keepit®

Wiederherstellung von SaaS-Anwendungen

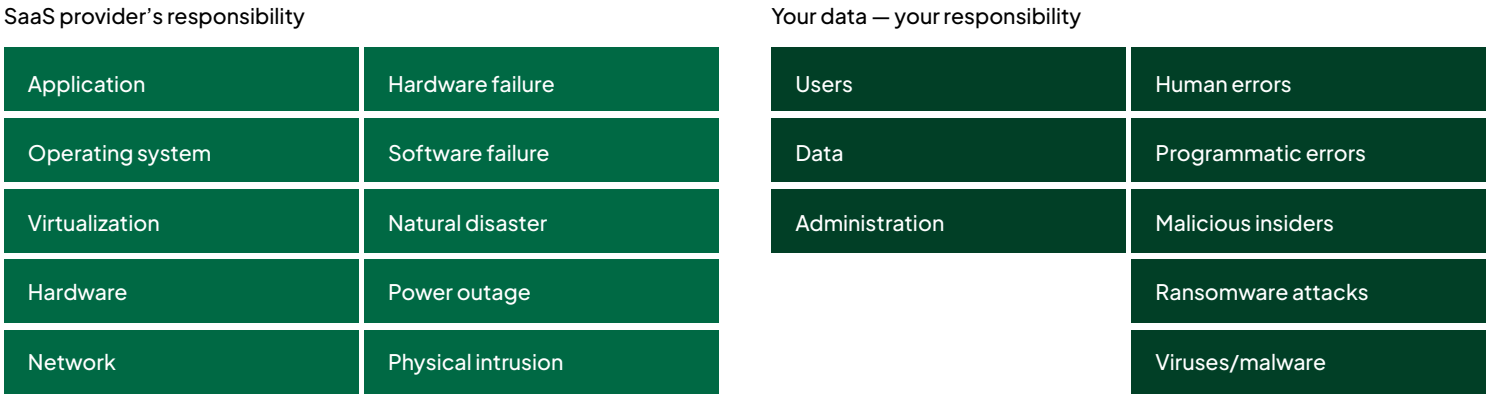
Wenn der Notfall eintritt

Ein Leitfaden für Datenwiederherstellung und Betriebskontinuität

Wiederherstellung von SaaS-Anwendungen: Wenn der Notfall eintritt

Tagtäglich verlagern Unternehmen wichtige Abläufe in cloudbasierte SaaS (Software-as-a-Service)-Anwendungen. Gleichzeitig konzentrieren sich jedoch auch Cyberkriminelle verstärkt auf Cloud-Dienste und bringen damit die Unternehmen in Gefahr.[1]

Die meisten Unternehmen verfügen über irgendeine Form von Kontinuitäts- und Disaster Recovery (DR-)Plan,[2] aber diese Pläne übersehen oft wichtige SaaS-Daten, die für die Aufrechterhaltung oder Wiederherstellung der Betriebsabläufe erforderlich sind - und stellen damit eine wesentliche Lücke im Bereitschaftsniveau der Unternehmen dar. Selbst erfahrenen IT-Fachleuten ist oft nicht klar, dass die Sicherung der Daten in ihrer eigenen Verantwortung liegt, nicht in der des SaaS-Anbieters.



Leider werden viele Unternehmen auf die harte Tour lernen müssen, dass sie sich nicht auf SaaS-Anbieter verlassen sollten, wenn es um die Sicherung ihrer Daten geht. Laut Gartner wird es bis 2022 in 70 % aller Unternehmen zu Störungen kommen, weil verlorene Daten in einer SaaS-Anwendung nicht wiederhergestellt werden können.[3]

Nach Angaben der ESG sind die häufigsten Gründe für Datenverlust Dienstausfälle, versehentliches Löschen und externe böswillige Löschungen wie Ransomware-Angriffe (Abbildung 2).

