10 Pasos de ciberresiliencia para Microsoft 365

Contenido

El aumento de los ciberataques a Microsoft 365

La protección de los datos de Microsof 365 es un aspecto esencial de una estrategia de ciberseguridad moderna, ya que las aplicaciones de la suite impregnan las operaciones diarias de innumerables empresas y operaciones. Con una amplia gama de herramientas de productividad, que incluye Exchange, Teams, SharePoint, OneDrive y más, Microsoft 365 contiene una gran cantidad de información confidencial y datos empresariales críticos, y es la razón por la que más organizaciones que nunca están invirtiendo en soluciones de terceros o servicios de backup administrados para protegerlos.[1] De hecho, hay evidencia de que el ransomware está siendo diseñado con el propósito específico de infiltrarse en Microsoft 365 y otras aplicaciones SaaS. Según un informe de Coalition, hubo un aumento del 12% en las reclamaciones cibernéticas en la primera mitad de 2023, impulsadas por los ataques ransomware, con una demanda media de rescate de $1.62 millones.[2] Como consecuencia de su uso generalizado, y a medida que más empleados instalan y utilizan Microsoft 365 en máquinas que trabajan desde casa, la plataforma se ha vuelto particularmente explotable para los atacantes que capitalizan esta infraestructura diversificada.

12%

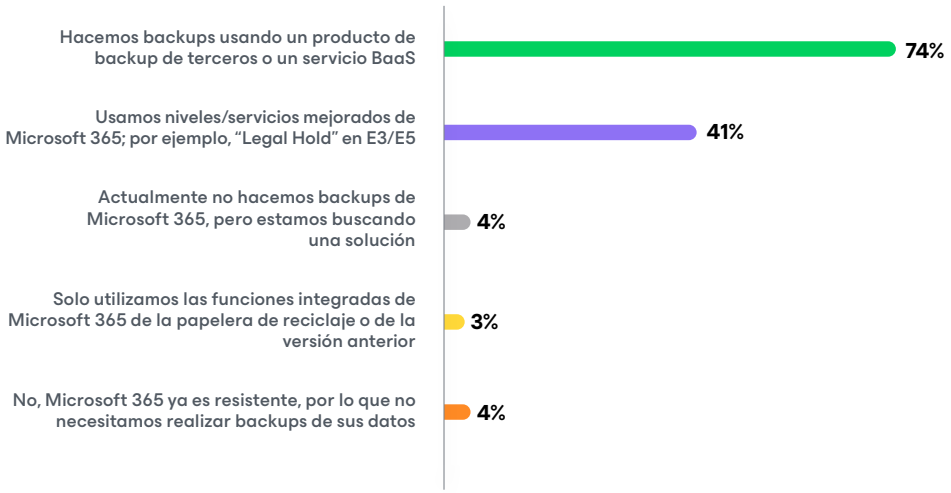
Aumento de la siniestralidad cibernética enel primer semestre de 2023

1,62

millones de dólares

es el rescate medio exigido

¿Su organización realiza backups de los datos desde Microsoft 365?



[1] Informe de tendencias de protección de datos 2024

[2] Microsoft 365 ransomware: Su guía completa para la comprensión, la prevención y la recuperación

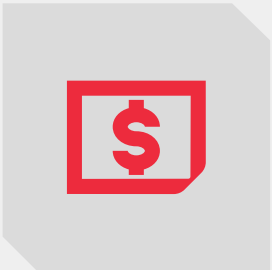
Los riesgos asociados con la pérdida de datos de Microsoft 365 no sólo son complejos, sino muy reales. La pérdida de datos resulta en graves interrupciones operativas y puede infligir daños financieros significativos debido al tiempo de inactividad y la pérdida de productividad. En un informe, los líderes de TI estimaron que el costo del tiempo de inactividad era de 1467 USD por minuto (88.000 USD por hora)[3], lo cual, dado el gran volumen de tiempo dedicado y el trabajo realizado con Microsoft 365 en un día laboral típico, es un costo que no es ninguna sorpresa. Además, cuando los datos confidenciales quedan expuestos, las organizaciones pueden sufrir fuertes sanciones por incumplimiento y daños a la reputación (en el caso de infracciones del RGPD, con multas de hasta 21 millones de dólares.[4] Dado que los datos de Microsoft 365 son enormemente delicados para las organizaciones y sus empleados, es más que probable que los eventos de pérdida de datos erosionen no solo la confianza de un cliente, sino también de un empleado, y que eventualmente conlleven una disminución en el negocio y un daño a la reputación a largo plazo tanto dentro como fuera de la compañía.

