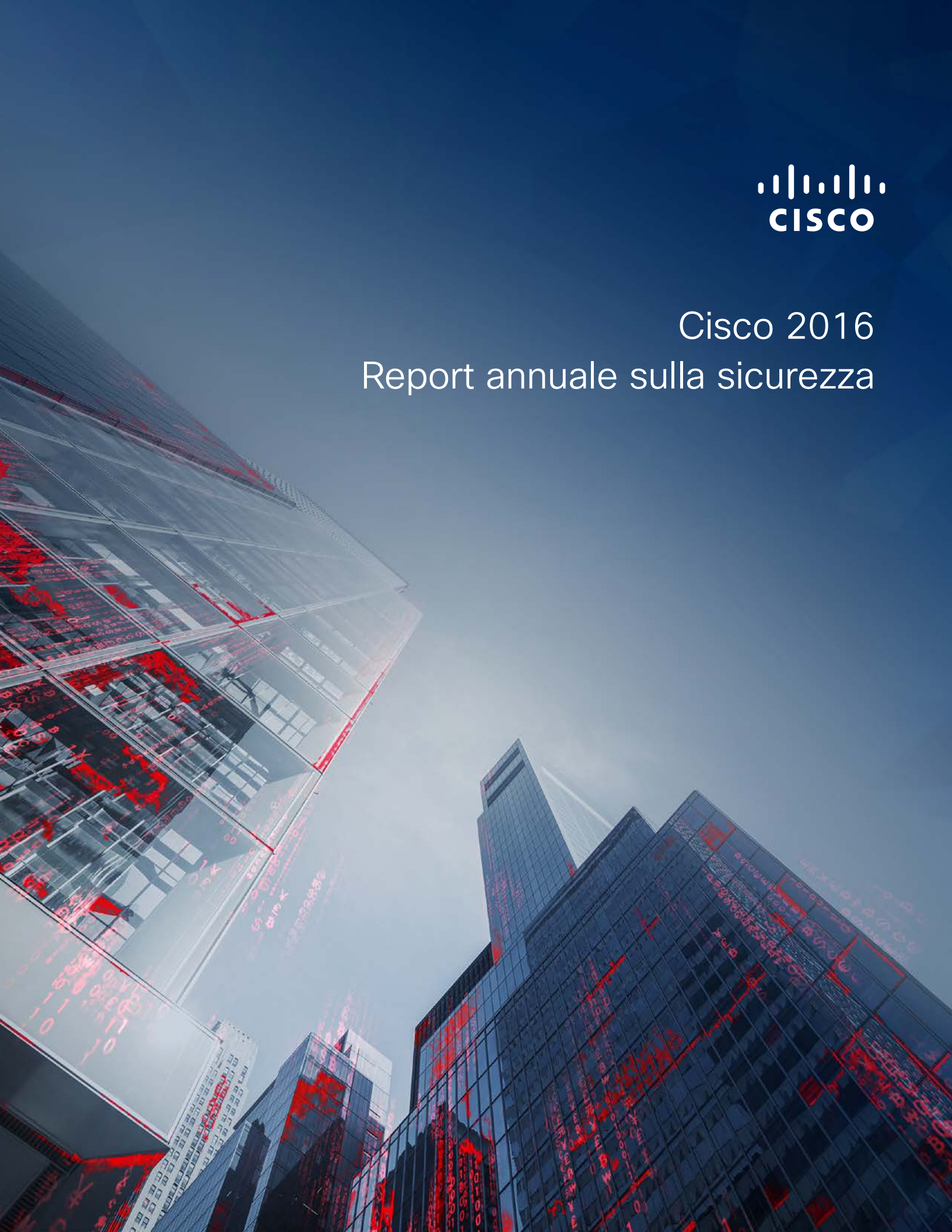


Cisco 2016
Report annuale sulla sicurezza

Panoramica generale

I professionisti della sicurezza devono ridefinire le proprie strategie di difesa.

Sia gli autori degli attacchi che gli addetti alla sicurezza stanno sviluppando tecnologie e tattiche sempre più sofisticate. Da parte loro, gli hacker creano potenti infrastrutture back-end per supportare le proprie campagne. I criminali informatici stanno affinando le proprie tecniche per estorcere denaro alle vittime e per sottrarre dati e proprietà intellettuali senza essere scoperti.

Il report annuale di Cisco sulla sicurezza 2016 comprende ricerche, analisi e opinioni di Cisco Security Research ed evidenzia le sfide affrontate dai professionisti della sicurezza per rilevare e bloccare gli hacker che oggi vantano un ricco arsenale di strumenti che si espande continuamente. Il report include anche una ricerca condotta da esperti esterni, come Level 3 Threat Research Labs, per aiutare a comprendere meglio le attuali tendenze nel campo delle minacce.

Esaminiamo in modo dettagliato i dati riportati dai ricercatori Cisco per illustrare le modifiche nel tempo, chiarire i significati di tali dati e spiegare come i professionisti della sicurezza dovrebbero reagire alle minacce.

In questo report presentiamo i seguenti argomenti:

INTELLIGENCE SULLE MINACCE

In questa sezione vengono esaminate alcune delle principali tendenze della sicurezza informatica individuate dai ricercatori, nonché gli aggiornamenti sui vettori e i metodi di attacco nel Web e le vulnerabilità. La sezione include inoltre un'analisi più ampia delle minacce emergenti, quali ad esempio il ransomware. Per esaminare le tendenze emerse nel 2015, Cisco Security Research ha utilizzato un set di dati telemetrici a livello mondiale.

ANALISI DEL SETTORE

Questa sezione esamina le tendenze nell'ambito della sicurezza che interessano le aziende, tra cui l'utilizzo sempre più diffuso della crittografia e i rischi potenziali che comporta. Analizziamo i punti deboli dei metodi utilizzati dalle piccole e medie imprese (PMI) per proteggere le proprie reti. Presentiamo inoltre una ricerca sulle aziende che si affidano a software obsoleto, non supportato o alla fine del ciclo di vita per il funzionamento dell'infrastruttura IT.

STUDIO COMPARATIVO DELLE INFRASTRUTTURE DI SICUREZZA

Questa sezione analizza i risultati del secondo studio comparativo delle infrastrutture di sicurezza condotto da Cisco. Lo studio si basa sulle opinioni dei professionisti della sicurezza in relazione all'infrastruttura di sicurezza delle aziende in cui operano. Dal confronto dei risultati del sondaggio 2015 con quelli del 2014, Cisco ha rilevato che i CISO (Chief Information Security Officer) e i manager delle operazioni di sicurezza (SecOps) sono meno fiduciosi di poter contare su un'infrastruttura di sicurezza all'avanguardia e di essere in grado di contrastare gli attacchi. Il sondaggio tuttavia indica anche che le aziende stanno aumentando le iniziative di formazione e altri processi di sicurezza per proteggere le proprie reti. I risultati dello studio vengono presentati in esclusiva nel Report annuale di Cisco sulla sicurezza 2016.

UNO SGUARDO AL FUTURO

Questa sezione analizza le conseguenze del panorama geopolitico per la sicurezza. Presentiamo i risultati di due studi effettuati da Cisco. Il primo prende in esame le priorità dei dirigenti riguardo alla sicurezza informatica, il secondo tratta le opinioni dei responsabili delle decisioni IT sui rischi per la sicurezza e l'affidabilità. Inoltre forniamo un aggiornamento sui progressi compiuti da Cisco nel ridurre i tempi di rilevamento e sottolineiamo l'importanza di adottare un'architettura integrata per contrastare le minacce in modo efficace.

Sommario

Sviluppi e scoperte importanti

Sviluppi e scoperte importanti

I criminali informatici hanno affinato le proprie infrastrutture back-end per sferrare attacchi sempre più efficaci e redditizi.

- Avvalendosi della collaborazione di Level 3 Threat Research Labs e del provider di hosting Limestone Networks, Cisco ha identificato e bloccato la più imponente attività dell'Angler exploit kit degli Stati Uniti. Angler prendeva di mira 90.000 vittime al giorno e fruttava agli artefici della campagna decine di milioni di dollari all'anno.
- SSHPsychos (Group 93), uno dei più grandi botnet DDoS (distributed denial of service) analizzati dai ricercatori Cisco, è stato fortemente indebolito grazie agli sforzi congiunti di Cisco e Level 3 Threat Research Labs. Come dimostra il case study di Angler illustrato in precedenza, questo successo sottolinea l'importanza della collaborazione all'interno del settore per contrastare il crimine informatico.
- Le estensioni dannose per i browser costituiscono una delle cause principali della sottrazione di dati per le aziende e sono un problema molto diffuso. Si stima che più dell'85% delle aziende esaminate sia stato interessato da estensioni dannose installate nei browser.
- Botnet famose come Bedep, Gamarue e Miuref rappresentavano la maggioranza dell'attività di comando e controllo che ha colpito un determinato gruppo di aziende analizzato da Cisco a luglio 2015.
- L'analisi di Cisco del malware ritenuto "notoriamente dannoso" ha rilevato che la maggior parte di esso, pari al 91,3%, utilizza il DNS (Domain Name Service) per le campagne del crimine informatico. Mediante l'indagine retrospettiva delle query DNS, Cisco ha scoperto l'uso di resolver DNS "non autorizzati" nella rete dei clienti. I clienti non erano consapevoli che i resolver venivano utilizzati dai dipendenti come elemento dell'infrastruttura DNS.
- Le vulnerabilità di Adobe Flash continuano a essere sfruttate dai criminali informatici. I fornitori software stanno tuttavia cercando di limitare i rischi di esposizione al malware che derivano dall'utilizzo della tecnologia Flash.
- Osservando le tendenze del 2015, i ricercatori ritengono che il traffico crittografato HTTPS abbia raggiunto un punto di svolta e che diventerà presto la forma predominante di traffico Internet. Sebbene la crittografia possa contribuire a proteggere i consumatori, potrebbe anche compromettere l'efficacia dei prodotti per la sicurezza, tanto da rendere difficoltoso il monitoraggio delle minacce alla stessa community. A complicare ulteriormente la sfida, alcuni tipi di malware potrebbero avviare comunicazioni crittografate attraverso porte diverse.
- Per le attività criminali gli hacker si servono dei siti Web compromessi creati dalla diffusa piattaforma di sviluppo WordPress. Da questa posizione possono amministrare le risorse server ed eludere il rilevamento.

- Il problema dell'obsolescenza infrastrutturale è sempre più rilevante e rende le aziende sempre più vulnerabili. Dall'analisi di 115.000 dispositivi Cisco connessi a Internet è emerso che il 92% del campione usava software con vulnerabilità note. Inoltre il 31% dei dispositivi Cisco operativi che sono stati inclusi nell'analisi risultano "a fine vendita" e l'8% è "alla fine del ciclo di vita".
- Secondo lo studio comparativo di Cisco delle infrastrutture di sicurezza del 2015, i responsabili della sicurezza hanno dimostrato un livello di fiducia inferiore negli strumenti e nei processi di sicurezza a loro disposizione nel 2015 rispetto all'anno precedente. Ad esempio, nel 2015 il 59% delle aziende affermava che l'infrastruttura di sicurezza era all'avanguardia. Ma nel 2014 la stessa opinione era condivisa dal 64%. D'altro canto, la maggiore preoccupazione rispetto alla sicurezza spinge le aziende a migliorare le strategie di difesa.
- Lo studio comparativo indica che le piccole e medie imprese (PMI) utilizzano meno strumenti di difesa rispetto alle grandi imprese. Ad esempio, nel 2015 il 48% delle PMI ha dichiarato di utilizzare la sicurezza Web, rispetto al 59% del 2014. E il 29% ha dichiarato di utilizzare strumenti di patching e di configurazione nel 2015, rispetto al 39% del 2014. Questi punti deboli possono esporre a rischi i clienti delle PMI, poiché gli autori degli attacchi sono in grado di violare più facilmente le reti delle PMI.
- Da maggio 2015, Cisco ha ridotto la mediana dei tempi medi di rilevamento (time to detect o TTD) delle minacce note nelle reti a circa 17 ore, vale a dire meno di un giorno. Questo risultato supera di gran lunga l'attuale stima del settore sui tempi di rilevamento, che va dai 100 ai 200 giorni.

La posta in gioco: l'obiettivo dei criminali informatici moderni è il profitto economico

La posta in gioco: l'obiettivo dei criminali informatici moderni è il profitto economico

In passato molti criminali informatici si nascondevano nei meandri di Internet. Per eludere il rilevamento effettuavano solo brevi incursioni nelle reti aziendali per lanciare i propri attacchi. Oggi alcuni criminali informatici più audaci utilizzano risorse online legittime. Prosciugano la capacità dei server, sottraggono dati e richiedono il riscatto alle vittime online, di cui tengono i dati in ostaggio.

Queste campagne sono un aspetto preoccupante della guerra tra hacker e professionisti della sicurezza. Se gli autori degli attacchi trovano più posizioni online da cui operare, allora la forza di impatto può crescere in maniera esponenziale.

In questo report i ricercatori della sicurezza Cisco evidenziano le tattiche utilizzate dai malintenzionati per formare una solida infrastruttura e creare campagne più potenti ed efficaci. Gli hacker continuano ad adottare metodi sempre più vantaggiosi per incrementare i profitti e molti dedicano particolare attenzione allo sfruttamento delle risorse server.

L'enorme diffusione del ransomware (vedere **pagina 10**) è un esempio eclatante. Il ransomware assicura ai criminali un modo semplice per sottrarre più denaro direttamente dai singoli utenti. Le campagne che compromettono decine di migliaia di utenti al giorno, con poche o nessuna interruzione, possono generare guadagni sconcertanti. Oltre a sviluppare metodi più efficaci per finanziare le proprie campagne, gli hacker violano le risorse legittime per usarle come terreno di attacco.

I creatori di alcune varianti di ransomware nonché gli sviluppatori di exploit kit stanno gradualmente spostando il traffico su siti Web violati di WordPress per eludere il rilevamento e utilizzare lo spazio nel server (vedere **pagina 33**). Inoltre gli autori di SSHPsychos, una delle più importanti botnet individuate dai ricercatori Cisco, utilizzavano reti standard praticamente senza alcuna interferenza, fino a quando la collaborazione di Cisco e Level 3 Threat Research Labs non ha persuaso i provider di servizi a bloccare il traffico della botnet.

Intelligence sulle minacce

Intelligence sulle minacce

Per la redazione di questo report, Cisco ha raccolto e analizzato un campione di dati telemetrici a livello mondiale. La nostra ricerca e l'analisi continua delle minacce rilevate, come il traffico malware, possono aiutare a prevedere eventuali attacchi futuri e a individuare le nuove minacce.

Casi reali

La collaborazione del settore aiuta Cisco a bloccare gli exploit kit e le campagne di ransomware di grande portata

Angler è uno dei più imponenti ed efficaci exploit kit apparsi sul mercato. È stato collegato a numerosi malvertising di alto livello e a campagne di ransomware. È stato inoltre un fattore determinante per l'enorme diffusione a livello mondiale dell'attività di ransomware che i ricercatori Cisco hanno monitorato attentamente negli ultimi anni. I criminali utilizzano il ransomware per crittografare i file degli utenti, fornendo la chiave di decrittografia solo dopo il pagamento di un riscatto, solitamente di un importo compreso tra i 300 e i 500 dollari.

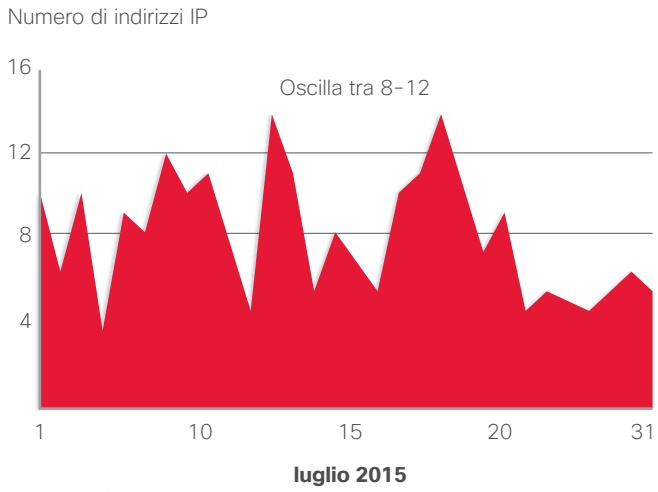
Come indicato nel Report semestrale di Cisco sulla sicurezza 2015, le criptovalute, come bitcoin, e le reti di anonimizzazione, come Tor, facilitano l'ingresso dei criminali informatici nel mercato del malware per realizzare profitti immediati. La diffusione del ransomware può essere collegata a due vantaggi principali: è un'operazione che richiede poca manutenzione da parte dei malintenzionati e garantisce un metodo veloce per guadagnare, perché gli utenti pagano gli hacker direttamente in criptovalute.

Con la ricerca su Angler e le tendenze del ransomware ad essa collegate, Cisco ha determinato che alcuni operatori dell'exploit kit stavano usando una percentuale straordinaria di server proxy in tutto il mondo, residenti su server gestiti da Limestone Networks. Questa modalità d'uso dei server è un esempio esemplificativo di un'altra tendenza osservata dai ricercatori nell'economia sommersa degli ultimi tempi: gli hacker mescolano insieme risorse legittime e dannose per condurre le loro campagne.

Nel caso specifico l'infrastruttura IP che supportava Angler non era grande. Il numero giornaliero di sistemi attivi era in genere compreso tra 8 e 12. La maggior parte era attiva solo per un giorno. La figura 1 mostra il numero di indirizzi IP univoci osservati da Cisco durante il mese di luglio 2015.

Cisco ha scoperto che gli operatori di Angler stavano muovendosi da un indirizzo IP all'altro in modo lineare per nascondere le attività di minaccia e prevenire eventuali ostacoli al loro sistema per arricchirsi.

Figura 1. Numero di indirizzi IP Angler per data a luglio 2015



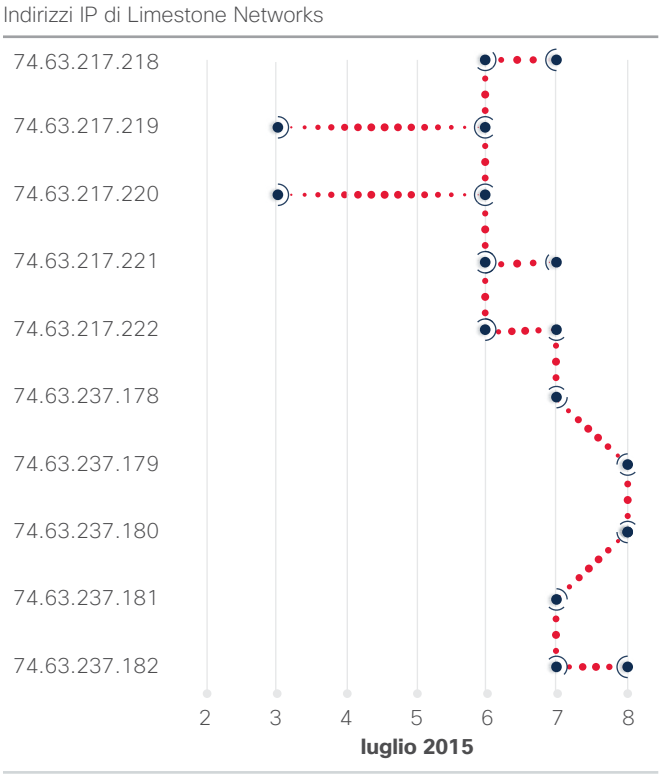
Fonte: Cisco Security Research

Come si può vedere nella figura 2, l'Angler inizia con un indirizzo IP (in questo caso, 74.63.217.218). Il sistema compromette gli utenti e allo stesso tempo genera elementi di disturbo che i responsabili della sicurezza iniziano a rilevare. A questo punto gli autori degli attacchi passano all'indirizzo IP adiacente (74.63.217.219). Questa attività prosegue attraverso blocchi quasi contigui di spazio IP di un unico provider di hosting.

Cisco ha esaminato le informazioni IP per identificare i numeri ASN e i provider associati agli indirizzi IP. Abbiamo determinato che la maggior parte del traffico correlato ad Angler aveva origine da server gestiti da due provider di hosting legittimi, Limestone Networks ed Hetzner (figura 3). I due provider nel mese di luglio erano responsabili di quasi il 75% del volume totale di traffico.

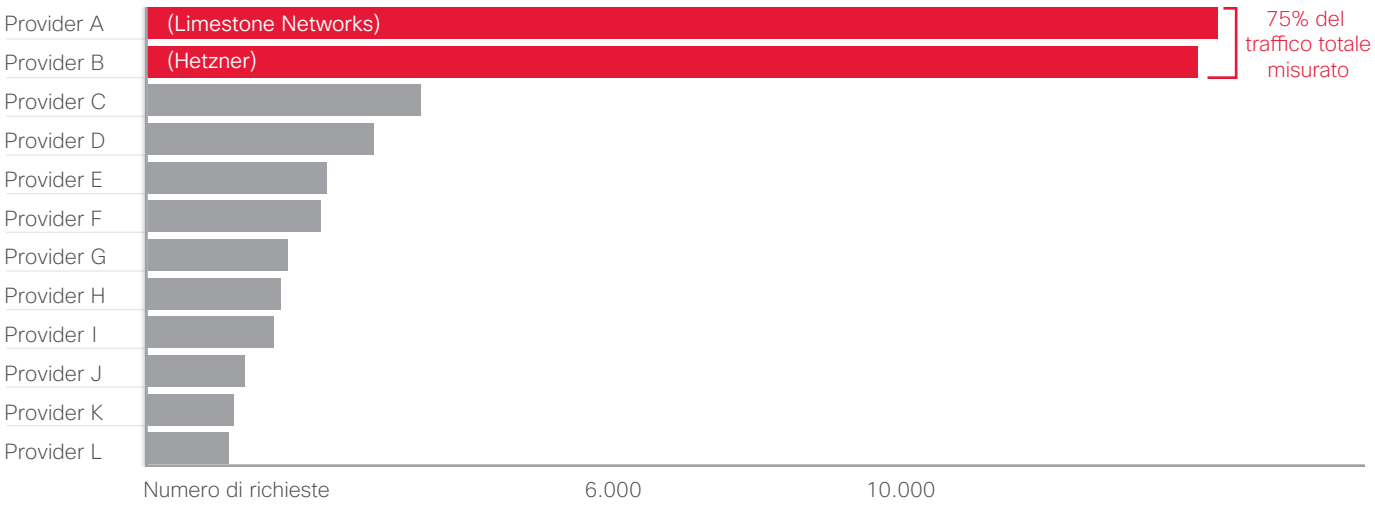
Cisco è entrata in contatto prima con Limestone Networks, che sembrava ospitare la parte più rilevante di Angler. Il provider si è subito reso disponibile a collaborare. L'azienda doveva far fronte ogni mese a un eccessivo numero di chargeback su carte di credito (storno di transazione) perché gli hacker utilizzavano nomi e carte di credito fraudolenti per acquistare batch casuali dei server del valore di migliaia di dollari.

Figura 2. Infrastruttura IP minima in grado di supportare Angler



Fonte: Cisco Security Research

Figura 3. Richieste HTTP di Angler per provider a luglio 2015



Fonte: Cisco Security Research

Questo sistema di acquisto dei server rendeva difficile associare l'attività fraudolenta a un singolo autore. Ad esempio, il criminale un giorno potrebbe acquistare tre o quattro server e il giorno successivo usare un nome e una carta di credito diversi per acquistarne altri tre o quattro. In questo modo gli hacker potevano passare da un indirizzo IP all'altro quando i server compromessi venivano identificati e messi offline dagli addetti alla sicurezza.

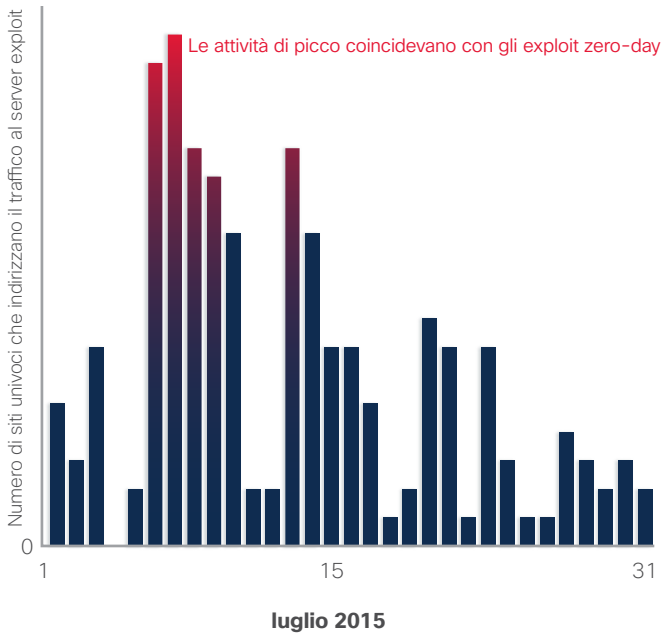
Per analizzare questa attività, Cisco si è avvalso dell'aiuto di Level 3 Threat Research Labs e di OpenDNS, un'azienda Cisco. Level 3 Threat Research Labs è stata in grado di fornire una visione globale più ampia della minaccia, consentendo a Cisco di approfondirne la portata e il livello di impatto nella fase di picco. OpenDNS da parte sua ha esaminato un aspetto specifico delle attività dei domini associati alle minacce, fornendo a Cisco una visione più completa delle tecniche introdotte dai malintenzionati, quali il domain shadowing.

I ricercatori Cisco hanno quindi esaminato in dettaglio le modalità con cui gli utenti si imbattevano in Angler, ricevendo payload dannosi. Sono stati individuati siti Web molto diffusi che reindirizzavano gli utenti all'Angler exploit kit mediante malvertising. I falsi annunci erano inseriti in centinaia di importanti siti informativi, immobiliari e di cultura di massa. Questi siti vengono comunemente ritenuti sicuri nella community degli esperti della sicurezza.

I ricercatori Cisco hanno inoltre rilevato innumerevoli esempi di piccoli siti Web apparentemente non associati che utilizzavano lo stesso tipo di reindirizzamento, incluso un necrologio pubblicato da un piccolo quotidiano rurale negli Stati Uniti. Molto probabilmente quest'ultima strategia era destinata a colpire gli utenti anziani. Questo segmento di popolazione in genere è più abituata a utilizzare browser Web predefiniti come Microsoft Internet Explorer e probabilmente non sono consapevoli della necessità di aggiornare regolarmente Adobe Flash per rimediare alle vulnerabilità.

Un altro aspetto importante da notare di questa operazione Angler era il numero di riferimenti univoci e la bassa frequenza con cui venivano usati (figura 4). Dai risultati è emerso che più di 15.000 siti univoci reindirizzavano gli utenti all'Angler exploit kit, il 99,8% dei quali è stato utilizzato meno di 10 volte. La maggior parte di riferimenti era quindi attivo solo per un breve periodo di tempo e i riferimenti venivano rimossi dopo aver colpito un numero limitato di utenti. Nell'analisi di luglio 2015 è stato notato che i picchi di attività coincidevano con vari exploit zero-day Hacking Team (CVE-2015-5119, CVE-2015-5122).[1]

Figura 4. Riferimenti univoci per giorno a luglio 2015

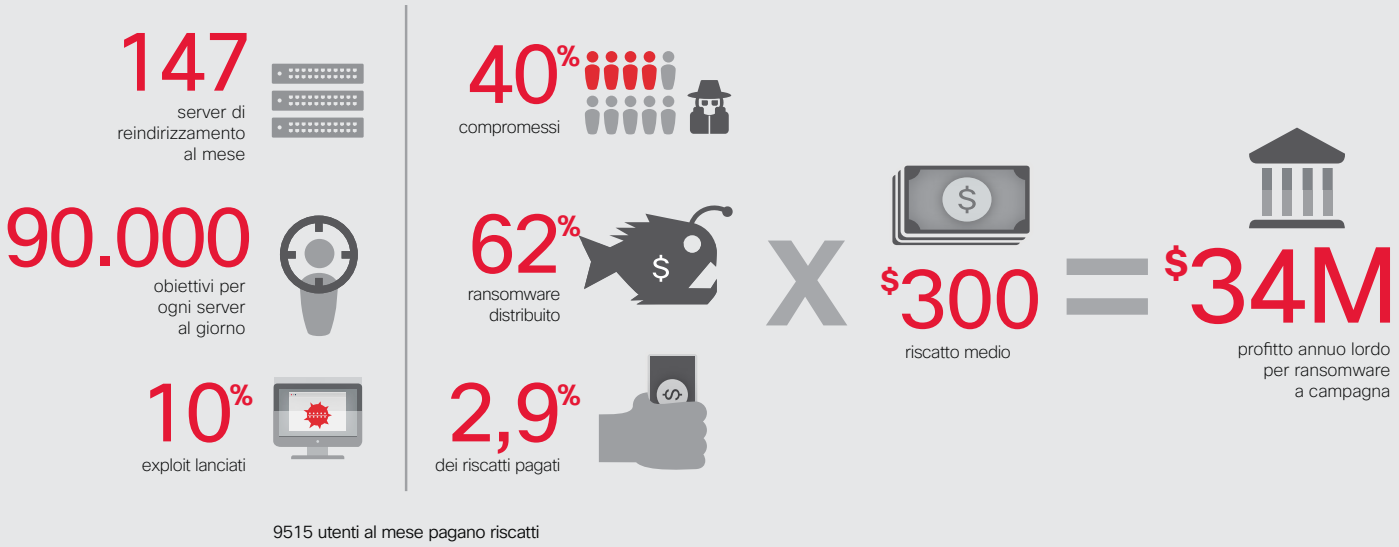


Fonte: Cisco Security Research

Cisco ha stabilito che circa il 60% dei payload Angler diffusi mediante questa specifica operazione diffondevano un tipo di variante del ransomware, nella maggior parte dei casi Cryptowall 3.0. Altri tipi di payload includevano Bedep, un downloader di malware comunemente usato per installare malware di campagne di clic fraudolenti. Vedere "Infezioni dei browser: un problema diffuso e una delle cause principali della sottrazione di dati" **pagina 16**. Entrambi i tipi di malware sono progettati per consentire agli autori di attacchi di ricavare molto denaro dagli utenti compromessi molto velocemente e con il minimo sforzo.

[1] "Adobe Patches Hacking Team's Flash Player Zero-Day," di Eduard Kovacs, *SecurityWeek*, 8 luglio 2015: **http://www.securityweek.com/adobe-patches-hacking-teams-flash-player-zero-day**.

Profitti di Angler



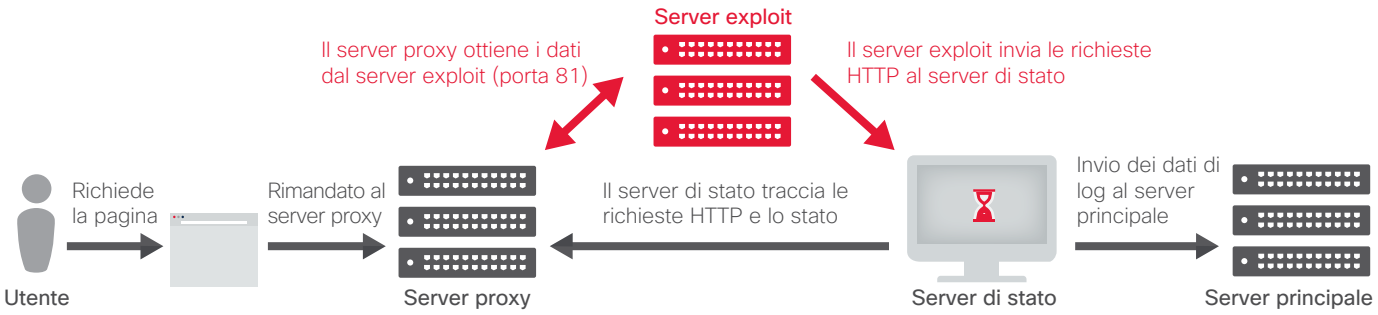
Fonte: Cisco Security Research

Secondo la ricerca Cisco, il principale autore responsabile di circa la metà dell'attività di Angler exploit kit in questa particolare campagna era in grado di colpire fino a 90.000 vittime al giorno. Secondo la nostra stima, la campagna stava fruttando agli autori degli attacchi più di 30 milioni di dollari all'anno.

CONDIVIDI

Presumibilmente la rete infetta di Hetzner aveva una simile percentuale di successo. Ciò significa che il responsabile di questa operazione che ha colpito i server di Limestone Networks ed Hetzner era anche responsabile di metà dell'attività Angler globale al momento dell'analisi condotta da Cisco. I ricercatori Cisco stimano che questa operazione fosse in grado di generare un reddito lordo di 60 milioni di dollari l'anno.

Figura 5. Infrastruttura di back-end di Angler



Fonte: Cisco Security Research

Cisco ha inoltre scoperto che i server a cui si collegavano gli utenti in realtà non ospitavano alcuna attività Angler dannosa, ma fungevano solo da veicolo. L'utente entrava nella catena di reindirizzamento e inviava una richiesta GET per una pagina di destinazione, che indirizzava al server proxy. Il server proxy instradava il traffico a un server exploit ubicato in un altro paese e gestito da un altro provider. Durante la ricerca è emerso che un unico server exploit era associato a più server proxy (vedere la figura 5).

Cisco ha individuato un server di stato che gestiva attività quali il monitoraggio dell'integrità. Ogni singolo server proxy monitorato dal server di stato disponeva di un paio di URL univoci. Se veniva eseguita la query del percorso, il server di stato restituiva un messaggio con codice di stato HTTP "204". Gli autori degli attacchi potevano identificare in modo univoco ogni server proxy e assicurarsi non solo che fosse operativo, ma anche che i responsabili della sicurezza non lo avessero messo fuori uso. Utilizzando l'altro URL, gli hacker potevano raccogliere i log del server proxy e determinare il grado di efficienza della propria rete.

La collaborazione del settore è stata determinante per l'opportunità di Cisco di analizzare l'attività dell'Angler exploit kit. Ha consentito infine di interrompere i reindirizzamenti ai server proxy Angler su un provider di servizi statunitense e di portare alla luce un'attività di crimine informatico estremamente sofisticata che stava colpendo migliaia di utenti ogni giorno.

Cisco ha collaborato strettamente con Limestone Networks per identificare i nuovi server non appena messi online, monitorandoli attentamente per assicurarsi che venissero bloccati. Qualche tempo dopo gli hacker hanno abbandonato Limestone Networks ed è seguito un calo generale di attività Angler.

