K&P COMPUTER
BLUE CONSULT

Disaster Recovery in der Cloud

Ein Backup allein reicht nicht aus

In Krisenfällen entscheidet eine funktionierende Disaster-Recovery-Strategie über Umsatz, Reputation und regulatorische Sicherheit.

Cyberangriffe, Systemausfälle oder menschliche Fehler sind tägliche Geschäftsrisiken, die sich oft nicht vermeiden lassen. Im Ernstfall zählt jede Minute! Und dabei steht für die Geschäftsführung und die IT-Leitung nicht die Technik im Vordergrund, sondern die Frage: **Wie schnell sind wir wieder handlungsfähig und können wir das nachweisen?**

Denn neben Umsatzeinbußen und Rufschädigung verlangen Regelwerke wie BCP/DRP, Datenschutzvorgaben und Audit-Anforderungen zum einen Backups, aber vor allem auch nachweislich getestete Wiederherstellungsprozesse. Nur wer den kompletten Recovery-Prozess regelmäßig testet, weiß im Ernstfall, ob Systeme, Daten und Abhängigkeiten tatsächlich wiederherstellbar sind.

Mit einem standardisierten Disaster-Recovery-Test in der Cloud lassen sich Risiken frühzeitig erkennen, Verantwortlichkeiten klären und Investitionen nachhaltig absichern.

Fakten-Check: Warum Disaster-Recovery-Tests entscheidend sind

- Bis zu **60 %** geringere Ausfallzeiten, gegenüber Organisationen ohne valide DR-Tests, bei Unternehmen, die ihre Disaster-Recovery-Konzepte regelmäßig real testen.
- **56 %** der Unternehmen erreichen ihre definierten RTO-Ziele nicht, meist weil Wiederherstellungsprozesse nur theoretisch existieren.
- **70 %** der IT-Verantwortlichen berichten, dass Wiederherstellungen deutlich länger dauern als geplant, da Abhängigkeiten und Abläufe ungetestet sind.
- Ein extrem hoher Anteil der Unternehmen schaffen es nicht, ihre Daten innerhalb der geforderten Zeit vollständig wiederherzustellen.
- **94 %** der Unternehmen hatten in den letzten 12 Monaten Datenverluste oder signifikante Ausfallzeiten, häufig trotz vorhandener Backups.
- Die Kosten ungeprüfter Wiederherstellung (Produktionsstillstand, Vertragsstrafen, Datenverlust, Reputationsschäden) übersteigen die Investitionen in regelmäßige DR-Tests und sichere Cloud-Backups oft um ein Vielfaches.

Quellen: Branchenumfragen, Statistiken

Wie ist die Lage bei Ihnen?

- Wie regelmäßig wird der Wiederherstellungsprozess validiert und **wer trägt im Ernstfall die Verantwortung**?
- Wie schnell kann Ihr DR-Plan eine vollständige Systemwiederherstellung tatsächlich starten?
- Welche **RPO- und RTO-Werte** sind real erreichbar und wann wurden diese zuletzt zuverlässig getestet?
- Wurden **alle kritischen Systeme** (Datenbanken, Applikationen, Identitäts- und Key-Dienste) in einem DR-Test wirklich wiederhergestellt?
- Sind Ihre Backups **verschlüsselt, unveränderlich und wirksam gegen Ransomware geschützt**?
- Ist Ihr DR-Konzept **nachvollziehbar dokumentiert und auditfähig**?

Ein getestetes Disaster-Recovery-Konzept ist kein technisches Detail, sondern eine strategische Absicherung Ihrer Geschäftsfähigkeit und Reputation.

Angebot der K&P Gruppe:

Die K&P Gruppe bietet einen standardisierten und regelmäßig validierten **Disaster-Recovery-Test in der Cloud** an. Grundlage bilden sichere **Restic-Backups für AIX- und Linux-Systeme**, die in der Cloud der K&P Gruppe gespeichert und getestet werden. Ziel ist es, die tatsächliche Wiederherstellbarkeit Ihrer Systeme transparent, nachvollziehbar und belastbar nachzuweisen.

Unser Ansatz kombiniert technische Sicherheit, strukturierte Abläufe und aussagekräftiges Reporting, von der Datensicherung bis zur erfolgreichen Wiederherstellung im Ernstfall. Dabei berücksichtigen wir sowohl organisatorische als auch technische Anforderungen an moderne Disaster-Recovery-Konzepte.

- Sicheres, zertifikatsbasiertes Backup in die Cloud der K&P Gruppe
- Restic-Backups für AIX und Linux, verschlüsselt und revisionssicher
- Regelmäßige DR-Tests
- Vollständige Wiederherstellungsprüfungen
- Validierung realer RPO- und RTO-Werte
- Benchmarking der Recovery-Zeiten
- Transparente Reports als belastbarer Nachweis der durchgängigen DR-Kette
- Klare Definition von Rollen, Verantwortlichkeiten und Abläufen

Mit Disaster Recovery in der Cloud schaffen Sie Sicherheit, Transparenz und Verlässlichkeit, wenn es darauf ankommt.

Warum jetzt Handlungsbedarf besteht

Backups allein vermitteln trügerische Sicherheit. Entscheidend ist nicht, ob Daten gesichert wurden, sondern ob Systeme, Anwendungen und Abhängigkeiten im Ernstfall tatsächlich und rechtzeitig wiederhergestellt werden können. Ungetestete Disaster-Recovery-Konzepte führen dazu, dass RPO- und RTO-Ziele nur auf dem Papier existieren, Verantwortlichkeiten unklar sind und wertvolle Zeit verloren geht – genau dann, wenn jede Minute zählt. Unternehmen, die ihre Wiederherstellung regelmäßig real testen, reduzieren Ausfallzeiten messbar, senken die Gesamtkosten von Störfällen und schaffen belastbare Nachweise gegenüber Geschäftsführung, Prüfern und Aufsichtsbehörden.

Benefits

- **Schnelle Wiederherstellung** und reduzierte Ausfallzeiten
- Schutz von **Umsatz, Reputation und Geschäftsprozessen**
- **Nachweisbare DR-Readiness** gegenüber Kunden, Prüfern und Aufsichtsbehörden
- **Klare Prozesse und Zuständigkeiten** im Krisenfall
- Hohe Sicherheit durch **verschlüsselte Backups und Zugriffskontrollen**
- Optimierte IT-Betriebsabläufe durch **regelmäßige Tests, Automatisierung und Standardisierung**
- Optional: **unveränderliche (immutable) Backups**

Ergänzende Dienstleistungen:

- **Testing-as-a-Service**
  Regelmäßig durchgeführte, gesteuerte DR-Tests inklusive Dokumentation
- **Optimierung von Backup- und DR-Strategien**
  Verbesserung von RPO/RTO und Datenarchitektur
- **Implementierung eines ganzheitlichen Disaster-Recovery-Konzepts**
- **Security Hardening** zur weiteren Absicherung Ihrer Systeme und Daten

Kontakt

Christoph Reigl, Berta-Cramer-Ring 10, 65205 Wiesbaden
reigl@kpc.de, Telefon: +49 6122 7071-380