Las posibles consecuencias de datos de Microsoft 365 sin protección no se pueden exagerar. Las infracciones que exponen información personal pueden conducir a robos de identidad y fraudes, causando daños mucho después del ataque inicial. Para las empresas, la pérdida de propiedad intelectual puede erosionar las ventajas competitivas y dar lugar a costosas batallas legales o multas, que también pueden enfrentarse a litigios si se determina que han sido negligentes a la hora de salvaguardar los datos de sus clientes.

No hay forma de evitarlo. Aplicar un enfoque proactivo para proteger los datos de Microsoft 365 es más que una idea innovadora: es un requisito imprescindible para garantizar que las empresas mantengan la continuidad, el cumplimiento de las responsabilidades legales y reglamentarias, y la confianza de los clientes.

[3] Informe de tendencias de protección de datos 2022
[4] ¿Cuáles son las multas del RGPD?

Costo asociado a la pérdida de datos



El costo del tiempo de inactividad será de 1467 USD por minuto (88.000 USD por hora)

En el caso de infracciones RGPD, multas de hasta $21 millones.

Las infracciones que exponen información personal pueden conducir al robo de identidades y a fraudes.

Pasos para prepararse ante ataques

1. Autenticación multifactor

La autenticación multifactor (MFA) es una medida de seguridad esencial que requiere que los usuarios proporcionen dos o más factores de verificación para obtener acceso a recursos digitales, como cuentas de correo electrónico, aplicaciones empresariales y servicios en línea. La MFA mejora significativamente la seguridad al agregar capas de protección más allá de una simple contraseña, lo que significa que incluso si un ciberdelincuente obtiene la contraseña de un usuario, aún debe eludir los factores de autenticación adicionales para obtener acceso. Esto representa una barrera formidable frente a los accesos no autorizados.

Los beneficios de MFA son muchos, especialmente en el contexto de Microsoft 365, donde los datos sensibles y las comunicaciones corporativas están siempre presentes. La MFA puede proteger contra las consecuencias de los ciberataques comunes como el phishing, donde los atacantes engañan a los usuarios para que revelen sus credenciales. Este paso de autenticación adicional puede ser algo que el usuario sabe (como un PIN o una pregunta de seguridad) o algo que el usuario tiene (como un teléfono inteligente o hardware de una empresa).

Incluso en escenarios en los que las contraseñas se ven comprometidas debido a contraseñas débiles o reutilizadas, una configuración de MFA seguirá protegiendo la cuenta del acceso no autorizado. Este nivel de seguridad es crítico en entornos de Microsoft 365, donde el acceso remoto es rutinario y los usuarios pueden conectarse desde redes no seguras o dispositivos personales. En general, como un hecho simple y tranquilizador, la MFA crea un mecanismo de defensa dinámico que se adapta al panorama cambiante de las amenazas.

Beneficios de MFA

Defiende contra las consecuencias de los ciberataques más comunes

Continúa protegiendo la cuenta del acceso no autorizado

Crea un mecanismo de defensa dinámico que se adapta al panorama de amenazas

2. Acceso de privilegio mínimo

El principio de privilegio mínimo, estrechamente relacionado con el concepto de una arquitectura Zero Trust, es una piedra angular de las prácticas de ciberseguridad efectivas y es fundamental para fortalecer a las organizaciones contra los posibles ataques cibernéticos. Una arquitectura Zero Trust opera bajo la suposición de que existen amenazas tanto fuera como dentro de la red, de modo que no se confía automáticamente en los usuarios o sistemas. [5] Esto encaja con el principio de privilegio mínimo, que dicta que a los usuarios se les deben otorgar niveles mínimos de acceso (o permisos) necesarios para realizar sus funciones laborales, y nada más. Para Microsoft 365, la implementación de estos principios puede significar restringir el acceso a determinados documentos, carpetas, sitios, configuraciones administrativas y aplicaciones en función del rol del usuario dentro de la organización.

