



## Protezione intelligente: il personale rappresenta un rischio per la sicurezza? E la colpa è dell'azienda?

**N**onostante il concetto del 'paperless office' sia ancora un mito, è indubbio che la maggior parte dei dati aziendali viene archiviata in formato elettronico, dai database dei clienti, agli archivi di posta elettronica fino ai file confidenziali dell'ufficio del personale. Associando questo trend alla proliferazione di dispositivi mobili quali computer portatili, PDA, hard disk esterni e chiavette USB, e al desiderio e/o esigenza di lavorare fuori ufficio, ecco che si materializza una seria minaccia alla sicurezza. In aggiunta, con oltre il 50% dei dipendenti che ritiene le policy di sicurezza così rigide da doverle "raggirare" per riuscire a lavorare, è necessario che queste ultime vengano definite in maniera precisa ed equilibrata, sostiene David Kelleher, communications and research analyst in GFI Software.

A meno che i dati aziendali siano identificati, protetti e gestiti da soggetti autorizzati consapevoli delle policy, informazioni preziose e cruciali potrebbero essere smarrite, vendute a terzi o usate in maniera fraudolenta. La sicurezza di dati e archivi può es-

sere compromessa in tre modi principali:

- disponibilità e capacità dei NAS (network attached storage) sono in costante aumento. Ciò significa che anche il numero di persone che accede ai dati è in crescita, così come il rischio che informazioni riservate siano accessibili da parte di soggetti non autorizzati.
- l'utilizzo incontrollato di dispositivi di storage portatili, come le unità flash, mette a rischio considerevoli volumi di dati. Questi dispositivi vengono smarriti o rubati con facilità e spesso sono provvisti di livelli minimi di crittografia o controllo degli accessi.
- il rischio di perdita di dati aumenta di pari passo con il numero di dipendenti che sceglie di utilizzare un laptop perché quest'ultimo offre loro la possibilità di lavorare fuori ufficio.

### UNA MINACCIA COSTANTE ALLA SICUREZZA: LE PERSONE

Da qualsiasi prospettiva si osservi la sicurezza degli archivi, si riscontrerà un comune denominatore: le persone che, a loro volta, portano con sé il fattore dell'errore umano. Contrastare la fallibilità naturale dell'utente soltanto con la tecnologia non proteggerà i dati aziendali. Contribuiranno invece a migliorare il livello di protezione la presenza di policy di sicurezza forti e applicabili e la consapevolezza di dipendenti e dirigenti.

La sicurezza degli archivi è qualcosa di più della semplice protezione dei dati ottenuta avvalendosi di tecnologie o mettendoli sottochiave. Si tratta altresì di un esercizio di gestione delle persone perché è l'utente la principale minaccia, nonché l'anello più debole.

I singoli che hanno accesso a dati sensibili, e che costituiscono un numero di persone molto superiore a quello che si pensi, sono spesso soggetti ad attacchi, frequentemente realizzati tramite malware o spam personalizzati come gli inviti a scaricare

[www.gfi-italia.com](http://www.gfi-italia.com)

**Gli amministratori non devono considerare la definizione e applicazione delle policy un fardello dispendioso in termini di tempo.**

software "essenziali". Ciò che irrita di più, forse, è che molti dipendenti presumono che le misure informatiche in vigore costituiscano tutto il necessario e che quindi le policy siano ridondanti. Tuttavia, gli amministratori non devono considerare la definizione e applicazione delle policy un fardello dispendioso in termini di tempo. Devono invece rendersi conto che, aiutare il management a capire l'importanza di tali policy, li agevolerà nell'ottenere i fondi necessari per implementare modifiche o introdurre nuovi sistemi di protezione al fine di tutelare i dati della società.

### **È BENE PARLARE**

Tuttavia, policy forti non servono a nulla se non vengono comunicate a tutto il personale. Pertanto, le aziende devono garantire i passaggi necessari volti a comunicare in modo chiaro ed efficace al personale le informazioni richieste per ottenere un'adeguata gestione del rischio. La formazione in tal senso è fondamentale.

La comunicazione interna è di vitale importanza e spesso trascurata. Gli amministratori devono spiegare in un linguaggio chiaro e semplice il significato di ogni policy e il modo e le ragioni per le quali sono state implementate. Se le policy riguardano l'utilizzo di dispositivi portatili (e dovrebbero senz'altro farlo), gli amministratori devono spiegare perché certi dispositivi sono vietati o acquisibili soltanto per mezzo e con l'autorizzazione del reparto informatico. Qualsiasi approccio alternativo è controproducente.

I dipendenti non dispongono delle capacità di giudizio tecni-



che di un amministratore. Anzi, *ché avere l'atteggiamento di chi si chiede "Cos'altro posso fare per prevenire una violazione della sicurezza"*, i dipendenti pensano "Non capiterà mai a me!" È necessario informarli anche sui rischi più ovvi, ad esempio, quello di lasciare le loro password scritte su post-it attaccati al monitor, e capire che la condivisione di password equivale a condividere le proprie chiavi di casa. Devono inoltre comprendere che le loro azioni sono controllate e che sono responsabili nei confronti della società.

### **IN PRATICA...**

*Le prassi aziendali cambiano così come i processi e i requisiti di storage e l'IT rappresenta una funzione adattabile per consentire alle aziende di massimizzare i propri investimenti. Allo stesso tempo, anche le policy devono essere aggiornate regolarmente per tener conto delle nuove minacce.*

Un contesto lavorativo così tipicamente flessibile implica che le policy siano altrettanto adattabili, altrimenti si corre il rischio che diventino impraticabili. Una policy efficace dovrebbe essere

un documento dinamico, rivisitato e aggiornato regolarmente.

Se così non fosse, le policy di sicurezza sarebbero viste come troppo difficili da applicare oppure come ostacolo a un modo di lavorare più immediato. Infatti, un nuovo studio a cura della divisione RSA di EMC ha rivelato che oltre il 50% dei dipendenti "raggira" le policy di sicurezza per poter svolgere il proprio lavoro.

Di conseguenza, una sicurezza efficace è in realtà una strada a doppio senso: da un lato la formazione del personale al fine di mostrare come si possa spesso essere a rischio di compromettere le policy aziendali e le relative conseguenze, specialmente in situazioni in cui il ruolo richiede l'accesso remoto e la mobilità. Dall'altro, le società devono adattare le loro misure di sicurezza in maniera tale che, pur mantenendo policy information-centriche, riconoscano le esigenze di business e vi si allineino. In sostanza, tutti i dipendenti di qualsiasi reparto hanno un qualche grado di responsabilità in tema di sicurezza informatica e nessuno può realisticamente considerarlo il problema di qualcun altro. ■