Per ulteriori informazioni su come Cisco sia riuscita a eliminare una notevole fonte di proventi internazionali generati dall'Angler exploit kit, leggere il post del blog Cisco sulla sicurezza "**Threat Spotlight: Cisco Talos Thwarts Access to Massive International Exploit Kit Generating $60M Annually from Ransomware Alone**".

Un'operazione coordinata consente di bloccare una delle più grandi botnet DDoS di Internet

Le tecnologie per la difesa integrata dalle minacce spesso consentono di bloccare gli attacchi di ampia portata prima che compromettano le reti aziendali. In molti casi, tuttavia, contrastare un attacco su vasta scala richiede non solo strumenti di difesa tecnologici, ma anche il coordinamento tra provider di servizi, fornitori di servizi di sicurezza e organizzazioni del settore.

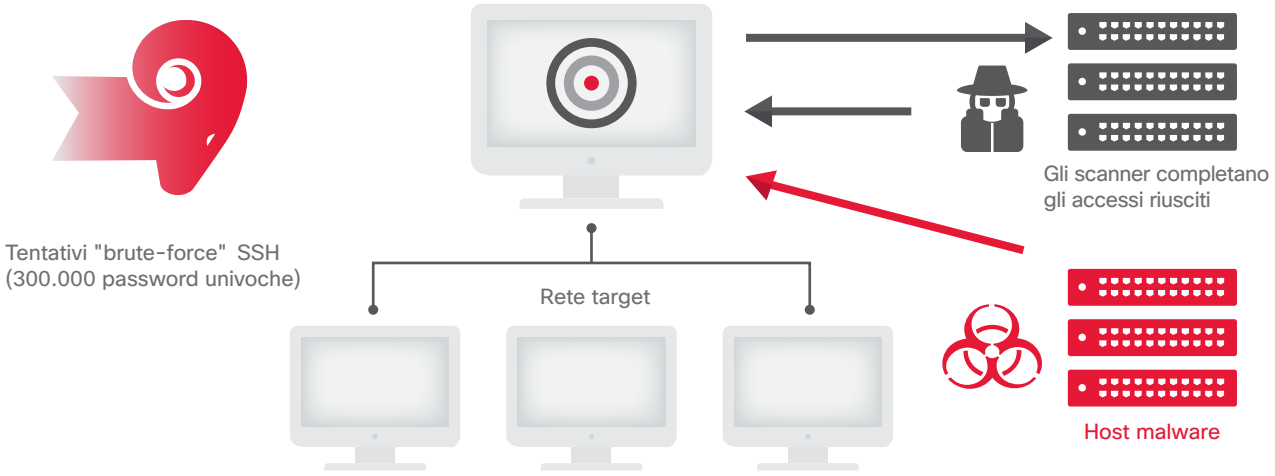
I criminali informatici si dimostrano sempre più determinati a generare profitti con le loro attività, perciò il settore tecnologico deve migliorare le strategie di collaborazione per sventare le campagne criminali. SSHPsychos (detto anche Group 93) è una delle più grandi botnet DDoS mai individuate dai ricercatori della sicurezza Cisco ed è stata significativamente indebolita in seguito alla collaborazione di Cisco con Level 3 Threat Research Labs.

UNA MINACCIA STRAORDINARIA

La rete DDoS SSHPsychos è una minaccia straordinaria per diversi motivi. Poiché utilizza decine di migliaia di computer distribuiti su Internet, ha la potenza necessaria per lanciare un attacco DDoS (distributed denial of service) che non può essere contrastato a livello dei singoli dispositivi. In questo caso, la botnet era stata creata utilizzando attacchi di tipo "brute-force" che coinvolgevano il traffico SSH (Secure Shell) (figura 6). Il protocollo SSH viene utilizzato per consentire comunicazioni sicure e viene generalmente utilizzato per l'amministrazione remota dei sistemi. Secondo l'analisi di Cisco e Level 3 a volte SSHPsychos era responsabile di più del 35% del traffico SSH globale su Internet (figura 7).

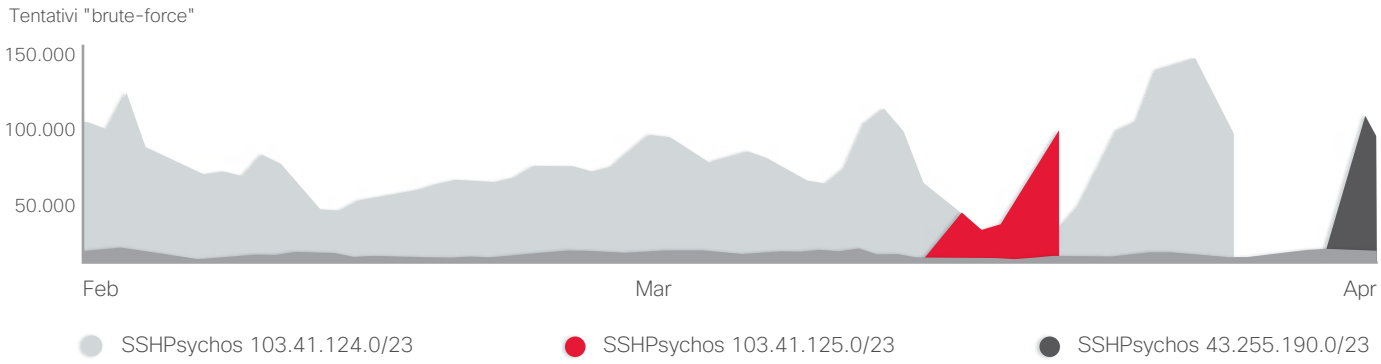
SSHPsychos è operativo in due paesi: Cina e Stati Uniti. I tentativi di accesso "brute-force", che utilizzano 300.000 password univoche, avevano origine da un provider di servizi di hosting con sede in Cina. Quando gli hacker riuscivano ad accedere indovinando la password radice corretta, gli attacchi "brute-force" cessavano. Ventiquattro ore più tardi gli hacker accedevano da un indirizzo IP negli Stati Uniti e installavano un rootkit DDoS sul computer colpito. Si trattava chiaramente di una tattica per eludere la diffidenza degli amministratori di rete. Gli obiettivi della botnet variavano, ma in molti casi sembravano essere i grandi provider di servizi Internet (ISP).

Figura 6. SSHPsychos utilizza gli attacchi "brute-force"



Fonte: Cisco Security Research

Figura 7. Nel periodo di picco, SSHPsychos era responsabile del 35% del traffico Internet mondiale



Fonte: Cisco Security Research

COLLABORAZIONE CON GLI ESPERTI DELLA SICUREZZA

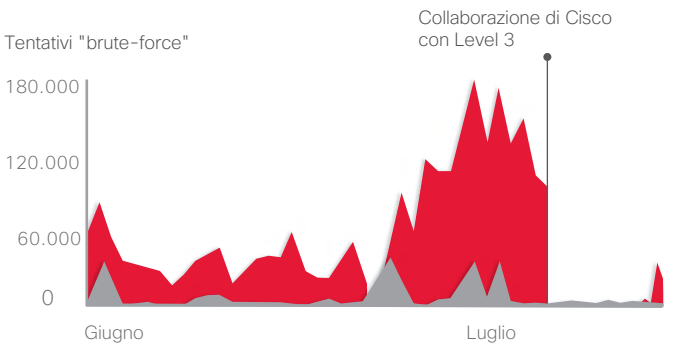
A causa della portata della rete DDoS, i nostri ricercatori ritenevano che il danno sarebbe stato difficile da contenere. Era essenziale lavorare in tandem con un'organizzazione in grado di eliminare il gruppo responsabile degli attacchi "brute-force" da Internet in modo efficace. Tuttavia i provider di servizi di backbone sono riluttanti a filtrare i contenuti dei clienti.

Cisco ha quindi contattato Level 3 Threat Research Labs. Level 3 ha analizzato il traffico a livello del netblock, vale a dire l'intervallo di indirizzi IP, dove si riteneva risiedesse SSHPsychos (103.41.124.0/23), confermando che nessun traffico legittimo proveniva o era diretto a tale indirizzo. Ha quindi rimosso il traffico ("null route") all'interno delle proprie reti. Successivamente ha contattato i provider di servizi responsabili dei domini chiedendo loro di rimuovere il traffico di rete.

I risultati di questa azione sono stati immediatamente visibili (figura 8). La rete originale non presentava quasi alcuna nuova attività. Una nuova rete del netblock 43.255.190.0/23 mostrava però elevati volumi di traffico di attacchi "brute-force" SSH ed era stato riscontrato lo stesso comportamento già associato a SSHPsychos. In seguito a questa ricomparsa improvvisa di traffico simile a SSHPsychos, Cisco e Level 3 hanno deciso di intervenire su 103.41.124.0/23 e anche sul nuovo netblock 43.255.190.0/23.

Il blocco dei netblock utilizzati da SSHPsychos non ha disabilitato in modo permanente la rete DDoS, ma ha sicuramente limitato la capacità dei suoi creatori di eseguire le operazioni, impedendo allo stesso tempo la diffusione di SSHPsychos su altri computer, almeno temporaneamente.

Figura 8. Il traffico SSHPsychos diminuisce drasticamente dopo l'intervento



Fonte: Cisco Security Research

Il settore della sicurezza deve avvalersi della collaborazione per fronteggiare minacce di ampia portata come SSHPsychos. I provider di domini, gli ISP, i provider di servizi di hosting, i resolver DNS e i fornitori leader di soluzioni di sicurezza non possono limitarsi a osservare quando i criminali informatici lanciano i propri attacchi su reti che dovrebbero essere destinate esclusivamente al traffico legittimo. In altre parole, quando i criminali generano un traffico dannoso in maniera più o meno visibile, il settore deve rimuovere i percorsi di accesso a tali reti legittime.

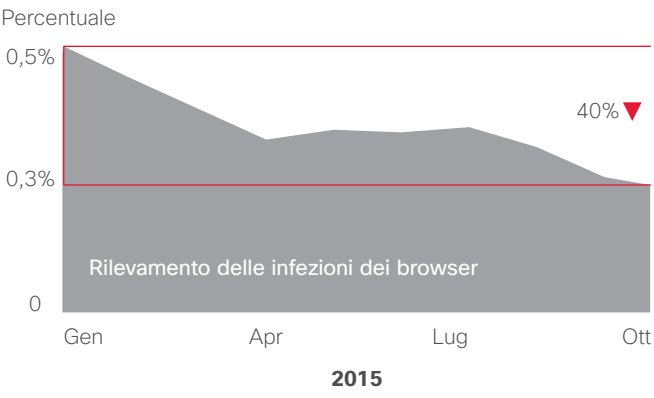
Per ulteriori informazioni sulla reazione di Cisco e Level 3 Threat Research Labs alla minaccia di SSHPsychos, leggere il post del blog Cisco sulla sicurezza "**Threat Spotlight: SSHPsychos**".

Infezioni dei browser: un problema diffuso e una delle cause principali della sottrazione di dati

I team responsabili della sicurezza spesso considerano i componenti aggiuntivi dei browser come una minaccia a basso rischio. Tuttavia il monitoraggio di tali componenti dovrebbe assumere una priorità più alta per poter individuare e correggere rapidamente questo tipo di infezioni.

La nostra ricerca infatti indica che le infezioni del browser sono molto più diffuse di quanto molte aziende possano immaginare. Da gennaio a ottobre 2015 abbiamo esaminato 26 famiglie di componenti aggiuntivi dannosi per browser (figura 9). Osservando i dati delle infezioni dei browser durante questi mesi, il numero di infezioni è apparso essere generalmente in calo.

Figura 9. Infezioni dei browser da gennaio a ottobre 2015



Fonte: Cisco Security Research

Questi dati sono tuttavia ingannevoli. Il volume di traffico HTTPS durante i mesi in esame ha reso difficile identificare gli indicatori di compromissione solitamente associati alle 26 famiglie monitorate, perché le informazioni URL non erano visibili a causa della crittografia. Per ulteriori informazioni sulla crittografia e sulle problematiche che presenta per la sicurezza, vedere "Crittografia: una tendenza in crescita e una sfida per gli addetti alla sicurezza", **pagina 30**.

Le estensioni dannose per i browser possono sottrarre informazioni e provocare la sottrazione di dati. Ogni volta che un utente apre una nuova pagina Web con un browser compromesso, le estensioni dannose procedono alla raccolta di dati. Queste sono in grado di esfiltrare molto più che i dettagli di base riguardanti ciascuna pagina Web interna o esterna visitata dall'utente, sono anche in grado di raccogliere informazioni estremamente riservate incorporate nell'URL. Tali informazioni possono includere le credenziali utente, i dati dei clienti e i dettagli sulle API e l'infrastruttura interna di un'azienda.

Le estensioni dannose per i browser vengono distribuite mediante pacchetti software o adware. Sono progettate per generare profitti sfruttando gli utenti in vari modi. In un browser infetto possono indurre gli utenti a fare clic su malvertising, come annunci o popup. Possono inoltre distribuire malware convincendo gli utenti a fare clic su un link compromesso o a scaricare un file infetto presente nel malvertising. Inoltre possono intercettare le richieste browser degli utenti e quindi inserire pagine Web dannose nelle pagine dei risultati del motore di ricerca.

Tra le 45 aziende del nostro campione, abbiamo rilevato che ogni mese oltre l'85% delle aziende è stato colpito da estensioni dannose per i browser, un risultato che sottolinea la vasta portata di queste operazioni. Poiché i browser infetti vengono spesso considerati una minaccia di minore entità, è possibile che non vengano rilevati o corretti per giorni o anche più a lungo, offrendo ai malintenzionati più tempo e opportunità di condurre le proprie campagne (vedere "Rilevamento: la corsa contro il tempo", **pagina 60**).

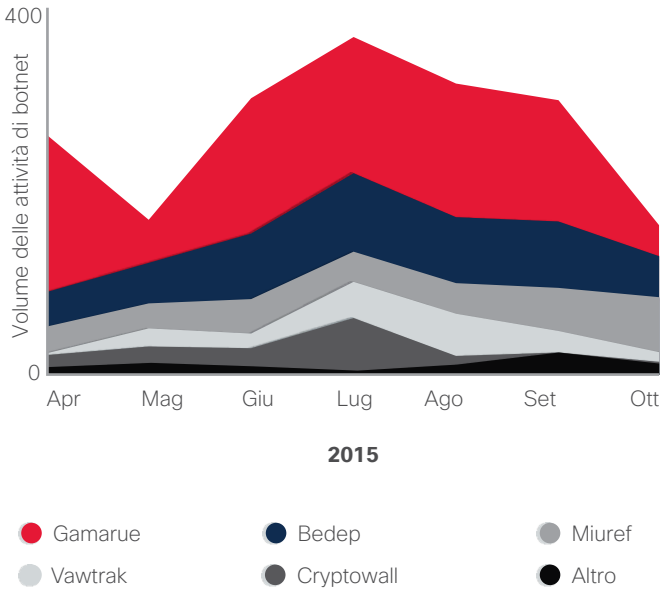
Il nostro suggerimento per i team della sicurezza è quindi che vale la pena dedicare più tempo e più risorse al monitoraggio di questo rischio e di prendere in considerazione l'automazione per assegnare la giusta priorità alle minacce.

Attività di comando e controllo delle botnet: panoramica globale

Le botnet sono reti di computer infettati da malware. Gli hacker possono controllarli in gruppo e gestirli per svolgere una specifica attività, ad esempio inviare spam o lanciare un attacco DDoS. Da anni stanno aumentando sia di dimensioni che di numero. Per avere una panoramica migliore delle minacce a livello mondiale, sono state analizzate le reti di 121 aziende da aprile a ottobre 2015 per identificare una o più delle otto botnet più comuni. I dati sono stati normalizzati per fornire una panoramica generale delle attività botnet (figura 10).

È emerso che nel corso di questo periodo la minaccia di tipo comando e controllo più diffusa era rappresentata da Gamarue, un programma di intercettazione di informazioni modulare e multifunzione in uso da anni.

Figura 10. Aumento delle minacce individuali (rapporto degli utenti infettati)



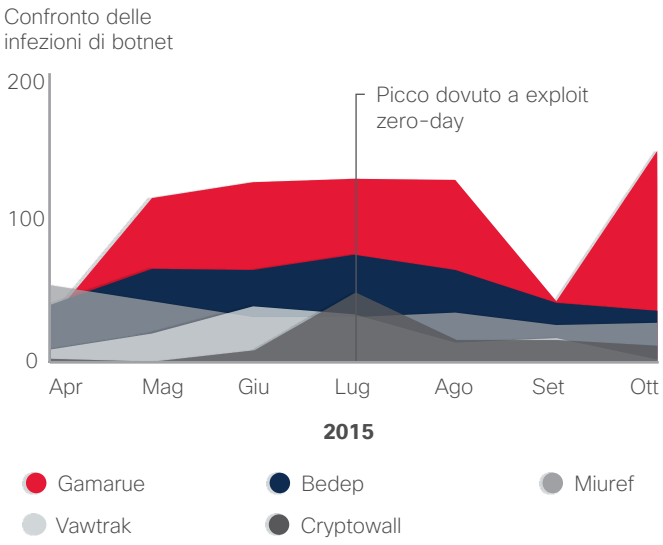
Fonte: Cisco Security Research

Una picco significativo del numero di infezioni in cui era coinvolto il ransomware Cryptowall 3.0 è stato identificato a luglio. Questa attività viene attribuita in gran parte all'Angler exploit kit, che notoriamente distribuisce il payload Cryptowall. Come indicato nel Report semestrale di Cisco sulla sicurezza 2015, gli autori di Angler e di altri exploit kit hanno approfittato dei ritardi nell'applicazione di patch di Adobe Flash. Hanno infatti agito nel periodo di tempo intercorrente tra il rilascio di un aggiornamento di Adobe e l'applicazione effettiva da parte degli utenti.[2] I ricercatori Cisco attribuiscono il picco di luglio 2015 all'attacco Flash zero-day CVE-2015-5119 annunciato in connessione con la violazione subita da Hacking Team.[3]

Angler exploit kit diffonde anche il Trojan Bedep che viene utilizzato per condurre campagne di clic fraudolenti. Durante il mese di luglio è stata notato anche un leggero aumento della prevalenza di questa minaccia (figura 11).

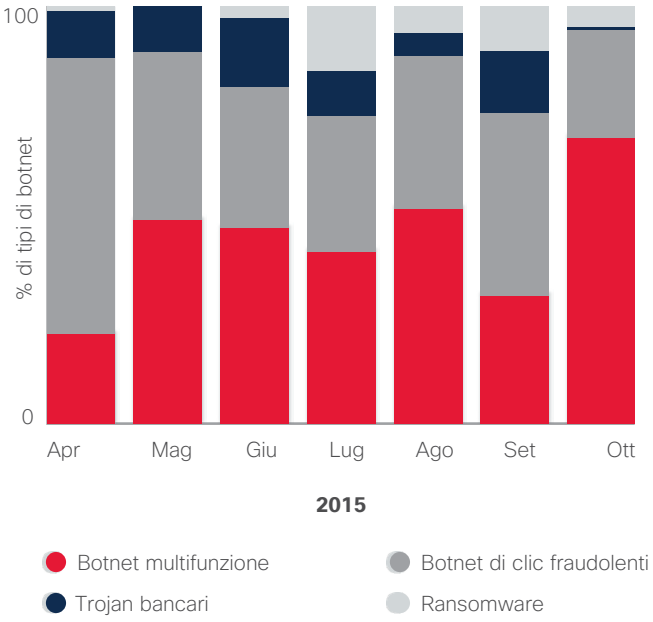
Bedep, Gamarue e Miuref (un altro Trojan e hijacker del browser in grado di eseguire clic fraudolenti) rappresentavano insieme più del 65% delle attività di comando e controllo botnet nella base utenti presa in esame.

Figura 11. Dati mensili sulle minacce in base al numero di utenti infetti



Fonte: Cisco Security Research

Figura 12. Dati mensili sulle minacce in base alle categorie



Fonte: Cisco Security Research

La percentuale di infezioni Bedep è rimasta relativamente stabile durante il periodo analizzato. È stata tuttavia osservata una riduzione sensibile delle infezioni Miuref. Ciò è attribuibile all'aumento del traffico HTTPS, che ha contribuito a nascondere gli indicatori di compromissione di Miuref.

La figura 12 mostra i tipi di botnet responsabili delle maggior parte delle infezioni durante l'intervallo di tempo monitorato. Le botnet multifunzione come Gamarue e Sality sono le minacce maggiori, seguite dalle botnet di clic fraudolenti. I Trojan bancari si sono classificati al terzo posto, indicando che questo tipo di minaccia, seppur non recente, sia ancora molto diffusa.

[2] Report semestrale di Cisco sulla sicurezza 2015: **http://www.cisco.com/web/offers/lp/2015-midyear-security-report/index.html**.
[3] "Adobe Patches Hacking Team's Flash Player Zero-Day," di Eduard Kovacs, *SecurityWeek*, 8 luglio 2015: **http://www.securityweek.com/adobe-patches-hacking-teams-flash-player-zero-day**.

Il punto debole del DNS: gli attacchi che usano DNS per comando e controllo

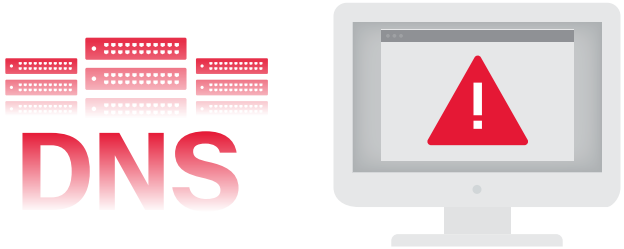
L'analisi di Cisco del malware ritenuto "notoriamente dannoso" ha rilevato che la maggior parte, pari al 91,3%, sfrutta il servizio DNS in uno dei tre seguenti modi:

- per ottenere comando e controllo
- per esfiltrare i dati
- per reindirizzare il traffico.

Per giungere a questa percentuale, abbiamo analizzato tutti i comportamenti campione tratti dalla nostra vasta gamma di sandbox. Non è stato incluso nel campione dell'analisi il malware che certamente non usava DNS in alcun modo o che si limitava ad usarlo per "controlli di integrità". Il malware restante utilizzava il DNS per connettersi a siti che sono stati ritenuti dannosi o considerati sospetti.

Nonostante gli hacker facciano affidamento sul DNS per condurre le campagne malware, sono poche le aziende che eseguono il monitoraggio del DNS per ragioni di sicurezza o che almeno eseguano un minimo di monitoraggio. Questa mancanza di controllo rende DNS il veicolo ideale per gli hacker. Secondo un nostro recente sondaggio (vedere la figura 13), il 68% degli esperti della sicurezza dichiara che le aziende in cui lavorano non monitorano le minacce da DNS ricorsivo (i nameserver di DNS ricorsivi forniscono gli indirizzi IP dei nomi di dominio previsti agli host richiedenti).

Figura 13. Monitoraggio delle minacce da DNS ricorsivo



Fonte: Cisco Security Research

Perché il DNS è diventato un punto debole della sicurezza di tante aziende? Una dei motivi principali è che i team della sicurezza e gli esperti di DNS in genere lavorano in gruppi IT differenti in azienda e non interagiscono frequentemente.

Ma dovrebbero farlo. Il monitoraggio del DNS è essenziale per individuare e contenere le infezioni malware che già utilizzano DNS per una delle tre attività elencate in precedenza. È inoltre un primo passo importante per la mappatura di altri componenti che possono essere utilizzati per analizzare l'attacco in modo più approfondito, ad esempio per determinare il tipo di infrastruttura che ha favorito l'attacco o per risalirne all'origine.

Il monitoraggio del DNS comporta tuttavia più di una semplice collaborazione tra i team della sicurezza e del DNS. È necessario ricorrere alle tecnologie e alle competenze appropriate per l'analisi dei rapporti di correlazione. Per ulteriori informazioni, vedere "La collaborazione del settore aiuta Cisco a bloccare gli exploit kit e le campagne di ransomware di grande portata" a **pagina 10** per scoprire come OpenDNS ha aiutato Cisco a ottenere maggiore visibilità sugli IP utilizzati dall'Angler exploit kit.

ANALISI RETROSPETTIVA DEL DNS

L'analisi retrospettiva di Cisco delle query DNS e del conseguente traffico TCP e UDP ha consentito di individuare una serie di sorgenti di malware. Fra queste ci sono i server di comando e controllo, i siti Web e i punti di distribuzione. La ricerca retrospettiva ha rilevato inoltre contenuti con minacce di livello elevato grazie all'uso di informazioni tratte dagli elenchi delle minacce, i report delle community, le tendenze osservate nelle violazioni informatiche e la conoscenza delle specifiche vulnerabilità di un determinato settore.

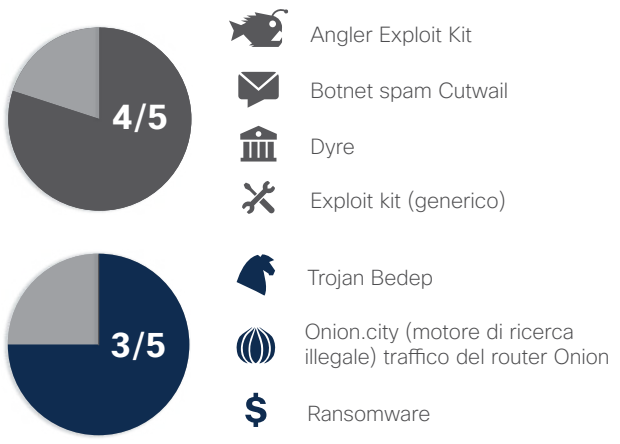
L'analisi retrospettiva aiuta a identificare i tentativi di esfiltrazione dei dati di livello basso e lenti, comunemente associati alle minacce avanzate persistenti (Advanced Persistent Threat, ATP) e che spesso sfuggono alle tradizionali tecnologie di rilevamento. L'obiettivo dell'analisi è identificare le anomalie nell'ambito dell'elevato volume di traffico delle comunicazioni in uscita. Questo approccio di analisi consente di individuare possibili violazioni di dati e attività di rete dannose che altrimenti potrebbero sfuggire.

In questo modo sono stati scoperti resolver DNS non autorizzati nella rete dei clienti. I clienti non erano consapevoli che i resolver venivano utilizzati dai dipendenti come elemento dell'infrastruttura DNS. L'incapacità di gestire e monitorare attivamente l'uso di resolver DNS può causare comportamenti dannosi come l'infezione della cache DNS e il reindirizzamento DNS.

Oltre a rilevare e identificare i resolver DNS non autorizzati, l'indagine retrospettiva ha anche scoperto i seguenti problemi nelle reti dei clienti:

- spazio degli indirizzi del cliente rilevato su blocklist di spam e malware di terze parti
- beaconing dello spazio degli indirizzi del cliente per i noti server di comando e controllo Palevo e Zeus
- campagne di malware attive, tra le quali CTB-Locker, Angler e DarkHotel
- attività sospetta, compreso l'utilizzo di Tor, l'inoltro automatico di e-mail e la conversione di documenti online
- tunneling DNS pervasivo su domini registrati in Cina
- "typosquatting" di DNS[4]
- clienti interni che eludono l'infrastruttura DNS attendibile del cliente.

Esaminando un campione selezionato di clienti Cisco Custom Threat Intelligence in più settori verticali, sono stati riscontrati anche i seguenti tipi di malware nelle rispettive percentuali di clienti totali analizzati:



[4] Il typosquatting è la pratica di registrare un dominio con un nome simile a un nome dominio esistente. Si tratta di una strategia utilizzata dagli hacker per colpire gli utenti che potrebbero inavvertitamente digitare nomi di dominio errati.

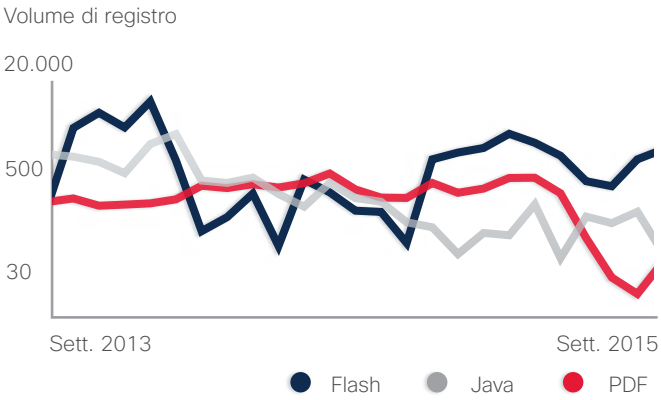
Analisi dell'intelligence sulle minacce

Vettori di attacco nel Web

ADOBE FLASH: UN DECLINO LENTO

Nonostante nell'ultimo anno abbiamo assistito a una riduzione del volume complessivo di applicazioni Flash (vedere la sezione successiva, **"Tendenze dei contenuti Adobe Flash e PDF"**), rimane sempre uno degli strumenti preferiti dagli sviluppatori di exploit kit. Di fatto nel 2015 non è stata riscontrata alcuna tendenza significativa, né in aumento né in diminuzione, del malware Flash (figura 14). È probabile che il malware correlato a Flash rimanga ancora per qualche tempo un vettore primario di attacco. Va inoltre notato che gli autori dell'Angler exploit kit prendono di mira le vulnerabilità Flash.

Figura 14. Analisi biennale della quota dei vettori di attacco



Fonte: Cisco Security Research

La pressione posta dal settore per la rimozione di Adobe Flash dall'esperienza di navigazione Web sta portando a una riduzione del volume di contenuti Flash (vedere la sezione successiva, **"Tendenze dei contenuti Adobe Flash e PDF"**). Vi sono analogie con quanto riscontrato nei contenuti Java degli ultimi anni e che ha portato a sua volta a una costante diminuzione dei volumi di malware Java. Gli autori di Angler non includono nemmeno più exploit Java. Nel frattempo, il volume di malware PDF è rimasto sostanzialmente invariato.

Anche Microsoft Silverlight ha perso importanza come vettore di attacco, perché molti fornitori hanno interrotto il supporto per le API utilizzate da Silverlight per l'integrazione nei browser. Molte aziende stanno passando da Silverlight a tecnologie basate su HTML5. Microsoft non prevede di rilasciare una nuova versione di Silverlight in futuro e attualmente sta rilasciando solo aggiornamenti relativi alla sicurezza.

TENDENZE DEI CONTENUTI ADOBE FLASH E PDF

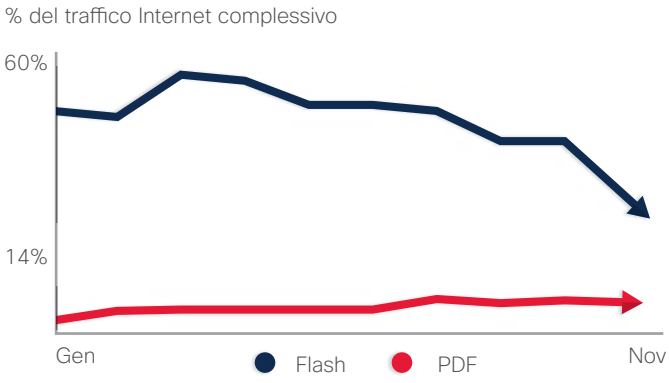
I ricercatori Cisco hanno osservato una generale riduzione del volume di contenuti Adobe Flash sul Web (figura 15). Le recenti azioni intraprese da Amazon, Google e altri protagonisti del panorama Internet sono state determinanti per la riduzione dei contenuti Flash. Queste aziende non accettano più pubblicità Web che utilizzi Flash, che eventualmente viene bloccata.

I contenuti PDF invece sono rimasti sostanzialmente stabili nell'ultimo anno e probabilmente rimarranno tali. Tuttavia non sono più un importante vettore di attacco da un po' di tempo.

È probabile che la riduzione dei contenuti Flash continui nel breve termine, e forse anche che subisca un'accelerazione, considerando che Adobe ha annunciato che Flash verrà eliminato gradualmente.[5] Probabilmente ci vorrà un po' di tempo prima che i contenuti Flash spariscano completamente. Flash è integrato in browser come Google Chrome, Microsoft Internet Explorer e Microsoft Edge ed è ancora ampiamente utilizzato nei contenuti Web, inclusi contenuti video e giochi.

Nei prossimi anni tuttavia con l'adozione di nuove tecnologie (come HTML5 e piattaforme mobili), la tendenza a lungo termine per i vettori di attacco Web come Java, Flash e Silverlight è sempre più ovvia. Col tempo saranno sempre meno diffusi. Di conseguenza è probabile che diventino vettori meno allettanti per i malintenzionati che puntano al profitto e preferiscono concentrarsi su vettori che consentano loro di compromettere facilmente ampie fasce di utenti e realizzare profitti rapidamente.

Figura 15. Percentuale di traffico complessivo per Flash e PDF

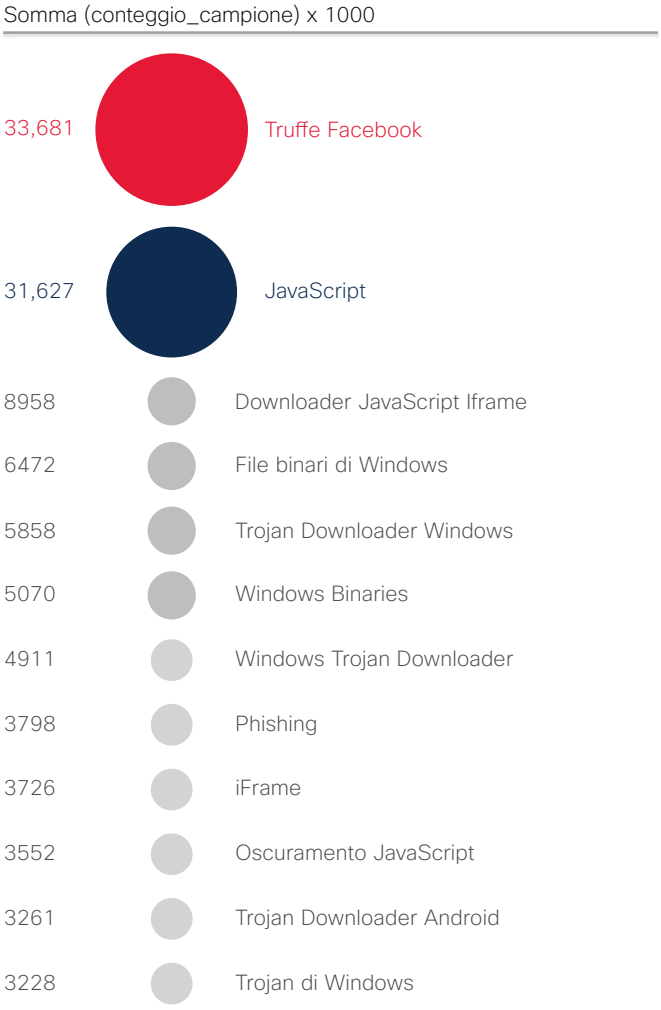


Fonte: Cisco Security Research

Metodi di attacco nel Web

Le figure 16 e 17 mostrano i vari tipi di malware che i criminali informatici utilizzano per accedere alle reti aziendali. La figura 16 illustra il malware più usato: adware, spyware, reindirizzamenti dannosi, exploit iFrame e phishing.

