

La necessità del controllo e del contenimento delle minacce

Le minacce rivolte alla sicurezza del network sono in grado di coartare significativamente la produttività, sconvolgere il business e le operazioni e causare la perdita di informazioni, con possibili conseguenze negative sia finanziarie che di compliance. Gli hacker continuano a sviluppare nuove tecniche, sempre più difficili da rilevare, per ottenere accesso alle informazioni a scopo di lucro. Le aziende hanno bisogno di soluzioni esaustive che siano altamente gestibili e proattive nel controbattere questi pericoli.

La problematica

Le imprese si trovano davanti a una miriade di problemi di sicurezza:

- Produttività IT e dei dipendenti durante l'attacco di un virus o worm
- Sicurezza delle informazioni riservate
- Protezione della reputazione e delle marche aziendali
- Sconvolgimento delle comunicazioni ed impatto sulle attività quotidiane
- Continuità delle applicazioni di e-business

Esempi di minacce vere subite da network veri

- Virus Zotob per la falsificazione di carte di credito—Il worm Zotob ha infettato organizzazioni quali la CNN, ABC News, il New York Times, Boeing ed il Dipartimento statunitense della Sicurezza Nazionale, nel tentativo di facilitare la contraffazione delle carte di credito. Gli investigatori dell'FBI ritengono che il creatore di Zotob sia stato assolto per creare più di una ventina di altri virus.
- Cavallo di Troia "rxbot" per fini truffaldini—Il cosiddetto rxbot ha infettato 400.000 computer con programmi di adware che hanno fruttato al suo creatore oltre 60.000 dollari di pagamenti a cliccata da parte dei produttori di software pubblicitario. Il presunto perpetratore è stato arrestato nel novembre del 2005 ed accusato di aver compromesso migliaia di macchine, comprendenti i computer della Divisione Armamenti del Naval Air Warfare Center e quelli dell'ente Defense Information Systems Agency del Dipartimento della Difesa statunitense.

- Cavallo di Troia personalizzato ai fini dello spionaggio industriale—I progettisti di un cavallo di Troia dedicato sono stati accusati di aver creato e distribuito spyware mirato alla raccolta di intelligence aziendale e di aver commercializzato il programma a tre agenzie private di investigazioni. Successivamente, queste agenzie avrebbero usato lo spyware per cingere dati dai concorrenti dei loro clienti. A detta della polizia, il programma sfruttava vulnerabilità del sistema operativo facendo uso di metodi standard di cattura dati, quali la registrazione delle battute, la cattura degli schermi e le trasmissioni dei file. I rapporti della polizia indicano che questo cavallo di Troia era stato introdotto con una e-mail o un dischetto promozionale apparentemente inviati alle imprese bersaglio da un loro contatto d'affari ben noto e stimato. Dozzine di aziende, presumibilmente sia negli Stati Uniti che in Europa sono finite preda di questo attacco.

La soluzione di controllo e di contenimento delle minacce

La soluzione Cisco offre ai clienti un approccio esaustivo di controllo e contenimento nella lotta contro le minacce, fornendo una protezione senza paralleli contro gli attacchi e le intrusioni sia mirate che basate su Internet, per le organizzazioni di qualsiasi dimensione.

- *Visibilità e protezione a 360°: una difesa di rete completa e proattiva.*
 - Conseguimento efficace sotto il profilo dei costi di intelligence contro le minacce rivolte all'intera infrastruttura, portabile su una varietà di sistemi e dispositivi
 - Identificazione delle minacce multivettore per rilevare le violazioni delle politiche, lo sfruttamento delle vulnerabilità ed i comportamenti anomali
- *Controllo semplificato: razionalizzazione delle politiche e della gestione sull'intera rete*
 - Gestione standardizzata delle politiche portabile su molteplici componenti del network.
 - Implementazione a livello infrastrutturale su una varietà di sistemi e di dispositivi

- *Continuità del business: una garanzia di salvaguardia delle operazioni dell'impresa*
 - Collaborazione e correlazioni senza precedenti tra i sistemi, gli endpoint e la direzione
 - Attivazione di risposte adattative alle minacce in tempo reale
 - L'elemento di base della strategia di rete autodifesa Cisco Self-Defending Network

Elementi di fondo della soluzione di controllo e contenimento delle minacce

- *Cisco Adaptive Security Appliance serie ASA 5500*—Una piattaforma modulare che offre servizi di sicurezza e VPN della prossima generazione, destinata ad una gamma di applicazioni, dal piccolo ufficio alla grande azienda. <http://www.cisco.com/go/asa>
- *Cisco ASA 5500 Anti-X Edition*—Combatte le minacce su Internet al gateway, sconfiggendo spyware, spam, virus ed altre minacce associate al contenuto di Internet. <http://www.cisco.com/go/asa>
- *Cisco Security MARS*—Offre una interfaccia di gestione della sicurezza contro le minacce che traduce i dati grezzi di network e di sicurezza in intelligence d'uso immediato. <http://www.cisco.com/go/mars>
- *Soluzioni Cisco Intrusion Prevention System (IPS)*—Proteggono server, applicazioni ed altri asset critici dagli attacchi e dai worm in rete ed applicativi, in corrispondenza al gateway, ai branch, ai centri dati e su tutta la LAN. <http://www.cisco.com/go/ips>
- *Cisco Security Agent*—Difende i server ed i desktop contro gli attacchi mirati, lo spyware, i rootkit e gli attacchi day-zero. <http://www.cisco.com/go/csa>
- *Cisco Network Admission Control (NAC)*—Convalida le credenziali degli utenti e di sicurezza del sistema proteggendo la rete e l'infrastruttura dalle infezioni. <http://www.cisco.com/go/nac>

Il portale Web Cisco Security Center costituisce una fonte unica ed integrata di indicazioni sugli eventi correnti nel campo della sicurezza, compresa intelligence applicata alle modalità offerte dai prodotti e dai servizi Cisco per mitigare le nuove minacce.

