Case Study Migration Fileserver zu Microsoft 365

- **Begrüßung: „Guten Tag, mein Name ist Jörg Brors.“,**
  - **Über 20 Jahre Erfahrung mit Fileservern**
  - **7 Jahre Erfahrung mit Sharepoint Online und Teams**
- ~~**Kurze Vorstellung des Themas**~~**: Ablösung klassischer Fileshares durch SharePoint Online & Microsoft Teams.**
- **Ziel des Projekts:**
  - **Nicht nur Daten verschieben, sondern Zusammenarbeit modernisieren.**
  - **Klare Berechtigungsmodelle und zentrale Governance-Struktur schaffen.**
  - **Informationsschutz (DLP, Sensitivity Labels) direkt integrieren.**
- **Vorgehensweise:**
  - **Technische und organisatorische Umsetzung kombinieren.**
  - **Einheitliches Berechtigungsmodell (Owner, Member, Visitor).**
  - **Governance-Prozesse und automatisierte Freigaben einführen.**
- **Nutzen:**
  - **Transparente Rechteverwaltung.**
  - **Einheitliche Zusammenarbeit in Teams & SharePoint.**
  - **Zukunftssichere Cloud-Architektur für Fachbereiche.**
- ~~**Abschluss der Einleitung**~~**:**
  - **„Ich zeige Ihnen, wie das Projekt aufgebaut ist,**
    welche Schritte notwendig sind
    und welche Faktoren über den Erfolg entschieden können.“

Agenda

- ~~**Überblick über die Präsentationsstruktur**~~**.**
- **Die Präsentation besteht aus zwei Hauptteilen.**
    - **Teil 1: Berechtigungen & Informationsschutz**
        - **Governance, Datenklassifizierung, sichere Freigaben.**
    - **Teil 2: Migrationsstrategie**
        - **Planung, Test und Durchführung der eigentlichen Datenmigration.**
        - **Ziel:**
    - **Zeigen, wie Technik, Organisation und Sicherheit zusammenspielen.**
    - ~~**Abschluss**~~**:**
    - **Kurzes Fazit mit den wichtigsten Ergebnissen und Erkenntnissen.**
    - ~~**Übergang**~~**:**
    - **„Beginnen wir mit dem ersten Teil – den Berechtigungen und dem Informationsschutz.“**

Teil 1 – Berechtigungen & Informationsschutz

- ~~**Einstieg in den ersten Hauptteil**~~**: Berechtigungen & Informationsschutz.**
- **Ziel: Aufbau eines neuen Sicherheits- und Berechtigungskonzepts in Microsoft 365.**
- **Fokus:**
    - **Zugriffe nachvollziehbar regeln.**
    - **Daten richtig klassifizieren.**
    - **Richtlinien konsequent anwenden – ohne Produktivität einzuschränken.**
- **Herausforderung: Balance zwischen Sicherheit und Benutzerfreundlichkeit.**
- **Aufbau in vier Themenblöcke:**
  1 Ziele & Grundprinzipien
  2 Freigaben & Lebenszyklus
  3 Governance & Onboarding
  4 Richtlinien, Benutzerakzeptanz & Support
- **Diese Struktur deckt den gesamten Datenlebenszyklus ab:**
    - **von der Rechtevergabe bis zum laufenden Betrieb.**
-
- ~~**Übergang**~~**:**

  Schauen wir uns nun an, wie diese Struktur in der Praxis funktioniert –
  beim Thema Ziel & Grundprinzipien

