6 ottimi motivi per eseguire il backup di Office 365

Il motivo per cui le organizzazioni devono proteggere i dati di Office 365

VEEAM

Introduzione

Hai sotto controllo i tuoi dati di Office 365? Hai accesso a tutto ciò che ti serve? Normalmente, la reazione istintiva è, "Certo che ce l'ho", oppure "Microsoft pensa a tutto".

Pensaci bene: ne se proprio sicuro?

Microsoft si prende cura di alcuni aspetti, e offre un ottimo servizio ai suoi clienti. Detto questo, l'obiettivo principale di Microsoft è gestire l'infrastruttura di Office 365 e mantenere l'uptime per i tuoi utenti. La responsabilità dei dati è soltanto TUA. Il malinteso secondo cui Microsoft esegue 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 Exchange Online, SharePoint Online e OneDrive for Business.

Questo report passa in rassegna i pericoli legati a non aver predisposto il backup di Office 365 e i motivi per cui le soluzioni di backup per Microsoft Office 365 colmano le lacune della retention a lungo termine e della protezione dei dati.

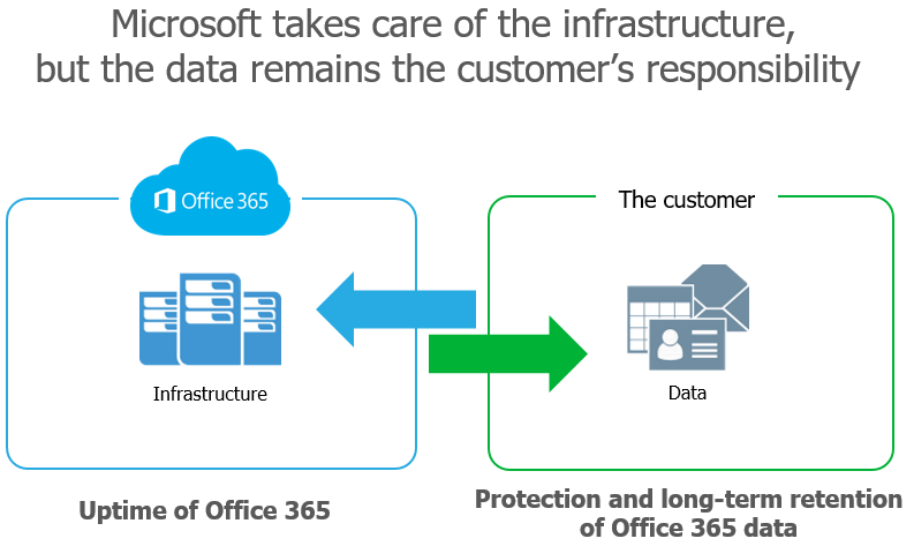
"Siamo preoccupati per le policy di backup e retention in Office 365. Microsoft si prende cura dei nostri dati, e proteggere i dati storici dell'e-mail è importante. Ecco perché abbiamo deciso di avere un backup dei nostri dati che risiedono in Office 365".

— ***Karen St.Clair***, IT Manager,
Columbia Power & Water Systems

Il grande malinteso di Office 365

Il malinteso si colloca tra la responsabilità percepita di Microsoft e l'effettiva responsabilità dell'utente di protezione e retention a lungo termine dei dati di Office 365. Il backup e la recuperabilità forniti da Microsoft e ciò che gli utenti presuppongono di avere sono spesso due cose ben diverse. Ciò significa che, a parte le normali precauzioni predisposte in Office 365, potrebbe essere necessario rivalutare il livello di controllo dei dati e il livello di accesso di cui si dispone veramente.

Microsoft Office 365 offre 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.



"Anche con l'utilizzo di Office 365, i dati rimangono tuoi. Li possiedi. Li controlli".

