

White Paper



Inc.

Una protezione totale contro le nuove minacce informatiche

Computer Associates International,
Inc. Pubblicato in collaborazione con Inc.
Giugno 2005

Una protezione totale contro le nuove minacce informatiche

Una piccola-media impresa su tre ha subito almeno un episodio di interruzione delle attività dovuto a problemi di sicurezza.¹⁻¹

Altrettanto preoccupanti per le aziende sono le perdite causate dalla violazione dell'integrità o della riservatezza dei dati, per non parlare dei danni e degli incidenti non imputabili alla volontà dei singoli.

Primo di una serie di approfondimenti pensati per aiutarvi a proteggere la vostra impresa, questo documento descrive i pericoli che gravano sul vostro business, oltre alle tecniche che possono contribuire ad attenuarli, se non ad eliminarli.

Il prezzo della mancata protezione

- > **Quando i dipendenti si affannano** per tentare di recuperare ciò che è stato perduto o sottratto anziché svolgere le proprie normali mansioni, l'azienda subisce ovviamente un calo di produttività.
- > **Perdita di utili per transazioni interrotte.** Se per ipotesi le vostre principali banche dati dovessero essere messe fuori uso per l'azione di un hacker o di un virus, ne subirebbero le conseguenze anche i vostri clienti, fornitori e partner commerciali.
- > **Sistemi violati**, che richiedono tempo e denaro per essere riportati al normale funzionamento.

Le minacce che dovete affrontare

Internet è diventato ormai uno strumento adottato universalmente, alla stessa stregua dell'automobile o del telefono. Pertanto, anche se la Rete non svolge un ruolo primario nella effettiva conduzione della vostra attività, riveste sicuramente una funzione secondaria, ma destinata ad assumere una importanza ancor maggiore (e critica) per la vostra capacità di mantenere la competitività, in quanto sia i clienti che le altre aziende si affidano in misura crescente proprio a Internet per comunicare ed effettuare transazioni commerciali.

Proviamo a riflettere: l'utilizzo di Internet è pratica comune per oltre due terzi degli abitanti del Nord America, mentre il Vecchio Continente ha già superato questa quota e in Asia la diffusione della Rete cresce ad un ritmo del 50% superiore a quello degli Stati Uniti.

Con Internet, la posta elettronica e la messaggistica istantanea sono diventati importanti mezzi di comunicazione, grazie alla loro capacità di velocizzare gli scambi di informazioni e di ridurre i tempi necessari per condurre transazioni commerciali.

Inoltre, sta anche cambiando irreversibilmente il modo in cui beni e servizi vengono commercializzati.

L'utilizzo di Internet, tuttavia, presenta anche alcuni pericoli concreti:

- Il livello di familiarità raggiunto da Internet presso gli utenti domestici e professionali è diventato tale da valergli l'elezione a sistema privilegiato per la ricerca e la commercializzazione dei prodotti. Su Internet, però, non circolano forze di polizia addette a controllare la

Il prezzo della mancata protezione

- > **Perdita di dati** quando il backup non funziona correttamente, o quando un virus o un cavallo di troia si infiltra nel vostro sistema.
- > **Furto di segreti concorrenziali**, unitamente alle potenziali opportunità di business e ai flussi di ricavi da prodotti/servizi che essi rappresentavano.
- > **Perdita della fiducia dei clienti** quando una violazione della sicurezza comporta ritardi nelle spedizioni, errori negli ordini, ecc.
- > **Responsabilità legale** quando i dati sensibili vengono sottratti e aprono la strada al furto di anagrafiche di clienti e/o dipendenti e/o vengono fatti oggetto di altro uso improprio. Le aziende si espongono al rischio anche quando non riescono ad assumere le dovute precauzioni contro i messaggi "pop-up" indesiderati e altri eventi potenzialmente perturbanti.

validità dei reclami e l'autenticità di informazioni, siti e venditori. Così, mentre i responsabili degli uffici vendita e marketing sgranano gli occhi dinanzi alla prospettiva di attingere a una fonte così incredibilmente vasta di clienti, liquidità e informazioni, Internet e il suo canale di vendita da miliardi di dollari viene monitorato con un approccio improntato al "laissez faire", lasciando ad hacker, ladri, spie e vandali ampi margini di libertà per depredare vittime ignare.