01/01 – Ziel & Grundprinzipien

- Warum:
  - Für eine Einheitliche Berechtigung Logik für Teams & SharePoint.
- **Umsetzen einer einheitlichen Berechtigungslogik:**
  - **In Teams nutzen wir das gruppenbasierte Berechtigungsmodell,**
  - **in SharePoint die klassischen SharePoint-Berechtigungen – beide folgen denselben Sicherheits- und Governance-Prinzipien.**
- Umsetzung des **Least-Privilege-Prinzips**:
  - Jeder bekommt nur die Rechte, die er für seine Arbeit braucht.
- **Rollenstruktur / Rollenmodell**:
  - **Owner** = Verwaltung, Mitgliederpflege, Freigaben
  - **Member** = aktive Mitarbeit
  - **Visitor** = Leserechte
  - **Guest** = zeitlich begrenzter Zugriff mit Genehmigung
- Zentrale Verwaltung in der Cloud:
  - **Teams** = Microsoft 365 Groups
  - **SharePoint** = Sicherheitsgruppen
  - **Warum**:
    - Gruppenpflege an einem Ort mit Mechanismen der Cloud
    - Keine Vermischung mit Gewachsene Prozessen von On-Prem
- **Einheitliches Modell**: **Eine Gruppe pro Team**
  - Keine doppelten oder verschachtelten Berechtigungen.
    - NTFS wurde teilweise Abteilung aus Team Gruppen gebildet
    - Cloud: **Owner Struktur** , **Access Reviews**, **Flache Strukturen**
  - **Zugriff ist somit klar nachvollziehbar und revisionssicher**.
- **Automatische Erstellung neuer Teams/Sharepoints über Vorlagen** (Namenskonventionen, **Berechtigungen**).
- Alle Arbeitsräume folgen denselben Regeln und Strukturen.
- Regelmäßige Prüfung & Archivierung inaktiver Teams.
- Ergebnis: **Einheitliche, sichere und standardisierte Berechtigungslogik – Grundlage für Governance, Informationsschutz und Compliance**.

01/02 – Freigabe & Lebenszyklus

- Fokus:
  - **Datenfreigaben und Lebenszyklussteuerung**.
- Ziel:
  - Zugriffe **gezielt, zeitlich begrenzt und nachvollziehbar**.
- **Interne Freigaben**:
  - Über Teams & zugehörige Microsoft 365-Gruppen.
  - „Closed by default“ – keine offenen Freigaben.
  - Freigaben erfolgen aktiv durch Owner.
- **Externe Freigaben**:
  - Keine anonymen Links.
  - Links Nur „Ausgewählte Personen“ **mit Ablaufdatum** ; oder **Gäste mit Ablaufdatum**.
  - Zugriff ausschließlich im Browser bei nicht verwalteten Geräten.
  - Downloads & Synchronisation blockiert (App-enforced Restrictions).
    - Technisch umgesetzt durch eine Kombination aus Conditional Access und Session Controls in Defender for Cloud Apps
- **Zugriffssteuerung & Ablauf**:
  - Access Packages & Group Expiration Policies → automatische Laufzeitbegrenzung
    - Wird über Entra ID Gesteuert Gruppen unter Gruppe Expiration.
  - Access Reviews → entfernen ungenutzter Berechtigungen.
  - Entweder über Entra ID Governance Lizenz bzw Microsoft Entra Suite oder Eigenentwicklung
- **Regelmäßige Prüfungen**:
  - Überprüfung bestehender Freigaben (manuell + automatisiert).
  - Inaktive oder veraltete Zugriffe werden entzogen.
- **Teams-Archivierung**:
  - Automatische Erkennung inaktiver Teams.
  - Archivierte Inhalte bleiben lesbar, aber geschützt.
- Ergebnis:
  - Vollständiger, geregelter Datenlebenszyklus –
    von der Freigabe bis zur Archivierung.
  - **Transparent, sicher und compliant**.

1/03 – Governance & Onboarding

- Thema:
  - **Governance & Onboarding**
- Ziel:
  - Regeln und Prozesse **dauerhaft verankern & messbar machen**.
- Das Thema Governance und Kontrolle erreichen wir durch :j
  - **Team-Erstellung nur über Templates**
    - Vordefinierte Rollen, Richtlinien
    - Einheitliche Struktur und Compliance ab Start
  - **Monitoring & Berichte**
    - Purview & SAM liefern kontinuierliche Reports zu:
      - Freigaben
      - Klassifizierungen
      - Compliance-Verstößen
- **DLP und Sensitivity Labels** schützen unsere Daten:
  - Labels klassifizieren und schützen Dokumente automatisch
  - DLP verhindert, dass sensible Informationen unkontrolliert geteilt werden. Das ist ein zentraler Baustein für Compliance und Datensicherheit
- **Regelmäßige Reviews**
  - Entfernen inaktiver Teams & Benutzer
  - Sicherstellung aktueller Strukturen
- **Automatisiertes Onboarding über Access Packages**
  - Beantragung von Teams oder Rollen
  - Genehmigungs-Workflows & Ablaufdaten integriert
- **Benutzerschulung & Awareness**
  - Regelmäßige Trainings direkt in Teams
  - Fokus: sicheres Arbeiten & Verständnis für Richtlinien
- Ergebnis:
  - Governance technisch umgesetzt **und** organisatorisch im Alltag verankert.