La adopción de un modelo de acceso de privilegio mínimo puede mejorar considerablemente la postura de seguridad de su entorno de Microsoft 365. En primer lugar, minimiza la superficie de ataque potencial de la suite para los ciberdelincuentes. Si la cuenta de un usuario se ve comprometida, el atacante está limitado a los derechos de acceso de esa cuenta, que idealmente deberían ser lo más restrictivos posible. Por ejemplo, si se roban las credenciales de un usuario, el atacante no podrá acceder a información confidencial ni realizar tareas administrativas si esos derechos no están asociados a la cuenta del usuario. Esta limitación de daños crea una zona de cuarentena para cualquier violación de la seguridad y es fundamental para controlar la propagación de unataque dentro deuna organización.

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

3. Backups periódicos

Como objetivo principal para los ciberdelincuentes, los backups son extremadamente importantes para Microsoft 365, especialmente cuando se considera el modelo de responsabilidad compartida de Microsoft[6], que establece que las organizaciones son responsables de la seguridad de sus datos. El ransomware representa una amenaza significativa para la integridad de los datos, ya que los atacantes intentan cifrar los archivos de una organización y exigir un pago para liberarlos. Sin embargo, las amenazas a los datos no se limitan a los ataques maliciosos. Los datos también pueden verse comprometidos por eliminaciones accidentales u otros percances. Mantener los backups actualizados permite a la organización recuperar rápidamente el acceso a sus datos, independientemente de si la pérdida es consecuencia de un ataque de ransomware, un error humano u otras razones críticas, para mantener los backups de Microsoft 365.[7] Esto no sólo minimiza los tiempos de inactividad, sino que también envía un mensaje fuerte de que la organización no es un blanco fácil para futuros ataques.

Implementar una rutina de backup regular significa establecer un cronograma que logre un equilibrio entre el volumen de datos manejados y los recursos disponibles para las operaciones de backup. Esto debería incluir el backup de correos electrónicos, documentos, contactos, calendarios y cualquier otro dato almacenado en el conjunto de aplicaciones de Microsoft 365.

Piense en ello como tener una póliza de seguro. Puede que no sea necesario todos los días, pero cuando ocurre un desastre, puede ser la diferencia entre una recuperación rápida y una catástrofe letal.

[6] Responsabilidad compartida en la nube

[7] 7 razones críticas para hacer backup de Microsoft 365

4. Backups inmutables

La inmutabilidad juega un papel fundamental a la hora de proteger los activos digitales de una organización frente a la alteración o eliminación, ya sea por ciberamenazas o por errores humanos. Para Microsoft 365, donde se generan, comparten y almacenan de forma rutinaria grandes cantidades de datos, garantizar que las copias de backup sean impermeables a los cambios es un elemento fundamental de una sólida estrategia de mitigación de amenazas. La inmutabilidad garantiza que una vez que se realiza el backup de la información, esta permanece en un estado prístino y es inalterable durante un período de tiempo determinado.

Para las organizaciones que usan Microsoft 365, los backups inmutables representan un escudo contra los ataques de ransomware, que apuntan no solo a datos operativos en tiempo real, sino también a los repositorios de los backups. De hecho, según una encuesta, casi todos los ataques de ransomware (93%) se dirigen específicamente a los backups.[8] Para otras medidas de seguridad, es importante disponer de una copia de backup inmutable de los datos. Al crear y aplicar políticas de retención que protejan los datos de backup para que no se sobrescriban o manipulen, las empresas pueden defender sus prácticas de continuidad contra el cifrado no deseado o la destrucción de datos. La inmutabilidad garantiza que, a pesar de cualquier violación de seguridad que afecte a los almacenes de datos actuales, la organización pueda restaurar las operaciones desde un backup limpio e inalterado.

93%

de los ataques de ransomware se dirigen explícitamente a los backups.

[8] Informe de tendencias de ransomware 2023

5. Plan de respuesta ante incidentes

Un plan de respuesta ante incidentes es un plan bien estructurado. Detalla los procesos que una organización debe seguir cuando se enfrenta a diversos incidentes de ciberseguridad, sirviendo como guías de tácticas para identificar, contener, erradicar y recuperarse de amenazas de seguridad, y asegurando que todas las partes interesadas estén informadas y preparadas para actuar.

