



Sicurezza integrata: come avere un'azienda sicura

ALL'INTERNO

- > Evoluzione degli ambienti IT e aziendali
- > L'impatto economico degli attacchi alle reti
- > La soluzione logica

Indice generale

| | |
|--|---|
| Quadro generale | 2 |
| Evoluzione degli ambienti IT e aziendali | 3 |
| Tipi di attacchi di rete | 3 |
| L'impatto economico degli attacchi alle reti | 4 |
| Attuali soluzioni di sicurezza | 5 |
| La soluzione logica: sicurezza integrata | 5 |
| Vantaggi della sicurezza integrata | 6 |
| Efficienza operativa delle funzioni di sicurezza | 6 |
| Impatto minimo degli attacchi sull'attività | 6 |
| Caratteristiche della sicurezza integrata | 6 |
| Il futuro della sicurezza integrata | 6 |
| Riferimenti | 7 |

> **Quadro generale**

Di fronte alla progressiva dipendenza delle organizzazioni dalle reti per tutte le attività di transazione economica, condivisione dei dati esterni e semplice comunicazione quotidiana, aumenta parallelamente la necessità di rendere tali reti sempre più accessibili ed efficienti. Tuttavia, se l'accesso alla rete diventa più semplice, è più facile raggiungere anche i dati cruciali che vi sono memorizzati. La sfida è garantire che l'accesso venga concesso solo alle persone autorizzate e impedito a tutte le altre. Tuttora, le soluzioni di sicurezza sono tipicamente composte da svariati prodotti mirati, determinando una carenza in termini di interoperabilità e gestibilità, e un maggiore costo di proprietà.

Un approccio efficace che sta emergendo per affrontare le sfide poste alle aziende della nuova economia è il concetto di sicurezza integrata. Questo metodo combina varie tecnologie di sicurezza con conformità alla politica, gestione del cliente, servizio e supporto e ricerca avanzata per una protezione completa. Tramite l'adozione di una strategia complessiva che affronti in modo globale la sicurezza a ogni livello della rete (ad esempio, client, server e gateway), le organizzazioni sono in grado di ridurre i costi, migliorare la gestibilità, accrescere le prestazioni, rafforzare la sicurezza e ridurre i rischi di esposizione. Se confrontato alle implementazioni basate sull'adozione di più prodotti mirati, un approccio integrato offre la visione più efficace della sicurezza con un rapporto costi-benefici ottimale. Questo documento fornisce una panoramica dei motivi principali che portano alla sicurezza integrata, tra i quali: il crescente numero degli attacchi alla rete ben progettati e sempre più sofisticati, l'impatto economico degli attacchi alle reti che non adottano una sicurezza integrata e infine si descrivono gli elementi e i vantaggi chiave di una soluzione di sicurezza integrata.

> Evoluzione degli ambienti IT e aziendali

La possibilità di disporre di comunicazioni e collaborazioni aperte tra i vari interlocutori di una società, tra cui clienti, impiegati, fornitori, partner, società di servizio e telecommuter, è indispensabile in un ambiente di rete aziendale.

I livelli gateway, server e client della rete sono interconnessi per soddisfare le esigenze dell'azienda interconnessa. Questo significa che le informazioni economiche cruciali risiedono su più livelli nella rete interna, ciascuno dei quali richiede una protezione specifica. Se tradizionalmente il personale IT era focalizzato sulla sicurezza centralizzata a livello di centro dati, ora si trova ad affrontare la definizione in costante evoluzione di raggio d'azione della rete e dei corrispondenti requisiti di sicurezza.

Allo stesso tempo, le minacce per la rete sono diventate sempre più sofisticate. Gli attacchi avanzati impiegano svariati metodi di propagazione, oltre a rilevare e sfruttare le vulnerabilità della rete.

