10 Mosse verso la Resilienza informatica di Microsoft 365

Indice

L'aumento degli attacchi informatici su Microsoft 365

La protezione dei dati di Microsoft 365 è un aspetto essenziale di una moderna strategia di sicurezza informatica, poiché le applicazioni della suite permeano le operazioni quotidiane di innumerevoli aziende e operazioni. Con un'ampia gamma di strumenti di produttività, tra cui Exchange, Teams, SharePoint, OneDrive e altri, Microsoft 365 contiene una grande quantità di informazioni sensibili e dati aziendali critici, ed è per questo che un numero sempre maggiore di organizzazioni sta investendo in soluzioni di terze parti o servizi di backup gestiti per proteggerli.[1] In effetti, ci sono prove che il ransomware è stato progettato con lo scopo specifico di infiltrarsi in Microsoft 365 e altre applicazioni SaaS. Secondo un rapporto di Coalition, nella prima metà del 2023 c'è stato un aumento del 12% dei sinistri informatici, trainato dagli attacchi ransomware, con una richiesta media di riscatto di 1,62 milioni di dollari.[2] A causa della sua diffusione e del fatto che un numero sempre maggiore di dipendenti installa e utilizza Microsoft 365 su computer usati per lavorare da casa, la piattaforma è diventata particolarmente vulnerabile agli aggressori che sfruttano questa infrastruttura diversificata.

12%

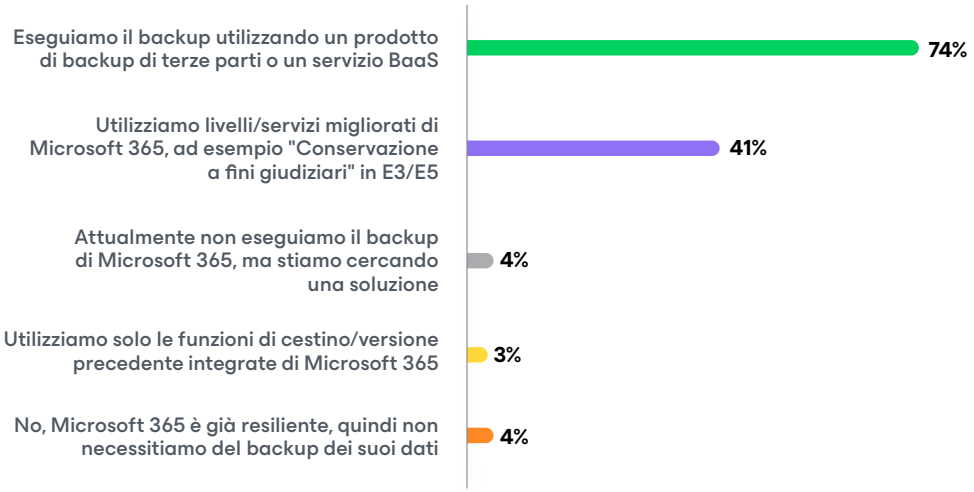
Aumento dei sinistri informatici nelprimo semestre 2023

1,62

milioni di dollari

è la richiesta di riscatto media

La tua organizzazione esegue il backup dei dati dall'interno di Microsoft 365?



[1] Report sulle tendenze nella protezione dei dati 2024

[2] Microsoft 365 ransomware: La tua guida completa alla comprensione, alla prevenzione e al ripristino

