Enterprise Strategy Group | Getting to the bigger truth.™

White paper

L'architettura integrata per la sicurezza della rete: il Next-Generation Firewall incentrato sulle minacce

Autore: Jon Oltsik, analista principale senior

Settembre 2014

Questo white paper ESG è stato commissionato da Cisco Systems e viene distribuito da ESG con licenza.

Sommario

Panoramica

Per garantire la sicurezza della rete, la maggior parte delle aziende installa in punti strategici molti strumenti mirati, quali firewall, gateway di VPN, sistemi IDS/IPS, proxy di rete, sandbox contro il malware, gateway Web ed e-mail e così via. Questo insieme eterogeneo di tecnologie rappresentava un rimedio accettabile diversi anni fa, ma oggi causa notevoli problemi operativi, di applicazione delle policy e di monitoraggio. Le difese allestite a protezione della rete sono inoltre sempre meno efficaci contro minacce mirate e sofisticate e gli attacchi da parte di malware sempre più avanzato.

Qual è la reale portata del problema e quali soluzioni si chiedono ai CISO responsabili della sicurezza informatica delle aziende?

- **Garantire la sicurezza della rete è sempre più difficile.** Chi si occupa quotidianamente dei problemi di sicurezza della rete deve far fronte a numerosi ostacoli dovuti alla sovrapposizione di processi e controlli, alla presenza di troppi strumenti specifici e processi manuali e alla carenza di personale qualificato per la sicurezza. In presenza di così tanti problemi nuovi o già noti, è difficile conciliare la sicurezza della rete con le esigenze aziendali.
- **Gli strumenti moderni per la sicurezza della rete non bastano più.** Molte aziende stanno adottando nuovi strumenti per la sicurezza della rete, quali i Next-Generation Firewall (NGFW). Sebbene i NGFW siano più efficaci, troppo spesso sono incentrati su controlli limitati alle applicazioni anziché offrire una protezione più globale contro le minacce informatiche. Inoltre, l'impiego di singoli strumenti, quali le sandbox di analisi del malware, ha un'applicazione strategica molto limitata che non garantisce né la protezione né una maggiore visibilità dello stato della sicurezza della rete o del cloud.
- **Le aziende di grandi dimensioni hanno bisogno di un'architettura interoperabile per la sicurezza della rete.** Serve un'architettura per la sicurezza della rete più incentrata sulle minacce, che offra scalabilità e automazione dei processi manuali e sostituisca gli strumenti specifici con servizi per la sicurezza della rete interoperabili. Un'architettura di questo tipo deve includere la gestione centralizzata, l'applicazione distribuita delle policy e l'intelligence integrata e disponibile in tempo reale.