01/04 – Richtlinien, User Adoption & Support

- ~~Thema:~~
  - ~~**Richtlinien, Benutzerakzeptanz und Support**~~
- Ziel:
  - **Stabiler Betrieb** und **aktive Benutzerbeteiligung**.

Governance-Richtlinien:

- Regeln für:
  - Team-Erstellung, Benennung, Klassifizierung, Archivierung.
  - Externe Freigaben & Sensitivity Labels.
- Alle Vorgaben im **Governance-Handbuch** dokumentiert.
- Regelmäßige Überprüfung & Aktualisierung durch Governance Board.

User Adoption & Awareness:

- Schulungen und kurze Video-Guides für Endanwender.
- Kommunikation über **Viva Engage** und interne Teams-Kanäle und ein Champions Programm
  - Das Champions Programmbedeutet, engagierte Mitarbeitende als geschulte Multiplikatoren zu fördern und zu fordern.
- Ziel: Verständnis für Sicherheit, Struktur & Effizienz in M365.
- **Hauptbotschaft**:
  - SharePoint & Teams sind **sicherer, strukturierter, effizienter** als Fileshares.

Support & Betrieb:

- **Dreistufiges Supportmodell:**
  1. 1st Level – Benutzeranfragen & Freigabeprobleme
  2. 2nd Level – Richtlinien, DLP, Berechtigungen
  3. 3rd Level – Governance, Entra ID, SAM
- Monitoring & Alerts (Admin Center, Purview, Defender).
- Regelmäßige Reviews zur Qualitätssicherung & Compliance.

Backup & Restore:

- Versionierung, Retention & Backups aktiv. Hier bieten sich Avepoint oder Veem an..
- Regelmäßige **Restore-Tests** zur Überprüfung der Wiederherstellbarkeit.
- Nutzung zertifizierter Cloud-Umgebungen für Datensicherung.

Ergebnis:

- Sicherer, stabiler und gut akzeptierter Betrieb von Microsoft 365.
- Governance & Support als feste Bestandteile des Alltagsbetriebs.

Übergang: danach kommen wir zur Migration Strategie , sind zu diesem Modul fragen

Migrationsstrategie

- Übergang zum zweiten Hauptteil der Präsentation.
    - Nun kommen wir nachdem wir die Grundlagen für Berechtigung und Informationsschutz gelegt haben zur Migrationsstrategie
      Migrieren von Dateifreigaben zu SharePoint und OneDrive - Migrate to Microsoft 365 | Microsoft Learn
      nach der Methode Migration / Bewerten und Korrektur/ Vorbereitung Ihrer Umgebung/ Migration / Benutzer-OnBoarding
- Fokus: **Migrationsstrategie** – der Weg von Fileserver zu Microsoft 365.
- Ziel: Migration technisch sauber, nachvollziehbar und steuerbar umsetzen.
- Wichtiger Punkt:
    - Nicht einfach „kopieren“, sondern **verstehen, bewerten, bereinigen, dann migrieren**.
- Strukturierter Ablauf in vier Phasen:
  1 Erfassen, Analysieren & Bewerten
  2 Planen & Pilotieren
  3 Migrieren
  4 Onboarding der Benutzer
- Grundidee: **Kontrollierter Veränderungsprozess** statt reiner Datenübertragung.
- Organisation:
    - Klare Verantwortlichkeiten
    - Definierte Zeitfenster
    - Sauberer Übergang in den produktiven Betrieb
- Ziel: Nachhaltige, nachvollziehbare Migration mit minimalem Risiko.

02/01 – Erfassen, Analysieren & Bewerten

- Ziel:
  - **Bestehende Datenlandschaft systematisch erfassen & bewerten**.
- Fokus:
  - **Relevante Daten identifizieren, Verantwortlichkeiten festlegen**.

