NOVASTOR

Best Practices beim Aufbau von Managed Backup Services

Best Practice

Eckpfeiler für Systemhäuser beim Aufbau von Managed Backup Services

Einleitung

Die Nachfrage nach professionellen Managed Backup Services wächst – und mit ihr die Chance für Systemhäuser, sich als unverzichtbarer Partner ihrer Kunden zu positionieren. Immer mehr Unternehmen erkennen, dass Datensicherung längst kein reines IT-Thema mehr ist, sondern ein geschäftskritischer Prozess, der über die Existenz des Unternehmens entscheiden kann.

Gleichzeitig steigen die Anforderungen: Ransomware-Angriffe nehmen zu, regulatorische Vorgaben wie DSGVO und NIS-2 verschärfen die Pflichten, und die IT-Infrastrukturen werden durch Cloud, Virtualisierung und hybride Arbeitsmodelle immer komplexer.

Viele Unternehmen – gerade im Mittelstand – können diese Herausforderungen mit eigenen Ressourcen nicht mehr bewältigen. Sie suchen einen Dienstleister, der die Datensicherung zuverlässig übernimmt und für deren Funktionsfähigkeit einsteht.

Für Systemhäuser bedeutet das:

Wer jetzt einen strukturierten Managed Backup Service aufbaut, sichert sich nicht nur wiederkehrende Umsätze, sondern stärkt die Kundenbindung und hebt sich nachhaltig vom Wettbewerb ab.

Doch der Aufbau eines solchen Services will gut geplant sein. Zwischen der ersten Idee und einem skalierbaren, profitablen Angebot liegen strategische, technische und organisatorische Entscheidungen, die von Anfang an richtig getroffen werden sollten.

Dieses Best-Practice-Dokument gibt Ihnen einen kompakten Leitfaden an die Hand: von der Service-Strategie über die technische Architektur und Sicherheitsanforderungen bis hin zu bewährten Betriebsprozessen und der richtigen Herstellerwahl.

Ergänzt wird der Leitfaden durch ein konkretes Praxisbeispiel, das zeigt, wie ein mittelständisches Systemhaus seinen ersten Managed Backup Kunden erfolgreich onboarded hat – Schritt für Schritt.

Nutzen Sie diese Eckpfeiler als Grundlage für Ihren eigenen Weg zum Managed Backup Service – und profitieren Sie dabei von der Erfahrung aus hunderten Backup-Projekten.

1. Service-Strategie und Konzeption

- **Klare Definition des Service-Umfangs:** Welche Systeme umfasst der Managed Backup-Service (z. B. Server-Backups, M365, Endpoint-Backups, Cloud-VMs, Datenbanken) – und welche nicht?
- **Mehrstufige Service-Level:** Welche Service-Level werden angeboten (z. B. Standard, Premium, Compliance) und wie grenzen sich diese voneinander ab?
- **Transparente SLAs:** Klarstellung, welche Wiederherstellungszeiten (RTO) und Datenstände (RPO) garantiert werden.
- **Angebotskalkulation:** Entwicklung eines verständlichen Preismodells (z. B. pro GB, pro Endgerät, pro Backup-Job) – nach Möglichkeit in verschiedenen Stufen.

---

2. Technische Infrastruktur

- **Zentrale Verwaltung:** Nutzung eines Backup-Management-Tools mit Multi-Tenant-Funktionalität, um Kunden sauber zu trennen.
- **Hybrid-Ansatz:** Kombination lokaler Backup-Ziele (z. B. NAS, dedizierter Backup-Server) mit Cloud-Zielen (z. B. S3-kompatibler Storage oder eigene Cloud).
- **Verschlüsselung:** End-to-End-Verschlüsselung (Client-Seite und im Ruhezustand). Schlüsselverwaltung muss klar geregelt sein.
- **Automatisiertes Monitoring und Reporting:** Backup-Jobs, Fehlermeldungen und Kapazitäten müssen automatisch überwacht werden.
- **Tested Restores:** Regelmäßige, automatisierte Wiederherstellungstests sind Pflicht.