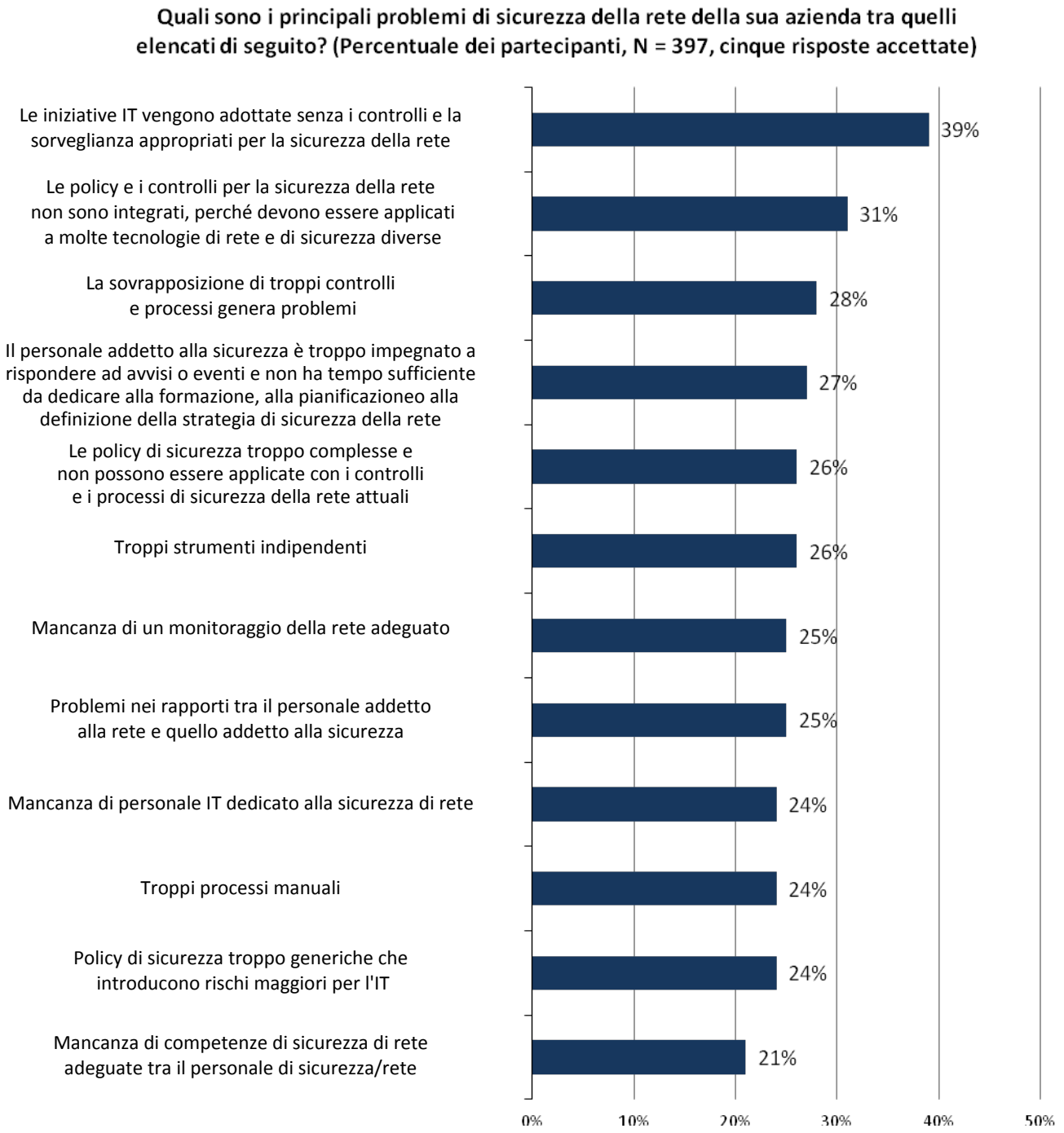
Le problematiche della sicurezza della rete

Le grandi aziende stanno rapidamente trasformando le infrastrutture IT legacy grazie a iniziative quali il cloud computing, l'analisi dei Big Data, la mobilità e le applicazioni di Internet of Things (IoT). L'entità di queste modifiche comporta vari problemi di sicurezza per le rete aziendali (vedere la Figura 1).[1] Spesso i responsabili della sicurezza informatica si ritrovano a fronteggiare vari ostacoli:

- **Troppe soluzioni e tecnologie eterogenee e isolate.** Quasi un terzo (31%) delle aziende è ostacolato dalla mancanza di coesione tra le policy e i controlli di sicurezza della rete, mentre il 28% deve gestire un numero eccessivo di controlli e policy sovrapposti e il 26% utilizza troppi strumenti indipendenti. In un ambiente con soluzioni e tecnologie così eterogenee e isolate, è difficile prevenire, rilevare e risolvere i problemi di sicurezza.
- **Uso eccessivo di processi manuali.** I dati di ESG indicano che il personale addetto alla sicurezza spesso si limita a risolvere i problemi più urgenti, anziché impiegare procedure e policy di sicurezza di rete più proattive. Inoltre, nel 24% dei casi le aziende sono ostacolate da troppi processi manuali. La risoluzione dei problemi urgenti e i processi manuali non sono sufficienti a soddisfare le esigenze attuali di gestione del rischio e risposta alle emergenze per la sicurezza di rete.
- **Carenza di personale qualificato che si occupi della sicurezza della rete.** I dati di ESG indicano inoltre che, per il 24% delle aziende, il problema è la mancanza di personale dedicato alla sicurezza della rete, mentre il 21% afferma di non disporre del personale qualificato per la sicurezza della rete. Questa carenza di personale qualificato a livello mondiale ha gravi ripercussioni potenziali per le aziende.