- Nel momento in cui trasmette un messaggio e-mail, Internet si comporta come una sorta di enorme sistema radiotelevisivo. In pratica, oltre agli indirizzi di tutti i destinatari, i messaggi vengono diffusi a tutte le stazioni in ascolto. Le stazioni collegate a ciascun destinatario sono in grado di raccogliere ogni messaggio. È estremamente semplice (e molto più rapido della posta tradizionale), pertanto, inviare lo stesso messaggio a centinaia o persino migliaia di persone contemporaneamente. Allo stesso modo, è facile e rapido inviare a chiunque sia collegato a Internet messaggi contenenti virus, scam o altre forme di codici maligni. Oppure messaggi capaci di auto-replicarsi e ripetere il processo sfruttando la rubrica di ciascun PC contaminato. Sono gli stessi destinatari dell'e-mail che devono essere in costante stato di allerta, bloccando o cancellando i messaggi sconosciuti, resistendo alle tentazioni di allettanti proposte dietro le quali non vi è nulla di reale.
- Nonostante il battage propagandistico, tuttavia, non è Internet a rappresentare di per sé il pericolo più grave. Nella maggior parte dei casi, le aziende hanno raggiunto un grado di consuetudine tale con le tecnologie informatiche che le minacce più pericolose provengono da situazioni più comuni, "tradizionali": guasti dell'hardware, errori umani, danni al software e calamità naturali, quali incendi, nubifragi e interruzioni della corrente elettrica.

Le 5 principali sfide tecnologiche e le soluzioni necessarie per affrontarle

Per poter continuare a condurre con successo la propria attività, tutte le aziende devono tutelarsi contro ogni probabile azione di disturbo, sia essa causata dolosamente o fortuitamente. Queste, in sintesi, sono le principali sfide che le aziende devono saper affrontare:

Proliferazione di malware e altre intrusioni: l'impatto di virus, phishing e altri agenti dannosi

È opinione diffusa che Internet sia il luogo più libero che esista sulla Terra. Per quanto i governi possano darsi da fare per sorvegliare i contenuti che circolano e si diffondono dai propri confini per prevenire attività criminali, nel cyberspazio generalmente non esistono ostacoli alla libera circolazione delle informazioni.

Quindi, anche ammesso l'innegabile ruolo di Internet come fonte smisurata di istruzione e conoscenza, di fatti e opinioni, di storia e predizione, è altrettanto facile trovarvi anche "ricette" per creare caos e distruzione. E non sono pochi coloro che sfruttano la Rete per intenti criminali. Non conviene, pertanto, essere concilianti o credere che, per il semplice fatto di operare in un'azienda piccola o relativamente sconosciuta, i propri dati, applicativi e sistemi siano sicuri. La natura di Internet in quanto mezzo di diffusione fa sì che il malware possa essere progettato per mettere alla prova le difese di chiunque, indipendentemente dall'entità o dalla complessità di un'azienda. L'obiettivo è quello di trovare l'ingenuo e il vulnerabile di turno.