---

3. Sicherheit und Compliance

- **Zero-Trust-Ansatz:** Backup-Systeme vom Produktivnetz trennen; minimal nötige Zugriffsrechte.
- **Offsite-/Air-Gap-Strategien:** Schutz vor Ransomware durch unveränderliche (immutable) oder offline verfügbare Kopien in der Cloud.
- **Rechtliche Aspekte:** DSGVO-konforme Datenspeicherung und Entwicklung von Auftragsverarbeitungsverträgen (AVV) mit allen Kunden.
- **Georedundanz:** Datenreplikation in verschiedene Rechenzentren oder Regionen.
- **Zertifizierungen:** Setzen Sie auf Rechenzentren mit ISO 27001, SOC 2 oder vergleichbaren Standards.

4. Betriebsprozesse

- **Automatisierung:** Backup-Jobs, Offsite-Kopien, Berichte und Fehlertickets automatisch auslösen.
- **Skalierbarkeit:** Prozesse so gestalten, dass neue Kunden einfach hinzukommen (Template- oder Policy-basierte Einrichtung).
- **Dokumentation:** Detaillierte technische und organisatorische Dokumentation (Backuppfade, RPO/RTO, Verantwortlichkeiten).
- **KPIs & Reporting:** Regelmäßig Reports über Backup-Erfolg, Speicherverbrauch und Wiederherstellungszeiten.

---

5. Kundenerlebnis und Support

- **Self-Service-Optionen:** Kunden können Berichte einsehen oder Wiederherstellungen anstoßen.
- **RTO-Übungen:** Testweise Restore mit dem Kunden durchführen, um Vertrauen und Awareness zu schaffen.
- **Proaktive Kommunikation:** Frühzeitige Meldungen bei Fehlversuchen oder Kapazitätsengpässen.

---

6. Hersteller- und Technologieauswahl

Empfohlene Kriterien bei der Tool-Wahl:

- Lokaler Anbieter aus Deutschland, um rechtliche Risiken (DSGVO, NIS-2 usw.) auszuschließen und Compliance-Anforderungen zu erfüllen
- Multi-Tenant-fähig
- API-Integration (für MSP-Automation/Abrechnung)
- Unterstützung verschiedener Plattformen (VMs, M365, Linux, Windows, NAS, Cloud-VMs)
- Immutable Storage-Option
- Unterstützung für automatisierte Test-Restores
- Enge Unterstützung und Begleitung beim Aufbau des Services durch den Backup-Hersteller
- Langfristig stabiles Preismodell

Praxisbeispiel

Inno GmbH* – Von der Idee bis zum ersten Managed Backup Kunden

Unternehmensprofil

Die Inno GmbH ist ein IT-Dienstleister mit 20 Mitarbeitenden, spezialisiert auf Systembetreuung, IT-Sicherheit und Cloudlösungen. Aufgrund von Kundenanfragen nach zuverlässigen und gemanagten Datensicherungen wird Managed Backup Service ins Portfolio aufgenommen.

Als erster Kunde wird ein Architekturbüro mit 30 Arbeitsplätzen und zwei virtuellen Hosts mit 10 virtuellen Maschinen (u. a. Dateiserver + ERP-System) ausgewählt, weil hier langjährige Kundenbeziehungen und ein gutes Vertrauensverhältnis bestehen.

*Fiktiver Name

1. Strategie und Planung

Ziel: Ein skalierbares, wiederkehrendes Serviceangebot schaffen, das die Daten der Kunden zuverlässig schützt und von der Inno GmbH zentral überwacht und gemanaged wird.

Schlüsselfragen in der Planungsphase:

- Welche Plattform ist technisch, wirtschaftlich und rechtlich geeignet?
- Wie sollen Backup-Ziele (RPO/RTO) definiert werden?
- Wie wird der Datenschutz sichergestellt (DSGVO, Auftragsdatenverarbeitung)?
- Wie werden Serviceverträge und SLAs gestaltet, um auch unter KRITIS und NIS-2 fallende Kunden zu bedienen?

