Acronis

WHITE PAPER

Sei lacune che mettono a rischio la protezione dei dati di Microsoft Office 365 e come colmarle

PROVA SUBITO

Scopri il backup dei dati di livello enterprise di Office 365 con **Acronis**

MICROSOFT OFFICE 365 E LE POTENZIALI PERDITE DI DATI: UN PERICOLO INCOMBENTE

In azienda, Microsoft Office 365 consente l'accesso affidabile alle applicazioni e un'operatività dei servizi molto elevata. Molti professionisti tuttavia lavorano in un'ottica pericolosamente errata, ritenendo che Microsoft offra una protezione dei dati di Office 365 completa e la conservazione degli stessi a lungo termine.

In realtà email, allegati e file condivisi archiviati in Office 365 non sono protetti dalle cause più comuni e gravi di perdita dei dati, che vanno dalle semplici eliminazioni involontarie agli attacchi malware più complessi.

Office 365 presenta importanti lacune nella protezione, con potenziali rischi incombenti. Le aziende potrebbero scoprire troppo tardi che Microsoft fornisce solo funzionalità limitate per il ripristino dei dati di Office 365 perduti, distrutti o danneggiati, e che non dispone né delle funzionalità né dell'affidabilità delle soluzioni di backup con le quali molte attività proteggono le proprie applicazioni critiche.

> Questo white paper spiega alcune delle limitazioni spesso non note delle capacità di protezione dei dati di Microsoft e offre indicazioni su come porre rimedio a queste carenze per garantire un ripristino rapido nel caso in cui si concretizzino le potenziali perdite di dati a cui Office 365 è soggetto.

SEI PUNTI DEBOLI NELLA PROTEZIONE DEI DATI DI OFFICE 365

Microsoft ha investito in modo significativo in hardware, software, reti, sicurezza e operatività dei propri data center, per garantire a Office 365 elevati livelli di prestazioni, accesso e disponibilità del servizio.

Il sistema è in grado di rilevare e correggere in tempi rapidi molti errori operativi, interruzioni dei siti, guasti hardware e problemi di rete, per rispettare gli accordi sui livelli di servizio incentrati sui tempi di attività delle applicazioni. Queste misure tuttavia non proteggono le aziende dalle perdite di dati comuni a cui è soggetto Office 365, ad esempio un messaggio email cancellato inavvertitamente, un file di OneDrive for Business spostato in una cartella sbagliata o una raccolta di contenuti di SharePoint Online danneggiata da un attacco malware.

> Per la maggior parte dei dati di Office 365, Microsoft offre capacità di ripristino limitate; inoltre, conserva i file solo per brevi periodi - da poche settimane a pochi mesi a seconda dell'applicazione e del contratto - e può accadere che i dati presenti nell'archivio di un ex dipendente o un progetto fermo da tempo diventino nuovamente necessari, per poi rendersi conto che Microsoft non ne ha conservato alcuna copia che sia possibile individuare e recuperare.

ELIMINAZIONE INVOLONTARIA	MINACCE ALLA SICUREZZA INTERNE
MIGRAZIONE DALLA VERSIONE LOCALE DI MICROSOFT OFFICE	PROBLEMI RELATIVI AI CRITERI DI CONSERVAZIONE
MINACCE ALLA SICUREZZA ESTERNE	QUESTIONI LEGALI E DI CONFORMITÀ

LE SEI CARENZE CHIAVE NELLA PROTEZIONE DEI DATI DI MICROSOFT DI CUI DEVONO OCCUPARSI GLI AMMINISTRATORI DI OFFICE 365

1. Eliminazione involontaria

DATI A RISCHIO. Durante le attività di routine, gli amministratori IT e i dipendenti eliminano profili utente di Office 365, email, allegati e file di Exchange Online, file di OneDrive for Business e contenuti di SharePoint Online. Può trattarsi di cancellazioni accidentali oppure intenzionali, che potrebbero poi rivelarsi errate: chi non ha avuto all'improvviso bisogno di quell'email eliminata proprio ieri?