Proteggere l'azienda: gli errori più comuni da evitare

- > **Password non sicure.** Le password non devono essere facilmente decifrabili (devono contenere almeno sette caratteri ed essere composte da una combinazione di cifre, lettere maiuscole e minuscole e simboli !@#\$%^&*()+); non devono essere condivise; devono essere cambiate almeno una volta al mese; e non devono essere trascritte, per evitare che vengano trovate da malintenzionati.
- > **Apertura di messaggi e-mail di provenienza ignota.** Ricordate: chiunque conosce qualcuno di nome Paolo, quindi accertatevi che i vostri dipendenti controllino l'indirizzo e-mail del mittente, l'oggetto e verifichino la validità degli eventuali allegati (i quali devono essere esplicitamente segnalati nel corpo del messaggio).
- > **Scarsa conoscenza degli asset.** Se non sapete esattamente cosa possedete, non sarete in grado di proteggerlo. È necessario conoscere tutto sui dati da cui dipende la vostra azienda (sia nei database, sia nei PC dei dipendenti), e su software, sistemi, storage e configurazioni di rete che utilizza. Per tenersi al passo con l'intera dotazione informatica, occorre utilizzare una apposita soluzione di asset management e non consentire ai dipendenti di installare software o apparecchiature personali non protette.

Gli effetti di queste aggressioni e intrusioni possono essere devastanti:

- **Danneggiamento** e/o perdita di dati, applicazioni e sistemi critici per l'azienda
- **Perdita di produttività** quando i vostri sistemi vengono rallentati sotto l'effetto del software clandestino e gli addetti faticano per ripristinare dati e operazioni
- **Violazioni della privacy dei dati** che possono esporre la vostra azienda a problemi di responsabilità legale
- **Furto di dati sensibili** (quali i nuovi modelli di prodotti) che mettono a repentaglio la capacità della vostra azienda di mantenere la competitività
- **Perdita della fiducia dei clienti** quando comincia a diffondersi la voce di attacchi e intrusioni subite

Da un sondaggio CSI/FBI condotto nel 2004 sulla sicurezza e i crimini informatici, a cui hanno partecipato circa 500 responsabili della sicurezza di pubbliche amministrazioni e grandi gruppi industriali americani, è emerso che le perdite finanziarie dovute agli attacchi di virus sono risultate le più ingenti in assoluto, oltre il doppio della seconda voce di questa particolare graduatoria.¹⁻²

La buona notizia: avete la possibilità di mantenere la vostra azienda al riparo dalle minacce, siano esse interne o esterne, con una accorta combinazione di valide politiche di sicurezza e una ben congegnata implementazione di strumenti di sicurezza (vedere colonna laterale).

Mancata conformità: il costo dell'inosservanza delle nuove leggi e normative

Dopo l'11 settembre e i numerosi scandali aziendali, i governi di vari Paesi si sono fatti promotori di nuove regolamentazioni riguardanti la gestione societaria, la correttezza dei rendiconti finanziari, la protezione dei dati e della privacy, la tutela dei consumatori, la lotta al terrorismo e altro ancora.

Si considerino le sanzioni in vigore per chi viola le disposizioni della legge degli Stati Uniti sulla riservatezza delle informazioni sanitarie dei pazienti (HIPAA, Health Insurance Portability and accountability Act):

pena civili pecuniarie pari a un massimo di 100 dollari per violazione (fino a 25.000 a persona); le violazioni penali possono incorrere in sanzioni fino a 250.000 dollari e condanne fino a 10 anni di detenzione.

In una prima fase, queste nuove leggi - la cui violazione comporta sanzioni sostanzialmente più aspre rispetto a quanto previsto dalla HIPAA - erano perlopiù dirette alle grandi società ad azionariato diffuso. Più recentemente, tuttavia, molte nuove leggi (riguardanti in particolare la privacy e la tutela di consumatori e dipendenti) hanno puntato l'obiettivo anche sulle piccole e medie imprese. Per di più, si assiste a un forte effetto di ricaduta dai clienti delle grandi imprese, avvertito presso numerose aziende di piccola e media grandezza.

