Come affrontare le minacce avanzate via e-mail:

proteggi i tuoi dati e il tuo brand

Panoramica

Fin dagli anni '90 l'e-mail si è evoluta, passando da strumento impiegato principalmente da tecnici e professionisti della ricerca fino a diventare la colonna portante delle comunicazioni aziendali. Ogni giorno, le aziende si scambiano oltre 100 miliardi di messaggi e-mail.[1] Ovviamente, la sicurezza è diventata una priorità essenziale. Le campagne di spam di massa non sono più l'unico problema per la sicurezza. Oggi lo spam e i malware costituiscono solo una parte di un quadro più complesso:

- le minacce in entrata stanno diventando più organizzate, più personali e più pervasive.
- Nel frattempo, sussiste un grave rischio di fughe di notizie verso l'esterno, con conseguenze devastanti per la reputazione e le finanze aziendali.

Per combattere queste minacce, le soluzioni di sicurezza e-mail Cisco® offrono:

- Difesa avanzata dalle minacce
- Massima sicurezza dei dati
- Gestione semplificata

L'espansione delle minacce in ingresso

Gli attacchi via e-mail sono diventati sempre più complessi e sofisticati.

Più organizzati

Oggi, criminali informatici esperti danno vita ad aziende per creare malware, scoprire exploit, realizzare kit di installazione di malware e vendere reti di spam botnet e servizi di attacco di tipo Denial of Service (DDoS). Altri vendono servizi per rendere più efficaci queste attività. Per facilitare il trasferimento di payload e link dannosi, i criminali offrono programmi che testano lo spam con filtri antispam open source e reti spam-bot a basso volume, non rilevate da molti servizi di blacklist.

Più personali

Gli attacchi sono diventati molto più mirati. Setacciando i siti Web dei social media, i criminali reperiscono informazioni sulle vittime designate e creano e-mail di spear phishing basate sull'ingegneria sociale. Queste e-mail pertinenti, dirette a persone o segmenti di popolazione, contengono link a siti Web che ospitano kit di exploit. Secondo il *Report annuale di Cisco sulla sicurezza 2015*, "i messaggi di spear phishing, che da anni costituiscono il metodo preferito dai criminali online, si sono evoluti al punto che persino gli utenti finali più esperti faticano a distinguere i messaggi falsi da quelli autentici".[2]

Il rapporto inoltre evidenzia che il volume dello spam, uno dei principali metodi di consegna di messaggi e-mail collegati a malware, è cresciuto del 250% da gennaio a novembre 2014.[3]

Più pervasivi

Una volta i dipendenti controllavano messaggi e-mail basati su testo da una postazione di lavoro protetta da un firewall aziendale, mentre oggi accedono, in qualsiasi momento e luogo, a messaggi HTML complessi provenienti dai dispositivi più diversi. L'HTML fornisce varie strade per attacchi combinati, mentre l'accesso da luoghi diversi crea nuovi punti di accesso alla rete, che attenuano i confini tra livelli di sicurezza storicamente segmentati. I destinatari involontari di malware legato alle e-mail propagano l'attacco aprendo un allegato o facendo clic su un URL, esponendo così al pericolo altri dipendenti e l'infrastruttura.

Rischi delle e-mail in uscita

Oltre alla difesa dalle minacce, la sicurezza dei dati è una priorità essenziale per la maggior parte delle aziende. Vista la crescente quantità di dati sensibili per l'azienda e di informazioni personali che consentono l'identificazione (PII), inviata tramite e-mail, il rischio di fughe di notizie è particolarmente elevato. Per esempio, nel luglio 2014 la società di servizi di investimento globali Goldman Sachs Group ha avvertito i consumatori di una violazione dei dati avvenuta quando un appaltatore esterno ha inviato per errore dati dei clienti tramite e-mail, incluse "informazioni su conti di intermediazione altamente riservate", all'account Gmail di uno sconosciuto; non è noto quanti clienti di Goldman Sachs siano stati interessati dalla violazione.[4]

[1] *Report sulle statistiche delle e-mail*, The Radicati Group, Inc.; 2012-2016.; [2] *Report annuale di Cisco sulla sicurezza 2015*, Cisco, gennaio 2015.; [3] Ibid.; [4] "Cronologia delle violazioni dei dati," Privacy Rights Clearinghouse, aggiornato 31 dicembre 2013.

