Infrastructure Readiness Check: Ergebnisbericht

MUSTER · ANONYMISIERTES BEISPIEL

> Kein realer Kunde. Dieses Dokument zeigt, wie ein fertiger Readiness-Check-Report von Alveqio aussieht (Check M, Maschinenbau, ein Standort). Firma, Systeme und Zahlen sind erfunden.

Kunde	Nordwest Präzisionstechnik GmbH (Beispiel)
Standort / Landschaft	ein Produktionsstandort im Münsterland, ein Cloud-Projekt (Microsoft 365)
Check-Stufe	M
Erhebungszeitraum	02.06.2026 bis 11.06.2026
Erstellt von	Alveqio Infrastructure UG (haftungsbeschränkt), Leon Ostendorf
Datum / Version	12.06.2026 · Version 1.0

OBJEKTE IM SCOPE	HOHE RISIKEN	GETESTETE RESTORES	EMPFOHLENES PAKET
16	3	0	Managed Core

1. Management-Zusammenfassung

BETRIEBSBEWERTUNG **in Beobachtung**

Der Betrieb läuft im Alltag stabil, aber die Wiederherstellbarkeit im Ernstfall ist nicht belegt und zentrale Zuständigkeiten hängen an einer Person.

Die Fertigung von rund 120 Mitarbeitenden hängt an drei Säulen: dem ERP, dem CAD- und Dateiserver und einem produktionskritischen Netzwerk mit zentraler Firewall und Core-Switch. Im Tagesbetrieb funktioniert das. Das Geschäftsrisiko liegt im Ernstfall: Ein Ausfall des ERP- oder Dateiservers ohne getesteten Restore träfe die Produktion mehrere Tage, und gegenüber Cyberversicherung oder Audit ließe sich heute kein belastbarer Nachweis führen. Alveqio empfiehlt, den Betrieb planbar zu stabilisieren und vorab die fünf Quick Wins aus Abschnitt 8 umzusetzen.

Die drei wichtigsten Punkte:

1. Die Backups laufen, ein vollständiger Restore wurde nie getestet. Die Rückkehr in den Betrieb ist damit unbelegt und zeitlich nicht kalkulierbar.
2. Switch- und Firewall-Konfigurationen sind nicht versioniert. Änderungen sind nicht nachvollziehbar, ein Gerätetausch verlängert jeden Ausfall unnötig.
3. Administrative Zugänge liegen faktisch bei einer Person plus dem bisherigen Systemhaus, ohne dokumentierten Vertretungs- und Notfallweg und ohne MFA auf Firewall- und VPN-Management.

> **Empfehlung:** Start mit Managed Core (3.200 EUR / Monat netto), Onboarding ab 5.000 EUR netto, ergänzt um das Network Evidence Pack. Vorab die Quick Wins aus Abschnitt 8.

2. Scope und Asset-Übersicht

Nur die im Check vereinbarte Landschaft. Quelle der Daten in der letzten Spalte.

SYSTEM / ASSET	ROLLE	UMGEBUNG	KRITIKALITÄT	STATUS	QUELLE
`erp-app-01`	ERP-Applikation	Produktion	hoch	🟡	begleitete Sichtung
`erp-db-01`	ERP-Datenbank	Produktion	hoch	🟡	begleitete Sichtung
`file-cad-01`	Datei- und CAD-Server	Produktion	hoch	🟡	begleitete Sichtung
`dc-01 / dc-02`	Domänencontroller	Produktion	hoch	🟢	Export
`ts-01`	Terminalserver	Produktion	mittel	🟢	begleitete Sichtung
`pve-host-01 / -02`	Virtualisierung (Proxmox)	Produktion	hoch	🟡	begleitete Sichtung
`nas-backup-01`	Backup-Ziel (NAS)	Produktion	hoch	🔴	begleitete Sichtung
`fw-01`	Firewall und VPN	Produktion	hoch	🟡	begleitete Sichtung
`core-sw-01`	Core-Switch	Produktion	hoch	🟡	Export
`acc-sw-01 bis -03`	Access-Switches	Produktion	mittel	🟢	Export
`wlan-ctrl-01`	WLAN-Controller	Produktion	mittel	🟢	Export
`m365`	Microsoft 365 (Mail, Teams)	Cloud	hoch	🟡	Unterlagen

Abdeckung: 16 Objekte aufgenommen (10 Server und Dienste, 6 Netzwerkgeräte), davon 9 mit Monitoring-Bezug, 6 mit Sicherungsnachweis, 0 mit getestetem Restore-Nachweis.