— *The Office 365 Trust Center*

6 motivi per cui il backup di Office 365 è importantissimo

Microsoft Office 365 è una piattaforma Software as a Service (SaaS) robusta ed estremamente funzionale, oltre a rispondere perfettamente alle esigenze di molte organizzazioni. Office 365 offre l'Availability e l'uptime delle applicazioni per garantire che i tuoi utenti non si perdano mai nulla, ma un backup di Office 365 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 [1]. 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.

Parlando con centinaia di professionisti IT di tutto il mondo che sono passati a Office 365, sono emerse sei principali vulnerabilità nella protezione dei dati:

Eliminazione accidentale

Lacune e confusione nella policy di retention

Minacce interne alla sicurezza

Minacce esterne alla sicurezza

Requisiti legali e di conformità

Gestione di distribuzioni e migrazioni di e-mail ibride a Office 365

[1] https://discover.office.com/6-steps-to-holistic-security/chapter1/

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 dati solo 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 maniera georeferenziata, 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 da prendere 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
Lacune e confusione nella policy di retention

Il ritmo frenetico del mondo aziendale di oggi si presta a policy che si evolvono continuamente, tra cui le policy di retention con cui è difficile tenere il passo e che sono complesse da gestire. Proprio come l'eliminazione definitiva e temporanea, Office ha limitato le policy di backup e retention che possono solo evitare perdite di dati occasionali, e non sono destinate ad essere soluzioni di backup complete.

Un altro tipo di ripristino, quello point-in-time degli elementi della casella di posta, non rientra nell'ambito d'azione di Microsoft. Nel caso di un problema catastrofico, una soluzione di backup può offrire la possibilità di tornare a un point-in-time precedente al problema, e salvare la situazione.

Con una soluzione di backup di Office 365 non sussistono lacune nella policy di retention o rigidità del ripristino. I backup a breve termine o gli archivi a lungo termine, i ripristini granulari o point-in-time, tutto è a tua disposizione per rendere il ripristino dei dati veloce, facile e affidabile.

N. 3
Minacce interne alla sicurezza

L'idea di una minaccia alla sicurezza richiama alla mente hacker e virus. Tuttavia, le aziende sono sottoposte a 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. Microsoft 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 file incriminanti, tenendo questi oggetti fuori dalla portata dei reparti legale, conformità o HR.

N. 4
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 di Exchange 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. 5
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. Microsoft ha predisposto un paio di reti di sicurezza (blocco per controversia legale), ma, di nuovo, non si tratta di una robusta soluzione di backup in grado di tenere la tua azienda lontana da guai legali. Ad esempio, se elimini per sbaglio un utente, vengono eliminati anche la casella postale in sospeso, il sito SharePoint personale e l'account OneDrive.

I requisiti legali, i requisiti di conformità e le normative di regolamentazione variano in base a settore e Paese ma multe, sanzioni e controversie legali sono tre cose per cui non c'è spazio nella lista delle cose da fare.

N. 6
Gestione di distribuzioni e migrazioni di e-mail ibride a Office 365

Le organizzazioni che adottano Office 365 normalmente hanno bisogno di una finestra temporale come transizione tra Exchange on-premises e Office 365 Exchange Online. Alcuni hanno persino lasciato attiva una piccola parte del sistema legacy per avere ulteriore flessibilità e controllo. Queste implementazioni di email ibride sono comuni, ma pongono ulteriori sfide in termini di gestione.

La corretta soluzione di backup di Office 365 dovrebbe essere in grado di gestire implementazioni di email ibride e trattare allo stesso modo i dati di Exchange, rendendo ininfluente la posizione di origine.

Conclusioni

Ti invitiamo ad approfondire la questione. Individuerai lacune della sicurezza di cui magari non ti sei accorto prima.

Hai già preso una decisione aziendale intelligente implementando Microsoft Office 365, ora trova una soluzione di backup che ti offra l'accesso e il controllo completo dei dati di Office 365 e ti consenta di evitare i rischi non necessari della perdita di dati.

Scopri di più sul backup di Office 365 su:
https://www.veeam.com/it/backup-microsoft-office-365.html


VEEAM