Para las organizaciones que utilizan Microsoft 365, la base de un plan sólido de respuesta a incidentes incluye la identificación de activos críticos dentro del ecosistema de Microsoft 365. Esto significa identificar dónde se almacenan los datos confidenciales, ya sea dentro de OneDrive, SharePoint, Exchange Online o en otro lugar. Una vez identificados estos activos, el plan debe definir las amenazas potenciales y crear una lista priorizada de riesgos, junto con estrategias para mitigarlos. Esto incluye el uso de herramientas de monitorización y detección integradas, estrategias de contención inmediata, erradicación de amenazas, comunicación sólida entre las partes e identificación y recuperación de cualquier dato perdido o comprometido.

El pegamento que mantiene unido un plan de respuesta a incidentes es la preparación minuciosa. Esto va más allá de las herramientas técnicas, la capacitación y la colaboración de los equipos de TI y de seguridad, sino que afecta también a todos los empleados. Para aquellos que utilizan Microsoft 365, las organizaciones deben realizar sesiones educativas periódicas adaptadas a su intrincado ecosistema. Los empleados que utilizan aplicaciones dentro de Microsoft 365 como Outlook y Teams deben estar equipados con el conocimiento para discernir y reaccionar ante actividades sospechosas, que pueden venir en forma de mensajes aparentemente legítimos, invitaciones a reuniones falsas de compañeros de trabajo o correos electrónicos de apariencia auténtica de líderes de empresas. Las personas pueden ser una debilidad en ciberseguridad para cualquier organización, pero los empleados bien formados tienen el potencial de formar una barrera formidable contra las amenazas.

Un plan de respuesta ante incidentes comienza con

Framework integral de respuesta a incidentes

Identificación de activos críticos

Importancia de la preparación de los empleados

6. Auditorías periódicas y pruebas de penetración

Las auditorías periódicas y las pruebas de penetración son componentes integrales para mantener un entorno resiliente de Microsoft 365. De hecho, el propio Microsoft 365 proporciona una serie de herramientas integradas para la auditoría y detección de amenazas[9], que sirven de base para reforzar su entorno frente a diversas amenazas de seguridad. Estas prácticas sirven como medidas proactivas que permiten a las empresas identificar y rectificar los problemas antes de que puedan ser explotados por los atacantes.

Las auditorías del ecosistema de Microsoft 365 implican la revisión sistemática de diversos aspectos, como los permisos de usuario, los controles de acceso a los datos y la configuración de seguridad. Aunque a veces es complicado, las auditorías regulares ayudan a garantizar que las configuraciones del sistema permanezcan alineadas con las mejores prácticas y las políticas de seguridad de la organización. Es, pues, un hábito muy saludable para desarrollar y mantener. Dado que Microsoft 365 abarca una variedad de servicios, estas auditorías deben ser exhaustivas y cubrir cada servicio para evitar vulnerabilidades que se pasen por alto.[10]

A menudo, las pruebas de penetración denominadas de "hacking ético" complementan las auditorías periódicas al permitir a las organizaciones evaluar la efectividad de sus medidas de seguridad. Esto implica simular ciberataques a la infraestructura de Microsoft 365 para identificar puntos débiles que los atacantes del mundo real podrían explotar. En las organizaciones que cumplan los requisitos, las pruebas de penetración deben sondear todas las capas de su ecosistema de Microsoft 365, desde la resistencia al phishing de los empleados hasta la resiliencia de herramientas técnicas como los firewalls, los sistemas de detección de amenazas y los planes de respuesta a incidentes. Los conocimientos recopilados de estas pruebas orientan a las organizaciones a la hora de ajustar sus programas de capacitación y estrategias de seguridad, lo que les permite desarrollar defensas más completas y efectivas cuando surge inevitablemente una amenaza cibernética.

[9] Guía de Microsoft 365 para seguridad y cumplimiento

[10] Seguridad nativa de Microsoft 365: desbloqueo de las características de cumplimiento y monitorización

7. Directivas de restricción de software

Una política de restricción de software (SRP) es una característica de seguridad que las organizaciones pueden usar para identificar y controlar la ejecución de software en hardware específico. Para las organizaciones empresariales que usan Microsoft 365, implementarlo puede actuar como un mecanismo de defensa crítico para proteger los numerosos dispositivos de los que son responsables. Como Microsoft 365 contiene una variedad de herramientas distintas, también invita a una variedad de vectores de amenazas distintos y explotables. Al dictar qué software puede y no puedeejecutarse en un sistema, los SRP reducen efectivamente la superficie de ataque disponible para los actores maliciosos.