Tatsächlich stellte ESG fest, dass im Jahr 2023 75 % der Unternehmen von mindestens einem erfolgreichen Ransomware-Angriff betroffen waren. Von den betroffenen Organisationen gaben 84 % an, einen Teil ihrer Daten verloren zu haben, was zeigt, dass die Wiederherstellungsfähigkeiten derzeit nicht ausreichen, um die wachsende Bedrohung zu bekämpfen.[4]

Zu den weiteren Gründen zählen Probleme mit Backup-Mechanismen und Missverständnisse rund um Aufbewahrungs-/Löschrichtlinien. Darüber hinaus fand die ESG heraus, dass 81 % der Microsoft Office 365-Nutzer schon einmal Daten wiederherstellen mussten, jedoch nur 15 % in der Lage waren, 100 % ihrer Daten zu retten.[5]

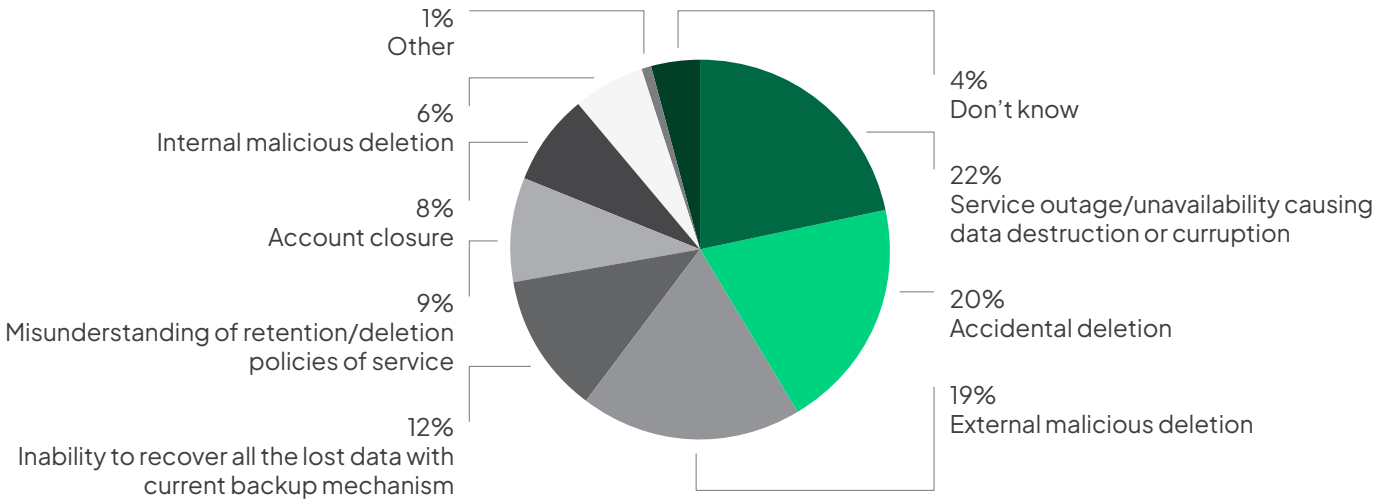


Abb. 2: Hauptursachen für SaaS-Datenverluste

Was ist die Hauptursache für Datenverluste in den SaaS-basierten Anwendungen, die Ihr Unternehmen nutzt? (Prozentsatz der Befragten, N=344)

Kritische Daten stets verfügbar

Keepit hat sich dem Schutz von Daten in der Cloud verschrieben. 2013 begannen wir mit der Entwicklung einer maßgefertigten Lösung. Heute stellen wir einen effizienten, sicheren Dienst bereit, der eine einfache, zuverlässige, kostengünstige und anbieterneutrale Sicherung und Wiederherstellung von SaaS-Workloads ermöglicht. Vor der SaaS-Ära konnten Unternehmen oft selbst eine vollständige Notfallwiederherstellung durchführen. Der Umstieg auf die Cloud hat jedoch neue Komplikationen und Abhängigkeiten mit sich gebracht:

- Für eine vollständige Wiederherstellung einer SaaS-Anwendung muss der Tenant wiederhergestellt und neu mit Daten befüllt werden.
- Um in der Zwischenzeit die Kontinuität zu wahren, muss das betroffene Unternehmen auf seine SaaS-Daten zugreifen können.