In molti paesi, ogni e-mail contenente PII deve essere inviata in modo crittografato. Se una persona non autorizzata può leggere e-mail non crittografate, l'azienda non è conforme alle norme Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA) o Sarbanes-Oxley Act (SOX), a seconda del settore. Centinaia di normative altamente variabili si aggiungono alla complessità e all'importanza del controllo dei dati in uscita. La maggior parte delle soluzioni di sicurezza non prevede metodi con cui i mittenti possano ritirare una violazione PII o sapere se i destinatari hanno letto il messaggio.

Infine, account e-mail compromessi possono diffondere un virus inviando ondate improvvise di spam verso l'esterno. Questo provoca l'inserimento in blacklist del dominio e-mail dell'azienda, anche se le e-mail sono firmate.

Il costo di una protezione inadeguata

Data l'ampia diffusione della protezione di base contro le e-mail non richieste e dannose, le aziende potrebbero credersi adeguatamente protette, tuttavia vengono creati sempre nuovi metodi per eludere questo livello di difesa. Di conseguenza, i costi delle violazioni della sicurezza annullano ogni risparmio a breve termine offerto dalla sola protezione di base.

100 banche di 30 paesi hanno perso centinaia di milioni di dollari, e potrebbero perderne anche di più in costi correlati, a causa di hacker che hanno utilizzato botnet per inviare e-mail contenenti malware a ignari dipendenti delle banche.[5] Quando i dipendenti hanno inavvertitamente aperto le e-mail, gli hacker hanno potuto prendere il controllo dei sistemi delle banche utilizzando le loro credenziali.[6]

Gli errori verso l'esterno possono danneggiare anche il valore del brand, la fiducia dei clienti e la reputazione delle e-mail di una società. Un mittente interno fuori controllo potrebbe compromettere irrimediabilmente la possibilità di un'azienda di inviare e-mail a destinatari legittimi. Gli errori possono anche comportare sanzioni per violazioni normative e produrre ulteriori perdite finanziarie. Nel 2013, un attacco e-mail di tipo phishing, diretto contro un fornitore terzo, è stato riconosciuto come l'origine della violazione dei dati di Target Corp., che ha esposto i dati delle carte di credito e personali di oltre 110 milioni di consumatori.[7] Nel febbraio 2015, i costi per la violazione della rete di questo dettagliante americano avevano raggiunto i 162 milioni di dollari.[8]

Sfide

Una protezione efficace delle e-mail richiede una prospettiva globale e multiprotocollo delle minacce, oltre a un'infrastruttura capace di affrontare tutte le fasi dell'attacco: prima, durante e dopo l'attacco. Inoltre sono necessarie scalabilità, conformità flessibile in uscita e capacità di crittografia, oltre alla capacità di evitare carichi gravosi sull'infrastruttura.

Cisco Email Security fornisce **difesa avanzata dalle minacce**, **massima sicurezza dei dati** e **gestione semplificata**, riducendo il TCO e le attività di amministrazione.

Difesa avanzata dalle minacce

Protezione rapida e completa delle e-mail sfruttando la rete di rilevamento delle minacce più ampia al mondo

La difesa avanzata dalle minacce Cisco inizia con il lavoro di Cisco Talos Security Intelligence and Research Group (Talos). Talos, è composto da ricercatori di spicco nel campo delle minacce, è il principale team che contribuisce all'ecosistema Cisco Collective Security Intelligence (CSI) con informazioni sulle minacce. L'ecosistema CSI include risposta alle minacce, intelligence e sviluppo (TRIAD), difesa gestita dalle minacce e operazioni di intelligence per la sicurezza. Cisco CSI è condiviso tra più soluzioni di sicurezza, offrendo una protezione e un'efficacia leader del settore.

[5] Jose Pagliery, "Ciò che sappiamo della rete di pirateria delle banche e chi vi si nasconde," CNN Money, 16 febbraio 2015.; [6] Ibid.;
[7] Bryan Krebs, "Attacco e-mail a fornitore crea violazione del bersaglio," KrebsOnSecurity blog, 12 febbraio 2014.; [8] John Fontana, "Il costo delle violazioni arriva a $ 162 milioni, report target," ZDNet, 17 febbraio 2015.

Talos utilizza set di dati di telemetria senza paragoni, basati su miliardi di richieste Web ed e-mail, milioni di campioni di malware, set di dati open source e milioni di intrusioni nelle reti, per produrre informazioni che forniscano una comprensione completa delle minacce. Questa capacità garantisce alle soluzioni di sicurezza Cisco un'efficacia leader del settore. Il nostro cloud di informazioni sulla sicurezza fornisce una "grande intelligence" e un'analisi della reputazione per il tracciamento delle minacce in reti, endpoint, dispositivi mobili, sistemi virtuali, Web ed e-mail.

