top.media
IT von Meisterhand

Was Sie über Cloud-Anwendungen wissen müssen & wie Sie sie schützen

Software as a Service (SaaS) ist ein Cloud-basierter Dienst, der es Benutzern ermöglicht, über Online-Anwendungen auf alles zuzugreifen, was sie benötigen. Dies ermöglicht mehr Freiheit und Flexibilität als traditionellere Desktop-Anwendungen.

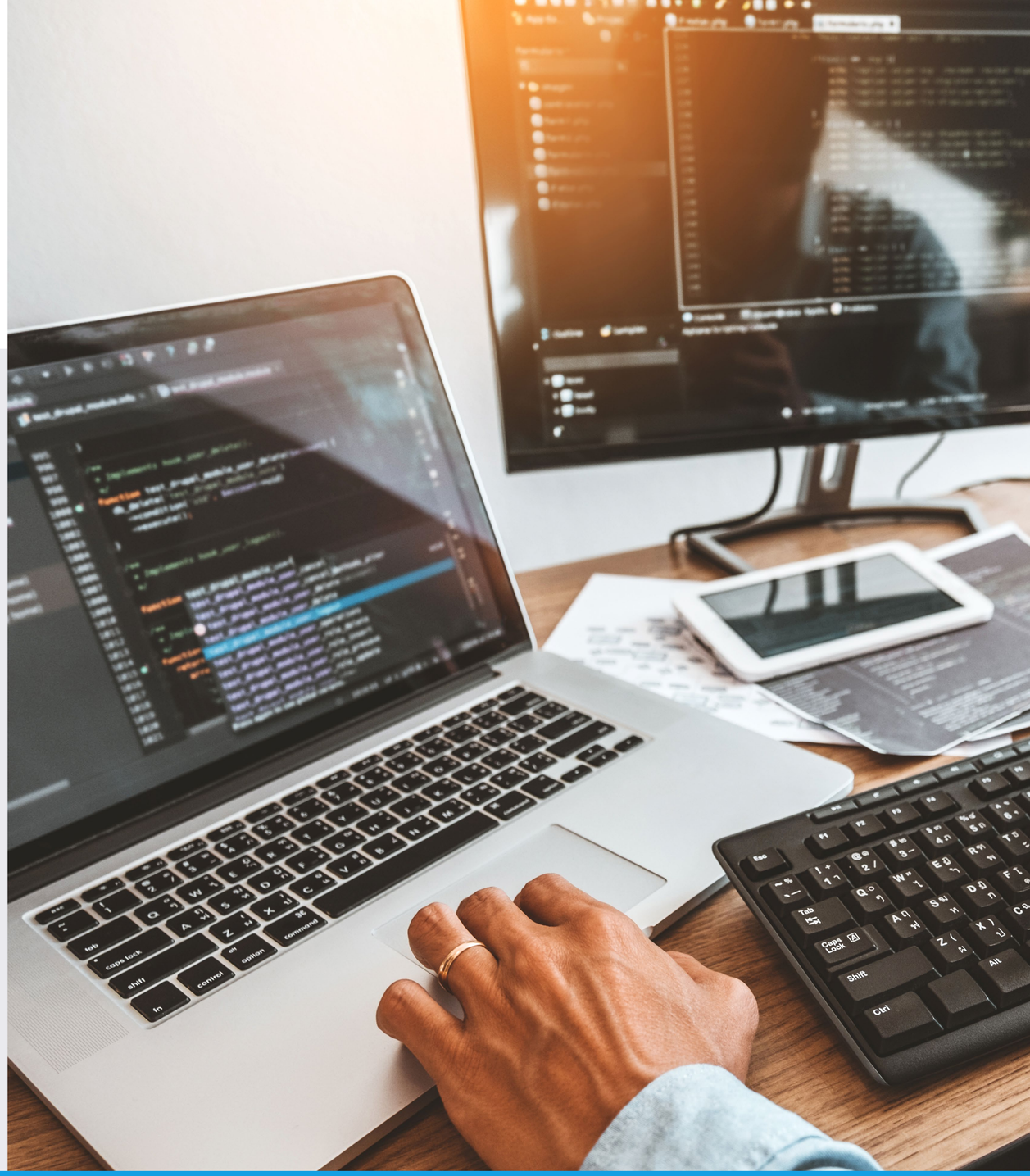
Die Akzeptanz von SaaS-Anwendungen ist mit der Zunahme von Home Office und Remote Work aufgrund der globalen COVID-Krise sprunghaft angestiegen. Doch auch schon zuvor – bevor Home Office für viele zur Norm wurde – boten Systeme zum einfachen Zugriff auf Dokumente von jedem Gerät aus offensichtliche Vorteile im Bereich der Kollaboration.