Figura 16. Malware più comuni



Fonte: Cisco Security Research

[5] "Adobe News: Flash, HTML5 and Open Web Standards", Adobe, 30 novembre 2015: **http://blogs.adobe.com/conversations/2015/11/flash-html5-and-open-web-standards.html**.

La figura 16 indica i tipi di malware che i criminali utilizzano per ottenere l'accesso iniziale. Questi sono i metodi comprovati e più convenienti per la compromissione di ampie fasce di utenti con relativa facilità. Secondo la nostra ricerca, gli exploit JavaScript e le truffe Facebook (social engineering) sono stati i metodi di attacco utilizzati più frequentemente.

La figura 17 mostra il volume inferiore di malware. Si noti che "volume inferiore" non significa "meno efficace". Secondo Cisco Security Research, il malware con volume contenuto può rappresentare minacce emergenti o campagne altamente mirate.

Molte di queste tecniche più complesse sono progettate per sottrarre il massimo possibile dagli utenti compromessi. Sono usate per rubare dati di elevato valore o sottrarre le risorse digitali degli utenti in cambio di un riscatto.

Di conseguenza, quando si monitora il malware Web non è sufficiente concentrarsi sui tipi di minacce che si riscontrano più comunemente, ma occorre considerare la serie completa degli attacchi.

Figura 17. Campione di malware a più basso volume osservato

Fonte: Cisco Security Research

Aggiornamenti sulle minacce

ADOBE FLASH ANCORA IN CIMA ALL'ELENCO DELLE VULNERABILITÀ

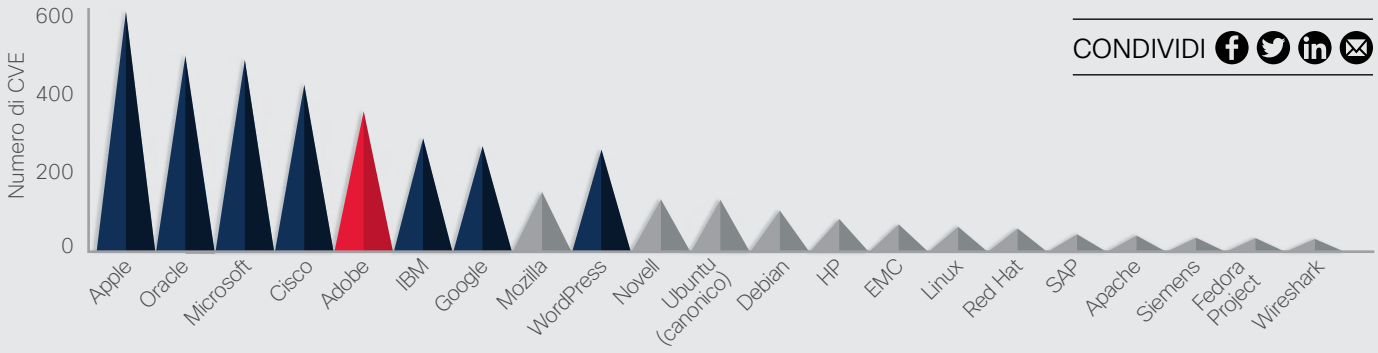
La piattaforma Adobe Flash è un vettore di minaccia diffuso per i criminali da diversi anni. Le vulnerabilità di Flash compaiono ancora frequentemente sugli elenchi di avvisi più urgenti. Nel 2015 un fattore positivo è stato il fatto che i fornitori di prodotti in cui si verificano comunemente tali attacchi, come i browser Web, hanno riconosciuto questo punto debole e stanno attualmente prendendo provvedimenti per ridurre le opportunità di attacco.

Nel corso del 2016 è molto probabile che i criminali concentrino i propri exploit e attacchi sugli utenti di Adobe Flash. Alcune di queste vulnerabilità hanno exploit disponibili pubblicamente online o in vendita come parte degli exploit kit. Come osservato a **pagina 21**, il volume di contenuti Flash è diminuito, ma Flash resta uno dei principali vettori di exploit.

Facendo seguito alle strategie utilizzate per ridurre l'impatto di Java, un altro vettore diffuso, molti browser Web bloccano il contenuto Flash o lo utilizzano in sandbox per proteggere gli utenti. Anche se si tratta di uno sviluppo positivo, è importante ricordare che gli hacker continueranno a lanciare exploit ancora per un po' di tempo. Gli utenti potrebbero ignorare i necessari aggiornamenti del browser e i criminali continueranno a lanciare attacchi mirati a versioni precedenti del software del browser.

I ricercatori Cisco ritengono comunque che le protezioni attualmente integrate in alcuni browser Web e sistemi operativi comunemente utilizzati, offriranno ai criminali meno opportunità di sfruttare Flash. Poiché i criminali informatici mirano a ottenere i migliori risultati possibili (ad esempio il massimo profitto) nel modo più efficiente, dedicheranno pochi sforzi in attacchi che non sono certi di fornire un ritorno sull'investimento.

Figura 18. Numero totale di CVE per fornitore



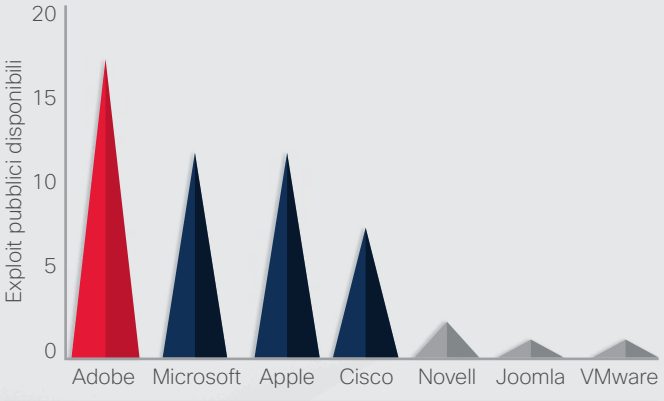
Fonte: Cisco Security Research, National Vulnerability Database

Il grafico riportato precedentemente mostra il numero totale di CVE (Common Vulnerabilities and Exposure) pubblicato nel 2015 dal fornitore. Si tenga presente che Adobe non è prominente in questo grafico come lo è nel grafico a destra, che mostra le vulnerabilità per cui sono disponibili gli exploit.

Inoltre WordPress riporta solo 12 vulnerabilità per il 2015 per il proprio prodotto. Le 240 vulnerabilità aggiuntive provengono da plug-in e script creati da terze parti.

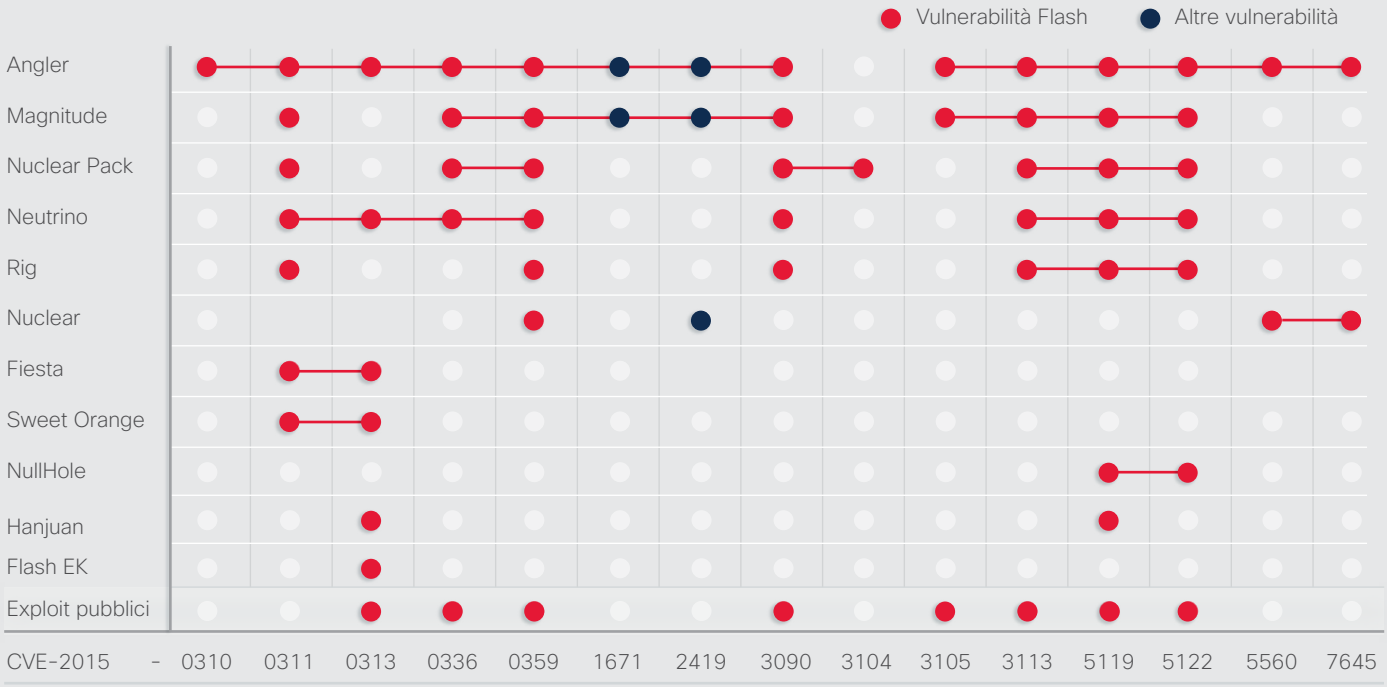
Come indicato nella figura 20, gli elenchi delle vulnerabilità e dei relativi exploit possono fornire indicazioni ai professionisti della sicurezza. È possibile utilizzarli per gestire e assegnare le priorità alle vulnerabilità ad alto rischio e più comuni e per applicare le patch più rapidamente rispetto alle vulnerabilità a basso rischio. Consultare il sito Web CVE Details **(https://www.cvedetails.com/top-50-products.php)** per ulteriori informazioni su CVE per fornitore.

Figura 19. Numero di exploit pubblici disponibili per vulnerabilità del fornitore



Fonte: Cisco Security Research, Metasploit, Exploit DB

Figura 20. Vulnerabilità comuni



Fonte: Cisco Security Research

La figura 20 mostra le vulnerabilità ad alto rischio e indica se la vulnerabilità fa parte di un exploit kit a noleggio (si veda la riga "Flash EK") oppure se ha exploit disponibili pubblicamente (si veda la riga "Exploit pubblici"). Le vulnerabilità per cui sono disponibili exploit funzionali sono una priorità assoluta per il patching.

L'elenco può essere utilizzato per aiutare i professionisti della sicurezza ad assegnare le priorità alle attività di patching e correzione. La presenza di un exploit per un determinato prodotto, pubblicamente o all'interno di un exploit kit, non indica necessariamente che siano in corso degli attacchi.

Rischi di malware per settore

Per ottenere i dati relativi al rischio di malware per i diversi settori verticali, abbiamo esaminato i volumi relativi del traffico di attacco ("capacità di blocco") e quelli del traffico "normale" o previsto.

La figura 21 mostra i 28 settori principali e la loro attività di blocco come percentuale del normale traffico di rete. Il quoziente 1,0 indica che il numero di blocchi è proporzionale al volume di traffico verificato. I valori maggiori di 1,0 rappresentano capacità di blocco superiori alle previsioni e quelli minori di 1,0 capacità inferiori alle previsioni.

Figura 21. Capacità di blocco mensili dei settori da novembre 2014 a settembre 2015

Fonte: Cisco Security Research

Come si può vedere nella figura 22 l'attenzione dei malintenzionati per i settori può variare. Zero indica l'assenza di una variazione netta. Da gennaio a marzo 2015, l'amministrazione pubblica è stato il settore con il maggiore indice di attività di blocco. Da marzo a maggio, è stato il settore dell'elettronica. A metà dell'estate, la maggior parte dei blocchi ha interessato i servizi professionali. Infine nell'autunno 2015 il settore della sanità deteneva il primato nel valore degli indici di blocco.

Secondo la nostra ricerca i quattro settori verticali che hanno registrato la maggiore attività di blocco nel 2015 sono stati tutti colpiti con attacchi legati a Trojan. Anche il settore dell'amministrazione pubblica ha affrontato un elevato numero di attacchi PHP injection, mentre il settore dei servizi professionali è stato colpito da un elevato numero di attacchi iFrame.

Figura 22. Analisi mensile delle capacità di blocco relative dei settori

Fonte: Cisco Security Research

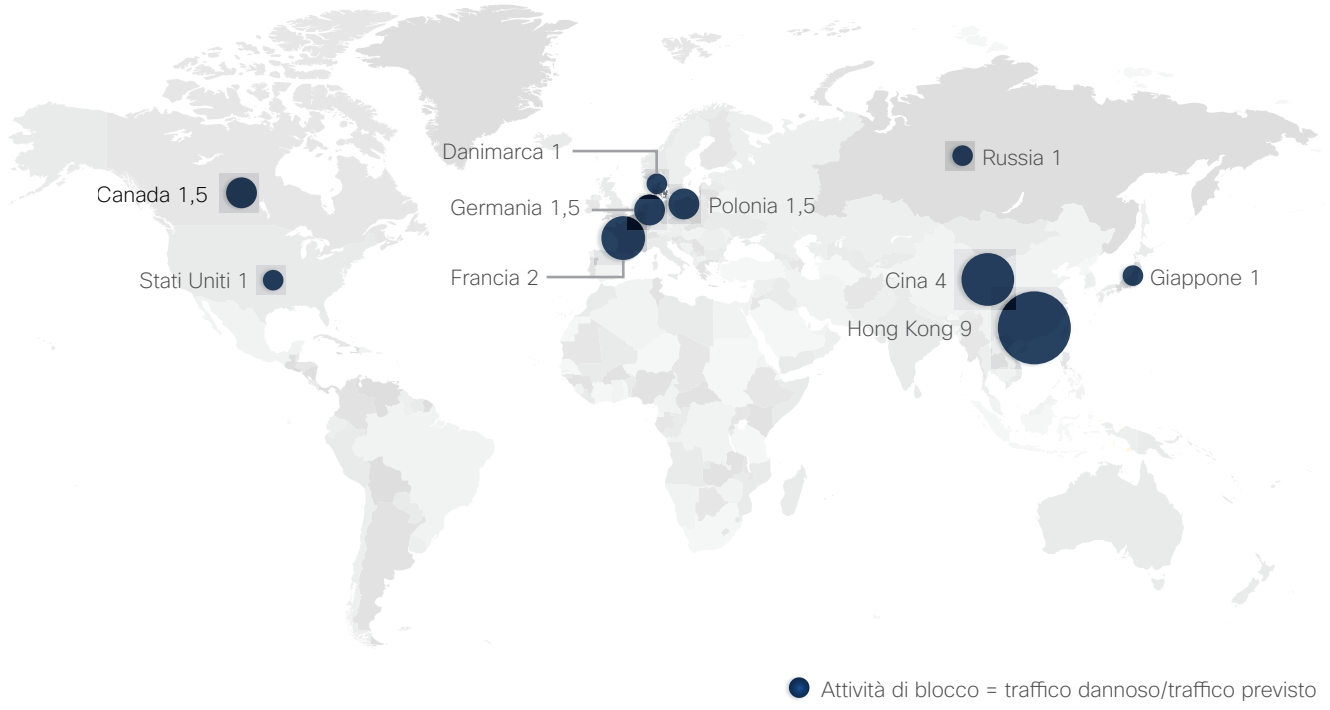
CONDIVIDI

Attività di blocco Web: panoramica geografica

Abbiamo esaminato anche i paesi o le aree in cui ha origine l'attività di blocco Web, come mostrato nella figura 23. I paesi sono stati selezionati per l'analisi in base al volume di traffico Internet. Il valore 1,0 per la capacità di blocco indica che il numero di blocchi osservati è proporzionale alle dimensioni della rete.

I paesi e le aree con attività di blocco considerate superiori alla norma hanno probabilmente nelle loro reti molti server e host Web che presentano vulnerabilità non risolte da patch. I malintenzionati non rispettano i confini di stato e ospitano il malware dove risulta più efficace.

Figura 23. Blocchi Web per paese o area



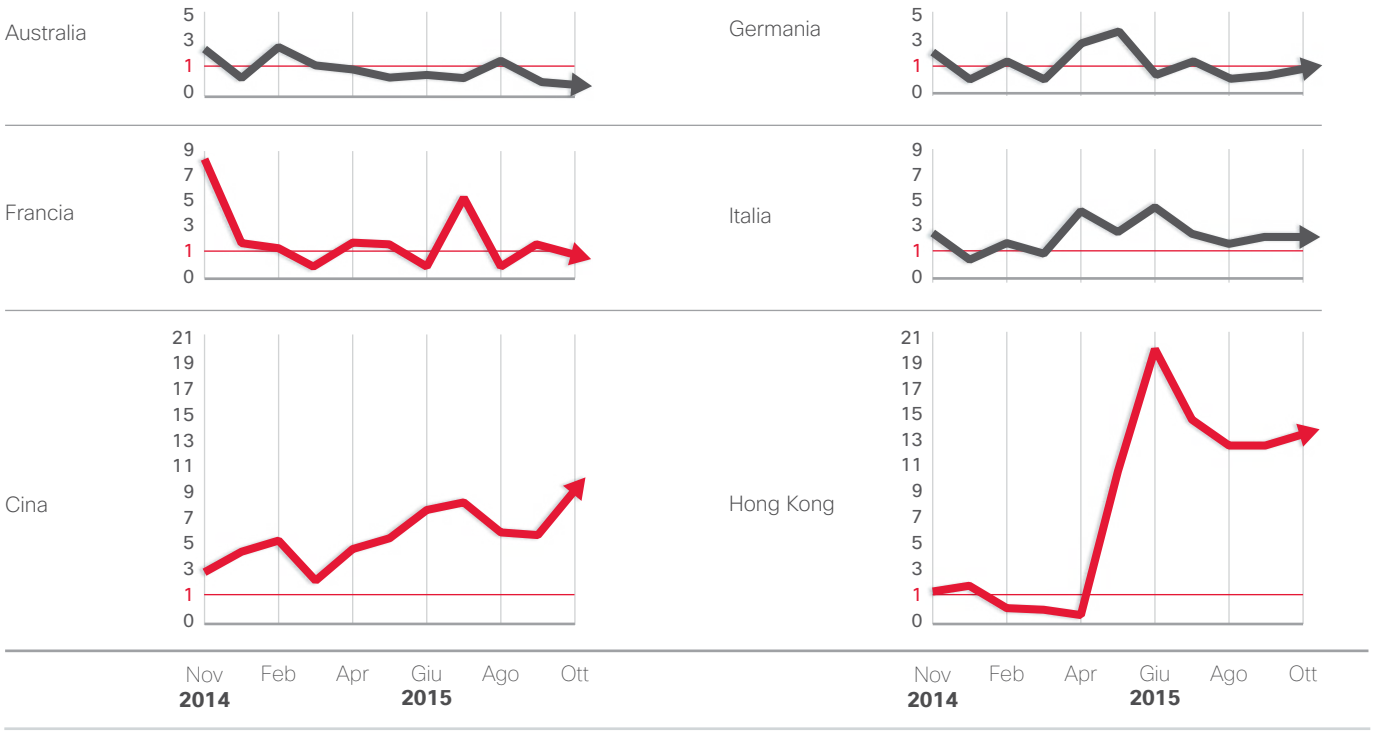
Fonte: Cisco Security Research

La presenza su grandi reti commerciali che gestiscono elevati volumi di traffico Internet è un altro fattore determinante per l'intensa attività di blocco ed è una delle ragioni per le quali Hong Kong è in cima all'elenco.

La figura 24, che mostra un confronto mensile dei blocchi Web per paese o area da novembre 2014 a ottobre 2015, fornisce ulteriori informazioni su queste classifiche.

Si tenga presente che Hong Kong è stata caratterizzata da un'attività di blocco Web superiore al normale a partire dalla primavera del 2015, come avvenuto per la Francia. Entrambe da allora hanno subito un significativo calo di attività di blocco Web, ma dati gli alti tassi di attività all'inizio di quest'anno, nettamente superiori al valore di riferimento, nonostante il recente calo di attività Hong Kong si mantiene ancora leggermente più in alto alla fine dell'anno rispetto all'inizio. Il picco delle attività di blocco in Francia è ritornato a un livello medio a metà dell'estate.

Figura 24. Analisi mensile dei blocchi Web per paese o area da novembre 2014 a ottobre 2015



Fonte: Cisco Security Research

Analisi del settore

Analisi del settore

Cisco conduce ricerche e analisi sulle tendenze e sulle procedure di sicurezza. Paradossalmente, alcune procedure possono rendere più arduo il rilevamento delle minacce da parte dei responsabili della sicurezza ed esporre le aziende e i singoli utenti a un rischio maggiore di compromissione o attacco.

Crittografia: una tendenza in crescita e una sfida per gli addetti alla sicurezza

La crittografia serve. Le società devono proteggere la proprietà intellettuale e altri dati sensibili, gli inserzionisti vogliono salvaguardare l'integrità dei dati analitici di back-end e dei contenuti pubblicitari e le aziende vogliono proteggere sempre più la privacy dei clienti.

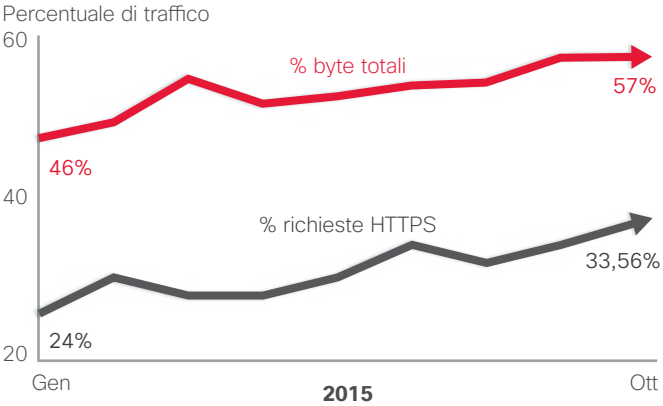
Ma la crittografia crea anche problemi e in alcuni casi rende le aziende troppo fiduciose delle misure di protezione adottate. Le aziende hanno fatto passi avanti nella crittografia dei dati quando questi vengono trasmessi tra entità, ma i dati archiviati vengono spesso lasciati senza protezione. Molte delle violazioni più rilevanti degli ultimi anni hanno sfruttato i dati non crittografati archiviati nel data center e in altri sistemi interni. Per gli hacker, è come seguire un furgone blindato che si dirige verso un magazzino aperto a tutti.

È anche importante che le aziende comprendano che la crittografia completa può ridurre l'efficacia di alcuni prodotti di sicurezza, poiché nasconde gli indicatori di compromissione utilizzati per identificare e monitorare le attività dannose.

Tuttavia, non c'è alcuna giustificazione al fatto di non crittografare i dati riservati. Gli strumenti di sicurezza e chi li usa devono adattarsi a questo Mondo Nuovo integrando le intestazioni e altre parti non crittografate del flusso di dati con le altre fonti di informazioni contestuali per analizzare il traffico crittografato. Gli strumenti che si basano sulla visibilità del payload, come l'acquisizione dei pacchetti completi, stanno diventando meno efficaci. Cisco NetFlow e le altre analisi basate sui metadati sono diventati essenziali.

Osservando le tendenze del 2015, i nostri ricercatori deducono che il traffico crittografato, soprattutto HTTPS, abbia raggiunto un punto di svolta: sebbene infatti non rappresenti ancora la maggior parte delle transazioni, diventerà presto la forma dominante di traffico in Internet. In effetti, la nostra ricerca indica che oltre il 50% dei byte trasferiti (Figura 25) è già regolarmente costituito dal traffico crittografato a causa dell'overhead dell'HTTPS e dei maggiori contenuti inviati tramite HTTPS, come i trasferimenti a siti di archiviazione dei file.

Figura 25. Percentuali di SSL



Fonte: Cisco Security Research

Per ogni transazione Web, vengono spediti (in uscita) e ricevuti (in entrata) vari byte. Le transazioni HTTPS hanno maggiori richieste in uscita rispetto a quelle HTTP, ossia circa 2000 byte in più. Al tempo stesso, anche le richieste HTTPS in entrata hanno un overhead, che però diventa meno significativo in corrispondenza di maggiori risposte.

Combinando i byte in entrata e in uscita per transazione Web, si può stabilire la percentuale complessiva di tutti i byte coinvolti in ogni transazione che vengono crittografati tramite HTTPS. Con l'aumento del traffico HTTPS e dell'ulteriore overhead, abbiamo determinato che i byte HTTPS rappresentavano il 57% di tutto il traffico Web a ottobre 2015 (Figura 25), dimostrando un aumento rispetto al 46% di gennaio dello stesso anno.

Attraverso l'analisi del traffico Web è stato anche stabilito che le richieste HTTPS sono aumentate gradualmente, ma in modo significativo, da gennaio 2015. Come illustrato nella Figura 25, a gennaio il 24% delle richieste utilizzava il protocollo HTTPS, mentre la percentuale restante utilizzava l'HTTP.

A ottobre, è stato osservato che le richieste HTTPS erano pari al 33,56%. Inoltre, è stato anche rilevato che la percentuale di byte HTTPS in entrata era aumentato. Una crescita sostenuta in tutto l'arco dell'anno. L'aumento del traffico tramite HTTPS genera maggiori esigenze di larghezza di banda: 5 kbps in più per ogni transazione.

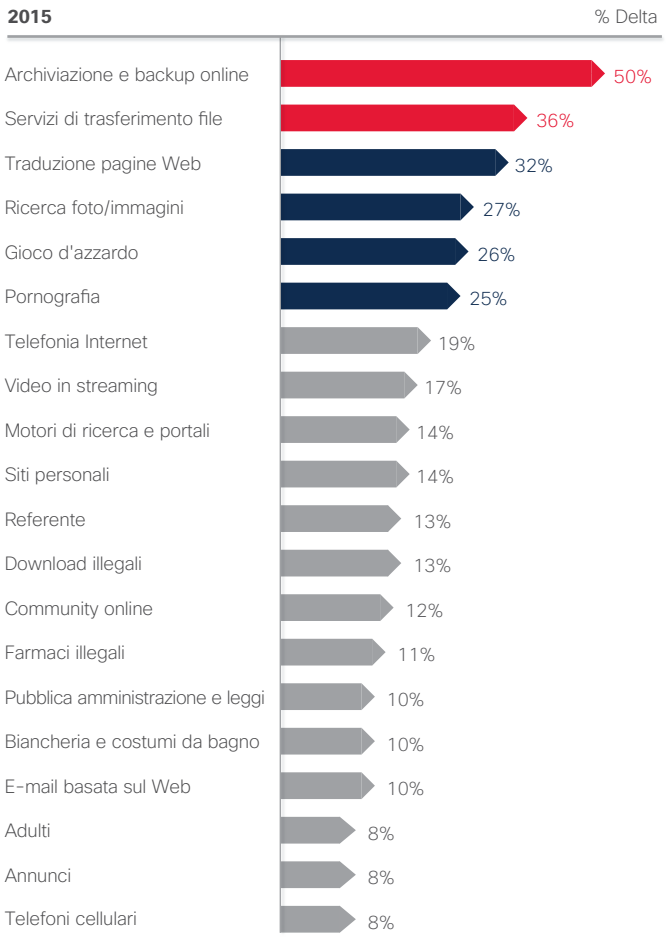
Riteniamo che l'aumento complessivo del traffico Web crittografato sia attribuibile principalmente a questi fattori:

- più traffico mobile dalle applicazioni, che applicano la crittografia in modo intrinseco
- maggiori richieste da parte degli utenti di scaricare video crittografati
- maggiori richieste ai server di backup e archiviazione che contengono dati sensibili archiviati che i criminali informatici sono impazienti di sottrarre.

Infatti, la Figura 26 mostra che le richieste HTTPS alle risorse di backup e di archiviazione online sono aumentate del 50% dall'inizio del 2015. Nello stesso periodo, anche i servizi di trasferimento file sono notevolmente aumentati, con una percentuale pari al 36%.

Infine, aumenta l'attività crittografata sia nel numero di transazioni crittografate che in quello di byte crittografati in ogni transazione. Ognuno comporta un vantaggio e un rischio potenziale, creando l'esigenza di una difesa integrata dalle minacce che aiuti ad aumentare la visibilità.

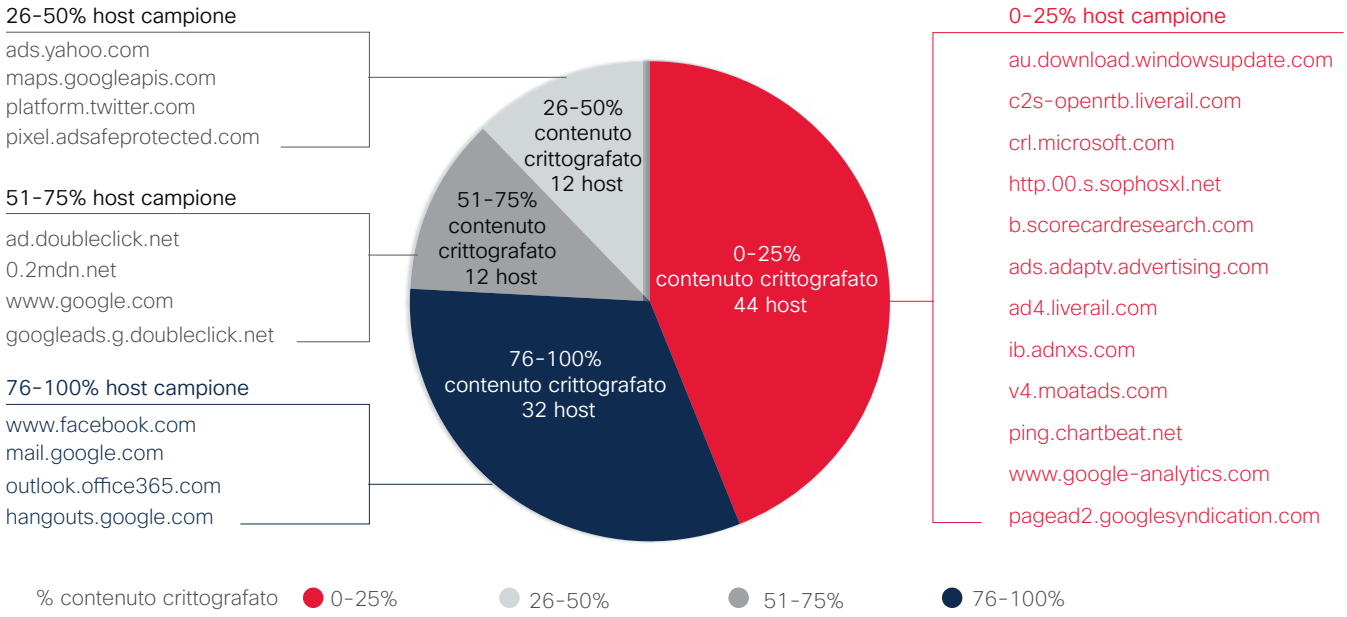
Figura 26. Richieste HTTPS: i principali cambiamenti da gennaio a settembre 2015



Fonte: Cisco Security Research

CONDIVIDI

Figura 27. I principali host che crittografano il traffico HTTPS



Fonte: Cisco Security Research

Osservando i dati dei domini principali in base alle richieste (Figura 27), si nota che molte delle principali pagine dei contenuti di Google e Facebook sono crittografate. In genere, solo il 10% del traffico pubblicitario delle due aziende è crittografato.

Indipendentemente dalle problematiche, la crittografia dei dati è una necessità imprescindibile nell'attuale panorama delle minacce. Gli hacker sono troppo abili ad aggirare il controllo degli accessi perché gli utenti possano rischiare di non proteggere le informazioni critiche in qualsiasi fase dell'archiviazione o del trasferimento.

Ecco perché è essenziale che i team responsabili della sicurezza monitorino le tendenze del traffico Web per assicurarsi che le richieste HTTPS non provengano o siano dirette verso posizioni sospette. Un avvertimento: il traffico crittografato non va cercato su un insieme predefinito di porte. Come illustrato nella sezione successiva, la nostra ricerca indica infatti che il malware tende ad avviare comunicazioni crittografate su porte diverse.

L'ENTROPIA

L'alta entropia è un segnale indicativo dei trasferimenti o della comunicazione di file crittografati o compressi.[6] L'aspetto positivo per i team della sicurezza è che l'entropia è relativamente semplice da monitorare perché non richiede la conoscenza dei protocolli crittografici sottostanti.

Dal 1° giugno 2015 e per i tre mesi successivi, i ricercatori della sicurezza Cisco hanno osservato 7.480.178 flussi di 598.138 campioni di malware inviati con un punteggio indicatore della minaccia pari a 100. In questo periodo i flussi ad alta entropia sono stati 958.851, pari al 12,82%.

Abbiamo anche identificato 917.052 flussi tramite il protocollo Transport Layer Security (TLS) (12,26%). Inoltre, 8.419 flussi TLS erano su una porta diversa dalla 443, ossia la porta predefinita per l'HTTP sicuro. Alcune delle porte utilizzate dal malware analizzato per comunicare erano le porte 21, 53, 80 e 500.

Con il costante aumento del livello di traffico Internet crittografato, per le aziende diventa sempre più importante adottare un'architettura integrata per la difesa dalle minacce (vedere "I sei principi della difesa integrata dalle minacce" a **pagina 62**). Le soluzioni puntuali non sono adatte a identificare le minacce potenziali del traffico crittografato. Le piattaforme di sicurezza integrata offrono ai team della sicurezza una maggiore visibilità su ciò che accade nei dispositivi o nelle reti, in modo da poter individuare più facilmente tipi di attività sospetti.

[6] Entropia: in informatica, il termine entropia (mancanza di ordine o di prevedibilità) si riferisce alla casualità con cui un sistema operativo o un'applicazione raccolgono dati da utilizzare per la crittografia o per altri impieghi che richiedono dati casuali.

