PROTEZIONE PER LA VOSTRA AZIENDA -
GUIDE INDISPENSABILI PER LA SICUREZZA INFORMATICA

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:
www.watchguard.com

E-MAIL:
italy@watchguard.com

VENDITE ITALY:
011.954.2227

FAX:
011.954.2228

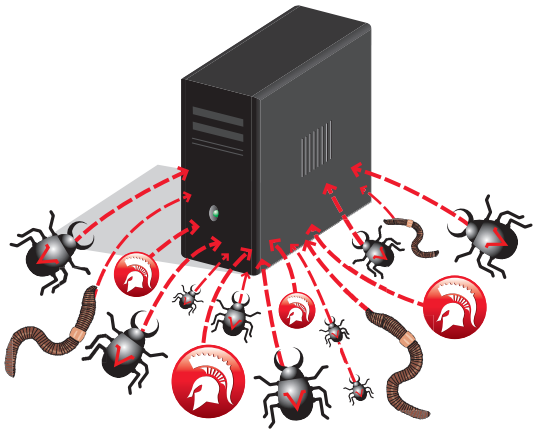
WatchGuard

1

PROTEZIONE PER LA VOSTRA AZIENDA - COMPRENDERE I PROBLEMI

WatchGuard

La società di analisi Canalys ha stimato che da un terzo fino alla metà delle PMI e la maggioranza delle piccole aziende non ha implementato una policy di protezione. In aggiunta, molte di queste aziende sembrano non rendersi conto dell'importanza degli investimenti nel settore della sicurezza anche se sono collegate direttamente ad Internet, in banda larga, senza utilizzare firewall hardware. Sebbene i firewall software siano in grado di fornire protezione, molti utenti di piccole aziende non conoscono in che modo installarli e configurarli, rimanendo in tal modo vulnerabili dei confronti di attacchi.



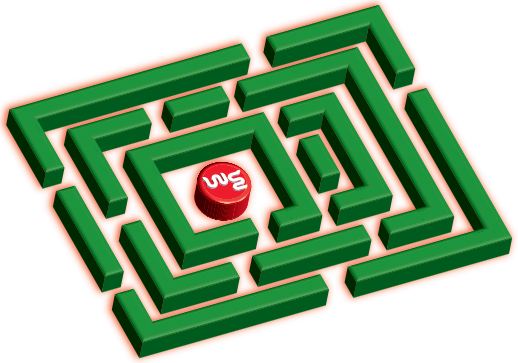
Questi dati sono allarmanti, soprattutto considerando che le minacce alla sicurezza rappresentate da hacker, virus e trojan, solo per citarne alcune, sono sempre più diffuse e che le loro conseguenze per le aziende possono essere devastanti.

Indipendentemente dalle sue dimensioni, senza adeguate protezioni un'attività può essere compromessa o distrutta in un baleno

Inoltre, il tradizionale profilo dell'hacker sta cambiando. Se ci eravamo abituati all'immagine di ragazzi annoiati che attaccavano le reti per divertimento, attualmente i protagonisti delle attività di hacking sono sempre più spesso legati alla criminalità organizzata e rivelano finalità come furto di identità, estorsione e commercio illegale.

NON SOLO PER LE GRANDI AZIENDE

Non solo le grandi aziende sono esposte ai rischi. Indipendentemente dalle sue dimensioni, senza adeguate protezioni un'attività può essere compromessa o distrutta in un baleno. Pur non potendo contare sulle maggiori esperienze e risorse delle grandi compagnie, le piccole aziende sono esposte alle stesse minacce ed hanno un'identica esigenza di protezione.



All'origine della sottovalutazione delle problematiche relative alla sicurezza IT da parte delle piccole aziende c'è spesso la convinzione che i sistemi di sicurezza sono estremamente costosi, molto difficili da utilizzare o non strettamente indispensabili. Nelle quattro guide seguenti, vi illustreremo i fondamenti della sicurezza, per aiutarvi ad individuare soluzioni adeguate alle possibilità economiche e alle specifiche esigenze della vostra azienda.

Questa prima guida offre un'analisi delle problematiche relative alla sicurezza e fornisce una pratica descrizione delle minacce attuali, illustrando alcuni dei più convenienti sistemi di protezione, in grado di prevenire i danni o, peggio ancora, la completa distruzione della vostra attività a seguito di un atto di pirateria informatica.

