

Von vorhandenen Unterlagen zu einer belastbaren technischen Entscheidung.

Anonymisiertes Beispiel für einen mittelständischen Maschinenbaubetrieb.
Management-Sicht, technische Befunde, Zielbild, Umsetzung und Abnahmekriterien in einem Bericht.

ENTSCHEIDUNGSVORLAGE · STAND 26.08.2026

DATENBASIS

7 Unterlagen

Exporte, Übersichten und bekannte Schmerzpunkte

RISIKEN

8 Befunde

davon drei mit hoher Priorität

TECHNISCHES ERGEBNIS

5 Zielbilder

inklusive Umsetzung und Prüfkriterien

Was ein IT-Leiter erhält

- Risiken mit technischer Ursache und Wirkung
- konkretes Zielbild statt allgemeiner Empfehlung
- Arbeitspakete, Owner und Abnahmekriterien

Saubere Grenze

- keine produktive Vollprüfung
- Annahmen sind sichtbar markiert
- Verifikation im 90-Tage-Betriebsstart

01

Die größte Lücke ist der unbelegte Wiederanlauf der produktionskritischen Daten.

Der Alltag wirkt stabil. Aus den bereitgestellten Informationen ist jedoch nicht erkennbar, ob ERP und CAD-Dateien nach einem größeren Ausfall innerhalb eines akzeptablen Zeitfensters wiederhergestellt werden können.



 OBJEKTE SICHTBAR

16

10 Systeme, 6 Netzwerkgeräte



 HOHE PRIORITÄT

3

Restore, Offsite, MFA



 VOLLRESTORE

0

belastbare Nachweise sichtbar



 DATENVERTRAUEN

mittel

mehrere Aussagen noch offen

GESCHÄFTLICHE WIRKUNG

- ERP- oder Dateiausfall kann Fertigung und Versand mehrere Tage blockieren.
- Ohne Restore-Beleg bleiben Wiederanlaufzeit und möglicher Datenverlust reine Annahmen.
- Unbelegte MFA- und Vertretungswege erhöhen Angriffs- und Personenrisiko.

TECHNISCHE ENTSCHEIDUNG

- RPO und RTO für ERP und CAD mit dem Fachbereich entscheiden.
- Getrennte, gegen Überschreiben geschützte Sicherung plus Restore-Test etablieren.
- Privilegierte Zugänge, Alarmweg und Netzwerkänderungen nachvollziehbar machen.

EMPFOHLENER RAHMEN

Managed Core

Warum dieser Rahmen?

- quartalsweiser Restore-Beleg
- Config- und Zugriffsnachweise
- Portal, Reports und priorisierte Reaktion

3.200 EUR / Monat

laufender Betrieb, netto

90 Tage - 3.900 EUR

Der kostenlose Quick-Check empfiehlt einen Rahmen. Verbindlich werden Scope und Verantwortung erst im 90-Tage-Betriebsstart festgelegt; danach beginnt der laufende Betrieb.

02

Jede Aussage bleibt auf ihre Quelle und ihr Vertrauen zurückführbar.

Der Quick-Check unterscheidet belegte Information, plausible Annahme und offene Aussage. Das verhindert Scheingenaugkeit und zeigt, was im 90-Tage-Betriebsstart verifiziert werden muss.

QUELLE	STAND	NUTZBAR FÜR	VERTRAUEN	LÜCKE
System- und VM-Liste	07.08.	Rollen, Kritikalität, Zuordnung	hoch	Owner
Backup-Jobübersicht	06.08.	Jobstatus, Aufbewahrung, Ziele	mittel	Restore
Netzskizze	2024	Zonen, Übergänge, Abhängigkeiten	niedrig	veraltet
Monitoring-Auszug	05.08.	Abdeckung, Alarmmenge, Empfänger	mittel	Eskalation
Firewall-Export	fehlt	Regelwerk, Fernzugriff, Exposition	offen	Export

Sichtbares Systembild

DOMÄNE	OBJEKTE	KRITIKALITÄT	DATENLAGE
ERP	Applikation, Datenbank	hoch	Liste + Jobauszug
Datei / CAD	Dateiserver, CAD-Ablage	hoch	Liste, Restore offen
Identity	2 Domänencontroller	hoch	Export, Vertretung offen
Virtualisierung	2 Hypervisor	hoch	begleitete Übersicht
Backup	NAS, Jobs, Aufbewahrung	hoch	nur Jobübersicht
Netzwerk	Firewall, Core, 3 Access-Switches, WLAN	hoch / mittel	Skizze veraltet
Cloud	Microsoft 365	mittel	Unterlagen

GRENZE

Keine produktiven Logins, Scans oder Änderungen. Vollständigkeit des Inventars, reale Restore-Dauer und technische Wirksamkeit der Kontrollen werden erst im 90-Tage-Betriebsstart verifiziert.

