conveniente? Sebbene ci siano molti fattori da considerare negli investimenti di sicurezza, una maggiore semplicità rappresenta un vantaggio per qualsiasi azienda.

Come mostrato nella **figura 63**, gli esperti della sicurezza sono spaccati in due in riferimento all'affidabilità o ai costi quando si tratta di scegliere tra soluzioni all'avanguardia e architetturali. Il 65% ha dichiarato di preferire soluzioni all'avanguardia perché le ritengono più affidabili rispetto a un approccio architetturale aziendale. D'altro canto, il 59% ha affermato di preferire un approccio architetturale perché lo ritiene più conveniente.

Non si tratta di scegliere tra uno o l'altro. Le aziende hanno bisogno sia di soluzioni all'avanguardia che di sicurezza integrata. Entrambi gli approcci offrono dei vantaggi e semplificano la sicurezza fornendo al tempo stesso strumenti di risposta automatizzata (**figura 63**).

Combinando soluzioni all'avanguardia e un approccio integrato, i team di sicurezza possono intraprendere azioni volte a ottenere una sicurezza meno complessa ma più efficace. L'approccio integrato consente agli esperti della sicurezza di capire che cosa succede in ogni fase del processo di difesa. Un approccio del genere riduce lo spazio operativo degli hacker. È semplice, il che consente ai team di implementare soluzioni scalabili. È aperto, quindi le soluzioni all'avanguardia possono essere adottate in base alle proprie esigenze. Ma è anche automatizzato, consentendo così un rilevamento più rapido.

Riepilogo: risultati emersi dallo studio comparativo

C'è un'enorme differenza tra accumulare gli strumenti di sicurezza e avere davvero la capacità di utilizzarli per ridurre i rischi e limitare lo spazio operativo degli hacker. Gli intervistati dello studio comparativo ritengono di disporre degli strumenti adeguati per contrastare gli hacker. Tuttavia, sono anche consapevoli del fatto che vincoli come la mancanza di personale e una scarsa compatibilità dei prodotti possono rendere strumenti di buona qualità molto meno efficaci di quanto sperato.

I risultati sconcertanti riguardo all'impatto delle violazioni dovrebbero fornire agli esperti della sicurezza molte prove sulla necessità di migliorare i processi e i protocolli. Di fronte a effetti reali e immediati come perdite di fatturato e clienti, le aziende non possono più semplicemente aspettare che le lacune nella sicurezza si risolvano da sole, perché la domanda non è se una violazione avverrà, ma quando.

Un aspetto importante che emerge dallo studio comparativo è che i vincoli che limitano una sicurezza agile ed efficace non verranno mai meno: non ci saranno mai budget e personale a sufficienza rispetto a quanto ritenuto necessario dagli esperti della sicurezza. Se accettiamo questi limiti, allora l'idea di semplificare la sicurezza e di implementare soluzioni automatizzate non fa una piega.

Una sicurezza semplificata si basa anche su soluzioni all'avanguardia e un'architettura integrata. Le aziende necessitano dei vantaggi di entrambi gli approcci.

Settore

Settore

Sicurezza della catena del valore: il successo nel mondo digitale dipende dalla mitigazione del rischio di terze parti

La sicurezza della catena del valore è un elemento essenziale di successo in un'economia connessa. È fondamentale assicurarsi che la giusta sicurezza sia attuata nel posto giusto al momento giusto in tutta la catena del valore: il ciclo di vita end-to-end di hardware, software e servizi.

Le otto fasi della catena del valore sono illustrate nella figura 64.

Nel mondo digitalizzato di oggi c'è una convergenza di information technology e tecnologia operativa. Non basta che le aziende si concentrino solo sulla protezione delle soluzioni, dell'infrastruttura e dei modelli di business interni. Le aziende devono adottare un approccio olistico nei confronti della catena del valore e valutare se ogni singola terza parte coinvolta nel proprio modello di business o nelle soluzioni costituisca un rischio per la sicurezza.

In sintesi è probabile che sia così. Infatti, dalla ricerca condotta dal SANS Institute, emerge che l'80 per cento delle violazioni dei dati deriva da terze parti.[15] Per ridurre i rischi, le aziende devono promuovere una catena del valore in cui l'affidabilità non sia implicita e la sicurezza sia una responsabilità di tutti. Come base di partenza per raggiungere questo obiettivo, le aziende devono:

- Identificare gli attori chiave nell'ecosistema di terze parti e capire che cosa offrano le terze parti stesse
- Sviluppare un'architettura di sicurezza flessibile che possa essere condivisa e implementata tra tutte le terze parti di quell'ecosistema
- Valutare se tali terze parti agiscono nel rispetto dei livelli di tolleranza definiti dall'architettura di sicurezza dell'azienda
- Prestare attenzione ai nuovi rischi per la sicurezza potenzialmente presentati dall'ecosistema a causa dell'aumento della digitalizzazione

Le aziende devono inoltre prendere in considerazione la sicurezza prima di introdurre un nuovo modello di business o una soluzione che implica il coinvolgimento, o che riguarda, l'ecosistema di terze parti. Tutti i vantaggi potenziali di produttività e valore devono essere valutati in relazione ai potenziali rischi, in particolare per quanto concerne la sicurezza e la privacy dei dati.

La consapevolezza dell'importanza della catena del valore sta crescendo sia a livello globale che in settori specifici. La recente legislazione statunitense in merito all'approvvigionamento IT prevede una valutazione della durata di un anno a opera del Dipartimento della Difesa riguardo agli standard tecnologici aperti nelle acquisizioni di Information Technology e cybersecurity.[16] Nel settore energetico, caratterizzato da un'elevata convergenza, la North American Electric Reliability Corporation (NERC) sta attivamente sviluppando nuovi requisiti relativi alla propria catena del valore informatico.[17]

Figura 64 Le fasi della catena del valore

Fonte: Cisco

CONDIVIDI

[15] *Combatting Cyber Risks in the Supply Chain,* SANS Institute, 2015: https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252.
[16] Public Law 114-92 §
[17] La NERC ha ordinato alla United States Federal Energy Regulatory Commission di assumersi questo compito 18 CFR parte 40 [Causa n. RM15-14-002; Ordine n. 829].

Le aziende, insieme alle terze parti, devono rispondere a domande come "In che modo verranno generati i dati e da chi?" e "I dati devono essere estratti digitalmente?" Per ulteriore chiarezza bisogna rispondere a domande come "Chi possiede le risorse digitali che stiamo raccogliendo o creando?" e "Con chi dobbiamo condividere tali informazioni?" Un'altra domanda fondamentale a cui rispondere: "Su chi ricadono responsabilità e obblighi in caso di violazione e di quali responsabilità e obblighi si tratta?"

Questo approccio incentrato sulla catena del valore assicura che le considerazioni sulla sicurezza siano integrate in ogni fase del ciclo di vita delle soluzioni. La giusta architettura, combinata con il rispetto degli standard di sicurezza adeguati, consente di promuovere una sicurezza completa e di garantire l'affidabilità in ogni fase della catena del valore.

Aggiornamento geopolitico: crittografia, affidabilità e una richiesta di trasparenza

Nei precedenti report sulla cybersecurity, gli esperti di geopolitica Cisco hanno esaminato l'incertezza che caratterizza il panorama della governance di Internet, i diritti dell'individuo rispetto ai diritti dello stato e le modalità in cui i governi e le aziende private possono affrontare il dilemma della protezione dei dati. Un elemento che viene discusso trasversalmente in questi ambiti è la crittografia. Riteniamo che nel prossimo futuro la crittografia continuerà a permeare, forse anche a dominare, il dibattito sulla cybersecurity.

La proliferazione delle leggi nazionali e locali sulla privacy dei dati hanno creato difficoltà a fornitori e utenti che tentano di capire tali leggi. In questo ambiente incerto, sono emersi problemi come la sovranità e la localizzazione dei dati, il che ha contribuito a promuovere la crescita del cloud computing e dell'archiviazione dei dati localizzati mentre le aziende cercano una soluzione creativa per rispettare le complesse normative sulla privacy che sono in continua evoluzione.[18]

Allo stesso tempo, il crescente numero di violazioni dei dati e le minacce persistenti avanzate, oltre alla divulgazione di attacchi hacker commissionati dagli stati nazionali, inclusi quelli condotti durante eventi di alto profilo come le elezioni negli Stati Uniti, rendono gli utenti ancora meno fiduciosi nel fatto che i propri dati sensibili e la propria privacy siano protetti.

I governi dell'era post-Snowden puntano sempre più a regolare le comunicazioni digitali e di accedere ai dati a seconda delle necessità. Tuttavia, la richiesta di privacy da parte degli utenti è altrettanto fervida. Eventi come il recente scontro tra Apple e l'FBI su un iPhone appartenente a un terrorista non hanno di certo tranquillizzato gli utenti in merito al problema della privacy. Quanto meno, ha insegnato a una generazione di utenti digitali, soprattutto negli Stati Uniti, cosa sia la crittografia end-to-end. Molti utenti ora richiedono ai provider di tecnologia la crittografia end-to-end e vogliono anche possedere le chiavi di crittografia.

In questo modo si configura un cambiamento fondamentale nel panorama della cybersecurity come lo abbiamo sempre conosciuto. Le aziende avranno bisogno di progettare i propri ambienti in modo da destreggiarsi con i programmi della concorrenza e rispondervi.

Mentre avviene questo cambiamento, sempre più governi si stanno attribuendo il diritto legale, spesso su ampia scala, di superare o infrangere la crittografia o le misure tecniche di protezione, spesso senza che produttore, provider delle comunicazioni o utente ne siano consapevoli. Ciò crea tensione non solo tra le autorità e le aziende di tecnologia ma anche tra i governi, che non intendo permettere che ai dati dei propri cittadini accedano autorità di paesi terzi. Molti governi raccolgono informazioni sulle vulnerabilità e gli exploit zero-day che scoprono nei software dei fornitori, ma non sempre sono chiari con i vendor sulle informazioni che possiedono, o non le condividono tempestivamente.

Tenere per sé tali informazioni preziose impedisce ai fornitori di migliorare la sicurezza dei propri prodotti e di fornire agli utenti una migliore protezione dalle minacce. Anche se i governi possono avere delle ottime ragioni per mantenere riservata parte dell'intelligence, serve anche una maggiore trasparenza e fiducia nel panorama globale della cybersecurity. Quindi i governi dovrebbero valutare con franchezza le attuali politiche relative alla non divulgazione degli exploit zero-day. Dovrebbero partire dal presupposto che la condivisione delle informazioni con i fornitori può soltanto portare a un ambiente digitale molto più sicuro per tutti.

[18] Per ulteriori informazioni su questo argomento, vedere "Data Localization Takes Off as Regulation Uncertainty Continues", di Stephen Dockery, 6 giugno 2016, *The Wall Street Journal*: http://blogs.wsj.com/riskandcompliance/2016/06/06/data-localization-takes-off-as-regulation-uncertainty-continues/.

Crittografia ad alta velocità: una soluzione scalabile per proteggere i dati in transito

Come spiegato nella sezione geopolitica a pagina 65, la crittografia end-to-end rimarrà un argomento di grande dibattito ed è destinata a suscitare costernazione tra governi e industria nel prossimo futuro. Tuttavia, a prescindere dalle tensioni che possono derivare da questo problema, gli utenti richiedono sempre più la crittografia dei dati end-to-end con chiavi gestite dai clienti stessi.

Gli esperti di geopolitica Cisco prevedono che molto probabilmente alcuni flussi e pool di dati saranno crittografati. ma la gestione delle chiavi rimarrà ad appannaggio dei fornitori, quantomeno a breve termine, in particolare nei modelli di business basati sulla pubblicità. In altre aree, però, in mancanza di normative vincolanti, si assisterà con tutta probabilità a un uso sempre maggiore della crittografia end-to-end in cui la gestione delle chiavi è affidata ai clienti.

Nel frattempo, anche le aziende puntano ad assicurarsi un maggiore controllo sulle modalità di protezione dei dati in transito, in particolare quando si spostano a elevata velocità da un data center a un altro. Un tempo questo compito era particolarmente arduo a causa delle limitazioni delle tecnologie legacy e dell'impatto sulle prestazioni di rete. Ad ogni modo, nuovi approcci stanno semplificando questo processo.

Una soluzione è la sicurezza a livello applicativo, in cui le applicazioni vengono modificate per crittografare i dati. L'implementazione di questo tipo di sicurezza può richiedere molte risorse, può essere complessa da attuare e può comportare spese dal punto di vista operativo a seconda del numero di applicazioni utilizzate dall'azienda.

Un altro approccio che acquisisce sempre più forza è quello delle funzionalità di crittografia integrate in una rete o in un servizio cloud per proteggere i dati in transito. Si tratta dell'evoluzione del tradizionale modello gateway VPN, una soluzione che affronta la natura dinamica delle reti e i tassi di trasmissione a elevata velocità del traffico dei data center. Le aziende utilizzano l'efficienza operativa e il contenimento dei costi forniti dalle nuove funzionalità per proteggere i dati provenienti da qualsiasi applicazione che si trova in quell'ambiente mentre questi si spostano ad alta velocità verso un'altra posizione.

Tuttavia, la crittografia basata sulla rete è solo uno degli strumenti per proteggere i dati. Per garantire ogni misura possibile per proteggere i dati mentre sono in transito o archiviati, le aziende devono adottare un approccio olistico nei confronti di questa sfida. Un buon punto di partenza è quello di porre ai fornitori di tecnologia domande basilari ma importanti come:

- In che modo vengono protetti i dati quando sono in transito?
- Come vengono protetti quando sono archiviati?
- Chi può accedere ai dati?
- Dove vengono archiviati i dati?
- Qual è policy per la cancellazione dei dati, quando e se devono essere eliminati?

Di nuovo, queste domande rappresentano solo un punto di partenza per un più ampio dialogo sulla protezione dei dati che deve evolversi per includere una discussione su argomenti come la resilienza e la disponibilità dei dati stessi.

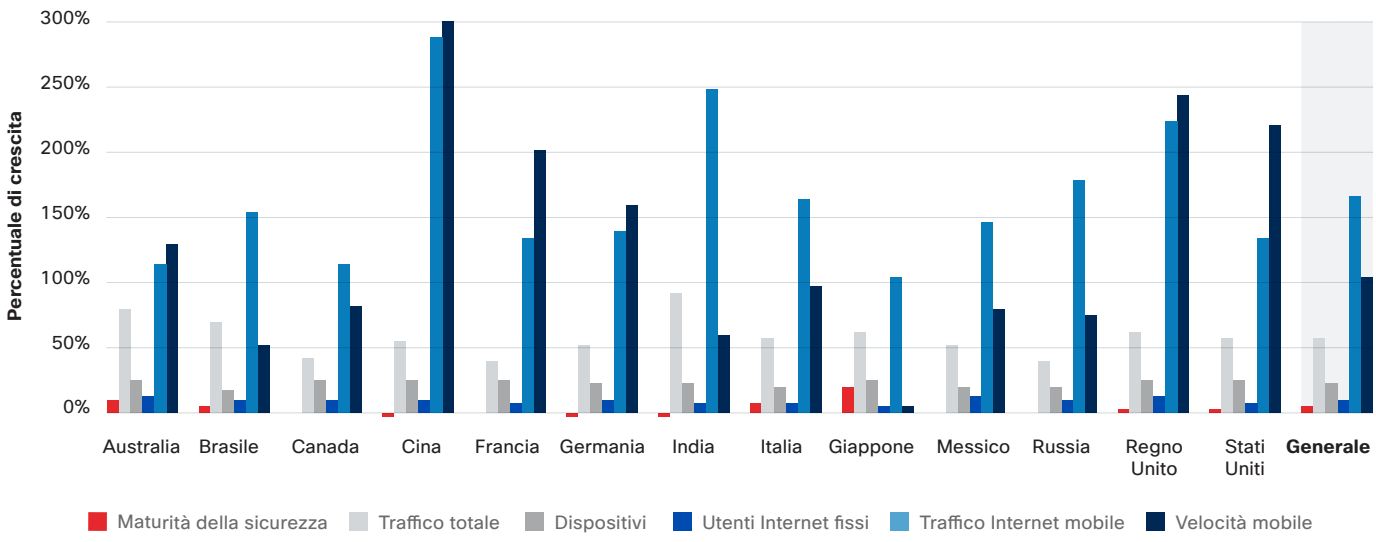
Prestazioni e adozione di rete contro maturità della sicurezza: velocità, traffico e preparazione online non stanno crescendo allo stesso ritmo

Gli addetti alla sicurezza vogliono anticipare i criminali informatici perché inseguirli significa essere in una posizione pericolosa. La preoccupazione, però, è che i primi non riescano a migliorare la propria postura della sicurezza allo stesso ritmo con cui gli hacker riescono a ottenere spazio e tempo per agire. Considerato il ritmo di crescita del traffico Internet mobile e fisso in tutto il mondo, i responsabili della sicurezza sono obbligati a colmare questa crescita con una maggiore maturità della propria infrastruttura di sicurezza.

Il Cisco VNI Forecast esamina il traffico IP globale su base annua, incluso il traffico mobile e Wi-Fi. Le previsioni forniscono proiezioni a cinque anni relative al traffico IP, al numero di utenti Internet e alla quantità di dispositivi personali e connessioni machine-to-machine (M2M) che verranno supportati dalle reti IP. (Visitare questa pagina per ulteriori informazioni sul VNI Forecast). Ad esempio, si stima che entro il 2020 gli smartphone genereranno il 30 per cento del traffico IP totale.

Cisco ha integrato il VNI Forecast con i dati sul livello di maturità della sicurezza, emersi dallo studio comparativo annuale di Cisco delle infrastrutture di sicurezza (vedere pagina 49). Esaminando i tassi di crescita della maturità nei report comparativi del 2015, 2016 e 2017, come mostrato nella **figura 65**, la maturità della sicurezza è insoddisfacente rispetto alla crescita del traffico Internet. Alcuni paesi, come la Cina e la Germania, in effetti mostrano una leggera riduzione della maturità in questo lasso di tempo. La velocità della banda larga, in particolare, sta migliorando e crescendo a un tasso significativamente maggiore rispetto ad altre variabili di networking come mostrato nella **figura 65**. Velocità più elevata e dispositivi più connessi incoraggiano un maggiore aumento del traffico, ma le aziende faticano a supportare con ritmi simili misure e infrastrutture di sicurezza.

