

Sicurezza dei dati: una tematica al centro del dibattito

Pubblicato: Venerdì 25 Novembre 2022



Il **tema della privacy** è ormai in maniera costante il punto focale del dibattito relativo alla sicurezza informatica, anche in relazione alla conservazione dei dati sensibili. Per le aziende italiane (così come del resto del mondo, ovviamente) risulta dunque indispensabile capire come fare per tenere i propri dati al sicuro prevenendo gli imprevisti di ogni giorno, che si possono verificare per distrazione umana, a causa di **cyber attacchi** o per colpa di guasti hardware. È importante dunque capire come realizzare una copia di sicurezza delle proprie cartelle e dei propri file, dal momento che il **backup dei dati** rappresenta la principale e più efficace modalità di protezione delle informazioni.

Le minacce ai dati

La **conservazione dei dati** può essere minacciata sia da fattori interni che da fattori esterni. In ogni caso, si sta parlando di un aspetto che non può e non deve essere sottovalutato, nemmeno nelle realtà di dimensioni più piccole. Sono due le categorie in cui è possibile distinguere le modalità dei backup: da una parte ci sono quelli che creano una copia dei file, a volte conservando anche la **struttura delle cartelle**; dall'altra parte, invece, ci sono quelli che impacchettano in un unico archivio di grandi dimensioni i file e la loro struttura di cartelle.

L'archiviazione locale e quella nel cloud

L'archiviazione nel cloud è una soluzione che viene adottata da aziende di tutte le dimensioni: si

differenzia rispetto a quella locale per gli standard di sicurezza più elevati che garantisce. Con l'**archiviazione locale**, il server aziendale si trova nell'infrastruttura dell'organizzazione, e spesso è fisicamente ubicato in sede. La rete locale aziendale consente la condivisione dei dati e delle informazioni e l'azienda gestisce tutti gli aspetti del server, dalla gestione alla manutenzione. Nel caso dell'**archiviazione in cloud**, invece, è un provider di servizi esterno a ospitare i dati: a tali servizi si può accedere tramite un web browser, da pc o usando un'app per i dispositivi mobili.

Perché passare al cloud

Il cloud offre numerosi benefici dal punto di vista della **sicurezza dei dati**, soprattutto se valutato in confronto a una soluzione locale. Peraltro, con il cloud vengono meno molti dei costi iniziali, perché la sola spesa da affrontare è rappresentata dall'abbonamento mensile. È il provider di servizi cloud che si occupa dei costi di supporto, di sicurezza, di **aggiornamenti software e di manutenzione**. Quasi tutti i provider per altro comprendono nei propri abbonamenti di base una quantità notevole di spazio di archiviazione. La migrazione verso il cloud è indispensabile anche perché offre una sicurezza – per così dire – a più strati, che si basa sulla protezione della rete, sui sistemi di controllo di accesso, sulla ridondanza dei dati, sulla sicurezza delle applicazioni, sulla crittografia dei dati inattivi e in movimento e sul costante monitoraggio delle minacce. Ma non è tutto, perché la sicurezza completa del cloud comprende anche il monitoraggio degli accessi e delle attività sospette, la protezione dall'eliminazione di file in massa e la convalida continua.

I servizi di cloud storage

I **servizi di cloud storage** agevolano la produttività e la collaborazione, anche perché consentono agli utenti di raggiungere i file in qualunque posto si trovino, a prescindere dal device che viene usato. Una soluzione indispensabile per proteggere i dati è rappresentata dalla **cifratura dei file**, un'operazione che deve essere effettuata prima che gli stessi siano caricati sul cloud, da uno qualunque degli endpoint gestiti. Tale operazione deve avvenire, però, in maniera che dal punto di vista degli utenti venga garantita la massima semplicità. Le procedure non devono interferire in alcun modo con le **attività lavorative**, e gli utenti devono essere messi nelle condizioni di poter raggiungere i dati cifrati da qualunque endpoint.

La cifratura dei dati

È auspicabile che i dati vengano cifrati in modo invisibile e automatico prima che gli stessi siano caricati sui **servizi di cloud storage**. Così, le informazioni possono essere gestite in maniera agevole: ciò è vantaggioso non solo sul piano della sicurezza, ma anche sotto il profilo economico, dal momento che contribuisce a ridurre in modo significativo le **spese di amministrazione**. È importante cifrare i dati anche per proteggere i server virtuali: così, anche nel caso in cui il provider di cloud storage dovesse essere **attaccato da un hacker**, i dati stessi sarebbero protetti e non finirebbero in mani sbagliate. Insomma, i dati – se sono cifrati – non possono essere visualizzati da chi non è autorizzato a farlo.

La protezione dei file aziendali su server e in cloud

Le imprese che hanno la necessità di garantire la **protezione dei file aziendali su server e in cloud** si possono rivolgere ad aziende specializzate come **Boolebox**, che mettono a loro disposizione tutti gli strumenti necessari per raggiungere questo obiettivo.

Redazione VareseNews
redazione@varesenews.it