Keepit repliziert zwar nicht die SaaS-Anwendung und alle ihre Funktionalitäten. Jedoch bietet die Lösung kontrollierten, komfortablen – und sofortigen – Zugriff auf die SaaS Daten in einem verwendbaren Format, sodass Unternehmen die Betriebskontinuität aufrechterhalten können. Zudem gewährleisten die sicheren Backups von Keepit, dass die SaaS-Daten wiederhergestellt werden können, sobald die Anwendung wieder problemfrei läuft.

Was die Cloud verändert hat

Beim On-Premises-Modell hängt die Einhaltung eines Ziels für die Wiederherstellungszeit (Recovery Time Objective, RTO) weitgehend von der Sicherung und Wiederherstellung der Systeme und der zugehörigen Kundendaten ab. Im Lauf der Zeit haben Unternehmen durch Investitionen in entsprechende Hardware- und Softwarelösungen dafür gesorgt, dass die Anforderungen an Kontinuität und Wiederherstellung erfüllt werden.

In der SaaS-Welt sieht die Sache jedoch ganz anders aus. Bei einem Notfall, von dem SaaS-Anwendungen betroffen sind, hängt die Aufrechterhaltung der Kontinuität – und die Wiederherstellung – von zwei Faktoren ab:

1. Wie vollständig und schnell auf die Daten zugegriffen werden kann, unabhängig vom Zustand der SaaS-Anwendung.
2. Wie vollständig und schnell die Daten wiederhergestellt werden können, wenn die Anwendung wieder betriebsbereit ist.

Damit ein Unternehmen seine DR-Ziele erreichen kann, muss also beides gewährleistet sein:

- Die Verfügbarkeit der Cloud-Daten, für die weitgehend der Kunde verantwortlich ist, und
- Die Verfügbarkeit der Cloud-Anwendung (z. B. M365), für die der Anbieter der Anwendung zuständig ist.

Die meisten Unternehmen – also alle, die nicht über spezifisches Know-how und umfangreiche Ressourcen verfügen – können die Verfügbarkeit von SaaS Daten am zuverlässigsten und kostengünstigsten gewährleisten, indem sie die Datensicherungsdienste eines Drittanbieters in Anspruch nehmen.

Eine allzu häufige Bedrohung: Ransomware

Nehmen wir nun einen fiktiven Ransomware-Vorfall als Beispiel, um den Unterschied zwischen Zugriff und Wiederherstellung deutlich zu machen und zu zeigen, welche Schlüsselrolle die Keepit Cloud sowohl für die Wahrung der Geschäftskontinuität als auch eine schnelle und sichere Notfallwiederherstellung spielt. Die verheerendsten Ransomware-Angriffe verfolgen heute einen zweigleisigen Ansatz, um möglichst viel Chaos anzurichten und Druck aufzubauen. Häufig gehen die Angreifer so vor:

- Sie vereiteln mithilfe eines kompromittierten Administratorkontos Wiederherstellungsoptionen (z. B. durch Deaktivieren der Versionierung, Leeren des Papierkorbs, Löschen/Verschlüsseln von Daten).
- Sie führen die Ransomware auf einem oder mehreren Endgeräten aus, um lokale Kopien von Daten zu verschlüsseln. Diese Kopien werden anschließend mit Cloud-Repositories synchronisiert, sodass auch die Online-Daten verschlüsselt und unzugänglich werden.

Solche Angriffe bedrohen große und kleine Unternehmen weltweit, befeuert von einem Teufelskreis: Mithilfe der erbeuteten Lösegelder können die Cyberkriminellen ihre Aktivitäten weiter verstärken[5], und so werden die Angriffe immer zahlreicher.[6]