Al construir un SRP para un entorno de Microsoft 365, el objetivo es garantizar que solo se permita la ejecución de aplicaciones, scripts y procesos confiables, incluidas las listas blancas y negras de vectores de amenazas según sea necesario. Para obtener la máxima efectividad, los SRP deben configurarse teniendo en cuenta el acceso de privilegio mínimo y actualizarse regularmente para reflejar los cambios en el software utilizado por una organización. Esto incluye actualizaciones de las herramientas de Microsoft 365, la adición de nuevo software o la interrupción de aplicaciones heredadas.

Al impedir que el malware aproveche las técnicas de explotación comunes, los SRP son muy eficaces para interrumpir la cadena de infección y mantener una zona de cuarentena. La integración de SRP en una estrategia de ciberseguridad es un enfoque orientado hacia el futuro que ayuda a proteger la infraestructura de una organización de la ejecución de software no confiable, algo que, a medida que las empresas crecen y contratan nuevos empleados, es una posibilidad cada vez mayor.

8. Monitorización y registro

La monitorización y el registro constituyen un paso vital para garantizar la seguridad e integridad de cualquier entorno de Microsoft 365. Al vigilar las actividades del sistema y mantener registros completos de eventos, las organizaciones pueden detectar posibles incidentes de seguridad en tiempo real, diagnosticar problemas del sistema, comprender el alcance de las violaciones y mejorar la postura general de seguridad.

Para los administradores de Microsoft 365, importar registros a un sistema de administración de eventos e información de seguridad (SIEM) puede simplificar enormemente este proceso. Azure Sentinel, por ejemplo, es un SIEM nativo de Microsoft que usa un conjunto de conectores de datos prediseñados para transmitir los datos de registro de una organización directamente a la aplicación SIEM. Estos datos se normalizan para lograr conjuntos de datos consistentes y se monitorean a través de herramientas de análisis integradas.

Una monitorización eficaz debería arrojar una amplia red para detectar una gama de posibles anomalías indicativas de una amenaza para la seguridad, desde intentos fallidos de inicio de sesión (que sugieren un ataque de fuerza bruta) hasta patrones de descarga inusuales (que sugieren una exfiltración de datos no deseada) y muchos otros. Un registro exhaustivo es igualmente importante, ya que sirve como documentación de todas las actividades supervisadas. Dichos registros deben capturar suficientes detalles para permitir la reconstrucción de los eventos a lo largo de todo un incidente: antes, durante y después. Esto se vuelve invaluable en el análisis forense posterior al incidente, pero también ayuda en las auditorías de cumplimiento y el refinamiento de las medidas de seguridad a lo largo del tiempo. El registro debe configurarse cuidadosamente para garantizar que los datos recopilados sean procesables, proporcionando información clara y relevante sin el ruido que se puede generar a partir de un alcance demasiado ambicioso.

Con el tiempo, la información obtenida de la monitorización y el registro proporciona a las organizaciones los datos necesarios para realizar cambios proactivos en las políticas y agilizar las actualizaciones de seguridad.

9. Separación de datos

La separación de privilegios es una estrategia de amplia aplicación y efectiva que utilizan las organizaciones para mejorar su infraestructura de seguridad. Es muy útil cuando se integran servicios basados en datos como Microsoft 365. Las estrategias como las arquitecturas multicliente, los límites administrativos y la restricción condicional de cuentas se centran en estructurar los datos y sus privilegios para reducir el acceso no autorizado y limitar el daño potencial de las infracciones de seguridad. Al mantener diferentes conjuntos de datos separados y dividir las redes en segmentos discretos, las organizaciones reducen significativamente el riesgo inicial de infracciones de seguridad y ponen en cuarentena de manera efectiva las incidencias en caso de que ocurran.

El uso de políticas de separación de privilegios dentro de Microsoft 365 permite a las organizaciones mantener reglas de acceso estrictas. Como mencionamos en nuestra sección anterior, las mejores de estas reglas garantizan que los usuarios, administradores y servicios reciban solo los permisos necesarios para realizar las tareas necesarias y nada más; por ejemplo, el principio de privilegio mínimo y el control de acceso basado en roles (RBAC).

