

JENSEITS DER CLOUD:
HYBRIDE BACKUPS
für mehr Datenresilienz bei KMUs

Schutz von Kundendaten, Datenverlustrisiken minimieren und Vertrauen durch intelligente Backup-Strategien schaffen: Ein praktischer Leitfaden für MSP.



INHALT

WARUM CLOUD-BACKUP FÜR KMU SO ATTRAKTIV IST	4
DIE 5 GRÖSSTEN MYTHEN RUND UM CLOUD-BACKUPS, DIE KMU SCHADEN	5
RISIKEN EINER AUSSCHLIESSLICH CLOUDBASIERTEN BACKUP- STRATEGIE	7
IST EINE HYBRIDE BACKUP-STRATEGIE DIE LÖSUNG FÜR KMUS?	10
BACKUP-TESTS & VERIFIZIERUNG	11
KOSTENÜBERLEGUNGEN UND ROI	14
PRAXISBEISPIEL: WIEDERHERSTELLUNG BEI EINEM KMU	16
SORGENFREIE DATENSICHERUNG	17
ÜBER NOVABACKUP	18



Cloud-Backup ist ein wichtiger Bestandteil der Backup-Strategien kleiner und mittlerer Unternehmen (KMU). Auch Managed Service Provider (MSPs), die KMU betreuen, setzen darauf. Der enorme Anstieg der Nutzung von Cloud-Speichern für Backups in den letzten beiden Jahren zeigt, wie essenziell cloudbasierte Datensicherung geworden ist.

Laut unseren Daten setzen KMU immer stärker auf Cloud-Backups: Von August 2023 bis August 2025 stieg die Nutzung um 91,6 %.

Beliebtheit allein garantiert keine Perfektion. Cloud-Speicher bietet Vorteile wie externen Zugriff, Flexibilität und Skalierbarkeit. Dennoch gibt es Fallstricke, die Unternehmen beachten sollten, etwa Compliance-Herausforderungen, langsamere Wiederherstellungen und die Abhängigkeit von Drittanbietern.

In diesem Leitfaden klären wir häufige Missverständnisse und zeigen die größten Risiken von Cloud-Only-Backups auf. Zudem erfahren Sie, wie **hybride Backup-Strategien** für Ihr Unternehmen und Ihre Kunden ein robustes, widerstandsfähiges Datenmanagement ermöglichen.





WARUM CLOUD-BACKUP FÜR KMU SO ATTRAKTIV IST

Für KMU bietet Cloud-Backup eine attraktive Mischung aus Kosteneinsparungen, Flexibilität und einfacher Bedienung. Im Gegensatz zu herkömmlichen Backup-Lösungen, die oft teure lokale Infrastruktur und laufende Wartungskosten erfordern, ermöglichen Cloud-Dienste eine unternehmensweite Datensicherung ohne hohe Anfangsinvestitionen.

Hier sind die Gründe, warum sich so viele Unternehmen für die Cloud entscheiden:

- **Lokale Hardwareverwaltung entfällt:** Der Bedarf an dedizierten Servern, Backup-Geräten oder komplexer Netzwerktechnik entfällt.
- **Kalkulierbare monatliche Kosten:** Abonnementbasierte Preise erleichtern die Budgetierung und Skalierung.
- **Remote-Zugriff:** Backups sind von überall mit Internetzugang erreichbar – ideal für Remote- oder Hybrid-Arbeit.
- **Skalierbarer Speicher:** Der Speicherplatz wächst mit den Daten, ohne dass die physische Infrastruktur aufgerüstet werden muss.
- **Automatisierte Prozesse:** Viele Services bieten geplante Backups, die das IT-Management vereinfachen.

