

Recessione? Dieci modi per aumentare la sicurezza

di David Kelleher - Communications and Research Analyst presso GFI

L'anno scorso le aziende di medie dimensioni hanno speso il 9,4% in meno in sicurezza rispetto al 2007", annuncia una ricerca condotta da Forrester Research (www.forrester.com). "Molte piccole e medie imprese continueranno a ridurre i budget IT nel 2009; tuttavia, un settore in cui la spesa è in crescita è proprio quello della sicurezza".

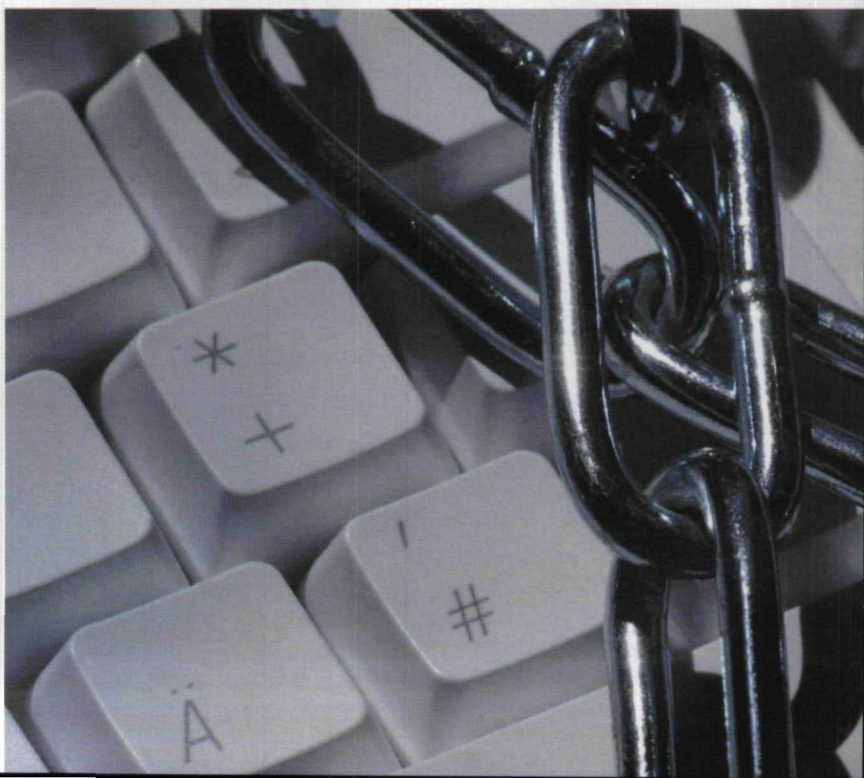
Sebbene molte aziende stiano comprensibilmente riducendo i fondi a causa dell'attuale clima finanziario, la sicurezza informatica rappresenta del resto un segmento dove le aziende non possono permettersi tagli. La protezione della rete e dei dati di una società costituisce infatti il cuore stesso del business. La sicurezza è quindi uno dei costi dell'attività e non una voce che si può aggiungere o rimuovere a piacimento da un elenco.

La sfida per molte PMI sta allora nel trovare il giusto equilibrio tra esigenze di sicurezza e contrazione delle spese. In che modo un amministratore IT può giustificare investimenti in sicurezza quando l'intera attività aziendale opera in modalità di risparmio?

Secondo gli analisti, molte piccole e medie imprese continueranno a ridurre i budget IT nel 2009; tuttavia la spesa per la sicurezza resta un elemento in crescita.

E del resto, sebbene le aziende stiano contraendo i budget a causa dell'attuale clima finanziario, la sicurezza informatica rappresenta un segmento dove le aziende non possono permettersi dei tagli perché il costo di una violazione al sistema, della perdita di dati e dell'inoperatività supera di gran lunga la spesa per proteggere dati e reti.

La sfida per molte PMI sta allora nel trovare il giusto equilibrio tra esigenze di sicurezza e riduzione dei budget. In che modo un amministratore IT può giustificare investimenti in sicurezza quando l'intera attività aziendale opera in modalità di risparmio?



L'errore umano è ancora, con ogni probabilità, la vulnerabilità più critica negli ambienti di archiviazione delle piccole e medie imprese. Con il previsto aumento del crimine cibernetico e del furto d'identità nel 2009, le PMI dovranno essere ancora più attente a difendersi dagli attacchi che fanno leva sull'ingenuità per indurre gli utenti a cedere ad attacchi di phishing (www.securindex.com/url.asp?id=71) e di ingegneria sociale (www.securindex.com/url.asp?id=72).

Le piccole e medie imprese non possono permettersi di ignorare il fattore protezione. Nonostante la limitazione dei budget, il costo complessivo di violazione, perdita di dati e inoperatività supera infatti di gran lunga la spesa per proteggere dati e reti. Il risparmio nel breve perio-

do può quindi tradursi in perdite di lungo termine se la sicurezza diventa un'altra vittima della recessione.

Una protezione adeguata è però ottenibile attraverso un mix di tecnologie e best practice in materia di sicurezza e i 10 suggerimenti di seguito elencati possono aiutare le PMI a far fronte alle minacce di sicurezza in un momento finanziario difficile.

1. Determinare le vulnerabilità

Condurre una verifica completa di tutte le misure di protezione in vigore - hardware, software e altri dispositivi - nonché di tutti i privilegi e le autorizzazioni di accesso a file conferiti ai dipendenti.