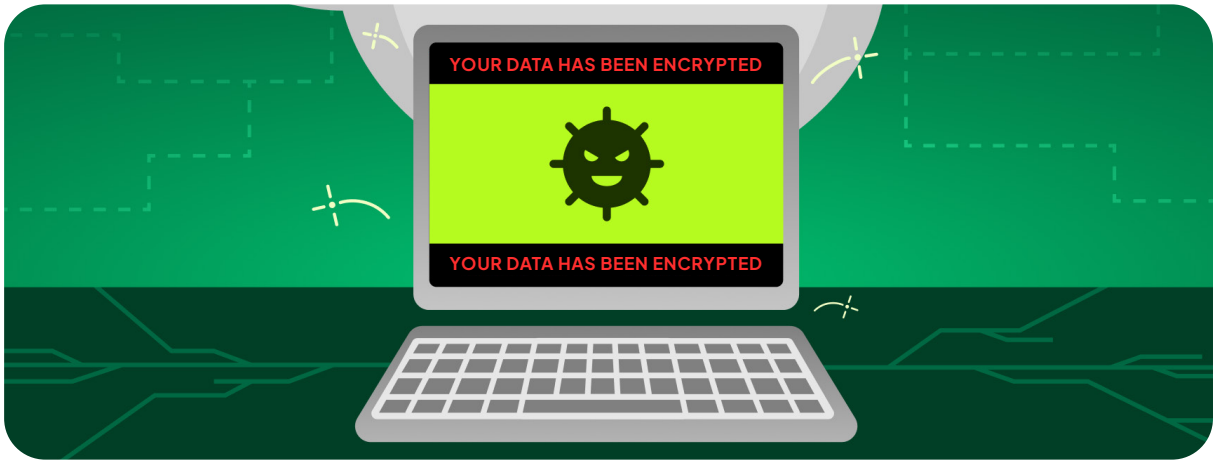
Nach Angaben des Weltwirtschaftsforums ist die Cyberkriminalität inzwischen die drittgrößte Wirtschaftsmacht der Welt, nur noch hinter den USA und China.[7] Cyberattacken treten daher immer häufiger auf. Gartner schätzt, dass bei 99% dieser Angriffe Backups und Sicherheitsprodukte ins Visier genommen werden, da die Angreifer versuchen, die Verteidigungsfähigkeit von Unternehmen auszuschalten.[8]

Notfall bei Acme: Ransomware und Wiederherstellung

„Acme“ (das fiktive Unternehmen für unser Beispiel) ist ein internationaler IT-Dienstleister mit 6.500 Mitarbeitern. Das Unternehmen arbeitet mit sensiblen Kundendaten, und sein Geschäft hängt davon ab, dass die vertraulichen Daten sicher und die Dienste verfügbar bleiben.

Detonation

An einem Feiertagswochenende führt ein Angreifer Ransomware in der Acme-Umgebung aus. Um den Geschäftsbetrieb des Unternehmens lahmzulegen, werden alle E-Mails verschlüsselt. In einer Nachricht droht der Angreifer, auch die OneDrive-Daten zu verschlüsseln, falls nicht innerhalb von 72 Stunden Lösegeld gezahlt wird.



Nachdem der Angriff erkannt wurde, beginnen die Verantwortlichen bei Acme, die Notfallpläne umzusetzen:

- Der Incident-Response (IR)-Plan umfasst Leitlinien für Geschäftsentscheidungen; Untersuchung, Eindämmung und Entschärfung der Bedrohung; regulatorische und vertragliche Verpflichtungen; interne und externe Kommunikation; Zusammenarbeit mit den Strafverfolgungsbehörden etc.

- Der Disaster-Recovery-Plan fokussiert darauf, den Betrieb (z. B. Daten und Dienste) schnell, sicher und nach Prioritäten geordnet wiederherzustellen.

Wiederherstellung von Microsoft OneDrive

Der DR-Plan von Acme orientiert sich an der Microsoft-Dokumentationsseite Wiederherstellung nach einem Ransomwareangriff in Microsoft 365[9]. Diese Microsoft-Dokumentation soll den Kunden vermitteln, welche Maßnahmen bei SaaS-Wiederherstellungsszenarien erforderlich sind, im Gegensatz zu Szenarien für On-Premises-Anwendungen.

Schritt 1

Überprüfen der Backups

Microsoft erklärt: „Wenn Sie über Offlinesicherungen verfügen, können Sie die verschlüsselten Daten wahrscheinlich wiederherstellen, nachdem Sie die Ransomware-Nutzlast (Schadsoftware) aus Ihrer Umgebung entfernt haben“, und fügt hinzu: „Wenn Sie keine Sicherungen haben oder Ihre Sicherungen ebenfalls von der Ransomware betroffen sind, können Sie diesen Schritt überspringen.“

Zwei Punkte sind hier für Acme wichtig:

- Microsoft gewährleistet nicht („wahrscheinlich“), dass eine Wiederherstellung möglich ist.
- Bei Acme ist man sich bewusst, dass viele Ransomware-Familien auch Backups infizieren[11]. Deshalb machen sich die IT-Mitarbeiter jetzt Sorgen, ob ihre Backups betroffen sind.