Für zeitlich eingeschränkte KMU mit wenig IT-Personal sind diese Vorteile verständlicherweise verlockend. Allerdings kann die scheinbare Bequemlichkeit ein trügerisches Sicherheitsgefühl erzeugen. Viele gehen fälschlicherweise davon aus, dass Daten allein durch die Speicherung in der Cloud vollständig geschützt sind – doch das ist nicht immer der Fall. Eine zu starke Fokussierung auf die Cloud kann Unternehmen anfällig für Datenverlust, Compliance-Verletzungen und lange Wiederherstellungszeiten machen.

Tipp für MSPs

Erinnern Sie Ihre Kunden daran, dass Cloud-Backups zwar kalkulierbare Kosten und einen geringeren IT-Aufwand bieten, eine sorgfältige Backup-Planung jedoch nicht ersetzen.



DIE 5 GRÖSSTEN MYTHEN RUND UM CLOUD-BACKUPS, DIE KMU SCHADEN

Cloud-Backup wird oft überhyped, sodass KMU glauben, es handle sich um eine „Set-and-forget“-Lösung. Als vertrauenswürdiger IT-Berater wissen Sie jedoch, dass die Realität deutlich komplexer ist. In diesem Leitfaden räumen wir mit den fünf häufigsten Vorurteilen rund um Cloud-Backup auf und zeigen auf, was sie für Ihre Kunden tatsächlich bedeuten.

Vorurteil Nr. 1: „Die Cloud ist zu 100 % sicher.“

Die Wahrheit: Auch wenn Cloud-Anbieter eine robuste Infrastruktur bieten, hängt die Datensicherheit letztlich von den Schutzmaßnahmen ab, die ein Unternehmen selbst umsetzt. Um Backups vor Cyberangriffen zu schützen, sind interne Maßnahmen wie Zugriffskontrollen, Multi-Faktor-Authentifizierung (MFA) und Verschlüsselung unerlässlich.

Vorurteil Nr. 2: „Der Anbieter regelt alles.“

Die Wahrheit: Viele KMU gehen davon aus, dass ihr Cloud-Backup-Anbieter die gesamte Verantwortung für die Datensicherheit übernimmt. Tatsächlich arbeiten die meisten jedoch nach einem Modell der geteilten Verantwortung. Das bedeutet, dass sie selbst für die Konfiguration von Sicherheitseinstellungen, die Überwachung der Backups und die Verifizierung der Wiederherstellungen verantwortlich sind.

Vorurteil Nr. 3: „Alle Cloud-Dienste sind gleich.“

Die Wahrheit: Nicht alle Anbieter sind gleich. Manche Cloud-Dienste konzentrieren sich auf Dateisynchronisierung, andere auf aktive Datenspeicherung, und wieder andere bieten Backups mit Versionierung, Verschlüsselung und Disaster-Recovery-Funktionen. Prüfen Sie daher stets die Details, testen Sie die Anbindung und machen Sie sich genau mit den Leistungen vertraut, bevor Sie einem Anbieter Ihre Daten anvertrauen.

Vorurteil Nr. 4: „Externe Festplatten und NAS sind überflüssig.“

Die Wahrheit: Cloud- und lokale Backups ergänzen sich, statt zu konkurrieren. Während Cloud-Backups die Wiederherstellung nach lokalen Katastrophen wie Feuer oder Überschwemmungen sichern, ermöglichen externe Festplatten und NAS-Geräte eine besonders schnelle Wiederherstellung großer Dateien, Images und ganzer Server.

Für eine schnelle Wiederherstellung empfiehlt es sich, mindestens eine Kopie lokal auf einer Festplatte oder einem NAS zu behalten. Zusätzlich sollte eine Kopie in der Cloud als externe Sicherung aufbewahrt werden.

VERWENDEN SIE DIE 3-2-1-BACKUP-STRATEGIE



Vorurteil Nr. 5: „Cloud-Backup = Disaster Recovery“

Die Wahrheit: Cloud-Backups bilden nur einen Teil des Disaster Recovery. Effektive Disaster-Recovery-Pläne für KMU setzen klar definierte Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) voraus. Verlassen sich Unternehmen ausschließlich auf Cloud-Backups, um den Geschäftsbetrieb im Notfall aufrechtzuerhalten, riskieren sie längere Ausfallzeiten.