Pur non essendo una competenza centrale per la maggior parte delle organizzazioni, la sicurezza si rivela un requisito indispensabile per le aziende che gestiscono transazioni on-line, diventando così un fattore economico determinante, non una semplice opzione IT. Per questa ragione, la sicurezza delle informazioni sta ricevendo una crescente attenzione da parte dei livelli direttivi più elevati, che sono interessati al modo in cui questa potrà aiutare l'azienda a ottenere gli obiettivi economici, più che al suo effettivo funzionamento tecnologico. Da un punto di vista della sicurezza, gli obiettivi del management comprendono:

- Implementare soluzioni che assicurano solide infrastrutture di rete aperte, ma sicure, per proteggere le risorse di informazioni e garantire la continuità operativa
- Tenere il passo con i variabili requisiti dell'e-business, ad esempio, alta disponibilità di rete, integrità dei dati e privacy, e le corrispondenti minacce alla sicurezza
- Soddisfare i requisiti di registrazione degli eventi, reporting, controllo e conformità
- Fronteggiare queste sfide con risorse limitate a costi contenuti
- Selezionare soluzioni che massimizzano la produttività degli impiegati, compresa quella del dipartimento IT, ad esempio, facilità di amministrazione gestione della soluzione di sicurezza

> Tipi di attacchi di rete

Esistono molti tipi di attacchi di rete, ciascuno con uno specifico grado di impatto. I comuni tipi di minacce comprendono:

- **ATTACCHI DI CODICE NOCIVO** Questi tipi di attacchi, capaci di danneggiare o compromettere la sicurezza di singoli computer oltre che di intere reti, sono in genere virus, worm e Trojan horse che si nascondono all'interno di file o codice di programmazione solo per riprodursi, propagarsi o essere diffusi da utenti di computer sconosciuti.¹
- **ATTACCHI DI TIPO DENIAL-OF-SERVICE (DOS)** Capaci di disattivare un singolo computer o intere reti, gli attacchi DoS sono espliciti tentativi di hacker con l'esclusiva intenzione di impedire che legittimi utenti di una rete utilizzino un certo servizio e/o di intralciare le normali attività operative. Esempi comprendono i tentativi di "sommersione" una rete, bloccando di conseguenza il traffico regolare, e i tentativi di ostacolare le connessioni tra due computer, impedendo così l'accesso a un servizio.

¹ "From Trojan Horses to Worms: Understanding Various Malicious Threats", articolo di Symantec, 13 giugno 2000.

- **ACCESSI NON AUTORIZZATI: HACKING INTERNO ED ESTERNO** Un hacker è qualcuno in grado di acquisire l'accesso e il controllo di computer, informazioni e tecnologia senza l'autorizzazione appropriata. Sfruttando le vulnerabilità della sicurezza nella rete di un'organizzazione, un hacker può acquisire l'accesso a importanti risorse di dati o di rete al fine di prelevarle, duplicarle o anche distruggerle. Indipendentemente dal fatto che il colpevole sia un impiegato malcontento, un fornitore esterno o un anonimo, l'invasione può portare a periodi di inattività dell'azienda, costi di ripristino e/o il costo spesso irrecuperabile di dati proprietari rubati.
- **MINACCE DI TIPO BLENDED** Queste minacce combinano le caratteristiche di virus, worm, Trojan horse e/o codice nocivo con vulnerabilità di server e di Internet per iniziare, trasmettere e diffondere un attacco. Utilizzando molteplici metodi di attacco e di propagazione, le minacce di tipo blended possono diffondersi rapidamente e causare danni generalizzati. Le minacce di tipo blended, come Nimda e CodeRed, sono state progettate per sfruttare le vulnerabilità di tecnologia di sicurezza che operano in modo indipendente tra loro.

> L'impatto economico degli attacchi alle reti

Gli attacchi di rete vanno da conseguenze di facile quantificazione, come l'interruzione delle attività, a perdite difficili da calcolare, come ad esempio, danni di immagine. Altre conseguenze degli attacchi di rete possono comprendere:

- **INTERRUZIONE DELLE ATTIVITÀ ECONOMICHE** I periodi di inattività dovuti a un attacco causano perdite di produttività e di profitti, e i costi associati con il ripristino di una rete violata possono aumentare l'impatto finanziario complessivo di un attacco. Una volta attaccata, un'organizzazione impegna tipicamente un team di ripristino per consentire a clienti, impiegati e partner di riprendere l'attività al più presto. Non solo l'attività viene interrotta fino all'implementazione di una soluzione correttiva, ma anche il team di ripristino viene distolto dai compiti quotidiani, aggravando ulteriormente la perdita di produttività.
- **ESPOSIZIONE LEGALE E POTENZIALI VERTENZE GIUDIZIARIE** Le organizzazioni che sono state attaccate possono ritrovarsi citate in tribunale come imputati o testimoni chiave. Le aziende che devono conformarsi alle normative sulla privacy e la sicurezza, come gli enti ospedalieri e le istituzioni finanziarie, possono avere la necessità di dimostrare il proprio impegno nel ridurre al minimo l'esposizione agli attacchi di rete. Questo processo contribuisce a limitare la produttività degli impiegati e la liquidità aziendale.
- **MINORE CAPACITÀ COMPETITIVA** Le informazioni vengono spesso considerate una delle risorse più preziose di un'azienda (il 70% o più del valore di un'azienda risiede nel proprio patrimonio di proprietà intellettuale)², la perdita o il furto di dati può rappresentare serie conseguenze, arrivando perfino a rendere insostenibile la posizione competitiva sul mercato. Secondo l'indagine sulla sicurezza e i crimini informatici condotta da CSI/FBI del 2002 (2002 CSI/FBI Computer Crime and Security Survey), le più gravi perdite finanziarie legate a violazioni della sicurezza comprendevano il furto di informazioni proprietarie (26 intervistati hanno indicato perdite superiori a 170.000.000 di dollari).³
- **DANNI DI IMMAGINE** Il danno dell'immagine di un'azienda può assumere varie forme, ciascuna delle quali è in grado di peggiorare la posizione competitiva sul mercato. Ad esempio, le aziende che hanno subito il furto di dati relativi ai clienti, come informazioni sulle carte di credito, che sono poi stati riportati pubblicamente su altri siti Web devono sostenere un compito molto arduo per recuperare la fiducia dei clienti.

² "Rapporto sull'indagine "Trends in Proprietary Information Loss", American Society for Industrial Security and PricewaterhouseCoopers, 1999.

³ Richard Power, Computer Security Institute, "Computer Security Issues and Trends", 2002 CSI/FBI Computer Crime and Security Survey.

> **Attuali soluzioni di sicurezza**

Le attuali soluzioni di sicurezza sono tipicamente composte da vari prodotti mirati. Si tratta di prodotti che possono essere acquistati, installati, distribuiti, gestiti e aggiornati separatamente. Con questo approccio, i responsabili IT devono affrontare i problemi relativi alle carenze di sinergia tra ciascuno dei prodotti. In genere la protezione non ha un effetto complessivo perché i problemi di interazione che sorgono tra prodotti di fornitori diversi spesso consentono alle minacce di approfittare delle falle che si creano per introdursi e compromettere la sicurezza. Inoltre, quando si verifica un'epidemia, le soluzioni fornite da ciascun fornitore devono essere testate e verificate attraverso le varie tecnologie presenti nella rete. Questo può rallentare la risposta agli attacchi, aumentando potenzialmente i costi conseguenti. Prodotti indipendenti possono anche degradare le prestazioni della rete; non essendo stati progettati per collaborare reciprocamente, presentano più di un problema per le prestazioni. Più in generale, vari prodotti mirati che non sono integrati si rivelano poco efficaci da gestire, contribuendo ad aumentare i costi di amministrazione e supporto IT.

Le implicazioni delle attuali soluzioni di sicurezza comprendono inefficienze, risultati deludenti (ad esempio, attenuazione del rischio inferiore al previsto e perdita di fiducia dei clienti e del mercato), e un maggiore costo di proprietà. Oltre a fornire una protezione inadeguata contro le minacce di tipo blended, i prodotti attuali richiedono impegnative attività di implementazione e configurazione. Tali prodotti fanno parte di una visione aziendale della sicurezza che può risultare difficile da comprendere e che fornisce una scarsa percezione della pianificazione e delle prestazioni.

> **La soluzione logica: sicurezza integrata**

La sicurezza integrata fornisce un sistema di sicurezza completo e globale in grado di affrontare le sfide e le opportunità delle odierne reti aziendali. Questo metodo combina varie tecnologie di sicurezza con conformità alla politica, gestione, servizio e supporto del cliente, e ricerca avanzata per una protezione completa. Utilizza i principi della difesa in profondità e adotta funzioni di sicurezza complementari a più livelli all'interno dell'infrastruttura IT.