Talos traccia costantemente oltre 200 parametri, inclusi:

- Elenchi della reputazione di domini, URL, indirizzi IP e file da bloccare
- Trappole di spam che attirano e-mail che potrebbero non passare attraverso i dispositivi Cisco
- Honeypot che trovano i responsabili degli attacchi, in modo che Cisco possa analizzarne i metodi
- Crawler che analizzano il Web segnalando i contenuti dannosi
- Ispezioni approfondite dei file che applicano analisi per rilevare contenuti dannosi
- Informazioni sui domini e WHOIS utilizzate per creare un database di domini dannosi

Difese antispam

Lo spam è un problema complesso, che richiede una soluzione sofisticata su più livelli: Cisco Anti-Spam fornisce la più elevata frequenza di cattura dello spam, con il tasso di falsi positivi più basso del settore, inferiore a 1 su 1 milione.

Per impedire ai messaggi di spam di raggiungere le caselle di posta, Cisco Anti-Spam combina un livello di filtraggio esterno, basato sulla reputazione del mittente, e uno interno, che esegue un'analisi approfondita del messaggio. Il filtraggio basato sulla reputazione blocca il 90% dello spam prima ancora che possa accedere alla rete, permettendo la scalabilità della soluzione attraverso l'analisi di un payload molto più ridotto. Il resto viene analizzato dal motore di Cisco Anti-Spam, dove noi chiediamo: Chi ha inviato il messaggio, quali sono le sue caratteristiche e quando è stato consegnato? Da quanto tempo il dominio e-mail è attivo? Dove porta l'URL contenuto nel messaggio?

Per Cisco Anti-Spam la categoria e reputazione dell'URL rappresenta uno dei parametri determinanti. La Figura 1 mostra il funzionamento di Cisco Anti-Spam.

Figura 1. Cisco Anti-Spam

Protezione antivirus e antimalware

L'unica soluzione antivirus zero-hour comprovata del settore protegge dai nuovi virus in meno di 60 minuti.

Advanced Malware Protection (AMP)

Cisco Advanced Malware Protection (AMP) è in grado di rilevare e bloccare il malware, eseguire un'analisi continua e fornire avvisi retrospettivi alla licenza della soluzione di sicurezza e-mail Cisco. Cisco AMP utilizza le vaste reti di informazioni sulla sicurezza nel cloud di Talos per fornire la massima protezione durante tutte le fasi dell'attacco: prima, durante e dopo un attacco.

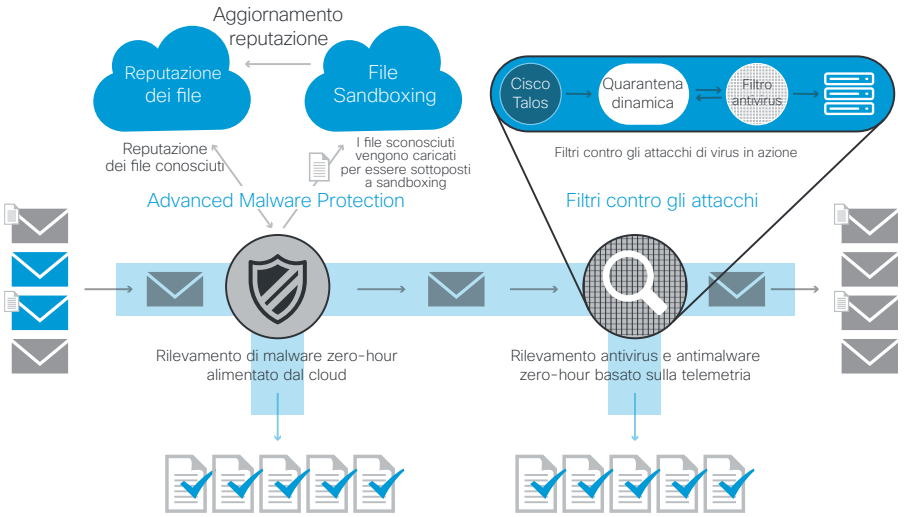
Cisco AMP utilizza una combinazione di valutazione della reputazione, sandbox e analisi retrospettiva dei file per identificare e bloccare le minacce nel corso dell'intero attacco. Le caratteristiche includono quanto indicato di seguito:

- **Reputazione dei file:** acquisisce un'impronta nel momento in cui un file attraversa il gateway di Cisco Email Security e la invia alla rete di intelligence basata sul cloud di AMP per un verdetto sulla reputazione. Con questi risultati, è possibile bloccare automaticamente file dannosi e applicare le policy definite dall'amministratore. L'interfaccia utente della soluzione Cisco Email Security è identica a quella di Cisco Web Security, mentre i framework di generazione dei report sulle policy rimangono pressoché invariati rispetto a quelli già conosciuti.
- **Sandbox dei file**: offre la possibilità di analizzare file sconosciuti che attraversano il gateway di Cisco Email Security. Un ambiente di sandboxing estremamente sicuro permette ad AMP di raccogliere dati sul comportamento dei file e di integrare queste informazioni con le analisi approfondite, eseguite da esperti o mediante sistemi automatizzati, per stabilire il livello di pericolosità dei file. Questa disposizione viene quindi inserita nella rete di informazioni sulle minacce di Talos e utilizzata per aggiornare e ampliare in modo dinamico la serie di dati cloud di AMP, ai fini di una migliore protezione.
- **Analisi retrospettiva dei file**: risolve il problema di quei file dannosi che riescono ad attraversare le difese perimetrali, ma che successivamente vengono riconosciuti come una minaccia. Anche le tecniche più avanzate potrebbero non essere in grado di identificare il malware a livello di perimetro, poiché tattiche come polimorfismo, offuscamento e timer di inattività sono particolarmente efficaci nell'impedirne il rilevamento. I file dannosi rimangono inattivi fino a quando non si trovano all'interno della rete.

  A questo punto, entra in azione l'analisi retrospettiva dei file. Essa assicura un'analisi continua dei file che hanno attraversato il gateway di sicurezza, utilizzando aggiornamenti in tempo reale da Talos per tenersi al passo con le nuove tattiche delle minacce. Quando un file viene identificato come una minaccia, AMP allerta gli amministratori, consentendo di individuare i potenziali utenti infetti della rete e il momento dell'attacco. In questo modo, AMP permette di identificare e gestire rapidamente un attacco prima che si propaghi.

I filtri contro gli attacchi di virus di Cisco forniscono un primo ed essenziale livello di difesa contro i nuovi attacchi, con un anticipo medio di 13 ore rispetto alla pubblicazione delle firme utilizzate dalle soluzioni antivirus tradizionali. Il Cisco Threat Operations Center (TOC) analizza i dati di Talos e definisce regole per mettere in quarantena i messaggi sospetti a livello mondiale (Figura 2). Man mano che acquisisce informazioni su un attacco, il TOC può modificare le regole e rilasciare messaggi di conseguenza dalla quarantena. I messaggi con allegati vengono mantenuti in quarantena fino al rilascio della firma aggiornata da parte di Sophos o McAfee.

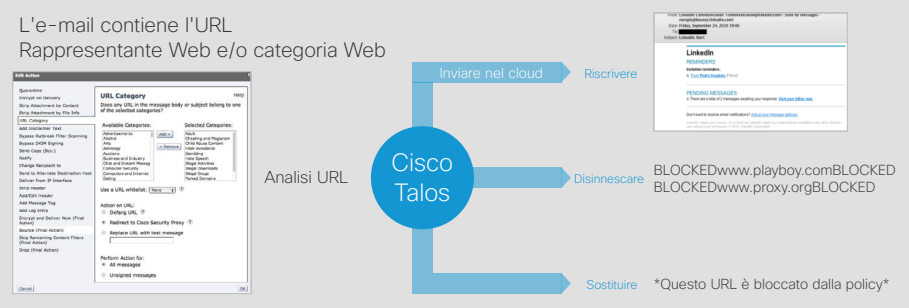
Figura 2. Protezione antivirus e antimalware di Cisco



I filtri contro gli attacchi di virus di Cisco proteggono anche da minacce combinate o attacchi mirati, con filtraggio degli URL collegati a messaggi sospetti. Cisco Email Security può riscrivere automaticamente o manualmente l'URL per:

- Reindirizzare il destinatario al proxy di Cisco Web Security; il contenuto del sito Web viene quindi analizzato attivamente e i filtri contro gli attacchi di virus di Cisco visualizzano una schermata iniziale, avvertendo l'utente che il sito contiene malware.
- "Disinnescare" l'URL, impedendo di potervi fare clic.
- Sostituire l'URL; questo viene rimosso completamente e viene visualizzato un messaggio per informare l'utente che parte del contenuto dell'e-mail è stato bloccato.