Figura 65 Tassi di crescita e di maturità della sicurezza



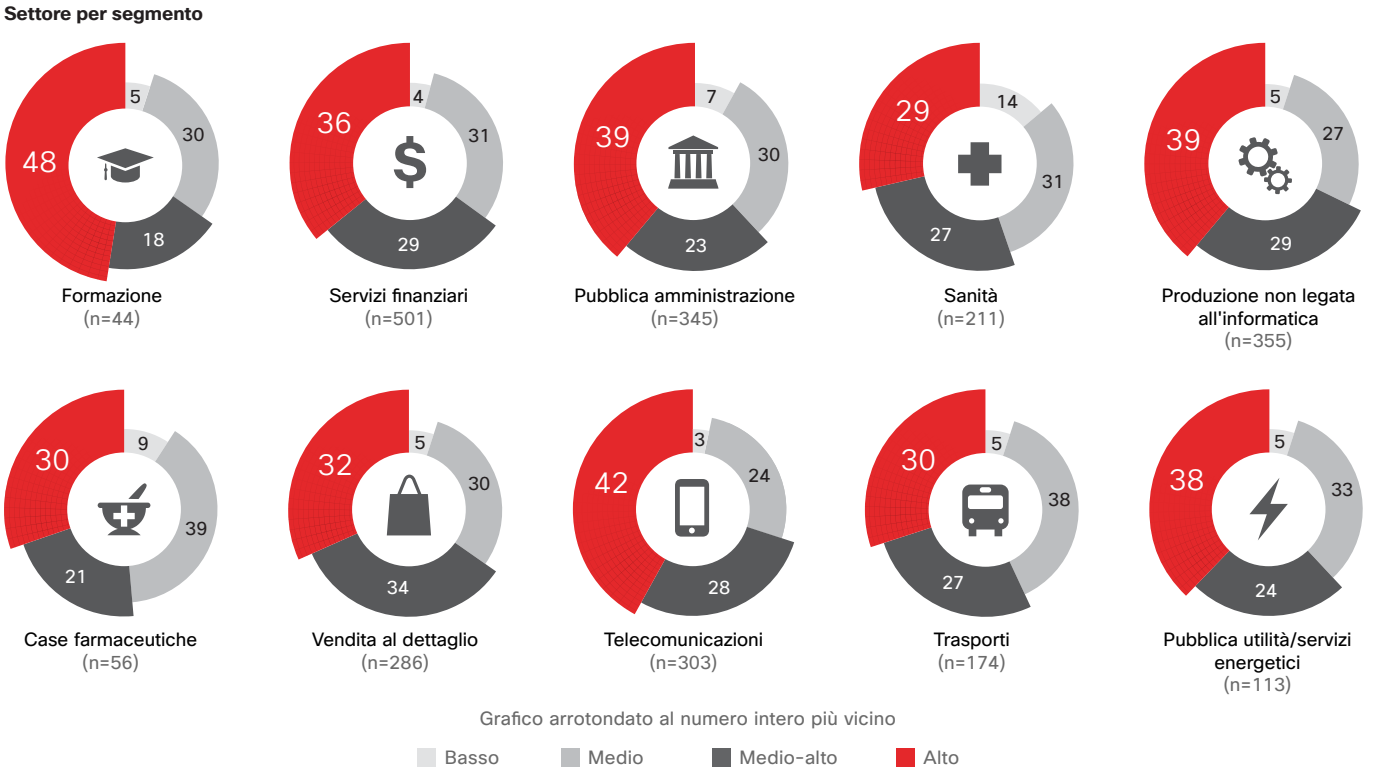
Fonte: Cisco Security Research, Cisco VNI (Visual Networking Index) e Studio comparativo di Cisco delle infrastrutture di sicurezza del 2017

Inoltre certi settori, in termini di maturità della sicurezza, non sono alla pari di altri, come mostrato nella figura 66. In particolare, il settore farmaceutico, della sanità e dei trasporti sono più indietro di altri.

È importante notare che il significativo aumento della velocità mobile è il risultato dell'ampia adozione delle reti 4G e LTE da parte dei provider di telecomunicazioni. Si prevede che, quando verso la fine di questo decennio le implementazioni su larga scala delle reti 5G saranno disponibili, la velocità mobile sarà simile alla velocità delle reti fisse. Secondo l'attuale Mobile VNI Forecast, è probabile che il traffico mobile globale otterrà una fetta maggiore del traffico IP totale quando il 5G verrà adottato diffusamente. Secondo il VNI Forecast, il traffico mobile globale era pari al 5% del traffico IP totale nel 2015 e si prevede che rappresenterà il 16% entro il 2020.

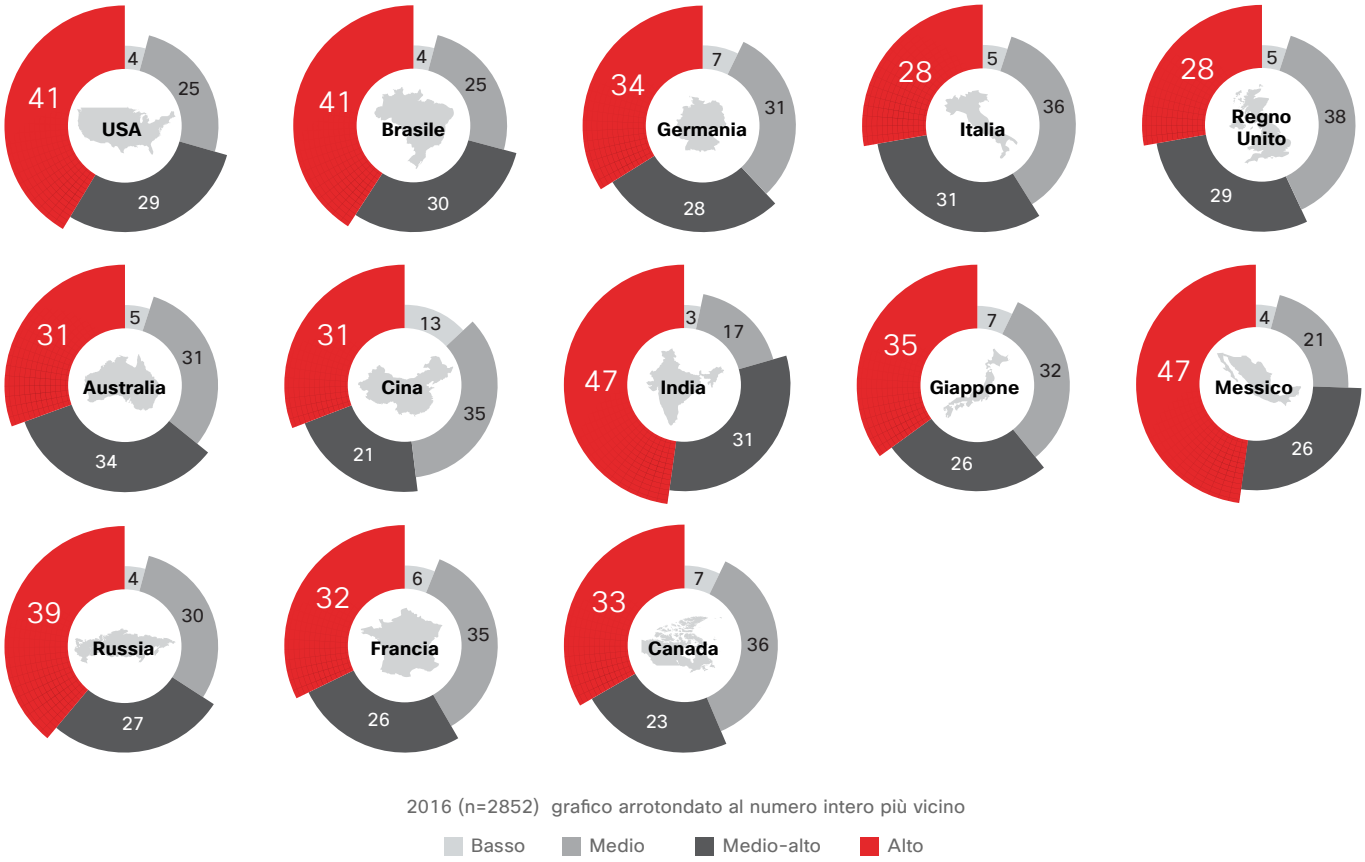
È evidente che le aziende di sicurezza devono incrementare i propri sforzi relativi alla maturità, e devono farlo rapidamente, se vogliono eguagliare l'aumento del traffico Internet, che fa presagire una crescita della superficie di attacco potenziale. Inoltre, le aziende devono rispondere all'incremento nell'utilizzo degli endpoint che non sono fissi o cablati alle reti aziendali. Devono inoltre consentire un utilizzo molto più diffuso di dispositivi personali da cui i dipendenti accedono ai dati aziendali.

Figura 66 Maturità della sicurezza per settori



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 67 Maturità della sicurezza per paese



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

La velocità più elevata non è l'unico fattore che determina la crescita del traffico Internet. IoT sta accelerando il numero di dispositivi collegati a Internet, non solo contribuendo alla crescita del traffico ma anche aumentando le vie che gli hacker potrebbero sfruttare.

Per ulteriori informazioni su Cisco VNI Forecast, visitare il sito Web di Cisco o leggere il post del blog Cisco sulle previsioni VNI annuali dal 2015 al 2020.

Conclusioni

Conclusioni

A fronte di una superficie di attacco in rapida espansione serve un approccio alla sicurezza integrato e interconnesso

Analizzando i dati dello Studio comparativo di Cisco delle infrastrutture di sicurezza (vedere pagina 49), è possibile esaminare i modelli e le decisioni che consentono alle aziende di ridurre i rischi. Si possono quindi individuare gli ambiti in cui devono effettuare investimenti di sicurezza che possono portare a una differenza significativa nell'esposizione al rischio. Abbiamo misurato il rischio analizzando la durata delle violazioni e le percentuali di interruzione dei sistemi (vedere la figura 53 a pagina 55 per quanto riguarda la durata delle violazioni e i sistemi colpiti).

Per comprendere in che modo le aziende si tutelano efficacemente dai rischi, è necessario analizzare i fattori che influenzano la capacità di prevenire, rilevare e mitigare i rischi stessi. (Vedere la figura 68). I fattori devono includere questi elementi:

- **Dirigenza:** i dirigenti di livello più elevato devono dare priorità alla sicurezza. Ciò è fondamentale per la riduzione degli attacchi e la loro prevenzione. Il team dirigenziale deve anche avere delle metriche chiare e prestabilite per valutare l'efficacia di un programma di sicurezza.
- **Policy:** la policy è strettamente legata alla mitigazione del rischio. Controllare i diritti di accesso a reti, sistemi, applicazioni, funzioni e dati influisce sulla capacità di mitigare i danni delle violazioni della sicurezza. Inoltre, le policy volte a garantire una revisione regolare delle procedure di sicurezza consentono di prevenire gli attacchi.
- **Protocolli:** i giusti protocolli possono consentire di prevenire e rilevare violazioni, ma sono anche strettamente legati alla mitigazione dei rischi. In particolare, revisioni periodiche delle attività di connessione in rete, per assicurarsi che le misure di sicurezza funzionino a dovere, sono basilari sia per la prevenzione che per la mitigazione. Nel corso del tempo è altresì utile verificare e migliorare le procedure di sicurezza in maniera sistematica, formale e strategica.
- **Strumenti:** l'applicazione assennata e appropriata degli strumenti è l'aspetto più strettamente legato alla mitigazione dei rischi. Con i giusti strumenti, gli utenti possono rivedere e fornire feedback fondamentali per il rilevamento, la prevenzione e la mitigazione dei rischi.

Figura 68 Fattori determinanti e misure di sicurezza per ridurre al minimo i rischi

Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Scaricare il grafico del 2017 al link seguente: **www.cisco.com/go/acr2017graphics**

Le misure di sicurezza utilizzate dalle aziende (prevenzione, rilevamento e mitigazione) possono essere viste come mezzi che influenzano la capacità di un'azienda di ridurre al minimo i rischi. (Vedere la figura 68).

Queste misure di sicurezza devono includere i seguenti elementi:

- **Prevenzione:** per ridurre al minimo l'impatto delle violazioni della sicurezza, i dipendenti devono segnalare gli errori e i problemi di sicurezza. È inoltre fondamentale che i processi e le procedure di sicurezza siano chiari e ben compresi.
- **Rilevamento:** i migliori metodi di rilevamento per ridurre al minimo l'impatto delle violazioni sono quelli che consentono alle aziende di individuare i punti deboli relativi alla sicurezza prima che diano luogo a una violazione effettiva. A tale scopo, è fondamentale disporre di un sistema efficace per categorizzare le informazioni sulle violazioni.
- **Mitigazione:** processi e procedure ben documentati per rispondere agli incidenti e tenere traccia delle violazioni sono essenziali per un'efficace riduzione delle violazioni. Le aziende hanno anche bisogno di protocolli solidi per gestire la risposta alle situazioni di crisi.

Tutti questi fattori e misure di sicurezza sono interconnessi e interdipendenti. Gli esperti della sicurezza non possono semplicemente scegliere un paio di fattori e una o due misure di sicurezza e pensare di aver risolto il problema della sicurezza. Serve ogni tipo di fattore e ogni misura di sicurezza. I team di sicurezza devono analizzare i propri punti deboli, ad esempio i bassi livelli di supporto da parte dei dirigenti o una mancanza di strumenti per mitigare le violazioni, e stabilire dove effettuare gli investimenti di sicurezza.

L'obiettivo chiave: ridurre lo spazio operativo degli hacker

Ridurre, e idealmente eliminare, il campo d'azione incontrollato a disposizione degli autori degli attacchi oltre a rendere nota la presenza di questi ultimi, devono essere le priorità principali dei responsabili della sicurezza. La realtà è che nessuno può bloccare tutti gli attacchi o proteggere tutto ciò che può e dovrebbe essere protetto. Tuttavia, se ci si focalizza sulla limitazione dello spazio operativo che serve ai criminali informatici affinché le loro campagne siano efficaci e redditizie, si può evitare che raggiungano sistemi e dati critici senza eludere completamente il rilevamento.

In questo report abbiamo categorizzato approcci diversi che gli hacker utilizzano per compromettere e attaccare utenti e sistemi. Le categorie (ricognizione, adescamento, dirottamento e installazione) sono basate sul punto in cui in genere vengono implementati gli attacchi lungo la catena delle fasi dell'attacco. Lo scopo era quello di illustrare come, quando e dove gli hacker sfruttano le vulnerabilità e altri punti deboli per introdursi in un dispositivo o in un sistema, lanciare le campagne e quindi raccogliere i risultati desiderati.

Il nostro suggerimento per gli addetti alla sicurezza è quello di adattare gli approcci alla sicurezza per anticipare i processi di base degli hacker. Ad esempio, per indebolire gli hacker durante la fase di ricognizione, i team di sicurezza devono:

- Raccogliere informazioni sulle ultime minacce e vulnerabilità
- Assicurarsi di controllare l'accesso alle reti
- Limitare l'esposizione dell'azienda in una superficie di attacco in espansione
- Gestire le configurazioni
- Sviluppare prassi e procedure coerenti di risposta di cui si mette al corrente in questo lavoro

Quando vengono scagliate minacce nella fase di adescamento, gli addetti alla sicurezza devono sfruttare ogni strumento del loro arsenale per evitare che si diffondano e peggiorino. È a questo punto che un'architettura di sicurezza integrata diventa fondamentale. Fornirà informazioni sulle minacce in tempo reale nonché rilevamento e difesa automatiche, che sono essenziali per migliorare il rilevamento delle minacce.

Nella fase di installazione, i team di sicurezza devono essere informati sullo stato dell'ambiente quando rispondono alla compromissione e la analizzano. Se quell'ambiente è semplice, aperto e automatizzato e se gli addetti alla sicurezza hanno adottato le altre misure proattive descritte sopra, possono concentrare le proprie risorse ad aiutare l'azienda a rispondere a domande fondamentali come:

- A cosa hanno avuto accesso gli hacker?
- Perché sono stati in grado di arrivarvi?
- Dove sono andati?
- Stanno ancora agendo nella nostra rete?

Le risposte a queste domande consentono ai team di sicurezza non solo di adottare le azioni adeguate per prevenire ulteriori attacchi, ma anche di informare la direzione e il consiglio di amministrazione sulle possibili esposizioni e sulla necessità di divulgarle. A quel punto, l'azienda può iniziare a verificare di disporre dei controlli e delle misure di mitigazione del rischio completi per colmare le lacune di sicurezza, ovvero i punti deboli che hanno fornito lo spazio operativo di cui gli hacker avevano bisogno perché l'attacco andasse a buon fine, e che sono stati identificati durante la compromissione.

Informazioni su Cisco

Cisco fornisce la sicurezza informatica intelligente con una gamma di soluzioni di protezione avanzata tra le più complete del settore e in grado di difendere contro una grande varietà di vettori di attacco. L'approccio alla sicurezza altamente operativo e incentrato sulle minacce adottato da Cisco riduce la complessità e la frammentazione, garantendo al tempo stesso livelli di visibilità superiori, controlli coerenti e una protezione avanzata dalle minacce, prima, durante e dopo l'attacco.

I ricercatori dell'ecosistema Cisco Collective Security Intelligence (CSI) hanno riunito in una singola soluzione le funzioni di analisi delle minacce leader del settore, utilizzando dati telemetrici ottenuti da una vasta gamma di dispositivi, sensori, feed pubblici e privati, oltre che dalla community open source. Ogni giorno vengono elaborati miliardi di richieste Web e milioni di e-mail, campioni di malware e intrusioni nelle reti.

I nostri sofisticati sistemi e infrastrutture utilizzano questi dati telemetrici, aiutando i ricercatori e i sistemi machine-learning a monitorare le minacce in più reti, data center, endpoint, dispositivi mobili, sistemi virtuali, siti Web, e-mail e cloud per identificare le cause profonde e l'ambito delle infezioni. Le informazioni dettagliate così ottenute si traducono in una protezione in tempo reale per i nostri prodotti e servizi, che viene immediatamente fornita ai clienti Cisco di tutto il mondo.

Per ulteriori informazioni sul nostro approccio alla sicurezza incentrato sulle minacce, visitare il sito www.cisco.com/go/security.

Contributi al report annuale di Cisco sulla cybersecurity 2017

CloudLock

CloudLock, un'azienda Cisco, è un fornitore leader di soluzioni Cloud Access Security Broker (CASB) che aiutano le aziende a utilizzare il cloud in modo sicuro. CloudLock offre visibilità e controllo per ambienti Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) e Infrastructure-as-a-Service (IaaS) per tutti gli utenti, i dati e le applicazioni. CloudLock offre intelligence utilizzabile sulla cybersecurity attraverso l'analisi della sicurezza fornita da tutta la community e dal CyberLab, che è guidato da esperti nell'analisi dei dati. Per ulteriori informazioni, visitare https://www.cloudlock.com.

