ENNEA TECHNOLOGY

4 ottimi motivi per eseguire il backup dei dati Cloud

Introduzione

Hai sotto controllo i tuoi dati aziendali nel cloud? Normalmente, la reazione istintiva è, “Certo che ce l’ho”, oppure “Il vendor pensa a tutto”. Pensaci bene: ne se proprio sicuro?
Microsoft, Google oppure Dropbox si prendono cura di alcuni aspetti, e offrono un ottimo servizio ai loro clienti. Detto questo, il loro obiettivo principale è gestire l’infrastruttura di e mantenere l’uptime per i tuoi utenti. La responsabilità dei dati è soltanto TUA. Il malinteso secondo cui i fornitori cloud eseguono il backup completo dei dati per tuo conto è abbastanza comune, e senza un cambio di approccio, è possibile andare incontro a ripercussioni negative quando tale responsabilità viene disattesa. In fondo, sei tu a doverti assicurare di avere l’accesso e il controllo sui dati di Microsoft 365, Google Workspace, SharePointOnline,OneDrive for Business e DropBox.

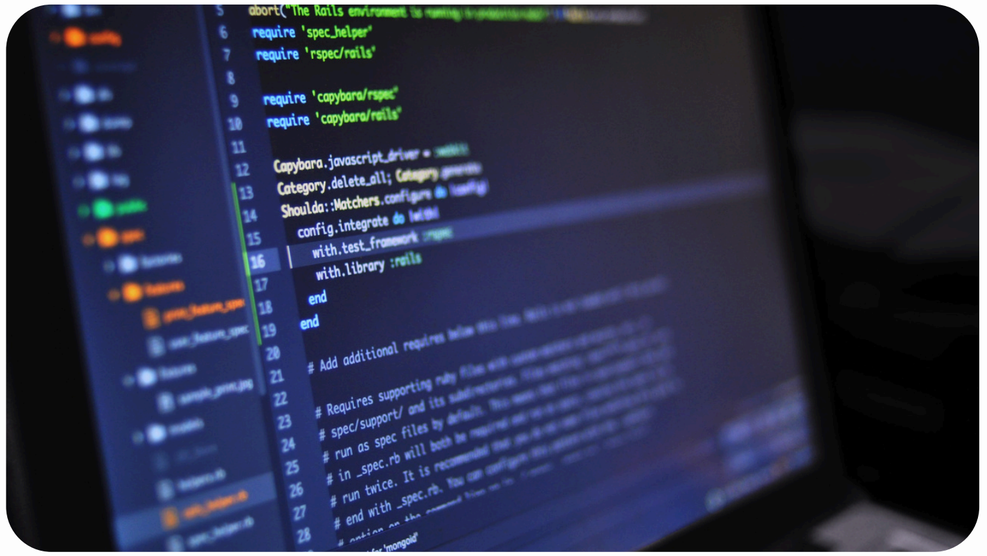
Ill malinteso si colloca tra la responsabilità percepita del vendor e l’effettiva responsabilità dell’utente di protezione e retention a lungo termine dei dati. Il backup e la recuperabilità forniti da Microsoft/ Google (o DropBox) e ciò che gli utenti presuppongono di avere sono spesso due cose ben diverse. Ciò significa che, a parte le normali precauzioni predisposte, potrebbe essere necessario rivalutare il livello di controllo dei dati e il livello di accesso di cui si dispone veramente.
I fornitori Cloud offrono la georidondanza, che spesso viene confusa con il backup. Il backup ha luogo quando viene effettuata una copia storica dei dati e quindi archiviata in un’altra posizione. Tuttavia, è ancora più importante avere l’accesso completo e poter controllare quel backup. Quindi, se i dati vengono persi, eliminati per errore o soggetti a un attacco informatico (ad esempio) possono essere ripristinati rapidamente. La georidondanza, d’altro canto, ti protegge da un guasto del sito o dell’hardware, per cui se si verifica un guasto o un'indisponibilità dell’infrastruttura, i tuoi utenti rimarranno produttivi e spesso non si renderanno neppure conto di questi problemi.