RISIKEN EINER AUSSCHLIESSLICH CLOUDBASierten BACKUP-STRATEGIE

Nachdem die größten Mythen zum Cloud-Backup entkräftet sind, betrachten wir nun die Risiken einer rein cloudbasierten Strategie. Die Cloud ist zwar praktisch, doch wenn Unternehmen ausschließlich darauf setzen, werden KMU anfällig für Störungen. Dazu zählen plötzliche Ausfälle, Verzögerungen bei der Wiederherstellung kritischer Daten und Compliance-Probleme, die Geldstrafen oder Sanktionen nach sich ziehen können.

Die wichtigsten Risiken sind:

Cloud-Ausfälle

Auch große Anbieter wie AWS, Microsoft Azure und Google Cloud können durch Netzwerkprobleme, Software-Fehlkonfigurationen oder DNS-Probleme regional oder global ausfallen.

Existieren unternehmenskritische Daten ausschließlich in der Cloud, können Ausfälle den Betrieb lahmlegen. KMU haben dann keinen Zugriff auf kritische Dateien oder Systeme. Schon kurze Ausfallzeiten können den Betrieb stoppen, den Kundenservice verzögern und Gehalts- oder Rechnungsprozesse blockieren.

Datenlecks und Cyber-Sicherheitsrisiken

Cloud-Anbieter gewährleisten zwar eine starke Infrastruktur-Sicherheit, doch Backup-Dateien können durch gestohlene Zugangsdaten, API-Schwachstellen oder falsch konfigurierte Zugriffskontrollen gefährdet werden.

Sind die Zugangskontrollen schwach oder die Verschlüsselung falsch umgesetzt, können Angreifer wichtige Geschäftsdaten beschädigen oder sperren. Das kann zu Umsatzverlust, Reputationsschäden oder Betriebsstillstand führen.

Lösungen mit **MFA, rollenbasierter Zugriffskontrolle (RBAC), clientseitiger Verschlüsselung** und **unveränderlichem Speicher** oder **unveränderlichen Backups** reduzieren das Risiko, da Backup-Daten für Cyberkriminelle schwerer zugänglich oder manipulierbar sind.

Cloud-Speicher vs. Cloud-Backup

Das Kopieren von Backup-Dateien in herkömmliche Cloud-Speicher oder Dateisynchronisationsdienste wie OneDrive, Google Drive oder Dropbox unterscheidet sich von einem dedizierten Backup.

Regulärer Cloud-Speicher kann:

- mehreren Nutzern Zugriff gewähren, wodurch das Risiko versehentlicher Löschungen oder Ransomware-Angriffe steigt,
- keine backup-spezifische Verschlüsselung oder Unveränderlichkeit bieten,
- nur eingeschränkte Versionierungs- oder Wiederherstellungsfunktionen bereitstellen.

Eine echte Cloud-Backup-Lösung speichert Dateien isoliert, verringert die Anzahl potenzieller Angriffsflächen und stellt sicher, dass ein Unternehmen seine Daten im Bedarfsfall zuverlässig wiederherstellen kann.

Mehr über die Unterschiede zwischen Dateisynchronisationsdiensten und Cloud-Backups erfahren Sie in unserem Blogbeitrag.

[Lesen Sie hier weiter.](#)

Compliance-Anforderungen

KMU, die besonderen Vorschriften unterliegen, müssen branchenspezifische Standards wie die DSGVO, PCI-DSS oder §75B SGBV im Gesundheitswesen einhalten. Diese Regeln legen fest, wie Daten gespeichert, verschlüsselt, geprüft und gelöscht werden müssen.