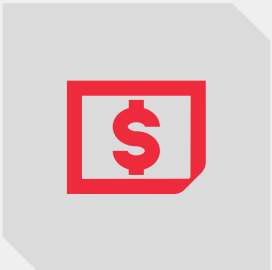
I rischi associati alla perdita dei dati di Microsoft 365 non sono quindi solo complessi, ma molto reali. La perdita di dati provoca gravi interruzioni dell'operatività e può infliggere danni finanziari significativi a causa delle interruzioni e della perdita di produttività. In un report, i responsabili del reparto IT hanno stimato il costo delle interruzioni che causano tempi di inattività è pari a 1.467 dollari al minuto (88.000 dollari all'ora)[3] il che, dato l'enorme volume di tempo dedicato e di lavoro svolto utilizzando Microsoft 365 nella tipica giornata lavorativa, è un costo che non sorprende. Inoltre, quando vengono esposti dati sensibili, le organizzazioni sono soggette a pesanti sanzioni per non conformità e danno di reputazione: in caso di violazioni del regolamento GDPR, multe fino a 21 milioni di dollari.[4] Siccome i dati di Microsoft 365 sono estremamente sensibili per le organizzazioni e i loro dipendenti, è più che probabile che gli eventi di perdita di dati erodano non solo la fiducia del cliente, ma anche quella del dipendente, portando potenzialmente a un calo del business e a un danno di reputazione a lungo termine sia all'interno che all'esterno dell'azienda.

Le possibili conseguenze dei dati di Microsoft 365 non protetti non possono essere sopravvalutate. Le violazioni che espongono delle informazioni personali possono portare a furti di identità e frodi, causando danni anche molto tempo dopo la compromissione iniziale. Per le aziende, la perdita di proprietà intellettuale può erodere i vantaggi competitivi e comportare costose battaglie legali o multe, che possono anche essere oggetto di contenziosi legali se vengono ritenute negligenti nella protezione dei dati dei propri clienti.

Non c'è modo di evitarlo. Un approccio proattivo alla protezione dei dati di Microsoft 365 è più di un'idea innovativa: è un imperativo per garantire alle aziende la continuità, sostenere le responsabilità legali e normative e mantenere la fiducia dei clienti.

[3] Report sulle tendenze della protezione dei dati 2022
[4] Quali sono le sanzioni relative al regolamento GDPR?

Costo associato alla perdita di dati



Il costo dei tempi di inattività è 1.467 dollari al minuto (88.000 dollari all'ora)

In caso di violazioni del regolamento GDPR, sanzioni fino a 21 milioni di dollari.

Le violazioni che espongono informazioni personali possono portare a furti di identità e frodi.

Passaggi per prepararsi agli attacchi

1. Autenticazione a più fattori (MFA)

L'autenticazione a più fattori (MFA) è una misura di sicurezza essenziale che richiede agli utenti di fornire due o più fattori di verifica per ottenere l'accesso alle risorse digitali, come account di posta elettronica, applicazioni aziendali e servizi online. L'MFA migliora significativamente la sicurezza aggiungendo livelli di protezione oltre una semplice password, ciò significa che anche se un criminale informatico ottiene la password di un utente, deve comunque aggirare i fattori di autenticazione aggiuntivi per ottenere l'accesso. Questa è a dir poco una formidabile barriera contro l'ingresso non autorizzato.

I vantaggi dell'MFA sono molteplici, soprattutto nel contesto di Microsoft 365, dove i dati sensibili e le comunicazioni aziendali sono perpetui. L'MFA può difendere dalle conseguenze di attacchi informatici comuni come il phishing, in cui gli aggressori ingannano gli utenti inducendoli a rivelare le credenziali. Questo passaggio di autenticazione aggiuntivo può essere qualcosa che l'utente conosce (come un PIN o una domanda di sicurezza) o qualcosa che l'utente ha (come uno smartphone o l'hardware dell'azienda).

Anche negli scenari in cui le password vengono compromesse a causa di password deboli o riutilizzate, una configurazione MFA continuerà a proteggere l'account da accessi non autorizzati. Questo livello di sicurezza è fondamentale negli ambienti Microsoft 365, dove l'accesso in remoto è di routine e gli utenti possono connettersi da reti non protette o dispositivi personali. Nel complesso, come fatto semplice e rassicurante, l'MFA crea un meccanismo di difesa dinamico che si adatta al panorama delle minacce in evoluzione.