Mit Keepit:

Keepit ist eine dedizierte SaaS-Backup und Recovery-Lösung, die durch eine unabhängige logische Infrastruktur vollständig von der Microsoft-Umgebung getrennt ist.

Selbst Angriffe auf das Azure-Ökosystem stellen daher keine Bedrohung für die Backups in Keepit dar, da sie sicher in unserer air-gapped cloud aufbewahrt werden.

Die bei Keepit gespeicherten Daten sind komplett unveränderbar - können also nicht verschlüsselt oder manipuliert werden - und sind immer zugänglich, unabhängig vom Zustand der SaaS-Anwendung.

Schritt 2

Deaktivieren von Exchange ActiveSync und der OneDrive-Synchronisierung

Um „das Fortschreiten der Datenverschlüsselung zu verhindern“, empfiehlt Microsoft, „den Benutzerzugriff auf die Postfächer vorübergehend zu deaktivieren“ und die OneDrive-Synchronisierung zu unterbrechen, um „Ihre Cloud-Daten vor einer Aktualisierung durch potenziell infizierte Geräte zu schützen.“

Mit Keepit:

Da die Backups von Keepit von der Microsoft-Umgebung getrennt und völlig unveränderbar sind, können die Kunden jederzeit auf die Daten zugreifen, unabhängig von der Verfügbarkeit der SaaS-Anwendung.

Fortsetzung
Die IT-Mitarbeiter von Acme sind sich zwar über den Sinn und die Notwendigkeit dieser Maßnahmen im Klaren, wissen aber auch, dass die Deaktivierung von ActiveSync und der OneDrive-Synchronisierung die Benutzer daran hindert, auf ihre Daten zuzugreifen. Und das ist für viele Aspekte des Incident-Response-Plans sehr nachteilig, insbesondere für diejenigen, die Kommunikation und Zusammenarbeit erfordern.

Fortsetzung
Dieser zeitnahe, sichere und eingeschränkte Zugriff – realisiert durch die einzigartige „Public Links"-Funktionalität von Keepit – sorgt dafür, dass die Mitarbeiter wichtige Aufgaben ausführen können, während die umfassenderen IR- und DR-Maßnahmen im Gang sind.[10]

Schritt 3

Entfernen der Malware von den betroffenen Geräten

Microsoft rät: „Führen Sie einen vollständigen, aktuellen Antivirus-Scan auf allen verdächtigen Computern und Geräten durch, um die Nutzlast zu erkennen und zu entfernen." Weiter heißt es: „Vergessen Sie nicht, Geräte zu überprüfen, die Daten oder die Ziele zugeordneter Netzlaufwerke synchronisieren."

Die IT-Mitarbeiter von Acme wissen, dass jede Minute Ausfallzeit ihrem Unternehmen schadet. Sie wissen aber auch, dass sie diesen entscheidenden Schritt – der selbst mit Automatisierungstools lange dauern wird – nicht überstürzen können, ohne Gefahr zu laufen, die Ransomware erneut in ihre Umgebung einzuschleusen.

Mit Keepit:

Keepit ermöglicht es, schon vor der Wiederherstellung der Anwendung auf SaaS-Daten zuzugreifen. So können Unternehmen während dieses potenziell langwierigen Wiederherstellungsschritts eine gewisse Kontinuität aufrechterhalten – und ihre DR- und IR-Pläne effizientumsetzen.

Der Zugriff kann sogar im Voraus über leistungsstarke APIs geskriptet werden, was die Wiederherstellung beschleunigt und die Wahrung der Kontinuität erleichtert.