PUNTO DEBOLE DI MICROSOFT. L'eliminazione della risorse viene replicata sulla rete. L'età della risorsa aggrava il problema: i dati più obsoleti possono essere stati eliminati definitivamente e ormai irrecuperabili. La cancellazione delle risorse più recenti può implicare meno problemi, poiché file e email eliminati temporaneamente sono ancora recuperabili, nel breve termine, dal Cestino o dalla cartella Elementi ripristinabili.

2. Problemi relativi ai criteri di conservazione

DATI A RISCHIO. La modifica o il mancato allineamento delle priorità dei criteri di conservazione dei dati di Office 365 possono determinare l'eliminazione definitiva dei dati. L'evento può essere parzialmente limitato solo con la revisione e l'aggiornamento periodico dei criteri di conservazione.

PUNTO DEBOLE DI MICROSOFT. Agli utenti di Office 365 spetta l'onere di gestire i criteri di conservazione dei dati, ma se per qualsiasi ragione la cancellazione definitiva è determinata dalla scadenza di un criterio esistente, Microsoft non offre alcuna possibilità di ripristinare la risorsa eliminata.

3. Minacce alla sicurezza interne

DATI A RISCHIO. Oltre che dalle cancellazioni di routine e involontarie, le risorse di Microsoft Office 365 devono essere protette da modifiche o eliminazioni intenzionali e dannose perpetrate da dipendenti, collaboratori occasionali o partner insoddisfatti o con i quali la collaborazione è stata interrotta.

PUNTO DEBOLE DI MICROSOFT. Ad eccezione delle eliminazioni relativamente recenti di risorse relativamente nuove, Microsoft non offre protezione contro le modifiche o le cancellazioni volontarie dei dati di Office 365 determinate da persone interne all'azienda.

4. Minacce alla sicurezza esterne

DATI A RISCHIO. I dati di Microsoft Office 365 sono vulnerabili ad attività di modifica o distruzione causate da varie minacce malware, in primo luogo dal ransomware, che crittografa i dati degli utenti e li tiene in ostaggio fino al pagamento di un riscatto in denaro. Questo tipo di attacco è in genere perpetrato da hacker, criminali informatici o altri aggressori istituzionali.

PUNTO DEBOLE DI MICROSOFT. Microsoft offre una protezione davvero limitata contro gli attacchi malware come il ransomware, e capacità minime di ripristinare i file alterati o crittografati allo stato precedente all'attacco.

5. Migrazione dalla versione locale di Microsoft Office

DATI A RISCHIO. La migrazione dalla classica suite di applicazioni Microsoft Office in locale ai servizi di Office 365 basati su cloud prevede in genere il passaggio da una soluzione di protezione dei dati esistente a una predisposta al cloud. Spesso tuttavia le due soluzioni di backup non sono compatibili e ciò rende impossibile il ripristino dei dati legacy nel nuovo ambiente.

PUNTO DEBOLE DI MICROSOFT. Microsoft non offre alcuna soluzione per i problemi correlati alla perdita dei dati durante la migrazione dalla versione di Office locale a Office 365. Sono poche anche le soluzioni di protezione di terze parti che integrano funzionalità di backup sia per Office sia per Office 365: in genere, eseguono l'uno o l'altro ma non entrambi.

6. Questioni legali e di conformità

DATI A RISCHIO. I costi aziendali correlati alle perdite di dati non protetti elencate fin qui sono aggravati dai requisiti legali e di conformità normativa, ad esempio il regolamento GDPR dell'Unione Europea. Una perdita irrecuperabile dei dati di Office 365 può esporre l'attività a sanzioni specifiche di settore, amministrative o penali, ad esempio azioni legali per danni o perdite causati dal mancato rispetto dei requisiti in materia di e-discovery o prove, perdite di profitto e azionarie, perdita della fiducia dei clienti e danni alla reputazione del marchio.

PUNTO DEBOLE DI MICROSOFT. Considerati tutti i rischi associati alla perdita dei dati fin qui elencati, è poco quel che Microsoft può fare per proteggere le organizzazioni che hanno adottato Office 365 contro i numerosi rischi legali e di conformità a cui sono esposte. Dopo un attacco ransomware, ad esempio, un'azienda che archivia i dati personali dei propri clienti UE in SharePoint Online potrebbe non essere più in grado di inviare le copie di tali dati su richiesta, violando quindi i requisiti del regolamento GDPR.