3. Risikoampel

Sortiert nach Auswirkung und Dringlichkeit. Jede Zeile endet mit einem konkreten nächsten Schritt, nicht mit einer reinen Mängelliste.

Ampel-Verteilung: 3 hoch 4 mittel 1 niedrig

#	BEFUND	PRIORITÄT	AUSWIRKUNG WENN UNBEHANDELT	EMPFOHLENER NÄCHSTER SCHRITT	WER
1	Vollständiger Restore nie getestet	hoch	Unkalkulierbarer Produktionsausfall, kein Nachweis für Versicherung	Quartals-Restore-Test für ERP-DB und Dateiserver einführen, Ergebnis dokumentieren	Alveqio
2	Alle Sicherungen am selben Standort, Offsite-Kopie unklar	hoch	Brand, Diebstahl oder Ransomware trifft Primär- und Sicherungsdaten gemeinsam	Offsite- oder Immutable-Kopie einrichten und überwachen	Gemeinsam
3	Kein MFA auf Firewall- und VPN-Management	hoch	Fernzugriff mit nur einem Passwort ist ein primäres Angriffsziel	MFA für Management- und VPN-Zugänge aktivieren	Gemeinsam
4	Switch- und Firewall-Konfigs nicht versioniert	mittel	Änderungen nicht nachvollziehbar, langer Wiederanlauf nach Gerätetausch	Nächtlicher Config-Pull mit Versionierung und Diff	Alveqio
5	Admin-Wissen an einer Person plus Systemhaus	mittel	Kein Vertretungsweg, Klumpenrisiko bei Ausfall oder Kündigung	Rollen-, Vertretungs- und Notfallzugriff dokumentieren	Gemeinsam

#	BEFUND	PRIORITÄT	AUSWIRKUNG WENN UNBEHANDELT	EMPFOHLENER NÄCHSTER SCHRITT	WER
6	Monitoring-Alarme laufen unpriorisiert in ein Sammelpostfach	mittel	Kritische Meldungen gehen im Rauschen unter	Alarme priorisieren, Eskalationsweg definieren	Alveqio
7	Firmware von Core-Switch und Firewall veraltet, kein Wartungsfenster	mittel	Bekannte Schwachstellen, Risiko ungeplanter Neustarts	Wartungsfenster planen, Firmware in Stufen aktualisieren	Alveqio
8	Domain- und Zertifikatsabläufe nicht überwacht	niedrig	Plötzliche Zertifikatswarnungen, kurzer Dienstausfall	Ablaufüberwachung mit Vorlauf-Tickets einrichten	Alveqio

4. Backup und Restore

- **Sicherungslage:** Nächtliche Sicherung von ERP-Datenbank, Dateiserver und VMs auf eine lokale NAS (nas-backup-01), Aufbewahrung 14 Tage. Keine belegte Offsite- oder Immutable-Kopie.
- **Wiederherstellbarkeit:** Einzelne Dateiwiederherstellungen wurden durchgeführt. Ein vollständiger Restore der ERP-Datenbank oder eines kompletten Servers wurde nie getestet. RPO und RTO sind nicht definiert.
- **Einschätzung:** kritisch Ein Backup ohne Restore-Nachweis ist nur eine Hoffnung. Genau das ist hier der Fall.
- **Empfehlung:** RPO und RTO je kritischem System festlegen, eine Offsite- oder Immutable-Kopie einrichten, einen Quartals-Restore-Test mit dokumentiertem Nachweis etablieren. In Managed Core abgedeckt.