Grazie alla combinazione di più funzioni, la sicurezza integrata è in grado di proteggere in modo più efficiente svariate minacce a ogni livello per ridurre al minimo gli effetti degli attacchi di rete. Le tecnologie di sicurezza chiave che possono essere integrate comprendono:

- **FIREWALLS** Controllano tutto il traffico di rete passando al vaglio le informazioni in entrata e in uscita dalla rete, o da una sua porzione, per aiutare a garantire che non si verifichino accessi non autorizzati ai computer e/o alla rete stessa
- **RILEVAZIONE DELLE INTRUSIONI** Rileva accessi non autorizzati e fornisce avvisi e report che possono essere analizzati per valutare i metodi e definire pianificazioni
- **FILTRO DEI CONTENUTI** Identifica ed elimina il traffico indesiderato
- **VIRTUAL PRIVATE NETWORK (VPN)** Proteggono le connessioni oltre il perimetro, consentendo alle organizzazioni di comunicare in modo sicuro con altre reti attraverso Internet
- **GESTIONE DELLA VULNERABILITÀ** Consente di svolgere valutazioni dell'atteggiamento sulla sicurezza di una rete svelando le lacune nella protezione e suggerendo miglioramenti
- **PROTEZIONE ANTIVIRUS** Protegge contro virus, worm e Trojan horse

Singolarmente, queste tecnologie di sicurezza possono risultare complicate da installare e in genere difficili e costose da gestire e aggiornare. Tuttavia, integrate in una singola soluzione, esse offrono una protezione più completa riducendo al contempo complessità e costi.

Per la maggior parte delle aziende, l'evoluzione dei problemi e dei criteri di sicurezza della rete ha comportato molto probabilmente l'implementazione successiva di vari prodotti, spesso ottenuti da fornitori diversi. È quindi abbastanza probabile che tali aziende migreranno gradualmente verso una soluzione di sicurezza integrata, per garantire la sinergia e l'integrazione dei prodotti concorrenti a ciascun livello della rete. Un tale approccio graduale comporterà l'integrazione iniziale di porzioni specifiche delle funzioni di sicurezza.

> **Vantaggi della sicurezza integrata**

EFFICIENZA OPERATIVA DELLE FUNZIONI DI SICUREZZA

La sicurezza integrata riduce la necessità di acquistare, installare, aggiornare e gestire più prodotti di sicurezza da fornitori diversi o di affrontare i problemi di sinergia tra prodotti di vari fornitori a ciascun livello della rete. Una tale soluzione consente di riallocare il personale IT su altri progetti strategici massimizzando la produttività del settore IT spesso sovraccaricato, e migliorando la gestione complessiva della sicurezza.

IMPATTO MINIMO DEGLI ATTACCHI SULL'ATTIVITÀ

Poiché può essere implementata a tutti i livelli della rete, una soluzione di sicurezza offre una maggiore protezione delle risorse proprietarie. La sicurezza integrata rende possibile un'operatività senza interruzioni, favorisce la produttività del personale, massimizza i ricavi e riduce la possibilità di implicazioni legali.

> **Caratteristiche della sicurezza integrata**

A causa della rapida evoluzione delle minacce, la sicurezza è un obiettivo in costante movimento. Il risultato è che la sua efficacia dipende strettamente dagli aggiornamenti più recenti sui virus e altri software. Applicando un approccio uniforme a sistemi e periferiche che contengono risorse di informazioni cruciali e importanti per l'attività, le organizzazioni possono garantire l'aggiornamento integrato di file con modelli di virus, schemi di rilevazione delle intrusioni, configurazioni di firewall e altri aspetti cruciali di un sistema di sicurezza.

La sola tecnologia non risolve i problemi della sicurezza. Una soluzione di sicurezza integrata funziona al meglio quando è realizzata su politiche e procedure rigorose, ed è supportata da personale appropriato e misure di protezione fisiche. Solide politiche e standard di sicurezza definiscono che cosa deve essere protetto, chi ha l'autorizzazione all'accesso e la ragione per la quale è stato richiesto l'accesso. Supporto di alto livello per la politica di sicurezza nell'organizzazione, oltre alla consapevolezza del personale che aiuta a garantire l'adozione di una politica coronata da successo.

