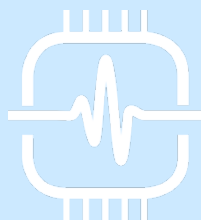


WHITEPAPER

Backup & Recovery

Die Lebensversicherung für Ihr Unternehmen!



Steinbeis Industrial IT

Healthy IT. Strong Business.



Persönliches Vorwort

Heute gehen wir auf das Thema „Backup & Recovery ein.

Das Thema umfasst sowohl das Datensicherungskonzept im „Office“-Bereich Ihres Unternehmens als auch im Detail die Datensicherungsprozesse im Fertigungsumfeld.

Backup & Recovery Prozesse werden als unangenehme Kostentreiber im Unternehmen gesehen. Sie kosten Geld für die IT-Infrastruktur und das betreuende Personal. Die Wichtigkeit des Prozesses wird erst erkannt, wenn wichtige Daten gelöscht oder unbeabsichtigt überschrieben werden. Dies hat zur Folge, dass Angebote nicht rechtzeitig versendet werden können oder bspw. aufgrund einer falschen Maschinenkonfiguration in der Produktion Fehlteile erzeugt werden.

Sobald solche Probleme auftauchen, wird es sehr schnell bis zur Chef-Etage zum Thema, dass eine Datensicherung unverzichtbar für ein Unternehmen ist, schon gar nicht zu sprechen von möglichen Cyberangriffen, die aktuelle Daten zerstören können.

Wir wünschen Ihnen wieder viel Spaß beim Lesen des Whitepapers und freuen uns sehr auf Ihre Kommentare und Anmerkungen – gerne auch direkt über LinkedIn – Steinbeis-Industrial-IT.

Ihr Team von Steinbeis-Industrial-IT, die IT-Health-Company.



Prozesse & Rollen – gute Organisation ist alles !

Inhaltsverzeichnis

1. Einleitung
2. Begriffsdefinitionen
3. Warum KMU besonders gefährdet sind
4. Typische Szenarien
5. Tools für KMU
6. Der Backup & Recovery-Prozess
7. Fazit & Handlungsempfehlungen

1. Einleitung

Angebote, Bestellungen als auch die Maschinensteuerungen liegen heute in den allermeisten Unternehmen nur noch digital vor.

Während Sie früher beispielsweise in den Leitzordner griffen und sich eine Papierkopie des letzten Angebotes erstellen konnten, verschwinden jetzt die digitalen Dokumente nach einem Löschvorgang von der Festplatte.

Viele KMU unterschätzen die Bedeutung von Datensicherung. „Wir haben doch ein Backup“ – dieser Satz ist weit verbreitet. Doch die Realität zeigt: Ein Backup allein reicht nicht. Erst ein getesteter Recovery-Plan stellt sicher, dass Daten im Ernstfall auch wirklich wiederhergestellt werden können. Angesichts zunehmender Cyberangriffe, steigender Datenmengen und wachsender Abhängigkeit von IT-Systemen ist Backup & Recovery längst keine Kür mehr, sondern Pflicht.

Deshalb ist es wichtig, dass alle wichtigen geschäftskritischen Daten Ihres Unternehmens regelmäßig gesichert werden und dass ein IT-Team einen eingespielten Prozess zur Wiederherstellung der Daten beherrscht und diesen auch



wiederkehrend erprobt – vergleichbar mit Übungen der Feuerwehr.

Im Whitepaper erklären wir Ihnen die Fachbegriffe, stellen einige KMU-taugliche Tools vor und erläutern, wie Sie diese am einfachsten einführen.

2. Begriffsdefinitionen

Backup

Ein Backup ist die gezielte Erstellung von Sicherungskopien digitaler Daten, um diese im Falle eines Verlusts, einer Beschädigung oder eines Angriffs wiederherstellen zu können. Dabei werden Dateien, Datenbanken oder ganze Systeme regelmäßig auf separaten Speichermedien oder in der Cloud gesichert. Ziel ist es, eine redundante Kopie zu besitzen, die unabhängig vom Originalsystem existiert.