Para las organizaciones que operan en varias jurisdicciones o tienen unidades de negocio distintas, separar los tenant de Microsoft 365 a través de una arquitectura multicliente puede ayudar a aislar los datos y controlar el acceso. Esto se refiere a la creación de límites administrativos distintos por tenant. Al hacer esto, los entornos aíslan sus propios datos, cuentas de usuario y controles de acceso, y se garantiza que la seguridad y los requisitos de cumplimiento se satisfagan individualmente y que una infracción de seguridad o un incidente dentro de un tenant no comprometa la integridad de los demás.

Dentro de estos límites administrativos, las directivas de acceso condicional y las restricciones de cuenta añaden otra capa de defensa y pueden implementarse directamente en Microsoft 365. Estas políticas permiten a las organizaciones definir e implementar reglas basadas en el contexto para cualquier cuenta dada, lo que permite que las reglas de seguridad de una organización se optimicen según el nivel de riesgo de una cuenta, la ubicación geográfica o las irregularidades dinámicas, como inicios de sesión o descargas sospechosas.

La separación metódica puede, como tal, aplicarse a todos los niveles de la jerarquía de una organización y proporciona una base sólida para proteger los datos de Microsoft 365 y otros activos digitales. Dado que la compartimentación estratégica no solo mitiga el riesgo de acceso no autorizado, sino que también proporciona salvaguardas en capas y alternativas contra las infracciones de seguridad, la separación de datos y privilegios se ha ganado su estatus como un enfoque confiable para que las organizaciones fortalezcan sus defensas cibernéticas, mantengan la continuidad de negocio y, en última instancia, den pasos para lograr la ciberresiliencia dentro de su entorno de Microsoft 365.

10. Cifrado

El cifrado es una medida de seguridad fundamental que sirve como línea de defensa principal en la protección de información sensible, asegurando que solo las partes autorizadas con la clave de descifrado correcta puedan acceder a la información original, y se aplica a los datos independientemente de su uso, movimiento o ubicación. En lo que respecta a Microsoft 365, el cifrado proporciona una capa de seguridad que ayuda a las empresas a proteger sus comunicaciones, documentos y otros datos, sin importar dónde se encuentren alojados dentro de su infraestructura en la nube.

Los correos electrónicos de phishing y los sitios web infectados son a menudo los precursores sutiles de graves ataques de ransomware. En los últimos años, el ransomware RobbinHood ha devastado de forma infame a las organizaciones, costándoles millones de dólares en rescates, tiempos de inactividad y esfuerzos de recuperación, todo debido a que un correo electrónico infectado se descargó involuntariamente y el malware se introdujo en el sistema.

Las herramientas integradas, como las etiquetas de confidencialidad de Microsoft 365, ayudan a evitar esto al adherirse a protocolos estrictos que pueden cifrar automáticamente documentos y correos electrónicos, evitando así la infección inicial al desconfiar de los correos electrónicos sospechosos y advertir al usuario de remitentes potencialmente peligrosos. Estas etiquetas pueden configurarse con políticas de gestión de derechos, lo que permite a los administradores determinar quién puede acceder a los datos y cómo pueden utilizarse; se trata de un nivel de clasificación y protección de contenido gobernado de forma centralizada por las organizaciones, lo que permite a los administradores de TI arbitrar el manejo, el intercambio y la manipulación de los datos. De este modo, los usuarios bien intencionados disponen de múltiples medidas de protección para evitar la introducción o la propagación de malware (y no obstaculizar los flujos de trabajo en el proceso).

En última instancia, un cifrado eficaz constituye la base sobre la que se construyen la privacidad y el cumplimiento normativo. Las organizaciones que utilizan eficazmente las funcionalidades de cifrado de Microsoft 365 en paralelo con sus políticas de seguridad ya existentes son mucho más ciberresilientes que las que no lo hacen. Las prácticas de cifrado sólidas son fundamentales para proteger los datos valiosos contra el ransomware y las ciberamenazas, respaldando la privacidad, garantizando el cumplimiento normativo y respaldando un espacio de trabajo seguro y colaborativo.