Servizi di sicurezza sull'intero ciclo utile integrati nelle soluzioni di controllo e di contenimento delle minacce

- Costituisce una fonte unica ed integrata di indicazioni sugli eventi correnti nel campo della sicurezza, compresa intelligence applicata alle modalità offerte dai prodotti e dai servizi Cisco per mitigare le nuove minacce offerte dai prodotti e dai servizi Cisco.
- I clienti di Cisco IPS Signature Subscription hanno accesso al database Cisco Security IntelliShield Alert Manager, che contiene esauriente intelligence sugli eventi IPS e che può correlare le firme IPS con gli allarmi IntelliShield, accelerando il recupero in caso di attacco.
- I servizi di consulenza sullo schieramento di Cisco IPS, Cisco Security MARS, Cisco NAC e di Cisco Security Agent semplificano l'impiego delle nuove soluzioni proposte dagli esperti Cisco mettendo in pratica oculati principi di progettazione della sicurezza ed una superba expertise di integrazione di network.

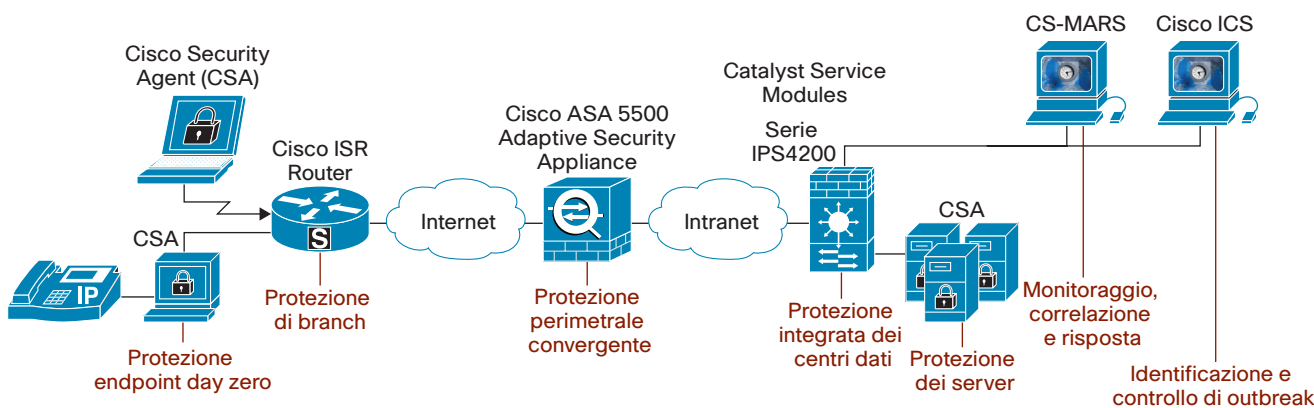
- Il servizio Cisco IPS Remote Update and Tuning semplifica le operazioni giornaliere dei dispositivi IPS, sviluppando e mettendo a punto gli aggiornamenti delle firme man mano che diventano disponibili.

Da dove cominciare

La maggior parte delle organizzazioni dispone di strumenti utili quale punto di partenza per realizzare un'architettura di prevenzione antiminaccia esaustiva e robusta. La tecnologia può essere introdotta in fasi successive, man mano che viene ridefinita la strategia di sicurezza dell'impresa. I processi di sicurezza vanno rivisti periodicamente per garantire che l'organizzazione continui ad adottare le pratiche migliori. Una strategia di sicurezza completa e proattiva è un processo in costante evoluzione, che comincia con l'identificazione dei punti cruciali. Per ulteriori dettagli sull'avvio della prossima fase della soluzione di sicurezza, fare riferimento al documento "Cisco Threat Control and Containment", disponibile presso il **rappresentante di account** Cisco.

La scelta Cisco

Cisco è il leader mondiale nel campo delle soluzioni di sicurezza di rete e vanta le più ampie capacità di combattere minacce sull'intera infrastruttura IT, da endpoint a network a layer di gestione. Le soluzioni di sicurezza Cisco sono integrate, collaborative ed adattative, rispondono in modo esaustivo alle minacce a cui sono esposte oggi le organizzazioni ed aiutano a salvaguardare la produttività IT e dei dipendenti e gli asset informatici critici dell'impresa. Sia che si tratti di minacce in Internet che di attacchi mirati, le soluzioni Cisco offrono agli amministratori IT e della sicurezza gli strumenti necessari per difendere le loro organizzazioni in un'era di minacce sempre più complesse e difficili da contrastare nel campo della sicurezza delle informazioni.



1 Fonte: <http://www.securityfocus.com/news/11297>

2 Fonte: <http://www.techweb.com/wire/security/177103378>

3 Fonte: TechWeb <http://www.techweb.com/article/showArticle.jhtml;jsessionid=U45GMNUB4Y4VOQSNLPSKH0CJUNN2JVN?articleId=181501294&pgno=2>