Eine kleine Einführung in resiliente Datensicherung

Andreas Rogge - Bareos GmbH & Co. KG – www.bareos.com

Wer bin ich?

Andreas Rogge

- hauptberuflicher Bareos-Entwickler
- Langzeit-Nutzer von Bareos
- ursprünglich Systemadministrator

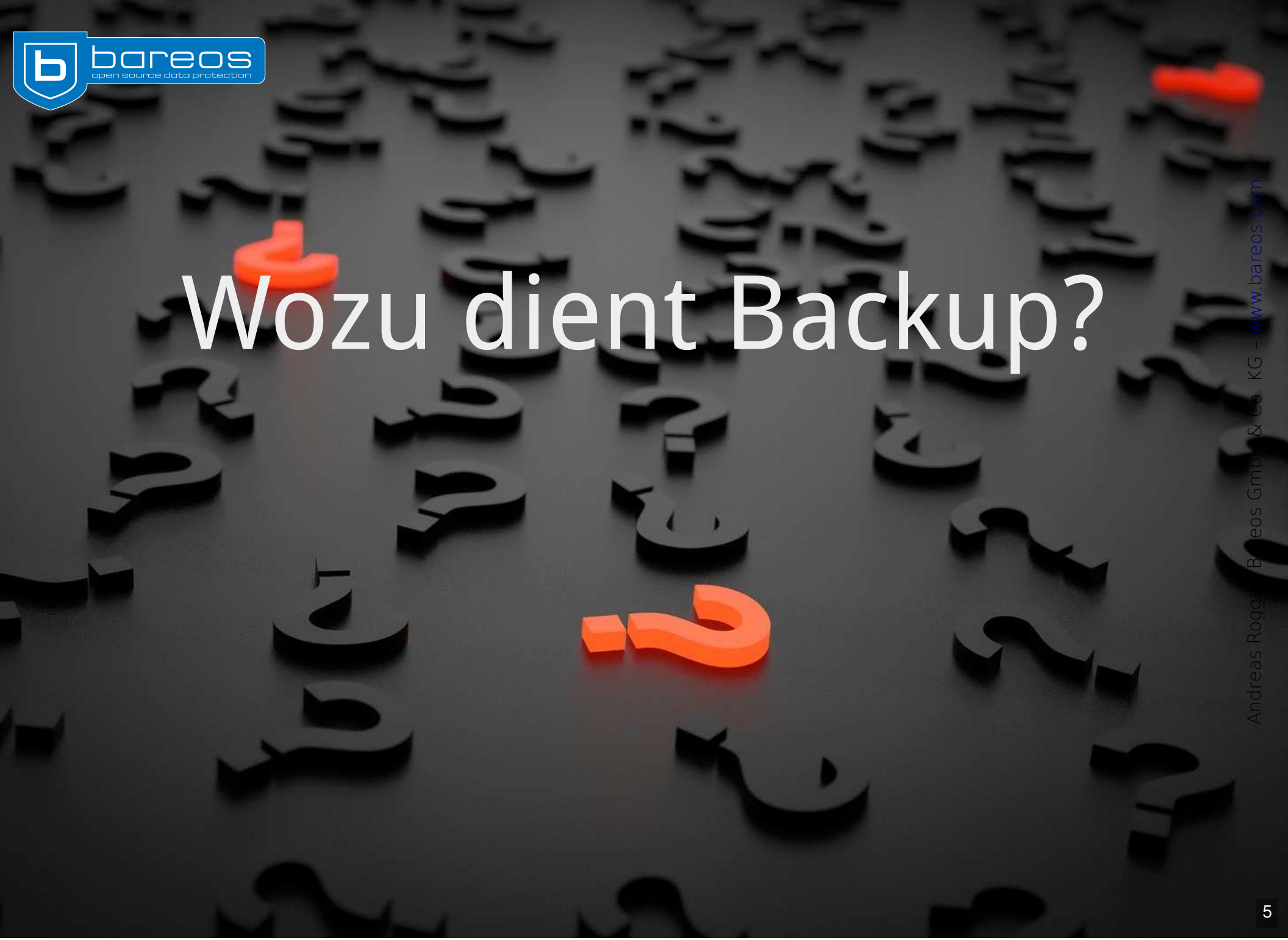
Wo arbeite ich?

Bareos GmbH & Co. KG

- finanziert das Bareos Projekt
- stellt Dienstleistungen rund um Bareos bereit
  - Binärpakete mit Langzeit-Support
  - technischer Kundendienst
  - Schulungen
  - Partnerschaften mit Dienstleistern vor Ort

Übersicht

- Wozu dient Backup?
- Backup Best Practice
- Resilientes Backup



Wozu dient Backup?

- reaktive Handlungsfähigkeit bei Datenverlust herstellen

Wozu dient Backup?

- reaktive Handlungsfähigkeit bei Datenverlust herstellen
- Geschäftskontinuität sicherstellen

Wozu dient Backup?

- reaktive Handlungsfähigkeit bei Datenverlust herstellen
- Geschäftskontinuität sicherstellen
- Backup ist die letzte Verteidigungslinie!