[1] Fonte: report di ricerca ESG *Network Security Trends in the Era of Cloud and Mobile Computing*, agosto 2014.

Figura 1. Le problematiche della sicurezza della rete



Fonte: Enterprise Strategy Group, 2014.

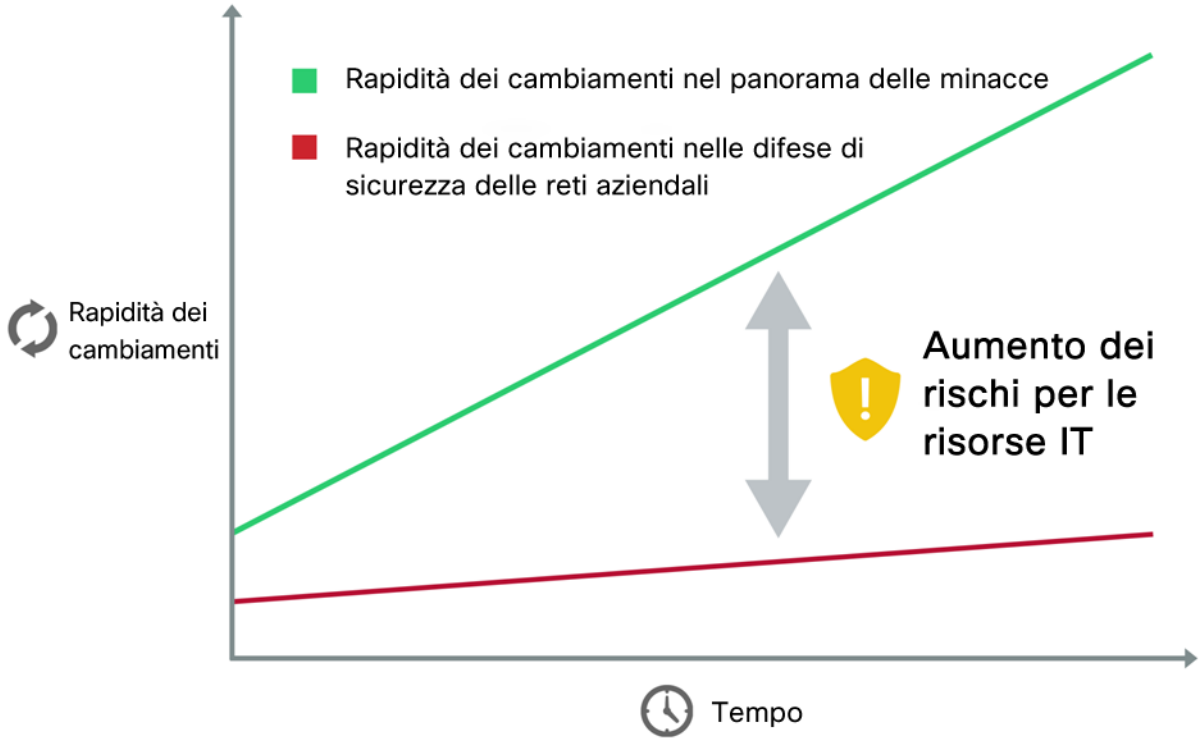
L'aumento dei rischi per la sicurezza della rete

I direttori e i CEO delle aziende devono comprendere che le sfide della sicurezza della rete fanno parte di un problema ben più grande relativo alla gestione del rischio della sicurezza informatica. L'approccio tradizionale alla sicurezza della rete, basato su processi manuali e tecnologie isolate che richiedono competenze avanzate, oggi non è più sufficiente ad affrontare minacce così numerose, variegate e sofisticate. La mancanza di integrazione tra le soluzioni crea punti deboli sfruttabili dagli attacchi più sofisticati ed è tra le cause delle violazioni della sicurezza subite da molte aziende: gli hacker possono sfruttare queste vulnerabilità della rete per penetrare indisturbati, aggirare i controlli di sicurezza e

compromettere le risorse IT. Una volta penetrati nella rete dell'azienda, spesso gli hacker rimangono invisibili per mesi e possono esplorare la rete, accedere ai sistemi importanti per le attività aziendali e impossessarsi di dati riservati.