Vantaggi dell'MFA

Difende dalle conseguenze dei comuni attacchi informatici

Continua a proteggere l'account da accessi non autorizzati

Crea un meccanismo di difesa dinamico che si adatta al panorama delle minacce

2. Accesso con privilegi minimi

Il principio del privilegio minimo è una pietra miliare delle pratiche di sicurezza informatica efficaci, integralmente correlato al concetto di architettura Zero Trust, ed è fondamentale per rafforzare un'organizzazione contro potenziali attacchi informatici. Un architettura Zero Trust parte dal presupposto che esistano minacce sia all'esterno che all'interno della rete, per cui nessun utente o sistema è automaticamente considerato affidabile.[5] Questo principio è in linea con il principio del minimo privilegio, secondo il quale agli utenti devono essere concessi i livelli minimi di accesso (o autorizzazioni) necessari per svolgere le loro mansioni lavorative, e non di più. Per Microsoft 365, l'implementazione di questi principi potrebbe significare limitare l'accesso a determinati documenti, cartelle, siti, impostazioni amministrative e applicazioni in base al ruolo dell'utente all'interno dell'organizzazione.

L'adozione di un modello di accesso con privilegi minimi può rafforzare notevolmente il livello di sicurezza del tuo ambiente Microsoft 365. In primo luogo, riduce al minimo la potenziale superficie di attacco della suite per i criminali informatici. Se l'account di un utente viene compromesso, l'aggressore è limitato ai diritti di accesso di quell'account, che idealmente dovrebbero essere il più restrittivi possibile. Ad esempio, se le credenziali di un utente vengono rubate, l'utente malintenzionato non sarà in grado di accedere a informazioni sensibili o eseguire attività amministrative se tali diritti non sono associati all'account dell'utente. Questa limitazione dei danni crea una zona di quarantena per eventuali violazioni della sicurezza ed è fondamentale per controllare la diffusione di unattacco all'interno diun'organizzazione.

[5] https://www.veeam.com/news/new-zero-trust-data-resilience-model-introduced-by-it-security-and-data-protection-experts.html

3. Backup regolari

Essendo un obiettivo primario per i criminali informatici, i backup sono estremamente importanti per Microsoft 365, soprattutto se si considera il Modello a responsabilità condivisa di Microsoft[6] che afferma che le organizzazioni sono responsabili della sicurezza dei loro dati. Il ransomware rappresenta una minaccia significativa per l'integrità dei dati, poiché gli aggressori mirano a crittografare i file di un'organizzazione e richiedono un pagamento per rilasciarli. Tuttavia, le minacce ai dati non si limitano agli attacchi dannosi. I dati possono anche essere compromessi da cancellazioni accidentali o vari altri incidenti. Mantenere aggiornati i backup consente all'organizzazione di riottenere rapidamente l'accesso ai propri dati, indipendentemente dal fatto che la perdita sia dovuta a ransomware, a un errore umano o a molti altri motivi critici per mantenere i backup di Microsoft 365.[7] In questo modo non solo riducono al minimo le interruzioni, ma si invia anche il forte messaggio che l'organizzazione non è un bersaglio facile per attacchi futuri.

Implementare una routine di backup regolare significa stabilire una pianificazione che trovi un equilibrio tra il volume di dati gestiti e le risorse disponibili per le operazioni di backup. Ciò dovrebbe includere il backup di e-mail, documenti, contatti, calendari e qualsiasi altro dato archiviato all'interno della suite Microsoft 365.

Pensa che è come avere una polizza assicurativa. Potrebbe non essere necessario tutti i giorni, ma quando si verifica un disastro, può fare la differenza tra un rapido ripristino e una catastrofe letale.

[6] Responsabilità condivisa nel cloud

[7] 7 motivi critici per eseguire il backup di Microsoft 365

4. Backup immutabili

L'immutabilità svolge un ruolo fondamentale nella protezione delle risorse digitali di un'organizzazione contro l'alterazione o l'eliminazione, sia a causa di minacce informatiche che di errore umano. Per Microsoft 365, in cui grandi quantità di dati vengono generate, condivise e archiviate regolarmente, garantire che le copie del backup siano impermeabili alle modifiche è un elemento critico di una solida strategia di mitigazione delle minacce. L'immutabilità garantisce che, una volta eseguito il backup, le informazioni rimangano in uno stato incontaminato e siano inalterabili per un determinato periodo di tempo.