Ergebnisse der Konzeptphase:

- Auswahl: NovaStor DataCenter Evolve mit lokaler Sicherung + Cloud-Storage in einem deutschen Rechenzentrum
- Einrichtung des NovaStor DataCenter Monitoring-Dashboards und der Abrechnungsreportings
- Definition eines Standard-Servicepakets (tägliche Sicherung, 30 Tage Vorhaltezeit, monatlicher Report, einmal pro Quartal automatisierte Restore-Tests)

2. Technische Umsetzung beim ersten Kunden

a) Analyse des Kundenbestands

- Welche Systeme sollen gesichert werden: 2 Hyper-V Hosts mit 10 virtuellen Maschinen, 1 NAS, 25 M365-Postfächer
- Datenvolumen: ca. 2,5 TB aktiv
- Kritische Systeme: ERP und CAD-Server

b) Backup-Design

- Lokales Vollbackup täglich auf NAS (inkrementell)
- Replikation in die Cloud jede Nacht
- Automatische Restore-Tests alle 90 Tage
- RPO = 4 Stunden, RTO = 3 Stunden

c) Technik einrichten

- Installation von Backup-Agenten auf Servern
- VPN-Verbindung zur Inno GmbH (technisch zwar nicht notwendig, aber gewünscht)
- Einrichtung von Benachrichtigungen im zentralen Dashboard

d) Initiales Vollbackup

- Seed-Backup auf transportable Festplatte, physisch ins Rechenzentrum gebracht (aufgrund der langsamen Internetverbindung)
- Danach nur inkrementelle Sicherungen über WAN

e) Automatisiertes Monitoring

- Alarme bei fehlgeschlagenen Backups an diensthabende Techniker
- Wöchentliche Qualitätssicherung

f) Test-Restore

- Wiederherstellung einer CAD-Projektdatei als Nachweis
- Kunde erhält Protokoll zur Abnahme

g) Dokumentation & Übergabe

- Backup-Plan + Notfallhandbuch werden erstellt und übergeben
- Regelmäßiger Audit-Report wird vereinbart, der Funktionalität sicherstellt

4. Betrieb, Kontrolle & Lessons Learned

Regelbetrieb:

- Dashboard-Prüfung täglich automatisiert (Ergebnis per E-Mail an Technik-Team)
- Monatlicher Backup-Bericht an Kunden
- albjährlicher Desaster-Drill (Restore-Test)

Wesentliche Erkenntnisse:

Standardisierung spart Zeit:
Einheitliche Templates und Prozesse ermöglichen Skalierung.

Kommunikation ist zentral:
Kunden wollen wissen, dass Sicherungen funktionieren.

Dokumentation zählt:
Klare Abgrenzung von Verantwortlichkeiten (Backup vs. Restore-Unterstützung).

Technische Redundanz ist Pflicht:
Zweites NAS als Ausfallsystem im Rechenzentrum.

Personelle Redundanz ist auch Pflicht:
Es werden insgesamt 3 Techniker auf das System und die Prozesse trainiert.

Hersteller der Backup Software muss unterstützen:
Nur mittels Unterstützung durch die Erfahrung des Herstellers ist es für ein Systemhaus wie die Inno AG möglich, neben dem Tagesgeschäft einen Managed Backup Service aufzusetzen.

5. Ergebnis

Der Kunde war nach dem erfolgreichen Test-Restore überzeugt und verlängerte den Vertrag nach drei Monaten auf einen erweiterten Serviceumfang (inkl. Microsoft 365 Backup).

Die Inno GmbH nutzte diesen Piloten als interne Referenz, schulte weitere Mitarbeitende und gewann innerhalb von sechs Monaten vier neue Kunden auf Basis des standardisierten Managed Backup Service.

Fazit

Die Inno GmbH hat nach den ersten 6 Monaten ein positives Fazit gezogen und kann nun den Managed Backup Service bei weiteren Kunden ausrollen. Gleichzeitig ist es möglich, dass die Inno GmbH weitere Managed Services einführt.

Kernaussage

Der erfolgreiche Start des ersten MBS-Kunden war für die Inno GmbH ein Wendepunkt:

Die Inno GmbH konnte zeigen, dass auch ein kleineres IT-Haus mit klarer Struktur, Lernbereitschaft und Kundenorientierung einen professionellen Managed Service mit Unterstützung des Herstellers etablieren und auch skalieren kann – dies trotz begrenzter Ressourcen.

NOVASTOR

www.novastor.de