L'adozione della crittografia: dati reali

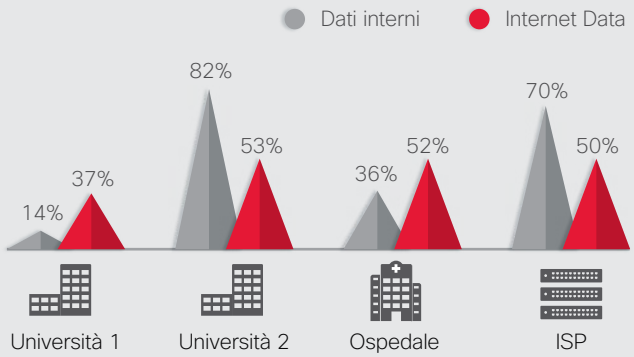
Lancope, un'azienda di Cisco, ha analizzato le percentuali di traffico crittografato sia interno che in Internet in tre settori di attività (due università, un ospedale e un provider ISP, tutti con sede negli Stati Uniti).

Lancope ha rilevato che in una delle università quasi tutto il traffico interno era crittografato (82%), mentre il traffico Internet crittografato era pari al 53%. Questi risultati sono in linea con le tendenze osservate da Lancope in altri settori.

Solo il 36% dei dati interni dell'ospedale era crittografato. Tuttavia, più della metà (52%) del traffico Internet era crittografato.

Presso il provider ISP, era crittografato il 70% del traffico interno e il 50% di quello Internet.

Lo studio di Lancope mostra che in diversi settori c'è un'adozione su vasta scala della crittografia dei dati in movimento. Cisco suggerisce di rivolgere ora una simile attenzione anche alla crittografia dei dati archiviati al fine di limitare gli impatti delle compromissioni per le aziende.



Fonte: Lancope Threat Research Labs

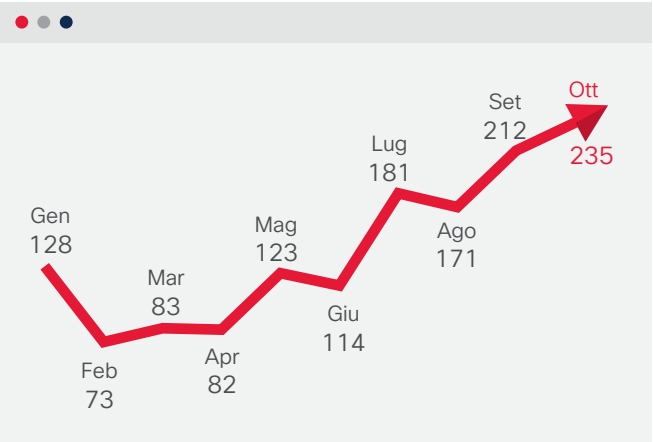
I criminali informatici incrementano l'attività dei server su WordPress

Come affermato nell'introduzione a questo report, i criminali informatici sono continuamente alla ricerca di metodi per rendere più efficienti ed economiche le loro operazioni, oltre a nuovi modi per eludere il rilevamento; in particolare trovano sempre più vantaggioso sfruttare i siti Web creati usando WordPress, la popolare piattaforma di sviluppo di siti Web e blog. Nei siti WordPress, gli hacker possono assumere il controllo di un flusso costante di server compromessi per creare un'infrastruttura che supporti il ransomware, le frodi bancarie o gli attacchi di phishing. Internet è pieno di siti abbandonati creati con WordPress non più gestiti in termini di sicurezza; con la comparsa di nuovi problemi di sicurezza, questi siti vengono spesso compromessi e inseriti nelle campagne degli attacchi informatici.

Analizzando i sistemi utilizzati per supportare il ransomware e altro malware, i ricercatori della sicurezza Cisco hanno rilevato che molti criminali informatici stanno spostando l'attività online sui server WordPress compromessi. Il numero di domini WordPress utilizzati dagli hacker è aumentato del 221% da febbraio a ottobre 2015 (vedere la Figura 28).

I ricercatori Cisco ritengono che questo cambiamento si sia verificato per un paio di motivi. Quando il ransomware utilizza altri strumenti per comunicare le chiavi di crittografia o altre informazioni di comando e controllo, tali comunicazioni possono essere rilevate o bloccate, il che impedisce di completare il processo di crittografia. Tuttavia, le comunicazioni che scambiano le chiavi di crittografia attraverso i server WordPress compromessi possono sembrare normali, aumentando così le probabilità che la crittografia dei file venga completata. In altre parole, i siti WordPress fungono da agenti di scambio.

Figura 28. Numero di domini WordPress utilizzati dagli autori di malware



Fonte: Cisco Security Research

Per evitare gli svantaggi di altre tecnologie, gli hacker ricorrono a WordPress, che utilizzano per ospitare i payload del malware e i server di comando e controllo. I siti WordPress offrono vari vantaggi, ad esempio, i molti siti abbandonati offrono ai criminali informatici maggiori opportunità per compromettere i siti con deboli difese di sicurezza.

Il rischio di utilizzare sistemi compromessi per eseguire un'operazione di malware è che uno dei server violati può essere disabilitato una volta scoperta la compromissione. Se ciò avviene nel mezzo di una campagna, il downloader del malware potrebbe non riuscire a recuperare il payload oppure il malware potrebbe non essere in grado di comunicare con i propri server di comando e controllo. I ricercatori della sicurezza Cisco hanno notato che il malware ovviava a questo problema utilizzando più di un server WordPress e hanno persino scoperto gli elenchi dei server WordPress compromessi archiviati nei siti di condivisione dei dati come Pastebin.

Il malware utilizzava questi elenchi per trovare server di comando e controllo operativi, consentendo al malware di agire anche in caso di mancato funzionamento di un server compromesso. I ricercatori hanno anche identificato i downloader del malware che contenevano un elenco di siti WordPress che archiviavano i payload. Se un sito di download non funzionava, il malware passava a quello successivo e scaricava i payload dannosi dal server WordPress funzionante.

I siti WordPress compromessi spesso non eseguivano la versione di WordPress più recente, avevano password di amministrazione deboli e usavano plug-in senza patch di sicurezza.

Queste vulnerabilità hanno permesso agli hacker di assumere il controllo dei server WordPress e utilizzarli come infrastruttura malware (vedere la Figura 29).

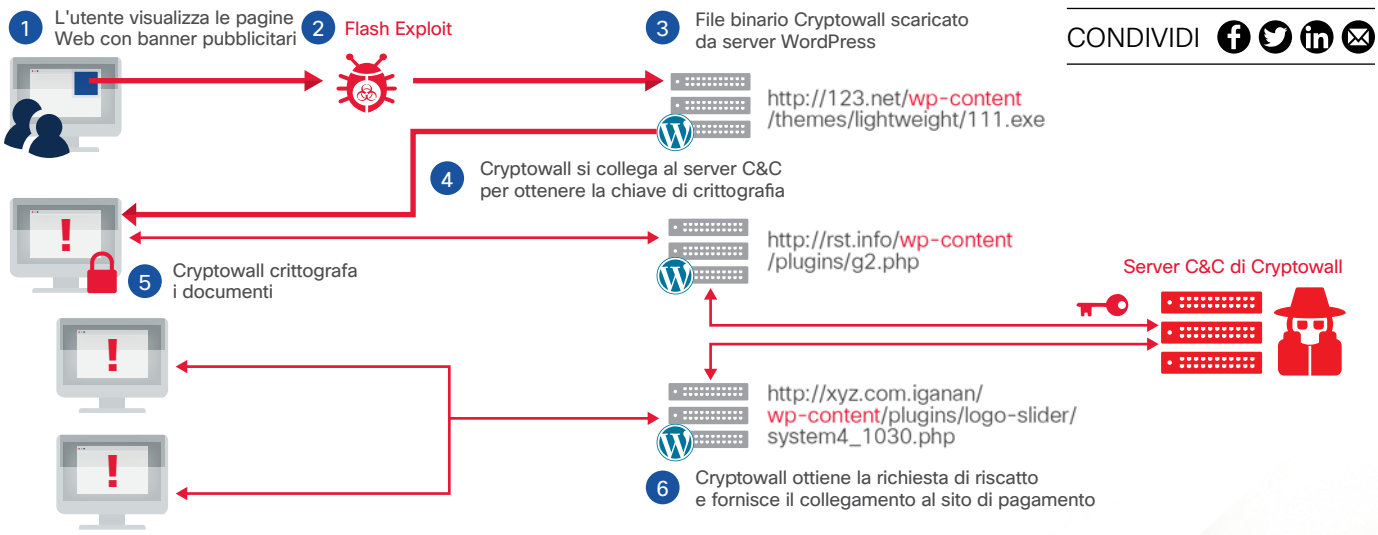
I ricercatori Cisco hanno identificato alcune delle tipologie di software e file ospitati di solito su siti WordPress compromessi:

- File eseguibili che fungono da payload per gli attacchi di exploit kit
- File di configurazione per il malware come Dridex e Dyre
- Codice proxy che trasmette la comunicazione di comando e controllo per nascondere l'infrastruttura di comando e controllo
- Pagine Web di phishing per raccogliere i nomi utente e le password
- Script HTML che reindirizzano il traffico ai server degli exploit kit

Inoltre, i ricercatori Cisco hanno identificato molte famiglie di malware che utilizzano come infrastruttura i siti WordPress compromessi:

- l'infostealer Dridex
- il password stealer Pony
- il ransomware TeslaCrypt
- il ransomware Cryptowall 3.0
- il ransomware TorrentLocker
- il botnet spam Andromeda
- il trojan dropper Bartallex
- l'infostealer Necurs
- le false pagine di accesso.

Figura 29. Sistema utilizzato per compromettere i siti WordPress



Fonte: Cisco Security Research

Gli esperti della sicurezza preoccupati per le minacce che presentano i siti WordPress controllati dagli hacker, dovrebbero cercare tecnologie di sicurezza Web che esaminino i contenuti provenienti da siti creati con WordPress. Tale traffico potrebbe essere considerato insolito se la rete scarica programmi da siti WordPress anziché solo pagine Web e immagini (sebbene i siti WordPress possano ospitare anche programmi legittimi).

Infrastruttura obsoleta: un problema decennale

Oggigiorno tutte le aziende sono in qualche modo aziende IT, perché dipendono dall'infrastruttura IT e OT (Operational Technology) per connessioni, digitalizzazione e successo. Ciò significa che la sicurezza IT deve diventare una priorità. Eppure molte aziende fanno affidamento su infrastrutture di rete che sono costituite da componenti vecchi, obsoleti e con sistemi operativi vulnerabili, e perciò, non sono sicure dal punto di vista informatico.

Di recente abbiamo analizzato 115.000 dispositivi Cisco in Internet e negli ambienti dei clienti per evidenziare i rischi per la sicurezza presentati dall'infrastruttura obsoleta e dalla mancanza di attenzione nell'applicazione delle patch per risolvere le vulnerabilità.

Abbiamo identificato i 115.000 dispositivi del nostro campione di un giorno con la scansione di Internet e quindi osservando i dispositivi da una prospettiva dall'esterno verso l'interno (ossia da Internet verso l'interno dell'azienda). Questa scansione e analisi hanno rivelato che 106.000 dei 115.000 dispositivi presentavano vulnerabilità note nel software usato. Ciò significa che, in tale campione, il 92% dei dispositivi Cisco su Internet è soggetto a vulnerabilità note.

Per ulteriori informazioni su questo argomento, consultare i post del blog Cisco sulla sicurezza:

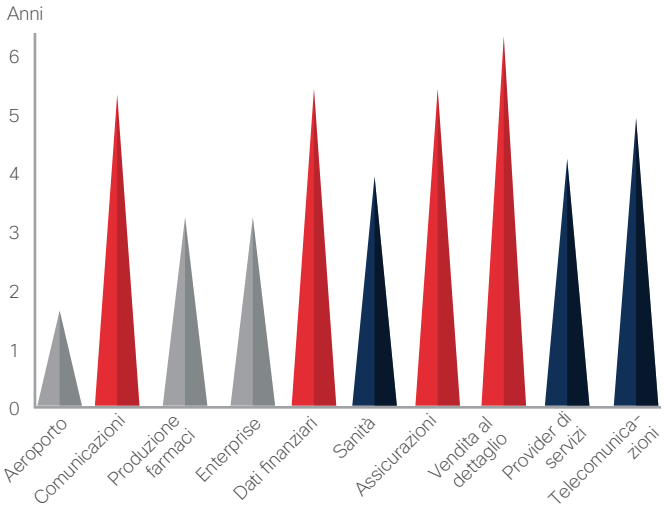
"IT Security: When Maturity Is Overrated"

"Evolution of Attacks on Cisco IOS Devices"

"SYNful Knock: Detecting and Mitigating Cisco IOS Software Attacks"

Cisco ha anche scoperto che la versione del software usata da quei dispositivi conteneva, in media, 26 vulnerabilità e che il software in uso nell'infrastruttura di rete di molte aziende era obsoleto (Figura 30). Alcuni clienti del settore finanziario, sanitario e della vendita al dettaglio utilizzavano versioni del software Cisco di più di 6 anni prima.

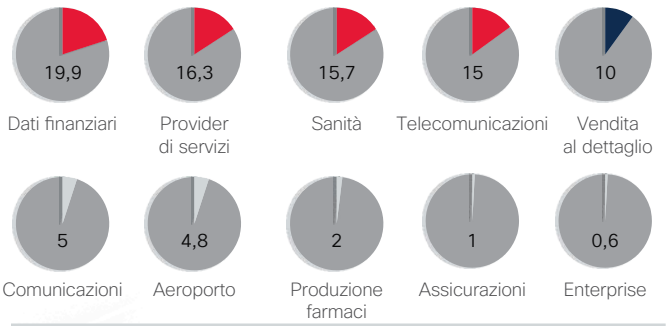
Figura 30. Età media del software in anni



Fonte: Cisco Security Research

È stato anche scoperto che molti dei dispositivi di infrastruttura analizzati avevano raggiunto l'ultimo giorno di supporto (LDoS), ossia che non possono essere aggiornati né resi più sicuri (Figura 31). Questi dispositivi non ricevono neppure le patch per le vulnerabilità note e quindi le informazioni sulle nuove minacce. I clienti sono stati informati di questo problema.

Figura 31. Percentuale di dispositivi dell'infrastruttura che hanno raggiunto l'ultimo giorno di supporto



Fonte: Cisco Security Research

Inoltre, l'8% dei 115.000 dispositivi del campione analizzato ha raggiunto la fine del ciclo di vita e un altro 31% raggiungerà la fine del supporto entro un periodo da uno a quattro anni.

Un'infrastruttura IT vecchia e obsoleta rappresenta una vulnerabilità per le aziende. Più ci avviciniamo a Internet of Things (IoT), e a Internet of Everything (IoE), più diventa importante per le aziende avere un'infrastruttura di rete sicura, per poter garantire l'integrità dei dati e delle comunicazioni che attraversano la rete. Si tratta di un fattore importante per il successo di IoE.

Numerosi clienti Cisco hanno realizzato la propria infrastruttura di rete dieci anni fa. Molti però non hanno tenuto conto del fatto che, nel tempo, la loro dipendenza da tale infrastruttura sarebbe stata totale e non hanno neppure previsto che la loro infrastruttura sarebbe diventata un bersaglio ambito dai criminali informatici.

Le aziende tendono a evitare di aggiornare l'infrastruttura perché è un'operazione costosa che comporta interruzioni dell'operatività della rete. Inoltre, in alcuni casi, un semplice aggiornamento non sarebbe sufficiente. Alcuni prodotti sono così obsoleti che non possono essere aggiornati per incorporare le ultime soluzioni di sicurezza necessarie per proteggere l'azienda.

I fatti parlano da soli: il mantenimento dell'infrastruttura è di importanza fondamentale. Le aziende devono pianificare aggiornamenti periodici e riconoscere l'importanza di assumere un controllo proattivo delle infrastrutture critiche, prima che lo faccia un hacker.

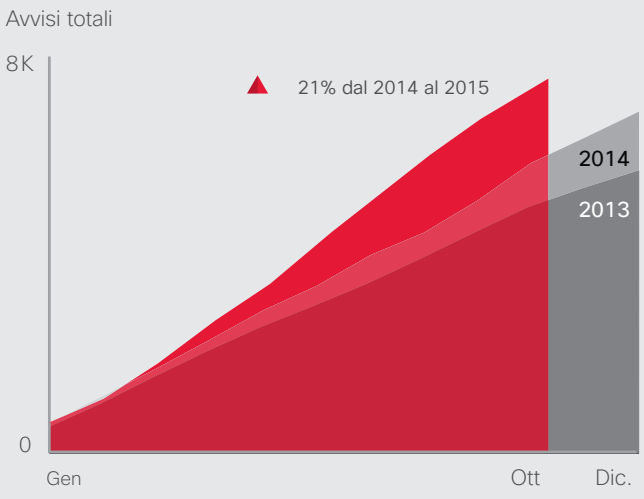
Le cifre degli avvisi cumulativi dimostrano maggiore impegno nella gestione delle vulnerabilità

Un'infrastruttura obsoleta facilita il lavoro degli hacker. Tuttavia, l'aumento degli avvisi cumulativi, che includono le vulnerabilità dei prodotti nelle soluzioni open source e proprietarie, è un segnale positivo che indica una maggiore attenzione da parte del settore della tecnologia per eliminare le opportunità per gli hacker.

Il totale degli avvisi cumulativi è aumentato del 21% dal 2014 al 2015. Da luglio fino a settembre 2015 si è verificato un incremento notevole. Questo aumento può essere attribuito in gran parte agli aggiornamenti importanti dei software di fornitori come Microsoft e Apple, in quanto l'aggiornamento dei prodotti genera più segnalazioni delle vulnerabilità software.

I principali fornitori di software oggi rilasciano più patch e aggiornamenti e sono più trasparenti su questa attività. Il maggiore numero di aggiornamenti e patch rappresenta un fattore importante per le aziende che automatizzano la gestione delle vulnerabilità mediante piattaforme di intelligence e gestione della sicurezza, che consentono di gestire l'intero volume delle informazioni sui sistemi, i software, le vulnerabilità e le minacce. L'utilizzo di questi sistemi e di API (Application Programming Interface) permette una gestione della sicurezza più efficiente, tempestiva ed efficace in aziende grandi e piccole.

Figura 32. Totale avvisi cumulativi annuale



Fonte: Cisco Security Research

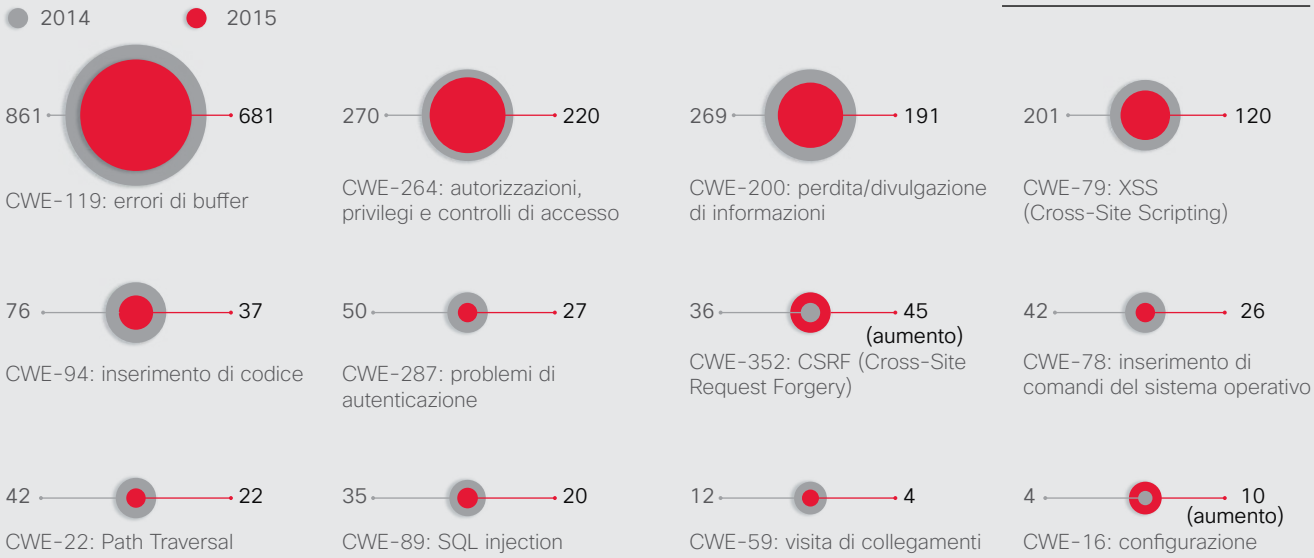
CONDIVIDI

Le categorie delle minacce: riduzione degli errori di buffer e della divulgazione o perdita di informazioni

Nell'esame delle categorie di vulnerabilità comuni, le vulnerabilità da scripting cross-site (XSS) si sono ridotte del 47% dal 2014 al 2015 (Figura 33). Tale riduzione può essere il risultato della maggiore attenzione rivolta ai test di vulnerabilità. Infatti i fornitori sono diventati più esperti nell'identificazione di queste vulnerabilità specifiche e nel risolverle prima che i loro prodotti raggiungano il mercato.

Le vulnerabilità da divulgazione o perdita di informazioni si sono ridotte del 15% nel 2015. Queste vulnerabilità includono le divulgazioni involontarie a soggetti che non hanno un accesso esplicito. Perciò, i fornitori hanno iniziato a prestare più attenzione ai controlli che consentono o impediscono l'accesso ai dati, rendendo meno frequente questa comune vulnerabilità.

Figura 33. Numero di vulnerabilità delle categorie comuni



Fonte: Cisco Security Research

Le piccole e medie imprese sono un rischio per la sicurezza delle grandi aziende?

Le PMI svolgono un ruolo fondamentale nelle economie nazionali e hanno anche la responsabilità di proteggere dagli attacchi informatici i dati che i clienti affidano loro. Tuttavia, come illustrato in dettaglio nello studio comparativo di Cisco delle infrastrutture di sicurezza del 2015 (vedere a **pagina 41**), le PMI rivelano che le proprie difese contro gli hacker sono troppo deboli per poter fronteggiare le sfide in atto. A loro volta, questi punti deboli possono mettere a rischio anche le aziende clienti delle PMI. Un hacker che violi la rete di una PMI potrebbe infatti riuscire a penetrare da lì nella rete di una grande azienda.

A giudicare dai risultati dello studio comparativo di Cisco delle infrastrutture di sicurezza del 2014, le PMI utilizzano meno processi per analizzare le violazioni e meno strumenti di difesa dalle minacce informatiche rispetto allo scorso anno. Ad esempio, nel 2015, il 48% delle PMI ha dichiarato di utilizzare la sicurezza Web, mentre nel 2014 lo affermava il 59%. Solo il 29% ha dichiarato di aver utilizzato patch e strumenti di configurazione nel 2015 rispetto al 39% del 2014.

Inoltre, fra le PMI intervistate che non dispongono di un dirigente direttamente responsabile della sicurezza, quasi un quarto non ritiene che la propria azienda sia un bersaglio ambito dai criminali informatici. Questa convinzione porta le aziende a pensare, con eccessiva fiducia, di riuscire a contrastare i sofisticati attacchi informatici di oggi o, più probabilmente, a credere che l'azienda non li subirà mai.

LE PMI SONO MENO PROPENSE AD AVVALERSI DI TEAM PER RISOLVERE LE VIOLAZIONI

In molti casi, le PMI sono meno propense delle grandi aziende a disporre di un team addetto a risolvere le violazioni e un team di intelligence sulle minacce. Ciò può essere dovuto ai limiti di budget: gli intervistati hanno indicato proprio questo fattore come uno dei principali ostacoli all'adozione di processi e tecnologie di sicurezza avanzata. Il 72% delle grandi aziende (quelle con oltre 1000 dipendenti) dispone di entrambi i team, rispetto al 67% delle aziende con meno di 500 dipendenti.

Le PMI utilizzano anche meno processi per analizzare le compromissioni, eliminare le cause di incidenti e ripristinare i sistemi ai livelli precedenti le violazioni (Figura 35). Ad esempio, il 53% delle aziende con più di 10.000 dipendenti utilizza l'analisi dei flussi di rete per esaminare i sistemi compromessi, rispetto al 43% delle aziende con meno di 500 dipendenti. Il 60% delle aziende con più di 10.000 dipendenti utilizza patch e aggiorna le applicazioni considerate vulnerabili, contro il 51% delle aziende con meno di 500 dipendenti.

L'utilizzo di determinate difese dalle minacce informatiche da parte delle PMI sembra essere in flessione. Ad esempio, nel 2014, il 52% delle PMI utilizzava la sicurezza per gli utenti mobili, rispetto al solo 42% del 2015. Inoltre, nel 2014, il 48% delle PMI utilizzava l'analisi delle vulnerabilità, rispetto al 40% del 2015 (vedere la Figura 36).

Figura 34. Principali ostacoli delle PMI

Quale dei seguenti fattori è secondo te l'ostacolo maggiore per l'adozione di processi e tecnologie avanzate per la sicurezza?

Dimensioni dell'azienda	250-499	500-999	1000-9999	10.000+
Limiti di budget	40%	39%	39%	41%
Problemi di compatibilità con sistemi legacy	32%	30%	32%	34%
Conflitti di priorità	25%	25%	24%	24%

Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Figura 36. Diminuzione delle misure di difesa delle PMI nel 2015

Quale di queste difese dalle minacce, se esistenti, sono attualmente in uso nella tua azienda?	2014	2015
Sicurezza degli utenti mobili	52%	42%
Rete wireless protetta	51%	41%
Analisi delle vulnerabilità	48%	40%
VPN	46%	36%
Security Information and Event Management (SIEM)	42%	35%
Test di penetrazione	38%	32%
Analisi forense della rete	41%	29%
Applicazione di patch e configurazione	39%	29%
Analisi forense degli endpoint	31%	23%

Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Figura 35. Le PMI usano meno processi di sicurezza rispetto alle grandi aziende

Quali dei seguenti processi, se esistenti, sono attualmente in uso nella tua azienda per analizzare i sistemi compromessi?

Dimensioni dell'azienda	250-499	500-999	1000-9999	10.000+
Analisi forense della memoria	30%	34%	34%	37%
Analisi dei flussi di rete	43%	47%	52%	53%
Analisi di log/eventi correlati	34%	34%	40%	42%
Team esterni (terze parti) per l'analisi o la risoluzione delle violazioni	30%	32%	34%	39%
Analisi dei log dei sistemi	47%	51%	55%	59%
Analisi del registro di sistema	43%	43%	49%	52%
Rilevamento degli IoC	31%	34%	37%	36%
Quali processi usa la tua azienda per ripristinare i sistemi compromessi al livello operativo precedente all'incidente?				
Vengono applicati aggiornamenti e patch alle applicazioni considerate vulnerabili	51%	53%	57%	60%
Vengono implementati sistemi di rilevamento e controllo nuovi o aggiuntivi	49%	55%	57%	61%

Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

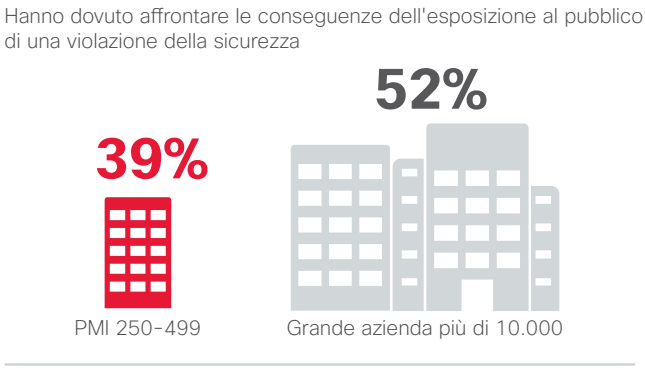
Perché è significativo il fatto che le PMI tendano a utilizzare meno difese rispetto alle aziende più grandi? Nel panorama attuale in cui i criminali informatici sviluppano tattiche sempre più sofisticate per violare le reti senza essere rilevati, nessuna azienda può permettersi di lasciare la rete non protetta o di rimandare l'implementazione di processi che potrebbero offrire informazioni dettagliate su come si è verificata una violazione e potenzialmente evitarne altre in futuro.

Inoltre, le PMI potrebbero non accorgersi che le loro vulnerabilità comportano rischi anche per le aziende dei loro clienti e le rispettive reti. Oggi i criminali informatici si insinuano spesso in una rete con lo scopo di accedere a un'altra rete che offre vantaggi più redditizi e le PMI possono rappresentare il punto di partenza di questo tipo di attacchi.

LE PMI SONO MENO ESPOSTE AL PUBBLICO PER LE VIOLAZIONI DEI DATI

Le PMI sono meno esposte al pubblico rispetto alle grandi aziende per le violazioni della sicurezza, probabilmente in conseguenza delle dimensioni inferiori delle loro reti. Mentre il 52% delle aziende con più di 10.000 dipendenti ha dovuto affrontare le conseguenze dell'esposizione al pubblico di una violazione della sicurezza, solo il 39% delle aziende con meno di 500 dipendenti si è trovato in una situazione simile.

Figura 37. Le PMI sono meno esposte al pubblico per le violazioni

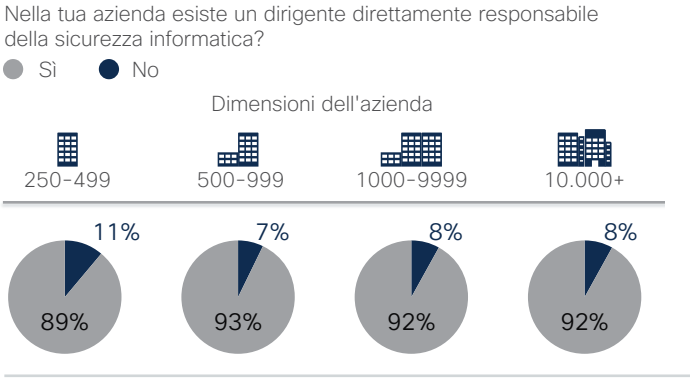


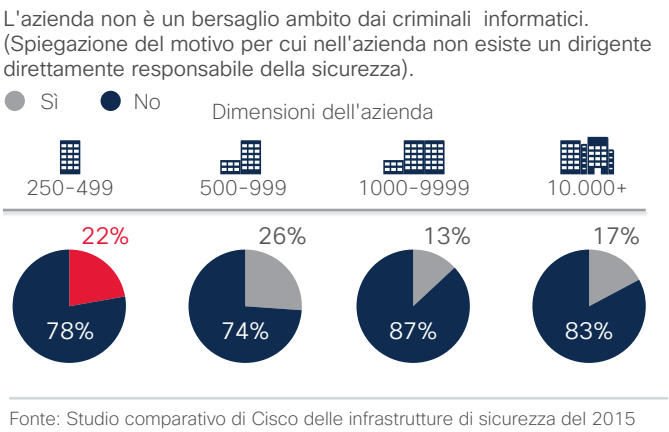
Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

CONDIVIDI

L'esposizione al pubblico delle violazioni della sicurezza sono ovviamente dannose per un'azienda, ma offrono un vantaggio: incoraggiano spesso le aziende a esaminare in modo più approfondito l'infrastruttura e i processi di sicurezza e a prendere in considerazione l'idea di potenziarle. I dati del sondaggio Cisco (vedere a **pagina 74**) indicano che, quando le grandi aziende sono esposte al pubblico per una violazione dei dati, migliorano sensibilmente la tecnologia di sicurezza e implementano processi più solidi.

Figura 38. Le PMI non si considerano un bersaglio ambito dai criminali informatici





Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

La percezione delle PMI della loro azienda come bersaglio dei criminali informatici può indicare una scarsa conoscenza del panorama delle minacce. Come illustrato sopra nella Figura 38, il 22% delle aziende con meno di 500 dipendenti ha dichiarato di non disporre di un dirigente con la responsabilità diretta della sicurezza informatica in quanto non crede che la propria azienda sia un bersaglio ambito dagli hacker.

LE PMI SONO PIÙ PROPENSE A ESTERNALIZZARE LE FUNZIONI DI SICUREZZA INFORMATICA NEL 2015

Sebbene il sondaggio indichi che un numero maggiore di PMI complessivamente si rivolga all'esterno per le funzioni di sicurezza, le PMI sono solitamente meno propense delle grandi aziende all'esternalizzazione di alcuni servizi, come la consulenza. Ad esempio, il 55% delle grandi aziende esternalizza i servizi di consulenza, rispetto al 46% delle aziende con meno di 500 dipendenti. Il 56% delle grandi aziende si rivolge all'esterno per le attività di controllo della sicurezza, rispetto al 42% delle aziende con meno di 500 dipendenti (vedere la Figura 39).

Tuttavia, nel 2015 un numero maggiore di PMI esternalizza almeno alcuni servizi di sicurezza. Nel 2014 il 24% delle PMI con meno di 499 dipendenti dichiarava di non esternalizzare alcun servizio. Nel 2015 solo il 18% delle PMI ha dichiarato la stessa scelta.

Il fatto che un numero crescente di PMI stia adottando l'esternalizzazione come modo per gestire la sicurezza informatica è positivo perché dimostra che le PMI sono alla ricerca di strumenti flessibili per proteggere le reti, che non vadano a pesare sul loro personale ridotto o sui budget limitati. Tuttavia, le PMI potrebbero credere erroneamente che l'esternalizzazione dei processi di sicurezza riduca notevolmente le probabilità di violazioni della rete oppure potrebbero trasferire la responsabilità della sicurezza a terze parti. Sarebbe un approccio eccessivamente ottimista, in quanto solo un sistema veramente integrato di difesa dalle minacce, che esamini, mitighi e impedisca gli attacchi, può garantire una protezione di livello aziendale.

Figura 39. Un numero maggiore di PMI esternalizza i servizi di sicurezza informatica nel 2015

Quale dei seguenti tipi di servizi relativi alla sicurezza, se esistenti, vengono esternalizzati completamente o in parte a terze parti?

Dimensioni dell'azienda	250-499	500-999	1000-9999	10.000+
Consulenza	46%	51%	54%	55%
Monitoraggio	45%	46%	42%	44%
Controllo	42%	46%	46%	56%
Risposta agli incidenti	39%	44%	44%	40%
Intelligence sulle minacce	35%	37%	42%	41%
Correzione	33%	38%	36%	36%
Nessuno	18%	12%	11%	10%

Perché la tua azienda (PMI 250-499) sceglie di esternalizzare questi servizi?

Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Studio comparativo di Cisco delle infrastrutture di sicurezza

Studio comparativo di Cisco delle infrastrutture di sicurezza

Per valutare le opinioni dei professionisti della sicurezza sullo stato della sicurezza informatica nelle rispettive aziende, Cisco ha chiesto a CSO (Chief Security Officer) e manager delle operazioni di sicurezza (SecOps), in molti 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 2015 offre informazioni approfondite sul livello di maturità delle operazioni e delle procedure di sicurezza informatica attualmente in uso e confronta anche questi risultati con quelli dello studio analogo del 2014.

Un calo di fiducia generale, ma maggiore preparazione

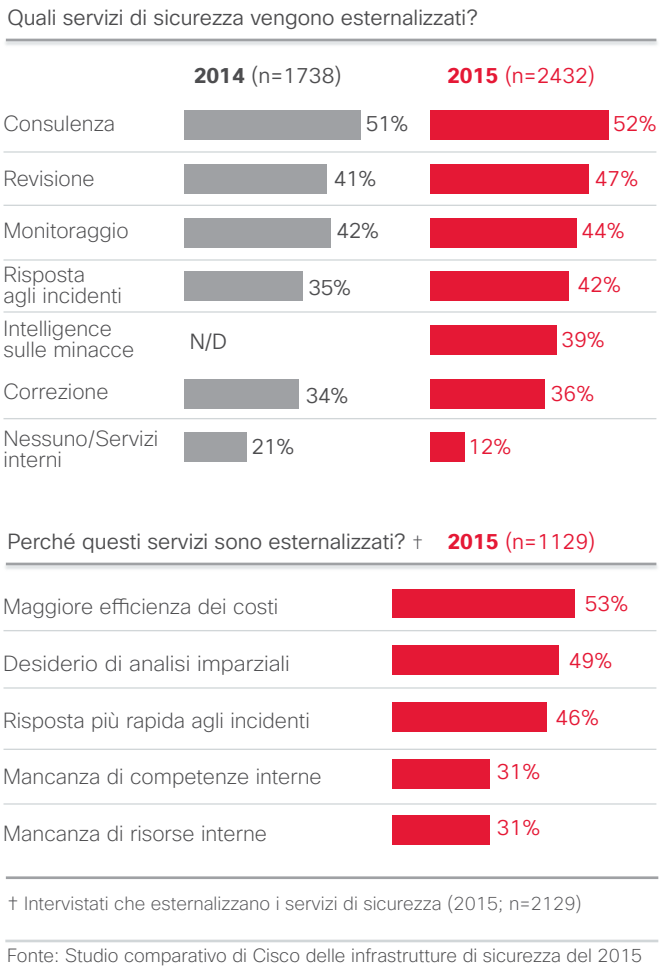
Di fronte all'emergere di minacce sempre più sofisticate, lo studio di Cisco suggerisce che la fiducia degli esperti della sicurezza sembra diminuire. D'altro canto, la maggiore preoccupazione cambia il modo in cui i professionisti proteggono le reti. Ad esempio, si assiste a un aumento della formazione sulla sicurezza, a una crescita nel numero delle policy formali scritte e a una maggiore esternalizzazione di attività come i controlli di sicurezza, la consulenza e la risposta agli incidenti. In breve, gli esperti della sicurezza si dimostrano più attivi nel combattere i rischi che minacciano le proprie reti.

Il maggiore ricorso alla formazione e all'esternalizzazione sono certamente aspetti positivi, ma il settore della sicurezza non può limitarsi a questo. Occorre continuare ad aumentare l'adozione di strumenti e processi per migliorare il rilevamento, il contenimento e la risoluzione delle minacce. Date le barriere rappresentate dai limiti di budget e dalla compatibilità delle soluzioni, il settore deve anche esplorare soluzioni efficaci che offrano una difesa integrata dalle minacce. Il settore deve inoltre migliorare la collaborazione tra le aziende quando si verificano violazioni pubbliche (come con la botnet SSHPsychos, vedere a **pagina 14**), dato che la condivisione delle conoscenze può contribuire a prevenire gli attacchi futuri.

RISORSE: LE AZIENDE PIÙ PROPENSE ALL'ESTERNALIZZAZIONE

A mano a mano che gli esperti della sicurezza prendono coscienza delle minacce, cercano modi per migliorare le loro difese, ad esempio esternalizzando le operazioni di sicurezza che possono essere gestite in modo più efficiente da consulenti o fornitori. Nel 2015 il 47% delle aziende intervistate ha esternalizzato i controlli della sicurezza, una percentuale maggiore rispetto al 41% del 2014. Sempre nel 2015, il 42% ha esternalizzato i processi di risposta agli incidenti, rispetto al 35% del 2014 (Figura 40).

Figura 40. Panoramica dei servizi esternalizzati



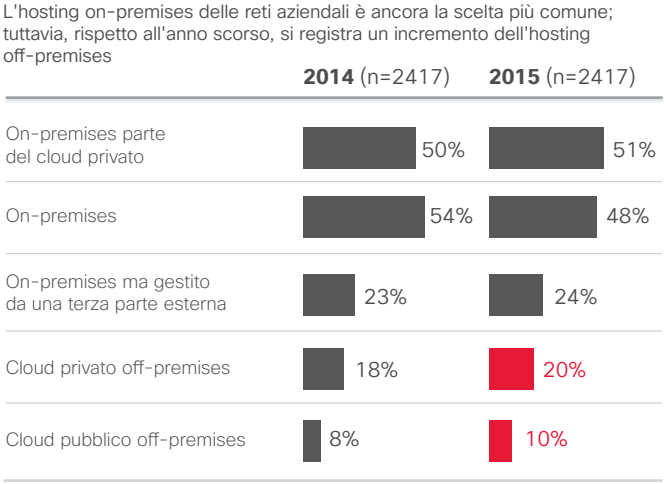
† Intervistati che esternalizzano i servizi di sicurezza (2015; n=2129)

Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Inoltre, un numero più elevato di esperti della sicurezza esternalizza almeno alcune funzioni di sicurezza. Nel 2014, il 21% degli intervistati dichiarava di non esternalizzare alcun servizio di sicurezza. Nel 2015, questa percentuale si è ridotta notevolmente fino al 12%. Il 53% ha dichiarato di esternalizzare i servizi per la maggiore efficienza di questo approccio, mentre il 49% ha dichiarato di esternalizzarli per ottenere analisi imparziali.

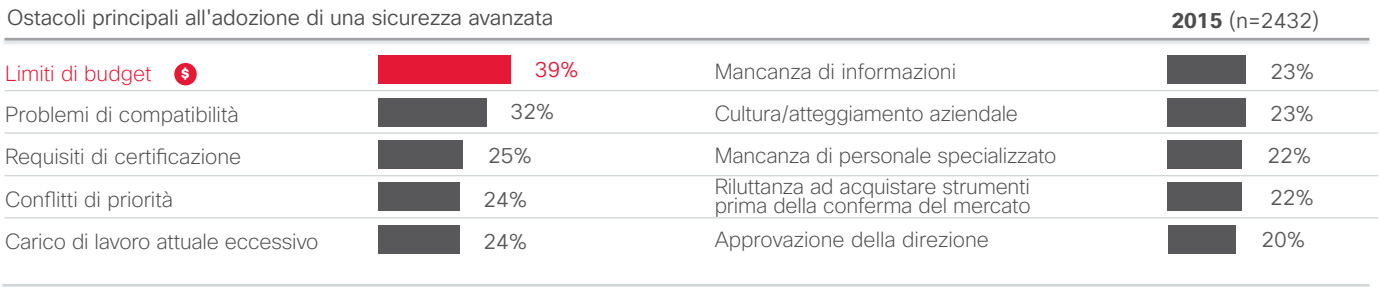
Per proteggere meglio le reti e i dati, gli esperti della sicurezza hanno dichiarato di essere interessati al concetto di hosting delle reti off-premises. Nonostante l'hosting on-premises sia tuttora l'opzione preferita, il numero di professionisti che utilizzano soluzioni off-premises è aumentato. Nel 2015 il 20% ha utilizzato soluzioni di cloud privato off-premises rispetto al 18% del 2014 (Figura 41).

Figura 41. Aumento dell'hosting off-premises



Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

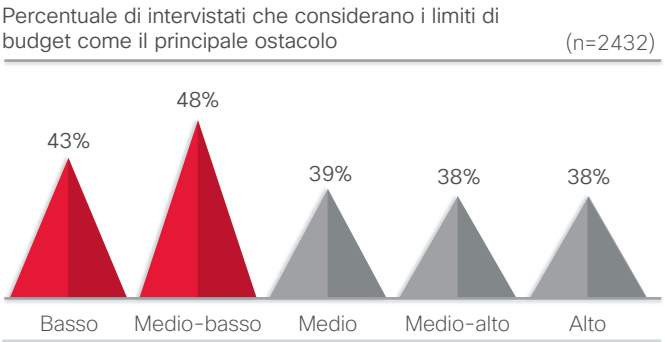
Figura 42. I limiti di budget sono l'ostacolo principale all'aggiornamento della sicurezza



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

I team di sicurezza che hanno partecipato allo studio di Cisco sono più propensi ad attuare una protezione più efficace delle loro reti, ma potrebbero non riuscire a farlo a causa dei vincoli con cui devono misurarsi. Gli esperti della sicurezza hanno affermato che la principale ragione per scegliere o rifiutare i servizi e gli strumenti di sicurezza è rappresentata dai limiti di budget (39%), mentre la compatibilità tecnologica al secondo posto (32%, Figura 42). I limiti di budget diventano un problema ancora maggiore per le aziende con un livello di maturità basso o medio-basso (vedere la Figura 43). Fra le risposte di tutti i professionisti della sicurezza, il 39% ritiene che i limiti di budget siano un ostacolo all'adozione di processi di sicurezza avanzati. Si registra il 43% per le aziende con un livello di maturità basso e il 48% per le aziende con un livello di maturità medio-basso.

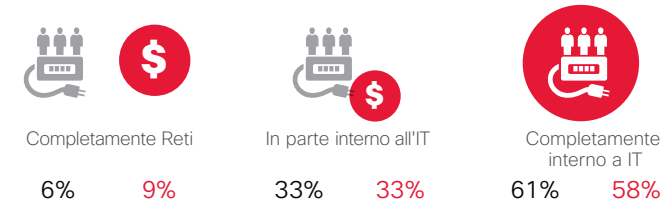
Figura 43. I limiti di budget sono un ostacolo maggiore per le aziende con un livello di maturità basso



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Un segnale che dimostra la maggiore attenzione di alcune aziende per le loro risorse di sicurezza è il modo in cui strutturano il budget per la sicurezza. Il sondaggio mostra un leggero aumento nel numero di aziende che separano il budget della sicurezza dal budget IT complessivo. Nel 2014 il 6% dei professionisti dichiarava di avere budget completamente separati per la sicurezza e l'IT; questa percentuale è salita al 9% nel 2015 (vedere la Figura 44).

Figura 44. Leggero aumento delle aziende con un budget separato per la sicurezza



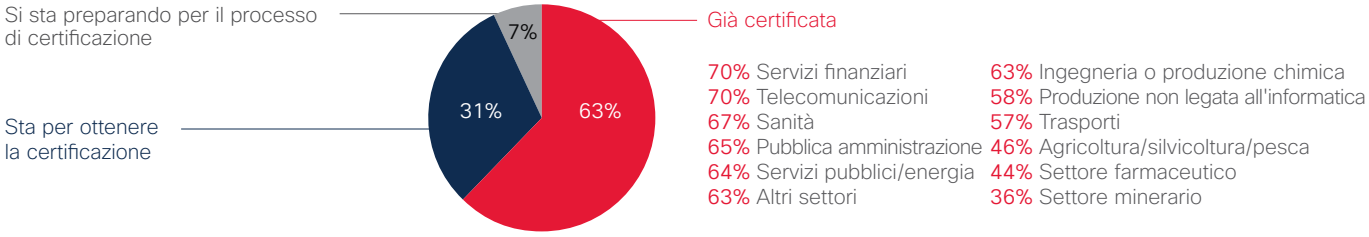
Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

CONDIVIDI

Quando le aziende adottano policy di sicurezza standardizzate o vogliono ottenere le certificazioni, mostrano un impegno a migliorare la sicurezza. Quasi due terzi degli esperti della sicurezza hanno dichiarato che le loro aziende hanno ottenuto o stanno per ottenere la certificazione per le policy o le procedure di sicurezza standardizzate (Figura 45). Questo è un altro segnale positivo del fatto che le aziende ritengono importante migliorare le loro conoscenze sulla sicurezza e rispondere alle minacce.

Figura 45. La maggior parte delle aziende ha ottenuto o sta per ottenere la certificazione

L'azienda segue procedure basate su policy standardizzate per la sicurezza dei dati (**2015**: n=1265)



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Nell'esame dell'uso delle difese di sicurezza, è risultato che i firewall sono gli strumenti di sicurezza più usati dalle aziende (65%), seguiti dagli strumenti di Data Loss Prevention (56%) e da quelli di autenticazione (53%, vedere la Figura 46). Nel 2015, le aziende sono state un po' meno propense a usare gli strumenti basati sul cloud. Sebbene i professionisti della sicurezza abbiano dimostrato la disponibilità all'esternalizzazione dei servizi di sicurezza informatica (vedere a **pagina 43**), potrebbero preferire l'implementazione interna di tali strumenti. Per l'elenco completo vedere a **pagina 71**.

Figura 46. I firewall e Data Loss Prevention sono gli strumenti di sicurezza più usati

Difese contro le minacce alla sicurezza utilizzate dalle aziende	**2014** (n=1738)	**2015** (n=2432)	Difese amministrate tramite servizi basati sul cloud (intervistati che utilizzano le difese contro le minacce alla sicurezza) **2014** (n=1646)	**2015** (n=2268)
Firewall*	N/D	65%		31%
Data Loss Prevention	55%	56%		
Autenticazione	52%	53%		
Crittografia/privacy/protezione dei dati	53%	53%		
Sicurezza e-mail/messaggistica	56%	52%	37%	34%
Web Security	59%	51%	37%	31%
Sicurezza di rete, firewall e prevenzione delle intrusioni*	60%	N/D	35%	

*Firewall e prevenzione delle intrusioni erano un'unica opzione nel 2014: "Sicurezza di rete, firewall e prevenzione delle intrusioni".

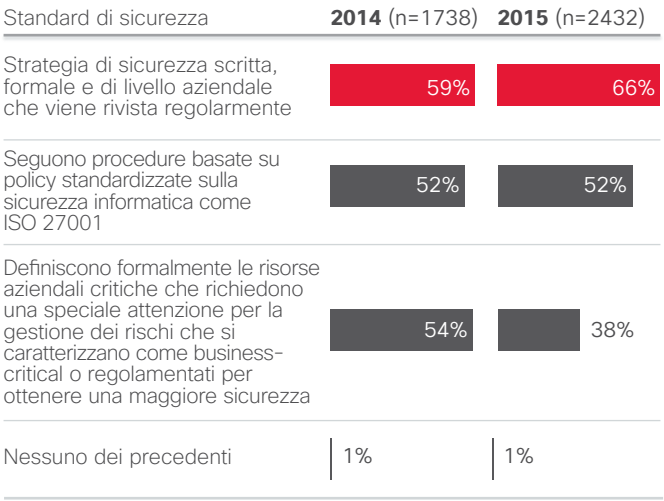
Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

CAPACITÀ: MINORE FIDUCIA NELLA PROPRIA INFRASTRUTTURA

Nel 2015 i professionisti della sicurezza erano meno sicuri che la loro infrastruttura di sicurezza fosse aggiornata rispetto a quanto non lo fossero nel 2014. Questa minore fiducia è dovuta senza dubbio alla sistematicità degli attacchi di alto profilo alle aziende importanti, ai furti dei dati riservati e alle scuse pubbliche da parte delle aziende che hanno subito violazioni nelle loro reti.

Tuttavia, la minore fiducia è accompagnata da un crescente interesse per lo sviluppo di policy più solide. Come mostrato nella Figura 47, un numero maggiore di aziende (66%) disponeva di una strategia di sicurezza scritta e formale nel 2015 rispetto a quelle nella stessa situazione nel 2014 (59%).

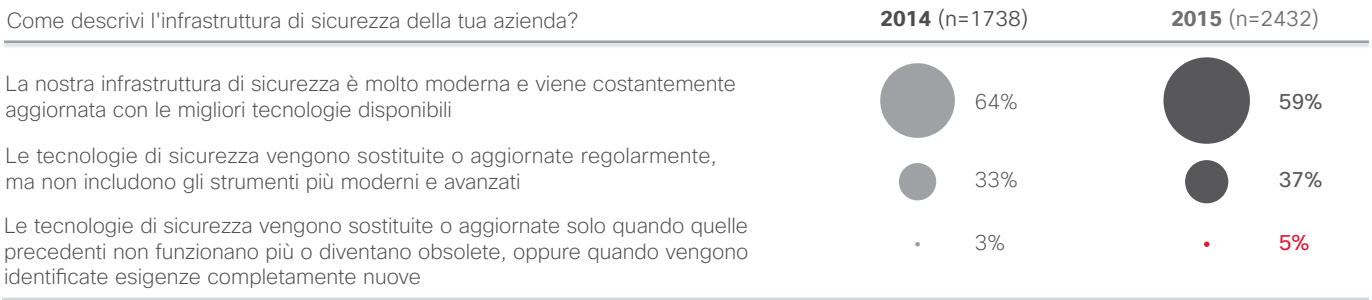
Figura 47. Aumento delle aziende che creano policy di sicurezza formali



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

CONDIVIDI

Figura 48. Calo della fiducia nel 2015

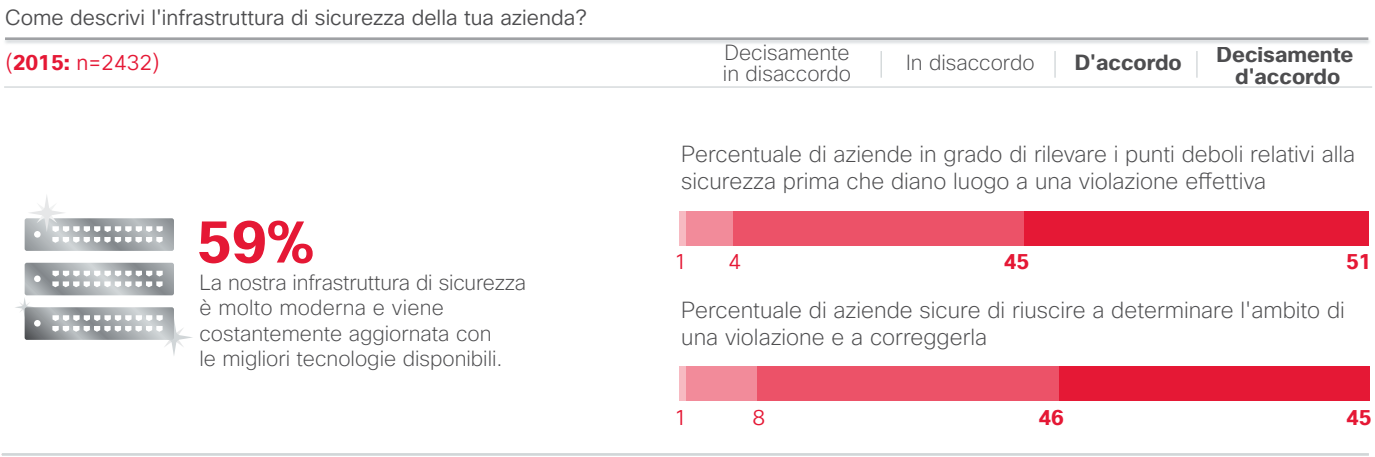


Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Un segnale della flessione di tale fiducia da parte dei professionisti della sicurezza è il fatto che siano un po' meno sicuri delle proprie tecnologie. Nel 2014 il 64% dichiarava che la propria infrastruttura di sicurezza era all'avanguardia e veniva costantemente aggiornata. Nel 2015 tale percentuale è scesa al 59% (Figura 48). Inoltre, nel 2014 il 33% ha affermato che la propria azienda non era fornita di strumenti di sicurezza aggiornati; il numero è salito al 37% nel 2015.

La fiducia è un po' maggiore fra i CSO, che sono più ottimisti dei manager di SecOps: il 65% dei CSO ritiene che la propria infrastruttura di sicurezza sia aggiornata, rispetto al 54% dei manager di SecOps. La fiducia dei manager di SecOps è probabilmente minore in quanto essi rispondono agli incidenti giornalieri di sicurezza e ciò offre loro una visione meno positiva del livello di sicurezza aziendale.

Figura 49. Fiducia variabile nella capacità di rilevare le violazioni

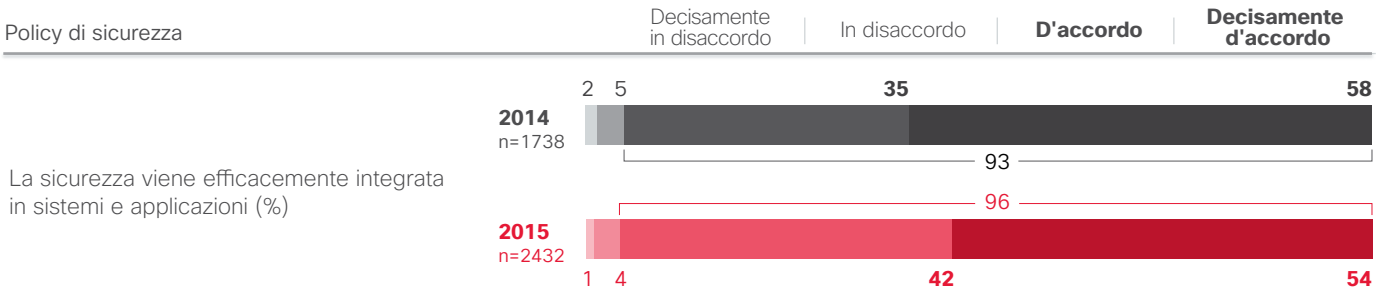


Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

I professionisti della sicurezza mostrano inoltre livelli diversi di fiducia in termini di capacità di contrastare gli attacchi. Il 51% ritiene di essere decisamente in grado di individuare i punti deboli relativi alla sicurezza prima che diventino violazioni vere e proprie; solo il 45% è sicuro della propria capacità di determinare l'ambito di una compromissione della rete e di rimediare al danno (vedere la Figura 49).

I professionisti della sicurezza mostrano anche minore fiducia nella propria capacità di difendere la rete da attacchi. Ad esempio, nel 2015 un numero minore di professionisti è decisamente convinto di riuscire a integrare efficacemente la sicurezza nelle procedure di acquisizione, sviluppo e mantenimento dei sistemi (il 54% nel 2015 rispetto al 58% del 2014, vedere la Figura 50). Per l'elenco completo vedere a **pagina 76**.

Figura 50. Minore fiducia nella capacità di integrare la sicurezza nei sistemi



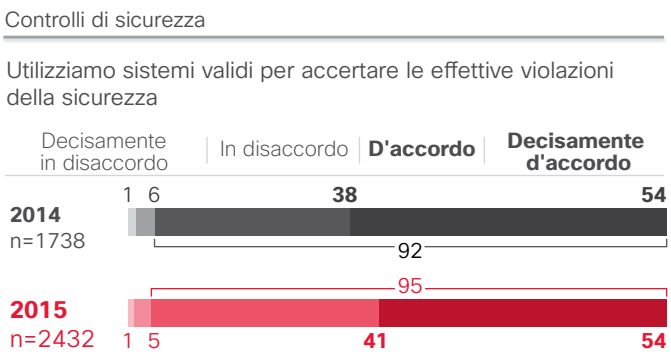
Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

CONDIVIDI

In alcune aree, i livelli di fiducia nelle capacità di sicurezza non sono molto alti. Ad esempio, nel 2015 solo il 54% degli intervistati ritiene di avere un ottimo sistema per accertare le effettive violazioni della sicurezza (vedere la Figura 51). Per l'elenco completo vedere a **pagina 77**.

Gli intervistati inoltre non sono completamente certi che i loro sistemi possano determinare l'ambito e contenere tali violazioni. Il 56% ha dichiarato di rivedere e migliorare le procedure di sicurezza in modo regolare, formale e strategico; il 52% ritiene che le proprie tecnologie di sicurezza siano ben integrate e interagiscano efficacemente (vedere la Figura 52). Per l'elenco completo vedere a **pagina 79**.

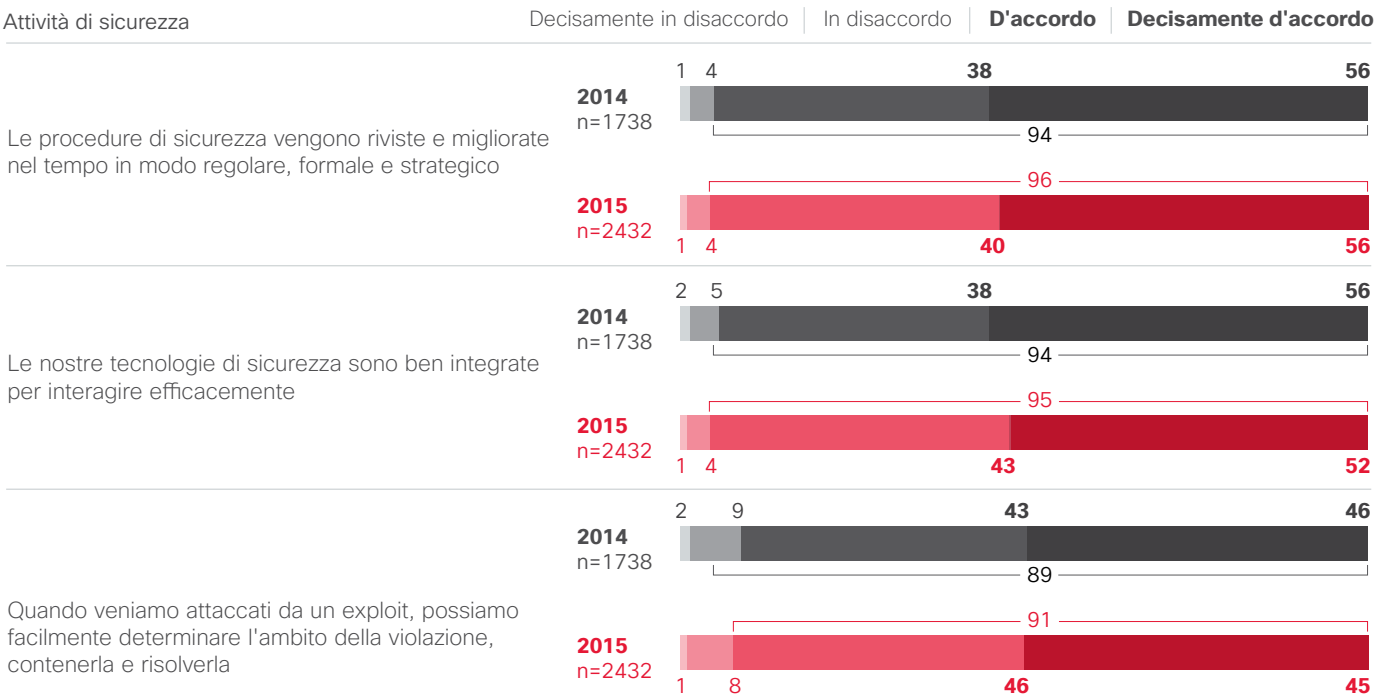
Figura 51. Le aziende ritengono di possedere validi controlli di sicurezza



Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

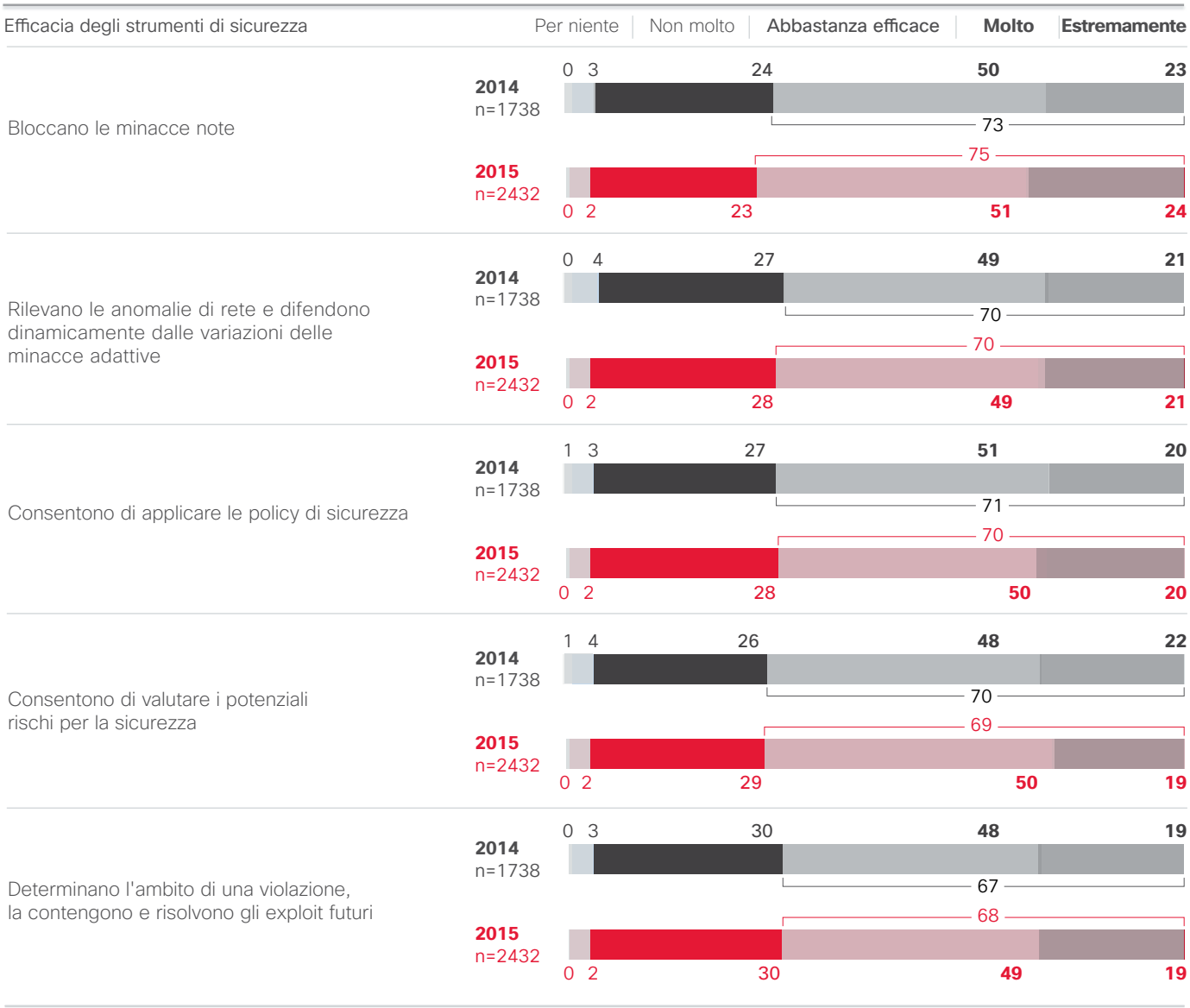
CONDIVIDI

Figura 52. Le aziende esprimono una fiducia variabile nella capacità di contenere le violazioni



Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Figura 53. Un quarto delle aziende ritiene che gli strumenti di sicurezza siano solo parzialmente efficaci



Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

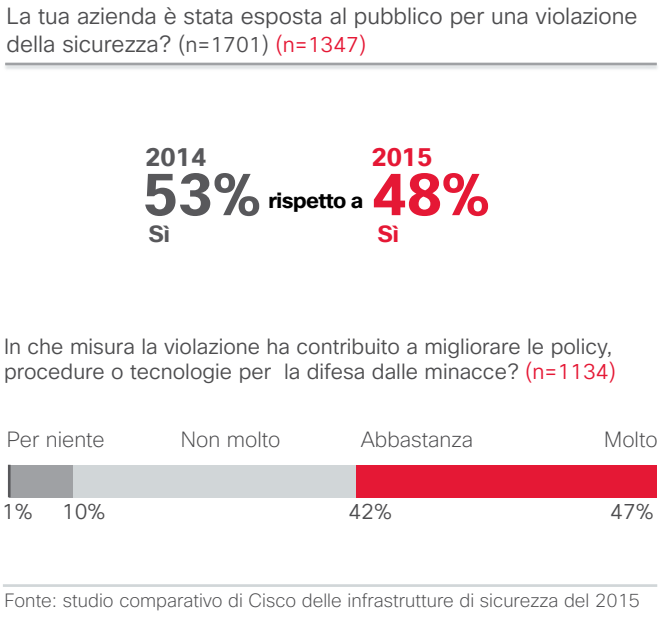
Analogamente agli intervistati del 2014, più di un quarto dei professionisti della sicurezza nel 2015 ha dichiarato di percepire i propri strumenti di sicurezza come solo parzialmente efficaci (Figura 53).

Le violazioni esposte al pubblico tendono a essere un evento determinante per le aziende. Quando si verificano, le aziende sembrano diventare più consapevoli della necessità di impedire violazioni future. Tuttavia, nel 2015 un numero minore di professionisti della sicurezza ha dichiarato che le proprie aziende hanno subito violazioni esposte al pubblico: in particolare il 53% dei professionisti nel 2014 e il 48% nel 2015 (Figura 54).

I professionisti riconoscono il valore delle violazioni in quanto campanelli d'allarme sull'importanza di rafforzare i processi di sicurezza: il 47% dei professionisti della sicurezza colpiti da violazioni pubbliche ha affermato che tali violazioni hanno dato origine a migliori policy e procedure. Ad esempio, il 43% degli intervistati ha dichiarato di aver potenziato la formazione sulla sicurezza dopo una violazione pubblica e il 42% ha affermato di aver incrementato gli investimenti nelle tecnologie di difesa.

L'aspetto positivo è che le aziende che hanno subito una violazione pubblica sono sempre più propense a rafforzare le procedure di sicurezza. Nel 2015 il 97% degli esperti della sicurezza ha affermato di effettuare formazione sulla sicurezza almeno una volta l'anno, un notevole incremento rispetto all'82% del 2014 (vedere la Figura 90 a **pagina 82**).

Figura 54. Le violazioni pubbliche possono contribuire a migliorare la sicurezza



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Figura 55. Un numero maggiore di aziende effettua formazione sulla sicurezza

Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

MATURITÀ: I LIMITI DI BUDGET SONO L'OSTACOLO PRINCIPALE A TUTTI I LIVELLI

A mano a mano che le aziende implementano procedure e policy di sicurezza più sofisticate, la loro percezione dei propri livelli di sicurezza può cambiare. Lo studio comparativo di Cisco delle infrastrutture di sicurezza del 2015 divide i partecipanti al sondaggio e le loro aziende in cinque categorie relativamente alla maturità in base alle risposte sui processi di sicurezza (Figura 56). Lo studio analizza il modo in cui diverse caratteristiche, come le capacità, i settori e i paesi, possono influire sui livelli di maturità.