03

Ein Befund ist erst handlungsfähig, wenn auch die technische Abnahme klar ist.

Die folgenden Punkte sind aus den bereitgestellten Unterlagen sichtbar. Die Verifikation und Umsetzung beginnt nach Vertrag und Scopefreigabe.

ID	PRIORITÄT	BEFUND	WIRKUNG	LÖSUNG	ABNAHME
R01	HOCH	kein Vollrestore belegt	RTO und Rückkehr offen	ERP und CAD isoliert testen	Start, Integrität, Dauer
R02	HOCH	Offsite / Immutable unklar	gemeinsamer Ausfallpfad	getrennte, geschützte Kopie	Löschschutz + Test
R03	HOCH	MFA für Firewall / VPN offen	privilegierter Angriffspfad	MFA, named accounts, Breakglass	100 % Scope, Ausnahmen
R04	MITTEL	Netzwerk-Configs unversioniert	Wiederanlauf und Ursachenanalyse langsam	täglicher Export, normalisierter Diff	unbekannter Diff alarmiert
R05	MITTEL	Alarmweg nicht eskaliert	kritische Meldung kann liegen bleiben	P1/P2-Matrix, Owner, Vertretung	Stichprobe bestanden
R06	MITTEL	EOL / Firmware unvollständig	Wartungsrisiko nicht planbar	Inventar, Supportstand, Frist	Roadmap freigegeben
R07	MITTEL	RPO / RTO nicht entschieden	Technik optimiert ohne Geschäftsziel	Ziele je kritischem Dienst	Fachbereichsfreigabe
R08	NIEDRIG	Abläufe nicht zentral sichtbar	vermeidbare Warnung / Ausfall	TLS- und Domainwächter	Vorlauf + Ticket

Technisches Zielbild für belegte Wiederherstellung

04

Backup-Erfolg wird in einen reproduzierbaren Wiederanlauf übersetzt.

Arbeitsvorschlag auf Basis der Unterlagen. RPO, RTO, Retention und Zielplattform werden im 90-Tage-Betriebsstart mit Fachbereich und IT bestätigt.

 HEUTE SICHTBAR 14 Tage lokale Aufbewahrung	 OFFSITE offen Trennung nicht belegt	 VOLLRESTORE 0 keine Messung sichtbar	 ZIELVORSCHLAG RPO 4 h RTO 8 h, zu bestätigen
--	---	--	--

Empfohlenes Sicherungsdesign

01 PRODUKTIV ERP, Datei, VMs Anwendungs- und VM-konsistente Sicherung, definierter Scope	02 SCHNELL ZURÜCK lokales Restore-Ziel kurze Wiederanlaufzeit, getrennte Backup-Credentials	03 GETRENNT GESCHÜTZT Offsite oder immutable separater Fehlerbereich, Löschschutz, längere Retention
--	---	--

ARBEITSPAKET	KONKRETE UMSETZUNG	ERGEBNIS / ABNAHME
Scope-Mapping	Inventar gegen Jobs, Ausschlüsse und Aufbewahrung abgleichen	12/12 zugeordnet
Schutz der Kopien	getrennte Identität, Löschschutz, Alarm bei Retention-Änderung	Testlöschung blockiert
ERP-Restore	DB plus Abhängigkeiten in isolierter Zielumgebung starten	Integrität und Dauer belegt
CAD-/Dateirestore	Berechtigungen, Pfade, Stichprobe und vollständigen Ordner prüfen	fachlich freigegeben
Wiederholung	Runbook, Termin, Owner und Evidenzvorlage festlegen	quartalsweise prüfbar

Abnahmekriterium

Ein Restore gilt erst als bestanden, wenn Zielsystem startet, Datenintegrität geprüft ist, gemessene Dauer zum freigegebenen RTO passt und offene Punkte mit Owner dokumentiert sind.