Ein gutes Backup erfüllt folgende Kriterien:

- **Regelmäßigkeit:** Automatisierte Sicherungen in festen Intervallen
- **Redundanz:** Mehrere Kopien auf unterschiedlichen Medien
- **Sicherheit:** Verschlüsselung und Zugriffsschutz
- **Verfügbarkeit:** Zugriff im Notfall, auch außerhalb des Unternehmensstandorts

Die 3-2-1-Regel gilt als bewährter Standard:

3 Kopien, 2 verschiedene Medien, 1 Kopie extern gelagert



Recovery

Recovery bezeichnet den Prozess der Wiederherstellung von Daten aus einem Backup nach einem Ausfall, Angriff oder Fehler. Es geht nicht nur darum, Daten zurückzuspielen, sondern auch darum, Systeme, Anwendungen und Prozesse schnellstmöglich wieder funktionsfähig zu machen.

Recovery umfasst:

- Technische Wiederherstellung: Dateien, Datenbanken, Systeme
- Organisatorische Abläufe: Wer übernimmt was im Ernstfall?
- Zeitliche Ziele:
 - RTO (Recovery Time Objective): Wie schnell muss alles wieder laufen?
 - RPO (Recovery Point Objective): Wie viel Datenverlust ist akzeptabel?

Ein Recovery ist nur dann erfolgreich, wenn:

- Die Backup-Daten intakt und aktuell sind
- Der Wiederherstellungsprozess getestet und dokumentiert wurde
- Die Verantwortlichen wissen, was zu tun ist



3. Warum KMU besonders gefährdet sind

KMU verfügen oft über begrenzte IT-Ressourcen. Häufig gibt es keine eigene IT-Abteilung, sondern nur externe Dienstleister oder einzelne Verantwortliche. Gleichzeitig sind KMU stark abhängig von wenigen Systemen: Fällt das ERP oder die Kundendatenbank aus, steht der Betrieb still. Studien zeigen: 60 % der KMU überleben einen schweren Datenverlust nicht länger als sechs Monate (Quelle: Bitcom 2025).

4. Typische Szenarien

- Ransomware-Angriff: Daten werden verschlüsselt und sind ohne Backup verloren.
- Versehentliches Löschen: Ein Mitarbeiter löscht einen wichtigen Ordner.
- Hardwareausfall: Defekte Festplatten oder Server zerstören Datenbestände.
- Naturkatastrophen/Stromausfälle: Externe Faktoren können Systeme lahmlegen.

Praxisbeispiel: Ein mittelständisches Handelsunternehmen wurde durch einen Ransomware-Angriff lahmgelegt. Dank eines getesteten Recovery-Plans mit Veeam und Cloud-Backup war das ERP-System nach 4 Stunden wieder online. Kein Datenverlust, kein Umsatzverlust – aber viel gelernt.



5. Tools für KMU

Tool	Typ	Preis	Vorteile und Besonderheiten
Veeam	Hybrid/Cloud	3,50-€ pro User und Monat bis zu 4500,-€/Jahr für professionelle KMU Lösung	Automatisierte Backups, schnelle Wiederherstellung, intuitive Oberfläche
Carbonite	Cloud	Ab 8,-€/Rechner pro Monat	Einfach zu bedienen, gute Preisstruktur, ideal für Remote-Teams
Novastar	Lokal/Server	Keine Angabe	Deutsche Lösung, DSGVO-konform, für Einzel-PCs und Server
Acronis	Hybrid	Ab 181,-/Monat	KI-gestützte Sicherheit, Bare-Metal-Recovery, hohe Flexibilität

Einige Erklärungen zur Spalte „Typ“

Unter Typ verstehen wir die Art des Hostings, also auf welchem System sich die Software und/oder die Daten befinden. Bei „**Hybrid**“ befindet sich die Backup/Recovery Software bei einem Cloud Dienstleister. Dieser verbindet sich remote mit Ihren zu sichernden Servern und Daten. Die Ablage der Backups findet aber in der Regel bei Ihnen im Unternehmen statt. Somit besteht keine Gefahr des Datenverlustes.