Testare attivamente la sicurezza dell'ambiente di archiviazione e controllare

i log della rete e degli archivi come firewall (www.securindex.com/url.asp?id=73), IDS (intrusion detection system www.securindex.com/url.asp?id=74) e di accesso per verificare se sia stato scoperto qualcosa o evidenziato un possibile evento di sicurezza. I log degli eventi rappresentano una risorsa importante, ma spesso trascurata, di informazioni sullo stato della sicurezza.

2. Controllare l'attività

Controllare continuamente e costantemente l'attività degli utenti. Per un singolo amministratore, il monitoraggio dei log degli eventi e l'esecuzione di verifiche regolari costituisce un'impresa enorme. Tuttavia, potrebbe essere più realistico controllare i registri dell'ambiente di archiviazione anziché tutta la rete. I log si

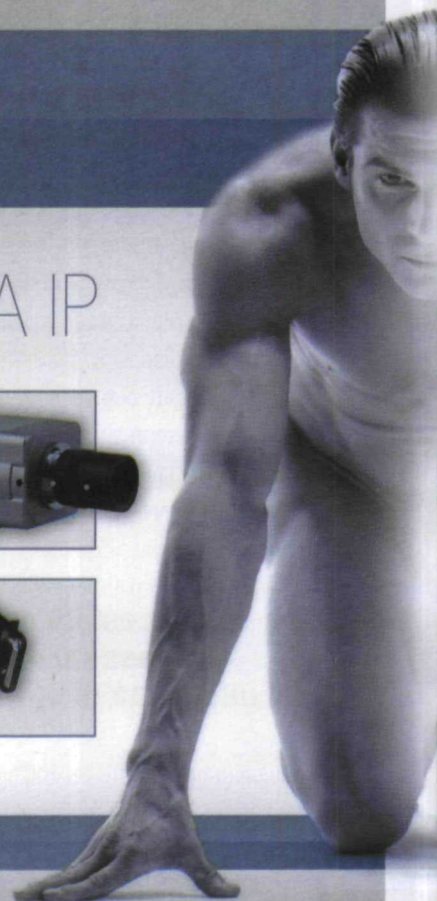


HRTM
HI RESOLUTION

SISTEMI E TECNOLOGIA IP



www.hrctv.com





sono dimostrati una fonte di grande valore in caso di violazione e di successiva indagine. L'analisi dei log va oltre tutto questo, non soltanto perché si tratta di uno strumento successivo all'evento, ma perché consente di comprendere meglio il modo in cui le risorse sono utilizzate, con conseguente possibilità di migliorarne la gestione.

3. Controllare gli accessi

L'accesso ai dati andrebbe conferito soltanto a coloro che ne hanno bisogno.

4. Proteggere le informazioni

Proteggere tutte le informazioni aziendali. L'utilizzo incontrollato di dispositivi di memoria portatili come le unità flash e i DVD mette a rischio considerevoli volumi di dati. Questi dispositivi possono essere smarriti o rubati con facilità. In molti casi, i dati presenti su dispositivi di memoria portatili spesso non sono neanche crittografati (www.securindex.com/url.asp?id=75).

5. Necessità di conoscenza e necessità di utilizzo

Implementare barriere tecnologiche che consentono l'utilizzo in base a criteri

chiari e definiti. Studi recenti dimostrano che la fuga di dati da parte del personale aumenta quando si verificano dei licenziamenti.

Dispositivi portatili come stick USB o PDA sono in grado di contenere grossi volumi di dati. Il monitoraggio e controllo del loro utilizzo sulla rete sono cruciali ai fini della riduzione del rischio di fuga di dati o attività illecite da parte di dipendenti insoddisfatti.

L'uso di dispositivi andrebbe limitato a coloro che hanno davvero bisogno di essere "mobili".

6. Criteri di gestione dei dati

Applicare criteri di protezione rigidi in tema di accesso, gestione e trasferimento dei dati. La tecnologia da sola non proteggerà i dati della società. Contribuirà molto a migliorare il livello della protezione degli archivi dell'organizzazione la presenza di criteri di sicurezza forti e la consapevolezza di dipendenti e personale dirigente in materia di problemi di sicurezza.

7. Comunicazione semplice con il personale

Spiegare il significato di ogni policy in un linguaggio semplice e chiaro, nonché la modalità di applicazione di ciascuna di esse in tutta l'organizzazione.

8. Formazione teorica del personale

È necessario ricordare ai dipendenti che non dovrebbero lasciare le password scritte su post-it attaccati al monitor. Devono capire che la condivisione di password equivale a condividere le proprie chiavi di casa. È necessario avvisarli di non divulgare informazioni a terzi senza prima verificare l'autenticità della richiesta. È necessario che abbiano una comprensione almeno di base delle minacce più comuni, ad esempio il phishing. Inoltre, è necessario ricordare loro che vengono monitorati e che sono responsabili nei confronti della società.

9. Backup completo

Effettuare il backup di tutte le comunicazioni e tutti i dati da, verso e interni all'azienda. Controllare i backup regolarmente per garantire che, in caso di indisponibilità della rete aziendale, sia possibile recuperare tutto in breve tempo. Non si desidera certo trovarsi nella circostanza in cui i file di backup siano danneggiati.

10. Gestione delle risorse umane

La sicurezza degli archivi è qualcosa di più della semplice protezione dei dati avvalendosi di tecnologie o mettendoli sottochiave: si tratta altresì di un esercizio di gestione delle persone. Le persone che usano e creano i dati rappresentano la principale minaccia alla sicurezza, nonché l'anello più debole. Anche se si prevede un aumento della spesa complessiva in sicurezza, la politica del "fare di più con meno" rimarrà l'elemento chiave del 2009. Seguendo questi elementari suggerimenti, le PMI potranno superare indenni l'attuale congiuntura economica senza compromettere la propria sicurezza informatica. www.gfi.com