Microsoft 365, Google Workspace und andere Cloud-Anwendungen bieten Anwendern eine “always on”-Verfügbarkeit auf jedem Gerät, egal wo sie sich gerade befinden. Ein absoluter Gamechanger in Sachen Effizienz und Produktivität am Arbeitsplatz.

Aber nur, weil alle Daten in der Cloud gespeichert werden und leicht zugreifbar sind, bedeutet das nicht, dass auch automatische Backups von ihnen erstellt werden. Die genannten SaaS-Tools ersetzen keine Backups. Backups sind genauso wichtig für Daten, die in Cloud-Anwendungen gespeichert werden, wie für lokal gespeicherte Daten.

Aus diesem Grund bietet top.media einen umfassenden Schutz für Cloud-Anwendungen.

Lesen Sie weiter – wir entlarven gängige SaaS-Mythen und zeigen Ihnen, warum SaaS-Backups unerlässlich für Ihr Unternehmenswachstum und Ihren langfristigen Erfolg sind.



Häufig vorkommende SaaS-Mythen und -Missverständnisse

top.media
IT von Meisterhand

“Cloud-Anwendungen brauchen keine Backups”

SaaS-Anwendungen verfügen zwar über eine eingebaute Redundanz, die vor Datenverlusten in den Cloud-Servern schützt – diese schützt aber nicht vor üblichen Faktoren wie:

- Benutzerfehler
- Versehentliche oder böswillige Löschung
- Ransomware-Angriffe

Während das versehentliche Löschen von Dateien die bei weitem häufigste Form des Datenverlusts bei SaaS-Anwendungen ist, kann Ransomware den größten Schaden anrichten. Das liegt daran, dass Ransomware darauf ausgelegt ist, sich über Netzwerke und in Cloud-Anwendungen zu verbreiten und viele Benutzer zu schädigen.

Ransomware ist kein rein lokales Problem. Sie kann sich ebenso in SaaS-Anwendungen ausbreiten – und tut dies auch. Unternehmen benötigen eine Möglichkeit, Dateien, Ordner, Einstellungen und Berechtigungen im Falle eines Angriffs schnell wiederherzustellen.

“Dateisynchronisierung ersetzt Backups”

Tools wie Microsoft OneDrive oder Google Drive erstellen zwar eine zweite Kopie von Daten und Ordnern, sind aber kein Ersatz für Backups. Bei der Dateisynchronisierung werden Veränderungen der Dateien automatisch auf die synchronisierten Dateien kopiert. Wenn also eine Datei oder ein Ordner mit Ransomware infiziert ist, wird die Malware automatisch auf alle synchronisierten Versionen dieser Datei kopiert.

Dateisynchronisationsdienste bieten zwar einige Wiederherstellungsfunktionen über die Versionierung, aber sie reichen nicht an eine echte SaaS-Backup-Lösung heran.

Und hier sind die Gründe:

- Versionen sind keine unveränderlichen Wiederherstellungspunkte. Wenn also eine Datei gelöscht wird, werden auch ältere Versionen der Datei gelöscht.

- Die Versionierung ermöglicht keine zentrale Verwaltung der Benutzerdaten. Mit anderen Worten: Sie haben keine Kontrolle über Backups und Wiederherstellung.

- Bei der Versionierung werden Wiederherstellungspunkte nicht über Dateien, Ordner, Einstellungen und Benutzer hinweg beibehalten. Wenn Sie nur ein paar Dateien wiederherstellen müssen, ist das keine große Sache. Aber große Wiederherstellungen sind ein zeitaufwendiger, manueller Prozess.

Häufig vorkommende SaaS-Mythen und -Missverständnisse

top.media
IT von Meisterhand

“Cloud-Anwendungen sind immer verfügbar”

Obwohl Cloud-Anwendungen sehr zuverlässig sind, kann es auch mal zu Ausfällen kommen. Im April 2021 erlebte Microsoft einen riesigen Cloud-Ausfall, der die meisten seiner Internetdienste offline nahm. Und erst kürzlich betraf ein massiver Google-Ausfall fast eine Milliarde Gmail-, Google Workspace- und YouTube-Benutzer.

Ausfälle und langsame Wiederherstellungszeiten sind nicht bloß "unangenehm" oder "lästig". Wenn Unternehmen nicht auf wichtige Geschäftsdaten zugreifen können, sinkt die Produktivität, und damit wird auch der Umsatz beeinträchtigt. Die Erstellung von Backups, die unabhängig von den Cloud-Servern eines SaaS-Anbieters sind, ist die einzige Möglichkeit, den Zugriff auf wichtige Dateien im Falle eines Ausfalls sicherzustellen.

