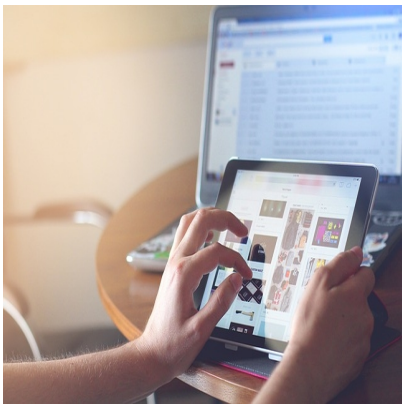
Data loss prevention nell’era mobile: una sfida per la sicurezza IT europea

La tecnologia mobile ha tracciato due direzioni all’interno del business: da un lato l’azienda vuole cogliere l'opportunità di soddisfare al meglio i clienti mobili, dall’altro sono i dipendenti stessi a chiedere che i dispositivi mobili diventino parte integrante dei loro strumenti di lavoro. In questo scenario i responsabili della sicurezza devono affrontare una serie di sfide per garantire la sicurezza dei dati

di TechTarget *06 Maggio 2016*



Il numero crescente di **dispositivi mobili nelle aziende** e le nuove versioni dei sistemi operativi stanno costringendo le organizzazioni a **ripensare le proprie strategie di protezione dei dati**. Se infatti da un lato la tecnologia mobile abilita nuovi approcci professionali e semplifica le operazioni dei dipendenti, dall’altro presta il fianco alle **diverse minacce del cybercrime** che potrebbero danneggiare (anche) in modo serio l’intero business.

Gli esperti sostengono che il passaggio da sistemi di file aperti (Windows 7) ad applicazioni sandbox (Android, iOS, Windows Phone) ha reso gli antimalware tradizionali e, in modo particolare gli antivirus, meno rilevanti. Le tradizionali **strategie per garantire la sicurezza IT**, dunque, possono rivelarsi ben poco efficaci quando si parla di mobile.

Ad esempio, su iOS, c'è poca necessità di prodotti antimalware o antivirus per la tipologia di progettazione nativamente sicura: le applicazioni sul dispositivo non possono accedere allo storage o alla memoria di un'altra applicazione.

Come regola geenrale, non esiste una strategia di sicurezza mobile universale. Ogni azienda, infatti, deve scegliere una soluzione cross-platform che funzioni su iOS e sui dispositivi mobili Android, così come su Windows, Mac OS X e Linux in modo tale che l'intera flotta delle postazioni di lavoro possa godere della giusta copertura.

Avere risorse sufficienti per garantire la protezione dei dati

Cosa stanno facendo le aziende per incorporare gli endpoint e gli strumenti di sicurezza mobili nelle applicazioni per avere la certezza che siano sicuri? Il consiglio degli esperti è di implementare nelle applicazioni **delle funzioni di data loss prevention** (DLP). Tuttavia, gli amministratori devono essere sicuri che le risorse IT sotto il loro controllo siano pronte

a cooperare con funzionalità avanzate come tracciamento e shadowing dei file. Con la data loss prevention **la quantità di dati che vengono monitorati** e il numero di copie memorizzate potrebbero assorbire rapidamente una fetta consistente delle risorse IT disponibili". Il CEO di CoSoSys riferisce che, secondo la sua esperienza, nei Paesi europei capita che **i CIO o gli amministratori IT** ritengano le proprie risorse insufficienti per **l'uso di funzioni DLP**. In questi casi il suo consiglio è quello di **valutare una gestione Cloud** della DLP e un mobile device management che offrano facilmente implementazione e scalabilità. Nei Paesi dell'Europa centrale e orientale, invece, sono molte le aziende che preferiscono sfruttare ancora i propri datacenter e la propria potenza di calcolo rispetto al Cloud.

Livelli di autorizzazione e flessibilità

Il software in uso nelle aziende sta cambiando: i responsabili della sicurezza IT e i loro team devono quindi conoscere e comprendere le diverse funzioni di protezione e i relativi limiti. Per quanto riguarda Android, aggiungono gli esperti, nelle prossime versioni c'è da aspettarsi di trovare più funzionalità di sicurezza aggiunte direttamente da Google. La funzionalità di blocco Android di Google, per esempio, dovrebbe contribuire ad **alleviare almeno alcune delle preoccupazioni in merito alla sicurezza degli accessi** e dei dati aziendali che gli amministratori IT potrebbero avere nel permettere ai dipendenti di utilizzare i dispositivi con tale sistema operativo. Uno dei compiti principali degli amministratori IT è quello di impostare i livelli di autorizzazione per i dipendenti in base alle esigenze dei diversi dipartimentali e alle relative attività. D'altro canto i responsabili IT devono anche garantire che la sicurezza non rappresenti un ostacolo per l'accessibilità. Per esempio, l'accesso di due utenti allo stesso dispositivo può implicare la presenza di **livelli di autorizzazione per il trasferimento dei dati completamente diversi**. Questo tipo di flessibilità sposa perfettamente la comodità con la sicurezza.