Per le organizzazioni che utilizzano Microsoft 365, i backup immutabili rappresentano uno scudo contro gli attacchi ransomware, che prendono di mira non solo i dati operativi in tempo reale, ma anche i repository di backup. Infatti, secondo un sondaggio, quasi tutti gli attacchi ransomware (93%) prendono di mira specificamente i backup.[8] Per ulteriori misure di sicurezza, è importante una copia di backup immutabile dei dati. Creando e applicando policy di retention che proteggono i dati di backup dalla sovrascrittura o dalla manomissione, le aziende possono difendere le proprie pratiche di continuità dalla crittografia o dalla distruzione indesiderate dei dati. L'immutabilità garantisce che, nonostante eventuali violazioni sicurezza che interessano gli attuali data store, l'organizzazione possa ripristinare le operazioni da un backup pulito e inalterato.

93%

degli attacchi ransomware prende di mira specificamente i backup.

[8] Report sulle tendenze nel ransomware 2023

5. Piano di risposta agli incidenti

Un buon piano di risposta agli incidenti è un piano ben strutturato. Descrive in dettaglio i processi che un'organizzazione deve seguire quando si trova ad affrontare vari incidenti di sicurezza informatica, fungendo da manuale operativo per identificare, contenere, sradicare e ripristinare dalle minacce di sicurezza e garantire che tutti gli stakeholder siano informati e preparati ad agire.

Per le organizzazioni che utilizzano Microsoft 365, la base di un solido piano di risposta agli incidenti include l'identificazione delle risorse critiche all'interno dell'ecosistema Microsoft 365. Ciò significa individuare con precisione dove sono archiviati i dati sensibili, che si trovino in OneDrive, SharePoint, Exchange Online o altrove. Una volta identificate queste risorse, il piano dovrebbe definire le potenziali minacce e creare un elenco prioritario di rischi, insieme alle strategie per mitigarli. Ciò include l'uso di strumenti di monitoraggio e rilevamento integrati, strategie di contenimento immediato, eliminazione delle minacce, una solida comunicazione tra le parti e l'identificazione e il ripristino di eventuali dati persi o compromessi.

Il collante che tiene insieme un piano di risposta agli incidenti è una preparazione accurata. Ciò va oltre gli strumenti tecnici, la formazione e la collaborazione dei team IT e di sicurezza, ma riguarda tutti i dipendenti. Per coloro che utilizzano Microsoft 365, le organizzazioni dovrebbero condurre regolari sessioni di formazione su misura per il suo intricato ecosistema. I dipendenti che utilizzano applicazioni all'interno di Microsoft 365 come Outlook e Teams devono essere dotati delle conoscenze per discernere e reagire ad attività sospette, che possono presentarsi sotto forma di messaggi apparentemente legittimi, falsi inviti a riunioni da parte di colleghi o e-mail dall'aspetto autentico da parte dei leader dell'azienda. Le persone possono essere un punto debole per la sicurezza informatica di qualsiasi organizzazione, ma i dipendenti ben addestrati hanno il potenziale per formare una barriera formidabile contro le minacce.

Un piano di risposta agli incidenti inizia con

Comprehensive Incident Response Framework

Identificazione delle risorse critiche

Importanza della preparazione dei dipendenti

6. Audit regolari e test di penetrazione

Controlli regolari e test di penetrazione sono componenti integranti del mantenimento di un ambiente Microsoft 365 resiliente. In effetti, Microsoft 365 stesso fornisce una serie di strumenti integrati per l'auditing e il rilevamento delle minacce,[9] che fungono da base per rafforzare l'ambiente contro varie minacce alla sicurezza. Queste pratiche fungono da misure proattive, consentendo alle aziende di identificare e correggere i problemi prima che possano essere sfruttati dagli aggressori.