Beispiele:

- Die **DSGVO** schreibt u. a. bestimmte Speicherorte, Löschfristen und die Möglichkeit zur Datenlöschung vor.
- **Branchenspezifische Regelungen** im Gesundheitswesen verlangen z. B. verschlüsselte Speicherung, sichere Authentifizierung und regelmäßige Backups sensibler Daten.

Ohne eine Datensicherungslösung, die diese Anforderungen erfüllt, riskieren KMU gescheiterte Audits, Strafzahlungen oder sogar vorübergehende Betriebsschließungen.

Alltägliche Herausforderungen für KMU

Für kleine Unternehmen sind nicht nur katastrophale Ereignisse, sondern auch alltägliche Probleme mit reinen Cloud-Backups eine Herausforderung.

- **Langsame Wiederherstellungen:** Die Wiederherstellung großer Datenmengen über das Internet kann je nach Dateigröße und Bandbreite Stunden oder Tage dauern.
- **Begrenzter Support:** Automatisierte oder E-Mail-basierte Hilfe kann in dringenden Situationen frustrierend sein. Schneller, kompetenter Support ist selten, aber entscheidend.
- **Unerwartete Kosten:** Manche Anbieter berechnen extra für Wiederherstellungen, Datentransfers, mehrere Versionen oder Speicherüberschreitungen, sodass ein günstiger Plan schnell zur Kostenfalle wird.



Tipp für MSPs

Erklären Sie Ihren Kunden, dass reine Cloud-Backups bei Ausfällen zu Downtime führen und die Daten ohne passende Schutzmaßnahmen gefährdet sind. Ein kombinierter Ansatz mit Verschlüsselung, MFA und rollenbasierter Zugriffskontrolle erhöht die Sicherheit erheblich.

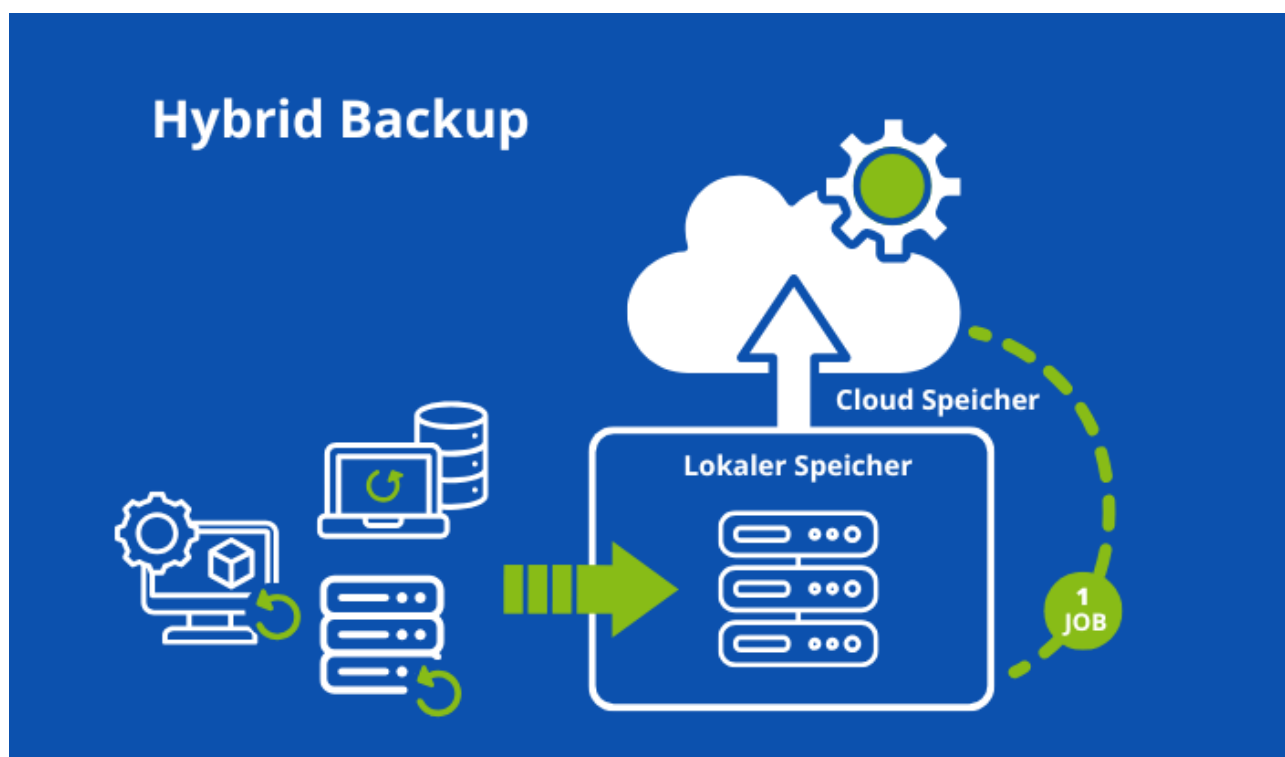
IST EINE HYBRIDE BACKUP-STRATEGIE DIE LÖSUNG FÜR KMUS?

