Empfehlung Datensicherung / Archivierung

Durch versehentliches Löschen, technisches Versagen, Hackerangriffe, Viren oder andere Ereignisse können Daten unwiederbringlich verloren gehen. Eine Datensicherung soll dem Desaster vorbeugen und den Datenbestand nicht nur sichern, sondern eine kurzfristige Wiederherstellung gewährleisten. Die Vorschriften der DSGVO sind einzuhalten.

1. Entwicklung eines Datensicherungskonzepts

Jeder Citadel-Kunde sollte einen organisatorischen und technischen Ablauf zur Datensicherung entwickeln. Zu den Parametern, die für die Datensicherung von Bedeutung sein können, zählen z.B. das eingesetzte System, das Daten- und Änderungsvolumen sowie die Verfügbarkeitsanforderungen.

2. Zuständigkeiten

Die schriftlich festgehaltenen Zuständigkeiten sollen nicht nur regeln, wer für die Datensicherung zuständig ist und wer die Passwörter kennt. Geregelt werden muss auch, wer die Wiederherstellung der Daten veranlasst. Zu diesem Zweck sollten immer mindestens zwei Personen benannt sein, falls einer der Verantwortlichen nicht verfügbar ist.

3. Konzept zum Wiederherstellen

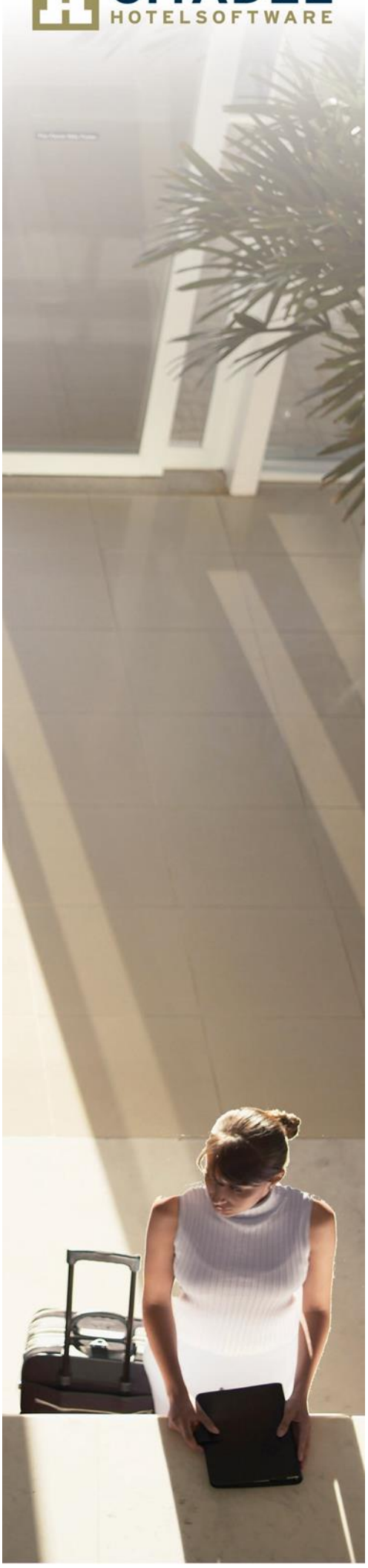
Ein gut ausgearbeitetes Datensicherungskonzept bringt im Notfall nichts, wenn eine lückenlose Anleitung zum Wiederherstellen der Daten nicht mitgeregelt wurde. Deswegen ist es wichtig, eine vollständige Anweisung festzuhalten, wie die Daten im Fall der Fälle wiederhergestellt werden können.

4. Anschaffung eines geeigneten Systems

Bei der Anschaffung eines Systems zur Datensicherung muss darauf geachtet werden, dass die Anforderungen aus dem Datensicherungskonzept erfüllt werden. Dabei sollte nicht nur die Leistungsfähigkeit, sondern auch die Bedienbarkeit im Fokus stehen.

5. Art der Datensicherung: Vollsicherung

Schließlich muss eine geeignete Datensicherungsart gewählt werden, die auf die eigenen Bedürfnisse zugeschnitten ist.



Aus unserer Sicht kommt nur eine Vollsicherung in Frage. Dabei werden sämtliche zu sichernde Daten zu einem bestimmten Zeitpunkt auf dem Sicherungsträger kopiert und gespeichert. Ob sich Daten seit der letzten Datensicherung geändert haben, bleibt dabei unberücksichtigt. Der Vorteil einer Vollsicherung liegt auch in der einfachen Wiederherstellung.

6. Häufigkeit und Zeitpunkt der Sicherung

Die Häufigkeit der Sicherungen sollte so gewählt werden, dass der Wiederherstellungsaufwand für geänderten Datenbestand, der seit der letzten Datensicherung erfolgt ist, minimal bleibt.

Empfohlen wird nicht nur eine feste periodische Zeit (täglich, unter Berücksichtigung des Tagesabschlusses), sondern auch außerplanmäßige Sicherungen bei besonderen Ereignissen, z.B. System- oder Jahreswechsel und größeren Änderungen sowie Speicherung von Daten, aus Gründen der Archivierung.

7. Verschlüsselung

Besonders Vertrauliche Daten können vor der Sicherung möglichst verschlüsselt werden. Diese gilt insbesondere bei Auslagerung der Backups. Dabei soll darauf geachtet werden, dass eine Entschlüsselung auch nach einem längeren Zeitraum möglich sein muss.

8. Regelmäßige Tests

Es müssen regelmäßige Tests durchgeführt werden, ob die gesicherten Daten problemlos zurückgespielt werden können.

9. Geeignete Aufbewahrung

Datensicherungskopien sollten in anderen Gebäuden oder zumindest in anderen Brandschutzbereichen aufbewahrt werden als die Original-Datenträger. Hierzu sind ggfls. die Vorgaben in bestehenden Versicherungspolicen zu überprüfen.

10. Haftung

Der Kunde trägt die Verantwortung über seine Betriebsdaten. Die Citadel Hotelsoftware GmbH übernimmt keinerlei Haftung für Folgen fehlender Programm- und Datensicherungen.