In passato, i CISO (Chief Security Information Officer) hanno fronteggiato queste minacce dedicando un numero sempre maggiore di tecnologie, processi e risorse di personale alla sicurezza della rete, ma questa strategia non è più sufficiente. In sostanza, assistiamo a una crescita esponenziale delle minacce informatiche a causa delle nuove tecnologie e di tecniche più avanzate di exploit. A fronte di ciò, gli investimenti incrementali nella sicurezza della rete offrono un aumento modesto della protezione, tenuto conto soprattutto dei problemi operativi appena discussi. Questa situazione crea ogni giorno maggiori rischi per la sicurezza delle risorse IT (vedere la Figura 2).

Figura 2. L'approccio reattivo alla sicurezza della rete genera maggiori rischi per le risorse IT



Fonte: Enterprise Strategy Group, 2014.

Le aziende hanno bisogno di un'architettura integrata e incentrata sulle minacce per la sicurezza della rete

Il problema che si pone alle aziende di grandi dimensioni non è di facile soluzione: da una parte le reti devono essere disponibili, scalabili, dinamiche e aperte per supportare i processi IT e di business odierni, dall'altra questo modello crea rischi notevolmente maggiori per la sicurezza. In presenza di un ambiente IT così fluido e di un panorama delle minacce in continua evoluzione, i controlli della sicurezza della rete tradizionali non sono più sufficienti.

Ma allora cosa serve? ESG ritiene che le attuali esigenze richiedano un approccio completamente nuovo per la sicurezza della rete. Per il futuro, i CISO dovranno adottare un nuovo modello di architettura che si estenda dai confini della rete fino al core e al cloud. ESG definisce l'architettura integrata per la sicurezza della rete come segue:

Un sistema integrato di software e hardware per la sicurezza della rete in cui sia possibile applicare ogni servizio di sicurezza in ogni punto della rete interna o estesa su dispositivi fisici o virtuali. L'architettura per la sicurezza della rete fornisce inoltre il livello di comunicazioni sottostante necessario ai servizi e ai componenti per condividere le informazioni e adattarsi in tempo reale, al fine di ottimizzare i controlli di sicurezza, rilevare eventi e apportare correzioni in presenza di sistemi compromessi.

L'architettura per la sicurezza di rete integrata e incentrata sulle minacce si basa sugli stessi tipi di firewall (standard e NGFW), sistemi IDS/IPS e altre tecnologie attualmente in uso. La differenza principale, tuttavia, è che i singoli dispositivi interagiscono e collaborano più fluidamente in tutta la rete, condividendo i dati di intelligence telemetrica e, così facendo, agendo in maniera più informata e coordinata. Inoltre, è possibile pensare alle funzioni di sicurezza quali l'applicazione di firewall o sistemi IDS/IPS come servizi distribuibili uniformemente in ambienti LAN, data center aziendali o cloud di provider esterni quando e dove necessario.

Per offrire integrazione, copertura completa e interoperabilità, l'architettura incentrata sulle minacce deve comprendere tre elementi fondamentali:

1. **Gestione centralizzata.**
2. **Applicazione distribuita delle policy.**
3. **Intelligence integrata e disponibile in tempo reale.**

Gestione centralizzata

Uno dei problemi principali associati alle tecnologie legacy per la sicurezza della rete è quello della gestione e delle attività operative. Ciascun dispositivo per la sicurezza della rete dispone del proprio motore di policy e di funzioni indipendenti di provisioning, configurazione e creazione di report; ciò crea problemi non trascurabili associati ai costi operativi e ad attività superflue. Inoltre, è molto difficile ottenere un quadro complessivo sullo stato della sicurezza aziendale a partire da una miriade di report creati da strumenti mirati.

Per attenuare questi problemi, alla base dell'architettura integrata per la sicurezza della rete deve esserci la gestione centralizzata delle seguenti capacità e attività.

