Backup Checkliste

Sind Ihre geschäftskritischen Daten ausreichend vor Cyberangriffen, Systemausfällen oder Datenverlust gesichert?

Die Sicherung geschäftskritischer Daten ist von entscheidender Bedeutung, um sich vor den zahlreichen Bedrohungen wie Cyberangriffen, Systemausfällen und Datenverlusten zu schützen. Diese Checkliste dient als praktisches Werkzeug, um sicherzustellen, dass Ihre Datensicherungsstrategie robust und effektiv ist. Die Sicherung und Wiederherstellung von Daten sind nicht nur elementare Bestandteile der IT-Sicherheit, sondern auch essenziell für die Aufrechterhaltung der Geschäftskontinuität. Lassen Sie uns gemeinsam durch die wichtigsten Aspekte gehen, um sicherzustellen, dass Ihre geschäftskritischen Daten in jeder Hinsicht geschützt sind.

1 Backup-Strategie	
☐	Sind regelmässige Backups Ihrer geschäftskritischen Daten eingerichtet?
☐	Werden Backups automatisch durchgeführt?
☐	Werden verschiedene Versionen der Daten gesichert?
2 Speicherort und Redundanz	
☐	Werden Ihre Backups an einem sicheren externen Ort gespeichert?
☐	Gibt es eine geografische Redundanz, um sich vor Naturkatastrophen zu schützen?
3 Datensicherheit	
☐	Sind Ihre Daten während der Übertragung und im Speicher verschlüsselt?
☐	Wer hat Zugriff auf die Backup-Daten, und sind die Zugriffsberechtigungen angemessen eingeschränkt?
4 Test der Wiederherstellung	
☐	Werden regelmässige Wiederherstellungstests durchgeführt, um sicherzustellen, dass die Daten im Bedarfsfall wiederhergestellt werden können?
5 Ransomware-Schutz	
☐	Gibt es Schutzmassnahmen, um Ransomware-Angriffe zu verhindern?
☐	Wird regelmässig überprüft, ob die Anti-Ransomware-Massnahmen wirksam sind?

Backup Checkliste

6 Systemausfall-Plan	
☐	Existiert ein Notfallwiederherstellungsplan im Falle eines kompletten Systemausfalls?
☐	Wurde der Plan getestet, um sicherzustellen, dass er im Ernstfall effektiv ist?
7 Datensicherheitsrichtlinien	
☐	Gibt es klare Richtlinien für die Speicherung und Sicherung geschäftskritischer Daten?
☐	Sind die Mitarbeiter über diese Richtlinien informiert und geschult?
8 Überwachung und Benachrichtigungen	
☐	Wird die Datensicherung kontinuierlich überwacht?
☐	Existieren Warnmeldungen für ungewöhnliche Aktivitäten oder Ausfälle?
9 Update und Patch-Management	
☐	Werden alle relevanten Software- und Sicherheitspatches regelmässig aktualisiert?
☐	Gibt es einen Prozess zur Überprüfung und Implementierung neuer Sicherheitsstandards?
10 Compliance und Regularien	
☐	Wird sichergestellt, dass alle Backup-Praktiken den geltenden Compliance-Anforderungen entsprechen?

Diese Checkliste kann je nach den spezifischen Anforderungen Ihres Unternehmens angepasst werden.
MOUNT10 freut sich Sie bei Ihrem Backup Konzept zu unterstützen, so dass Ihre Daten optimal geschützt sind.