Schritt 4

Wiederherstellen der Dateien auf einem bereinigten Computer oder Gerät

Nachdem die Ransomware entfernt wurde, ist es jetzt gefahrlos möglich, „den Dateiverlauf ... oder den Systemschutz ... zu verwenden, um zu versuchen, Ihre lokalen Dateien und Ordner wiederherzustellen".
Die Anweisungen von Microsoft enthalten jedoch zwei wichtige Vorbehalte:

Mit Keepit:

Sobald eine Anwendung wieder in Betrieb ist, ermöglicht Keepit eine schnelle und einfache Wiederherstellung der Daten.

Unsere granulare Wiederherstellungsfunktionalität fügt sich nahtlos in die Disaster-Recovery-Pläne unserer Kunden ein, und erlaubt ihnen, kritische Daten aus bestimmten Zeiträumen für eine schnellere Wiederherstellung zu priorisieren und so Ausfallzeiten minimieren.

- „Manche Ransomware verschlüsselt oder löscht auch die Backup-Versionen, sodass Sie den Dateiverlauf oder den Systemschutz nicht verwenden können, um Dateien wiederherzustellen.“
- „Wenn ein Ordner mit OneDrive synchronisiert wird und Sie nicht die neueste Version von Windows verwenden, kann es bei der Verwendung des Dateiverlaufs zu Einschränkungen kommen.“

Zum jetzigen Zeitpunkt hofft Acme noch, diese Komplikationen vermeiden zu können.

Schritt 5

Wiederherstellen der Dateien in OneDrive for Business

Für Dateien, die sich mithilfe des Dateiverlaufs oder Systemschutzes nicht wiederherstellen lassen, bietet Microsoft Folgendes an: „Mit der Dateiwiederherstellung in OneDrive for Business können Sie eine gesamte OneDrive auf einen früheren Zeitpunkt innerhalb der letzten 30 Tage wiederherstellen.“

Die IT-Mitarbeiter von Acme hatten mit Einschränkungen gerechnet, doch das 30-Tage-Fenster ist eine unangenehme Überraschung. In diesem frühen Stadium der Untersuchung konnten sie noch nicht feststellen, wann sich der Angreifer erstmals Zugang zur Umgebung verschafft hat. Es ist demnach gut möglich, dass zumindest einige Dateien auf einen Zeitpunkt wiederhergestellt werden müssten, der vor dem 30-Tage-Fenster liegt.

Mit Keepit:

Mit dem 30-Tage-Fenster wird vorausgesetzt, dass der Microsoft Tenant irgendwann in diesem Zeitraum problemfrei und richtig konfiguriert war. Was aber, wenn bereits ein Problem mit dem Tenant bestand oder die Daten schon kompromittiert waren?

In einem Angriffsszenario ist demnach unklar, ob überhaupt Tenant-Daten verwendet werden können. Bei Keepit dagegen sind alle gespeicherten Daten unveränderbar und sofort zugänglich. Das betroffene Unternehmen kann den Benutzern Zugriff auf Daten von jedem beliebigen Zeitpunkt im Backup-Set ermöglichen – so weit zurück wie nötig.

Schritt 6

Wiederherstellen gelöschter E-Mails

Die Verschlüsselung der E-Mails stellt Acme vor ein großes Problem – genau wie der Angreifer gehofft hatte. Leider macht Microsoft deutlich, dass eine Wiederherstellung nicht gewährleistet ist. Microsoft schreibt dazu: „In dem seltenen Fall, dass die Ransomware alle E-Mails in einem Postfach gelöscht hat, können Sie die gelöschten Elemente wahrscheinlich wiederherstellen“, und verweist dann auf weitere Ressourcen.

Mit Keepit:

Die Backups von Keepit stellen sicher, dass Unternehmen Daten auf jeden beliebigen Zeitpunkt und in jeder gewünschten Granularität wiederherstellen können – von einzelnen Elementen und Postfächern über ganze SharePoint-Websites und OneDrive-Repositories bis hin zu kompletten Tenants.

Schritt 7

Erneutes Aktivieren von Exchange ActiveSync und OneDrive-Synchronisierung

Nachdem die Endpunkte und anderen Geräte bereinigt und die Daten wiederhergestellt wurden, „können Sie Exchange ActiveSync und OneDrive-Synchronisierung erneut aktivieren“. Erst nach der Wiederherstellung und Synchronisierung – die leicht mehrere Tage in Anspruch nehmen kann –, kann das Acme-Team also auf seine Daten zugreifen und den Normalbetrieb zu einem gewissen Grad wiederherstellen.