- **La gestione dei servizi.** Il provisioning, la configurazione e la modifica dei servizi per la sicurezza della rete devono essere gestiti in maniera centralizzata, con il supporto di una GUI intuitiva e di un motore del flusso di lavoro, e interagire con altri strumenti operativi IT. Ad esempio, è opportuno che il personale addetto alla sicurezza della rete possa eseguire il provisioning e la configurazione di regole di firewall, VLAN ed elenchi ACL di router e switch da un'unica GUI. Ciò basterebbe per semplificare i controlli della sicurezza della rete, ottimizzarne le attività e migliorare la protezione.
- **L'interoperabilità con la virtualizzazione dei server e l'orchestrazione del cloud**. È necessario supportare gli strumenti di livello superiore necessari per la configurazione dei carichi di lavoro virtuali per VMware, Hyper-V, OpenStack o AWS con controlli di sicurezza di rete appropriati. La giusta architettura per la sicurezza della rete con la gestione centralizzata rende disponibili le API appropriate per associare ai vantaggi del cloud, quali la rapidità del provisioning e il self-service, i livelli adeguati di protezione della rete**.**
- **Il monitoraggio e la creazione di report.** A prescindere da funzioni operative e gestionali, è opportuno che un'architettura integrata per la sicurezza della rete offra funzioni centrali di monitoraggio e creazione di report in linea con attività quali la gestione degli eventi. Per ottenere informazioni sullo stato della rete in modo più accurato e tempestivo, gli analisti della sicurezza devono potere passare da un report all'altro o correlare più report rapidamente. Per ridurre le vulnerabilità, è inoltre opportuno che le funzioni centrali di monitoraggio e creazione di report agiscano sui controlli virtuali e basati sul cloud, oltre che sui dispositivi per la sicurezza della rete fisici.
- **La visibilità avanzata.** Oltre al monitoraggio, è necessario offrire agli analisti di sicurezza una visibilità approfondita degli ambienti che consenta di rilevare minacce a vettore multiplo ed esaminare il numero e le attività di utenti, applicazioni, contenuti e dispositivi presenti nella rete. In tal modo potranno implementare policy di sicurezza efficaci per ridurre i tempi di rilevamento e risposta alle minacce.

Applicazione distribuita delle policy

La gestione centralizzata consente ai responsabili della sicurezza di creare policy globali, che vanno tuttavia applicate affidandosi a vari servizi disseminati in tutta la rete. La giusta architettura integrata per la sicurezza della rete può soddisfare anche tale requisito grazie a queste funzioni:

- **Supporto di qualsiasi tipo di dispositivo in qualunque punto della rete.** I servizi per la sicurezza della rete devono essere disponibili in qualsiasi punto, in qualsiasi tipo di dispositivo e in qualunque combinazione di questi. In tal modo, gli addetti alla sicurezza possono applicare policy granulari a segmenti, flussi, applicazioni o gruppi specifici di utenti di rete. Ad esempio, un'azienda che si occupa di commercio al dettaglio può utilizzare una combinazione di controlli di sicurezza per reti fisiche e virtuali per garantire che i sistemi POS possano collegarsi solo con indirizzi IP specifici passando i controlli di vari firewall, sistemi IDS/IPS e strumenti di rilevamento del malware avanzati. Oppure, è possibile applicare agli utenti di una rete LAN aziendale policy di accesso diverse da quelle di chi lavora da casa tramite una rete pubblica.
- **Una serie di servizi per la sicurezza della rete.** Un'architettura per la sicurezza della rete deve eseguire attività di L2-7 e supportare tutti i tipi di filtri dei pacchetti in qualsiasi punto di una rete LAN o WAN, così come nel cloud. Le attività di filtro dei pacchetti costituiscono un'ampia categoria che include la ricerca di minacce quali virus, worm, attacchi DDoS, spam, phishing, minacce del Web, perdite di contenuto e attacchi a livello di applicazioni. La combinazione di più tipi di dispositivi e servizi consente alle aziende di creare stack di sicurezza multilivello più efficaci, personalizzabili in base ai flussi di rete, ai gruppi di utenza e ai requisiti di mobilità o regolabili in tempi rapidi in risposta a nuovi tipi di minaccia.
- **Integrazione della sicurezza degli endpoint e della rete.** In passato, la sicurezza della rete e quella degli endpoint erano spesso gestite da gruppi diversi che utilizzavano processi e strumenti separati. Le insidie del panorama delle minacce odierno hanno reso questo approccio inefficace. Per colmare questa lacuna, l'architettura per la sicurezza della rete deve favorire la stretta integrazione tra i controlli preventivi e le analisi di rilevamento a livello di endpoint e quelli a livello di rete. Ad esempio, per proteggere gli asset riservati quando gli utenti si collegano alla rete tramite la LAN aziendale o una qualsiasi rete pubblica remota, è necessario garantire l'uniformità dei controlli delle applicazioni a livello di NGFW così come negli endpoint. Per migliorare il rilevamento degli incidenti, occorre inoltre agevolare l'interazione tra le sandbox di analisi e gli agenti degli endpoint, in modo da correlare il traffico di rete sospetto con le attività di sistema anomale.