I controlli dell'ecosistema di Microsoft 365 comportano la revisione sistematica di vari aspetti come le autorizzazioni utente, i controlli di accesso ai dati e le impostazioni di sicurezza. Sebbene a volte sia complicato, gli audit regolari aiutano a garantire che le configurazioni del sistema rimangano allineate con le best practice e le politiche di sicurezza dell'organizzazione; è una sana abitudine da costruire e mantenere. Poiché Microsoft 365 comprende una varietà di servizi, questi controlli devono essere completi e coprire ogni servizio per evitare vulnerabilità trascurate.[10]

Spesso indicato come "hacking etico", il test di penetrazione integra gli audit regolari consentendo alle organizzazioni di valutare l'efficacia delle loro misure di sicurezza. Ciò comporta la simulazione di attacchi informatici all'infrastruttura di Microsoft 365 per identificare i punti deboli che gli aggressori del mondo reale potrebbero sfruttare. Per le organizzazioni applicabili, i test di penetrazione dovrebbero sondare tutti i livelli del loro ecosistema Microsoft 365, dalla resistenza al phishing dei dipendenti alla resilienza di strumenti tecnici come firewall, sistemi di rilevamento delle minacce e piani di risposta agli incidenti. Le informazioni raccolte da questi test guidano le organizzazioni nella messa a punto dei programmi di formazione e delle strategie di sicurezza, consentendo loro di sviluppare difese più complete ed efficaci quando si presenta inevitabilmente una minaccia informatica.

[9] Linee guida di Microsoft 365 per la sicurezza e la conformità

[10] Sicurezza nativa di Microsoft 365: Sbloccare le funzionalità di conformità e monitoraggio

7. Criteri di restrizione software

Un criterio di restrizione software (SRP) è una funzionalità di sicurezza che le organizzazioni possono utilizzare per identificare e controllare l'esecuzione del software su hardware specifico. Per le organizzazioni enterprise che utilizzano Microsoft 365, la sua implementazione può fungere da meccanismo di difesa fondamentale per proteggere i numerosi dispositivi di cui sono responsabili. Poiché Microsoft 365 contiene una serie di strumenti distinti, invita anche una serie di vettori di minaccia distinti e sfruttabili. Determinando quale software può e non puòessere eseguito su un sistema, gli SRP riducono efficacemente la superficie di attacco disponibile ai malintenzionati.

Nella creazione di un SRP per un ambiente Microsoft 365, l'obiettivo è garantire che solo le applicazioni, gli script e i processi attendibili possano essere eseguiti, inclusi i vettori di minaccia nella whitelist e nella blacklist, se necessario. Per la massima efficacia, gli SRP devono essere configurati tenendo conto dell'accesso con privilegi minimi e regolarmente aggiornati per riflettere le modifiche nel software utilizzato da un'organizzazione. Ciò include gli aggiornamenti agli strumenti di Microsoft 365, l'aggiunta di nuovo software o l'interruzione delle applicazioni legacy.

Impedendo ai malware di sfruttare le comuni tecniche di attacco, gli SRP sono estremamente efficaci nell'interrompere la catena di infezione e nel mantenere una zona di quarantena. L'integrazione degli SRP in una strategia di sicurezza informatica è un approccio lungimirante che aiuta a proteggere l'infrastruttura di un'organizzazione dall'esecuzione di software non affidabile - qualcosa che, man mano che le imprese crescono e assumono nuovi dipendenti, è una possibilità sempre crescente.

8. Monitoraggio e registrazione

Il monitoraggio e la registrazione costituiscono una fase fondamentale per garantire la sicurezza e l'integrità di qualsiasi ambiente Microsoft 365. Tenendo d'occhio le attività del sistema e mantenendo registri completi degli eventi, le organizzazioni possono rilevare potenziali incidenti di sicurezza in tempo reale, diagnosticare problemi di sistema, comprendere la portata delle violazioni e migliorare la posizione di sicurezza complessiva.