Die zuvor aufgezeigten Risiken zeigen, wie verwundbar KMU bei reinen Cloud-Backups sind. Eine hybride Strategie, die lokale Backups für schnelle Wiederherstellungen und Cloud-Backups für maximale Resilienz kombiniert, reduziert diese Risiken deutlich.

Kritische Workloads wie SQL-Datenbanken, virtuelle Maschinen und geschäftskritische Anwendungen lassen sich über lokale Backups schnell wiederherstellen. Ergänzende Cloud-Backups sichern die Daten extern und schützen sie vor Feuer, Flut, Diebstahl oder anderen Katastrophen am Standort.

Vorschriften und Branchenstandards verlangen häufig, dass Unternehmen mehrere Kopien kritischer Daten aufbewahren, mindestens eine davon außer Haus. Hybrid-Backups unterstützen diese Anforderungen und geben KMU die Kontrolle über Backup-Frequenz, Aufbewahrungsrichtlinien und Wiederherstellungsziele.

Kurz gesagt: Sie bieten Betriebsresilienz, Compliance und kosteneffiziente Flexibilität, und das ganz ohne komplexe IT-Ressourcen.



Die Vorteile eines hybriden Ansatzes für KMU sind hier zusammengefasst:

- ✓ **Schnellere Wiederherstellung:** Lokale Backups ermöglichen eine schnelle Wiederherstellung von Dateien, Datenbanken und Anwendungen und minimieren so die Downtime.
- ✓ **Externer Schutz:** Cloud-Backups bieten im Falle von Feuer, Flut, Diebstahl oder anderen Katastrophen am Hauptstandort ein sicheres Backup.
- ✓ **Redundanz:** Kopien an beiden Standorten stellen sicher, dass der Ausfall eines Systems keinen Datenverlust bedeutet.
- ✓ **Individuelle Kontrolle:** Hybrid-Backups erlauben die Feinabstimmung von Zeitplänen, Aufbewahrungsrichtlinien und Wiederherstellungseinstellungen je nach Wert und Sensibilität der Daten.
- ✓ **Compliance-Unterstützung:** Durch die Kombination aus Verschlüsselung, Zugriffskontrolle und auditfähigen Logs helfen hybride Lösungen KMU dabei, regulatorische Anforderungen zu erfüllen, ohne dass ein komplizierter IT-Overhead entsteht.



Backup-Tests & Verifizierung

Selbst die beste Backup-Strategie ist nutzlos, wenn sich die Daten nicht wiederherstellen lassen. Testen Sie daher regelmäßig die Wiederherstellung von lokalen und Cloud-Backups, um sicherzustellen, dass die Dateien vollständig und zugänglich sind.