4 motivi per cui il backup dei dati cloud è importantissimo

Microsoft Office 365 e Google Workspace sono piattaforme Software as a Service (SaaS) robuste ed estremamente funzionale, oltre a rispondere perfettamente alle esigenze di molte organizzazioni. Entrambi i vendor offrono l'Availability e l'uptime delle applicazioni per garantire che i tuoi utenti non si perdano mai nulla, ma un backup dei dati può proteggerti da molte altre minacce alla sicurezza. Tu o il tuo capo potreste pensare che "Probabilmente il cestino è più che sufficiente". Ed è proprio qui che molte persone si sbagliano. In media, il periodo di tempo che passa da quando i dati vengono compromessi alla scoperta di questo fatto è di oltre 140 giorni. Davvero tanto. Esiste un'alta probabilità di non accorgersi che qualcosa manca o è andato perso finché non è troppo tardi per recuperarla dal cestino.

N. 1 Eliminazione accidentale

Se elimini un utente, intenzionalmente o meno,l'eliminazione viene replicata sulla rete insieme all'eliminazione del sito personale su SharePoint e ai relativi dati di OneDrive. I cestini e le cronologie di versione nativi inclusi in Office 365 possono proteggerti dalla perdita dei datisolo in modo limitato. Questo può trasformare un semplice ripristino da un backup vero e proprio in un grosso problema dopo che Office 365 ha eliminato i dati per sempre in manierageoreferenziata, oppure il periodo di retention è terminato.
Ci sono due tipi di eliminazione nella piattaforma di Office 365, l'eliminazione temporanea e l'eliminazione definitiva. Un esempio del primo caso è svuotare la cartella Elementi eliminati, anche detta "Elementi eliminati definitivamente". In questo caso, l'avverbio "definitivamente" non è daprendere alla lettera, poiché l'elemento può ancora essere trovato nella casella Elementi ripristinabili.
Un'eliminazione definitiva comporta che un elemento venga taggato per essere cancellato completamente dal database della casella postale. Una volta che questo accade, non è più recuperabile, punto.



N. 2 Minacce interne alla sicurezza

L'idea di una minaccia alla sicurezza richiama alla mente hacker e virus. Tuttavia, le aziende sono sottopostea minacce provenienti dall'interno, e tutto questo accade molto più spesso di quanto si pensi. Le organizzazioni sono vittime delle minacce generate dai propri dipendenti, intenzionalmente o meno.
L'accesso a file e contatti cambia così rapidamente che può essere difficile tenere d'occhio anche chi gode dalla più completa fiducia. Il vendor cloud non ha modo di riconoscere la differenza tra un normale utente e un dipendente licenziato che tenta di distruggere dati aziendali d'importanza critica prima di andarsene. Inoltre, alcuni utenti creano inconsapevolmente gravi minacce scaricando file infetti o comunicando involontariamente nome utente e password a siti ritenuti affidabili.
Un altro esempio è la manomissione di prove. Immagina un dipendente che elimina strategicamente email o fileincriminanti, tenendo questi oggetti fuori dalla portata dei reparti legale, conformità o HR.

N. 3 Minacce esterne alla sicurezza

Malware e virus, come il ransomware, hanno causato gravi danni a organizzazioni di tutto il mondo. Non solo la reputazione aziendale è a rischio, ma anche la privacy e la sicurezza dei dati, interni e dei clienti.
Le minacce esterne possono infiltrarsi attraverso email e allegati, e non sempre è sufficiente istruire gli utenti sulle cose a cui bisogna prestare attenzione, specialmente quando i messaggi infetti sembrano davvero convincenti.
Le limitate funzioni di backup/ ripristino delle piattaforme online sono inadeguate per gestire gravi attacchi.
Eseguire il backup con regolarità garantisce che una copia separata dei dati sia priva di infezioni e facilmente recuperabile.

N. 4 Requisiti legali e di conformità

Talvolta è necessario recuperare inaspettatamente email, file e altri tipi di dati in seguito ad azioni legali.
A volte non avresti mai pensato che ti potesse accedere qualcosa finché non accade davvero.
I requisiti legali, i requisiti di conformità e le normative di regolamentazione variano in base a settore e Paesema multe, sanzioni e controversie legali sono tre coseper cui non c'è spazio nella lista delle cose da fare