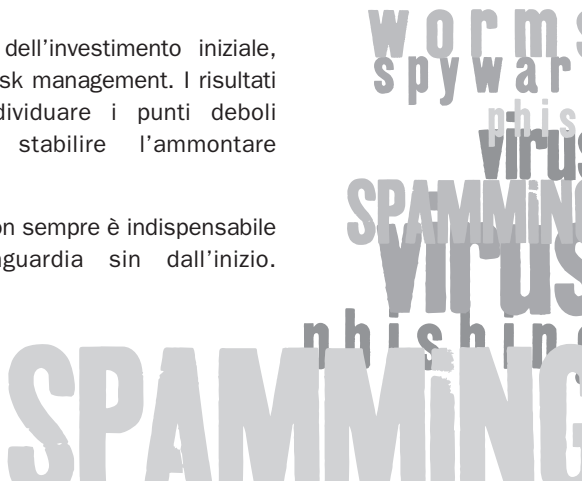
I COSTI

Le aziende sono spesso poco propense ad affrontare investimenti per sistemi di sicurezza, soprattutto se il ritorno non risulta immediatamente visibile. Le esigenze di sicurezza però aumentano e, grazie ad una sempre maggiore disponibilità di soluzioni su misura con le quali affrontare le specifiche necessità di aziende di ogni dimensione, l'investimento iniziale può anche rivelarsi inferiore alle previsioni.

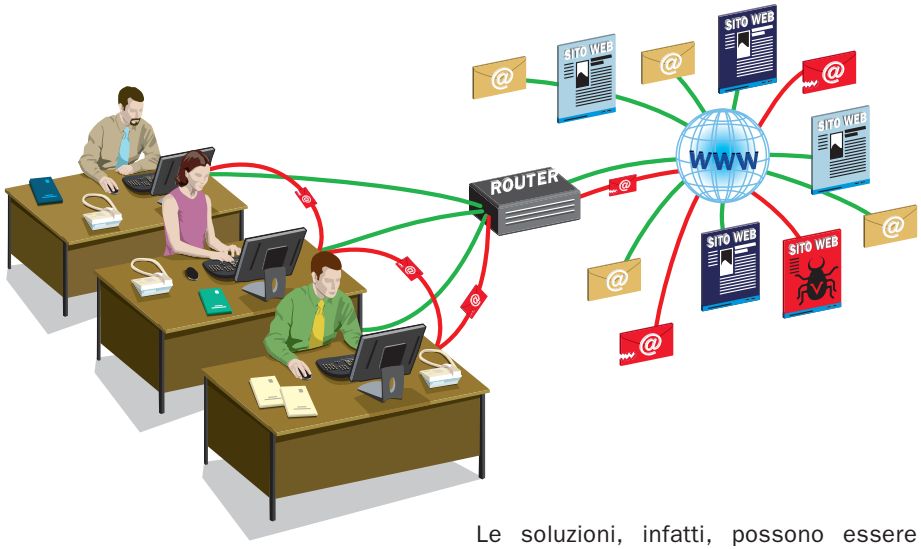
DA DOVE COMINCIARE

È importante partire dalla definizione dell'investimento iniziale, ottenuta attraverso una valutazione del risk management. I risultati di questa analisi consentono di individuare i punti deboli dell'infrastruttura esistente e di stabilire l'ammontare dell'investimento necessario.

Inoltre è fondamentale considerare che non sempre è indispensabile investire in una protezione d'avanguardia sin dall'inizio.



* Dynamic Markets 2005 http://www.dynamicmarkets.co.uk



Le soluzioni, infatti, possono essere ampliate successivamente, secondo le disponibilità finanziarie e in funzione delle specifiche esigenze aziendali.

Sottolinea le debolezze nelle infrastrutture esistenti ed indica i costi di investi mento richiesti

Maggiori informazioni sui sistemi di sicurezza sono riportate sulla seconda guida di questa serie.

L'ALLOCAZIONE DELLE RISORSE

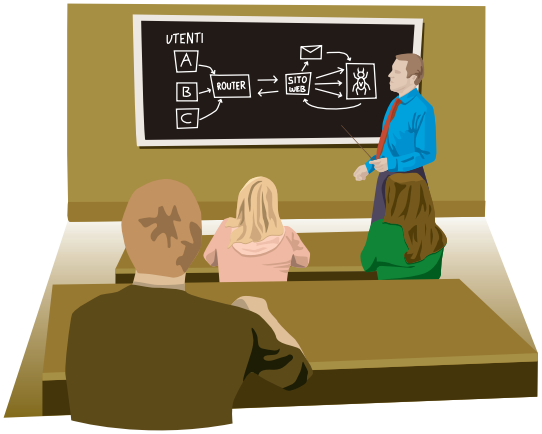
Il tempo necessario per la gestione e il mantenimento di un sistema di sicurezza non è un fattore da sottovalutare. La mancanza di supporto tecnico interno potrebbe rappresentare motivo di perplessità, ma, come già accennato, grazie ad una valutazione del risk management è possibile definire il livello delle risorse da allocare. Se non sono disponibili adeguate risorse interne, potrebbe essere necessario ricorrere all'outsourcing, affidando parte del processo a fornitori esterni.