Als IT-Dienstleister unterstützen Sie Ihre Kunden mit folgenden Leistungen:

- Regelmäßige Test-Wiederherstellungen von Dateien, Ordnern oder kompletten Systemen
- Verifizierung der Integrität von lokalen und Cloud-Backup-Kopien
- Protokollierung der Ergebnisse, um Probleme vor katastrophalen Datenverlusten zu erkennen

So wählen KMU die richtige hybride Backup-Lösung

Hybride Backup-Lösungen unterscheiden sich stark. Vergleichen Sie Anbieter anhand folgender Kriterien, um Ihre Kunden bestmöglich abzusichern.

Bietet das hybride Setup eine einfache Einrichtung und nahtlose Integration?

Die besten Lösungen speichern Daten zunächst lokal, um eine schnelle Wiederherstellung zu ermöglichen, und übertragen sie dann automatisch in die Cloud, sodass ein externer Schutz gewährleistet ist – alles in einem einzigen, leicht zu verwaltenden Vorgang ohne komplizierte Konfigurationen.

Werden Backups bei der Übertragung und im Ruhezustand verschlüsselt?

Eine starke Verschlüsselung schützt die Daten vor Cyber-Bedrohungen sowohl während der Übertragung als auch bei der Speicherung.

Lassen sich die Aufbewahrungsfristen für lokale und Cloud-Kopien leicht anpassen?

Suchen Sie nach Lösungen, die unterschiedliche Aufbewahrungsfristen für lokale und Cloud-Speicherung ermöglichen, beispielsweise 30 Tage lokal für schnellen Zugriff und 60 Tage in der Cloud für langfristigen Schutz. So vermeiden Sie die parallele Verwaltung mehrerer Backup-Jobs.



Ist technischer Support inklusive und reaktionsschnell?

Für MSPs, die Kundendaten schützen und Ausfallzeiten minimieren müssen, ist schneller Support entscheidend. Achten Sie auf Anbieter, die Live-Hilfe bieten, statt nur automatisierte E-Mail-Antworten. So können Sie Probleme direkt lösen und Ihre Kunden optimal betreuen.

Werden die Compliance-Anforderungen Ihrer Kunden erfüllt?

Stellen Sie sicher, dass die Lösung die für Ihre Kunden relevanten Vorschriften unterstützt, z. B. die DSGVO, branchenspezifische Standards wie PCI-DSS oder § 75B SGBV im Gesundheitswesen.

Wie schnell und einfach lassen sich Daten wiederherstellen?

Die besten hybriden Lösungen erkennen automatisch den schnellsten Weg zur Wiederherstellung: lokal für Sofortzugriff oder aus der Cloud, falls die lokale Kopie fehlt. KMU sollten sich keine Gedanken darüber machen müssen, wo ein Backup liegt. Die Software findet die neueste Version und stellt sie mit minimaler Downtime wieder her.

Lässt sich der Backup-Status Ihrer Kunden zentral überwachen?

Mit übersichtlichen Dashboards und automatisierten Berichten behalten Sie alle Backups im Blick, erkennen Probleme frühzeitig und können Ihre Kunden proaktiv beraten – für mehr Sicherheit und Vertrauen.

Die besten hybriden Backup-Lösungen bieten mehr als nur Datensicherung. Sie gewährleisten eine schnelle und zuverlässige Wiederherstellung und vereinfachen das Backup-Management.

Tipp für MSPs

Da Sie für die Backups Ihrer Kunden verantwortlich sind, sollten Sie hervorheben, wie Ihre Dienstleistung Zeit und Geld spart und im Falle eines Datenverlusts für Sicherheit sorgt.



Kostenüberlegungen und ROI

Als MSP können Sie Ihren Kunden die finanziellen Vorteile hybrider Backups aufzeigen. Auch wenn eine zusätzliche lokale Sicherung zunächst nach Mehraufwand aussieht, lässt sich dadurch langfristig Geld sparen.

