7 motivi critici per eseguire il backup di Microsoft 365

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

Introduzione

Hai il controllo dei dati di Microsoft 365? Hai accesso a tutto ciò che ti serve? Normalmente, la reazione istintiva è "certo che ce l'ho" oppure "Microsoft pensa a tutto". Ma se ci pensate bene, ne siete sicuri?

Microsoft si occupa di un bel po' di cose. Offre un ottimo servizio ai suoi clienti, gestendo l'infrastruttura di Microsoft 365 e mantenendo l'uptime per i tuoi utenti. Ma, dall'altro canto, stanno affidando a TE la responsabilità dei tuoi dati. È opinione comune che Microsoft esegua il backup dei dati per conto dell'utente per impostazione predefinita, ma un backup completo dei dati non è incluso nella licenza standard di Microsoft 365. Senza un cambiamento di mentalità, potrebbero esserci ripercussioni dannose quando questa responsabilità viene lasciata incustodita.

In fondo, devi assicurarti di avere l'accesso e il controllo sui dati di Exchange Online, SharePoint Online, OneDrive for Business e Microsoft Teams. Inoltre, anche se non si vuole gestire l'infrastruttura di backup, esistono servizi di backup che vengono implementati velocemente senza alcuna gestione o manutenzione manuale continua. Pensa all'accesso istantaneo alla protezione dei dati personalizzabile, al ripristino velocissimo e alla sicurezza di avere sempre il controllo. Ora pensa a cosa stai rischiando non avendoli.

Questo report esplora i pericoli legati a non avere un piano di backup di Microsoft 365 nel tuo arsenale. Discuteremo di come le soluzioni di backup per Microsoft 365, in particolare i servizi di backup basati sul cloud, colmino le lacune della retention a lungo termine e della protezione dei dati e siano davvero fondamentali per le moderne organizzazioni.

> "Sun Chemical è un'azienda realmente globale: ogni giorno i dipendenti sparsi in tutto il mondo si affidano alle app Microsoft 365 per scambiare dati critici. Veeam Data Cloud for Microsoft 365 protegge questa parte fondamentale del nostro ambiente, aiutando i nostri dipendenti a lavorare in modo più produttivo e offrendoci un ulteriore livello di resilienza informatica."
>
> **Stuart Hudson**
> Manager Senior dell'Infrastruttura IT Globale
> Programmi infrastrutturali strategici - AP,
> Sun Chemical

Il grande malinteso di Microsoft 365

Il malinteso si colloca tra la responsabilità percepita di Microsoft e l'effettiva responsabilità dell'utente riguardo alla protezione e retention a lungo termine dei dati di Microsoft 365. La resilienza e la retention fornite da Microsoft nella licenza standard di Microsoft 365 e ciò che gli utenti pensano di ottenere sono spesso diverse. Ciò significa che, a parte le normali precauzioni predisposte in Microsoft 365, potrebbe essere necessario rivalutare il livello di controllo dei dati e il livello di accesso di cui si dispone veramente.

Microsoft 365 offre la geo-ridondanza, che spesso viene confusa con il backup. La geo-ridondanza protegge da un guasto del sito o dell'hardware, in modo tale che se si verifica un guasto o un'indisponibilità dell'infrastruttura, gli utenti rimarranno produttivi e spesso non si renderanno neppure conto di questi problemi. I backup, d'altro canto, hanno luogo quando viene effettuata una copia storica dei dati che viene quindi archiviata in un'altra posizione, separata dall'ambiente di produzione. Ciò garantisce che esista una copia dei dati indipendentemente da ciò che accade all'interno di Microsoft 365 e che l'opzione di ripristino sia sempre disponibile.

I backup, oltre alla ridondanza geografica, sono l'ultima linea di difesa di un'organizzazione, ma altrettanto importante è assicurarsi di avere accesso diretto e controllo su di essi. Quando i dati vengono persi, cancellati accidentalmente o subiscono un attacco informatico, devi essere certo di poterli ripristinare rapidamente.

"Per tutti i tipi di implementazione cloud, sei il proprietario dei tuoi dati e delle tue identità."

Fonte: https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

7 motivi per cui un piano di backup di Microsoft 365 è essenziale

Microsoft 365 è una piattaforma Software as a Service (SaaS) robusta ed estremamente funzionale, oltre a rispondere perfettamente alle esigenze di molte organizzazioni. Microsoft 365 fornisce la disponibilità e l'uptime delle applicazioni per garantire che i tuoi utenti non si perdano mai nulla. Tuttavia, una soluzione di backup completa può proteggerti da molte altre minacce alla sicurezza, offrendo tranquillità e una robusta protezione dei dati.

Tu o il tuo capo potreste pensare che "Il cestino potrebbe bastare". Ed è proprio qui che molte persone sbagliano. Il periodo di tempo che passa dalla compromissione dei dati alla scoperta di questo fatto è di circa 140 giorni, un divario incredibilmente grande. È molto probabile che non ci si accorga che qualcosa è mancante o perso di finché non è troppo tardi per recuperarlo dal cestino, e questo non è certo il problema più urgente.