Bestandsaufnahme:

- Vollständige Analyse der Fileshares:
  - Verzeichnisse, Dateitypen, Größen, Nutzungshäufigkeit.
  - Bestehende NTFS-Berechtigungen erfassen.
- Prüfung technischer Grenzen:
  - Pfadlängen, Dateigrößen, Sonderzeichen.
  - Nicht migrierfähige Inhalte anpassen oder ausschließen.

ROT-Analyse (Redundant, Obsolete, Trivial):

- **Redundant:** doppelte oder mehrfach gespeicherte Daten.
- **Obsolete:** veraltete oder nicht mehr genutzte Daten.
- **Trivial:** Inhalte ohne geschäftlichen Mehrwert.
- ROT-Daten werden **bereinigt oder archiviert,** und zwar vor der Migration.

Datenherkunft & Nutzung:

- Unterscheidung:
  - Benutzerdateien vs. Prozess-/Systemdaten.
- Prozessdaten & technische Dateien → bleiben im Archiv oder Azure Storage.
- Nur **relevante, aktive Arbeitsdaten** gehen in Teams & SharePoint.
  - Teamarbeitsdaten gehen in Teams, unternehmensweite oder langfristige Daten in SharePoint.

Verantwortlichkeiten:

- Jeder Datenbereich muss mindestens zwei **Owner** besitzen, es kann auch über eine Stellvertreter Regelung gelöst werden.
- Verantwortlichkeiten im **Governance-Dashboard** dokumentiert.

DLP & Klassifizierung:

- Einsatz von **Data Loss Prevention (DLP)-Scans**.
- Automatische Erkennung sensibler Inhalte.
- Zuweisung passender **Sensitivity Labels**.

Berechtigungen & Struktur:

- Alte NTFS-Rechte überprüft & bereinigt.
- Berechtigungen in **Microsoft 365-Gruppen** überführt.
- Nur eine Berechtigungsebene pro Datenbereich (keine Verschachtelungen).

Ergebnis:

- Saubere, geprüfte und **compliancegerechte Datenbasis**.
- Grundlage für die **Pilotmigration** geschaffen.

02/02 Planen & Pilotieren

Start der **Planungs- und Pilotphase** nach Abschluss der Datenanalyse.

- Ziel:
  - **Strukturierte, risikoarme Migrationsstrategie** entwickeln und testen.

Clusterbildung:

- Bildung logischer Datencluster:
  - Nach Fachbereichen, Datentyp, Komplexität, Sicherheitsstufe.
- Vorteil: Gezielte Planung & Steuerung pro Cluster.

Migrationswelle defenieren

- **Fachbereiche/ Teams** werden in Wellen definiert; **Wichtig** → Aus den Verschieden Clustern. Dier ersten Wellen sind Piloten, daher nicht die komplexen Cluster zuerst

Toolauswahl:

- Einsatz von **Migration Manager** und **ShareGate**.
- Vergleich & Validierung von:
  - Performance & Stabilität.
  - DLP-Regeln & Sensitivity Labels.
  - Berechtigungsübernahmen & Metadaten.

Pilotmigration / Pilotphase:

- Start mit **einfachen, gut strukturierten Clustern**.
- Ziel: Tools, Prozesse & Berechtigungsübernahme **realitätsnah testen**.

Ablauf der Pilotmigration:

1. **Initial Load** – erste Datenübertragung.
2. **Read-Only-Phase** auf Fileserver → keine Änderungen mehr möglich.
3. **Delta-Sync & Cutover** – finale Synchronisation & Umstellung.

Feedback & Optimierung:

- Rückmeldung aus Pilotgruppen werden genutzt, um:
  - **Kommunikations- und Benachrichtigungswege** zu verbessern.
  - **Ablaufprozesse zu verfeinern**.
    - Vor allem Themen wie Copilot und Zugriffe sollten in die Bewertung mit einfliesen.

Dokumentation:

- **Ergebnisse festgehalten**:
  - Datenintegrität, Berechtigungen, Labels, Metadaten.
- Alle Tests im **Migrations-Dashboard** nachvollziehbar dokumentiert.

