Fit in Sachen Backup?

Lesen Sie den ultimativen Backup-Leitfaden für Unternehmen

Eine zuverlässige Cybersicherheitsstrategie ist nicht nur eine Option, sondern ein Muss. Ob kleines Start-up oder großes Unternehmen – der Schutz von Daten, Infrastruktur und Ruf ist entscheidend. Dieser Leitfaden hilft Ihnen bei der Erstellung eines zuverlässigen Backup-Plans, um Ihre wertvollen digitalen Ressourcen vor versehentlichem Verlust, Cyberangriffen oder Naturkatastrophen zu schützen.

Entwicklung eines Aktionsplans

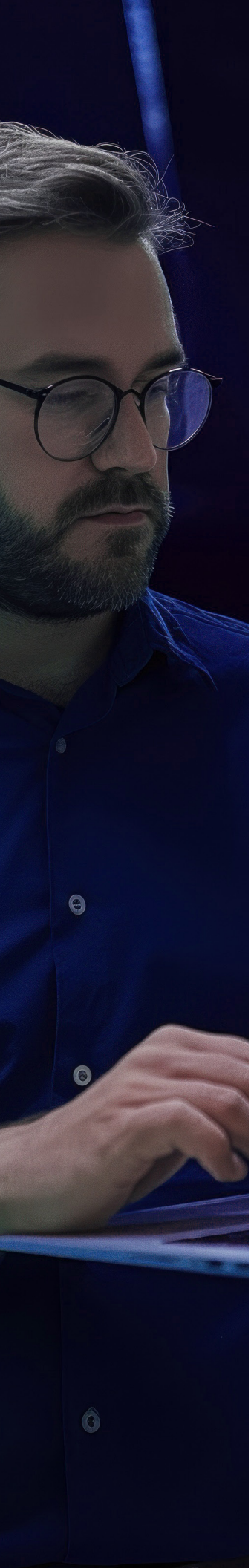
Checkliste für eine professionelle Backup-Strategie

- Kritische Daten identifizieren: Ermitteln Sie, welche Daten für Ihr Unternehmen am wichtigsten sind.
- Auswahl der richtigen Tools: Wählen Sie Backup-Lösungen, die zu Ihren Geschäftsanforderungen und Ihrem Budget passen.
- Umsetzung der 3-2-1-Backup-Regel: Stellen Sie sicher, dass mehrere Kopien Ihrer Daten an verschiedenen Orten gespeichert werden.
- Automatisieren und überwachen: Richten Sie automatische Backups und eine regelmäßige Überwachung ein.
- Regelmäßige Tests: Führen Sie Testwiederherstellungen durch, um sicherzustellen, dass Ihre Backups zuverlässig sind.
- Backups schützen: Verschlüsseln Sie Ihre Daten und verwenden Sie starke Sicherheitsvorkehrungen.

Backup-Grundlagen

Backups sind Ihre erste Verteidigungslinie gegen Ransomware-Angriffe, versehentliches Löschen von Daten und Systemausfälle. Eine der besten Methoden ist die 3-2-1-Backup-Regel:

- Bewahren Sie drei Kopien Ihrer Daten auf: Eine Hauptkopie und zwei zusätzliche Sicherungskopien.
- Zwei Kopien auf unterschiedlichen Medien speichern: Verwenden Sie eine Kombination aus Festplatte, SSD-Laufwerk und Cloud-Storage.
- Eine Kopie außerhalb des Unternehmens aufbewahren: Bewahren Sie eine Backup-Kopie an einem sicheren, entfernten Ort auf, um sie vor physischen Schäden zu schützen.
- Wenn Sie diese Regel befolgen, minimieren Sie Ausfallzeiten, erhalten die Produktivität und vermeiden finanzielle Verluste aufgrund von Hardware-Fehlern, Ransomware-Angriffen oder versehentlichem Löschen.



Erstellen einer Backup-Strategie für Ihr Unternehmen

Wichtige Daten, die gesichert werden müssen:

- Kundendaten: Kundeninformationen, Kontaktdaten und Aufzeichnungen über Transaktionen.
- Finanzunterlagen: Rechnungen, Quittungen und Jahresabschlüsse.
- Proprietäre Informationen: Geschäftsgeheimnisse, geistiges Eigentum und interne Dokumente.

Tools für Unternehmen:

- Cloud-Lösungen: Acronis, Google Drive und Microsoft OneDrive bieten skalierbaren und sicheren Cloud-Storage.
- Enterprise-Server: Lokale Server bieten robuste und zuverlässige Backup-Lösungen.
- Hybride Systeme: Kombination von Cloud- und physischem Storage als ausgewogene Speicherlösung.

Automatisierung und Überwachung:

- Backups automatisieren: Automatisierte Backups stellen sicher, dass Ihre Daten ohne Ihr Zutun regelmäßig gesichert werden. Das reduziert menschliche Fehler und stellt sicher, dass Ihre Backups immer auf dem neuesten Stand sind.
- Überwachung: Überprüfen Sie Ihre Backup-Systeme regelmäßig, um sicherzustellen, dass sie ordnungsgemäß funktionieren. Verwenden Sie Überwachungstools, um Alarmmeldungen zu erhalten, wenn Backups fehlschlagen.