Fonte: https://info.microsoft.com/rs/157-GQE-382/images/EN-GB-CNTNT-eBook-Security-HolisticVision.pdf

Abbiamo parlato con centinaia di professionisti IT che, in tutto il mondo, sono passati a Microsoft 365, e dalle loro osservazioni sono emerse sette vulnerabilità nella protezione dei dati:

1. Cancellazione accidentale

2. Lacune e confusione nella policy di retention

3. Minacce interne alla sicurezza

4. Minacce esterne alla sicurezza

5. Requisiti legali e di conformità

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

7. Struttura dei dati di Teams

1. Cancellazione accidentale

Supponiamo che tu elimini un utente. Intenzionalmente o non, la cancellazione viene replicata sulla rete insieme alla cancellazione dell'account e della casella di posta di OneDrive for Business. In assenza di alternative, i cestini nativi di Microsoft 365 e le cronologie delle versioni offrono una protezione limitata dalla perdita di dati, trasformando un job di backup altrimenti semplice in un grosso problema dopo che Microsoft 365 ha cancellato tali dati per sempre in modo geograficamente ridondante, o se il periodo di retention è scaduto.

Esistono due tipi di cancellazioni nella piattaforma Microsoft 365: cancellazione temporanea e cancellazione definitiva. Un esempio del primo caso è svuotare la cartella "Elementi cancellati". Viene anche definito "Cancellato definitivamente", anche se in questo caso "definitivamente" non è completamente permanente, poiché l'elemento può ancora essere trovato nella cartella "Elementi ripristinabili". Una cancellazione 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 e basta. Tuttavia, utilizzando una soluzione di backup a livello di failsafe, la perdita di dati dovuta acancellazione accidentale è impossibile.

2. Lacune e confusione nella policy di retention

Il ritmo frenetico del mondo aziendale di oggi si presta a policy in continua evoluzione, incluse policy di retention con cui è difficile tenere il passo e molto complesse da gestire. Proprio come la cancellazione definitiva e temporanea, Microsoft 365 dispone di policy di backup e retention limitate 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 delle caselle di posta, non rientra nell'ambito di una licenza standard di Microsoft 365. Nel caso di un problema catastrofico, una soluzione di backup può offrire la possibilità di tornare a un point-in-time precedente al problema, salvando la situazione. Inoltre, con una soluzione di backup su misura per Microsoft 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 sempre a tua disposizione per rendere il ripristino dei dati veloce, facile e affidabile.

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 della più completa fiducia.

Microsoft non ha modo di riconoscere la differenza tra un normale utente e un dipendente licenziato che tenta di eliminare dati aziendali critici 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 grave è la manomissione delle prove. Immagina un dipendente che elimina strategicamente e-mail o file incriminanti, tenendo questi oggetti fuori dalla portata dei reparti legale, conformità o risorse umane. Quando i dati di Microsoft 365 sono adeguatamente protetti, off-site e nel cloud, vengono aggiunti livelli di protezione per combattere queste minacce interne, garantendo che i dati rimangano sicuri e recuperabili.

4. Minacce esterne alla sicurezza

Poi, naturalmente, ci sono le minacce esterne e dannose. 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 spesso si insinuano facilmente attraverso e-mail e allegati. Non è sempre sufficiente istruire gli utenti su cosa cercare, soprattutto quando i messaggi infetti sembrano così convincenti. Le limitate funzioni di backup e ripristino di Exchange Online sono inadeguate per gestire gravi attacchi. I backup regolari, in particolare quelli gestiti off-site e nel cloud tramite un servizio di backup, garantiscono che una copia separata dei dati sia priva di infezioni e rapidamente ripristinabile, superando di gran lunga le funzionalità limitate di backup e ripristino di Exchange Online. Inoltre, le migliori soluzioni per i servizi di backup si sono integrate con Microsoft 365 Backup Storage, rendendo il ripristino rapido a causa del ransomware di grandi set di dati una realtà per le organizzazioni.

5. Requisiti legali e di conformità

A volte è necessario recuperare inaspettatamente e-mail, file o altri tipi di dati in seguito a un'azione legale. Qualcosa che non pensi mai che ti accadrà finché non succede. Microsoft 365 include alcune reti di sicurezza (blocco per contenzioso e retention), integrate nel software, ma sono ben lontane da una solida soluzione di backup e non manterranno la tua azienda al riparo da problemi legali.

Con un servizio di backup affidabile, se elimini accidentalmente e-mail o documenti prima di implementare un blocco legale, sarai comunque in grado di recuperarli per assicurarti di adempiere ai tuoi obblighi legali. I requisiti legali, i requisiti di conformità e le normative di regolamentazione variano a seconda dei settori e dei Paesi, ma le multe, le sanzioni e le controversie legali sono tre cose che la tua lista di cose da fare è felice di non avere.