Intelligence integrata e disponibile in tempo reale

Se da una parte alcune tecnologie per la sicurezza di rete, come i dispositivi per le minacce Web, i sistemi IDS/IPS e i gateway antivirus, dipendono dagli aggiornamenti delle firme e dei dati di intelligence dal cloud, molte altre richiedono l'intervento del personale di sicurezza per le modifiche alla configurazione o la scrittura di nuove regole di blocco delle connessioni di rete. L'architettura integrata per la sicurezza della rete è invece progettata fin dall'inizio per basarsi sull'intelligence, grazie alle caratteristiche seguenti:

- **Si basa su diverse sorgenti di dati.** Rispetto ai sistemi SIEM, che in genere eseguono analisi di sicurezza in base agli eventi dei log, l'architettura per la sicurezza della rete offre molti altri tipi di dati da analizzare. Si tratta di dati raccolti da funzionalità di rete quali NetFlow e strumenti per l'acquisizione dei pacchetti di dati completi, ma anche dati forensi sugli endpoint e informazioni dettagliate su profili, modelli di accesso di utenti e dispositivi e controlli delle applicazioni cloud. Se combinati, correlati e analizzati correttamente, questi nuovi dati consentono alle aziende di migliorare la gestione del rischio e ridurre i tempi di rilevamento e risposta a un incidente.
- **Integrata con l'intelligence sulle minacce basata sul cloud.** L'architettura per la sicurezza della rete deve inoltre includere i dati di intelligence sulle minacce basata sul cloud, per tenere conto ad esempio di vulnerabilità del software, indirizzi IP non validi, URL non autorizzati, canali C&C noti, file dannosi, indicatori di compromissione (IoC) e modelli di attacco che si evolvono in continuazione.

- **Costruita per l'automazione.** In ultima analisi, l'architettura per la sicurezza della rete sfrutta l'intelligence interna ed esterna per facilitare l'automazione delle difese a protezione delle reti aziendali. Ad esempio, un traffico anomalo nel data center può attivare una regola di firewall automatica che interrompe i flussi di dati in base a fattori quali l'indirizzo IP di origine, la porta, il protocollo e le attività DNS. Oppure, una volta rilevata la presenza di malware, è possibile analizzare i file scaricati per individuare retroattivamente gli endpoint responsabili dei download di file sospetti da URL specifici e apportare le correzioni necessarie. Queste attività di correzione automatica portano a un costante miglioramento dei controlli di sicurezza della rete e facilitano l'esecuzione di indagini sistematiche per ridurre i tempi di risposta.

In più, l'architettura per la sicurezza della rete può non solo risolvere i problemi esistenti, ma offrire vantaggi più generali alle attività di business, IT e relative alla sicurezza (vedere la Tabella 1).