Per gli amministratori di Microsoft 365, l'importazione dei log in un sistema di Security Information and Event Management (SIEM — Gestione delle informazioni e degli eventi di sicurezza) può semplificare notevolmente questo processo. Azure Sentinel, ad esempio, è un SIEM nativo di Microsoft che utilizza una serie di connettori dati precostituiti per salvare i dati dei log di un'organizzazione direttamente all'applicazione SIEM. Questi dati vengono quindi normalizzati per ottenere set di dati coerenti e monitorati attraverso strumenti di analisi integrati.

Un monitoraggio efficace dovrebbe gettare un'ampia rete per rilevare una serie di possibili anomalie indicative di una minaccia alla sicurezza: dai tentativi di accesso falliti (che suggeriscono un attacco a forza bruta) a schemi di download insoliti (che suggeriscono un'esfiltrazione di dati indesiderata) a molti altri. Altrettanto importante è una registrazione completa, che funge da documentazione di tutte le attività monitorate. Tali registri dovrebbero acquisire dettagli sufficienti per consentire la ricostruzione degli eventi di un intero incidente, prima, durante e dopo. Questo diventa prezioso nell'analisi forense post-incidente, ma aiuta anche negli audit di conformità e nel perfezionamento delle misure di sicurezza nel tempo. La registrazione deve essere configurata con attenzione per garantire che i dati raccolti siano fruibili, fornendo informazioni chiare e pertinenti senza il rumore che può essere generato da un ambito troppo ambizioso.

Nel corso del tempo, le informazioni raccolte dal monitoraggio e dalla registrazione forniscono alle organizzazioni i dati necessari per apportare modifiche proattive alle policy e semplificare gli aggiornamenti di sicurezza.

9. Separazione dei dati

La separazione dei privilegi è una strategia ampiamente applicabile ed efficace utilizzata dalle organizzazioni per migliorare la propria infrastruttura di sicurezza ed è altamente applicabile quando si integrano servizi basati sui dati come Microsoft 365. Strategie come le architetture multi-tenant, i confini amministrativi e la limitazione condizionale degli account si concentrano sulla strutturazione dei dati e dei relativi privilegi per ridurre gli accessi non autorizzati e limitare i danni potenziali derivanti dalle violazioni della sicurezza. Tenendo separati i diversi set di dati e dividendo le reti in segmenti distinti, le organizzazioni riducono significativamente il rischio iniziale di violazioni della sicurezza e mettono in quarantena efficacemente i focolai qualora si verifichino.

L'utilizzo dei criteri di separazione dei privilegi all'interno di Microsoft 365 consente alle organizzazioni di mantenere regole di accesso rigorose. Come abbiamo detto nella sezione precedente, la migliore di queste regole garantisce che gli utenti, gli amministratori e i servizi ricevano solo le autorizzazioni necessarie per eseguire le attività necessarie e non di più, ad esempio il principio del privilegio minimo e l'accesso basato sul ruolo (RBAC).

Per le organizzazioni che operano in più giurisdizioni o che hanno unità aziendali distinte, separare i tenant di Microsoft 365 tramite un'architettura multi-tenant può aiutare a isolare i dati e controllare l'accesso. Questo si riferisce alla creazione di confini amministrativi distinti per tenant. In questo modo si isolano gli ambienti dai loro dati, account utente e controlli di accesso, garantendo che i requisiti di sicurezza e conformità vengano rispettati individualmente e che una violazione o un problema di sicurezza all'interno di un tenant non comprometta l'integrità degli altri.

All'interno di questi limiti amministrativi, i criteri di accesso condizionale e le restrizioni dell'account aggiungono un altro livello di difesa e possono essere implementati direttamente in Microsoft 365. Questi criteri consentono alle organizzazioni di definire e implementare regole basate sul contesto per un determinato account, consentendo l'ottimizzazione delle regole di sicurezza di un'organizzazione in base al livello di rischio di un account, alla posizione geografica o a irregolarità dinamiche come accessi o download sospetti.