Meglio ancora, se non sai da dove cominciare, poiché molti di noi semplicemente non hanno la capacità o il tempo per tenere il passo con legislazioni, regolamenti e requisiti in continua evoluzione, un servizio di backup se ne occuperà per te. Con le capacità di monitoraggio e reportistica che ti aiutano a soddisfare i requisiti di conformità e normativi, e con la velocità e la facilità di cui sono capaci le implementazioni dei servizi di backup, puoi avere la tranquillità di soddisfare questi requisiti in pochi minuti.

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

Le organizzazioni che adottano Microsoft 365 in genere necessitano di una finestra transitoria tra Exchange on-premises e Microsoft 365 Exchange Online. Questa configurazion e, in cui una parte del sistema di posta elettronica rimane on-premises mentre il resto si sposta in Microsoft 365 Exchange Online, può offrire maggiore flessibilità e controllo ed è davvero comune. A sua volta, tuttavia, introduce ulteriori complessità di gestione, in particolare quando si tratta di backup. La gestione di più ambienti richiede un'attenta supervisione affinché i dati fluiscano senza intoppi e siano protetti.

È qui che il servizio di backup di Microsoft 365 diventa prezioso. Il servizio di backup Microsoft corretto gestisce in modo efficiente le implementazioni di email ibride, trattando allo stesso modo i dati di Exchange provenienti dai sistemi on-premises e Microsoft 365. In questo modo, la posizione di origine è irrilevante, semplifica il processo di backup ed elimina la necessità di gestire diversi sistemi separati.

7. Struttura dei dati di Teams

Ora più che mai, le persone utilizzano Teams per collaborazioni, progetti e iniziative speciali, il tutto a un ritmo sempre più rapido. Ma una volta completato un progetto, è importante conservarne una copia per esigenze a lungo termine come richieste legali e di conformità. È proprio qui che le organizzazioni spesso incontrano problemi. Più spesso di quanto si vorrebbe, questi Teams vengono erroneamente cancellati o la retention non viene applicata correttamente, rendendo così indisponibili file e documenti essenziali.

Con un servizio di backup di Microsoft 365, questo non accada mai. I tuoi dati sono sempre a disposizione, indipendentemente da chi o cosa li cancella. Può essere utile anche in scenari a breve termine. Ad esempio, se un dipendente dice qualcosa di inappropriato in una conversazione su Teams e poi cancella il messaggio, è facile accedere ai backup. I dati di Teams sono sempre a pochi clic dal ripristino e disponibili per le risorse umane ai fini della revisione.

La fiducia nei propri backup è fondamentale più di ogni altra cosa. Sapere che esistono e sono adeguatamente protetti protegge dall'ignoto, ma offre anche una serie di modi per ripristinare Teams o i canali mancanti o cancellati accidentalmente. L'adozione di un servizio di backup appositamente creato per Microsoft Teams garantisce che i dati siano sempre disponibili, in qualsiasi momento o circostanza.

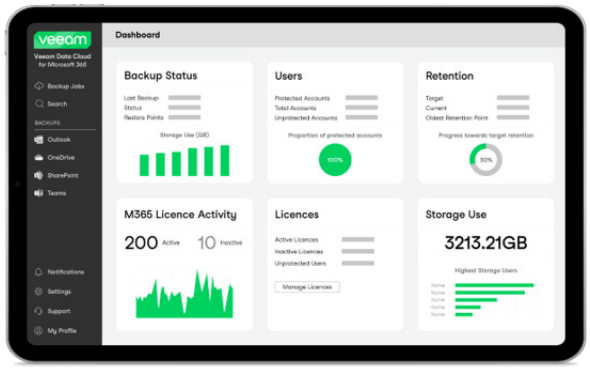
Conclusione

Prenditi un momento per valutare la tua attuale strategia di sicurezza. Potrebbero esserci delle lacune di cui non ti sei reso conto. Hai già preso una decisione intelligente implementando Microsoft 365. Ora abbinalo a un servizio di backup che ti garantisca un accesso completo e il controllo totale sui dati, evitando così i rischi inutili di perdita dei dati.

Non è più necessario investire il tempo, il denaro e le risorse associati a una soluzione software. Con **Veeam Data Cloud *for Microsoft 365***, è possibile usufruire di un unico servizio con storage illimitato incluso e scegliere tra uno dei tre piani per soddisfare gli obiettivi di backup e disaster recovery. Sia che ti serva velocità e scalabilità, controllo e flessibilità del backup e del ripristino, o di una combinazione di entrambi, Veeam ha collaborato con Microsoft per garantire che i tuoi dati siano sempre protetti, ripristinabili e scalabili in base alle esigenze della sua azienda.

Se hai trovato utile questo report, ti invitiamo a inviarlo a un collega:
Inoltra questo report.

Veeam Data Cloud *for Microsoft 365*:
La protezione dei dati resiliente resa semplice



- Tecnologia di backup di Microsoft 365 affidabile e leader di settore
- Servizio di backup all-inclusive con storage illimitato
- Basato su Microsoft 365 Backup Storage

→ Richiedi una demo

→ Contattaci