Mantenere la conformità alle nuove leggi e normative richiede in misura crescente l'adozione da parte della quasi totalità delle aziende di pratiche e tecnologie di sicurezza di base, backup dei dati e gestione della documentazione contabile. Malgrado tutto, in questa nostra era di

- > **Non tenersi aggiornati su patch e update di sistemi operativi/applicazioni/software e antivirus.** Tra gli hacker e i criminali on-line è una gara continua a chi batte il precedente record di velocità con cui approfittare dei difetti. La mancata installazione dei software di patch e aggiornamento permette a questi individui di introdursi nella vostra azienda con sempre maggior facilità; a voi pertanto il compito di verificare regolarmente presso i vostri fornitori di software che siate al passo con i più recenti update e patch.
- > **Trattamento inadeguato dei dati sensibili.** Vengono sottoposti a backup? E se vengono modificati di frequente, è prevista una procedura per il backup di tali modifiche? Vengono bloccati? Siete in grado di eseguire il ripristino dei dati di backup in modo tempestivo? Accertatevi.
- > **Mancata introduzione della codifica ogni volta che è possibile.** È fortemente probabile che il vostro personale invii dati tramite Internet, che è un po' come un deposito di cassette postali il cui contenuto può essere facilmente letto e copiato. Se queste comunicazioni hanno carattere riservato, è necessario che vengano criptate.
- > **Privilegiare la praticità a scapito della sicurezza.** Non permettete, ad esempio, ai vostri dipendenti di installare modem di accesso remoto nel proprio ufficio per poi poter accedere da casa al PC con cui lavorano. Non consentite ai dipendenti di ignorare le policy di sicurezza perché pensano che sia soltanto una scocciatura. Stabilite una policy e aderite alle sue regole.

massiccio affidamento alla tecnologia, questi criteri di salvaguardia sono diventati una buona procedura operativa per le aziende di qualsiasi grandezza e tipologia.

Quando il disastro colpisce: potete fare affidamento sui vostri dati di backup?

Quando i vostri computer e sistemi di rete subiscono un guasto, quale che ne sia la causa, la vostra azienda si trova con tutta probabilità in una situazione di grave rischio, ed è facile prevedere che la maggior parte degli inconvenienti sarà dovuta alla perdita dei dati critici necessari per mandare avanti le attività operative.

Secondo un recente studio, le aziende che subiscono interruzioni di corrente elettrica protrattesi per oltre dieci (10) giorni non riescono più a ristabilirsi pienamente a livello finanziario e in più della metà dei casi queste ditte sono costrette a chiudere i battenti nel giro di cinque anni.¹⁻³ Date queste premesse, appare quantomeno prudente sviluppare una strategia che risponda a criteri di fattibilità e garantisca un rapido recupero dei dati, contenendo il danno in termini di affari e soddisfazione clienti.

Il segreto per uscire indenni da tali calamità, piccole o grandi che siano, risiede nella capacità di preservare i dati. Senza le informazioni che ne costituiscono la linfa vitale, la vostra azienda può dirsi in pericolo. Fortunatamente, potete trarre profitto dall'opera di avanguardia condotta dalle grandi aziende che sono riuscite a mettere a punto le procedure necessarie per sopravvivere ai più gravi eventi di interruzione dell'attività, coniugando queste conoscenze con prodotti e i servizi di backup/ripristino e archiviazione dati attualmente disponibili a costi ampiamente accessibili.

Far fronte alla crescita dell'azienda: nuove opportunità, nuovi server e PC, nuovo software

Parallelamente alla crescita della vostra azienda, l'informatica assume un ruolo di crescente rilevanza, ma in un simile contesto riuscire ad allinearla alle effettive esigenze aziendali diventa un compito sempre più arduo.

Perché un'azienda e i suoi processi possano funzionare regolarmente, è necessario che sistemi, reti e dati vengano gestiti tutti in modo economicamente vantaggioso, anche in una situazione di crescente complessità della realtà aziendale. Per fare la differenza, sarà necessario operare una scelta oculata di soluzioni per archiviazione dati, gestione delle licenze software, migrazione PC e modellazione aziendale.

Mettere Internet al servizio del vostro marchio aziendale

Nella grande quantità di informazioni che circolano su Internet, è un'impresa sempre più impegnativa riuscire a far emergere il proprio marchio e attirare l'attenzione che desiderate. Quasi tutte le aziende ormai possiedono un sito Web, ma sono relativamente rare quelle che riescono ad avvalersi appieno degli strumenti e delle funzionalità disponibili per dare impulso alla propria visibilità. Malgrado le centinaia di milioni di visitatori giornalieri della Rete, numerosissimi siti rimangono pressoché inosservati.