La separazione metodica può, come tale, essere applicata a tutti i livelli della gerarchia di un'organizzazione e fornisce una solida base per proteggere i dati di Microsoft 365 e altre risorse digitali. Poiché la compartimentazione strategica non solo mitiga il rischio di accesso non autorizzato, ma fornisce anche protezioni a più livelli e ripieghi contro le violazioni della sicurezza, la separazione di dati e privilegi si è giustamente guadagnata lo status di approccio affidabile per le organizzazioni per rafforzare le loro difese informatiche, mantenere la continuità aziendale e, in definitiva, fare passi avanti verso il raggiungimento di resilienza informatica all'interno del proprio ambiente Microsoft 365.

10. Crittografia

La crittografia è una misura di sicurezza fondamentale che funge da linea di difesa primaria nella protezione delle informazioni sensibili, garantendo che solo le parti autorizzate con la chiave di decrittografia corretta possano accedere alle informazioni originali e si applica ai dati indipendentemente dal loro utilizzo, spostamento o posizione. Per quanto riguarda Microsoft 365, la crittografia fornisce un livello di sicurezza che aiuta le aziende a salvaguardare le proprie comunicazioni, i documenti e gli altri dati, indipendentemente da dove risiedono all'interno della loro infrastruttura cloud.

E-mail di phishing e siti Web infetti sono spesso i subdoli precursori di gravi attacchi ransomware. Negli ultimi anni, il ransomware RobbinHood ha tristemente devastato le organizzazioni, costando loro milioni di dollari in riscatti, interruzioni e sforzi di ripristino, tutto a causa del download involontario di un'e-mail infetta e dell'introduzione del malware nel sistema.

Strumenti integrati come le etichette di riservatezza di Microsoft 365 aiutano a prevenire questo fenomeno aderendo a rigorosi protocolli in grado di crittografare automaticamente i documenti e le e-mail, prevenendo così l'infezione iniziale grazie alla diffidenza verso le e-mail sospette e avvertendo l'utente riguardo a mittenti potenzialmente pericolosi. Queste etichette possono essere configurate con criteri di gestione dei diritti, che consentono agli amministratori di determinare chi può accedere ai dati e come possono essere utilizzati; si tratta di un livello di classificazione del contenuto e protezione governato centralmente dalle organizzazioni, che consente agli amministratori IT di arbitrare la trasmissione, la condivisione e la manipolazione dei dati. In questo modo, gli utenti ben intenzionati hanno a disposizione molteplici misure di sicurezza per impedire l'introduzione o la diffusione di malware (e al contempo non ostacolare i flussi di lavoro).

Una crittografia efficace costituisce in definitiva il fondamento su cui si basano la privacy e la conformità normativa. Le organizzazioni che utilizzano efficacemente le capacità di crittografia di Microsoft 365 in affiancamento alle politiche di sicurezza già esistenti sono molto più resilienti dal punto di vista informatico rispetto a quelle che non lo fanno. Solide pratiche di crittografia sono fondamentali per salvaguardare dati preziosi da ransomware e minacce informatiche, rafforzando così la privacy, assicurando la conformità normativa e supportando uno spazio di lavoro sicuro e collaborativo.

La resilienza informatica di Microsoft 365 inizia con il backup

Considerando il panorama futuro della gestione e della sicurezza dei dati, il Backup as-a-Service (BaaS) è emerso come il metodo preferito per proteggere le app SaaS come Microsoft 365. Il BaaS è un approccio basato sul cloud che offre alle organizzazioni un sistema online in remoto per il backup e l'archiviazione dei dati. L'integrazione del BaaS con una strategia di Microsoft 365 è in linea con la necessità di soluzioni di protezione dei dati robuste, scalabili e flessibili, tutti componenti critici per garantire la resilienza organizzativa.

