



Paket D

Azure Backup & Recovery

Professionelle Azure Backup und Wiederherstellungslösung für kleine und mittlere Unternehmen

Dieses Paket richtet sich an Unternehmen, die Azure Workloads, virtuelle Maschinen und geschäftskritische Daten zuverlässig sichern und im Notfall strukturiert wiederherstellen möchten.

Unternehmensgröße	5 bis 30 Mitarbeitende
Azure Nutzung	Vorhandene Azure Umgebung
Azure VM	Vorhandene virtuelle Maschinen
Kritische Daten	Geschäftskritische Daten und Systeme vorhanden
Interne IT	Keine oder kleine interne IT
Ziel	Professionelle Datensicherung mit dokumentierter Recovery Strategie

Kernnutzen

- ✓ Strukturierte Azure Backup Architektur statt ungeplanter Einzellösungen
- ✓ Schutz von Azure VM, Azure Files und ausgewählten Storage Ressourcen
- ✓ Klare Backup Policies, Aufbewahrungsrichtlinien und Recovery Abläufe
- ✓ Dokumentierter Restore Test als Nachweis der Wiederherstellbarkeit
- ✓ Abschlussdokumentation als PDF für Management und Administration

Wichtige Abgrenzung

Paket D ist eine Projektleistung für Backup und Recovery. Es ersetzt keine monatliche Betreuung, kein 24/7 Monitoring und keine Business Continuity Planung.

Viele Unternehmen glauben: Azure = Backup. Das ist falsch. Azure stellt Verfügbarkeit bereit. Backup und Recovery müssen separat geplant, eingerichtet und getestet werden.

Enthaltene Leistungen

1. Azure Analyse

Leistungsbereich	Enthalten	Klare Abgrenzung
Analyse bestehender Azure Ressourcen	Prüfung von Subscriptions, Resource Groups, Virtual Machines, Storage Accounts, Netzwerken, Berechtigungen, Tags, Ressourcenzuständen und Kostenverursachern.	Keine Azure Migration, kein neues Infrastrukturdiseign, keine Architekturprojekte.
Analyse vorhandener Sicherungen	Prüfung vorhandener Backup Jobs, Recovery Services Vaults, Backup Policies, Aufbewahrung, geschützter Ressourcen und möglicher Sicherungslücken.	Keine Backup Optimierung, kein Restore Test und keine operative Backup Administration, sofern nicht vereinbart.
Analyse Recovery Anforderungen	Bewertung von RTO, RPO, Wiederherstellungsszenarien,	Keine Disaster Recovery Implementierung und keine Notfallübung.

Leistungsbereich	Enthalten	Klare Abgrenzung
	Abhängigkeiten und vorhandenen Wiederherstellungsprozessen.	
Analyse Business Anforderungen	Ermittlung kritischer Geschäftsprozesse, Anwendungen, Datenverlustgrenzen und organisatorischer Anforderungen.	Keine rechtliche Beratung, keine Compliance Audits und kein Business Continuity Plan.
Risikoanalyse	Bewertung von Backup Lücken, Wiederherstellungsrisiken, Single Points of Failure, Berechtigungsrisiken und möglichen Auswirkungen.	Keine Incident Response, keine Forensik und keine technischen Gegenmaßnahmen außerhalb des Projekts.

2. Backup Architektur und Recovery Konzept

Leistungsbereich	Enthalten	Klare Abgrenzung
Azure Backup Architektur	Planung geeigneter Backup Komponenten, Recovery Services Vaults, Schutzebenen, Backup Bereiche und Ressourcenzuordnungen.	Keine Azure Site Recovery Architektur und kein vollständiger Azure Neuaufbau.
Backup Konzept	Definition schützenswerter Systeme, Backup Umfang, Frequenzen, Schutzklassen und Verantwortlichkeiten.	Keine laufende Backup Überwachung und keine Business Continuity Planung.
Backup Design	Technische Ausarbeitung von Backup Strukturen, Policies, Zeitplänen, Sicherungszielen und Aufbewahrungsstufen.	Keine produktive Aktivierung außerhalb des vereinbarten Umfangs.
Recovery Konzept	Definition von Recovery Szenarien, Wiederherstellungsprioritäten, RTO, RPO, Verantwortlichkeiten und Eskalationswegen.	Keine produktive Wiederherstellung und kein Incident Response Management.
Aufbewahrungsrichtlinien	Festlegung täglicher, wöchentlicher, monatlicher und jährlicher Aufbewahrungszeiträume.	Keine rechtliche Bewertung und kein Compliance Audit.

3. Azure Recovery Services Vault

Leistungsbereich	Enthalten	Klare Abgrenzung
Recovery Services Vault	Planung und Einrichtung eines Azure Recovery Services Vault als zentrale Backup Verwaltungsinanz.	Keine Azure Site Recovery Implementierung.
Einrichtung Recovery Services Vault	Erstellung des Vaults, Basiskonfiguration und Anbindung unterstützter Ressourcen.	Keine Backup Aktivierung für nicht vereinbarte Systeme.
Strukturierung Backup Vault	Namenskonventionen, Schutzklassen, Backup Bereiche und organisatorische Trennung.	Keine Azure Landing Zone und kein Governance Projekt.
Backup Policies	Konfiguration von Sicherungsintervallen, Zeitplänen und Aufbewahrung für vereinbarte Ressourcen.	Keine individuelle Sonderarchitektur außerhalb der Azure Standardfunktionen.
Absicherung Backup Umgebung	Prüfung von Rollen, Zugriffen, Soft Delete, Multi User Authorization Optionen und Backup Warnmeldungen.	Kein vollständiger Security Review und kein Privileged Identity Management Projekt.