Security and Trust Organization

La Security and Trust Organization di Cisco sottolinea l'impegno dell'azienda nei confronti di due delle questioni più importanti e anche priorità assolute per vertici aziendali e leader mondiali. I principali obiettivi dell'organizzazione includono la protezione dei clienti pubblici e privati di Cisco, l'implementazione e la sicurezza del Cisco Secure Development Lifecycle e dell'impegno di Trustworthy Systems sulla gamma di prodotti e servizi Cisco, oltre alla protezione dell'impresa Cisco dalle minacce nuove ed esistenti. Cisco adotta un approccio olistico per la sicurezza e la fiducia che include persone, policy, processi e tecnologia. La Security and Trust Organization guida l'eccellenza operativa attraverso InfoSec, Trustworthy Engineering, Data Protection and Privacy, Cloud Security, Transparency and Validation e Advanced Security Research and Government. Per ulteriori informazioni, visitare http://trust.cisco.com.

Global Government Affairs

Cisco collabora con le amministrazioni pubbliche a vari livelli per definire le politiche e le normative pubbliche che supportano il settore della tecnologia e le amministrazioni pubbliche stesse nel raggiungimento dei propri obiettivi. Il team Global Government Affairs sviluppa e influenza le politiche e le normative pubbliche a supporto della tecnologia. Collaborando con gli stakeholder del settore e i partner associativi, il team stabilisce rapporti con i dirigenti della pubblica amministrazione per influenzare le politiche che riguardano le attività di Cisco e l'adozione ICT globale, aiutando a definire le decisioni politiche a livello globale, nazionale e locale. Il team Government Affairs è composto da ex funzionari eletti, parlamentari, regolatori, funzionari senior e consulenti della pubblica amministrazione statunitense che aiutano Cisco a promuovere e proteggere l'uso della tecnologia nel mondo.

Cognitive Threat Analytics

Cisco Cognitive Threat Analytics è un servizio basato su cloud che rileva le violazioni, il malware operante all'interno di reti protette e altre minacce alla sicurezza mediante un'analisi statistica dei dati sul traffico di rete. Gestisce le vulnerabilità nelle difese perimetrali identificando i sintomi della diffusione di malware o della violazione dei dati tramite l'analisi comportamentale e il rilevamento delle anomalie. Cisco Cognitive Threat Analytics si basa su modelli statistici avanzati e sull'apprendimento automatizzato per identificare in modo autonomo le nuove minacce, apprendere dal contesto e adattarsi nel tempo.

IntelliShield Team

Il team IntelliShield si occupa di ricerca su vulnerabilità e minacce, di analisi, integrazione e correlazione di dati e informazioni provenienti da tutto il gruppo Cisco Security Research and Operations, oltre che da fonti esterne. Il team produce IntelliShield Security Intelligence Service, che supporta vari prodotti e servizi Cisco.

Talos Security Intelligence and Research Group

Talos è l'organizzazione di intelligence sulle minacce di Cisco, un gruppo esclusivo di esperti della sicurezza dedicati a garantire la massima protezione di clienti, prodotti e servizi Cisco. Talos è composto da ricercatori esperti che si avvalgono di sistemi sofisticati per mettere a punto un sistema di intelligence sulle minacce per i prodotti Cisco, atto a rilevare, analizzare e proteggere i clienti contro le minacce note ed emergenti. Talos ottempera alle norme ufficiali di Snort.org, ClamAV, SenderBase.org e SpamCop ed è il team principale che fornisce le informazioni sulle minacce all'ecosistema Cisco CSI.

Security Research and Operations (SR&O)

Security Research and Operations (SR&O) è responsabile della gestione di vulnerabilità e minacce di tutti i prodotti e servizi Cisco, incluso il team leader di settore Product Security Incident Response Team (PSIRT). SR&O aiuta i clienti a comprendere il panorama delle minacce nel corso di eventi come Cisco Live e Black Hat, nonché tramite la collaborazione con altre organizzazioni di Cisco e del settore. SR&O offre inoltre nuovi servizi come Custom Threat Intelligence (CTI) di Cisco, che è in grado di identificare gli indicatori di compromissione che non sono stati rilevati o mitigati dalle infrastrutture di sicurezza esistenti.

Cisco Visual Networking Index (VNI)

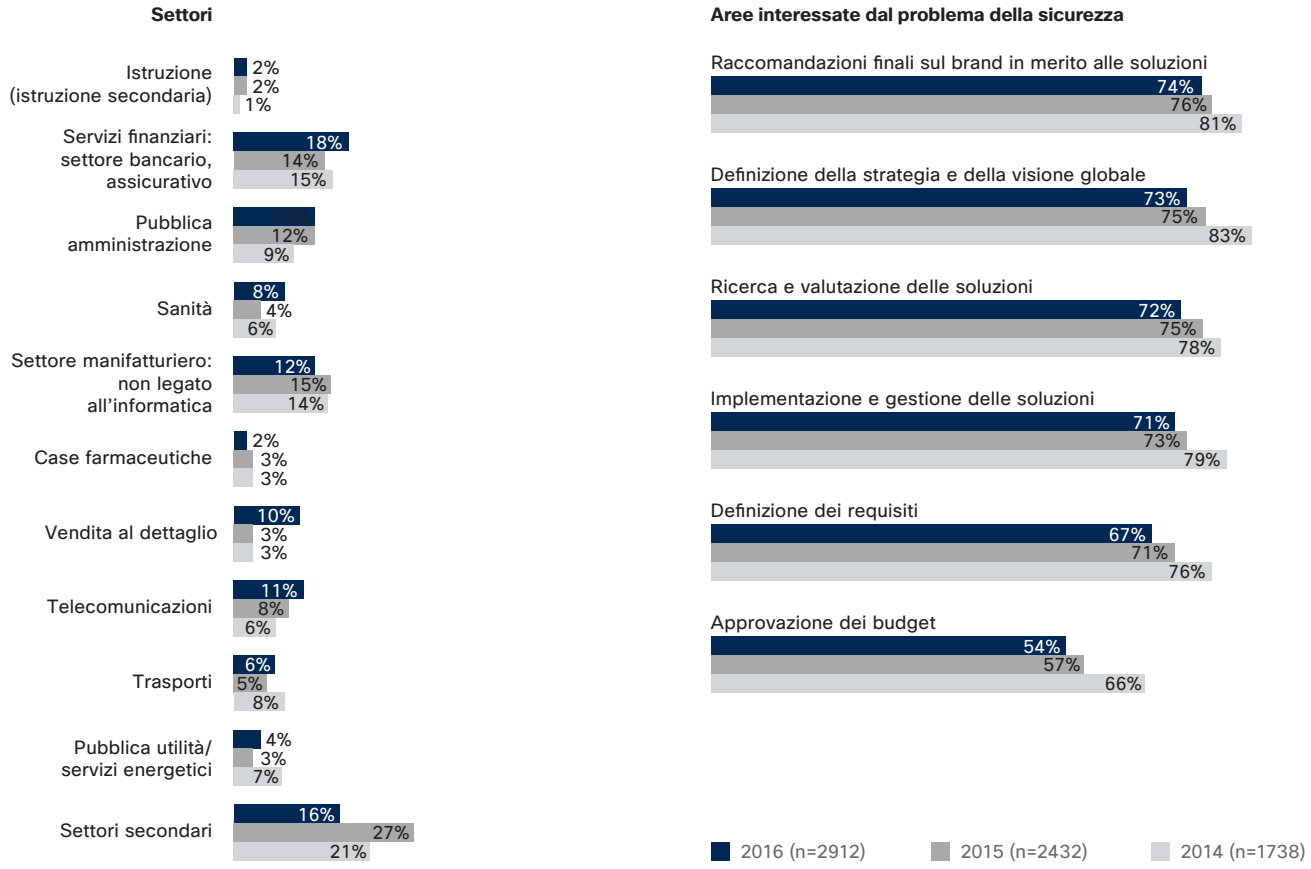
Il Cisco VNI Global IP Traffic Forecast 2015–2020 si basa sulle previsioni di analisti indipendenti e sui dati reali di utilizzo della rete. Su questi dati si basano le stime di Cisco per il traffico IP globale e l'adozione dei servizi. Una descrizione dettagliata della metodologia è contenuta nel report completo. Nei suoi 11 anni di storia, la ricerca Cisco VNI è riuscita a conquistarsi una grande considerazione per quanto concerne le stime sulla crescita di Internet. I governi nazionali, i regulator di rete, i ricercatori accademici, le aziende di telecomunicazioni, i tecnici esperti, gli analisti e la stampa di settore e aziendale si basano sullo studio annuale per pianificare il futuro digitale.

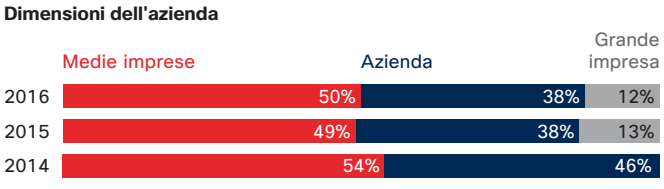
Appendice

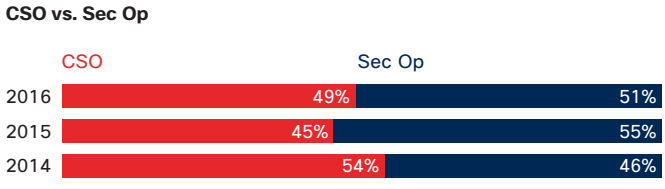
Appendice

Studio comparativo di Cisco delle infrastrutture di sicurezza del 2017

Figura 69 Indagine dello studio comparativo delle infrastrutture di sicurezza







Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 70 Numero di esperti di sicurezza dedicati

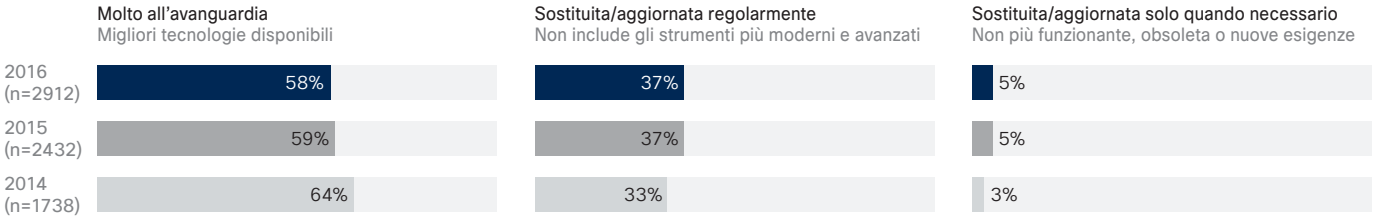
	2014 (n=1738)	2015 (n=2432)	2016 (n=2912)
1-9	18%	17%	15%
10-19	16%	18%	17%
20-29	12%	17%	13%
30-39	8%	9%	8%
40-49	4%	4%	6%
50-99	19%	16%	19%
100-199	9%	9%	9%
200 o più dipendenti	15%	10%	12%
Numero medio di esperti dedicati alla sicurezza	**30**	**25**	**33**

Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Opinioni

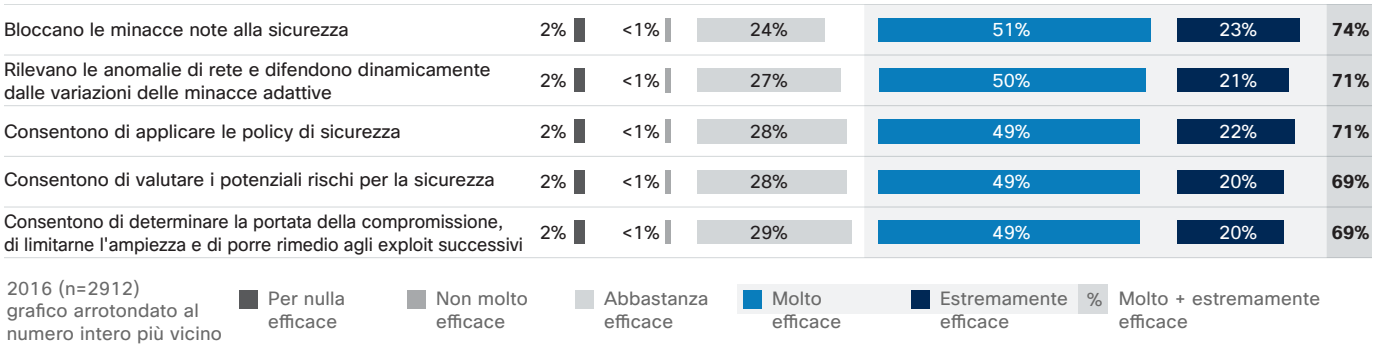
Figura 71 La maggior parte dei professionisti della sicurezza ritiene che la propria infrastruttura di sicurezza sia aggiornata

Come descrivi l'infrastruttura di sicurezza della tua azienda?



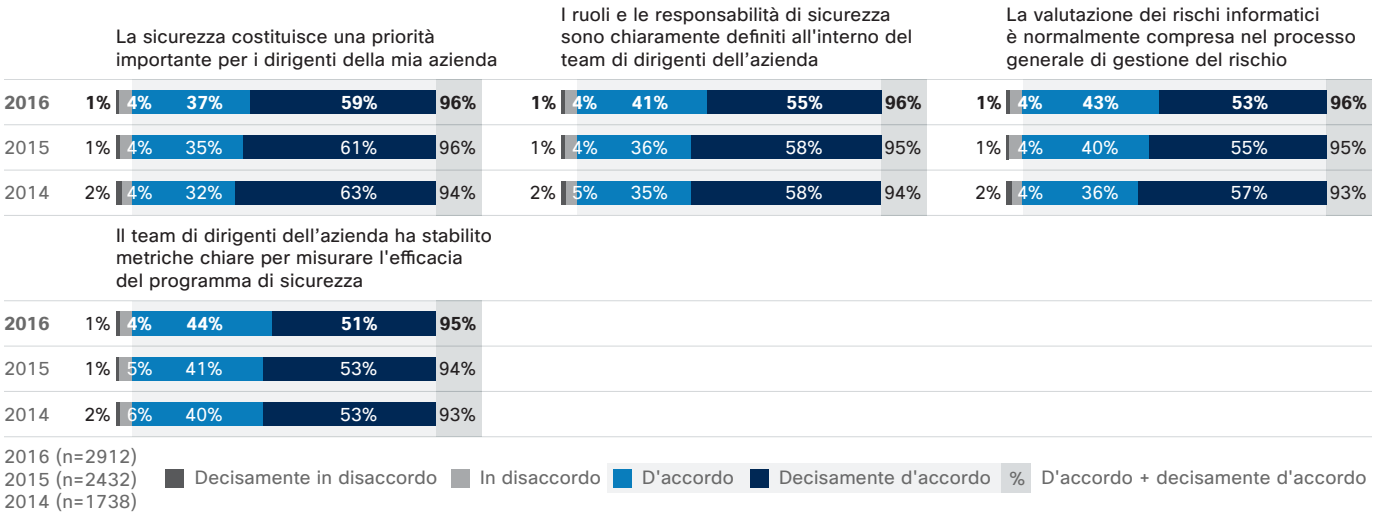
Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 72 Percentuali di esperti della sicurezza che giudicano diversi strumenti di sicurezza estremamente efficaci



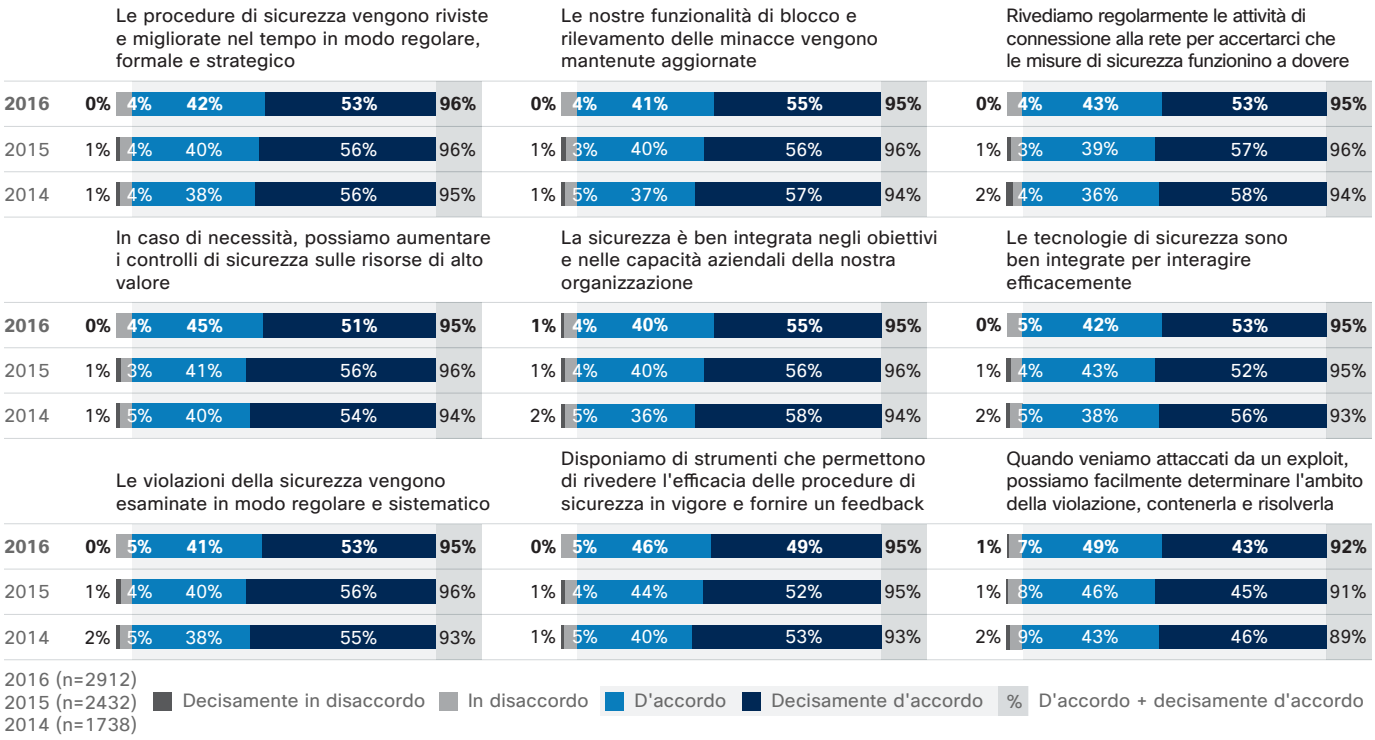
Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 73 Percentuali di professionisti della sicurezza secondo cui la sicurezza è una priorità assoluta a livello dirigenziale