Tabella 1. Le caratteristiche dell'architettura per la sicurezza della rete

Proprietà dell'architettura per la sicurezza di rete	Dettagli	Funzionalità	Vantaggi
Gestione centralizzata	Gestione dei servizi, interoperabilità dell'orchestrazione della virtualizzazione cloud/server, monitoraggio e creazione di report centralizzati	Centralizzazione del provisioning e della gestione di policy, configurazioni, modifiche, eventi e così via	Ottimizzazione delle attività operative di sicurezza, facilità d'uso, controllo centrale e visibilità di tutti gli elementi della sicurezza indipendentemente dalla loro posizione nella rete o dal tipo di dispositivo
Applicazione distribuita delle policy	Qualsiasi servizio per la sicurezza della rete, in qualunque punto della rete, per qualunque tipo di dispositivo e integrazione tra la sicurezza della rete e quella degli endpoint	Coordinamento dei servizi di rete ed estensione dell'applicazione di policy di sicurezza al cloud	Sicurezza a più livelli personalizzata per vari scenari d'uso a protezione di utenti, dispositivi e applicazioni, facilmente migliorabile o modificabile in base a nuovi tipi di minacce
Intelligence integrata e disponibile in tempo reale.	Sorgenti di dati diversificate che includono intelligence sulle minacce integrata e basata sul cloud	Dettagli granulari sul traffico delle applicazioni e di rete, sulle attività degli endpoint e sulle nuove minacce	Possibilità per gli addetti alla sicurezza di prendere decisioni basate su intelligence in tempo reale e automazione dei processi di correzione

Fonte: Enterprise Strategy Group, 2014.

L'architettura Cisco per la sicurezza della rete: il Next-Generation Firewall incentrato sulle minacce

La reputazione di Cisco Systems si basa da sempre anche sui suoi prodotti per la sicurezza della rete. L'azienda ha dovuto adattare la sua visione tecnologica alle nuove esigenze delle aziende e a un panorama delle minacce sempre più pericoloso. Per conseguire questo obiettivo, nel 2013 Cisco ha completato l'acquisizione di Sourcefire, azienda innovatrice nel campo della sicurezza della rete.

La fusione Cisco/Sourcefire ha unito due aziende leader del settore, ma ha richiesto un grande impegno per integrare le tecnologie necessarie per la creazione dell'architettura per la sicurezza della rete di livello enterprise descritta in precedenza. L'annuncio della soluzione Cisco ASA con FirePOWER Services è il risultato di questo impegno. L'integrazione in un unico dispositivo del firewall Cisco ASA e dei sistemi di Sourcefire Next-Generation IPS (NGIPS) e Advanced Malware Protection (AMP) consente a Cisco di offrire un insieme completo di servizi per la sicurezza della rete caratterizzato da:

- **Visibilità e controllo granulari delle applicazioni.** Al pari di altri NGFW, il firewall Cisco può rilevare e creare report sulle connessioni delle applicazioni, nonché applicare policy di controllo granulare in base a utenti, gruppi, dispositivi e così via. L'aggiunta delle funzionalità FirePOWER consentirà probabilmente di estendere la visibilità e il controllo delle applicazioni a tutta la rete e di integrarli con altri asset Cisco, quali TrustSec e Identity Services Engine (ISE).
- **Protezione incentrata sulle minacce in tutta la rete e negli endpoint.** Grazie a FirePOWER per la protezione della rete e FireAMP per la sicurezza degli endpoint, l'architettura Cisco per la sicurezza della rete offre protezione completa dalle minacce e funzioni di rilevamento e prevenzione contro il malware avanzato. La prevenzione e il rilevamento delle minacce sono ancora più efficaci grazie ai sistemi FirePOWER NGIPS, ai filtri URL basati su reputazione e categoria e ai dati estesi di intelligence sulle minacce. FireAMP consente inoltre di tenere traccia delle attività degli endpoint per analisi cronologiche. Quando viene rilevato un nuovo file di malware, è infatti possibile applicare retroattivamente le policy di sicurezza per identificare gli endpoint che sono entrati a contatto con il file e apportare le correzioni necessarie. Infine, la soluzione Cisco integra gli eventi IPS, l'intelligence sulle minacce e gli eventi malware per fornire IoC dettagliati che consentono agli addetti alla sicurezza di migliorare o automatizzare le indagini sulla sicurezza e i processi di correzione.
- **Più servizi per la sicurezza con visibilità completa.** Cisco offre ora una gamma completa di servizi per la sicurezza fisici e virtuali per i firewall, il controllo delle applicazioni, i sistemi IDS/IPS, l'applicazione di filtri URL, il rilevamento e la prevenzione contro il malware avanzato e così via. Le aziende possono in tal modo personalizzare la protezione a più livelli per gli utenti, le applicazioni, i segmenti e i flussi in tutti i punti della rete e supportando più tipi di dispositivo. La soluzione Cisco offre inoltre funzioni di monitoraggio e visibilità per tutti i servizi e le posizioni per eliminare i punti deboli.
- **Valutazione dell'impatto.** L'architettura Cisco per la sicurezza della rete è progettata per correlare gli eventi di intrusione all'impatto potenziale di un attacco a un bersaglio specifico. Tale correlazione viene visualizzata tramite una serie di "indicatori di impatto": un indicatore di primo livello si riferisce a un evento corrispondente a una vulnerabilità mappata a un determinato host che richiede un intervento immediato, mentre gli altri indicatori definiscono priorità più basse. In questo modo, in situazioni di sovraccarico di lavoro è più facile per gli addetti alla sicurezza assegnare le limitate risorse in maniera oculata, a vantaggio della sicurezza stessa e dell'efficienza operativa.