Datenverlust

häufigste Ursachen:

Datenverlust

häufigste Ursachen:

- Menschliche Fehler

Datenverlust

häufigste Ursachen:

- Menschliche Fehler
- Hardware- oder Systemausfall

Datenverlust

häufigste Ursachen:

- Menschliche Fehler
- Hardware- oder Systemausfall
- Softwarefehler

Datenverlust

häufigste Ursachen:

- Menschliche Fehler
- Hardware- oder Systemausfall
- Softwarefehler
- Malware

Datenverlust

häufigste Ursachen:

- Menschliche Fehler
- Hardware- oder Systemausfall
- Softwarefehler
- Malware
- externe Einflüsse

Datenverlust

häufigste Ursachen:

- Menschliche Fehler
- Hardware- oder Systemausfall
- Softwarefehler
- Malware
- externe Einflüsse
- Verlust / Diebstahl

Praxisbeispiel

S3-kompatibles Speichersystem mit Object-Lock zur Ablage gewährleistungsrelevanter Akten.

Praxisbeispiel

S3-kompatibles Speichersystem mit Object-Lock zur Ablage gewährleistungsrelevanter Akten.

- Appliance mit RAID-6 Speicherpool

Praxisbeispiel

S3-kompatibles Speichersystem mit Object-Lock zur Ablage gewährleistungsrelevanter Akten.

- Appliance mit RAID-6 Speicherpool
- Replikation auf 2. Appliance

Praxisbeispiel

S3-kompatibles Speichersystem mit Object-Lock zur Ablage gewährleistungsrelevanter Akten.

- Appliance mit RAID-6 Speicherpool
- Replikation auf 2. Appliance
- Replikation auf 3. Appliance an anderem Standort

Praxisbeispiel

S3-kompatibles Speichersystem mit Object-Lock zur Ablage gewährleistungsrelevanter Akten.

- Appliance mit RAID-6 Speicherpool
- Replikation auf 2. Appliance
- Replikation auf 3. Appliance an anderem Standort
- Broschüre sagt: "macht Backup überflüssig"

Praxisbeispiel

S3-kompatibles Speichersystem mit Object-Lock zur Ablage gewährleistungsrelevanter Akten.

- Appliance mit RAID-6 Speicherpool
- Replikation auf 2. Appliance
- Replikation auf 3. Appliance an anderem Standort
- Broschüre sagt: "macht Backup überflüssig"
- Object-Lock Policy auf 10 Monate statt 10 Jahre eingestellt

Backup Best Practice

Bewährte Methoden und Vorgehensweisen für eine Datensicherung auf die man vertrauen kann.

3-2-1-Regel

3-2-1-Regel

- mindestens 3 Kopien

3-2-1-Regel

- mindestens 3 Kopien
- mindestens 2 davon auf unterschiedlichen Speichermedien

3-2-1-Regel

- mindestens 3 Kopien
- mindestens 2 davon auf unterschiedlichen Speichermedien
- mindestens 1 davon an einem externen, entfernten Standort

RPO planen

Recovery Point Objective - wie oft muss ich sichern?

RPO planen

Recovery Point Objective - wie oft muss ich sichern?

- welchen Verlust kann ich akzeptieren?

RPO planen

Recovery Point Objective - wie oft muss ich sichern?

- welchen Verlust kann ich akzeptieren?
- häufig proportional zur Menge der Bewegtdaten

Vorhaltezeit planen

Vorhaltezeit - wie lange muss ich die Sicherungen aufheben?

Vorhaltezeit planen

Vorhaltezeit - wie lange muss ich die Sicherungen aufheben?

- kann ich Daten verlieren ohne es zu bemerken?

Vorhaltezeit planen

Vorhaltezeit - wie lange muss ich die Sicherungen aufheben?

- kann ich Daten verlieren ohne es zu bemerken?
- häufig proportional zur Seltenheit des Zugriffs

Validierung & Test

Validierung & Test

- Wird überhaupt gesichert?

Validierung & Test

- Wird überhaupt gesichert?
- Stimmt der Umfang?

Validierung & Test

- Wird überhaupt gesichert?
- Stimmt der Umfang?
- Kann restauriert werden?

Validierung & Test

- Wird überhaupt gesichert?
- Stimmt der Umfang?
- Kann restauriert werden?
- Sind die restaurierten Daten verwertbar?

Validierung & Test

- Wird überhaupt gesichert?
- Stimmt der Umfang?
- Kann restauriert werden?
- Sind die restaurierten Daten verwertbar?
- Regelmäßig überprüfen!

Automatisierung

Automatisierung

- Datensicherung

Automatisierung

- Datensicherung
- Überwachung

Automatisierung

- Datensicherung
- Überwachung
- Test der Rücksicherung

Automatisierung

- Datensicherung
- Überwachung
- Test der Rücksicherung
- veraltete Sicherungen entfernen

Katalogisierung

Katalogisierung

- Liste der bestehenden Sicherungen

Katalogisierung

- Liste der bestehenden Sicherungen
- Inhaltsverzeichnis der Sicherungen

Katalogisierung

- Liste der bestehenden Sicherungen
- Inhaltsverzeichnis der Sicherungen
- Standort der Sicherungen

Resilienz

Fähigkeit technischer Systeme, bei einem Teilausfall nicht vollständig zu versagen.