05

Drei technische Kontrollen schließen die größten Betriebsblindstellen.

Jede Kontrolle beschreibt Ausgangslage, Zielzustand, Umsetzung und den Nachweis, der anschließend regelmäßig geliefert wird.

01

Privilegierter Zugriff

SICHTBARER BEFUND

MFA und Vertretung nicht vollständig belegt

TECHNISCHES ZIELBILD

Personengebundene Konten, rollenbasierte Rechte, MFA, überwachte Notfallidentität und regelmäßige Rezertifizierung.

WIEDERKEHRENDER NACHWEIS

Zugriffsmatrix, MFA-Abdeckung, Ausnahmen, Last-Login und Freigabehistorie.

02

Netzwerk-Config

SICHTBARER BEFUND

Firewall- und Switch-Stände nicht versioniert

TECHNISCHES ZIELBILD

Herstellerkonformer Read-only-Export, Normalisierung volatiler Zeilen, täglicher Hash und Diff, Zuordnung zum Change.

WIEDERKEHRENDER NACHWEIS

Lesbarer Config-Änderungsnachweis mit Vorher/Nachher, Risiko, Owner und Rückfallplan.

03

Monitoring & Eskalation

SICHTBARER BEFUND

Mailflut ohne klare Priorität und Vertretung

TECHNISCHES ZIELBILD

Servicebasierte Checks, P1/P2-Matrix, deduplizierte Alarime, Owner, Stellvertretung, Quittierung und Runbook.

WIEDERKEHRENDER NACHWEIS

Abdeckungsreport, Alarmtimeline, Reaktionszeit und bestandene Eskalationsstichprobe.

06

Technik wird betreibbar, wenn Verantwortung und Rhythmus eindeutig sind.

Die Matrix ist ein Arbeitsvorschlag. Sie verhindert, dass Alarm, Freigabe, Umsetzung und Nachweis zwischen Kunde und Dienstleister liegen bleiben.

KONTROLLE	ALVEGIO	KUNDE	FREIGABE / NACHWEIS
Inventar & Kritikalität	Pflege, Drift, Report	Owner und Geschäftswirkung	monatlich
Backup-Health	Überwachung, Analyse, Ticket	Scope und Wartungsfenster	täglich
Restore-Test	Plan, Durchführung, Beleg	Ziel, Freigabe, Fachtest	quartalsweise
Monitoring	Checks, Priorität, Eskalation	Empfänger, Vertretung	laufend
Netzwerkänderung	Diff, Risiko, Dokumentation	Change-Freigabe	täglich / je Change
Privilegierte Zugriffe	Matrix und Review vorbereiten	Rollen und Entzüge freigeben	jährlich
Risiko & Roadmap	Bewertung, Vorschlag, Tracking	Entscheidung und Budget	monatlich

Nachweisrhythmus im Managed Core

TÄGLICH Backup-Health, Zertifikate, Config-Diffs	WÖCHENTLICH Health-Report und offene Maßnahmen	MONATLICH Operations Report, Patch, Kapazität, EOL
QUARTALSWEISE Restore-Test mit Ergebnisbeleg	HALBJÄHRLICH Firewall-Regelreview	JÄHRLICH Zugriffs-Rezertifizierung

07

Jede Phase endet mit einem überprüfbaren Ergebnis.

Der Plan macht Aufwand, Kundenzuarbeit und Abnahme sichtbar. Termine werden nach Scope- und Zugriffsfreigabe konkretisiert.

PHASE	TECHNISCHE ARBEIT	KUNDENZUARBEIT	EXIT-KRITERIUM
0 Vorbereitung	Scope, AVV, Zugriffsweg, Wartungsfenster	Owner, Freigaben, Systemliste	Scope signiert
1 Verifikation	Inventar, Abhängigkeiten, Backup- und Alarmquellen	Fachbereich, bestehende Exporte	Datenlücken benannt
2 Baseline	Monitoring, Zugriff, Backup, Config-Erfassung	Konten und Changes freigeben	Kontrollen aktiv
3 Nachweise	Restore, Alarmstichprobe, Config-Diff, Reports	Fachtest und Ergebnisfreigabe	Belege bestanden
4 Betrieb	Rhythmus, Ticketweg, Monatsreview, Roadmap	Entscheider und Budgetowner	Betriebsabnahme

Abnahme des Betriebsstarts

SCOPE

Alle betreuten Systeme, Ausschlüsse, Kritikalität und Owner sind bestätigt.