Mit Keepit:

Wäre Acme ein Keepit-Kunde gewesen, hätten die Mitarbeiter und vertrauenswürdige Dritte die ganze Zeit über Zugriff auf die Daten gehabt. So hätten sie durchgehend eine gewisse Kontinuität aufrechterhalten und sowohl die IR- als auch DR-Maßnahmen leichter bewerkstelligen können.

Die wichtigsten Erkenntnisse

Für dieses Beispiel wurde Microsoft 365 gewählt, doch die gleichen Konzepte gelten auch für andere SaaS-Dienste (z. B. Google Workspace, Salesforce usw.). Egal, wer Ihr Anbieter ist und aus welchem Grund Sie auf Ihre Daten und Backups zugreifen müssen, sollten Sie deshalb bedenken:

Auf Daten zugreifen (d. h., sie lokalisieren und nutzen) zu können ist für ein Unternehmen in der Regel dringlicher als die vollständige Wiederherstellung (d. h. das Wiedereinspielen der Daten in die Dienste und Anwendungen).

„Wiederherstellung" bedeutet für den SaaS-Anbieter, dass er die Infrastruktur und die Anwendung wieder verfügbar macht – unabhängig davon, ob Ihre Daten dann vorhanden sind oder nicht.

Die Wiederherstellung kann leicht Tage, Wochen oder gar Monate in Anspruch nehmen.

Essentiell ist die Festlegung von Prioritäten für Benutzer oder Daten, die zuerst wiederhergestellt werden müssen, um die Betriebskontinuität zu gewährleisten. Mit granularen, priorisierten Wiederherstellungen können Unternehmen den Betrieb wieder aufnehmen, während die vollständige Wiederherstellung noch im Gange ist.

Daher brauchen Sie unbedingt eine Datenbackup-Lösung, die von der Infrastruktur des SaaS-Anbieters unabhängig ist, Benutzern bei Bedarf sofort Zugriff auf ihre Daten gibt, und eine schnelle, einfache und granulare Wiederherstellung der Daten in einem brauchbaren Format direkt in der Anwendung ermöglicht.

Risiken minimieren, Notfälle sicher bewältigen

Um Unternehmen vor Betriebsunterbrechungen aufgrund verlorener oder unzugänglicher SaaS-Daten zu schützen, hat Keepit eine dedizierte, anbieterneutrale SaaS Backup und Recovery-Lösung entwickelt. Eine Lösung, die resilient, sicher und benutzerfreundlich ist – denn was nützt Ihnen ein Backup, wenn Sie die gesuchten Daten nicht finden können oder die Wiederherstellung zu lange dauert?

Zudem ist die Lösung von Keepit schnell einsetzbar und bietet eine kalkulierbare All-Inclusive-Preisstruktur, die keinen Kapitaleinsatz erfordert. Sie können Ihr Backup also sofort in Betrieb nehmen.

Die Kontinuität aufrechterhalten

Keepit repliziert zwar nicht die Anwendung und ihre gesamte Funktionalität, stellt aber sicher, dass Ihre SaaS-Daten immer sofort und in einem verwendbaren Format verfügbar sind. So können Ihre Mitarbeiter weiterarbeiten, auch wenn Anwendungen und Dienste noch nicht laufen.

Die Administratoren können jedem Benutzer einen spezifischen Link zur Verfügung stellen, der ihm sicheren Zugriff auf alle Daten oder Teile davon (und bei Bedarf auch auf die Daten eines anderen Benutzers) aus der gesamten Backup-Historie gibt. Dabei können die Administratoren auch zusätzliche Sicherheitsmaßnahmen einbauen, zum Beispiel den Zugriff nur für eine konfigurierbare Zeitspanne gewähren.

Diese Vorgänge können über die Benutzeroberfläche ausgeführt werden. Für Disaster Recovery und andere umfangreiche Maßnahmen empfehlen wir jedoch, Skripte zu erstellen und die API zu verwenden.