Resilientes Backup

Resilientes Backup

- Verfügbarkeit

Resilientes Backup

- Verfügbarkeit
- Integrität

Resilientes Backup

- Verfügbarkeit
- Integrität
- Authentizität

3-2-1-1-0-Regel

Erweiterung der 3-2-1-Regel

3-2-1-1-0-Regel

Erweiterung der 3-2-1-Regel

- 1 unveränderbare Kopie

3-2-1-1-0-Regel

Erweiterung der 3-2-1-Regel

- 1 unveränderbare Kopie
- 0 Fehler bei Überprüfung

Sichere Offsite

Sichere Offsite

- Entfernung

Sichere Offsite

- Entfernung
- Erreichbarkeit

Sichere Offsite

- Entfernung
- Erreichbarkeit
- hinreichende Trennung

Praxisbeispiel

Betrieb einer Anwendung in einer der großen Clouds.

Praxisbeispiel

Betrieb einer Anwendung in einer der großen Clouds.

- Datensicherung am selben Standort

Praxisbeispiel

Betrieb einer Anwendung in einer der großen Clouds.

- Datensicherung am selben Standort
- zweite Sicherung an anderem Standort

Praxisbeispiel

Betrieb einer Anwendung in einer der großen Clouds.

- Datensicherung am selben Standort
- zweite Sicherung an anderem Standort
- hinterlegte Kreditkarte gesperrt

Praxisbeispiel

Betrieb einer Anwendung in einer der großen Clouds.

- Datensicherung am selben Standort
- zweite Sicherung an anderem Standort
- hinterlegte Kreditkarte gesperrt
- Cloud-Konto gesperrt

Praxisbeispiel

Betrieb einer Anwendung in einer der großen Clouds.

- Datensicherung am selben Standort
- zweite Sicherung an anderem Standort
- hinterlegte Kreditkarte gesperrt
- Cloud-Konto gesperrt
- Anwendung nicht mehr verfügbar

Praxisbeispiel

Betrieb einer Anwendung in einer der großen Clouds.

- Datensicherung am selben Standort
- zweite Sicherung an anderem Standort
- hinterlegte Kreditkarte gesperrt
- Cloud-Konto gesperrt
- Anwendung nicht mehr verfügbar
- Recovery nicht möglich

RTO

Recovery Time Objective - Wie schnell muss alles wieder funktionieren?

RTO

Recovery Time Objective - Wie schnell muss alles wieder funktionieren?

- Analog zum RPO unterschiedlich

RTO

Recovery Time Objective - Wie schnell muss alles wieder funktionieren?

- Analog zum RPO unterschiedlich
- Kosten-Nutzen abwägen

RTO

Recovery Time Objective - Wie schnell muss alles wieder funktionieren?

- Analog zum RPO unterschiedlich
- Kosten-Nutzen abwägen
- Abhängigkeiten berücksichtigen!

RTO

Recovery Time Objective - Wie schnell muss alles wieder funktionieren?

- Analog zum RPO unterschiedlich
- Kosten-Nutzen abwägen
- Abhängigkeiten berücksichtigen!
- Machbarkeit prüfen!

Verschlüsselung

Verschlüsselung

- Vertraulichkeit vs. Verfügbarkeit

Verschlüsselung

- Vertraulichkeit vs. Verfügbarkeit
- Schlüsselmaterial

Verschlüsselung

- Vertraulichkeit vs. Verfügbarkeit
- Schlüsselmaterial
  - muss verfügbar sein

Verschlüsselung

- Vertraulichkeit vs. Verfügbarkeit
- Schlüsselmaterial
  - muss verfügbar sein
  - muss zugeordnet werden können

Verschlüsselung

- Vertraulichkeit vs. Verfügbarkeit
- Schlüsselmaterial
  - muss verfügbar sein
  - muss zugeordnet werden können
- eventuell schlechteres RTO

Manipulationssicherheit

Manipulationssicherheit

- Schutz vor Löschung (Verfügbarkeit erhalten)

Manipulationssicherheit

- Schutz vor Löschung (Verfügbarkeit erhalten)
- Schutz vor Veränderung (Integrität erhalten)

Zugriffskontrolle

Zugriffskontrolle

- Backup-Systeme bitte *nicht* an SSO anbinden

Zugriffskontrolle

- Backup-Systeme bitte *nicht* an SSO anbinden
- Wenn SSO, dann minimale Privilegien

Zugriffskontrolle

- Backup-Systeme bitte *nicht* an SSO anbinden
- Wenn SSO, dann minimale Privilegien
- privilegierter Zugriff sollte Zweifaktor-Authentifizierung erfordern!

Fazit

Fazit

- Menschen machen Fehler

Fazit

- Menschen machen Fehler
- habe ein getestetes Backup

Fazit

- Menschen machen Fehler
- habe ein getestetes Backup
- auch wenn etwas grob schief gelaufen ist

Vielen Dank!