MISURE PREVENTIVE

» SVILUPPARE LA CULTURA DELLA SICUREZZA

Un'organizzazione può adottare le soluzioni tecnologicamente più avanzate, ma queste non rappresentano necessariamente una protezione contro la minaccia più grande: il proprio personale.

In primo luogo, un'azienda che voglia proteggere il proprio network, deve sensibilizzare e rendere consapevoli i suoi collaboratori dell'importanza della sicurezza, informando tutti i dipendenti dei rischi legati a software non autorizzato, a messaggi e-mail dal mittente sconosciuto o con allegati sospetti e alla frequentazione di siti web contenenti dati illeciti. Inoltre, è fondamentale raccomandare ai collaboratori la massima cautela nella protezione di password e username. Troppo spesso, i collaboratori rivelano la password del proprio PC, esponendo ad attacchi l'intero network. Infine, definire una policy per la sicurezza del network con linee guida da adottare da tutti. Senza alcuna spesa iniziale, questo permette di fare il primo passo verso un'attività sicura e di evitare costi incalcolabili.



Un'azienda che voglia proteggere il proprio network, deve sensibilizzare e rendere consapevoli i suoi collaboratori dell'importanza della sicurezza

» VALUTAZIONE DEL RISK MANAGEMENT

Questo è il secondo passo da affrontare nella creazione di un sistema di sicurezza per il network. Si tratta del sistema più efficace per localizzare i punti deboli dell'organizzazione esistente e comporta quattro semplici azioni:

1) Identificare il pericolo, individuando cosa potrebbe accadere e come prevenirlo. Sono disponibili numerose fonti informative, on-line e off-line, che possono aiutarvi a scoprire i tipi di minacce esistenti, quindi utilizzatele. Per cominciare, è utile anche consultare il vostro attuale fornitore IT e la lettura di articoli sulle riviste specializzate.

Il sistema più conveniente per proteggere un network e, di conseguenza, un'azienda, è la pubblicazione di una policy per la protezione del network

2) Valutare le minacce e decidere se le precauzioni esistenti sono sufficienti o se è necessario potenziarle. È importante confrontare il costo della protezione delle risorse con il valore delle stesse, per non incorrere in spese non giustificate.

3) Raccogliere le informazioni. Registrando i dati reperiti, le vostre scelte e le loro motivazioni, comincerete a raccogliere informazioni che vi aiuteranno a prendere decisioni in futuro.

4) Rivedere regolarmente, riconsiderare e aggiornare le potenziali minacce.

» POLICY PER LA PROTEZIONE DEL NETWORK

Il sistema più conveniente per proteggere un network e, di conseguenza, un'azienda, è la pubblicazione di una policy per la protezione del network. Questo consente di illustrare ai collaboratori l'importanza dell'attenzione alle potenziali fonti di pericolo, riducendo così il rischio di attacchi provenienti, per esempio, da messaggi e-mail e da siti web. Gli esperti sono concordi sull'efficacia di una policy scritta per una corretta gestione aziendale. La policy per la sicurezza stabilisce adeguate normative sull'utilizzo e sulla gestione del patrimonio IT aziendale. Anche se sicuramente specifiche per ogni singola azienda, le informazioni riportate dalla policy devono essere categorizzate secondo i seguenti punti:

Affrontando esaurientemente queste tematiche, è possibile stilare un documento in grado di garantire la sicurezza e la protezione del network e dell'azienda. Va sottolineato che la gestione di una policy per la sicurezza è un processo in costante evoluzione. I pericoli cambiano continuamente nel tempo ed è importante che la policy sia gestita e aggiornata di conseguenza. Naturalmente, tutto il personale all'interno di un'organizzazione dovrebbe essere responsabilizzato sulla sicurezza aziendale e conoscere i dettagli della policy, inclusi quelli relativi ai livelli più alti. Nella gestione, l'esempio è sempre un fattore fondamentale.

Va ricordato che un'azienda che non sia in grado di dimostrare l'adeguatezza dei sistemi di sicurezza del proprio network, può ritrovarsi a rispondere per il mancato rispetto delle normative sulla sicurezza e sulla privacy, con eventuali conseguenze pecuniarie o legali.