Wiederherstellung von einem Backup

Keepit bietet bei der Wiederherstellung eine marktweit einzigartige Effizienz. Um Daten aus einem Backup wiederherzustellen, suchen Sie einfach die benötigten Daten oder navigieren zu ihnen und klicken dann auf „Wiederherstellen“. Daraufhin stehen alle Ihre Daten mit dem gesamten Verlauf auf einer modernen, webbasierten Benutzeroberfläche zur Verfügung. Diese bietet nicht nur Live-Browsen, sondern auch Vorschau, Download und Wiederherstellung Ihrer Datenelemente.

Und das war’s - weitere Schritte sind nicht erforderlich. Für schnelle und abgestufte Wiederherstellungsvorgänge (z.B. zuerst Geschäftsleitung und IT, dann Betriebsteams, dann Support usw.) können Sie die Datenwiederherstellung zudem über unsere API mit Skripten steuern, was noch mehr Effizienz und Anpassungsmöglichkeiten bietet.

Diese granulare, nach Prioritäten geordnete Wiederherstellung ist entscheidend für die Minimierung kostspieliger Ausfallzeiten und die Gewährleistung einer nahtlosen Betriebskontinuität. Unsere Software fügt sich damit nahtlos in Ihre bestehenden Disaster-Recovery-Prozesse und Ihren Betriebsablauf ein.

Keepit future proof

Take the next step toward protecting your SaaS data

Request a demo

Über Keepit

Keepit ist die weltweit einzige unabhängige, anbieterneutrale Cloud für den Schutz von SaaSDaten. Tausende von Unternehmen weltweit vertrauen auf Keepit, um ihre Cloud-Daten zu schützen und zu verwalten. Führende Analysten sind sich einig: Keepit ist die schnellste und sicherste SaaS-Lösung für Backups und Wiederherstellung in Unternehmen. Keepit – dedizierter SaaS-Datenschutz, auf den die Kunden bauen. Besuchen Sie keepit.com.

HQ – Copenhagen
Denmark
Keepit A/S
Per Henrik Lings Allé 4, 7.
2100 København, Denmark
CVR: 30806883
+45 8987 7792
sales@keepit.com

Dallas, Texas
United States
Keepit USA Inc.
3232 McKinney Avenue Suite 820
Dallas TX 75204, USA
TIN: 85-358 6335
+1 469-461-4892
sales@keepit.com

London
United Kingdom
Keepit Technologies UK, LTD.
Warnford Court
29, Throgmorton Street
London EC2N 2AT, UK
Company reg. no.: 13785045
sales@keepit.com

Munich
Germany
Keepit Germany GmbH
Maximiliansplatz 22
D-80333 München
Amtsgericht München,
HRB 270094
Geschäftsführer Morten Felsvang
sales@keepit.com

End notes

1 In January 2021, the United States' Cybersecurity and Infrastructure Security Agency (CISA) warned of the increasing threat, in Analysis Raeport (AR21-013A): Strengthening Security Configurations to Defend Against Attackers Targeting Cloud Services [CISA]

2 See Only 54% of organizations have a company-wide disaster recovery plan in place [Security Magazine]

3 Gartner, Assuming SaaS Applications Don't Require Backup Is Dangerous, Nik Simpson & Michael Hoeck, 5 August 2021

4 ESG 2023 Ransomware Preparedness: Lighting the way to readiness and mitigation

5 ESG, Technical Validation, Keepit: Dedicated Data Protection for SaaS Workloads, Kerry Dolan, October 2021

6 Research from Palo Alto suggests the average ransom in the first half of 2021 is $570,000 USD, an increase of 171% over the year prior; see Average Ransomware Payment Hits $570,000 in H1 2021 [Dark Reading]

7 Moschetta, et al., 2023. Cybersecurity in this era of polycrisis (https://www.weforum.org/agenda/2023/02/cybersecurity in an-era-of-polycrisis/)

8 Research from Check Point reports that ransomware incidents increased 93% year over year; see Ransomware

9 All excerpts from this page are as they appeared in October 2021

10 To learn more about this valuable feature—demonstrated with a short tutorial video—see Share data with a public link [Keepit]

11 In response to these developments, the United Kingdom's National Cyber Security Centre (NCSC) updated their malware guidance; see Updating our malware & ransomware guidance [NCSC]