Cove Data Protection™ from N-ABLE

Otto ragioni per sottoporre a backup i dati di Microsoft 365

E-book

Otto ragioni per sottoporre a backup i dati di Microsoft 365

Le aziende si stanno affidando sempre più frequentemente ai servizi cloud, che eliminano alcune complessità poiché la manutenzione di back-end passa nelle mani del fornitore. In più, adottando l'approccio software as a service (SaaS) per i sistemi critici è possibile ridurre i costi rispetto all'acquisto di hardware on-premise.

Uno dei fornitori leader in questo ambito è Microsoft®, che offre la soluzione basata su cloud Microsoft 365™ (precedentemente Office 365®) a cui si affida un numero sempre maggiore di aziende. Microsoft 365 comprende una suite completa di strumenti per la posta elettronica, lo storage dei dati e la produttività, tra le altre cose.

Tuttavia, quando si tratta di conservare e recuperare i dati di Microsoft 365, può essere conveniente prendere in considerazione il backup.

Il rischio è reale. Secondo una ricerca, oltre il 30% delle aziende ha persoi dati memorizzati nella applicazioni SaaS.[1]

Gli MSP rappresentano consulenti di fiducia per i clienti, i quali si affidano a questi professionisti per restare produttivi e prendere decisioni IT strategiche per l'impresa. Ne risulta che gli MSP debbano adottare misure aggiuntive opportune per proteggere i dati dei propri clienti. Chi vorrebbe trovarsi nella condizione di dover spiegare ai clienti che i loro dati non possono più essere recuperati?

Considerando questi aspetti, affiancare alle istanze di Microsoft 365 dei clienti una soluzione aggiuntiva per il backup e la protezione dei dati è essenziale. Il presente e-book illustra otto ragioni per cui è fondamentale farlo. Comprenderle può aiutarti a identificare eventuali falle nella tua attuale offerta e a rafforzare le presentazioni commerciali, così sarà più facile dimostrare il valore del servizio e convertire i potenziali interessati in clienti a lungo termine.

---

[1] "The Hidden Dangers of Your Cloud Data", Jacksonville Business Journals, bizjournals.com/jacksonville/news/2021/06/01/the-hidden- dangers-of-your-cloud-data.html (consultato ad agosto 2021).

[2] "An Alarming 85% of Organizations Using Microsoft 365 Have Suffered Email Data Breaches Research by Egress Reveals", Business Wire, businesswire.com/news/home/20210511005132/en/An-Alarming-85-of-Organizations-Using-Microsoft-365-Have-Suffered-Email- Data-Breaches-Research-by-Egress-Reveals (consultato ad agosto 2021).

[3] "2021 Cost of a Data Breach Report", IBM and Ponemon Institute, ibm.com/security/data-breach (consultato ad agosto 2021).

Perché sottoporre a backup i dati di Microsoft 365? Perché Microsoft 365 non è una soluzione sufficiente?

Eliminazione accidentale

Succede. Basta un clic per eliminare accidentalmente una cartella contenente documenti critici. Magari l'autore dell'eliminazione non ha realizzato che i contenuti presenti in quella cartella fossero condivisi con altri, oppure potrebbe essere presente una nidificazione di cartelle. Inoltre, può accadere di eliminare e-mail meno recenti senza pensare che informazioni ricevute mesi o anni prima potrebbero ancora essere necessarie.

Inoltre, nella versione Business Standard il cestino viene svuotato per impostazione predefinita ogni 14 giorni, anche se l'amministratore può estendere questo termine a 30 giorni. Se le informazioni vengono eliminate e non ripristinate rapidamente, potrebbero diventare irrecuperabili. Disporre, quindi, di un backup aggiuntivo consente di evitare questi problemi che potrebbero danneggiare in modo significativo i vostri clienti.

Lacune riguardo alla conservazione

Microsoft conserva i dati della posta elettronica fino a che l'utente rimane attivo, ma siamo onesti: nessuno vuole continuare a pagare un abbonamento dopo che un dipendente è andato via. Questo potrebbe comportare la perdita di informazioni importanti o della proprietà intellettuale archiviata nella posta elettronica.

Naturalmente è sempre possibile condividere le caselle di posta prima che il dipendente vada via, ma si tratta di una misura piuttosto complicata che presuppone che si comunichi che il dipendente andrà via ed è soggetta a errori. Perché rischiare? Cove Data Protection conserva i dati di Microsoft 365 Exchange per un massimo di sette anni, così non dovrai più preoccuparti di perdere informazioni importanti quando un dipendente lascia l'azienda.

Minacce interne

Tutti noi vorremmo assumere dipendenti mossi dalle migliori intenzioni, e nella maggior parte dei casi è così. In alcune circostanze, tuttavia, anche i dipendenti modello possono incattivirsi, ad esempio dopo aver ricevuto un feedback negativo dal capo, e cancellare dati critici per vendicarsi. Se succede e questi dipendenti aspettano di comunicarlo fino allo scadere del periodo di conservazione di 14 o 30 giorni (qualora l'azienda abbia scelto la versione Business Standard), quei dati andranno persi per sempre.

Il sabotaggio è una pratica piuttosto rara, ma è un rischio di cui bisogna tenere conto. Con una soluzione di backup secondaria, eviterai che questo rischio diventi realtà.

Minacce esterne

Naturalmente, i dipendenti con intenzioni malevole non rappresentano l'unica minaccia: anche quelle provenienti dall'esterno sono piuttosto comuni. In particolare, impostare password poco complesse può essere pericoloso e c'è inoltre il rischio che gli utenti finali riutilizzino la stessa password per diversi account. Se utilizzano credenziali già violate in precedenza, i criminali informatici potrebbero trovare una corrispondenza e violare anche l'account Microsoft 365 di un dipendente e rubare o eliminare dati importanti.