- **Schnellere Wiederherstellungen verringern die Ausfallzeit:** Eine schnelle Wiederherstellung aus lokalem Speicher minimiert Betriebsverluste.
- **Schwerwiegende Wiederherstellungskosten vermeiden:** Mehrere Kopien garantieren eine Datenwiederherstellung in jedem Szenario.
- **Optimierte Speicheraufteilung: Häufig genutzte Dateien bleiben lokal, ältere Informationen werden sicher in der Cloud gespeichert.**

Durch solche Berechnungen verstehen KMU Backups als Investition, nicht nur als Kostenfaktor.

Nach einem erfolgreichen Cyberangriff muss fast jedes fünfte KMU das Geschäft schließen.

Doch unabhängig vom Angriff kann der Verlust wichtiger Geschäftsdaten verheerende Folgen haben – ganz gleich, aus welchem Grund die Daten verloren gingen. Fragen Sie Ihre Kunden: Was würde passieren, wenn sie auf ihre wichtigsten Informationen einen Tag, eine Woche oder länger keinen Zugriff hätten?

Der Vergleich zeigt, wie lokale, cloudbasierte und hybride Ansätze abschneiden und warum das hybride Backup die beste Kombination aus Geschwindigkeit, Schutz und ROI bietet.

	Nur lokal 	Nur Cloud 	Hybrid 
Anschaffungskosten	Mittel (500–2.000 €)	Niedrig	Mittel + Anbieter-Gebühren
Jährliche Kosten	Niedrig	Mittel–Hoch (1.000–5.000+ €)	Mittel–Hoch (1.000–5.000+ €)
Wiederherstellungsgeschwindigkeit	● Sehr schnell	● Abhängig von Bandbreite	● Schnell (lokal) + ● Zuverlässig (Cloud-Fallback)
Sicherheit/ Compliance	● Mittel	● Mittel–Hoch	● Hoch (Verschlüsselung + isolierte Backups)
Risiko Datenverlust	● Mittel–Hoch	● Mittel	● Niedrig
Verwaltungsaufwand	● Manuelle Einrichtung & Überwachung	● Meist automatisiert	● Automatisiert + Einzeljob für lokal + Cloud
ROI/ Auswirkungen auf das Geschäft	● Mittel Die laufenden Kosten sind gering, allerdings ist das Risiko hoch und der Schutz außerhalb des Standorts begrenzt. Eine manuelle Verwaltung ist möglicherweise erforderlich.	● Mittel Die Skalierung ist einfach, Offsite-Schutz ist inklusive, aber die Wiederherstellung und Compliance können bei großen Datenmengen eine Herausforderung darstellen.	● Hoch Kombiniert schnelle Wiederherstellung mit Offsite-Schutz, erfüllt gesetzliche Anforderungen und reduziert das Risiko von Ausfallzeiten. Der ROI ist hoch, da Ausfallzeiten minimiert, die Wiederherstellung beschleunigt und Kosten durch Datenverlust vermieden werden.

Tipp für MSPs

Verwenden Sie Kostenvergleiche wie diesen, um Ihren Kunden zu verdeutlichen, dass Backups nicht nur Ausgaben darstellen, sondern eine wertvolle Investition in die Sicherheit und Kontinuität ihres Geschäftsbetriebs sind.

PRAXISBEISPIEL: WIEDERHERSTELLUNG BEI EINEM KMU

Im Nordosten von Texas sind Tornados und plötzliche Stromausfälle keine Seltenheit. Dort kann eine schnelle Datenwiederherstellung den Unterschied zwischen einer kleinen Panne und einer größeren Störung ausmachen.