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 74 Percentuali di intervistati che si dichiarano decisamente d'accordo con le affermazioni sulla gestione operativa della sicurezza



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

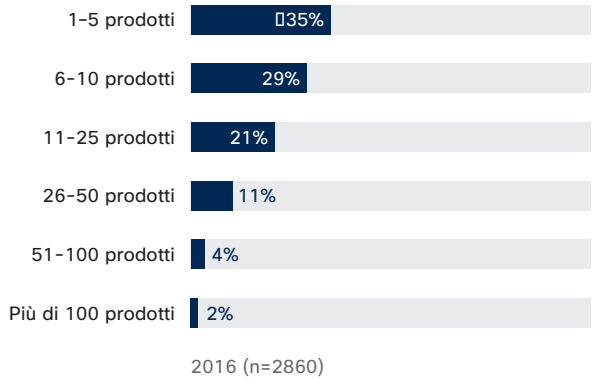
Vincoli

Figura 75 Maggiori ostacoli alla sicurezza

	2015 (n=2432)	2016 (n=2912)
Limiti di budget	39%	35%
Problemi di compatibilità	32%	28%
Requisiti di certificazione	25%	25%
Mancanza di personale specializzato	22%	25%
Conflitti di priorità	24%	24%
Carico di lavoro attuale eccessivo	24%	23%
Mancanza di informazioni	23%	22%
Riluttanza ad acquistare prima della conferma del mercato	22%	22%
Cultura/atteggiamento aziendale	23%	22%
L'azienda non è un bersaglio ambito per gli attacchi	N/D	18%
La sicurezza non è una priorità a livello dirigenziale	N/D	17%

Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 76 Numero di fornitori e prodotti di sicurezza utilizzati dalle aziende



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 77 Numero di fornitori di sicurezza utilizzati in base alle dimensioni dell'azienda

Quanti fornitori di soluzioni di sicurezza (ad esempio marchi, produttori) sono presenti nell'ambiente di sicurezza?	Medie imprese 250-1.000 dipendenti	Aziende 1.000-10.000 dipendenti	Grandi imprese più di 10.000 dipendenti
1-5	46,9%	43,4%	39,9%
6-10	28,4%	30,9%	21,3%
11-20	17,6%	15,8%	23,1%
21-50	5,6%	7,1%	8,7%
Più di 50	1,4%	2,8%	6,9%
Aziende totali	**1435**	**1082**	**333**

Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 78 Numero di prodotti di sicurezza utilizzati in base alle dimensioni dell'azienda

Quanti prodotti per la sicurezza sono presenti nell'ambiente di sicurezza?	Medie imprese 250-1.000 dipendenti	Aziende 1.000-10.000 dipendenti	imprese più di 10.000 dipendenti
1-5	37,9%	32,7%	25,1%
6-10	29,0%	30,1%	22,5%
11-25	19,8%	20,4%	23,7%
26-50	9,6%	10,5%	15,6%
51-100	3,0%	4,3%	7,8%
Più di 100	0,8%	1,9%	5,4%
Aziende totali	**1442**	**1084**	**334**

Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 79 Riduzione su base annua del budget per la sicurezza rientrante nel budget IT

Il budget per la sicurezza informatica fa parte del budget IT? (Personale del reparto IT)	2014 (n=1673)	2015 (n=2374)	2016 (n=2828)
Completamente interno a IT	61%	58%	55%
Parzialmente interno a IT	33%	33%	36%
Completamente separato	6%	9%	9%

Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

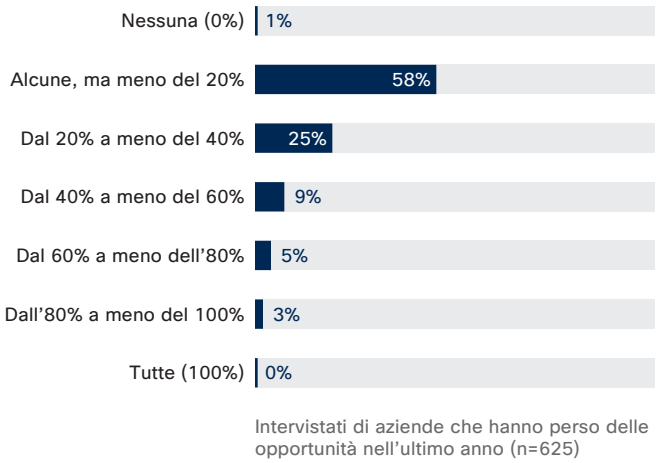
Figura 80 Riduzione su base annua della spesa per la sicurezza in proporzione al budget IT

Budget IT speso per la sicurezza come funzione	2014 (n=1673)	2015 (n=2374)	2016 (n=2828)
0%	7%	9%	10%
1-5%	4%	3%	4%
6-10%	12%	11%	16%
11-15%	23%	23%	27%
16-25%	29%	31%	26%
26%-50%	21%	19%	15%
Almeno il 51%	5%	4%	2%

Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

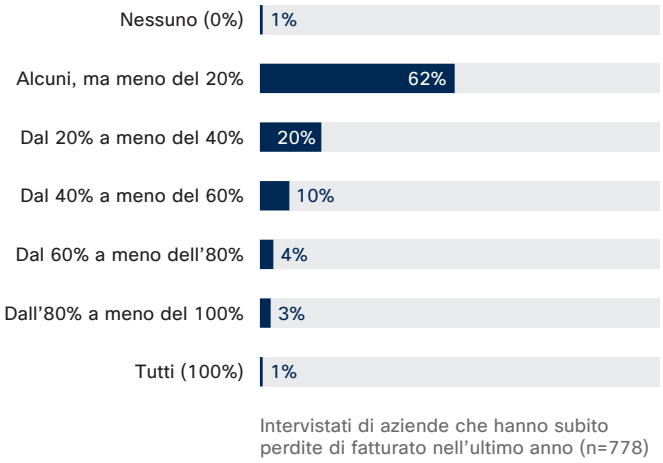
Impatti

Figura 81 Percentuali delle opportunità aziendali perse a causa degli attacchi



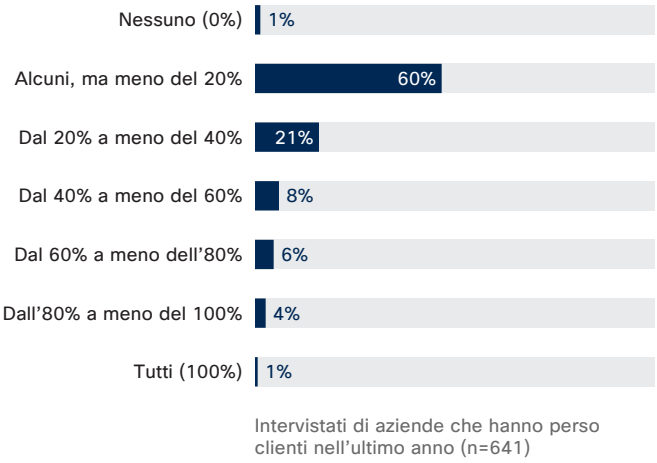
Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 82 Percentuali dei profitti aziendali persi a causa degli attacchi



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 83 Percentuali dei clienti persi dall'azienda a causa degli attacchi



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Risultati

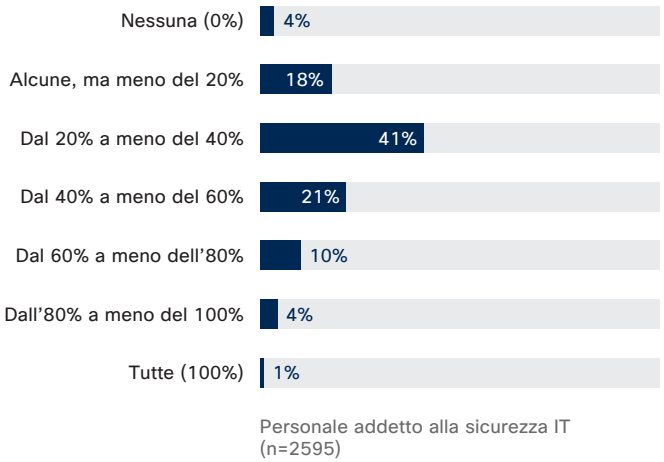
Figura 84 Percentuali di aziende che si affidano all'esternalizzazione

Quali servizi di sicurezza vengono esternalizzati?	2014 (n=1738)	2015 (n=2432)	2016 (n=2912)
Consulenza	51%	52%	51%
Revisione	41%	47%	46%
Reazione agli incidenti	35%	42%	45%
Monitoraggio	42%	44%	45%
Intelligence sulle minacce	N/A	39%	41%
Correzione	34%	36%	35%
Nessuno/Solo servizi interni	21%	12%	10%

Perché questi servizi sono esternalizzati?	2015 (n=2129)	2016 (n=2631)
Maggiore efficienza dei costi	53%	52%
Desiderio di analisi imparziali	49%	48%
Risposta più rapida agli incidenti	46%	46%
Mancanza di competenze interne	31%	33%
Mancanza di risorse interne	31%	33%

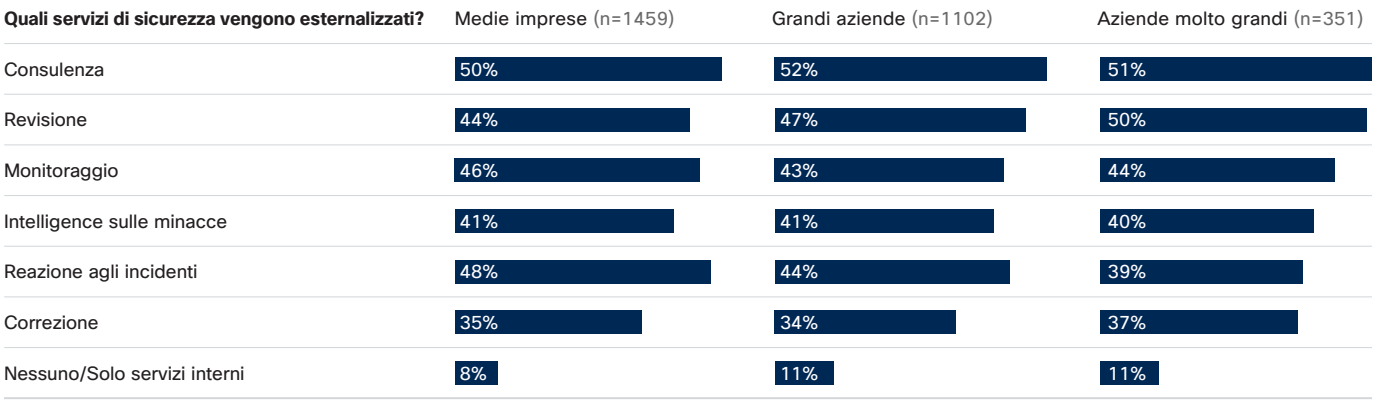
Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 85 Percentuali di soluzioni di sicurezza che le aziende affidano a fornitori terzi



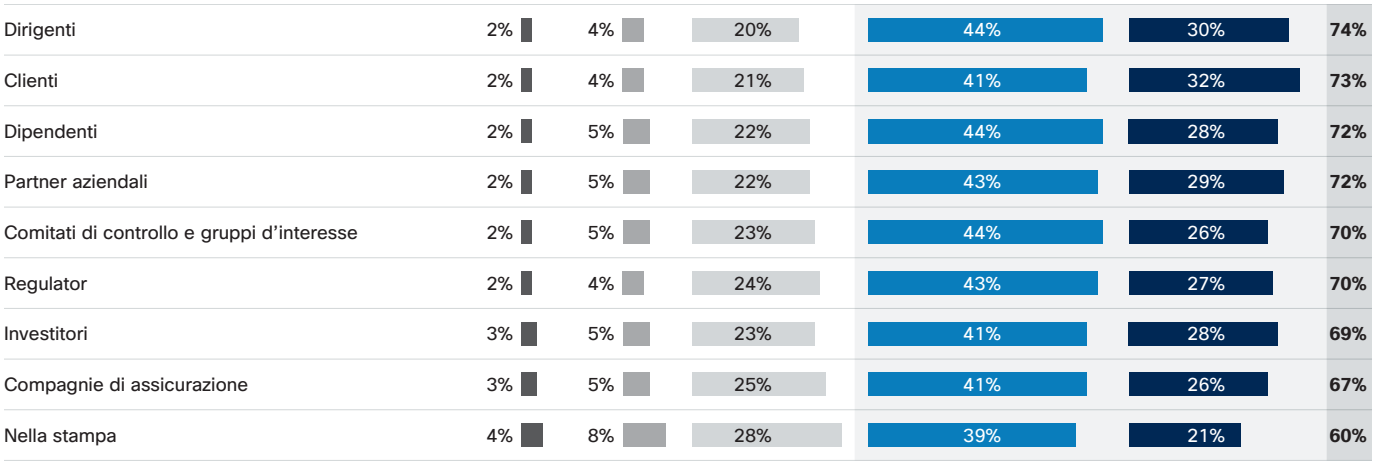
Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 86 Percentuali di servizi di sicurezza esternalizzati in base alle dimensioni dell'azienda



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 87 Fonti di maggiori controlli



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

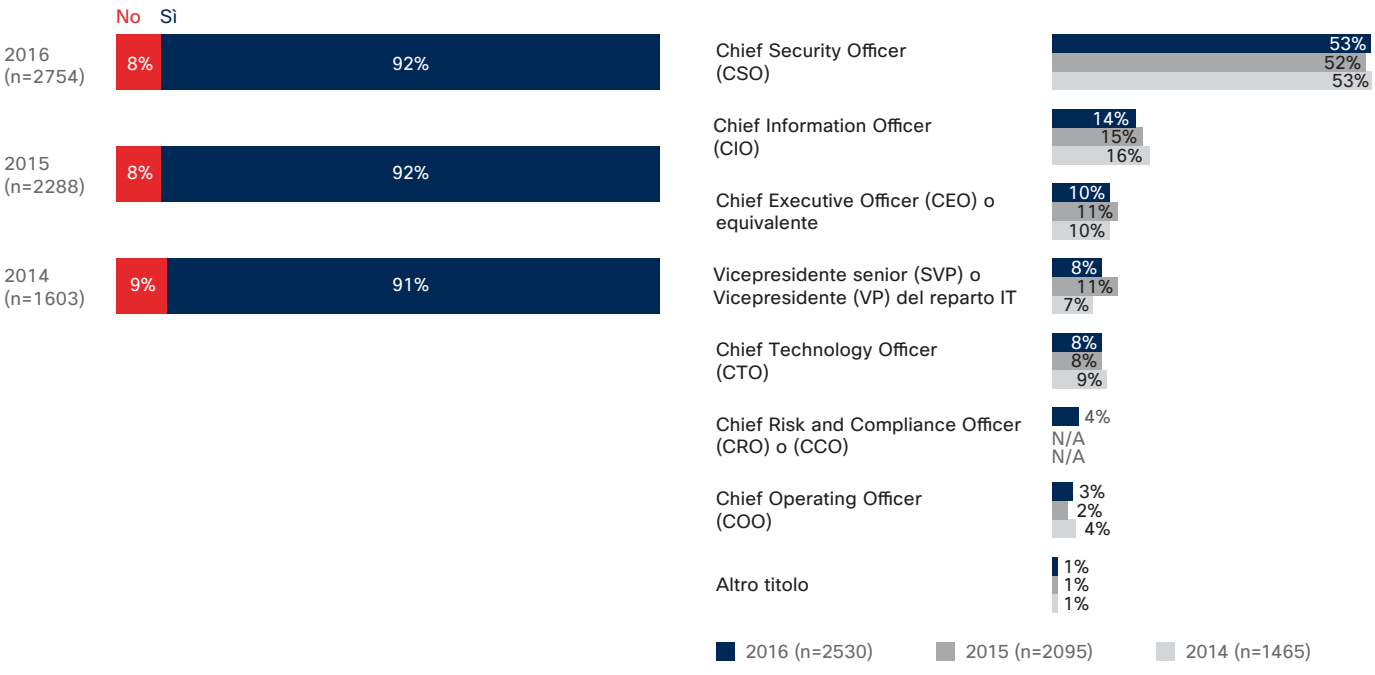
Figura 88 Aumento del cloud privato off premises e dell'hosting on-premises gestito da terze parti

Dove si trovano le reti	2014 (n=1727)	2015 (n=2417)	2016 (n=2887)
On-premises parte del cloud privato	50%	51%	50%
On-premises	54%	48%	46%
On-premises ma gestito da una terza parte esterna	23%	24%	27%
Cloud privato off-premises	18%	20%	25%
Cloud pubblico off-premises	8%	10%	9%

Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

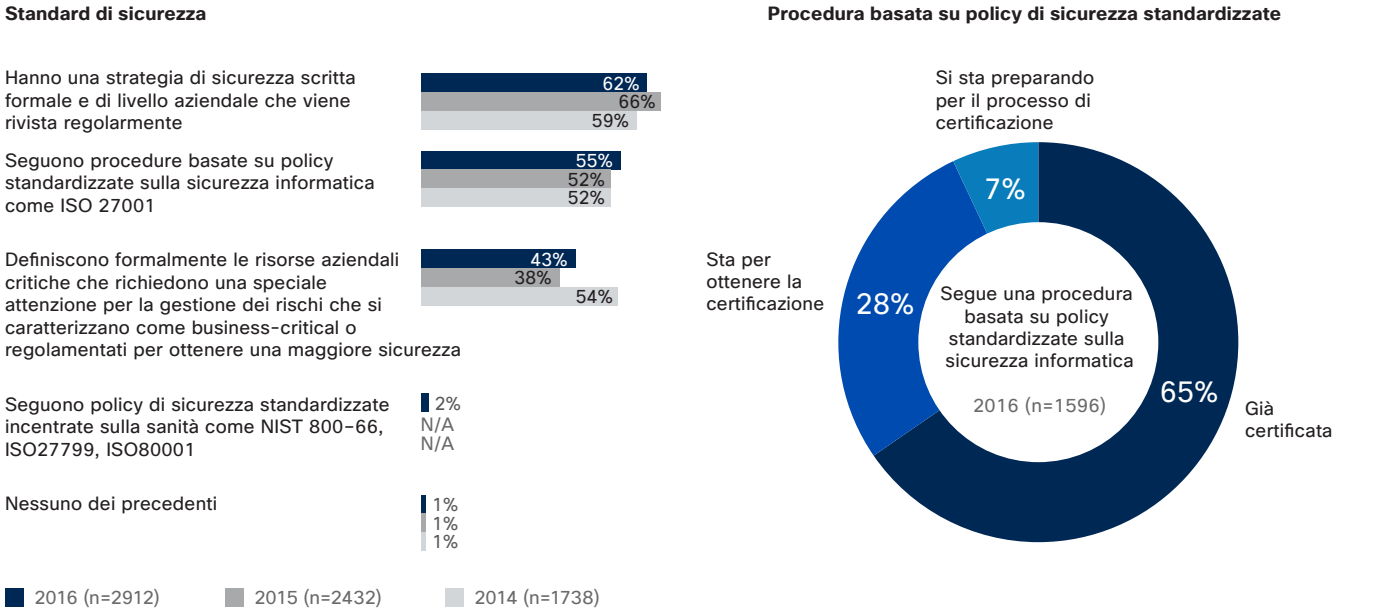
Operazioni, policy, procedure e funzionalità