I servizi di backup consentono alle aziende di esternalizzare le proprie esigenze di backup a fornitori specializzati, che offrono soluzioni end-to-end in grado di automatizzare i processi di backup, ridurre la quantità di infrastruttura on-premises necessaria e fornire misure di sicurezza di alto livello, il tutto fornendo loro allo stesso tempo accesso diretto e controllo sui propri dati. Per gli utenti di Microsoft 365, BaaS significa sicurezza dei dati migliorata, efficienza operativa e tranquillità.

La protezione di un ecosistema Microsoft 365 è un'azione multiforme che richiede alle organizzazioni di impegnarsi sia in misure strategiche di prevenzione che in efficaci piani di risposta agli incidenti. Il percorso verso la resilienza informatica di Microsoft 365 è continuo e richiede un impegno per l'uso efficace dei progressi tecnologici. Fortunatamente, esistono fornitori di backup dedicati, creati su misura per i dati di Microsoft 365.

Veeam Data Cloud *for Microsoft 365*

Veeam Data Cloud *for Microsoft 365* consente una resilienza radicale per i dati di Microsoft 365 con una soluzione moderna. La soluzione di backup per Microsoft 365 leader di settore, Veeam Backup *for Microsoft 365*, viene ora fornita come servizio.

Semplifica la tua strategia di backup con software, infrastruttura di backup e storage illimitato in un servizio cloud "tutto compreso" che ti consente di sfruttare una potente tecnologia di protezione e sicurezza dei dati nell'ambito di un'esperienza utente semplice e fluida.

Veeam Data Cloud *for Microsoft 365* è un servizio di backup che offre protezione e ripristino completi dei dati per **Microsoft Exchange, SharePoint**, **OneDrive for Business** e **Teams**, offrendoti il controllo completo del tuo ambiente Microsoft 365.

Con **Veeam Data Cloud *for Microsoft 365***, ottieni:

- **Tecnologia affidabile e leader di settore:** La soluzione di protezione dei dati più completa con oltre un decennio di innovazione continua costruita su larga scala.
- **Piattaforma moderna, sicura e intuitiva:** Crea facilmente job di backup, porta a termine i ripristini e ottieni informazioni approfondite su Microsoft 365 da una moderna interfaccia utente Web.
- **Servizio all-inclusive:** Software, infrastruttura di backup e spazio di storage illimitato insieme alla manutenzione continua coperta dagli esperti.

Richiedi una demo di
Veeam Data Cloud for Microsoft 365

Sii preparato, rimani informato

Il tuo viaggio verso la resilienza informatica di Microsoft 365 non finisce qui, è solo all'inizio. Amplia la tua comprensione, perfeziona le tue strategie e rimani all'avanguardia nel 2024. Lascia che ti aiutiamo a trasformare le sfide in opportunità dando un'occhiata alla nostra più ampia raccolta di risorse:

- 8 vantaggi di un servizio di backup per Microsoft 365
- Backup di Microsoft 365 per principianti
- Best practice sul ripristino di Microsoft 365

Informazioni su Veeam Software

Veeam®, il leader del mercato globale n. 1 nella protezione dei dati e nel ripristino da ransomware, ha la missione di aiutare ogni organizzazione non solo a riprendersi da un'interruzione o perdita di dati, ma a fare un balzo in avanti. Con Veeam, le organizzazioni raggiungono una resilienza radicale attraverso la sicurezza dei dati, il ripristino dei dati e la libertà dei dati per il proprio cloud ibrido. Veeam Data Platform offre un'unica soluzione per ambienti cloud, virtuali, fisici, SaaS e Kubernetes, offrendo ai responsabili IT e della sicurezza la tranquillità di sapere che dati e applicazioni sono protetti e sempre disponibili. Con sede a Seattle e uffici dislocati in oltre 30 Paesi, Veeam protegge più di 450.000 clienti in tutto il mondo, incluso il 74% delle aziende Global 2000, che si affidano a Veeam per mantenere operativi i propri business. La resilienza radicale inizia con Veeam. Per maggiori informazioni, visitare www.veeam.com o seguire Veeam su LinkedIn @veeam-software e X @veeam.