È interessante osservare come aziende a diversi livelli di maturità sembrino condividere alcuni degli ostacoli all'implementazione di processi e strumenti di sicurezza più sofisticati. Sebbene le esatte percentuali possano variare, il problema dei limiti di budget si colloca al primo posto a tutti i livelli di maturità (Figura 57).

Figura 56. Il modello della maturità classifica le aziende in base ai processi di sicurezza

Cisco ha esaminato varie opzioni di segmentazione del campione prima di scegliere una soluzione con cinque segmenti basata su una serie di domande relative ai processi di sicurezza. I cinque segmenti della soluzione possono essere facilmente associati ai livelli del modello CMMI (Capability Maturity Model Integration).

	Livello		Soluzione con 5 segmenti
In fase di ottimizzazione	1	Attenzione rivolta al miglioramento dei processi	Alto
Gestito in modo quantitativo	2	Processi misurati e monitorati in modo quantitativo	Medio-alto
Definito	3	Processi caratterizzati per l'organizzazione, spesso proattivi	Medio
Ripetibile	4	Processi caratterizzati per i progetti, spesso reattivi	Medio-basso
Iniziale	5	Processi ad hoc, imprevedibili	Basso

Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Figura 57. Gli ostacoli all'adozione di una sicurezza migliore indipendentemente dal livello di maturità

Quale dei seguenti fattori è secondo te l'ostacolo maggiore per l'adozione di processi e tecnologie avanzate per la sicurezza?

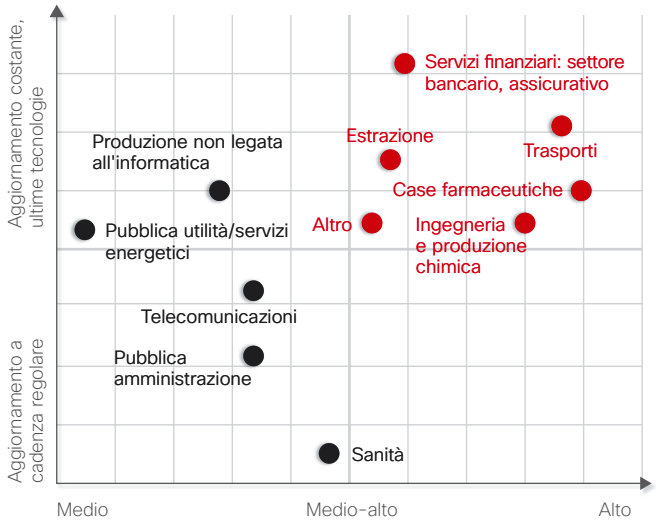
Livello di sofisticatezza	Basso	Medio-basso	Medio	Medio-alto	Alto
Limiti di budget	43%	48%	39%	38%	38%
Approvazione della direzione	14%	20%	20%	22%	19%
Conflitti di priorità	19%	27%	26%	26%	22%
Mancanza di personale specializzato	21%	27%	22%	19%	23%
Mancanza di informazioni su processi e tecnologie di sicurezza avanzata	31%	20%	25%	23%	22%
Problemi di compatibilità con sistemi legacy	21%	28%	29%	34%	33%
Requisiti di certificazione	14%	17%	26%	27%	25%
Atteggiamento e cultura aziendale sulla sicurezza	31%	23%	23%	22%	21%
Riluttanza ad acquistare strumenti prima della conferma del mercato	12%	25%	24%	25%	19%
Carico di lavoro attuale eccessivo per poter assumere nuove responsabilità	36%	23%	25%	25%	22%

Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Il grafico a destra mostra la relazione tra la qualità dell'infrastruttura di sicurezza e i livelli di maturità dei vari settori e si basa sul modo in cui gli intervistati percepiscono i propri processi di sicurezza. I settori che appaiono nel quadrante in alto a destra mostrano i massimi livelli di maturità e di qualità dell'infrastruttura.

Il grafico seguente illustra le posizioni dei livelli di maturità definiti da Cisco per settore. Nel 2015 quasi la metà delle aziende di trasporti e farmaceutiche intervistate si trova nel segmento con maturità elevata. Le aziende di telecomunicazioni e di servizi pubblici hanno meno probabilità di trovarsi nel segmento con maturità elevata nel 2015 rispetto al 2014. I risultati sono basati sul modo in cui gli intervistati percepiscono i propri processi di sicurezza.

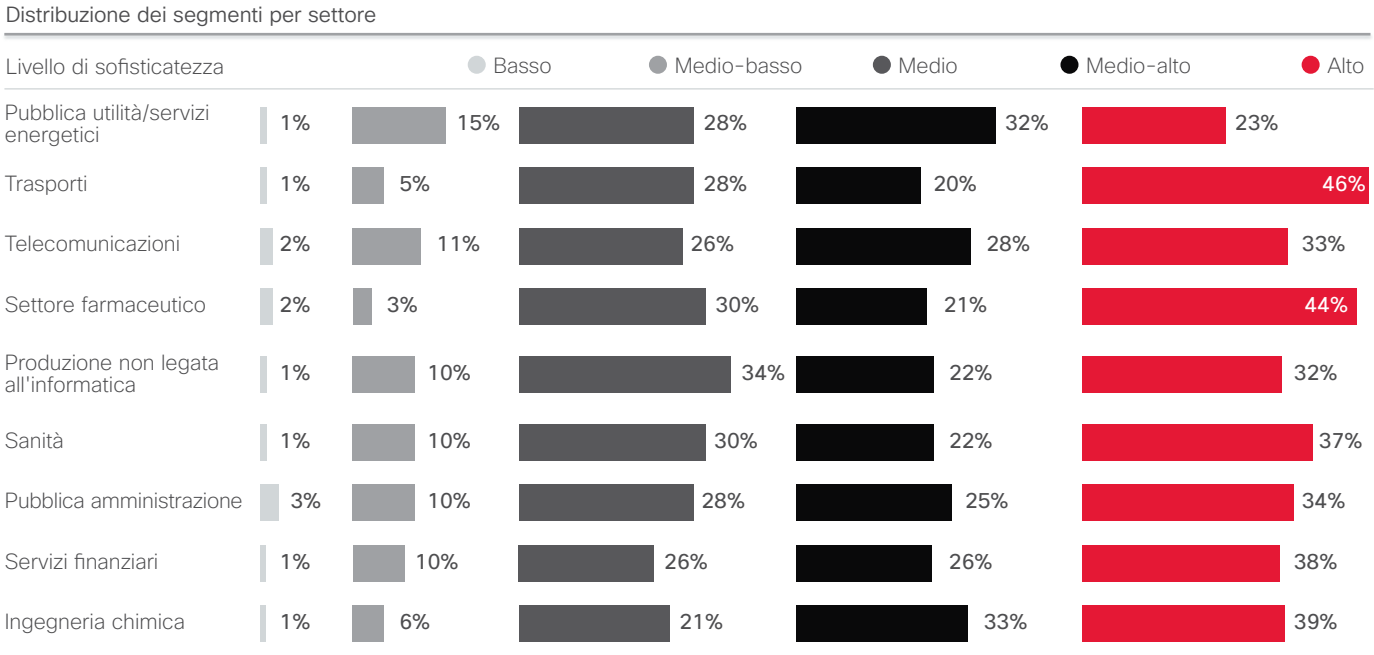
Figura 58. Valutazione della maturità della sicurezza per infrastruttura e settore



Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

CONDIVIDI

Figura 59. Livelli di maturità per settore

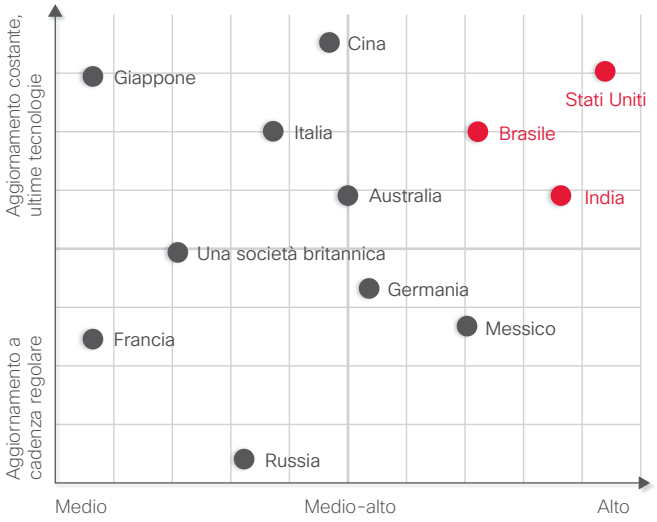


Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Il grafico a destra mostra la relazione tra la qualità dell'infrastruttura di sicurezza e i livelli di maturità di vari paesi. I paesi che appaiono nel quadrante in alto a destra mostrano i massimi livelli di maturità e di qualità dell'infrastruttura. È importante notare che questi risultati sono basati sul modo in cui gli esperti della sicurezza percepiscono il proprio livello di sicurezza.

Il grafico seguente illustra le posizioni dei livelli di maturità definiti da Cisco per paese. I risultati sono basati sul modo in cui gli intervistati percepiscono i propri processi di sicurezza.

Figura 60. Valutazione della maturità della sicurezza per infrastruttura e paese



Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Figura 61. Livelli di maturità per paese

Distribuzione dei segmenti per paese — **2014** (n=1637) — **2015** (n=2401)

Livello di sofisticatezza	2014	Basso	Medio-basso	Medio	Medio-alto	Alto
Stati Uniti	3% / 2%	10% / 4%	27% / 22%	16% / 27%	44% / 45%	
Brasile	2% / 1%	5% / 9%	24% / 24%	35% / 26%	34% / 40%	
Germania	1% / 1%	4% / 12%	27% / 24%	25% / 24%	43% / 39%	
Italia	1% / 4%	23% / 3%	13% / 36%	25% / 23%	38% / 34%	
Regno Unito	8% / 0%	8% / 14%	25% / 32%	18% / 22%	41% / 32%	
Australia	9% / 1%	7% / 5%	19% / 29%	35% / 36%	30% / 29%	
Cina	0% / 0%	3% / 6%	32% / 37%	29% / 25%	36% / 32%	
India	7% / 1%	3% / 4%	20% / 21%	16% / 34%	54% / 40%	
Giappone	7% / 2%	15% / 16%	14% / 34%	40% / 16%	24% / 32%	
Messico	6%	8%	20%	16%	50%	
Russia	1%	14%	27%	26%	32%	
Francia	1%	15%	35%	20%	29%	

Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

CONSIGLI: REAGIRE ALLA REALTÀ DELLE MINACCE

Come dimostra lo studio comparativo delle infrastrutture di sicurezza, i professionisti della sicurezza stanno prendendo consapevolezza della realtà. La fiducia degli esperti della sicurezza nella loro capacità di bloccare gli hacker vacilla. Tuttavia, la lezione appresa dagli exploit di alto profilo ha avuto un impatto positivo sul settore, a giudicare dall'aumento della formazione sulla sicurezza e dello sviluppo di policy formali. Inoltre, la più frequente esternalizzazione dei controlli e dei servizi di risposta agli incidenti indica che i responsabili della sicurezza cercano l'assistenza di esperti.

Le aziende devono continuare a misurare le proprie capacità in termini di sicurezza informatica e i professionisti della sicurezza devono promuovere la crescita del budget destinato alla tecnologia e al personale. Inoltre, la fiducia aumenterà quando i professionisti della sicurezza adotteranno strumenti in grado non solo di rilevare le minacce, ma anche di contenerne l'impatto e di facilitare la prevenzione degli attacchi futuri.

Uno sguardo al futuro

Uno sguardo al futuro

Gli esperti di geopolitica Cisco presentano un'analisi dettagliata del panorama della governance di Internet, che include i cambiamenti nella legislazione che regola il trasferimento dei dati e il dibattito sull'uso della crittografia. In questa sezione sono inoltre riportati alcuni risultati tratti da due studi condotti da Cisco. Il primo prende in esame le problematiche della sicurezza informatica dal punto di vista dei vertici aziendali. Il secondo è incentrato sulle opinioni dei responsabili delle decisioni IT relativamente ai rischi per la sicurezza e l'affidabilità. Presentiamo anche una panoramica dei vantaggi offerti da un'architettura integrata per la difesa dalle minacce e un aggiornamento sui progressi realizzati da Cisco nel ridurre i tempi di rilevamento delle minacce.

Prospettiva geopolitica: le incertezze nel panorama della governance di Internet

Nell'era post Edward Snowden, il panorama geopolitico per la governance di Internet è sensibilmente cambiato. Oggi c'è un senso di incertezza generale rispetto al libero flusso di informazioni tra gli stati. Il caso di riferimento introdotto dall'attivista austriaco per la privacy Max Schrems contro il gigante dei social network Facebook ha forse avuto l'impatto maggiore, portando la Corte di giustizia dell'Unione Europea (CGUE) a invalidare la decisione relativa ai principi dell'approdo sicuro (safe harbor) per lo scambio di dati degli Stati Uniti il 6 ottobre 2015[7].

Di conseguenza le aziende sono ora costrette a fare affidamento su meccanismi e tutele legali diverse dai principi dell'approdo sicuro (safe harbor) nel momento in cui trasferiscono dati dall'Unione Europea agli Stati Uniti che, a loro volta, sono soggetti a indagine. Le aziende che gestiscono dati stanno ancora tentando di valutare le conseguenze di questo cambiamento. Inoltre mentre le autorità di Stati Uniti e UE da due anni collaborano a una proposta per sostituire i principi dell'approdo sicuro (safe harbor), sorgono timori sul nuovo meccanismo previsto. Potrebbe non essere pronto entro la scadenza prevista di gennaio 2016 oppure, più probabilmente, non riuscire nel suo intento di ripristinare la fiducia del mercato se non è in grado di rispondere pienamente alle preoccupazioni della CGUE, andando così ancora incontro al rischio di invalidamento[8].

Gli esperti di protezione dei dati non si aspettano che i principi Safe Harbor 2.0 siano meno controversi di quelli precedenti. È altresì possibile che seguano lo stesso percorso e vengano sottoposti al giudizio della corte e magari dichiarati invalidi[9].

Un ulteriore argomento che nel nuovo anno sarà oggetto di grande dibattito tra governi e industria è la crittografia completa, che porta con sé vantaggi per i consumatori e per le aziende, ma anche difficoltà poste alle forze dell'ordine durante le indagini sulle attività criminali e terroristiche. Gli attacchi terroristici del novembre 2015 a Parigi hanno spinto alcuni governi a cercare di offrire maggiore libertà alle indagini per accedere ai contenuti delle comunicazioni crittografate[10]. Questa situazione potrebbe fornire nuovo slancio allo sviluppo dei principi del Safe Harbor 2.0, ponendo i diritti civili in secondo piano rispetto ai timori per la sicurezza pubblica.

[7] "La Corte dichiara invalida la decisione della Commissione che attesta che gli Stati Uniti garantiscono un adeguato livello di protezione dei dati personali trasferiti", CGUE, 6 ottobre 2015: **http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117it.pdf**.

[8] "Safe Harbor 2.0 framework begins to capsize as January deadline nears", di Glyn Moody, *Ars Technica*, 16 novembre 2015: **http://arstechnica.com/tech-policy/2015/11/safe-harbour-2-0-framework-begins-to-capsize-as-january-deadline-nears/**.

[9] "Safe Harbor 2.0 framework begins to capsize as January deadline nears", di Glyn Moody, *Ars Technica*, 16 novembre 2015: **http://arstechnica.com/tech-policy/2015/11/safe-harbour-2-0-framework-begins-to-capsize-as-january-deadline-nears/**.

[10] "Paris Attacks Fan Encryption Debate" di Danny Yadron, Alistair Barr e Daisuke Wakabayashi, *The Wall Street Journal*, 19 novembre 2015: **http://www.wsj.com/articles/paris-attacks-fan-encryption-debate-1447987407**.

A fronte di tali incertezze, cosa devono chiedere le aziende ai provider di dati per essere certe di essere conformi alle normative sul trasferimento dati? Nell'immediato devono sicuramente ottenere dai fornitori la garanzia di usare le clausole contrattuali tipo della UE o le norme vincolanti d'impresa, e non solo il Safe Harbor, quando trasferiscono i dati al di fuori dell'Unione Europea.

Un'altra grande questione geopolitica che le aziende dovrebbero monitorare riguarda le vulnerabilità e gli attacchi. Alcuni governi esprimono grandi preoccupazioni circa la crescita di un mercato rivolto alle vulnerabilità non risolte da patch, il cosiddetto software "armato". Questi strumenti sono indispensabili alla community di ricercatori sulla sicurezza, dal momento che permettono di cercare modi per proteggere le reti in tutto il mondo. Nelle mani sbagliate, in particolare quelle di regimi oppressivi, questa tecnologia progettata a fin di bene potrebbe però essere utilizzata per crimini finanziari, per rubare segreti commerciali e nazionali, per la repressione politica o per interferire con infrastrutture importanti.

Come limitare l'accesso alle vulnerabilità non risolte senza ostacolare la ricerca è un problema che i governi dovranno sicuramente affrontare nei mesi e negli anni a venire. Mentre i governi cercano di risolvere questo problema spinoso, devono anche valutare attentamente come le loro decisioni influiscano sulla sicurezza. Ad esempio, il clima di incertezza che circonda le norme che disciplinano la trasmissione di informazioni sulle vulnerabilità non pubblicate potrebbe da un lato frenare il progresso della ricerca o dall'altro incoraggiare la pubblicazione delle vulnerabilità prima che i fornitori abbiano la possibilità di creare le patch. Qualsiasi approccio per la risoluzione di questa incertezza dovrà essere applicabile a livello mondiale.

Le problematiche della sicurezza informatica gravano sui vertici aziendali

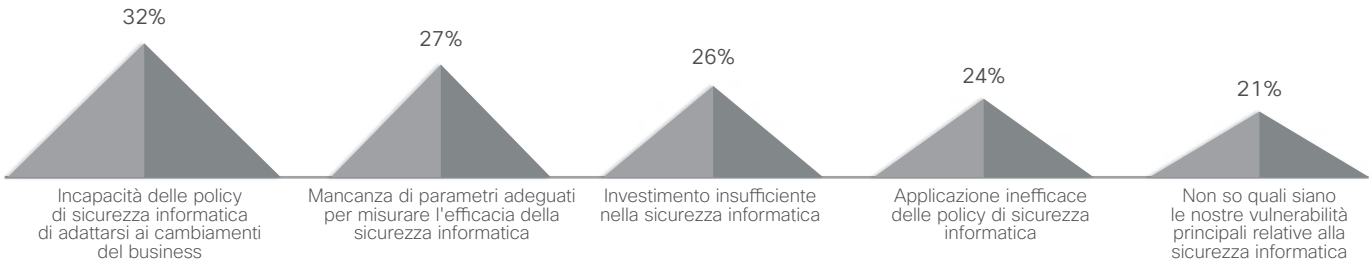
Come è ovvio, un'infrastruttura di sicurezza solida può aiutare le aziende a evitare intrusioni e attacchi catastrofici. Ma può migliorare le possibilità di successo economico di un'azienda? Secondo uno studio condotto da Cisco a ottobre 2015 per valutare l'opinione dei dirigenti dei reparti finanziari e delle line-of-business in merito al ruolo della sicurezza informatica nel business e nella strategia digitale, i vertici delle imprese sono consapevoli che proteggere l'azienda possa essere la discriminante tra successo e fallimento. Man mano che le aziende adottano il digitale, la crescita dipenderà sempre di più dalla capacità di proteggere la piattaforma digitale.

Come mostrato dal sondaggio, la sicurezza informatica è una preoccupazione per i dirigenti: il 48% ha affermato di essere molto preoccupato e il 39% ha dichiarato di essere abbastanza preoccupato dalle violazioni. Tali timori sono in aumento; il 41% ha dichiarato di essere molto più preoccupato per le violazioni della sicurezza rispetto a tre anni fa e il 42% ha dichiarato di essere un po' più preoccupato rispetto al passato.

I leader aziendali prevedono anche che le esigenze e i requisiti degli investitori e dei regolatori in merito ai processi di sicurezza diventeranno più rigidi, analogamente alle altre funzioni aziendali. Il 92% degli intervistati concorda sul fatto che i regolatori e gli investitori in futuro richiederanno alle aziende più informazioni riguardo all'esposizione ai rischi di sicurezza informatica.

Le aziende inoltre sembrano essere consapevoli delle sfide per la sicurezza informatica che devono affrontare. L'incapacità delle policy di sicurezza informatica di adattarsi ai cambiamenti del business è stata la difficoltà citata più spesso, seguita dalla mancanza di parametri adeguati per misurare l'efficacia della sicurezza (figura 62).

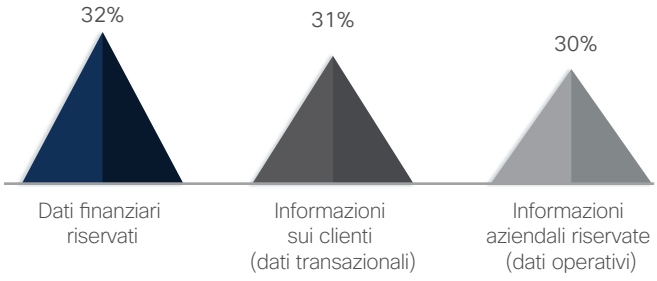
Figura 62. Le aziende devono affrontare sfide complesse per la sicurezza informatica



Fonte: Cisco Security Research

Circa un terzo dei dirigenti è inoltre preoccupato per la propria capacità di salvaguardare i dati importanti. Alla domanda che chiedeva di specificare il tipo di informazioni più difficili da proteggere, il 32% ha indicato i "dati finanziari riservati". Gli altri due tipi di dati indicati dagli intervistati sono "informazioni sui clienti" e "informazioni aziendali riservate" (vedere la figura 63).

Figura 63. I dirigenti sono preoccupati per la protezione dei dati importanti



Fonte: Cisco Security Research

Studio sull'affidabilità: evidenziare i rischi e le sfide per le aziende

L'aumento inesorabile delle violazioni della sicurezza informatica evidenzia la necessità fondamentale per le aziende di essere certe che sistemi, dati, partner, clienti e cittadini siano protetti. L'affidabilità sta diventando uno dei fattori principali considerati dalle aziende nella scelta dell'infrastruttura IT e di rete. Di fatto molte aziende ora richiedono che la sicurezza e l'affidabilità vengano integrate per tutto il ciclo di vita delle soluzioni implementate nell'infrastruttura.

Nell'ottobre 2015 Cisco ha condotto uno studio per valutare le opinioni dei responsabili IT rispetto ai rischi e alle problematiche per la sicurezza e per stabilire quanto sia determinante l'affidabilità del fornitore negli investimenti IT effettuati. Abbiamo intervistato i responsabili delle decisioni sia della sicurezza informatica che di altre aree presso alcune aziende di paesi diversi. Vedere l'**Appendice** per ulteriori informazioni sullo Studio sul rischio per la sicurezza e l'affidabilità, inclusa la nostra metodologia.

DI SEGUITO RIPORTIAMO ALCUNI RISULTATI DELLA NOSTRA RICERCA:

Abbiamo rilevato che il 65% degli intervistati pensa che la propria azienda debba fronteggiare un livello significativo di rischio per la sicurezza, dovuto in particolare all'uso di soluzioni per la mobilità, per la sicurezza IT e soluzioni basate sul cloud nell'azienda (figura 64).

Figura 64. La percezione del rischio per la sicurezza informatica

Fonte: Studio di Cisco sul rischio per la sicurezza e sull'attendibilità

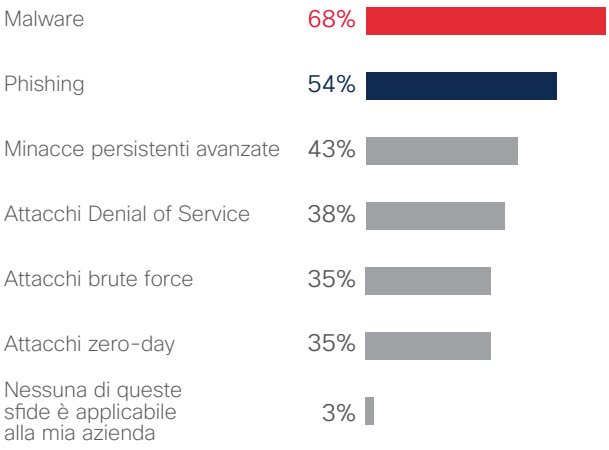
Il 68% degli intervistati ha indicato il malware come il rischio principale esterno per la sicurezza dell'azienda. Phishing e minacce avanzate persistenti completano la classifica delle prime tre risposte, attestandosi rispettivamente al 54% e al 43% (vedere la figura 65).

Per quanto riguarda i rischi interni (vedere la figura 66), oltre la metà (54%) degli intervistati ha citato il download di software dannoso come minaccia principale, seguita dalle violazioni interne della sicurezza da parte dei dipendenti (47%) e dalle vulnerabilità di hardware e software (46%).

Abbiamo rilevato inoltre che la maggior parte delle aziende (92%) dispone di un apposito team interno responsabile della sicurezza. L'88% degli intervistati ha dichiarato di disporre di una strategia di sicurezza formale a livello aziendale che viene rinnovata regolarmente. Tuttavia solo il 59% degli intervistati dispone di policy e procedure standardizzate per approvare l'affidabilità dei fornitori IT (vedere la figura 67).

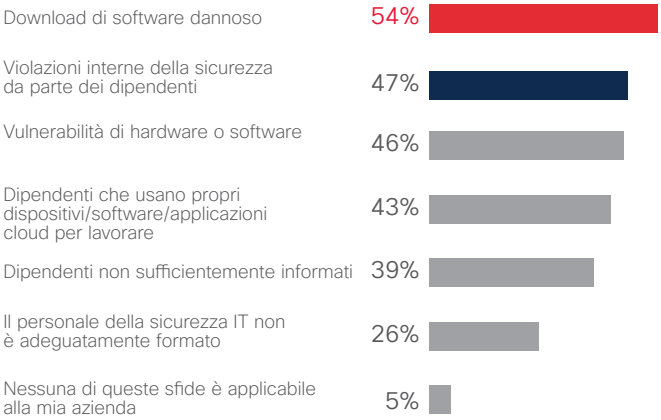
Inoltre circa la metà (49%) delle grandi aziende mantiene aggiornata la propria infrastruttura di sicurezza con le tecnologie più recenti e la maggior parte delle altre aggiorna regolarmente la propria infrastruttura. Secondo il nostro studio, un numero molto basso di aziende invece attende che la tecnologia in uso diventi obsoleta prima di procedere con l'aggiornamento.

Figura 65. I rischi esterni della sicurezza (totale intervistati)



Fonte: Studio di Cisco sul rischio per la sicurezza e sull'attendibilità

Figura 66. I rischi interni della sicurezza (totale intervistati)



Fonte: Studio di Cisco sul rischio per la sicurezza e sull'attendibilità

Figura 67. La maggior parte delle grandi aziende ha un team di sicurezza interno

Fonte: Studio di Cisco sul rischio per la sicurezza e sull'attendibilità

In che modo i fornitori possono dimostrare la propria affidabilità

Nell'attuale panorama delle minacce per stabilire un rapporto duraturo tra fornitori e aziende è fondamentale che le aziende abbiano fiducia in processi, policy, tecnologie e personale del fornitore e la possibilità di verificare tutti questi punti.

I fornitori di tecnologia possono dimostrare la propria affidabilità in questi modi:

- integrando la sicurezza nelle loro soluzioni e nella catena del valore fin dall'inizio
- definendo e adottando policy e processi che riducano il rischio
- promuovendo una cultura di informazione sulla sicurezza
- rispondendo alle violazioni in tempi rapidi e in modo trasparente
- fornendo un intervento di risoluzione rapido e la vigilanza costante dopo un incidente.

L'aggiornamento dell'infrastruttura è naturalmente una buona pratica. Le aziende di ogni dimensione hanno bisogno di implementare un'infrastruttura sicura e affidabile in cui la sicurezza sia integrata in tutti gli aspetti della rete. Possono tuttavia contribuire a ridurre la superficie di attacco promuovendo una cultura aperta e informata sulle esigenze della sicurezza.

Per creare questa cultura è necessario implementare policy e processi coerenti a livello aziendale per garantire che la sicurezza sia profondamente integrata in tutti gli aspetti dell'attività. Le aziende devono quindi fare in modo che questa cultura incentrata sulla sicurezza venga adottata anche dal proprio ecosistema di partner e fornitori e devono dimostrare continuamente la trasparenza e l'affidabilità nei confronti di clienti, partner e altri stakeholder.

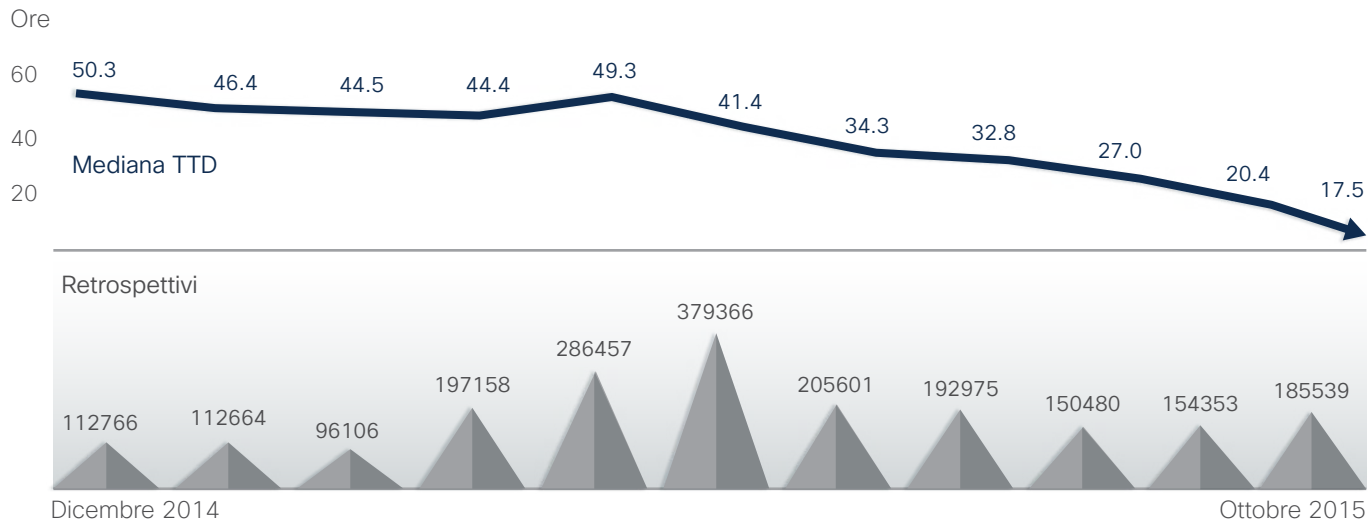
Rilevamento delle minacce: la corsa contro il tempo

Il termine tecnico "time to detection" o "TTD" indica il periodo di tempo che intercorre fra la prima osservazione di un file sconosciuto e il rilevamento della minaccia. Questo periodo di tempo viene determinato utilizzando dati telemetrici di sicurezza, raccolti con il consenso degli utenti dai prodotti di sicurezza Cisco distribuiti in tutto il mondo.

La categoria "retrospettivi" della figura 68 mostra il numero di file che Cisco ha classificato inizialmente come "sconosciuti" e in seguito ridefinito come "notoriamente dannosi".

Come indicato nel Report semestrale di Cisco sulla sicurezza 2015, la mediana del TTD è di circa due giorni (50 ore).

Figura 68. Time to detection da dicembre 2014 a ottobre 2015



Fonte: Cisco Security Research

Da gennaio a marzo la mediana del TTD è rimasta sostanzialmente invariata, attestandosi tra 44 e 46 ore, ma con una leggera diminuzione. Ad aprile è aumentata leggermente, raggiungendo le 49 ore. Verso la fine del mese di maggio il TTD per Cisco era comunque diminuito arrivando a circa 41 ore.

Da quel momento la mediana del TTD ha continuato a diminuire rapidamente. A partire da ottobre Cisco ha ridotto la mediana del TTD a circa 17 ore, ossia meno di un giorno. Questo supera di gran lunga l'attuale stima del settore per il TTD (da 100 a 200 giorni). La velocità è dovuta all'inclusione di maggiori dettagli su come mitigare il rischio delle infezioni di breve durata.

La trasformazione delle attività degli hacker in un vero e proprio settore commerciale e l'uso del "commodity malware" rivestono un ruolo importante nella nostra capacità di ridurre il TTD. Non appena una minaccia viene commercializzata, si diffonde maggiormente e quindi è molto più facile da rilevare.

Pensiamo tuttavia che la combinazione di sofisticate difese contro le minacce e la stretta collaborazione tra i ricercatori esperti di sicurezza abbia avuto probabilmente un ruolo ancora più importante per la nostra capacità di ridurre notevolmente la mediana del TTD nel corso del 2015.

Figura 69. Confronto tra time to detection da dicembre 2014 a ottobre 2015

Fonte: Cisco Security Research

Il confronto del TTD nella figura 69 indica che molte minacce a giugno sono state rilevate in circa 35,3 ore. A partire da ottobre, ulteriori minacce sono state bloccate entro circa 17,5 ore. Riteniamo che la riduzione del TTD medio sia attribuibile in parte a una più rapida identificazione del commodity malware, ad esempio Cryptowall 3.0, Upatre e Dyre. L'integrazione di nuove tecnologie, come quelle di ThreatGRID, un'azienda Cisco, è un altro fattore.

Alcune minacce continuano a essere più difficili da rilevare di altre, anche con un TTD inferiore. I downloader che hanno come obiettivo gli utenti di Microsoft Word sono generalmente i più facili da rilevare (<20 ore). Gli attacchi adware e browser injection sono tra le minacce più difficili da rilevare (<200 ore).

Uno dei motivi per cui queste ultime minacce sono così impegnative è che in genere sono considerate meno prioritarie dai team della sicurezza. Per questo spesso vengono ignorate nella foga della lotta contro gli attacchi zero-day (vedere "Infezioni dei browser: un problema diffuso e una delle cause principali della sottrazione di dati" a **pagina 16**).

La figura 70 fornisce una panoramica dei tipi di minacce che solitamente emergono entro 100 giorni.