Figura 89 Percentuale di aziende con un dirigente responsabile della sicurezza



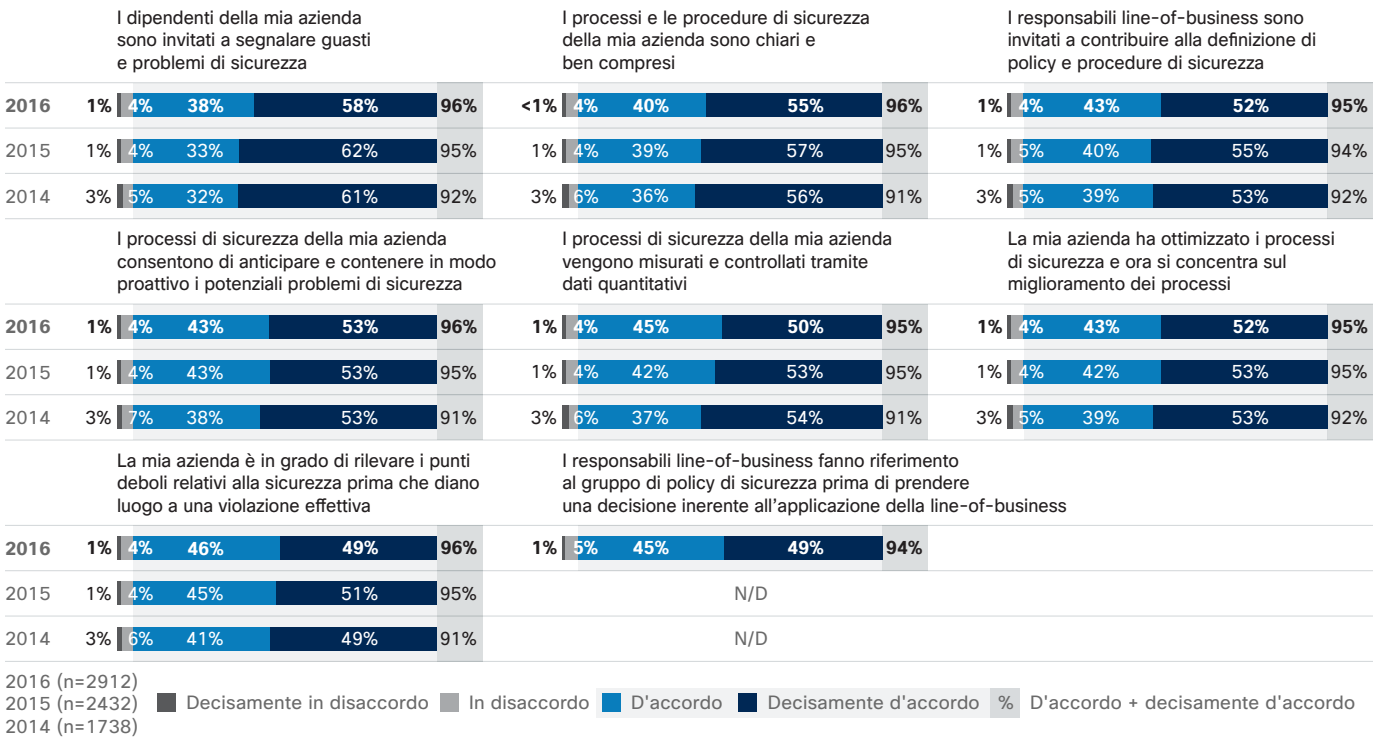
Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 90 Percentuale di aziende che possiedono una strategia di sicurezza formale di livello aziendale e che seguono procedure basate su policy di sicurezza standardizzate



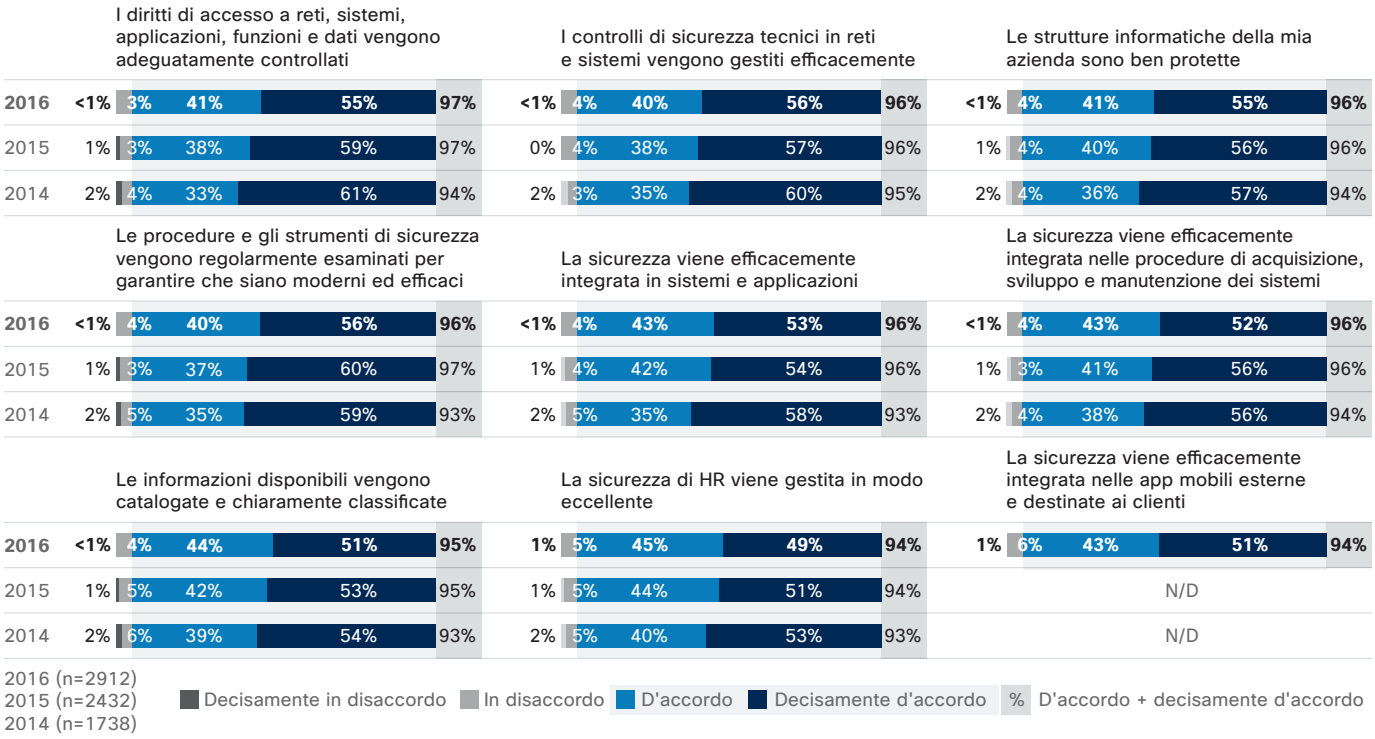
Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 91 Percentuali di intervistati che si dichiarano decisamente d'accordo con le affermazioni sui processi di sicurezza



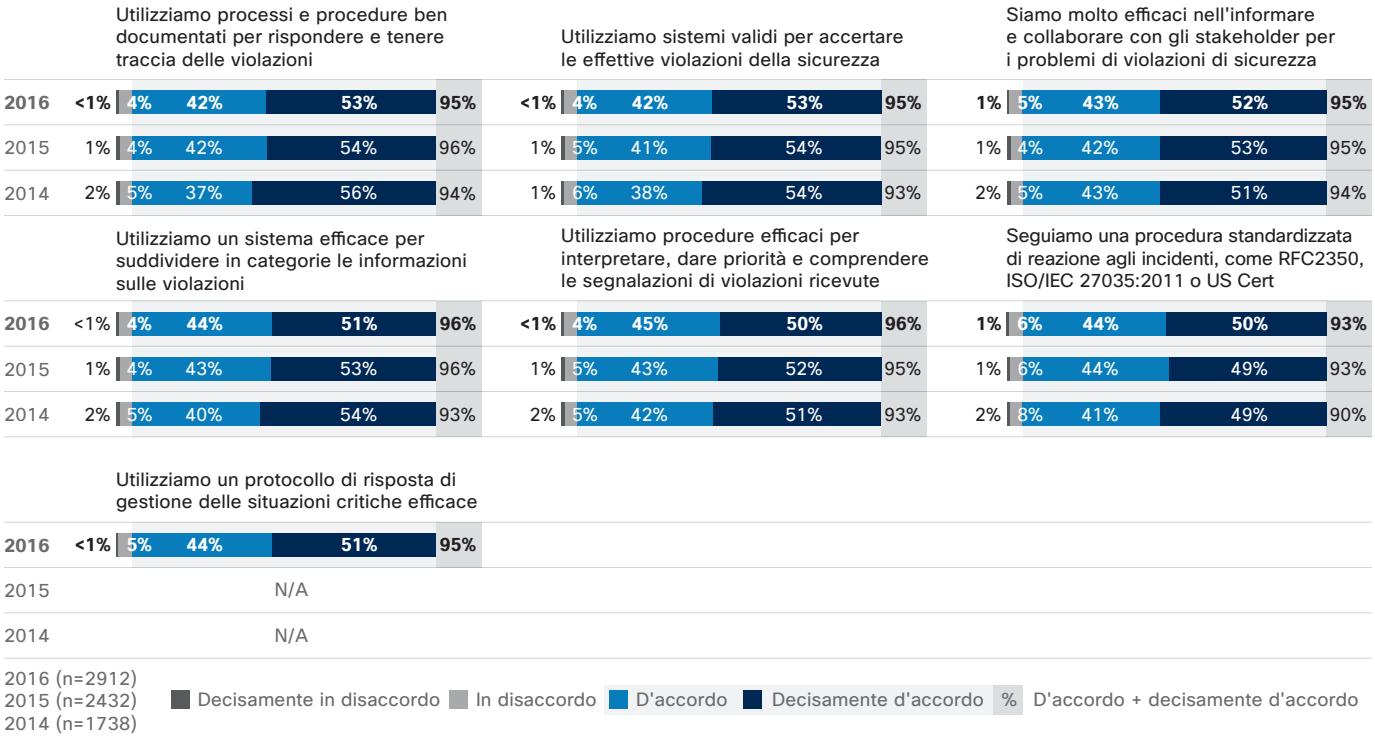
Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 92 Percentuali di intervistati che si dichiarano decisamente d'accordo con le affermazioni sui processi di sicurezza



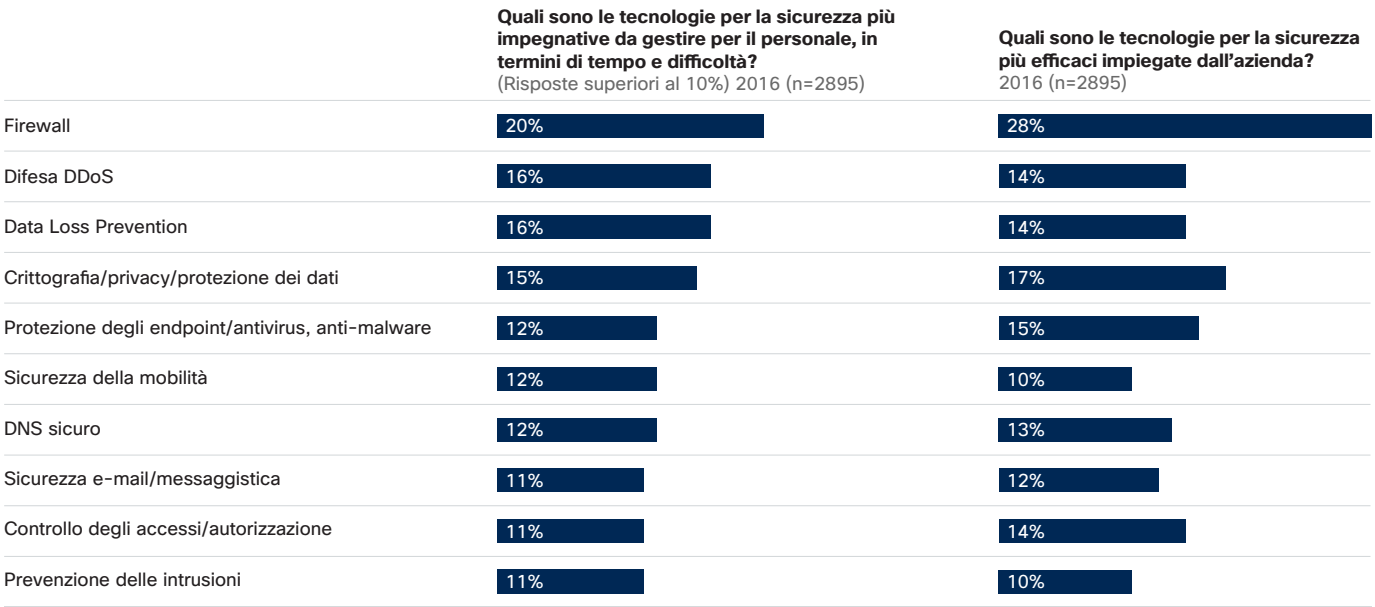
Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 93 Percentuali di intervistati che si dichiarano decisamente d'accordo con le affermazioni sui controlli di sicurezza



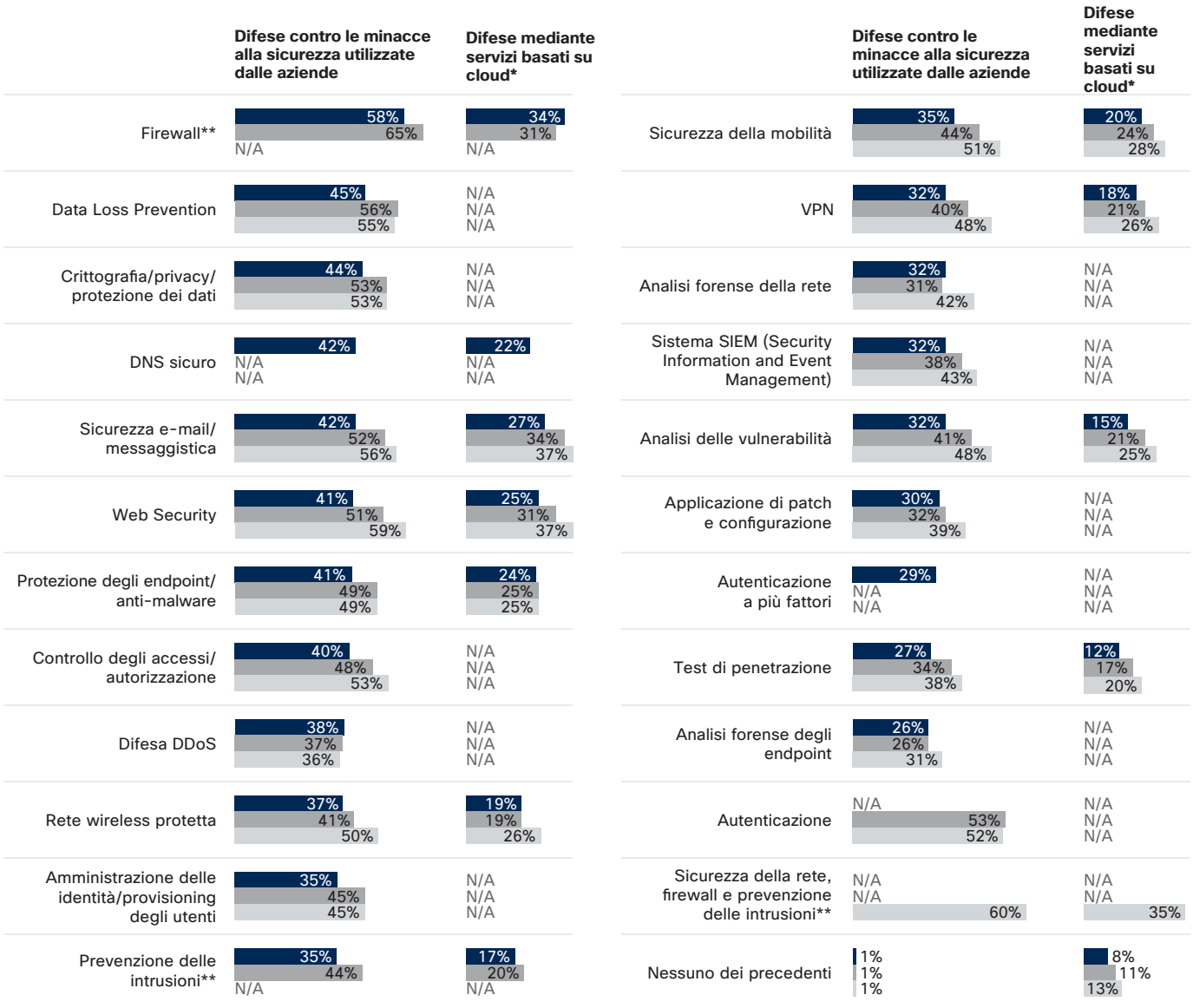
Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 94 Gestione ed efficacia delle tecnologie per la sicurezza