Tony Linton, Inhaber von TLC Netcon Inc., erinnert sich an einen Kunden, dessen Festplatte komplett ausgefallen war. „Sie war nicht mehr wiederherstellbar. Dank NovaBACKUP hatten wir ein zuverlässiges Backup. Ich gab dem Kunden den Verschlüsselungs-Key und wir konnten seine Daten sehr schnell wiederherstellen.“



Für Tonys KMU-Kunden ist Managed Backup mehr als nur ein Zusatzservice. Es ist ein zuverlässiger Schutz. Er überwacht, verwaltet und aktualisiert Backups, sodass sich seine Kunden auf ihr Geschäft konzentrieren können. Dank der Cloud-Integration und der breiten Speicherkompatibilität von NovaBACKUP verbringt Tony weniger Zeit mit der Behebung von Problemen und hat mehr Zeit, um mehr Kunden effizient zu unterstützen.

[Lesen Sie die vollständige Fallstudie zu TLC Netcon.](#)



SORGENFREIE DATENSICHERUNG

Cloud-Backups sind ein leistungsstarkes Tool für die Datensicherung von KMUs, sollten jedoch niemals die einzige Backup-Strategie sein. Um die Ausfallsicherheit der Unternehmen Ihrer Kunden und die Sicherheit ihrer Daten zu gewährleisten, sollten Sie eine **hybride Backup-Strategie** verfolgen. Diese kombiniert die Geschwindigkeit und Kontrolle lokaler Backups mit der Sicherheit und Skalierbarkeit der Cloud.

Warten Sie nicht, bis ein Ransomware-Angriff, eine versehentliche Löschung oder ein Systemausfall Lücken in Ihrer Backup-Strategie aufdeckt. Übernehmen Sie jetzt die Kontrolle und sorgen Sie dafür, dass alle Backups zuverlässig, vollständig und jederzeit einfach wiederherstellbar sind.

Ihre nächsten Schritte

Wenn Sie beim Lesen zustimmend genickt haben, weil Sie die Herausforderungen von Ausfallzeiten, Compliance-Risiken und unzuverlässigen reinen Cloud-Backups erkannt haben, gibt es gute Nachrichten: Sie müssen diese Probleme nicht allein bewältigen.

Für KMU: KMUs sollten mit ihrem IT-Dienstleister über die Entwicklung einer hybriden Backup-Strategie sprechen, die sie mit einer stärkeren Datensicherungsstrategie für schnellere Wiederherstellungen unterstützt.

Für MSP: Wenn Sie eine Backup-Plattform suchen, die all diese Vorteile für Ihre Kunden bietet, ohne Ihre Arbeitsbelastung zu erhöhen, ist NovaBACKUP die richtige Lösung. [Lassen Sie uns besprechen, wie wir Ihre MSP-Dienste mit einer speziell entwickelten Backup-Lösung unterstützen können.](#)



ÜBER NOVABACKUP

NovaBACKUP liefert robuste hybride Backup-Lösungen für kleine Unternehmen und die sie betreuenden MSPs. Die Plattform ermöglicht schnelle lokale Wiederherstellungen, sicheren Cloud-Schutz außerhalb des Standorts und bietet reaktionsschnellen Experten-Support – alles in einer einfach zu verwaltenden Lösung.

Weitere Informationen zu NovaBACKUP und unseren Produkten finden Sie unter <https://www.novabackup.de>

Unser Service-Versprechen

Wir versprechen Ihnen, den Schutz und die Sicherheit Ihrer Daten so zu behandeln, als wären es unsere eigenen. Unser Ziel ist es, die Datensicherung so einfach und zuverlässig wie möglich zu gestalten. Sie können sich darauf verlassen, dass wir Sie professionell und fachkundig unterstützen, um Ihren Anforderungen an Ihre Datensicherung gerecht zu werden. Wenden Sie sich an unser Team, wenn Sie Unterstützung bei der Datensicherung und -wiederherstellung benötigen.



📍 NovaBACKUP Europe GmbH
Marienstrasse 89, 30171 Hannover,
Deutschland

☎ Tel.: +49 (40) 80811371

✉ Email: kontakt@novabackup.de

🏠 www.novabackup.de