Una strategia di sicurezza integrata migliora l'approccio globale alla sicurezza della rete in un modo non possibile attraverso l'implementazione di singoli prodotti di fornitori diversi. Indipendentemente dal fatto che la sicurezza sia gestita internamente o in outsourcing, la garanzia che tutte queste caratteristiche siano attive è indispensabile per mantenere un'infrastruttura vitale protetta.

> **Il futuro della sicurezza integrata**

Le organizzazioni possono ora beneficiare della sicurezza integrata in vari modi, comprendenti la maggiore efficienza delle funzioni di sicurezza, l'impatto economico minimo degli attacchi e un approccio globale alla sicurezza potenziato. Infatti, le aziende che adottano oggi una strategia di sicurezza integrata si troveranno nella posizione migliore per sfruttare la fase successiva, nella quale tutti i livelli della rete saranno integrati e gestiti in modo centralizzato. Attraverso questa integrazione della sicurezza a livello di azienda, le risorse dell'amministratore saranno ottimizzate, in quanto installazione, reporting e aggiornamenti saranno possibili da una singola console. Questa possibilità di gestione migliorerà ulteriormente la protezione, riducendo i costi di amministrazione, supporto e proprietà tipicamente associati alla sicurezza dell'azienda.

> **Riferimenti**

1. "From Trojan horses to worms: understanding various malicious threats", articolo di Symantec, 13 giugno 2000.
2. "Trends in proprietary information loss", American Society for Industrial Security and PricewaterhouseCoopers, <http://www.asisonline.org/spi.pdf>, 1999.
3. Richard Power, Computer Security Institute, "Computer Security Issues and Trends", 2002 CSI/FBI Computer Crime and Security Survey, <http://www.gocsi.com/forms/fbi/pdf.html>.

Note:

SYMANTEC, IL LEADER MONDIALE NELLA TECNOLOGIA DELLA SICUREZZA IN INTERNET, FORNISCE UN'AMPIA GAMMA DI SOLUZIONI PER LA PROTEZIONE DELLE RETI E DEI CONTENUTI PER SINGOLI UTENTI E AZIENDE. LA SOCIETÀ È UN FORNITORE LEADER DI PROTEZIONE ANTIVIRUS, FIREWALL E VIRTUAL PRIVATE NETWORK, GESTIONE DELLA VULNERABILITÀ, RILEVAZIONE DELLE INTRUSIONI, FILTRO DI CONTENUTI INTERNET E POSTA ELETTRONICA, TECNOLOGIE DI GESTIONE REMOTA, E SERVIZI DI PROTEZIONE ALLE AZIENDE IN TUTTO IL MONDO. IL MARCHIO NORTON DI SYMANTEC DEI PRODOTTI DI PROTEZIONE NELLA FASCIA CONSUMER GUIDA IL MERCATO IN TERMINI DI VENDITE E RICONOSCIMENTI MONDIALI. CON SEDE PRINCIPALE A CUPERTINO, CALIFORNIA, SYMANTEC SVOLGE ATTIVITÀ A LIVELLO MONDIALE CON SEDI IN 38 PAESI.

PER ULTERIORI INFORMAZIONI, VISITATE [HTTP://ENTERPRISESECURITY.SYMANTEC.COM](http://ENTERPRISESECURITY.SYMANTEC.COM)

SEDE MONDIALE
20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
1.408.253.9600
1.800.441.7234

ITALIA (MILANO)
Symantec srl
Via Rivoltana, 2D
20090 Segrate (MI)
Italia
Tel: +39 2 7033 21
Servizio Clienti
Tel: +39 2 48270000
Sito Web: www.symantec.it

Symantec è presente in 38 paesi.
Per informazioni sui contatti di ogni
specifico paese vi preghiamo di
visitare il nostro sito Web:
www.symantec.com

Per il Servizio Clienti ed il
Supporto Tecnico la prego di
visitare il nostro sito:
www.symantec.com/eusupport