Cisco ritiene che la combinazione delle soluzioni ASA e FirePOWER può migliorare la sicurezza in tutte le fasi: prima, durante e dopo un attacco. Nella fase che precede un attacco, l'architettura Cisco per la sicurezza della rete può risultare utile per rilevare le risorse della rete, applicare le policy di sicurezza e rafforzare i controlli per una maggiore protezione. Durante un attacco, le soluzioni ASA e FirePOWER consentono di rilevare attività sospette o dannose sia in rete sia a livello di endpoint, nonché di bloccare le connessioni di rete per offrire una difesa globale. Infine, un'architettura di questo tipo risulta vantaggiosa anche dopo un attacco, poiché consente agli analisti di sicurezza di valutare l'impatto di una violazione, modificare i controlli di contenimento e sfruttare i dati forensi per ridurre i tempi dei processi di correzione.

L'architettura Cisco può essere ulteriormente migliorata ed è prevista l'introduzione di nuove funzioni a partire dal prossimo anno e successivamente. Molti CISO vorranno valutare le difese attualmente disponibili nella rete aziendale e creare un piano di implementazione di un'architettura per la sicurezza della rete. A tale scopo, Cisco offre alle aziende diversi servizi specifici.

Uno sguardo d'insieme

In generale, c'è una convergenza di opinioni su vari aspetti della sicurezza informatica:

1. Le infrastrutture IT sono sempre più complesse a causa di innovazioni quali la virtualizzazione, la mobilità e il cloud computing.
2. Il panorama delle minacce è sempre più vasto ed è particolarmente difficile prevenire, rilevare e porre rimedio agli attacchi mirati.
3. La difesa offerta dalle misure di sicurezza della rete tradizionali è meno efficace che in passato.
4. Molte aziende non dispongono del personale qualificato in una o più aree della sicurezza della rete.

Complessivamente, si tratta di uno scenario preoccupante in cui i rischi legati alla sicurezza informatica crescono ogni giorno.

Albert Einstein affermò che "la definizione di follia è ripetere le stesse azioni all'infinito aspettandosi risultati diversi". Parole sagge, eppure è proprio quello che i CISO stanno facendo per cercare di risolvere i problemi. È giunto il momento per le aziende, i reparti IT e i leader nel settore della sicurezza di rivedere i piani di intervento. I criminali informatici seguono nuove strategie e dispongono di armi più sofisticate, ed è pertanto necessario che le aziende si dotino di nuove difese che consentano di migliorare la protezione, il rilevamento e la capacità di risposta.

ESG non ritiene che questi miglioramenti alla sicurezza della rete potranno venire da modifiche mirate e incrementali alle difese tradizionali. È invece necessario un cambiamento più strategico, ovvero un'architettura integrata e completa per la sicurezza della rete. La fusione di Cisco e Sourcefire nel 2013 ha aperto le porte a scenari decisamente interessanti. Con l'integrazione delle migliori funzioni del firewall ASA, dei sistemi FirePOWER NGIPS, Advanced Malware Protection e dell'intelligence complessiva sulle minacce, l'architettura Cisco per la sicurezza della rete ha il potenziale per raggiungere nuovi traguardi di leadership nel settore.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 USA | Tel.: +1 508 482 0188 Fax: +1 508 482 0218 | www.esg-global.com