Typische Fehler bei der Datensicherung und wie man sie vermeidet

Auf eine einzige Methode vertrauen:

- Risiko: Wenn Sie sich ausschließlich auf Cloud-Storage oder physische Speichermedien verlassen, ist Ihr Unternehmen gefährdet. Cloud-Storage kann kompromittiert werden und physische Speichermedien können beschädigt werden oder verloren gehen.
- Lösung: Verwenden Sie einen mehrschichtigen Backup-Ansatz, der Cloud-Storage und physischen Speicher kombiniert.

Backups werden nicht getestet:

- Risiko: Nicht wiederherstellbare Backups können Ihre Backup-Strategie zunichte machen.
- Lösung: Testen Sie Ihre Backups regelmäßig, um sicherzustellen, dass sie wiederhergestellt werden können. Führen Sie Testwiederherstellungen durch, um die Integrität Ihrer Daten zu überprüfen.

Cyber Security wird vernachlässigt:

- Risiko: Nicht autorisierte Benutzer:innen können auf unverschlüsselte Backups zugreifen.
- Lösung: Verschlüsseln Sie Ihre Backups und verwenden Sie starke, eindeutige Kennwörter. Implementieren Sie Mehrfaktor-Authentifizierung (MFA) für zusätzliche Sicherheit.

Recovery-Tipps für den Ernstfall

Was tun im Katastrophenfall:

- Schadensbeurteilung: Ermitteln Sie das Ausmaß des Datenverlusts.
- Backup-Plan ausführen: Nehmen Sie das aktuellste Backup und beginnen Sie mit dem Wiederherstellungsprozess.
- Recovery überwachen: Stellen Sie sicher, dass die Daten korrekt wiederhergestellt werden und alle Systeme wie erwartet funktionieren.

Zusammenarbeit mit Ihrem MSP:

- Unterstützung durch Managed Service Provider (MSP): Als Ihr MSP bieten wir kompetente Unterstützung bei der Datenwiederherstellung, von der ersten Beurteilung des Schadens bis zur vollständigen Wiederherstellung. Damit Datenverluste in Zukunft keine Chance mehr haben, unterstützen wir Sie auch bei der Optimierung Ihrer Backup-Strategie.

Kontinuierliche Verbesserung und Weiterbildung

So bleiben Sie Cyberbedrohungen immer einen Schritt voraus:

- Backup-Plan regelmäßig aktualisieren: Technologien und Bedrohungen entwickeln sich weiter, daher ist es wichtig, Ihre Backup-Strategie zu überprüfen und zu aktualisieren. Informieren Sie sich über die neuesten Lösungen und Best Practices im Bereich der Datensicherung.

Schulung des Personals:

- Schulen Sie Ihr Team: Stellen Sie sicher, dass alle Mitarbeiter:innen die Bedeutung von Backups verstehen und wissen, wie sie Backup-Tools effektiv einsetzen können. Führen Sie regelmäßige Schulungen durch, um alle Beteiligten zu informieren und vorzubereiten.

Feedback und Audits:

- Feedback einholen: Ermutigen Sie Ihr Team, Vorschläge für den Backup-Prozess zu machen. Ihre Vorschläge können Ihnen dabei helfen, Bereiche mit Verbesserungspotenzial zu identifizieren.
- Regelmäßige Audits durchführen: Überprüfen Sie regelmäßig, ob Ihre Backup-Strategie wirksam ist. Identifizieren Sie Lücken und nehmen Sie die notwendigen Anpassungen vor.

Wie gut ist Ihr Unternehmen durch Backups geschützt?

Beantworten Sie folgende Fragen, um es herauszufinden:

- Sichern Sie Ihre Daten mindestens einmal pro Woche?
- Sind Ihre Backups automatisiert?
- Bewahren Sie eine Backup-Kopie außerhalb des Unternehmens auf?
- Haben Sie einen Backup-Plan entwickelt?
- Testen Sie Ihre Backups regelmäßig?
- Bieten Sie Ihrem Personal Cybersicherheitsschulungen an?
- Wenn Sie einen Backup-Plan haben, wird dieser regelmäßig aktualisiert?

Wenn Sie eine dieser Fragen mit „Nein“ beantwortet haben, sind Ihre Daten gefährdet. Setzen Sie sich noch heute mit uns in Verbindung, um sicherzustellen, dass Ihr Unternehmen mit Backups für den Ernstfall gerüstet ist.

Warten Sie nicht, bis Sie Daten verlieren, um die Bedeutung von Backups zu erkennen. Schützen Sie Ihre Unternehmensdaten noch heute! Kontaktieren Sie uns für fachkundige Unterstützung oder Beratung.

UNIMISSION AG
E-mail: info@unimission.ch
Telefon: +41585211800
https://www.unimission.ch