Figura 70. Tag cloud per 100 giorni

Fonte: Cisco Security Research

CONDIVIDI

I sei principi della difesa integrata dalle minacce

Nel Report semestrale di Cisco sulla sicurezza 2015, gli esperti della sicurezza affermavano che la necessità di soluzioni flessibili e integrate porterà a cambiamenti significativi nel settore della sicurezza informatica entro i prossimi cinque anni. I risultati saranno il consolidamento del settore e una tendenza uniforme verso un'architettura di difesa scalabile e integrata contro le minacce. Tale architettura fornirà visibilità, controllo, intelligence e contesto per molte soluzioni.

Questo modello di "rilevamento e risposta" consentirà di reagire con maggiore rapidità alle minacce sia note che emergenti. Al centro di questa nuova architettura ci sarà una piattaforma per la visibilità in grado di offrire informazioni contestuali complete e costantemente aggiornata per consentire la valutazione delle minacce, la correlazione dell'intelligence globale e locale e l'ottimizzazione delle difese. Lo scopo di questa piattaforma è creare una base operativa disponibile per tutti i fornitori e a cui tutti possono contribuire. La maggiore visibilità determinerà maggiore controllo, il che a sua volta porterà a una protezione migliore su più vettori di minacce e la capacità di impedire ancora più attacchi.

Di seguito presentiamo i sei principi della difesa integrata contro le minacce per aiutare le aziende e i loro fornitori della sicurezza a comprendere meglio l'intento e i potenziali vantaggi di questa architettura.

1. **Un'architettura di rete e sicurezza più ricca è necessaria per contrastare l'aumento delle minacce informatiche e del loro livello di sofisticazione.**

   Negli ultimi 25 anni, il tradizionale modello per la sicurezza è stato: "per risolvere un problema, compra una soluzione". Tuttavia queste soluzioni, che sono spesso composte da un insieme di tecnologie provenienti da molti fornitori di sicurezza differenti, non comunicano tra loro in modo efficace. Producono dati e intelligence sugli eventi di sicurezza, che sono integrati in una piattaforma eventi e quindi analizzate da personale addetto alla sicurezza.

   Un'architettura per la difesa integrata contro le minacce è un framework di rilevamento e risposta che offre maggiori capacità e supporta risposte più rapide alle minacce raccogliendo più informazioni dall'infrastruttura implementata in modo automatizzato ed efficiente. Il framework osserva l'ambiente di sicurezza in modo più intelligente. Anziché limitarsi ad avvisare i team responsabili della sicurezza di eventi sospetti e violazioni della policy, è in grado di riprodurre un'immagine chiara della rete e degli eventi in corso per favorire maggiormente il processo decisionale in merito alla sicurezza.

2. **La migliore tecnologia non è in grado da sola di contrastare le minacce attuali e future; va semplicemente ad aumentare la complessità dell'ambiente della rete.**

   Le aziende investono nelle migliori tecnologie per la sicurezza, ma come fanno a sapere se queste soluzioni sono veramente efficaci? Le notizie dei famosi casi di violazioni della sicurezza avvenute lo scorso anno sono la prova che molte tecnologie per la sicurezza non funzionano come dovrebbero. E quando non funzionano, l'esito è disastroso.

   La proliferazione di fornitori di sicurezza che offrono soluzioni di alta qualità non aiuta a migliorare l'ambiente, a meno che questi fornitori non offrano soluzioni che siano completamente diverse (non solo parzialmente diverse) da quelle della concorrenza. Al giorno d'oggi però non vi sono grosse differenze nelle offerte proposte dai principali fornitori nella maggior parte delle aree critiche.

3. **L'aumento del traffico crittografato richiederà una difesa integrata dalle minacce in grado di difendere dall'attività dannosa crittografata contro la quale molti prodotti sono inefficaci.**

   Come spiegato in questo report, il traffico Web crittografato è in aumento. Come è ovvio la crittografia è utile, ma al tempo stesso questa rende problematico il monitoraggio delle minacce da parte dei team della sicurezza.

   La risposta al "problema" della crittografia è avere maggiore visibilità su quanto accade su dispositivi o reti. Le piattaforme per la sicurezza integrata possono aiutare a ottenere questa visibilità.

4. **Le API aperte sono fondamentali per un'architettura di difesa integrata contro le minacce.**

   Gli ambienti con soluzioni di fornitori diversi necessitano di una piattaforma comune che offra maggiore visibilità, contesto e controllo. La creazione di una piattaforma di integrazione front-end può supportare una migliore automazione e offrire una maggiore conoscenza dei prodotti di sicurezza stessi.

5. **Un'architettura di difesa integrata contro le minacce richiede meno apparecchiature e software da installare e gestire.**

   I fornitori dei servizi di sicurezza devono cercare di offrire piattaforme con il maggior numero di funzionalità in un'unica piattaforma. Questo consente di ridurre la complessità e la frammentazione dell'ambiente di sicurezza, fattori che facilitano l'accesso nascosto dei criminali informatici.

6. **Gli aspetti di coordinamento e automazione di una difesa integrata contro le minacce contribuiscono a ridurre i tempi di rilevamento, contenimento e risoluzione.**

   La riduzione dei falsi positivi aiuta i team di sicurezza a concentrarsi sugli aspetti più importanti. La contestualizzazione supporta l'analisi iniziale degli eventi in corso, aiuta i team a valutare la necessità di intervento immediato e genera risposte automatizzate e analisi più approfondite.

L'unione fa la forza: l'importanza della collaborazione del settore

La collaborazione del settore è fondamentale, non solo per sviluppare una nuova architettura per la difesa integrata che consenta una risposta più rapida alle minacce. Serve anche per stare al passo con la community globale degli hacker sempre più audaci, innovativi e persistenti. I criminali informatici stanno diventando sempre più abili nell'implementare campagne difficili da rilevare e altamente redditizie. Molti ora riescono a utilizzare le risorse autorizzate dell'infrastruttura per supportare le proprie campagne.

In questo contesto non sorprende che i professionisti della sicurezza intervistati per lo studio comparativo di Cisco delle infrastrutture di sicurezza del 2015 abbiano meno fiducia nella propria capacità di riuscire a proteggere la loro azienda. Secondo noi i responsabili della sicurezza dovrebbero prendere in considerazione il grande impatto che una collaborazione proattiva e continuativa all'interno del settore può avere per portare alla luce l'attività dei criminali informatici, frenare la loro capacità di generare profitto e ridurre le opportunità di lanciare nuovi attacchi.

Come si è visto con maggiori dettagli in precedenza (vedere "Casi reali" a partire da **pagina 10**), la collaborazione con un partner Cisco e con l'ecosistema Cisco Collective Security Intelligence (CSI), ha contribuito in modo significativo alla capacità di Cisco di scoprire, verificare e ostacolare le operazioni a livello globale dell'Angler exploit kit e di indebolire una delle più grandi botnet DDoS osservata dai nostri ricercatori, ovvero SSHPsycos.

Informazioni su Cisco

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 nell'infrastruttura, garantendo al tempo stesso livelli di visibilità superiori, controlli coerenti e protezione avanzata dalle minacce, prima, durante e dopo l'attacco.

I ricercatori dell'ecosistema 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 comunità open source di Cisco. 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 sicurezza 2016

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.

ADVANCED SERVICES CLOUD AND IT TRANSFORMATION, OPTIMIZATION TEAM

Il team fornisce consigli e contribuisce a ottimizzare le reti, i data center e le soluzioni cloud per i principali provider di servizi e le aziende di tutto il mondo. Questo servizio di consulenza si concentra sull'ottimizzazione di disponibilità, prestazioni e sicurezza delle soluzioni chiave dei clienti. Il servizio di ottimizzazione viene offerto a oltre il 75% delle aziende di Fortune 500.

ACTIVE THREAT ANALYTICS TEAM

Il team Cisco Active Threat Analytics (ATA) aiuta le aziende a difendersi da intrusioni note, attacchi zero-day e minacce persistenti avanzate, sfruttando sofisticate tecnologie Big Data. Questo servizio completamente gestito è fornito dai nostri esperti della sicurezza e dalla nostra rete globale di centri operativi per la sicurezza. Offre la vigilanza costante e l'analisi su richiesta 24 ore al giorno, sette giorni alla settimana.

CISCO THOUGHT LEADERSHIP ORGANIZATION

La Cisco Thought Leadership Organization evidenzia le opportunità globali, i cambiamenti del mercato e le soluzioni chiave che trasformano aziende, settori ed esperienze. L'organizzazione fornisce una prospettiva incisiva e predittiva del mercato futuro per consentire alle aziende di prepararsi per essere più competitive. Gran parte della leadership di pensiero del gruppo fornisce alle aziende supporto nella trasformazione digitale, connettendo gli ambienti fisici e virtuali in modo uniforme e sicuro, per innovare più rapidamente e raggiungere i risultati di business desiderati.

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.

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 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 gruppo di lavoro Global 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.

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 & Operations, oltre che da fonti esterne. Il team produce IntelliShield Security Intelligence Service, che supporta vari prodotti e servizi Cisco.

LANCOPE

Lancope è un'azienda Cisco ed un fornitore leader di visibilità di rete e intelligence di sicurezza per la protezione delle aziende dalle principali minacce di oggi. Analizzando NetFlow, IPFIX e altri tipi di telemetria di rete, il sistema StealthWatch® di Lancope offre analisi di sicurezza sensibile al contesto per individuare rapidamente un'ampia gamma di attacchi, da APT e DDoS al malware zero-day e minacce interne. Grazie alla combinazione di monitoraggio continuo laterale nelle reti aziendali con informazioni contestuali su utenti, dispositivi e applicazioni, Lancope accelera la capacità di reazione agli incidenti, migliora l'analisi forense e riduce il rischio aziendale.

OPENDNS

OpenDNS è un'azienda Cisco ed è la principale piattaforma di sicurezza sul cloud del mondo, che serve oltre 65 milioni di utenti al giorno, distribuiti in oltre 160 paesi. OpenDNS Labs è il team responsabile della ricerca presso OpenDNS che supporta la piattaforma di sicurezza. Per ulteriori informazioni, visitare **www.opendns.com** o **https://labs.opendns.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 informatiche esistenti e nuove. 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**.

SECURITY RESEARCH AND OPERATIONS (SR&O)

Security Research & 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 innovativi 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.

Contributi di partner Cisco

LEVEL 3 THREAT RESEARCH LABS

Level 3 Communications è un provider di comunicazioni di portata mondiale con sede a Broomfield in Colorado (USA), che fornisce servizi di comunicazione ad aziende, amministrazioni pubbliche e operatori. Supportata dalle ampie reti in fibra ottica in tre continenti e collegata da infrastrutture sottomarine, la nostra piattaforma di servizi globale offre risorse metropolitane che raggiungono oltre 500 mercati in oltre 60 paesi. La rete Level 3 offre una panoramica estesa delle minacce a livello mondiale.

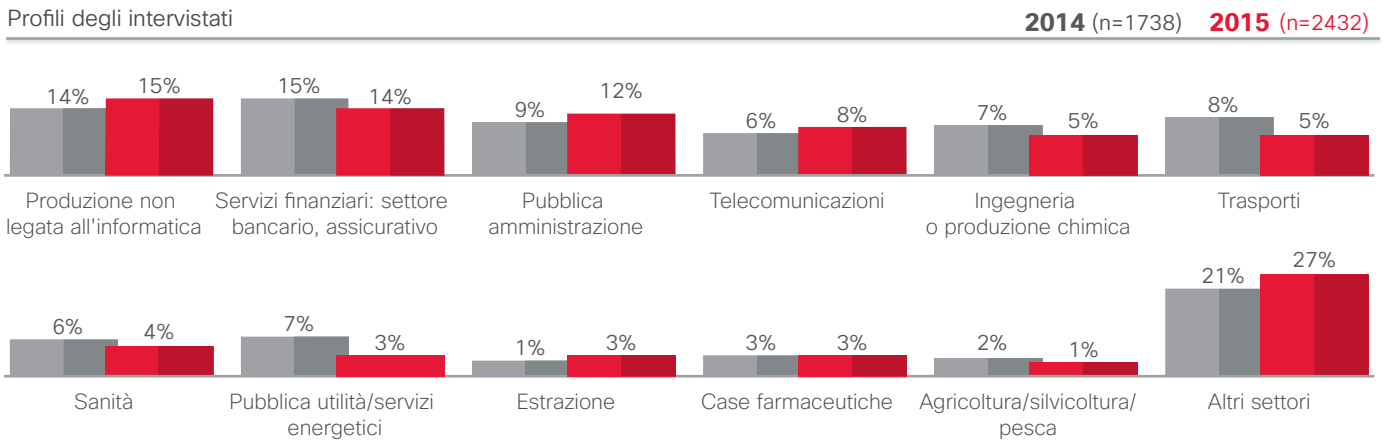
Level 3 Threat Research Labs è il gruppo della sicurezza dedito all'analisi proattiva delle minacce a livello mondiale e organizza le informazioni ricevute da fonti interne ed esterne per proteggere i clienti di Level 3, la sua rete e la rete Internet pubblica. Il gruppo collabora regolarmente con i leader del settore come Cisco Talos per individuare e contenere le minacce.

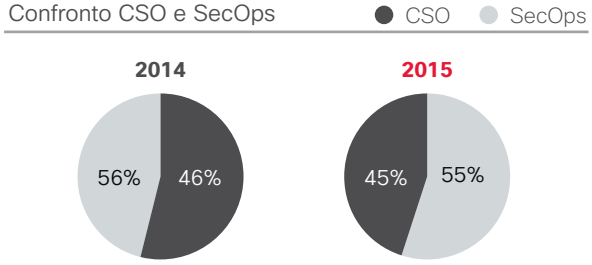
Appendice

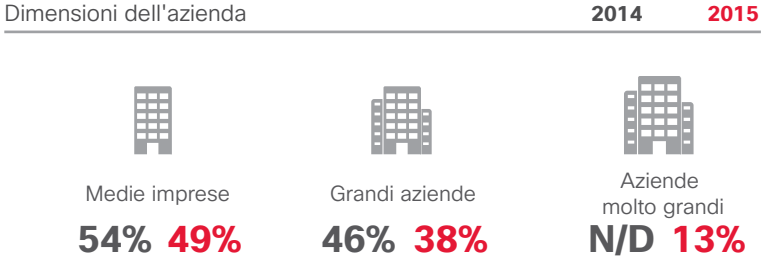
Appendice

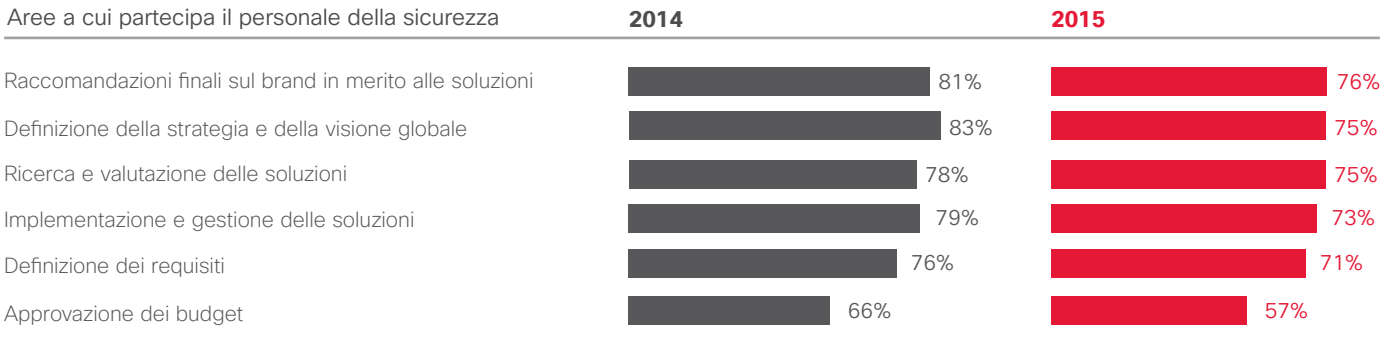
Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015: profilo degli intervistati e risorse

Figura 71. Profili degli intervistati









Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Figura 72. Sebbene solo il 9% disponga di un budget per la sicurezza separato dal budget IT, si registra un notevole aumento dal 2014

Il budget per la sicurezza informatica fa parte del budget IT? (Personale del reparto IT)

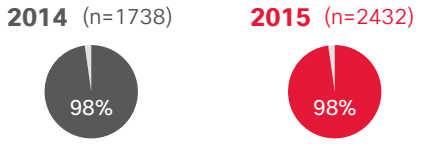
Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Figura 73. Qualifiche: intervistati e loro manager

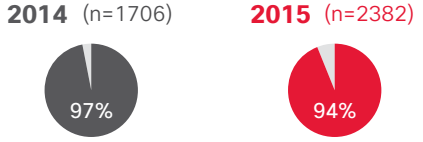
Personale del reparto IT

2014 97% rispetto a 2015 98%

Reparto o team dedicato alla sicurezza



Personale del team di sicurezza



Qualifica		Qualifica del manager	
Chief Security Officer	22%	Chief Executive Officer	34%
Chief Technology Officer	18%	Presidente/proprietario	18%
Direttore o Manager dell'IT	16%	Chief Security Officer	16%
Chief Information Officer	13%	Chief Information Officer	6%
Direttore di Security Operations	7%	Chief Technology Officer	6%
VP della sicurezza IT	5%	Direttore o Manager dell'IT	4%
Risk and Compliance Officer	4%	VP della sicurezza IT	4%
Security Operations Manager	4%	VP dell'IT	2%
Security Architect	4%	Direzione generale	2%
VP dell'IT	3%	Chief Operations Officer	1%
Chief Operations Officer	3%	Chief Financial Officer	1%
Altro titolo	2%	Altro titolo	0%

Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Figura 74. Il firewall è lo strumento di difesa dalle minacce alla sicurezza più diffuso; nel 2015 sono state amministrate meno difese tramite servizi basati sul cloud rispetto al 2014

Difese contro le minacce per la sicurezza utilizzate dalle aziende	**2014** (n=1738)	**2015** (n=2432)	Difese amministrate tramite servizi basati sul cloud (intervistati che utilizzano le difese contro le minacce alla sicurezza) **2014** (n=1646)	**2015** (n=2268)
Firewall*	N/D	65%		31%
Data Loss Prevention	55%	56%		
Autenticazione	52%	53%		
Crittografia/privacy/protezione dei dati	53%	53%		
Sicurezza e-mail/messaggistica	56%	52%	37%	34%
Sicurezza Web	59%	51%	37%	31%
Protezione degli endpoint/anti-malware	49%	49%	25%	25%
Controllo degli accessi/autorizzazione	53%	48%		
Amministrazione delle identità/provisioning degli utenti	45%	45%		
Prevenzione delle intrusioni*	N/D	44%		20%
Sicurezza della mobilità	51%	44%	28%	24%
Rete wireless protetta	50%	41%	26%	19%
Analisi delle vulnerabilità	48%	41%	25%	21%
VPN	48%	40%	26%	21%
Security Information and Event Management	43%	38%		
Difesa DDoS	36%	37%		
Test di penetrazione	38%	34%	20%	17%
Applicazione di patch e configurazione	39%	32%		
Analisi forense della rete	42%	31%		
Analisi forense degli endpoint	31%	26%		
Sicurezza di rete, firewall e prevenzione delle intrusioni*	60%	N/D	35%	
Nessuno dei precedenti	1%	1%	13%	11%

*Firewall e prevenzione delle intrusioni erano un'unica opzione nel 2014 "Sicurezza di rete, firewall e prevenzione delle intrusioni."

Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

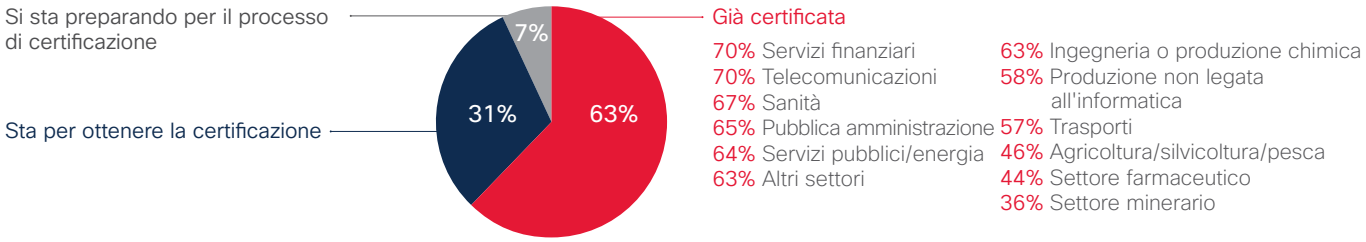
Esternalizzazione

Figura 75. I servizi di consulenza sono ancora i principali servizi di sicurezza esternalizzati

Incrementi significativi riscontrati nell'esternalizzazione del controllo e della risposta agli incidenti. L'esternalizzazione è considerata più economica.

La metà (52%) segue una procedura basata su policy di sicurezza standardizzate come ISO 27001, come l'anno scorso. Di queste, la grande maggioranza ha ottenuto o sta per ottenere la certificazione.

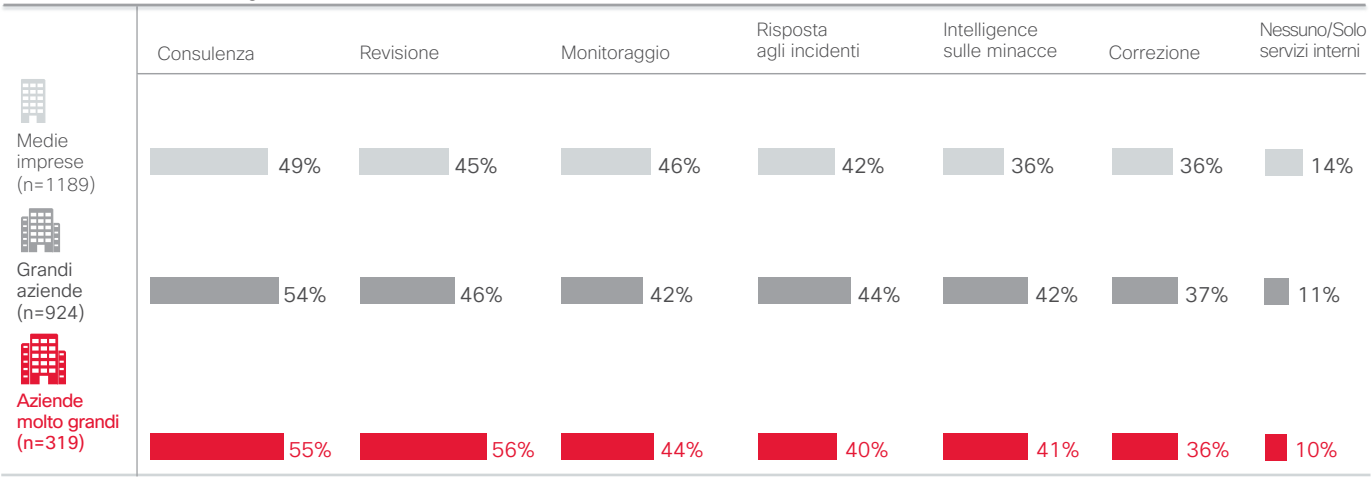
Procedura basata su policy di sicurezza standardizzate
L'azienda segue una procedura basata su policy standardizzate per la sicurezza dei dati (**2015**; n=1265)



Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Figura 76. L'esternalizzazione in base alle dimensioni delle aziende: le aziende molto grandi sono più inclini a esternalizzare controlli e servizi vari di consulenza

Quali servizi di sicurezza vengono esternalizzati?



Fonte: studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

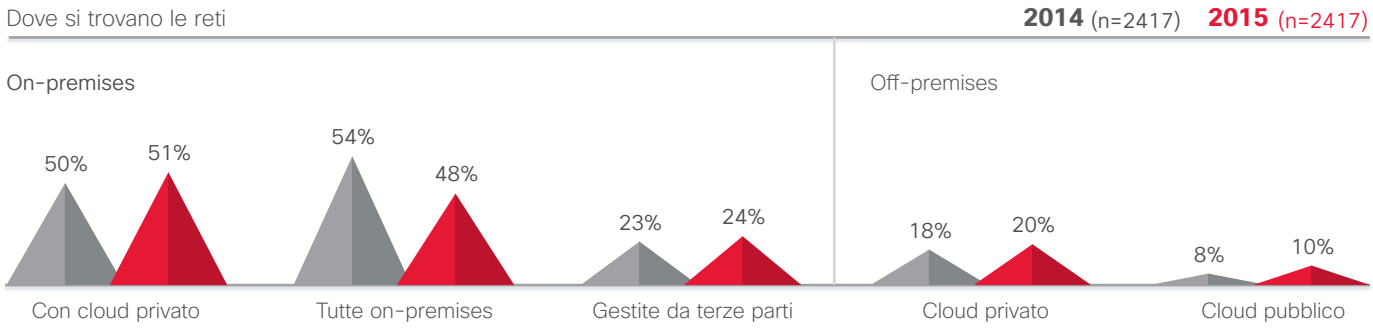
Figura 77. L'esternalizzazione in base al paese: il Giappone è molto più incline a esternalizzare i vari servizi di consulenza

Quali servizi di sicurezza vengono esternalizzati?

	TOTALE	Stati Uniti	Brasile	Germania	Italia	Regno Unito	Australia	Cina	India	Giappone	Messico	Russia	Francia
Consulenza	52%	52%	51%	49%	51%	44%	54%	52%	54%	64%	58%	41%	55%
Controllo	47%	50%	55%	38%	48%	50%	36%	33%	51%	41%	63%	40%	59%
Monitoraggio	44%	48%	49%	32%	39%	41%	52%	31%	51%	51%	49%	37%	50%
Risposta agli incidenti	42%	46%	39%	32%	38%	43%	53%	34%	49%	53%	45%	27%	54%
Intelligence sulle minacce	39%	42%	40%	37%	46%	36%	16%	36%	48%	47%	44%	42%	39%
Correzione	36%	34%	32%	38%	34%	31%	47%	37%	41%	40%	21%	41%	41%
Nessuno/Solo servizi interni	12%	18%	9%	18%	13%	19%	4%	19%	12%	10%	3%	16%	4%

Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Figura 78. L'hosting on-premises delle reti è ancora il più comune; tuttavia l'hosting off-premises è aumentato rispetto all'anno precedente



Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Esposizione al pubblico per le violazioni della sicurezza

Figura 79. Nel 2015 un numero inferiore di aziende ha riportato di essere stata esposta al pubblico per le violazioni della sicurezza per stimolare i miglioramenti della sicurezza:

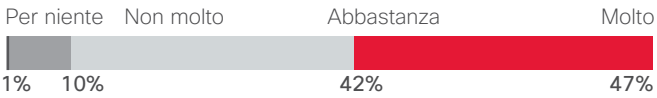
Rispetto al **2014**, nel **2015** un numero inferiore di aziende ha riportato di essere stata esposta al pubblico per le violazioni della sicurezza.

2014 **53%** rispetto a 2015 **48%**

Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Figura 80. L'esposizione al pubblico per le violazioni può contribuire a migliorare la sicurezza

In quale misura la violazione ha favorito i miglioramenti di policy di sicurezza, procedure o tecnologie di difesa dalle minacce? (n=1134)



I CSO riportano più miglioramenti dopo una violazione della sicurezza rispetto ai manager di SecOps.

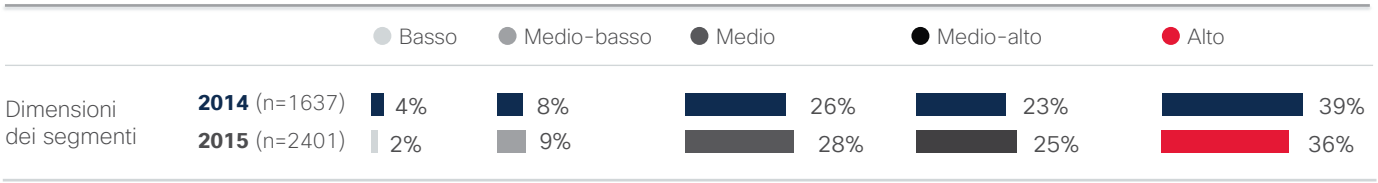
Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Leadership e maturità

Figura 81. Il modello con 5 segmenti è simile al Capability Maturity Model (CMM).

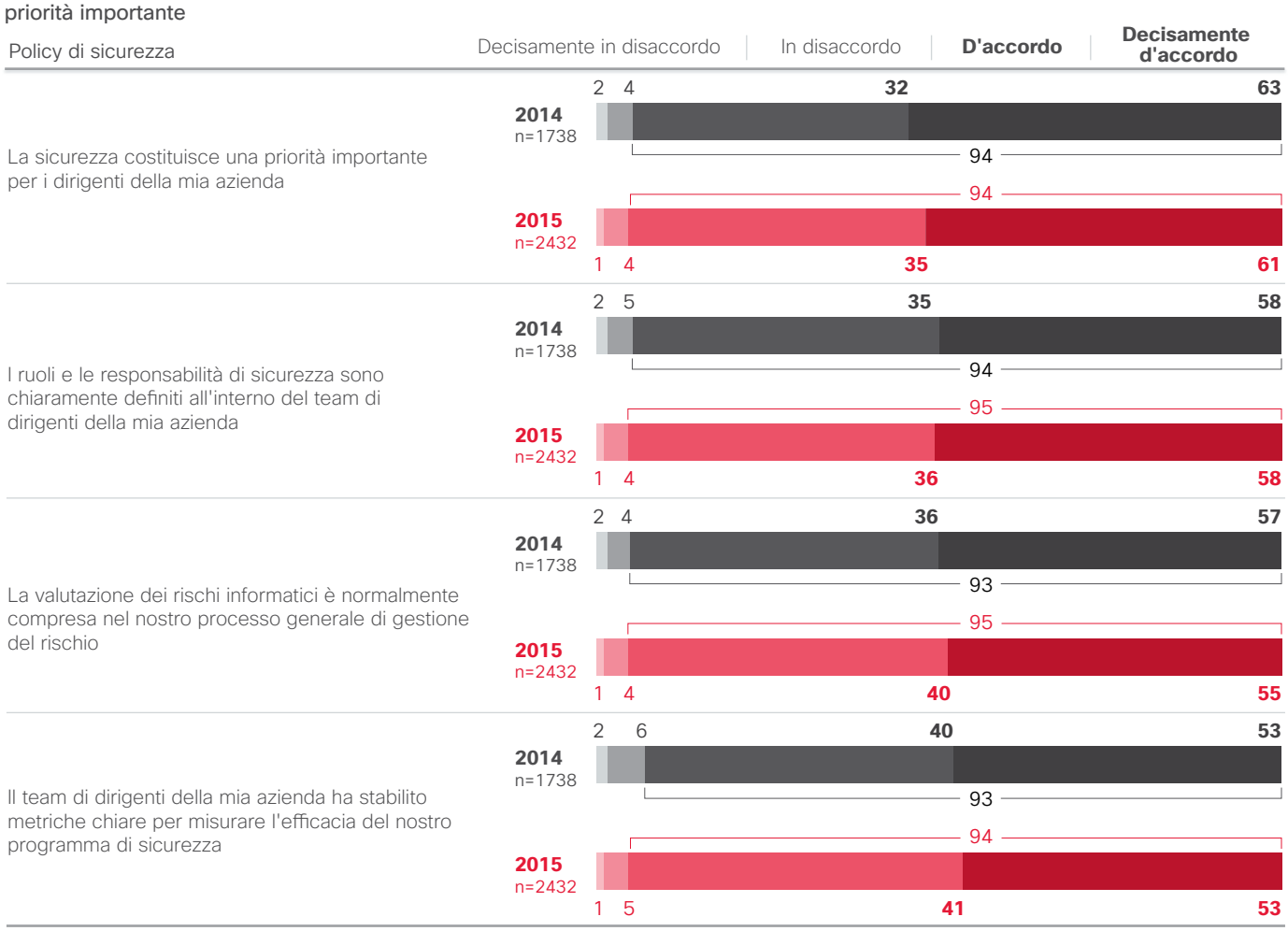
I segmenti rispecchiano un percorso simile a quello dello studio dell'anno scorso in termini di maturità nei confronti della priorità alla sicurezza e di come questo si traduca in processi e procedure.

Il **60%** o più corrisponde a profili di sicurezza più maturi. Ciò vale per quasi tutti i paesi e i settori.



Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Figura 82. Come nel 2014 quasi tutti sono d'accordo o decisamente d'accordo che i vertici aziendali considerino la sicurezza una priorità importante



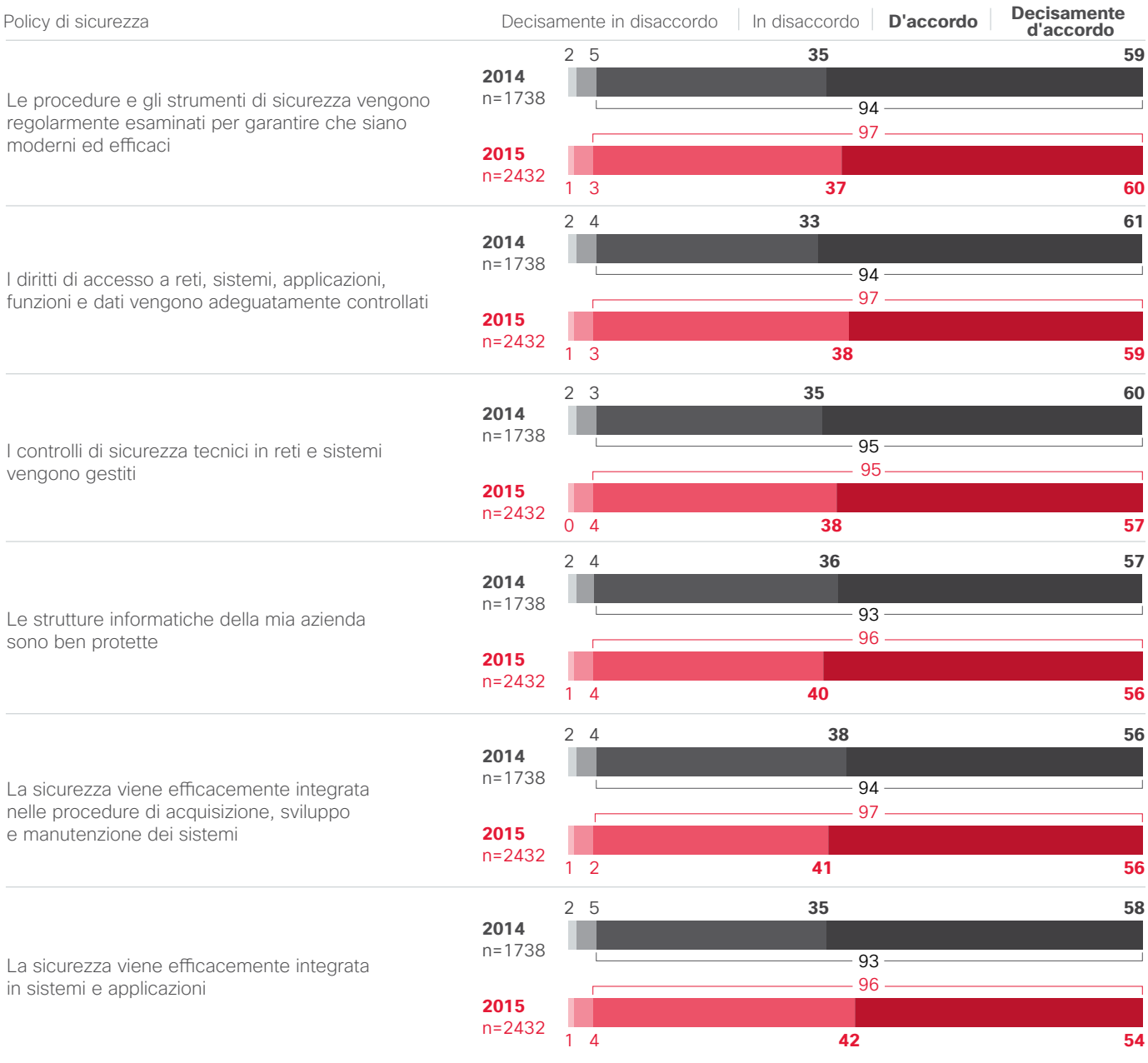
Sono molto più numerosi gli operatori del settore farmaceutico che concordano con l'affermazione "il team di dirigenti della mia azienda ha stabilito metriche chiare per misurare l'efficacia del nostro programma di sicurezza" rispetto ai professionisti di quasi tutti gli altri settori.