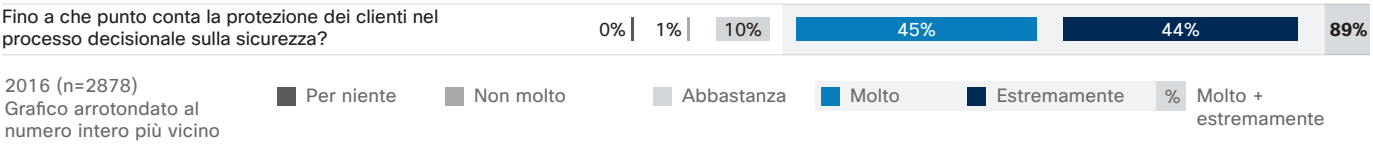
Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 95 Utilizzo su base annua della difesa dalle minacce alla sicurezza



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

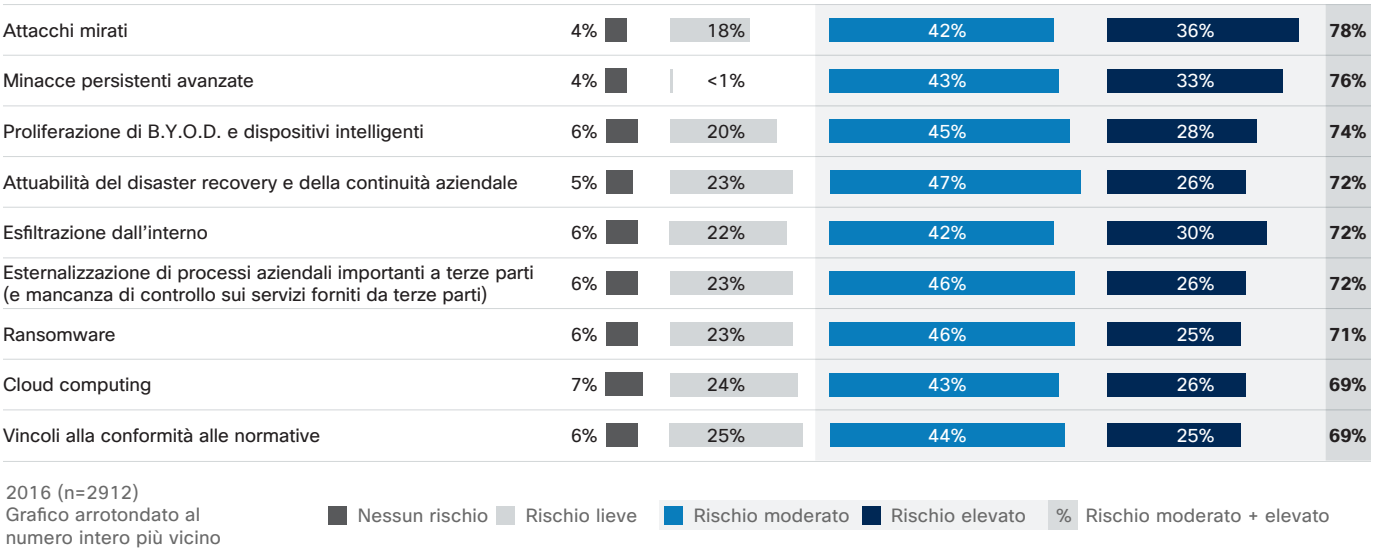
Figura 96 Quanto conta la protezione dei clienti nel processo decisionale sulla sicurezza



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

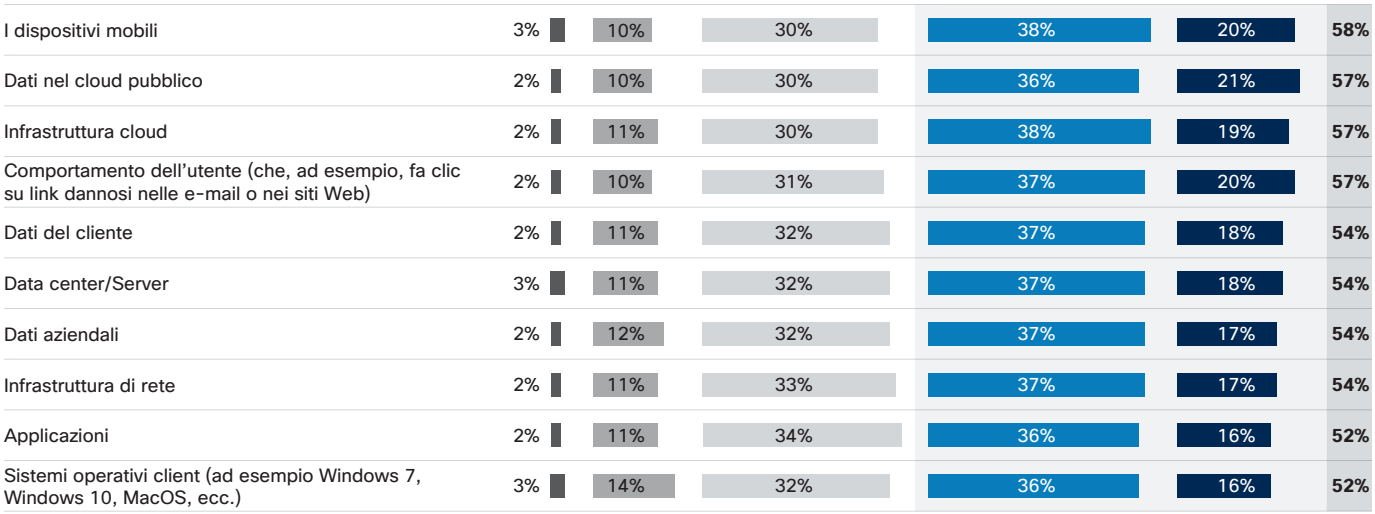
Rischi e vulnerabilità

Figura 97 Le principali fonti di preoccupazione del personale IT addetto alla sicurezza in merito agli attacchi informatici



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 98 Le principali fonti di preoccupazione degli esperti della sicurezza in merito agli attacchi informatici



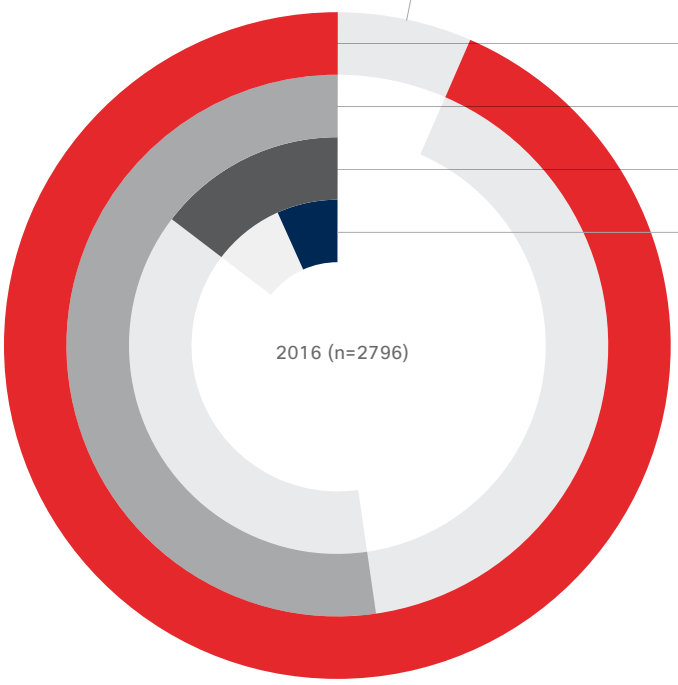
Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 99 Suddivisione degli interventi dei team di sicurezza

Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Reazione agli incidenti

Figura 100 Percentuali di avvisi di sicurezza analizzati o corretti



7% non ha ricevuto avvisi di sicurezza

93% ha ricevuto avvisi di sicurezza

56% degli avvisi rilevati viene esaminato

28% degli avvisi esaminati è legittimo

46% degli avvisi legittimi viene risolto

Media degli avvisi rilevati dall'azienda quotidianamente	
Meno di 5.000	50%
Da 5.000 a 10.000	15%
Da 10.000 a 50.000	11%
Da 50.000 a 100.000	8%
Da 100.000 a 150.000	6%
Più di 150.000	4%

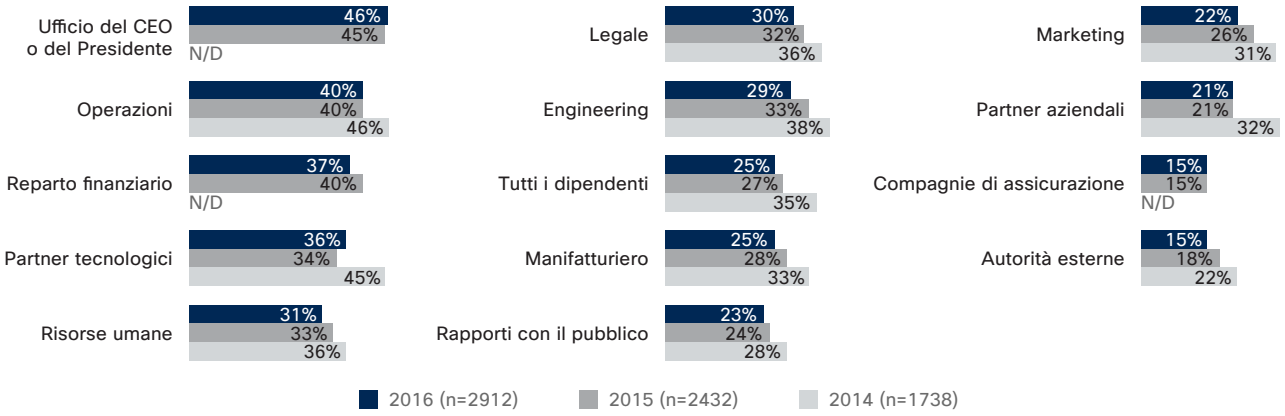
Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 101 Tempo medio di rilevamento delle violazioni della sicurezza

	2016 (n=2860)
Massimo 8 ore	43%
9-24 ore	25%
25-48 ore	15%
Più di 2 giorni ma meno di 1 settimana	7%
1-2 settimane	5%
Da 3 settimane a 1 mese	3%
Da 1 a 3 mesi	1%
Più di 3 mesi ma meno di 1 anno	1%
1 o più anni	0%

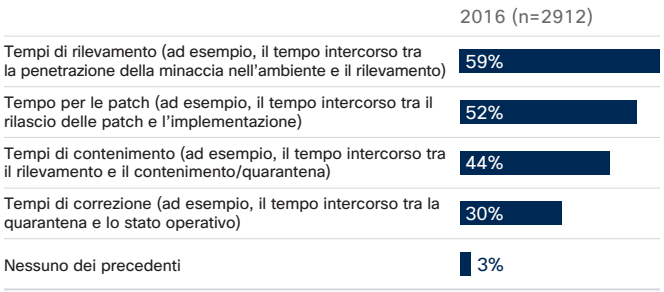
Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 102 Gruppi informati in caso di violazione



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 103 KPI utilizzato dalle aziende per valutare le prestazioni di sicurezza



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 104 Utilizzo su base annua del processo per analizzare i sistemi compromessi

Procedure per l'analisi dei sistemi compromessi	2014 (n=1738)	2015 (n=2432)	2016 (n=2912)
Registro firewall	61%	57%	56%
Analisi dei log dei sistemi	59%	53%	50%
Analisi dei flussi di rete	53%	49%	49%
Analisi di regressione di malware o file	55%	48%	47%
Analisi del registro di sistema	50%	47%	43%
Analisi dell'acquisizione dei pacchetti completi	47%	38%	40%
Rilevamento degli IoC	38%	35%	38%
Analisi forense del disco	40%	36%	36%
Analisi di log/eventi correlati	42%	37%	35%
Analisi forense della memoria	41%	34%	34%
Team esterni per l'analisi o la reazione agli incidenti	37%	33%	34%
Nessuno dei precedenti	2%	1%	1%

Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 105 Utilizzo su base annua del processo per eliminarne la causa degli incidenti di sicurezza

Procedure per l'eliminazione delle cause delle violazioni della sicurezza	2014 (n=1738)	2015 (n=2432)	2016 (n=2912)
Quarantena o rimozione della applicazioni dannose	58%	55%	52%
Analisi delle cause profonde	55%	55%	51%
Interruzione delle comunicazioni con il software dannoso	53%	53%	48%
Monitoraggio aggiuntivo	52%	48%	48%
Aggiornamenti delle policy	51%	47%	45%
Interruzione delle comunicazioni con l'applicazione compromessa	48%	47%	43%
Sviluppo di correzioni a lungo termine	47%	40%	41%
Ripristino dell'immagine di sistema a uno stato precedente	45%	41%	39%
Nessuno dei precedenti	2%	1%	1%

Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 106 Utilizzo su base annua del processo per ripristinare i sistemi colpiti

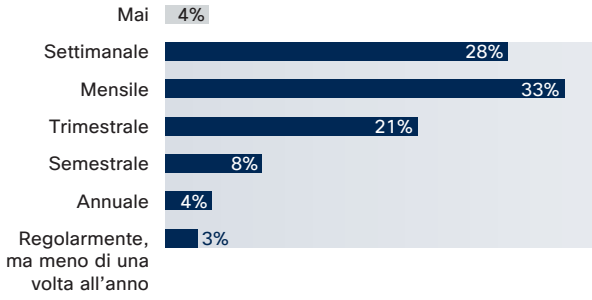
Processi di ripristino dei sistemi colpiti	2014 (n=1738)	2015 (n=2432)	2016 (n=2912)
Implementazione di controlli e metodi di rilevamento nuovi o aggiuntivi in base ai punti deboli identificati dopo le violazioni	60%	56%	56%
Ripristino da un backup creato prima della violazione	57%	59%	55%
Patch e aggiornamento delle applicazioni ritenute vulnerabili	60%	55%	53%
Ripristino differenziale (eliminando le modifiche determinate da incidenti)	56%	51%	50%
Ripristino da un'immagine di riferimento sicura	35%	35%	34%
Nessuno dei precedenti	2%	1%	1%

Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 107 Simulazioni di attacco: frequenza e portata dei miglioramenti ai sistemi di difesa

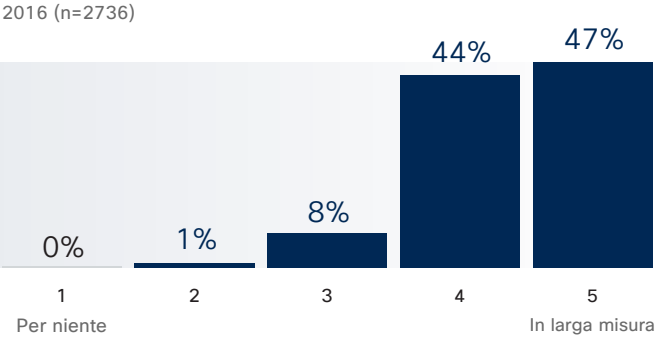
Con che frequenza l'azienda effettua simulazioni di attacchi?

2016 (n=2868)



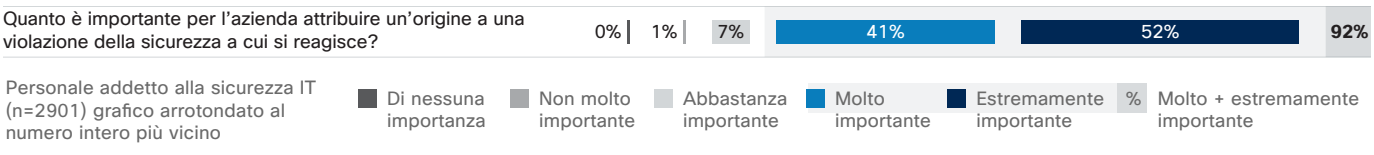
In quale misura i risultati delle simulazioni di attacco hanno favorito i miglioramenti di policy di sicurezza, procedure o tecnologie per la sicurezza?

2016 (n=2736)



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

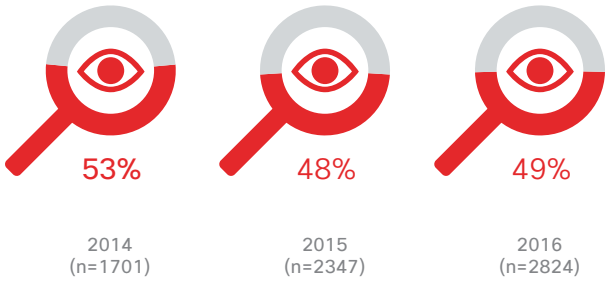
Figura 108 Importanza di attribuzione dell'origine a una violazione della sicurezza



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

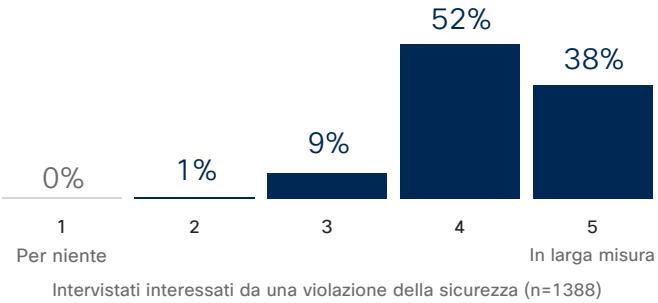
Violazioni e relativo impatto

Figura 109 Percentuale di aziende che hanno subito una violazione di dominio pubblico



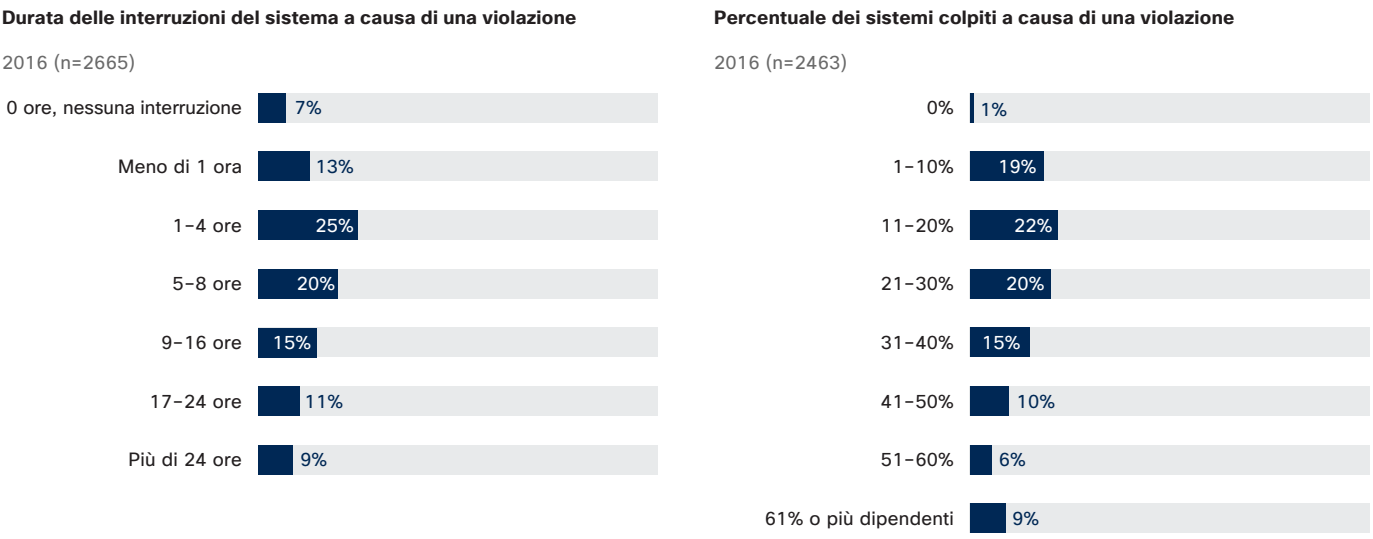
Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 110 In quale misura la violazione ha favorito i miglioramenti di policy di sicurezza, procedure o tecnologie di difesa dalle minacce?