» LAYERED SECURITY

Le soluzioni di protezione multi-livello rappresentano un metodo estremamente efficace che le aziende possono adottare garantire per la sicurezza del proprio network, grazie alla costituzione di difese a tutti i livelli in cui un network è potenzialmente vulnerabile basate su tecnologie multiple. Per maggiori informazioni sulle soluzioni di layered security, consultare ***www.watchguard.com***.

CONCLUSIONI

Le minacce per i network non scompariranno in futuro, ma saranno caratterizzate da una sempre più rapida evoluzione e da una maggiore pericolosità. Con l'aumento della dipendenza delle aziende, di ogni dimensione, da Internet e dalla connettività in rete per lo svolgimento delle loro attività, la sicurezza del network diventa un fattore fondamentale per la sopravvivenza. Le organizzazioni più piccole sono più vulnerabili e, con l'aiuto di questa serie di guide, vogliamo dimostrarvi che esistono soluzioni semplici e convenienti per ottenere tutta la sicurezza che vi occorre ed esattamente quando ne avete bisogno.

CODICI NOCIVI »

Provenienza

- E-mail
- The Internet

Conseguenze
I codici nocivi comprendono virus, worm e trojan. Questi poi creano una serie di istruzioni concepite espressamente per danneggiare i file dei computer e/o l'intero sistema. Questo può avvenire semplicemente bloccando un programma o cancellando l'hard drive. Dopo aver infettato il network, il codice comincia a propagarsi e può colpire singole workstation o l'intero network.

DENIAL E DISTRIBUTED DENIAL OF SERVICE (DOS E DDOS) »

Provenienza

- Sistemi danneggiati in internet

Conseguenze
Con il DDoS, gli hacker penetrano in centinaia di migliaia di computer in tutta la rete, acquisendo il controllo totale. Dopo aver installato su ogni macchina software per l'attacco, lanciano attacchi coordinati sui siti danneggiati, esaurendo ampiezza di banda, router processing e altre risorse di rete, e distruggendo la connettività del network per le vittime.

HACKING ESTERNO »

Provenienza

- Estranei che ottengono accesso non autorizzato alla rete di un'organizzazione attraverso i punti deboli del network

Conseguenze
Gli obiettivi principali delle attività di hacking sono furto, duplicazione e distruzione. Questo può causare interruzioni, perdita di produttività e notevoli costi.

HACKING INTERNO »

Provenienza

- Personale

Conseguenze
Le stesse conseguenze dell'hacking esterno, ma anziché provenire da estranei con un accesso non autorizzato, la minaccia viene direttamente dall'interno del sistema.

MINACCE COMBINATE »

Provenienza

- E-mail
- The Internet

Conseguenze
Le minacce combinate associano le caratteristiche delle altre forme di codici nocivi per lanciare attacchi che si diffondono provocando danni molto estesi. Queste minacce sono in grado di sfruttare le tecnologie per la sicurezza che operano autonomamente sul network.

SPAMMING »

Provenienza

- E-mail

Conseguenze
Il 70 per cento di tutti i messaggi e-mail in internet è costituito da spamming. I creatori di virus e worm utilizzano tecniche di spamming per diffondere i loro attacchi ed è fondamentale che i collaboratori siano vigili, evitando di aprire allegati di provenienza sospetta.

SPYWARE »

Provenienza

- Programmi nascosti inavvertitamente scaricati da internet

Conseguenze
La tecnologia spyware si avvale dell'utilizzo di cookie per monitorare l'attività on-line dell'utente. Questo consente agli hacker di raccogliere informazioni sugli utenti e sui siti da loro visitati, per poi trasmetterle a terzi, soprattutto con finalità pubblicitarie.

PHISHING »

Provenienza

- Falsi messaggi e-mail che sembrano provenire da una fonte ufficiale, per esempio una banca

Conseguenze
In questa forma di attacco, viene ricevuto un messaggio e-mail apparentemente proveniente da una fonte ufficiale. Un link nel messaggio invita l'utente ad un sito web che sembra quello autentico, ma che in realtà è fasullo. Lo scopo di questo raggiro è indurre l'utente a rivelare dati personali, permettendo a volte agli hacker di ottenere informazioni sui conti bancari o sull'identità. Ad operazione ultimata, il sito viene chiuso. Le vittime sono sia l'utente, che ha rivelato le informazioni, sia l'azienda, che vede compromessi il proprio marchio e la sua reputazione.