La ciberresiliencia de Microsoft 365 comienza con el backup

Al considerar el panorama futuro de la gestión de datos y la seguridad, el Backup as a Service (Backup como servicio) se ha convertido en el método preferido para proteger aplicaciones SaaS como Microsoft 365. BaaS es un enfoque basado en la nube que proporciona a las organizaciones un sistema remoto en línea para realizar backups y almacenar sus datos. La integración de BaaS con una estrategia de Microsoft 365 se alinea con la necesidad de soluciones de protección de datos robustas, escalables y flexibles, todos ellos componentes críticos para garantizar la resiliencia organizativa.

Los servicios de backup permiten a las empresas externalizar sus necesidades de respaldo a proveedores especializados, que ofrecen soluciones integrales que pueden automatizar los procesos de backup, reducir la cantidad de la infraestructura necesaria en las instalaciones locales y proporcionar medidas de seguridad de primer nivel. Y todo ello proporcionándoles acceso directo y control sobre sus datos. Para los usuarios de Microsoft 365, BaaS significa seguridad de datos mejorada, eficiencia operativa y tranquilidad.

Proteger un ecosistema de Microsoft 365 es una tarea polifacéticaque requiere que las organizaciones adopten medidas estratégicas de prevención y planes eficaces de respuesta ante incidentes. La transición hacia la ciberresiliencia de Microsoft 365 está en marcha y requiere un compromiso con el uso eficaz de los avances tecnológicos. Afortunadamente, hay proveedores de backup dedicados creados a medida para los datos de Microsoft 365.

Veeam Data Cloud *for Microsoft 365*

Veeam Data Cloud *for Microsoft 365* ofrece una resiliencia radical para los datos de Microsoft 365, con un toque moderno. La solución de backup de Microsof 365 líder en la industria, Veeam Backup *for Microsoft 365*, ahora se entrega como un servicio.

Simplifique su estrategia de backup con software, infraestructura de backup y almacenamiento ilimitado en un servicio en la nube todo en uno que le permite convertir una potente tecnología de seguridad y protección de datos en una experiencia de usuario sencilla y sin problemas.

Veeam Data Cloud *for Microsoft 365* es un servicio de backup que proporciona recuperación de datos y protección de datos completa para **Microsoft Exchange, SharePoint, OneDrive for Business y Teams**, que le dan un control completo de su entorno de Microsoft 365.

→ Solicite una demostración de Veeam Data Cloud *for* Microsoft 365

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

- **Tecnología confiable y líder en la industria:** La solución de protección de datos más completa, con más de una década de innovación continua, construida a escala.
- **Plataforma moderna, segura e intuitiva:** Cree fácilmente trabajos de backup, lleve a cabo restauraciones y obtenga información de Microsoft 365 desde una interfaz de usuario web moderna.
- **Servicio Todo Incluido:** Software, infraestructura de backup y almacenamiento ilimitado junto con un mantenimiento continuo realizado por expertos.

Prepárese, manténgase informado

Su viaje hacia la ciberresiliencia de Microsoft 365 no termina aquí, recién comienza. Amplíe sus conocimientos, perfeccione sus estrategias y manténgase a la vanguardia en 2024. Permítanos ayudarlo a transformarlos desafíos en oportunidades consultando nuestra colección ampliada de recursos:

- 8 Beneficios de un servicio de backup para Microsoft 365
- Microsoft 365 Backup for Dummies
- Mejores prácticas de recuperación de Microsoft 365

Acerca de Veeam Software

Veeam®, el líder n.º 1 del mercado mundial en protección de datos y recuperación de ransomware, tiene la misión de ayudar a cada organización, no solo a recuperarse de una interrupción de datos o una pérdida de datos, sino a avanzar. Con Veeam, las organizaciones logran una resiliencia radical mediante seguridad de datos, recuperación de datos y libertad de datos para su nube híbrida. Veeam Data Platform proporciona una solución única para entornos cloud, virtuales, físicos, SaaS y Kubernetes que proporciona a los responsables de TI y seguridad la tranquilidad de saber que sus datos y aplicaciones están siempre protegidos y disponibles. Con sede en Seattle y oficinas en más de 30 países, Veeam protege a más de 450 000 clientes en todo el mundo, incluido el 74% de las empresas de Global 2000, que confían en Veeam para mantener sus negocios en funcionamiento. La resiliencia más innovadora comienza con Veeam. Obtenga más información en www.veeam.com o siga a Veeam en LinkedIn @veeam-software y X @veeam.