COSA FARE?

Dopo aver compreso i tanti punti deboli nella capacità di Microsoft di proteggere i dati di Office 365, è bene iniziare a individuare soluzioni di protezione in grado di colmare queste carenze. È chiaro come la posta in gioco sia alta: l'incapacità di evitare una perdita di dati può causare perdite finanziarie importanti.

BACKUP COMPLETO E GRANULARE PER OFFICE 365, CON FUNZIONALITÀ DI RICERCA AVANZATE

Acronis Backup protegge i dati di Office 365 con un backup diretto e senza agente dalla maggior parte dei data center Microsoft alla rete globale di data center Acronis. Le numerose funzionalità avanzate facilitano la ricerca e il recupero delle risorse di Office 365 in Microsoft Exchange Online, OneDrive for Business e SharePoint Online, con un elevato livello di granularità. Il modello di licenza non implica investimenti iniziali né costi di manutenzione periodici. La Tabella 1 illustra la gamma di funzionalità e la flessibilità di Acronis Backup per Office 365:

FUNZIONALITÀ DI ACRONIS BACKUP PER OFFICE 365	EXCHANGE ONLINE	ONEDRIVE FOR BUSINESS	SHAREPOINT ONLINE
Dati sottoposti a backup	Email, caselle di posta archiviate, calendari, contatti, attività	File e cartelle	Siti, siti secondari, raccolte di documenti, elenchi, raccolte di pagine
Ripristino granulare point-in-time	Sì	Sì	Sì
Ricerca nel backup	Ricerca di elementi nelle caselle di posta	Ricerca di file	Ricerca di elementi del sito
Ripristino tra più utenti e più organizzazioni	Sì	Sì	Sì
Ripristino sulla cartella personalizzata tramite l'analisi in tempo reale	Sì	Sì	–
Anteprima contenuto email	Sì	–	–
Download dal backup	Sì, per allegati	Sì, per file	Sì, per file
Invio di email dal backup	Sì	–	–
Ripristino delle autorizzazioni	–	Sì	Sì

Tabella 1. Funzionalità di Acronis Backup per Office 365

> Queste funzionalità di ricerca e ripristino altamente granulari consentono di scaricare i file richiesti direttamente dal backup, di scaricare qualsiasi versione dei documenti e non solo la più recente, di inviare email dal backup senza dover ripristinare prima i messaggi nella casella di posta di Exchange Online e, infine, di ripristinare qualsiasi elemento dati nella posizione originale o in una nuova destinazione.

PROTEZIONE DELL'INTERO AMBIENTE MICROSOFT (E NON SOLO)

Acronis Backup è un'**unica soluzione di protezione dei dati per l'intero ambiente Microsoft**, ovunque si trovino i carichi di lavoro: in locale, in hosting su cloud pubblici o privati e/o in hosting presso Microsoft.

Protegge inoltre le **macchine virtuali Microsoft eseguite su Hyper-V** e i server, i desktop e i dispositivi mobile Windows. La protezione si estende a un'**ampia gamma di piattaforme non Microsoft**, compresi ambienti fisici, virtuali e cloud, server che eseguono altri diffusi sistemi operativi e hypervisor, numerosi database, sistemi operativi desktop come macOS e sistemi operativi mobile come iOS e Android.

Un'unica piattaforma per la protezione dei dati per l'intero ambiente IT elimina l'incompatibilità reciproca delle soluzioni di backup predisposte solo per il locale o solo per il cloud, e contribuisce altresì a ridurre i costi di licenza, formazione e integrazione. Nella Figura 1 sono elencate le oltre 20 piattaforme protette da **Acronis Backup.**

Inoltre, la soluzione è dotata di un'intuitiva interfaccia utente, che ne consente l'impiego immediato anche ai non esperti; contribuisce alla riduzione dei costi operativi quotidiani, migliora il livello dei servizi erogati e permette di concentrare l'attenzione sui progetti aziendali strategici.