“Microsoft und Google sind für Backups verantwortlich”

Cloud-Anbieter stellen mit eingebauter Redundanz und anderen Maßnahmen für hohe Verfügbarkeit sicher, dass Sie Ihre Cloud-Daten nicht verlieren. Allerdings übernehmen sie nicht die Verantwortung für die Wiederherstellung von Daten, wenn Sie diese selbst verlieren. Microsoft nennt dies das "Shared Responsibility Model" für Datensicherheit. Aus diesem Grund empfiehlt Microsoft in seiner Nutzungsvereinbarung die Sicherung von SaaS-Daten durch Dritte.

Das Shared Responsibility Model:

Das Shared Responsibility Model legt die Last des Datenschutzes direkt auf Unternehmen, die sich auf SaaS-Dienste verlassen. Cloud-Anbieter sind dafür verantwortlich, ihre Infrastruktur am Laufen zu halten, aber Unternehmen sind für den Erhalt und die Sicherheit ihrer Daten verantwortlich.

Die richtige Cloud-Backup-Lösung für Ihr Unternehmen wählen

top.media
IT von Meisterhand

Aufgrund der zahlreichen Produkte auf dem Markt ist es für Unternehmen äußerst schwierig, die richtige Lösung für ihre speziellen Anforderungen zu finden.

Hier sind einige Schlüsselfaktoren, auf die Sie unbedingt achten sollten:

Umfassender Schutz

Manche SaaS-Backup-Lösungen schützen nur E-Mails, Dateien und Ordner. Es gibt aber auch Lösungen, die Ihr Unternehmen viel umfassender absichern.

Wenn Sie ein Cloud-Backup-Tool wählen, achten Sie darauf, dass es auch Schutz für Kontakte, Shared-Drive-Ordner sowie Kollaborations- und Chat-Tools und Kalender bietet. Cloud-Sicherheitslösungen, die dieses Ausmaß an Abdeckung bieten, sind bei der Aufrechterhaltung der Geschäftskontinuität wesentlich effektiver als weniger robuste Anbieter.

RPO/RTO

Auch Recovery Point Objective (RPO) und Recovery Time Objective (RTO) sollten Sie in Ihre Entscheidung mit einbeziehen. Diese Metriken beziehen sich auf den Zeitpunkt, zu dem Sie wiederherstellen können, bzw. wie schnell Sie eine Wiederherstellung durchführen können. Bei SaaS-Backups werden diese Werte weitgehend von der Häufigkeit der Backups und den zu sichernden Daten bestimmt.

Lösungen, die häufige Backups anbieten, adressieren den RPO, da sie die Wiederherstellung zu einem aktuellen Zeitpunkt ermöglichen und so den Datenverlust minimieren. Wie bereits erwähnt, machen diese die Wiederherstellung schneller und einfacher, indem sie den manuellen Aufwand zur Durchführung von Wiederherstellungen reduzieren.

Sicherheit & Compliance

Jedes Unternehmen – ob groß oder klein – muss sich an strenge Datenschutzbestimmungen halten. Deshalb ist es essentiell wichtig, eine Cloud-Sicherheitslösung zu wählen, die diesen Bestimmungen entspricht.

Stellen Sie sicher, dass Ihre Lösung alle Grundlagen abdeckt und keine Ihrer kritischen Daten durch Schlupflöcher angegriffen werden können.

Warum lohnt sich ein SaaS-Schutz?

top.media
IT von Meisterhand

top.media arbeitet nur mit den besten Drittanbietern zusammen, um sicherzustellen, dass unsere Kunden Zugang zu den innovativsten Lösungen auf dem Markt haben.

Wir wissen, wie wichtig es für Unternehmen ist, sich auf die Sicherheit ihrer Daten verlassen zu können. Deshalb speichern wir alle Daten in EU-Datenzentren, um den Cloud-Schutz für unsere Kunden effizient verwalten und aufrechterhalten zu können.

Der von uns angebotene SaaS-Schutz ist eine Cloud-to-Cloud-Backup-Lösung, die eine umfassende Sicherung und Wiederherstellung von kritischen Cloud-Daten in Microsoft 365 und Google Workspace ermöglicht.

Er schützt vor dauerhaftem Datenverlust, was es uns ermöglicht, die Daten unserer Kunden nach einem Ransomware-Angriff mit täglichen Point-in-Time-Backups einfach wiederherzustellen. Die Backups werden sicher in der Cloud gespeichert, mit intakten Dateien, Ordnern, Einstellungen und Berechtigungen für eine schnelle Wiederherstellung, egal ob ein einzelnes Element oder ein ganzes Benutzerkonto wiederhergestellt werden soll.