Proteggere l'azienda: gli errori più comuni da evitare

- > **Ignorare la sicurezza fisica.** Significa che non dovete mai lasciare i computer senza un presidio umano. Non lasciate i portatili privi di dispositivi di protezione sparsi ovunque, persino fuori delle pareti dell'ufficio. All'occorrenza chiudete le porte a chiave, anche se è scomodo.
- > **Ignorare i comportamenti inconsueti.** La maggior parte delle violazioni della sicurezza avvengono dall'interno del posto di lavoro. Quando le attività di un individuo sono palesemente insolite e nessuno sa cosa le motivi, alzate il livello di attenzione.
- > **Mancanza di una adeguata formazione per utenti e amministratori di sistemi.** Risultati potenziali: installazione di programmi e servizi non necessari, destinati a diventare punti di vulnerabilità, in quanto presto dimenticati da tutti; ci si dimentica di testare le macchine che invece sono ancora "vive".
- > **Discontinuità tra policy e implementazione della sicurezza.** I vostri strumenti e sistemi preposti alla sicurezza devono essere configurati in modo tale da attuare le policy di sicurezza. In caso contrario, l'azienda diventa pericolosamente vulnerabile.

Fra le tecniche che possono aiutarvi in questa sfida, vi è ovviamente un efficace design del sito, che tuttavia deve essere accompagnato da attività di marketing basate su Web, generazione di contatti, comunicazioni ai clienti che ne hanno fatto richiesta, ottimizzazione dei motori di ricerca, ausili alla gestione dei contenuti e, per chi desidera vendere on-line, un sito Web di e-commerce. L'ultimo articolo di questa serie di white paper è proprio dedicato al tema delle best practice per il commercio elettronico e il marketing on-line e saprà orientarvi nella giusta direzione.

In conclusione

Ottenere la protezione di cui un'azienda ha bisogno per sopravvivere e prosperare - e potenziare la propria presenza on-line - è economicamente accessibile come non lo è mai stato prima.

Di più: le piccole imprese non sono più costrette ad adattare prodotti e servizi concepiti per le grandi aziende, poiché esistono prodotti sul mercato progettati per soddisfare le esigenze di organizzazioni di tutte le dimensioni e che si distinguono per semplicità e facilità d'uso.

Note finali

- 1-1 Security breaches affect majority of SMBs, The Yankee Group, Settembre 2004
- 1-2 2004 CSI/FBI Computer crime and Security Survey, The Computer Security Institute
- 1-3 Jon Toiga, Disaster Recovery Planning: Managing Risk and Catastrophe in Information Systems, Yourdon Press, 1989

Per maggiori informazioni sulle soluzioni CA per la piccola e media impresa, visitare il sito ca.com/smb.



Computer Associates®

© 2005 Computer Associates International, Inc. (CA). Tutti i marchi, i nomi commerciali, i marchi di servizio e i logotipi menzionati nel presente documento sono di proprietà delle rispettive aziende. Il presente documento ha carattere puramente informativo. Nella misura di quanto consentito dalla legge, questo documento viene fornito "as is" da CA, senza garanzie di sorta, comprese, senza intento limitativo, garanzie implicite di commerciabilità, idoneità per scopi specifici e non violazione. In nessuna circostanza CA sarà responsabile degli eventuali danni o perdite, dirette o indirette, derivanti dall'uso di questo documento, compresi, senza intento limitativo, il mancato profitto, l'interruzione di esercizio, la perdita di dati o di avviamento, anche qualora CA sia stata esplicitamente informata di tali danni.

Inc. and Inc. 500 sono marchi registrati di proprietà di Gruner + Jahr Printing & Publishing Co.

BSS178884 ITATYFWP.0805 MP282960605