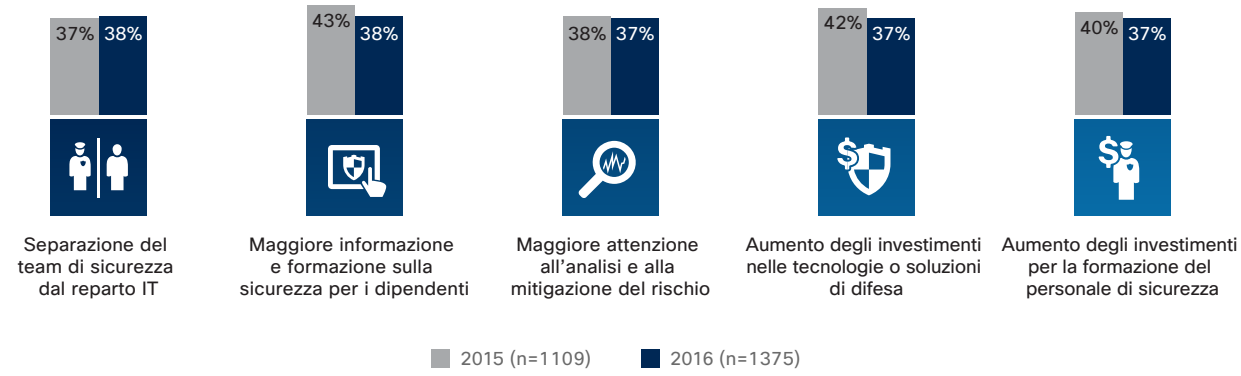
Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 111 Durata e dimensioni delle interruzioni causate da violazioni della sicurezza



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 112 Miglioramenti apportati per proteggere l'azienda dalle violazioni della sicurezza



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Scelta e aspettative dei fornitori

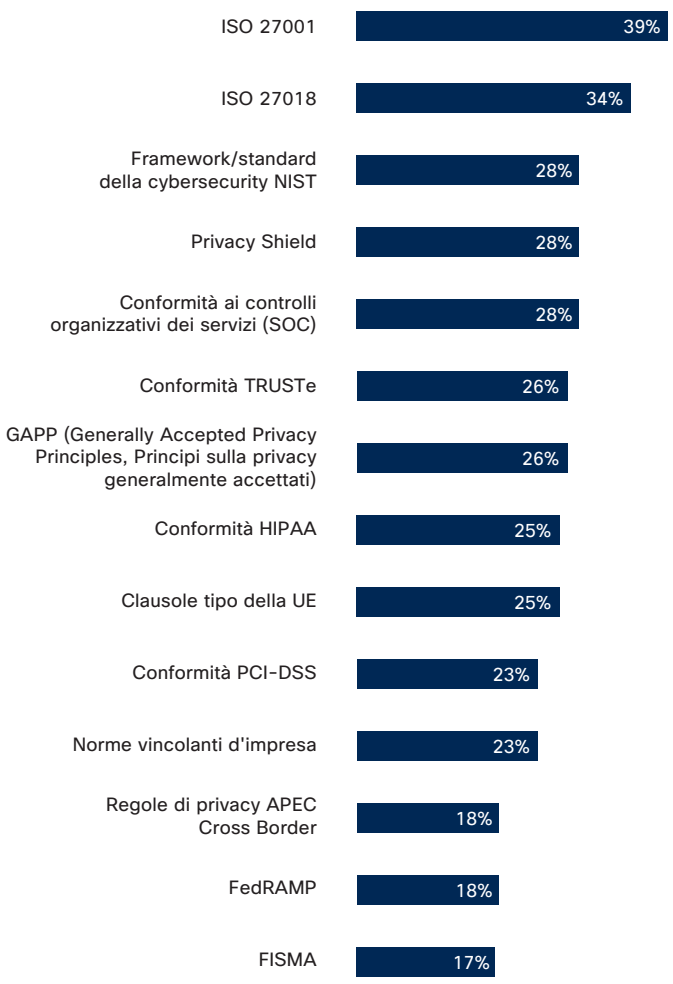
Figura 113 Importanza della protezione dei dati e della privacy per i fornitori

Quali processi e policy per la protezione dei dati e della privacy deve assolutamente attuare un fornitore?

2016 (n=2912)

Quali standard e certificazioni per la privacy e la protezione dei dati sono necessari affinché un fornitore possa collaborare con la tua azienda?

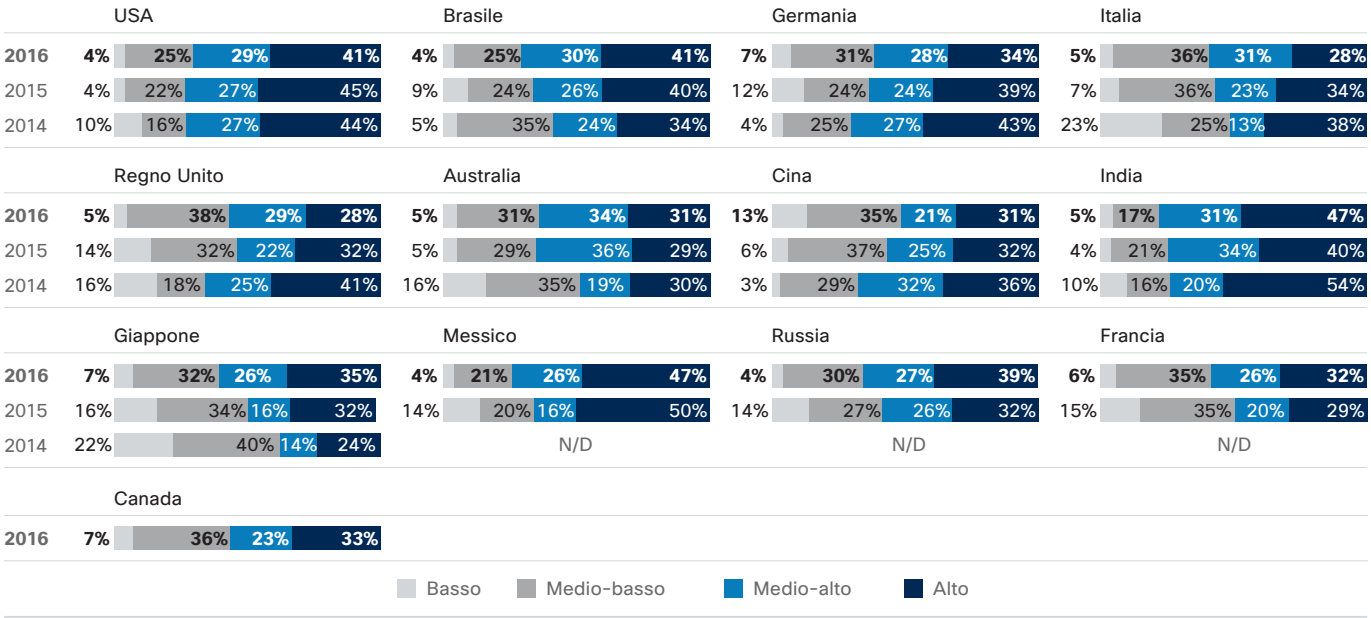
2016 (n=2870)



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Modello di maturità delle funzionalità di sicurezza

Figura 114 Maturità della sicurezza per paese

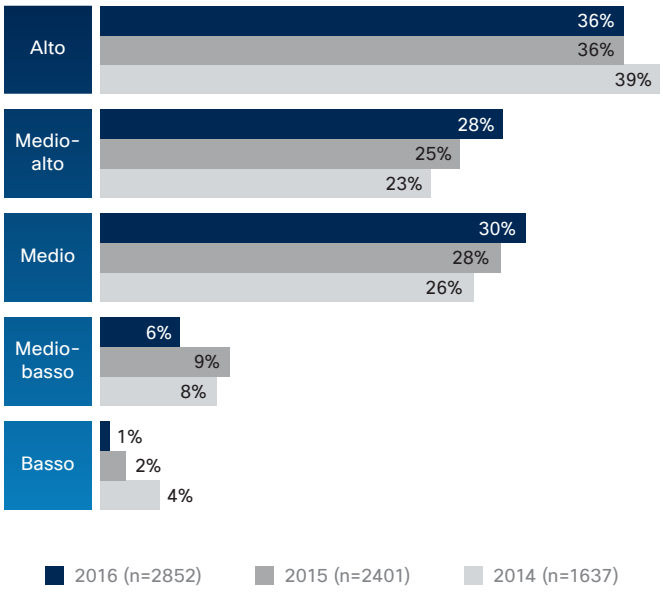


Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 115 Il modello della maturità classifica le aziende in base al processo di sicurezza

Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 116 Dimensione dei segmenti per modello di maturità

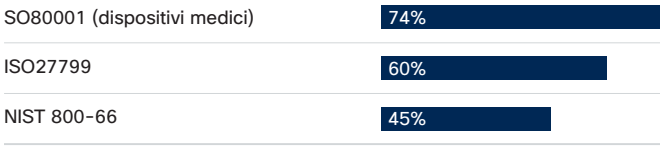


Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Per settore

Figura 117 Percentuale di aziende sanitarie che hanno implementato policy di sicurezza standardizzate

Policy di sicurezza standardizzate implementate
L'azienda sanitaria segue procedure basate su policy specifiche sulla sicurezza informatica appositamente per la sanità, 2016 (n=65)



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

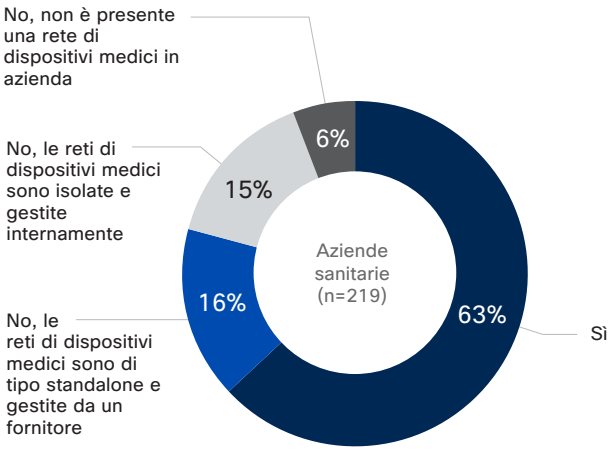
Figura 118 Risorse utilizzate delle aziende sanitarie per misurarsi con le regole HIPAA sulla privacy

Quali risorse vengono utilizzate dalle aziende sanitarie per misurarsi con la sicurezza e le regole HIPAA sulla privacy?	Aziende sanitarie nel 2016 (n=219)
Guida per la sicurezza HIT	52%
Attuale documento HIPAA (attualmente omnibus)	52%
Framework di controllo HHS.OCR	40%
HITRUST o altri framework privati	37%
Valutazioni di terze parti	24%
Nessuno dei precedenti	6%

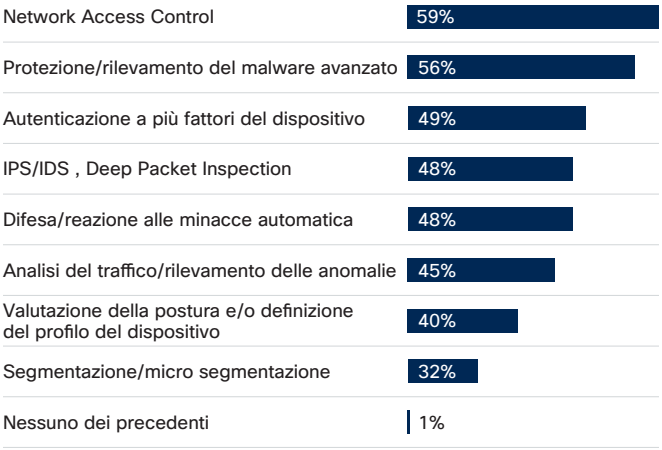
Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 119 Misure di sicurezza più diffuse tra le aziende sanitarie con reti di dispositivi medici

La tua azienda ha una rete di dispositivi medici che converge con la rete principale dell'ospedale?



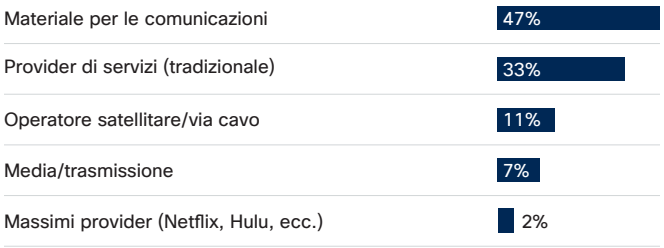
Quale di queste misure di sicurezza, se presenti, sono state implementate dalla tua azienda per proteggere e mettere in sicurezza la rete di dispositivi medici?
Società con una rete di dispositivi medici nella propria azienda (n=207)



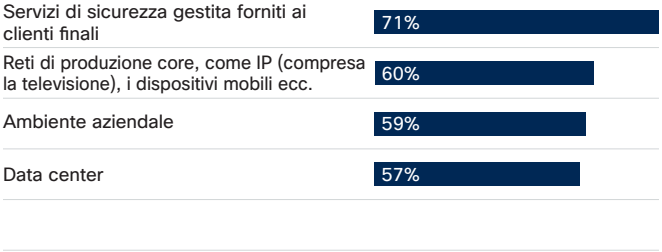
Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 120 Profilo campione per le telecomunicazioni

In quale sottosettore delle telecomunicazioni è coinvolta principalmente la tua azienda?
Aziende di telecomunicazioni (n=307)



Quali di questi servizi offre la tua azienda ai clienti?
Aziende di telecomunicazioni (n=308)



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

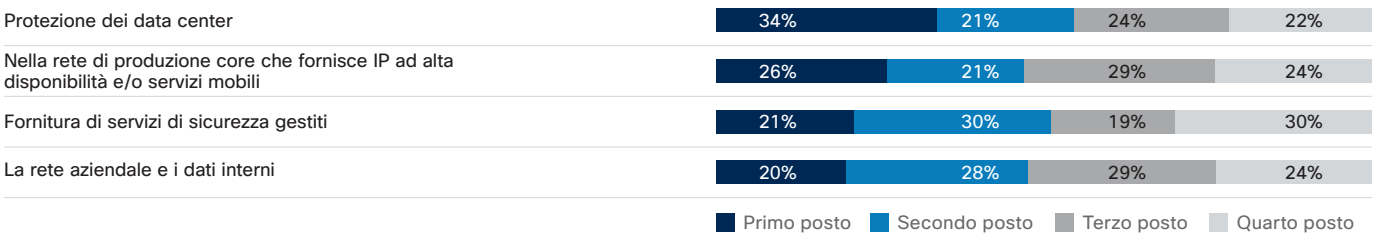
Figura 121 Strategie di sicurezza per le telecomunicazioni

Priorità relativa per i protocolli e le strategie di sicurezza
Aziende di telecomunicazioni (n=308)

Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 122 Priorità di sicurezza per le telecomunicazioni

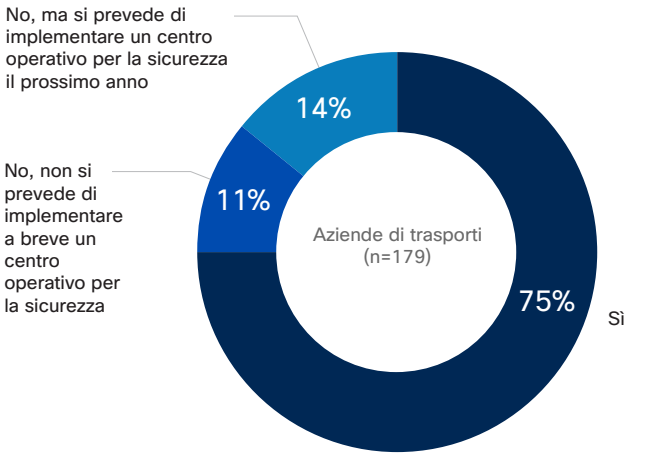
Classifica in termini di priorità per la sicurezza all'interno dell'azienda
Aziende di telecomunicazioni (n=308)



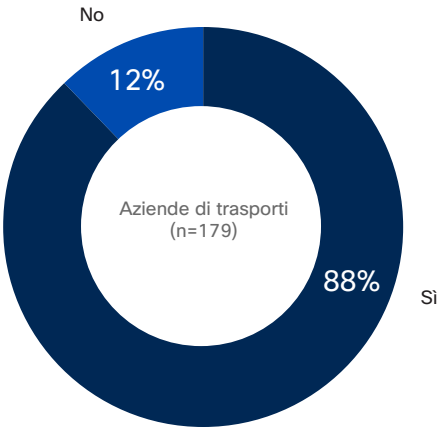
Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 123 Profilo campione per i trasporti

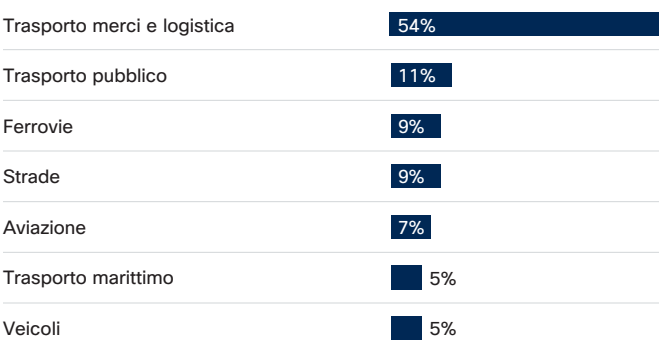
La tua azienda utilizza un centro operativo per la sicurezza (SOC)?