Migrationsplan anpassen nach erfolgreicher **Pilotphase:**

- **Getestete, skalierbare und sichere Migrationsstrategie**.
- Grundlage für den **produktiven Rollout**.

2/ 3 Migrieren

- Phase:
  - **Produktive Migration** – Umsetzung der getesteten Strategie.
- Ziel:
  - **Sichere, nachvollziehbare und stabile Datenübertragung**.

Plan & Vorbereitung:

- Durchführung nach Rollout-Plan:
  - Definierte **Cluster, Zeitfenster und Verantwortlichkeiten**.
- Vor jedem Durchlauf:
  - **Abhängigkeiten prüfen** (Applikationen, Benutzer, Freigaben).
  - **Backups sicherstellen** – z. B. über Veeam oder AvePoint.

Schulung & Begleitung:

- Parallel: **Trainings für Fachbereiche**.
  - Themen: Freigaben, Versionierung, Sensitivity Label Prozesse und den Umgang mit DLP-Einschränkungen.
  - Ziel: Sicherer Umgang mit der neuen Umgebung.

Durchführung der Migration:

- Einsatz von **Migration Manager** oder **ShareGate**.
- **Automatisierte Übertragungen** pro Cluster.
- Fortschritt & Fehler z.B. über **Power BI-Dashboards** überwacht

Ablauf in Migrationswellen:

1. **Initial Load** – erste vollständige Datenübertragung.
2. **Delta-Sync** – Synchronisation der Änderungen.
3. **Cutover** – Umstellung, alter Fileshare nur noch lesbar.

Validierung & Qualitätssicherung:

- Nach jeder Welle: Prüfung auf
  - Vollständigkeit der Dateien,
  - Metadaten, Sensitivity Labels, Berechtigungen.
- Ergebnisse im **Migration Summary Report** dokumentiert.

Abschluss & Übergabe:

- Alte Strukturen archiviert oder gelöscht nach Freigabe.
- Übergabe an **Governance-Team** für den laufenden Betrieb.
- Überwachung durch **Microsoft Purview & SAM**:
  - DLP-Regeln, Freigaben & Compliance-Verstöße automatisch geprüft.

Ergebnis:

- Migration **technisch & organisatorisch abgeschlossen**.
- **Stabiler, sicherer Betrieb** in Microsoft 365 etabliert.

Fazit

Klare Migrationsstrategie & strukturierte Umsetzung

- Ablösung der alten Fileserver-Strukturen durch moderne Cloud-Lösungen
- Einheitliche Datenhaltung in SharePoint & Teams
- Automatische Versionierung & zentrale Überwachung
- Grundlage für einen nachhaltigen, skalierbaren Betrieb gelegt

Sichere Cloud-Architektur mit Governance & DLP

- Höhere Sicherheit, Transparenz und Governance
- Microsoft Entra ID: Zugriffsschutz, Identitäten, Conditional Access
- Microsoft Purview: DLP, Sensitivity Labels, Compliance
- SharePoint Advanced Management: Kontrolle von Freigaben & Sites
- Sensible Daten werden aktiv geschützt (DLP + Labels)

Einheitliche Richtlinien und Supportprozesse

- Klare Rollenstruktur:
- Owner verwalten Teams & Freigaben
- Member arbeiten aktiv mit
- Visitor haben Leserechte
- Zentral definierte Governance-Regeln
- Prozesse & Policies in der gesamten Plattform einheitlich umsetzbar

Benutzerakzeptanz durch gezielte Schulung

- Regelmäßige Schulungen & Awareness-Maßnahmen
- Mitarbeitende verstehen Freigaben, Labels & DLP
- Regeln werden im Alltag aktiv angewendet
- Mehr Sicherheit durch besseres Benutzerverhalten

Zukunftsfähige Plattform für Zusammenarbeit

-
- • Kombination aus Technik, Governance und Benutzerkompetenz
- • Konform, sicher und langfristig skalierbar
- • Moderne Grundlage für digitale Zusammenarbeit über Teams & SharePoint

Abschluss

- • Dank für die Aufmerksamkeit
- • Einladung zu Fragen & Diskussion