KONTROLLEN

Monitoring, Backup, Zugriff und Config-Nachweise liefern verwertbare Signale.

WIEDERANLAUF

Mindestens ein kritischer Restore und der Alarmweg sind praktisch belegt.

Wesentliche Abhängigkeiten

fachlicher Owner für ERP und CAD · genehmigtes Testziel · Wartungsfenster · lesbarer Export der Firewall · Zugriff auf Backup- und Monitoringdaten · definierter Entscheidungsweg

08

Der Wert liegt nicht in einer einmaligen PDF, sondern in wiederholbaren Belegen.

Jeder Nachweis besitzt Scope, Datenstand, Ergebnis, offene Punkte, Owner und nächsten Prüftermin. Technische Rohdaten bleiben verknüpft, der Bericht bleibt lesbar.

NACHWEIS	INHALT	RHYTHMUS	ENTSCHEIDUNG
Backup-Lücken-Report	Inventar gegen Jobs, Ausschlüsse, Retention	monatlich	Scope
Restore-Zertifikat	Quelle, Ziel, Dauer, Integrität, offene Punkte	quartalsw.	RTO
Config-Änderungsnachweis	Vorher/Nachher, Change, Risiko, Rückfallplan	täglich	Freigabe
Patch-Compliance	kritische Lücken, Ausnahmen, Fristen, Trend	monatlich	Risiko
EOL-Roadmap	OS, Firmware, Hardware, Supportende, Ersatz	monatlich	Budget
Monitoring-Abdeckung	kritische Dienste, Alarmweg, blinde Flecken	monatlich	Scope
SLA-/Reaktionsnachweis	Zeitlinie, Priorität, Annahme, Maßnahme	monatlich	Service
Firewall-Regelreview	breite, verwaiste und unnötige Regeln	halbjährl.	Change
Zugriffs-Rezertifizierung	Adminrechte, MFA, Ausnahmen, Entzüge	jährlich	Freigabe
Management Report	Status, Wirkung, Entscheidungen, 90-Tage-Plan	monatlich	Roadmap

Prinzip

Ein grüner Status ohne Scope, Datum und Prüfmethode ist kein belastbarer Nachweis. Jeder Bericht zeigt deshalb auch Datenlücken, Ausnahmen und den nächsten konkreten Schritt.

09

Der vorgeschlagene Rahmen schließt genau die sichtbaren Betriebs- und Nachweislücken.

Die Einordnung ist keine pauschale Verkaufsempfehlung. Sie folgt Scope, Kritikalität, Restore-Bedarf, Netzwerkanteil und dem gewünschten Nachweisniveau.

GRUNDLAGE

Ops Foundation

Portal, Inventar, Monitoring- und Backup-Gesundheit, Monatsreport und dokumentierter Betriebsverlauf.

EMPFOHLEN

Managed Core

Quartals-Restore, Config-Diffs, Patch/EOL, sichere Zugriffe, wöchentliche Reports und priorisierte Bearbeitung.

HÖHERE KRITIKALITÄT

Resilience Partner

1-Stunden-Reaktion, monatlicher Restore, Wirkungsanalyse, DR-Readiness und externe Angriffsflächenprüfung.

Managed Core

3.200 EUR / Monat

laufender Betrieb, netto

Betriebsstart 3.900 EUR

- mehrere kritische Geschäftsservices oder Bereiche
- 4 Stunden Reaktion bei kritisch im Servicefenster
- Scope nach Verantwortung und Betriebsintensität

Im vorgeschlagenen Scope enthalten

- Monitoring und priorisierter Alarmweg
- Backup-Health und Lückenreport
- quartalsweiser Restore-Test
- Config- und Änderungsnachweise
- Patch-, EOL- und Kapazitätsberichte
- sicheres Admin-Zugriffskonzept
- Firewall-Review und Zugriffsprüfung
- Portal, Betriebschronik und Reports

Nächster Schritt

Offene Daten bestätigen, Zielwerte mit IT und Fachbereich abstimmen und den Scope für den 90-Tage-Betriebsstart festlegen.

[QUICK-CHECK ANFRAGEN](#)

alveqio-infrastructure.com/quick-check/