Microsoft

- **Exchange**
- **Tasks**
- **OneDrive**
- **SharePoint**
- **Teams**

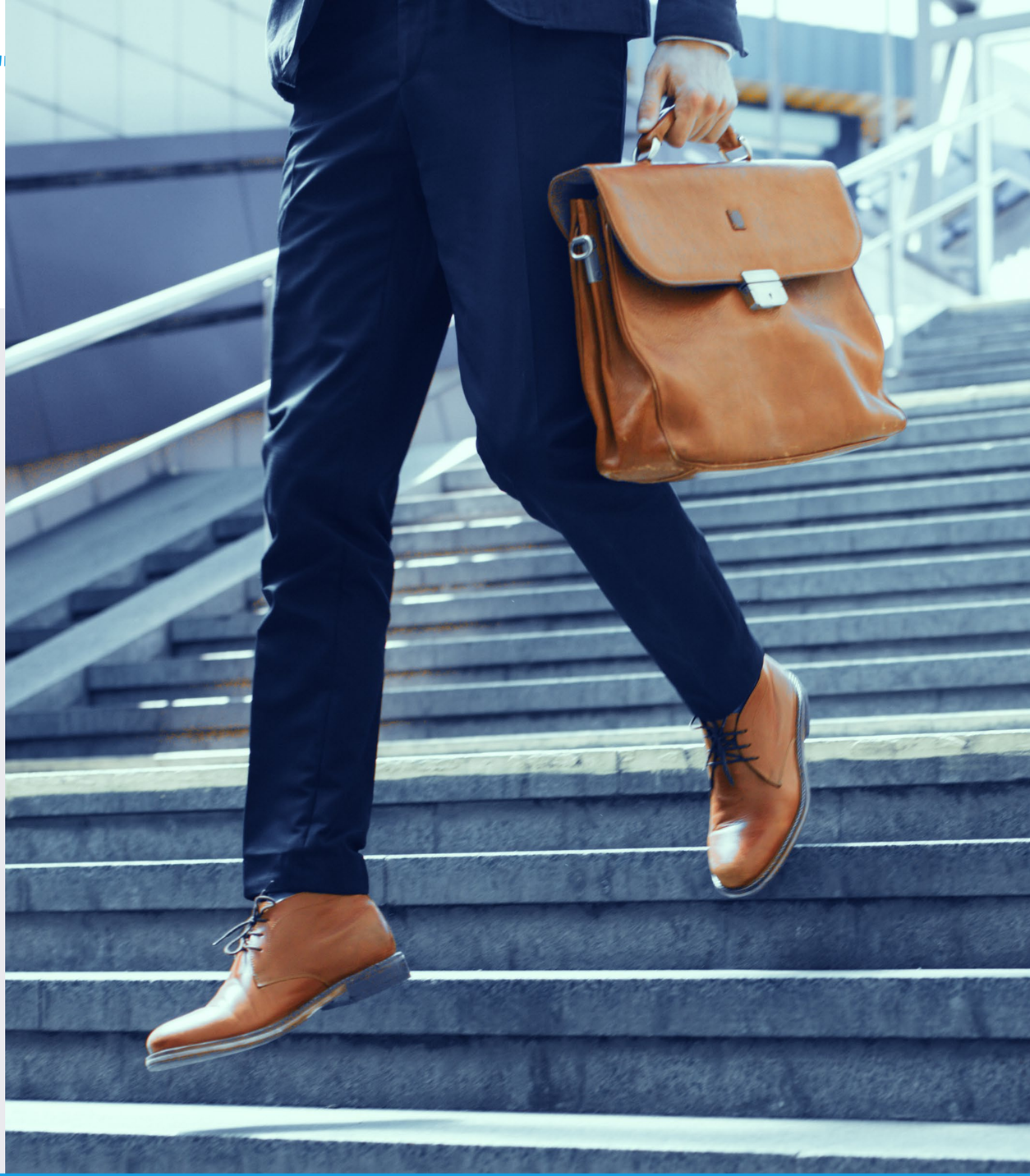
Google Workspace

- **Gmail**
- **Google Docs**
- **Calender**
- **Contacts**
- **Shared Drives**

Ihre nächsten Schritte

Unser Expertenteam bei top.media kann Ihr Unternehmen dabei unterstützen, erfolgreich zu sein. Ob zu Hause, im Büro oder unterwegs - wir sorgen dafür, dass Ihr gesamtes Team sicher auf alles zugreifen kann, was benötigt wird.

- top.media beschäftigt sich bereits seit mehr als 20 Jahren mit Daten-Backups.
- Wir sichern Ihre Daten in EU-Datenzentren, wo wir sie im Augen behalten und sicherstellen können, dass sie sich in sicheren Händen befinden.
- Unseren Kunden bieten wir stets die besten, vertrauenswürdigsten Lösungen, die speziell auf ihre Anforderungen zugeschnitten sind.



top.media
IT von Meisterhand

Fangen Sie noch heute an,
Ihre Daten besser zu schützen.

info@topmedia.de
www.top.media/kontakt

Buchen Sie Ihr kostenloses Beratungsgespräch