C'è anche la possibilità che venga diffuso un keylogger in grado di intercettare e catturare segretamente tutto ciò che viene digitato sulla tastiera, tra cui nomi utente e password. In ogni caso, le password possono rappresentare il punto debole che consente ai malintenzionati di accedere agli account Microsoft 365.

Le app basate su cloud come Microsoft 365 sono obiettivi a elevato valore per i criminali informatici. Trovare il modo per violare gli account utente o per tormentare i malcapitati può essere un obiettivo molto redditizio per gli hacker. Che sia tramite attacchi di phishing finalizzati a diffondere malware o mediante la violazione degli account con il furto o l'hacking delle credenziali, i criminali informatici stanno prendendo sempre più di mira gli utenti dei servizi cloud. Per questa ragione, disporre di una robusta soluzione di backup è cruciale per proteggere i dati degli utenti.

Ragioni legali e legate alla conformità

Come probabilmente saprai, molte normative circa la conformità impongono regole riguardo ai tempi di conservazione dei dati. Ad esempio, le aziende del settore sanitario potrebbero dover rispettare specifici requisiti di conservazione dati. Senza una soluzione di backup potresti involontariamente violare tali politiche e non rispettare requisiti importanti.

Esperienza clienti

Come parte del proprio lavoro, gli MSP devono garantire un'esperienza di eccellenza ai propri clienti che si rivolgono ai provider di servizi gestiti per risolvere una serie di problemi IT. Per questo motivo devi rappresentare per i tuoi clienti un punto di contatto unico per qualsiasi problematica. Disponendo di un'adeguata soluzione di backup, avrai maggiore controllo sui dati in caso di incidente.

Oltre a questo, potrai offrire ai clienti una maggiore tranquillità. La perdita di dati è un evento catastrofico per le imprese, che si tratti di informazioni sui clienti, di dati finanziari o di proprietà intellettuale. Con un'opportuna soluzione di backup, sarete per i vostri clienti un vero e proprio partner aziendale, pronto a evitare la perdita dei dati e le relative conseguenze per le aziende.

Risparmi sui costi

Sono tanti i motivi per cui un'azienda potrebbe desiderare una soluzione più avanzata rispetto alla versione Business Standard di Microsoft 365, ad esempio con un maggior numero di funzionalità e applicazioni. Tuttavia un'altra priorità per le imprese è risparmiare sui costi! Se i tuoi clienti hanno a disposizione un budget ridotto, aggiungendo Cove Data Protection, potrai offrire loro una maggiore protezione dei dati e tempi di conservazione più lunghi per i dati di Microsoft 365.

Suggerimento di Microsoft®

Molti clienti danno per scontato che sia già presente un servizio di backup per i dati di Microsoft 365, ma è proprio Microsoft a dichiarare esplicitamente di non essere responsabile della perdita dei dati dei clienti; l'azienda, infatti, nel proprio contratto di servizi, consiglia ai clienti di sottoporre regolarmente a backup contenuti e dati o di archiviarli utilizzando app e servizi di terze parti. Sezione 6. Contratto di servizi Microsoft

Perché affidarsi a Cove per proteggere Microsoft 365?

Per gli MSP l'erogazione di una protezione sicura, affidabile e scalabile dei dati degli ambienti Microsoft 365 dei clienti è essenziale. Con Cove Data Protection fornire questo servizio è semplicissimo.

Cove sottopone a backup posta, contatti e calendari di Microsoft 365 Exchange®, oltre ai dati di OneDrive®, SharePoint® e Teams®, dalla stessa dashboard basata su web utilizzata per proteggere server, workstation e documenti aziendali critici. Questo approccio semplificato migliora l'efficienza, semplifica la gestione e contribuisce a erogare un servizio affidabile ai clienti.

Grazie al controllo flessibile e granulare, puoi scegliere quali account e caselle di posta Microsoft 365 proteggere, così la copertura di sicurezza è personalizzabile in base alle esigenze dei singoli clienti.

Inizia a proteggere i dati di Microsoft 365 dei tuoi clienti con Cove oggi stesso.

Scopri di più

N-able fornisce materiali di vendita personalizzabili e brandizzabili sulla piattaforma MarketBuilder, concepita per aiutare gli MSP a dimostrare il valore della protezione dei dati e a favorire il coinvolgimento dei clienti.

Scopri MarketBuilder https://www.n-able.com/it/partner-success/marketbuilder per accedere a risorse pronte all'uso.

Cove
Data Protection™
from N-ABLE

Protezione dei dati basata su cloud come servizio

Cove Data Protection™ ti mette al riparo dalle complessità del backup, da eventuali carenze di personale e dalle incertezze sul ripristino in modi in cui altre soluzioni non riescono a fare.

n-able.com/it/products/cove-data-protection

Il presente documento viene fornito per puro scopo informativo e i suoi contenuti non vanno considerati come una consulenza legale. N-able non rilascia alcuna garanzia, esplicita o implicita, né si assume alcuna responsabilità legale per le informazioni qui contenute, per l'accuratezza, la completezza o l'utilità dei dati qui inclusi.

I marchi registrati, i marchi di servizio e i loghi di N-able sono di esclusiva proprietà di N-able Solutions ULC e N-able Technologies Ltd. Tutti gli altri marchi registrati sono di proprietà dei rispettivi titolari.

© 2025 N-able Solutions ULC e N-able Technologies Ltd. Tutti i diritti riservati.