Beim Typ „**Cloud**“ befindet sich sowohl die Backup/Recovery Software in der Cloud als auch Ihre gesicherten Daten. In diesem Fall ist es wichtig zu erfahren, was mit Ihren Daten passiert. Oftmals werden diese Daten innerhalb der Cloud abhängig vom Provider in die USA gespiegelt. Durch sogenannte „**Multi-**



Tenant“ Architekturen ist aber sichergestellt, dass andere Kunden dieser Software keinerlei Zugriff auf Ihre Daten haben. Beim letzten Typ **„Server“** befinden sich sowohl Backup/Recovery Software als auch die gesicherten Daten innerhalb Ihres Unternehmens auf Ihren Servern.

6. Der Backup & Recovery-Prozess

Ein klarer Prozess ist entscheidend. Für KMU empfiehlt sich ein schlanker Ablauf:

Daten klassifizieren

Vergeben Sie für Ihre Daten unternehmensweit Klassifizierungen. Typischerweise benennen Sie die Klassen als Data-Security-Level 1 bis 3 (DSL1 bis DSL3).

- **DSL1** bedeutet, die Daten sind für alle Mitarbeiter des Unternehmens zugänglich und sind nicht geschäftskritisch. Dies können Dokumentationen, Notizen, Fremddokumente, leicht wiederherstellbare Dokumente sein.
- **DSL2** bedeutet, dass die Daten nur von bestimmten Mitarbeitern bearbeitet werden dürfen
- **DSL3** bedeutet, dass die Daten Unternehmenswissen enthalten, geschäftskritisch sind. Bei Angriffen von außen gefährdet sind.

Weiterhin beschreiben Sie, ob und in welcher Form die Daten sicherungswürdig sind.

Entwicklungsdaten müssen beispielsweise täglich gesichert werden und mehrere Versionsstände in den Sicherungen vorhalten, um auf ältere Stände zugreifen zu können.

Freigegebene Entwicklungsdaten, die eher statisch sind, werden nur zum Zeitpunkt ihrer Freigabe einmalig gesichert.



Ebenso verhält es sich mit gültigen Angeboten. Der Versionsstand eines offiziellen Angebotes wird einmalig gesichert.

Ein weiterer Aspekt ist die Verfügbarkeit der gesicherten Daten. Dynamische, sich täglich ändernde Daten, werden täglich gesichert, jedoch nach einer gewissen Zeit wieder überschrieben, um den zur Verfügung stehenden Plattenplatz nicht unnötig zu belegen, was erhebliche Kosten verursachen kann.

Die Kombination aller Kategorien erzeugt eine gewisse Komplexität.

Halten Sie diese so gering als möglich, lieber einmal mehr sichern lautet hier das Motto. Damit stellen Sie auch gesetzliche Anforderungen (NIS-2) sicher.

Zu diesem Thema haben sich viele Institutionen detaillierte Gedanken gemacht. Vorschläge dazu finden Sie u.a. in Datensicherungsrichtlinien, wie sie beispielsweise das Landesamt für Sicherheit in der Informationstechnik Bayern zur Verfügung stellt.

Letztendlich ist es für Sie wichtig, den Überblick zu behalten. Wir verwenden hierzu eine Datensicherungsmatrix, in der beschrieben ist, welche Daten auf welche Art und Weise gesichert werden.



1. Backup-Strategie definieren (3-2-1-Regel)

Die wichtigste Grundregel lautet:

- 3 Kopien Ihrer Daten, d.h. unterschiedliche Zeitstände einer Datei
- 2 verschiedene Speichermedien, unterschiedliche Datenserver auch wenn möglich an unterschiedlichen physikalischen Standorten
- 1 externes Backup, hierzu eignet sich idealerweise ein günstiger Cloud-Speicher

2. Automatisierung & Monitoring

Ein Backup-System ist nur dann zuverlässig, wenn es automatisch funktioniert und ständig überwacht wird. Manuelle Sicherungen sind fehleranfällig, werden oft vergessen und bieten keine Echtzeitkontrolle. Deshalb sind Automatisierung und Monitoring zentrale Bausteine jeder professionellen Backup-&-Recovery-Strategie – gerade für KMU mit begrenzten IT-Ressourcen.