4. Azure VM, Azure Files und Storage Backup

Leistungsbereich	Enthalten	Klare Abgrenzung
Azure VM Backup	Einrichtung und Konfiguration von Azure Backup für vereinbarte Azure Virtual Machines inklusive erstem Backup Status.	Keine Betriebssystemadministration, kein Patch Management und kein Application Backup.
Betriebssystem Backup	Sicherung des Betriebssystemzustands der Azure VM über Azure Backup.	Keine Betriebssystemoptimierung oder Anwendungskonfiguration.
Daten Disk Backup	Einbindung angeschlossener Daten Disks in die Sicherungskonfiguration.	Keine Datenklassifizierung und keine Datenmigration.
Backup Zeitpläne	Definition und Konfiguration geeigneter Sicherungsintervalle.	Keine laufende Optimierung nach Projektabschluss.
Azure Files Backup	Einrichtung der Sicherung ausgewählter Azure Files File Shares.	Keine File Migration und kein Archivierungskonzept.
Azure Storage Backup	Analyse von Storage Accounts, Azure Files, Datenvolumen und Zugriffsmustern im Backup Kontext.	Keine Speicheroptimierung und keine Kostenoptimierung.

5. Monitoring, Reporting und Dokumentation

Leistungsbereich	Enthalten	Klare Abgrenzung
Backup Status Kontrolle	Prüfung von Backup Jobs, Sicherungsständen, Warnmeldungen und sichtbaren Backup Informationen.	Keine dauerhafte Betriebsüberwachung und kein 24/7 Monitoring.
Backup Erfolgsprüfung	Kontrolle abgeschlossener Sicherungen, Ausführungszeiten und verfügbarer Wiederherstellungspunkte.	Keine individuelle Auswertung außerhalb der Standardfunktionen.
Backup Fehleranalyse	Analyse sichtbarer Fehler und Warnmeldungen innerhalb bestehender Azure Backup Prozesse.	Keine Microsoft Support Eskalation und keine tiefgehende Fehlerbehebung außerhalb des Projekts.
Backup Reporting	Bericht über erfolgreiche Sicherungen, Fehler, Warnmeldungen, geschützte Ressourcen und Sicherungsstände.	Keine individuellen Management Dashboards und keine Compliance Reports.
Recovery Dokumentation	Dokumentation von Wiederherstellungsszenarien, Verantwortlichkeiten, Abläufen und empfohlenen Recovery Prozessen.	Kein Notfallhandbuch und keine laufende Dokumentationspflege.
Wiederherstellungsanleitung	Strukturierte Anleitung zur Wiederherstellung gesicherter Azure Ressourcen.	Keine Schulung und keine produktive Wiederherstellung.

6. Restore Tests

Leistungsbereich	Enthalten	Klare Abgrenzung
Test Restore VM	Geplanter Wiederherstellungstest für eine gesicherte Azure Virtual Machine inklusive Kontrolle der erfolgreichen Wiederherstellung.	Keine produktive Wiederherstellung und kein Disaster Recovery Test.
Test Restore Dateien	Geplanter Wiederherstellungstest einzelner Dateien oder Ordner inklusive Prüfung der Datenintegrität.	Keine umfangreiche produktive Datenrücksicherung.
Test Recovery Prozess	Überprüfung des definierten Recovery Prozesses anhand eines geplanten Testfalls.	Keine Notfallübung und kein Business Continuity Test.
Dokumentation der Ergebnisse	Dokumentation von Testergebnis, Auffälligkeiten, Wiederherstellungszeiten, Risiken und Empfehlungen.	Keine technische Umsetzung der Empfehlungen, sofern nicht separat vereinbart.

Fair Use und Projektumfang

Azure Subscription	1
Recovery Vault	1
Azure VMs	bis 5
Storage Accounts	bis 3
Restore Tests	1 Test

Ergebnis für den Kunden

- ✓ Vollständige Azure Backup Architektur
- ✓ Konfigurierter Recovery Services Vault
- ✓ Funktionierende Backup Jobs für vereinbarte Ressourcen
- ✓ Dokumentierte Backup Strategie
- ✓ Nachweis eines erfolgreichen Restore Tests
- ✓ PDF Dokumentation mit Architektur, Konfigurationen, Testergebnissen und Empfehlungen

Nicht enthalten

- Azure Migration
- Azure Architektur Neuaufbau
- Azure Site Recovery

- Disaster Recovery Standort
- Business Continuity Planung
- 24/7 Monitoring
- SOC, SIEM und Security Incident Response
- Microsoft 365 Backup, Intune Backup und On Premises Backup

Verwendete Portale

Azure Portal	Backup Vault erstellen, Backup Policies, Backup Monitoring, Restore Verwaltung
Azure Backup Center	Zentrale Backup Übersicht, Backup Jobs, Recovery Punkte, Backup Reports
Azure Monitor	Backup Alerts, Fehlererkennung und Monitoring

Preise

Leistung	Preis
Azure Backup Assessment	ab 350 €
Azure Backup Einrichtung	ab 800 €
Azure Backup + Restore Test	ab 1.200 €
Azure Backup Komplettpaket	ab 1.500 €
Weitere Azure VM	ab 80 €
Weitere Storage Accounts	ab 60 €
Zusätzlicher Restore Test	ab 250 €
Backup Dokumentation erweitert	ab 200 €
Backup Monitoring Erweiterung	ab 250 €

Kurzfazit

Paket D schafft eine klare, nachvollziehbare und getestete Backup Struktur für Azure Umgebungen. Der entscheidende Punkt ist nicht nur, dass Backups vorhanden sind, sondern dass der Kunde nachweisen kann, welche Systeme geschützt sind und ob eine Wiederherstellung tatsächlich funktioniert.