5. Monitoring und Reaktion

- **Heutige Sichtbarkeit:** Teilweises Monitoring von Verfügbarkeit einzelner Server und NAS-Füllstand über ein vorhandenes Werkzeug. Alarme gehen per Mail in ein Sammelpostfach.
- **Lücken:** Keine Priorisierung, kein definierter Eskalationsweg, keine Abdeckung von Firewall, Switches und Backup-Ergebnissen. Es ist nicht klar geregelt, wer Alarme sichtet.
- **Empfehlung:** Monitoring-Baseline über den vereinbarten Scope, priorisierte Meldungen, klarer Eskalationsweg, Backup- und Zertifikatergebnisse als aktive Signale.

6. Zugriffe und Nachweise

- **Zugriffsmodell:** Gemeinsam genutzte Domänen-Admin-Konten, ein Firewall-Admin-Konto, VPN ohne MFA. Notfallzugänge sind nicht dokumentiert.
- **Nachweislage:** Keine strukturierte Historie zu Wartung, Patches, Changes oder Restores. Ein Teil des Betriebswissens liegt beim bisherigen Systemhaus.
- **Empfehlung:** Im Onboarding ein Rollen- und Zugriffskonzept mit minimal notwendigen Rechten, MFA und dokumentiertem Notfallweg. Ab dann werden Wartung, Changes und Restores laufend als Nachweise geführt.

7. Empfohlenes Betriebsmodell

Folgestufe: Onboarding plus Managed Core.

PAKET	Managed Core, 3.200 EUR / Monat netto
ONBOARDING (EINMALIG)	ab 5.000 EUR netto

REAKTIONSZIEL	4 Stunden bei kritisch im Servicefenster
BEGRÜNDUNG	Rund zehn Server und Dienste plus sechs Netzwerkgeräte, produktionskritisches Netzwerk, Bedarf an Portal, Reports und belegten Restore-Nachweisen
OPTIONALE ZUSATZLEISTUNGEN	Network Evidence Pack (ab 390 EUR / Monat) für Switch- und Firewall-Diffs, zusätzlicher Restore-Test bei Bedarf

Hinweis: 50 Prozent des Check-Preises (Check M, 3.900 EUR netto) können auf das erste Onboarding angerechnet werden, wenn der Betrieb innerhalb von 30 Tagen beauftragt wird.

8. Quick Wins (sofort, geringer Aufwand)

1. Restore der ERP-Datenbank einmal vollständig testen und das Ergebnis dokumentieren.
2. Eine Offsite- oder Immutable-Kopie der wichtigsten Sicherungen einrichten.
3. MFA für Firewall- und VPN-Management aktivieren.
4. Monitoring-Alarme priorisieren und einen Eskalationsweg festlegen.
5. Wartungsfenster und Verantwortlichkeiten schriftlich festhalten.

9. Nächste Schritte

1. Bericht gemeinsam besprechen (30 Minuten).
2. Bei Zustimmung: Onboarding nach Managed Core starten, mit Zugriffskonzept, Monitoring, Reports und Kundenportal.
3. Erster Monatsbericht und erster dokumentierter Restore-Nachweis innerhalb der ersten 6 Wochen.

Methodik und Prüftiefe: Erhebung über vorhandene Unterlagen, Exporte, begleitete Sichtung und punktuell zeitlich begrenzte Leserechte. Im Check-Schritt wurden keine produktiven Änderungen vorgenommen. Bewertungen beruhen auf dem zum Erhebungszeitpunkt freigegebenen Informationsstand.
Alle Preise netto zzgl. USt. Der Readiness Check ist eigenständig beauftragbar und verpflichtet nicht zum Betrieb.
Alveqio Infrastructure UG (haftungsbeschränkt) · Kuckucksweg 12b · 48432 Rheine · contact@alveqio-infrastructure.com