Automatisierung

- Zeitpläne definieren: Tägliche inkrementelle Backups, wöchentliche Vollbackups – je nach Datenvolumen und Geschäftsmodell.
- Automatische Versionierung: Mehrere Generationen von Dateien sichern, um versehentliche Änderungen rückgängig machen zu können.
- Cloud-Synchronisation: Backups werden automatisch in externe Speicherorte (z. B. Cloud) übertragen – ohne manuelles Zutun.
- Skripte & Policies: Regeln, wann, wie und was gesichert wird – z. B. nur geänderte Dateien oder bestimmte Ordner.



Monitoring

- Statusberichte & Dashboards: Übersicht über letzte Backups, Fehler, Speicherstatus – ideal für Geschäftsführung und IT-Verantwortliche.
- Benachrichtigungen bei Fehlern: Sofortige Alerts per E-Mail oder App, wenn ein Backup fehlschlägt oder ein Speicherlimit erreicht wird.
- Integritätsprüfungen: Automatische Validierung, ob Backups vollständig und wiederherstellbar sind.
- Audit-Logs & Protokolle: Nachvollziehbarkeit aller Backup-Aktivitäten – wichtig für Compliance und interne Kontrolle.

Tipp

- die meisten Backup-Tools bieten eine integrierte Automatisierung und Monitoring-Funktionen.
- Wichtig: das Monitoring nicht nur aktivieren – sondern regelmäßig auswerten und bei Problemen sofort handeln.

3. Recovery-Plan erstellen (RTO/RPO, Verantwortlichkeiten)

Im Folgenden beschreiben wir einen konkreten Recovery-Plan für ein KMU:

Anforderung: Im Beispiel-KMU müssen nach einem Datenverlust die ERP-Systeme innerhalb von 6 Stunden wieder verfügbar sein

RecoveryZiele

- RTO (Recovery Time Objective), maximale Zeit zur Wiederherstellung 6 Stunden



- RPO (Recovery Point Objective), Maximale Datenmenge, die verloren gehen darf, 4 Stunden

Als kritische IT-Anwendungen, für die diese Recovery Ziele gültig sind: ERP-System, CRM-System, E-Mail-Server, Dateiablage

Verantwortlichkeiten

Rolle	Aufgaben
IT-Leitung	Koordination und Kommunikation mit Geschäftsleitung
Systemadministrator	Wiederherstellung der Daten
Externer Dienstleister	Unterstützung beim Cloud-Restore
Geschäftsführung	Entscheidung über externe Kommunikation und Eskalation
Mitarbeitende	Meldung von Problemen

Recovery-Ablauf (Schritt-für-Schritt)

1. Alarmierung: Backup-Fehler oder Angriff wird erkannt → IT-Leitung informiert
2. Analyse: Betroffene Systeme identifizieren, Schadensumfang bewerten
3. Recovery starten:
 - ERP-System aus Cloud-Backup wiederherstellen
 - Datenbank aus inkrementellem Backup zurückspielen
4. Validierung: Funktionstest, Datenintegrität prüfen
5. Kommunikation: Geschäftsführung informiert Kunden und Partner
6. Dokumentation: Ablauf, Dauer, Probleme festhalten
7. Lessons Learned: Prozess evaluieren, ggf. verbessern



Recovery-Test

- Letzter Test: 15. September 2025
- Ergebnis: ERP-System in 4 Stunden wiederhergestellt, keine Datenverluste
- Nächster Test geplant: Januar 2026

7. Fazit

Backup & Recovery sind keine Luxusoptionen, sondern überlebenswichtig für KMU. Wer heute handelt, schützt morgen seine Existenz.

Handeln Sie jetzt: Prüfen Sie Ihre Backup-Strategie, definieren Sie klare Recovery-Ziele und führen Sie einen Test durch. Denn Backup ist Pflicht – Recovery ist die Kür.

Wir hoffen, dass wir Ihnen unser Beitrag zum Thema „Backup & Recovery“ gefallen hat.

Sollten Sie Fragen oder Anregungen zu unserem Beitrag haben, dann freuen wir uns über Ihre Kontaktaufnahme per E-Mail. Folgen Sie uns gerne auch auf LinkedIn und besuchen Sie unsere Website.

E-Mail: info@steinbeis-industrial-it.com

LinkedIn: <https://www.linkedin.com/in/steinbeis-industrial-it>

Website: <https://steinbeis-industrial-it.com>