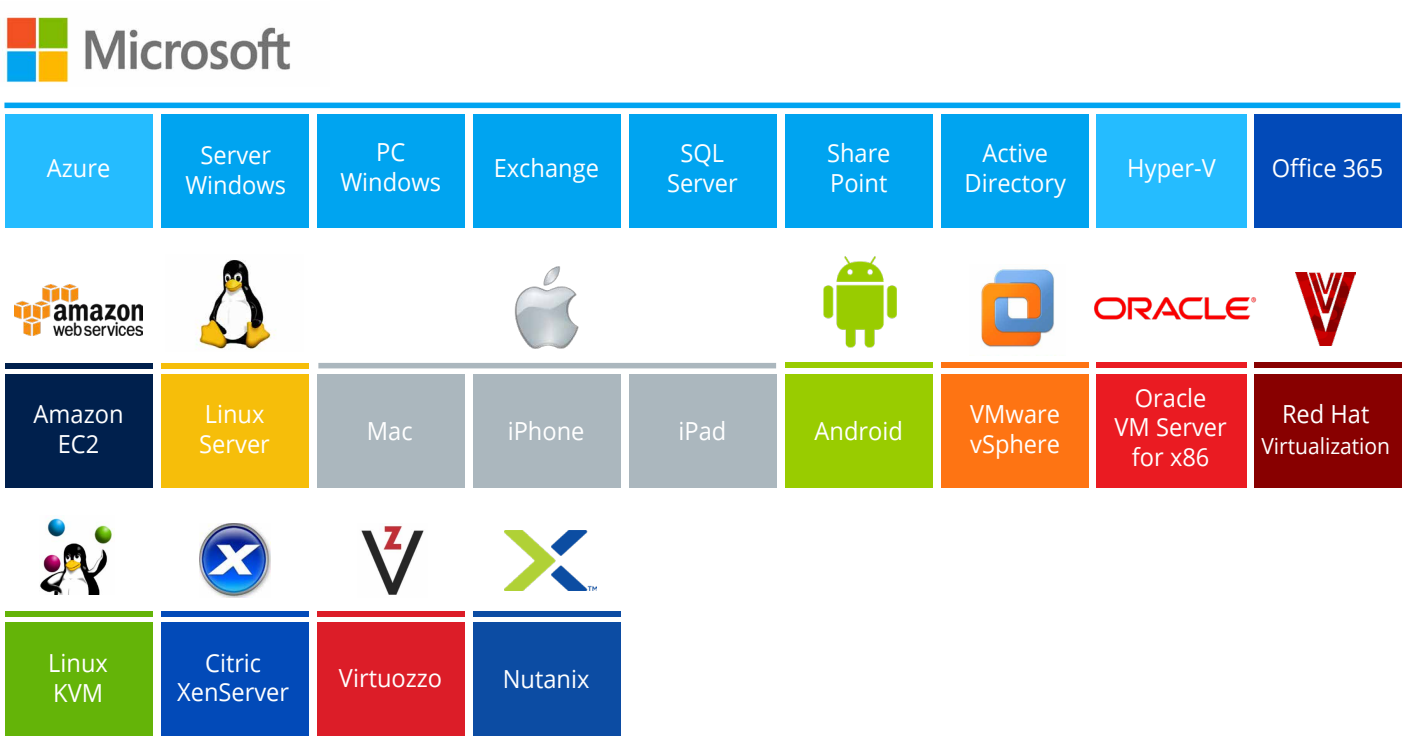

Figura 1. Piattaforme protette da Acronis Backup

IL BACKUP SEMPLICE, EFFICIENTE E SENZA AGENTE

L'agente di backup di **Acronis Backup per Microsoft Office 365** è un componente eseguito nel cloud protetto Acronis e non in locale nella sede dell'utente, con conseguenti procedure di configurazione e manutenzione ottimizzate e semplificate.