È significativo il maggior numero di CSO che concorda con tutte le affermazioni relative all'impegno della dirigenza rispetto a SecOps.

Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

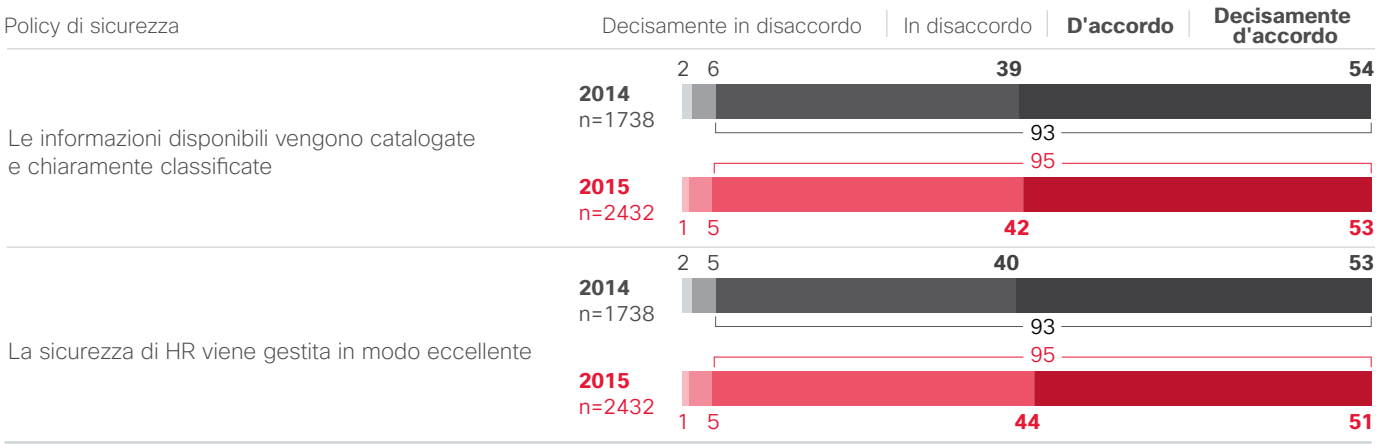
Processi

Figura 83. Fiducia variabile nella capacità di integrare la sicurezza nei sistemi



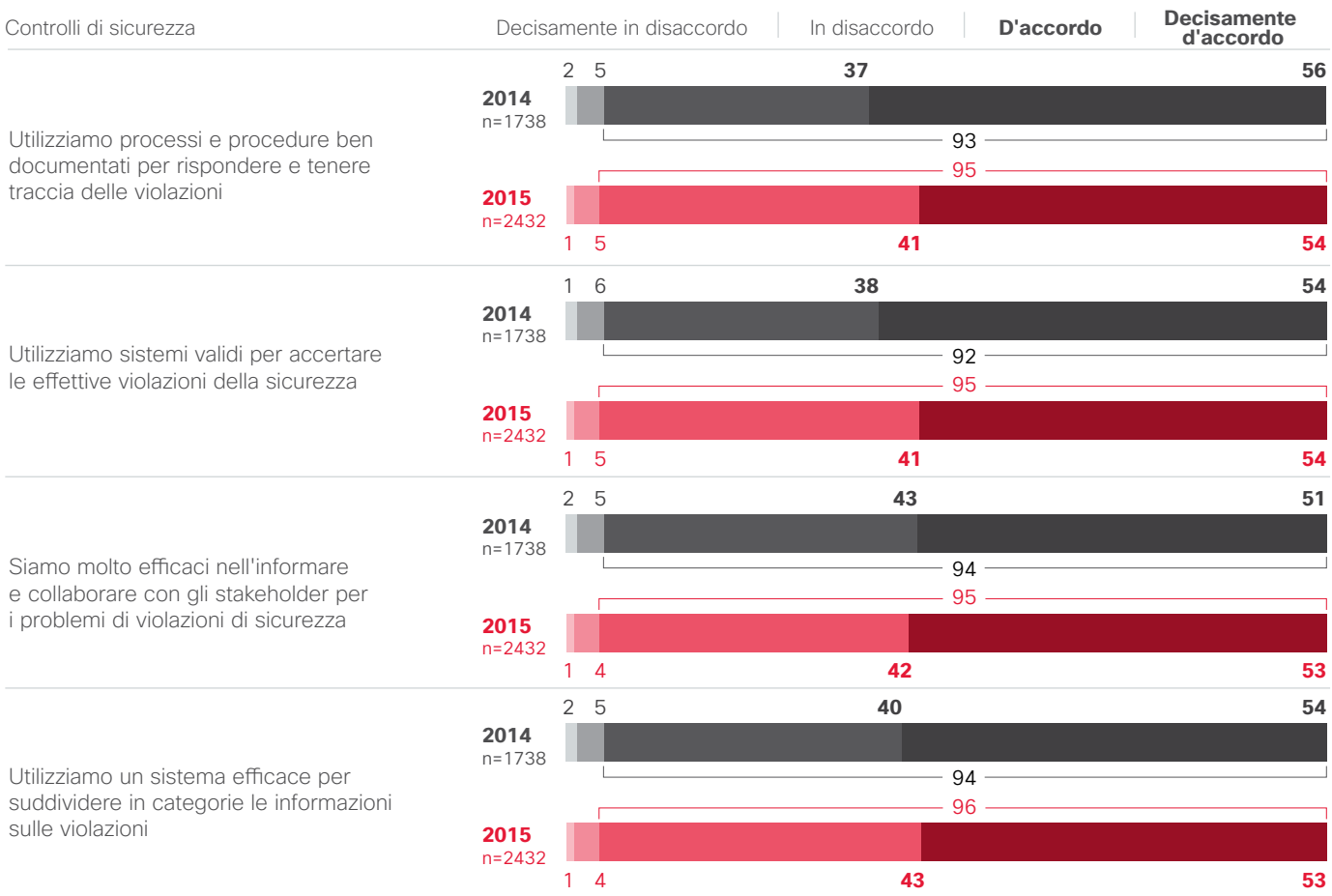
Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Figura 83. Fiducia variabile nella capacità di integrare la sicurezza nei sistemi (continua)



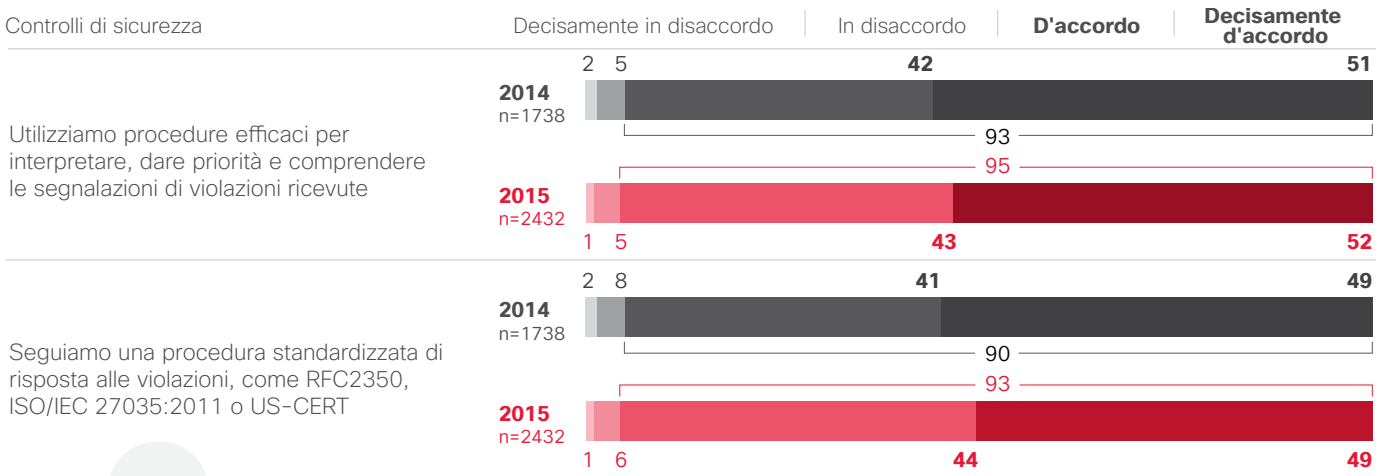
Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Figura 84. Le aziende ritengono di possedere validi controlli di sicurezza



Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Figura 84. Le aziende ritengono di possedere validi controlli di sicurezza (continua)



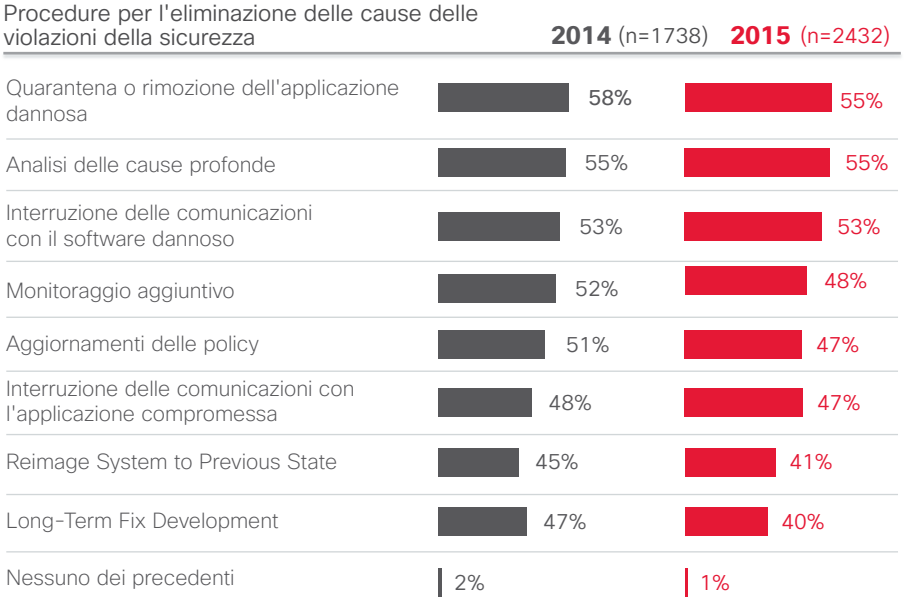
Gli intervistati nel settore dei servizi finanziari sono più propensi a concordare fermamente con l'affermazione "Utilizziamo un sistema efficace per suddividere in categorie le informazioni sulle violazioni" rispetto ai professionisti di quasi tutti gli altri settori.

Fatta eccezione per l'affermazione "Siamo molto efficaci nell'informare e collaborare con gli stakeholder per i problemi di violazioni di sicurezza" i CSO sono più positivi nei confronti degli attributi che circondano i controlli di sicurezza rispetto ai manager di SecOps.

Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

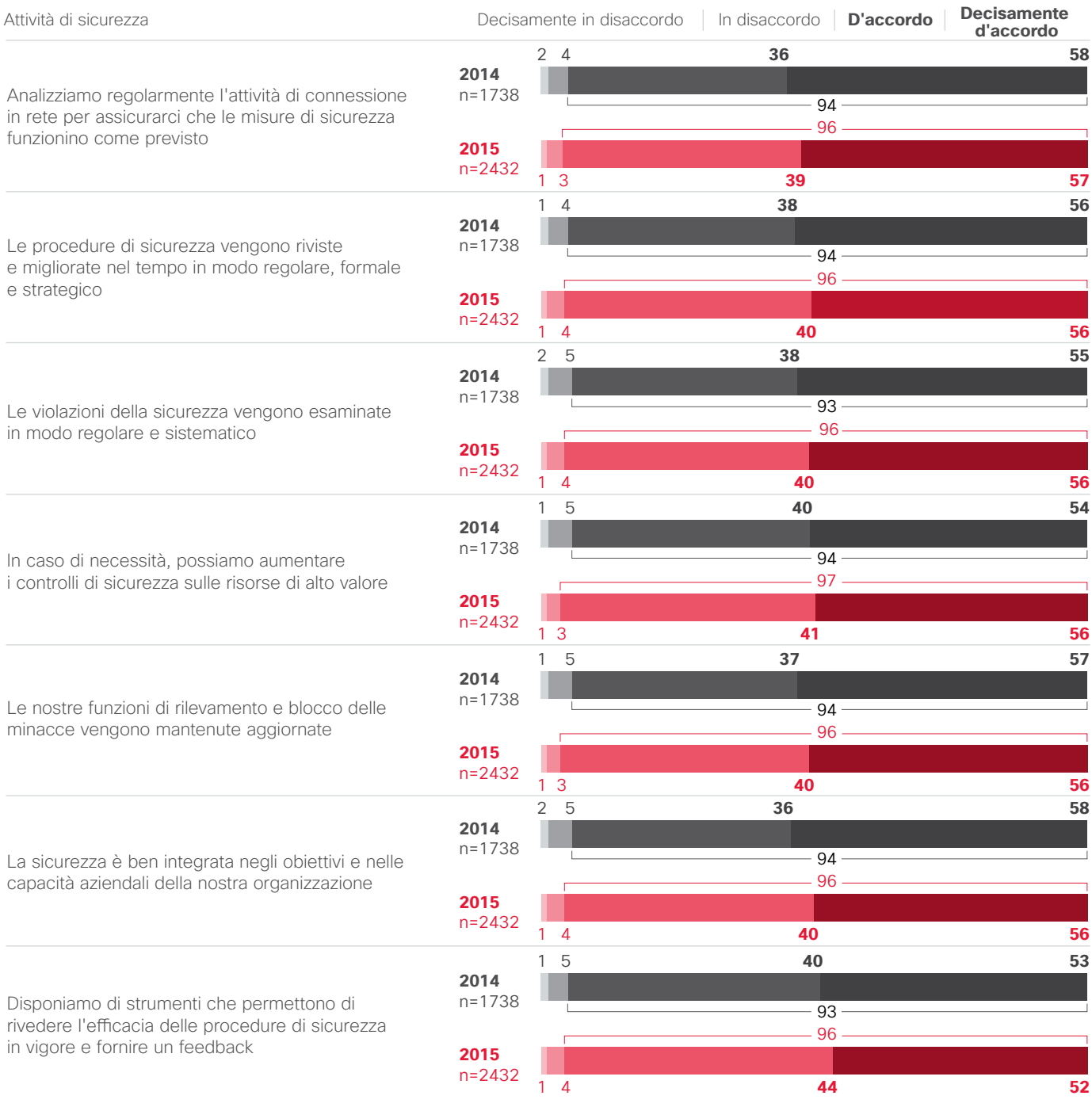
Figura 85. La quarantena/rimozione delle applicazioni dannose e l'analisi delle cause profonde continuano a essere i principali processi utilizzati

È significativo il maggior numero di intervistati negli Stati Uniti che menzionano "Nessuno dei precedenti" quando viene chiesto loro di parlare dei processi che eliminano la causa di una violazione della sicurezza rispetto agli intervistati nella maggior parte degli altri Paesi.



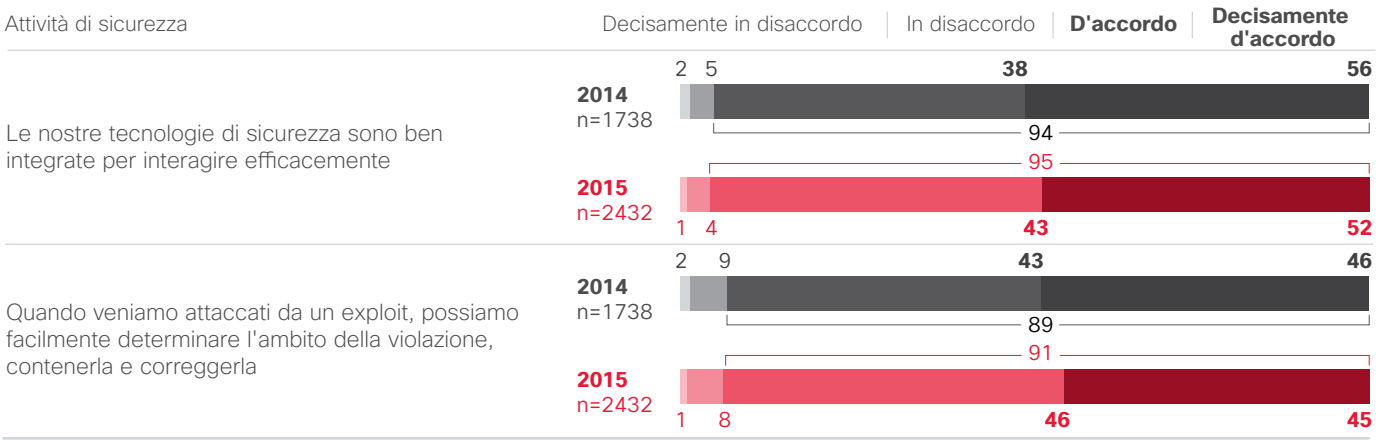
Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Figura 86. Le aziende dimostrano fiducia variabile nella capacità di contenere le violazioni



Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

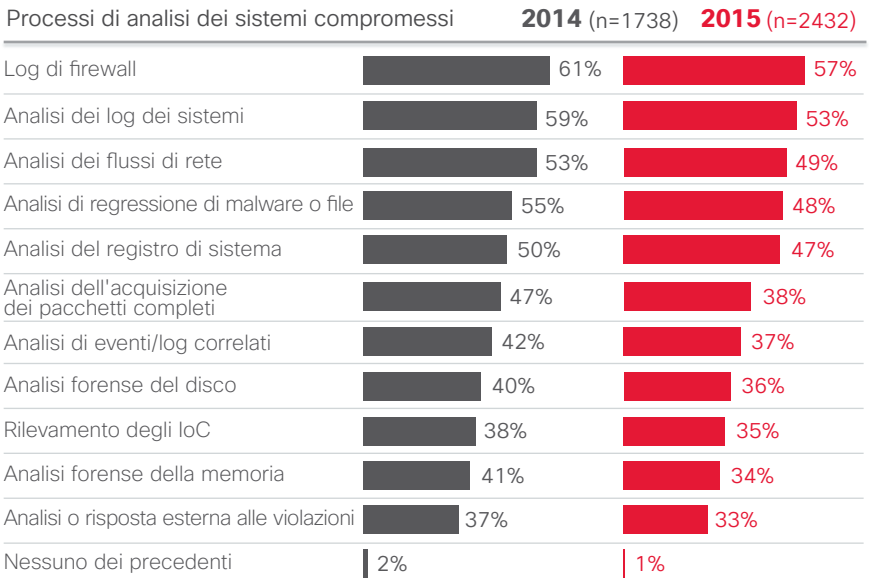
Figura 86. Le aziende dimostrano fiducia variabile nella capacità di contenere le violazioni (continua)



Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Figura 87. I log dei firewall e l'analisi dei log dei sistemi continuano a essere i processi più diffusi per analizzare i sistemi compromessi

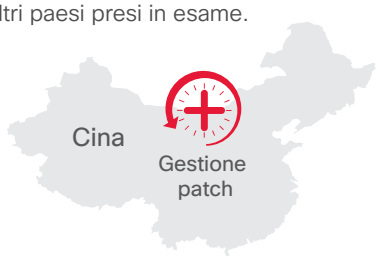
Le aziende grandi e molto grandi riferiscono un uso più consistente di processi per analizzare i sistemi compromessi rispetto alle medie imprese.



Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Figura 88. Il ripristino da un backup creato prima della violazione rimane il processo più diffuso per ripristinare i sistemi colpiti nel 2015

Gli intervistati in Cina affermano di correggere e aggiornare le applicazioni considerate vulnerabili con maggiore frequenza rispetto agli intervistati degli altri paesi presi in esame.



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

Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Figura 89. Il CEO o il presidente è normalmente la persona che viene informata degli eventi relativi alla sicurezza, seguito dalla divisione delle operazioni e dal reparto finanziario

È significativo che siano più gli intervistati appartenenti ad aziende molto grandi a notificare le autorità esterne in caso di violazione rispetto agli appartenenti alle medie imprese e alle grandi aziende.

Aziende molto grandi

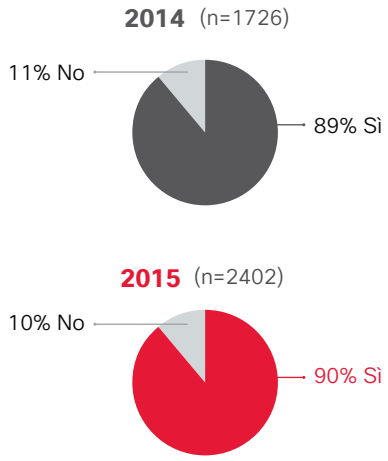
Gruppi notificati in caso di violazione	2014 (n=1738)	2015 (n=2432)
Chief Executive Officer	N/D	45%
Operazioni	46%	40%
Reparto finanziario	N/D	40%
Partner tecnologici	45%	34%
Engineering	38%	33%
Risorse umane	36%	33%
Legale	36%	32%
Manifatturiero	33%	28%
Tutti i dipendenti	35%	27%
Rapporti con il pubblico	28%	24%
Partner aziendali	32%	21%
Autorità esterne	22%	18%
Compagnie di assicurazione	N/D	15%

Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

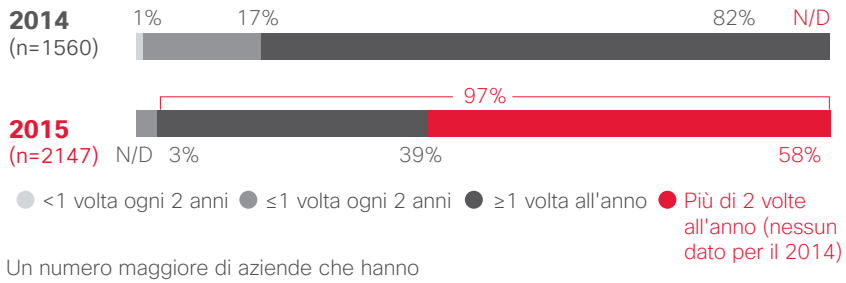
Formazione

Figura 90. Quasi tutte le aziende (97%) offrono una formazione sulla sicurezza almeno una volta all'anno

I programmi di sensibilizzazione e/o formazione sulla sicurezza vengono offerti al personale interessato con cadenza regolare? (Intervistati dedicati alla sicurezza)



Con quale frequenza si tengono le iniziative di formazione sulla sicurezza?
(Intervistati il cui team di sicurezza partecipa a iniziative di formazione)



Un numero maggiore di aziende che hanno subito una violazione svolgono regolarmente programmi di sensibilizzazione e/o formazione sulla sicurezza (96%) rispetto alle aziende che non hanno subito alcuna violazione (83%).

Hanno **96%** rispetto a Non hanno **83%**

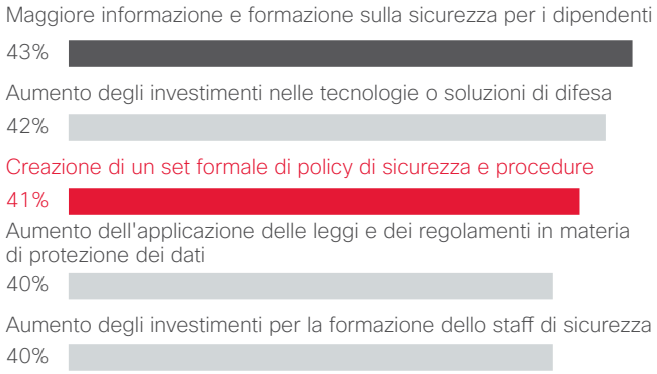
Un numero maggiore di aziende molto grandi afferma di svolgere regolarmente programmi di sensibilizzazione e/o formazione sulla sicurezza (93%) rispetto alle medie imprese (88%) e alle grandi aziende (89%).

Aziende molto grandi **93%** Medie imprese **88%** Grandi aziende **89%**

Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Figura 91. La frequenza della formazione sulla sicurezza e l'incidenza di policy di sicurezza formali sono entrambe aumentate dal 2014

(Prime 5 risposte) Intervistati interessati da una violazione della sicurezza (**2015** n=1109)



Maggiore informazione e formazione sulla sicurezza per i dipendenti

Nel 2015, il 43% degli intervistati ha dichiarato di aver aumentato la formazione sulla sicurezza dopo una violazione pubblica.

43%

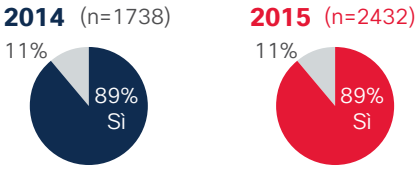
Nel 2015, il 41% degli intervistati ha dichiarato di aver stabilito un set formale di policy di sicurezza e procedure.

41%

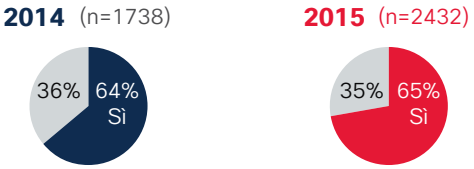
Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Figura 92. Come nel 2014, quasi 9 su 10 hanno affermato che il proprio personale dedicato alla sicurezza ha partecipato a conferenze o corsi di formazione incentrati sulla sicurezza

I membri del team di sicurezza partecipano a conferenze e/o corsi di formazione esterni per migliorare e aggiornare le proprie competenze?
(Intervistati dedicati alla sicurezza)



I dipendenti partecipano ad associazioni settoriali o comitati per la sicurezza?
(Intervistati dedicati alla sicurezza)



Fonte: Studio comparativo di Cisco delle infrastrutture di sicurezza del 2015

Studio sul rischio per la sicurezza e sull'affidabilità

Figura 93. Background e metodologia

L'obiettivo di Cisco è ottenere una maggiore comprensione di quale sia la percezione dei responsabili delle decisioni IT di aziende e provider di servizi dei rischi e delle problematiche per la sicurezza dell'azienda e il ruolo che svolge l'affidabilità del fornitore IT negli acquisti di soluzioni IT.

Obiettivi specifici:

- Misurare il livello di rischio dalle minacce e delle vulnerabilità esterne e interne
- Comprendere strategie, policy e soluzioni che vengono implementate per ridurre i rischi per la sicurezza
- Identificare il processo di acquisto per le soluzioni IT e il ruolo che svolge attendibilità del fornitore IT in tale processo
- Misurare l'interesse a ricevere comunicazioni su come verificare l'affidabilità del fornitore IT
- Stabilire se esistono differenze nelle prospettive di rischio per la sicurezza o approcci di riduzione del rischio tra settori e utenti

Metodologia: approccio quantitativo e qualitativo

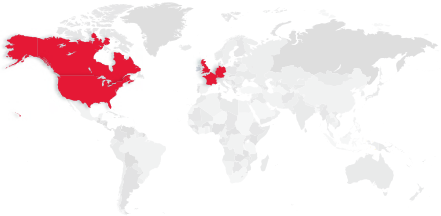
Sono state utilizzate due metodologie per fornire informazioni dettagliate in ognuno di questi obiettivi di ricerca:

(Tutti i partecipanti coinvolti nella decisione di acquisto IT)

Sondaggio quantitativo basato su Web
1050 responsabili decisioni IT di aziende
(402 USA, 282 Regno Unito, 197 Germania, 169 Francia)

Interviste qualitative approfondite
20 provider di servizi
(7 USA, 3 Canada, 3 Regno Unito, 4 Germania, 3 Francia)

La ricerca è stata condotta negli Stati Uniti, Regno Unito, Francia, Germania e Canada (solo IDI)



La raccolta dei dati si è svolta tra agosto e settembre 2015

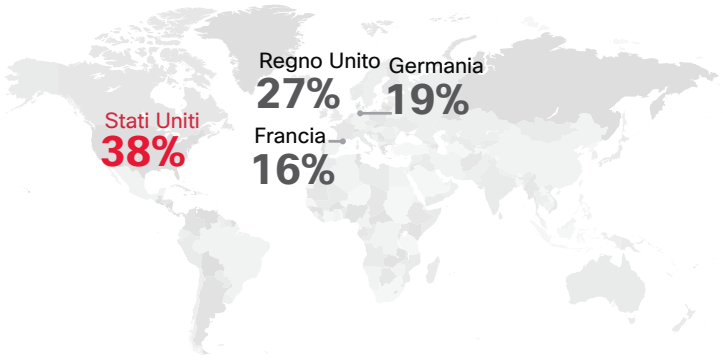
20 minuti Sondaggio basato su Web

45 minuti Interviste approfondite

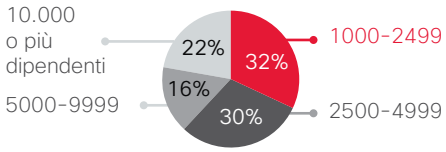
Fonte: Studio di Cisco sul rischio per la sicurezza e sull'attendibilità

Figura 94. Profilo dei partecipanti delle aziende: approccio quantitativo

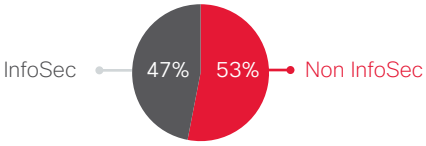
Paese



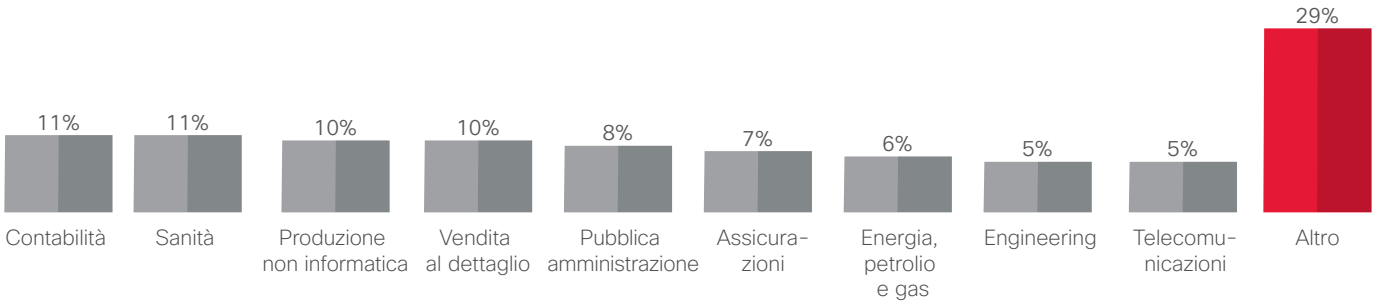
Dimensioni dell'azienda



Classificazione InfoSec



Settore (più del 5% riferito)



Posizione

Livello C (CIO, CSO, CTO, ecc.)	25%
Vice Presidente	9%
Amministratore	30%
Ingegnere/architetto senior	6%
Ingegnere	3%
Manager	26%
Legale	2%

Partecipazione all'acquisto

Definizione di visione/strategia	69%
Garanzia di conformità	71%
Approvazione degli acquisti importanti	69%
Ricerca/valutazione delle soluzioni	77%
Fornire input o decisioni finali sul brand	80%
Implementazione/gestione di soluzioni	77%
Autorizzazione di finanziamento/ approvazione del budget	53%

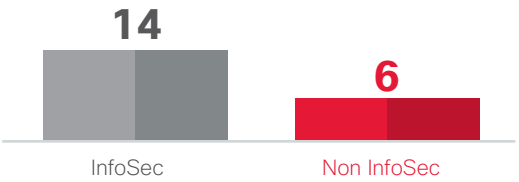
Fonte: Studio di Cisco sul rischio per la sicurezza e sull'attendibilità

Figura 95. Profilo dei partecipanti dei provider di servizi: approccio qualitativo

Paese

Dimensioni dell'azienda

Classificazione InfoSec



Tipo di fornitori di servizi

Servizi applicativi	11%
Servizi tecnici	11%
Telecomunicazioni mobili	6%
Servizi multimediali	4%
Telecomunicazioni cablate	3%

Qualifica

CIO/CTO/CSO	7%
VP dell'IT	1%
Direttore IT	8%
Senior Manager	1%
Ingegnere/architetto senior	2%
Manager	1%

Partecipazione all'acquisto

Definizione di visione/strategia	80%
Garanzia di conformità	100%
Approvazione degli acquisti importanti	70%
Ricerca/valutazione delle soluzioni	95%
Decisioni finali sul brand	85%
Implementazione/gestione di soluzioni	75%
Autorizzazione di finanziamento/ approvazione del budget	60%

Fonte: Studio di Cisco sul rischio per la sicurezza e sull'attendibilità

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

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

Sede centrale Europa
Cisco Systems International BV Amsterdam,
Paesi Bassi

Le sedi Cisco nel mondo sono oltre 200. Gli indirizzi, i numeri di telefono e di fax sono disponibili sul sito web Cisco all'indirizzo **www.cisco.com/go/offices.**

Pubblicato a gennaio 2016