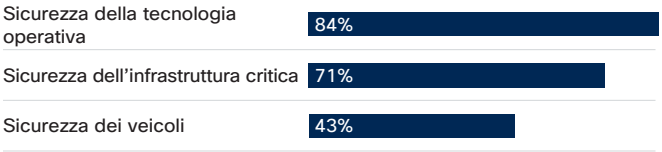
La tua azienda aderisce a organismi di certificazione della sicurezza o a organizzazioni di settore?



In quale sottosettore dei trasporti è coinvolta principalmente la tua azienda?
Aziende di trasporti (n=180)



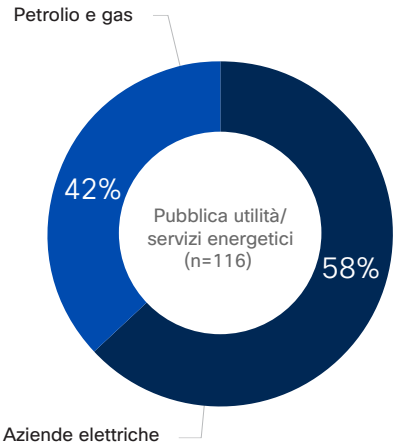
Di quale delle seguenti aree della sicurezza sei responsabile?
Aziende di trasporti (n=180)



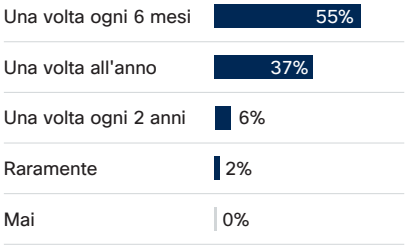
Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

Figura 124 Profilo campione per servizi pubblici e settore energetico

In quale sottosettore dei servizi pubblici/ energetici è coinvolta principalmente la tua azienda?

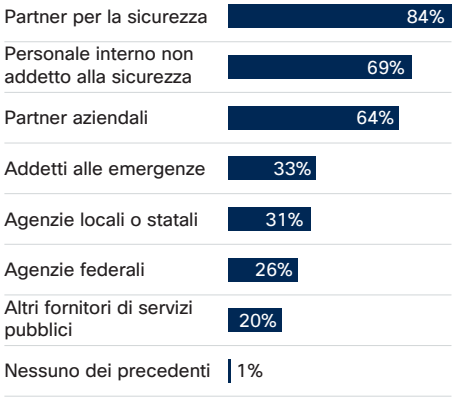


Con che frequenza la tua azienda effettua prove o esercitazioni per testare il piano di reazione agli incidenti di cybersecurity?



Pubblica utilità/servizi energetici (n=116)

Con che frequenza la tua azienda effettua prove o esercitazioni per testare il piano di reazione agli incidenti di cybersecurity?

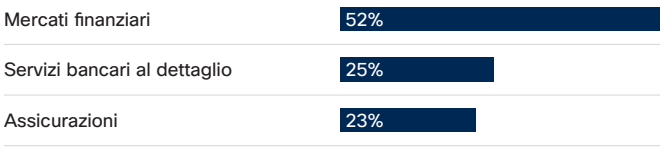


Pubblica utilità/servizi energetici (n=116)

Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

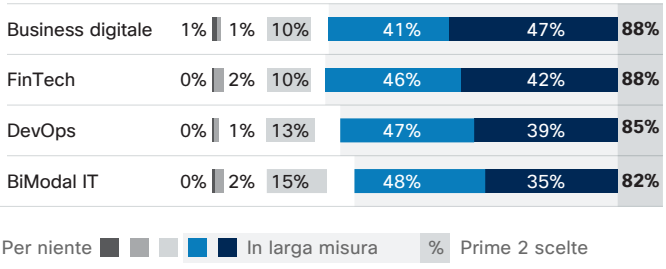
Figura 125 Profilo campione per i servizi finanziari

In quale sottosettore dei servizi finanziari è coinvolta principalmente la tua azienda?



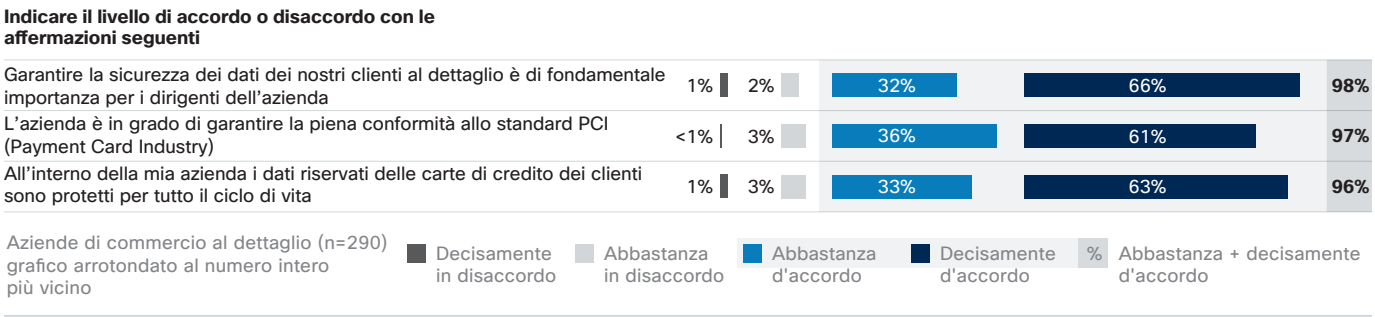
Aziende di servizi finanziari (n=509)
Grafico arrotondato al numero intero più vicino

In che misura la sicurezza è stata influenzata dalle seguenti tendenze?



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

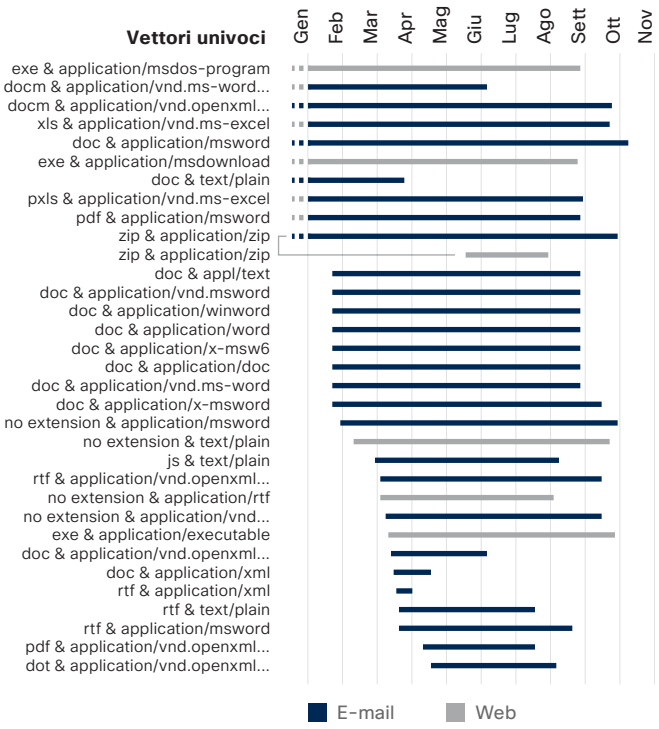
Figura 126 Sicurezza dei dati per il commercio al dettaglio



Fonte: studio di valutazione sulle funzioni di sicurezza Cisco 2017

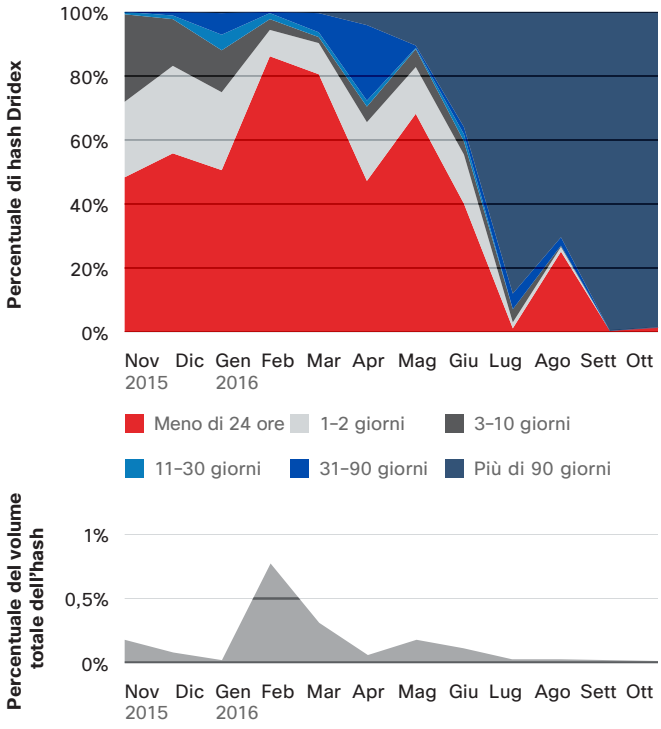
Famiglie di malware

Figura 127 Estensioni di file e combinazioni MIME per Dridex (vettori e-mail e Web)



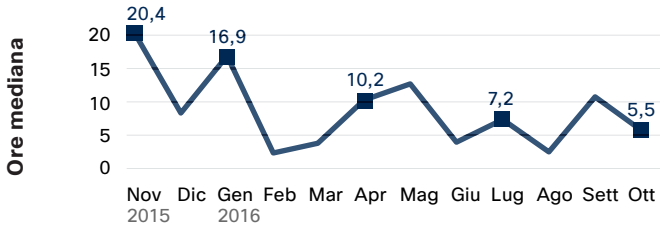
Fonte: Cisco Security Research

Figura 128 Età degli hash per la famiglia di malware Dridex e percentuale del volume hash totale osservato mensilmente



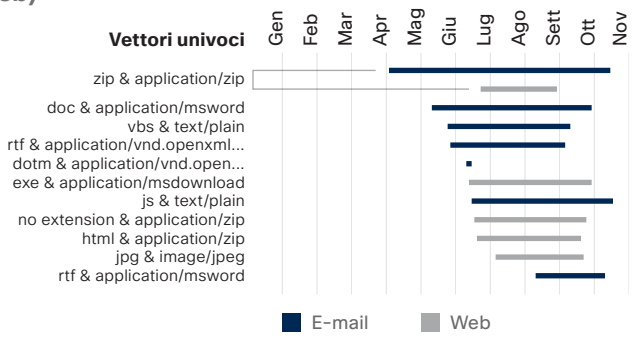
Fonte: Cisco Security Research

Figura 129 TTD per la famiglia di malware Dridex



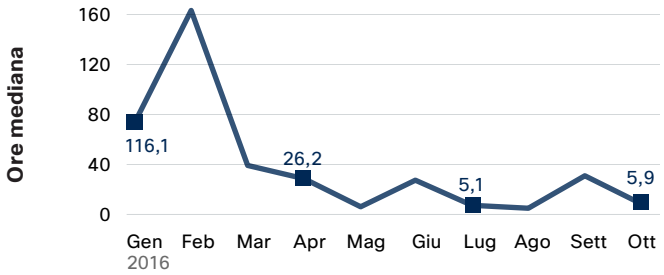
Fonte: Cisco Security Research

Figura 130 Estensioni di file e combinazioni MIME per la famiglia di minacce e gli indicatori che rimandano al payload Cerber e lo contengono (vettori e-mail e Web)



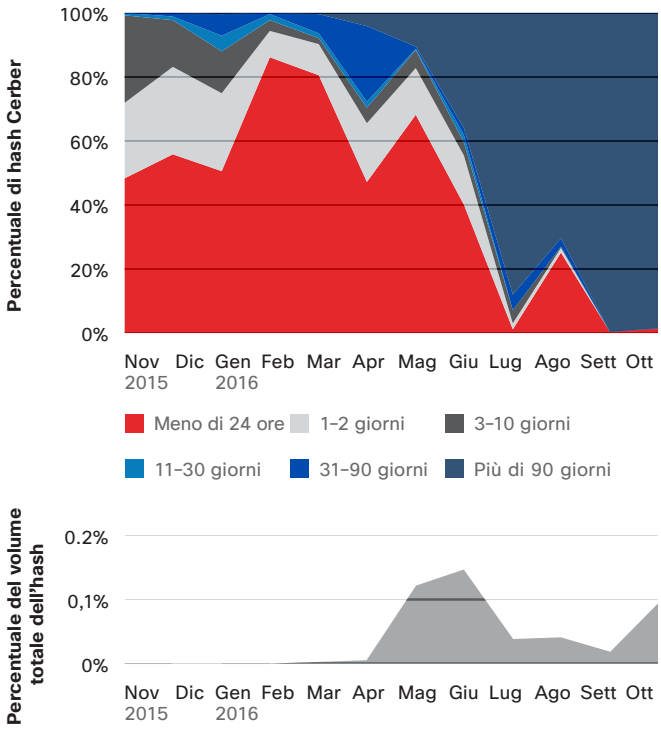
Fonte: Cisco Security Research

Figura 131 TTD per la famiglia di malware Cerber



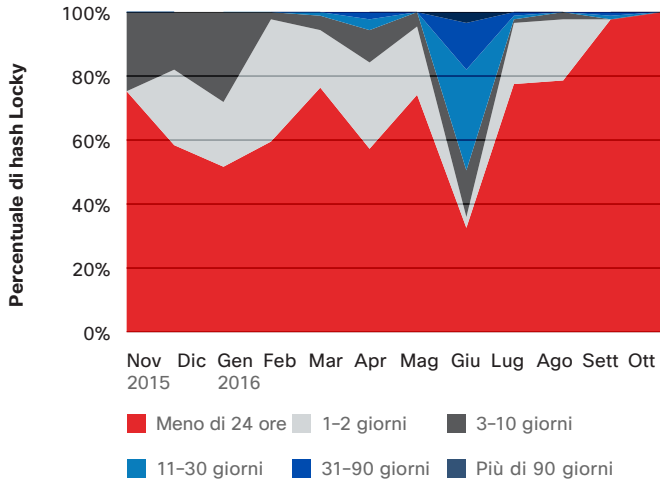
Fonte: Cisco Security Research

Figura 132 Età degli hash per la famiglia di malware Cerber e percentuale del volume hash totale osservato mensilmente



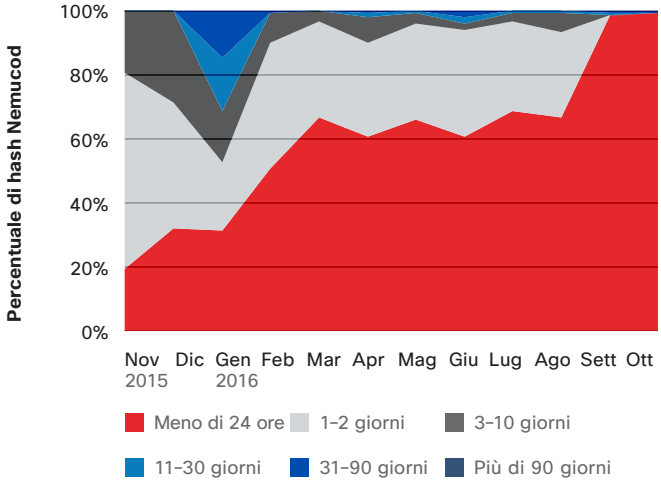
Fonte: Cisco Security Research

Figura 133 Età degli hash per la famiglia di malware Locky su base mensile



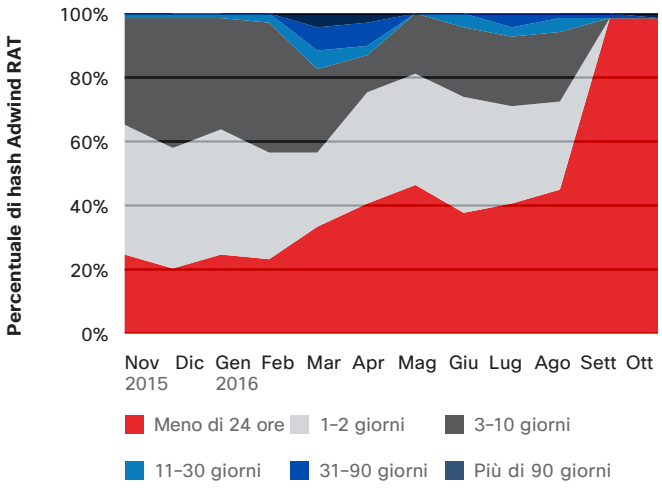
Fonte: Cisco Security Research

Figura 134 Età degli hash per la famiglia di malware Nemucod su base mensile



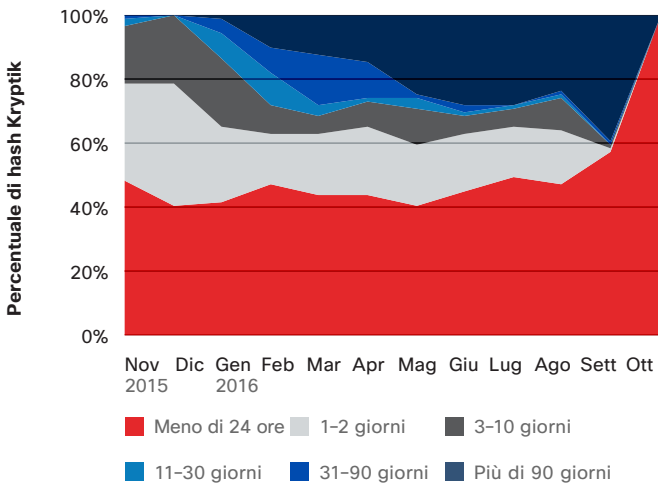
Fonte: Cisco Security Research

Figura 135 Età degli hash per la famiglia di malware Adwind RAT su base mensile



Fonte: Cisco Security Research

Figura 136 Età degli hash per la famiglia di malware Kryptik su base mensile



Fonte: Cisco Security Research

Download dei grafici

Tutti i grafici di questo report possono essere scaricati all'indirizzo:
www.cisco.com/go/acr2017graphics

Aggiornamenti e correzioni

Per vedere gli aggiornamenti e le correzioni delle informazioni di questo report, visitare:
www.cisco.com/go/acr2017errata

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

Sede centrale Asia Pacifica
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 www.cisco.com/go/offices.

Pubblicato nel gennaio 2017