BACKUP DEI DATI DI OFFICE 365 NEL CLOUD ACRONIS AD ELEVATA SICUREZZA

Acronis esegue il backup dei dati di Office 365 **dai dati center Microsoft direttamente in Acronis Cloud**, una rete globale di data center protetti con un programma completo di sicurezza delle informazioni e di gestione della conformità, con controlli amministrativi, fisici e tecnici basati sulla valutazione continua del rischio.

Le policy e i processi per la sicurezza delle informazioni Acronis si basano su **standard riconosciuti a livello internazionale** come ISO 27001 e NIST (National Institute of Standards and Technology) e tengono in considerazione i requisiti dei quadri normativi locali correlati, come il GDPR (Regolamento generale sulla protezione dei dati) dell'Unione Europea e lo statunitense HIPAA (Health Insurance Portability and Accountability Act). Le funzionalità di sicurezza di Acronis Cloud prevedono:

- **Controllo degli accessi enterprise** basato su ID utente univoci e password complesse, protocolli di autenticazione sicura (LDAP, Kerberos, certificati SSH), autenticazione a due fattori e web application firewall.
- **Sicurezza dei dati multi-layer, basata su zone** e rafforzata da crittografia dei dati in tempo reale in transito e a riposo, trasferimento dei dati sicuro su HTTPS (TLS), crittografia AES-256 dei dati utente di livello enterprise, tecnologia Acronis CloudRAID per la massima disponibilità dei dati.
- **Sicurezza fisica garantita da alte grate**, accesso controllato da scansioni biometriche della geometria della mano e da schede di prossimità, videosorveglianza con 90 giorni di archiviazione e personale di sicurezza disponibile 24x7x365.
- **Data center ridondanti ad alta disponibilità** protetti a livello di infrastruttura con gruppi di continuità e generatori diesel di riserva, HVAC, reti e UPS ridondanti, campionamento dell'aria VESDA, sistemi antincendio sprinkler bizonali, a secco e a preazione (con tubazioni a secco), monitoraggio continuo della temperatura e dell'umidità.

Figura 2. Acronis Backup per Office 365 con distribuzione cloud

PROTEZIONE AVANZATA DELLA PRIVACY

Acronis Backup protegge la privacy dei dati da occhi indiscreti con **crittografia del backup su più livelli**, consolidata da trasferimenti dei dati sulla rete con crittografia TLS, archiviazione in data center con crittografia avanzata del disco e crittografia AES-256 di ogni singolo archivio.

PROTEZIONE AUTOMATICA DI NUOVI UTENTI, GRUPPI E SITI DI OFFICE 365

Dopo aver configurato il piano iniziale di backup e averlo abilitato per uno specifico ambiente di Office 365, il personale IT non dovrà modificarlo ogni volta che viene aggiunto un nuovo utente, gruppo o sito di Office 365. **Acronis Backup individua automaticamente** l'aggiunta di nuovi elementi e li inserisce nel piano di backup.

SUPPORTO PER L'AUTENTICAZIONE MICROSOFT

Acronis supporta l'autenticazione a più fattori di Microsoft, abilitando l'uso di misure di autenticazione quali dispositivi attendibili o impronta digitale.

STRUMENTI DI MONITORAGGIO E CREAZIONE DI REPORT ALL'AVANGUARDIA

Acronis offre **capacità avanzate di monitoraggio dello stato del backup e di creazione di report** che contribuiscono ad aumentare l'efficienza e la reattività dei team IT. Sul portale di gestione Acronis sono disponibili widget compatti e di facile impiego che presentano tutte le statistiche di backup e ripristino, oltre a report, notifiche e avvisi per eventi critici.

CONCLUSIONI

Se la vostra azienda ha adottato Office 365, dovrebbe completare la protezione dei dati di base di Microsoft con Acronis Backup, il backup più affidabile e intuitivo per le imprese di ogni dimensione.

Per saperne di più su **come Acronis Backup può significativamente migliorare,** semplificare e rendere più economica la protezione dei dati di Office 365, richiedete una versione di prova gratuita valida 30 giorni qui oppure trovate un rivenditore Acronis qui.

Acronis

Per maggiori informazioni, visitate **www.acronis.com**