Figura 3. I filtri contro gli attacchi proteggono da minacce combinate e attacchi mirati



Massima sicurezza dei dati

Efficacia, precisione e semplicità sia nell'applicazione della policy sulla prevenzione della perdita di dati, sia nella crittografia delle e-mail

Prevenzione della perdita di dati: conformità garantita entro 60 secondi

I filtri per la prevenzione della perdita di dati (DLP) sono inclusi nelle soluzioni di sicurezza e-mail Cisco. Attraverso una partnership con RSA Security, leader in tecnologia DLP, la nostra soluzione di sicurezza e-mail fornisce oltre 100 policy predefinite, relative a norme governative, norme del settore privato e norme personalizzate della specifica azienda. Tra le soluzioni possibili figurano: crittografia, aggiunta di piè di pagina ed esclusioni di responsabilità, aggiunta in copia per conoscenza nascosta (BCC), notifiche, quarantena e altro. L'RSA Security Information Policy and Classification Research Team crea e aggiorna automaticamente policy predefinite con una metodologia comprovata, per la precisione migliore del settore. Con un filtro come "HIPAA", "GLBA" o "DSS", è possibile analizzare automaticamente le e-mail in uscita e crittografarle di conseguenza.

Per le aziende che richiedono una policy complessa, i componenti fondamentali necessari per la personalizzazione sono disponibili immediatamente e rendono il processo rapido e semplice.

Crittografia: Controllo completo del mittente, nessun costo aggiuntivo

Cisco Email Security è l'unica soluzione a offrire una revoca della chiave di crittografia per messaggio, per destinatario, che può essere effettuata dal mittente o dall'amministratore. Il mittente di un messaggio crittografato riceve una notifica di lettura una volta che il destinatario ha aperto il messaggio. Risposte e inoltri vengono crittografati automaticamente per mantenere privacy e controllo end-to-end. Per richiamare un messaggio, il mittente può bloccare o far scadere una chiave in qualunque momento.

Cisco Registered Envelope Service fornisce registrazione e autenticazione di tutti gli utenti come servizio gestito ad alta disponibilità, senza che i clienti debbano implementare infrastrutture aggiuntive. Per una maggiore sicurezza e un minore rischio, solo la chiave viene conservata nel cloud. Il contenuto del messaggio viene trasferito direttamente dal gateway del mittente al destinatario.

Gestione semplificata

Controllo completo, sempre aggiornato

Un dashboard di sistema centralizzato, personalizzato e consolidato indica lo stato del sistema e della coda di lavoro, lo stato della quarantena e le attività degli attacchi, oltre ad altre metriche fondamentali. Il sistema di quarantena centralizzato offre una singola posizione da cui gli utenti delle e-mail possono amministrare autonomamente le proprie quarantene dello spam e gli amministratori possono gestire le policy e le quarantene DLP.

Le regole di rilevamento dei messaggi contenenti minacce e gli aggiornamenti vengono applicati automaticamente, senza tempi di inattività o la necessità di intervento umano. Il risultato è una gestione senza necessità di intervento e una protezione di qualità superiore.

> "Con Cisco, una riduzione notevole del TCO e nuove funzioni per contrastare i virus e lo spam sono una realtà".
>
> – Kenichi Tabata, supervisore di reparto, Komatsu Ltd.

Conclusioni

Cisco fornisce soluzioni leader di mercato su larga scala, utilizzando il metodo più adatto per la tua azienda.

Cisco offre le seguenti soluzioni, basate su appliance, basate su cloud e ibride:

- **Cisco Email Security Appliance (ESA)** consente di conservare i dati sensibili on-premise, con prestazioni ottimali e facilità di gestione.
- **Cisco Email Security Virtual Appliance (ESAv)** fornisce implementazione rapida, scalabilità su richiesta ed efficienza operativa derivante dall'utilizzo degli investimenti esistenti.
- **Cisco Cloud Email Security** fornisce un modello di implementazione flessibile per la sicurezza e-mail in ogni luogo e momento.
- **Cisco Hybrid Email Security** fornisce il controllo avanzato dei messaggi in sede, sfruttando la convenienza della sicurezza nel cloud.
- **Cisco Managed Email Security** offre le prestazioni e la sicurezza di un'ESA on-premise, combinate con l'affidabilità del Cisco TOC.

Ulteriori informazioni

Per ulteriori informazioni, visita il sito all'indirizzo www.cisco.com/go/emailsecurity. Lavora con un addetto alle vendite, un partner di canale o un tecnico sistemista Cisco per valutare i prodotti Cisco più adatti a te.