



Partner-Webinar

Teilnehmer Handout
21. September 2022

Von der Serverstruktur zum
kollaborativen Datenmanagement mit Microsoft 365

netrics

Über uns...



Urs Wermelinger
irs.wermelinger@netrics.ch

netrics



Andreas Naef
andreas.naef@beetroot.ag

beetroot
Strategien für die digitale Arbeitswelt

Fakten & Zahlen



140 Experten



4 Büros

Biel
Zürich

Basel
Thun



1 CISO
6 SCRUM Master
8 Change Practitioner
8 Cloud Solution Architects
> 14 DevOps Engineers



1. Platz
Cloud Service Provider
Bilanz Rating 2020



Zertifizierung

ISO 9001 / 20000 /
27001 / 27018

Modern Workplace
Cloud Transformation
Communication
Network
Datacenter

> 350

Kunden in der Cloud



Firmengründung im 2002



7x24x365 Support



10 Network Engineers
> 40 System Engineers
> 5 Service Manager
> 15 Customer Care Specialists



Microsoft
Partner

Gold Application Development
Gold Application Integration
Gold Cloud Platform
Gold Cloud Productivity
Gold Collaboration and Content
Gold Data Platform
Gold Datacenter
Gold DevOps
Gold Small and Midmarket Cloud Solutions
Gold Windows and Devices



SAP® Certified
in Cloud and Infrastructure Operations



Microsoft Azure

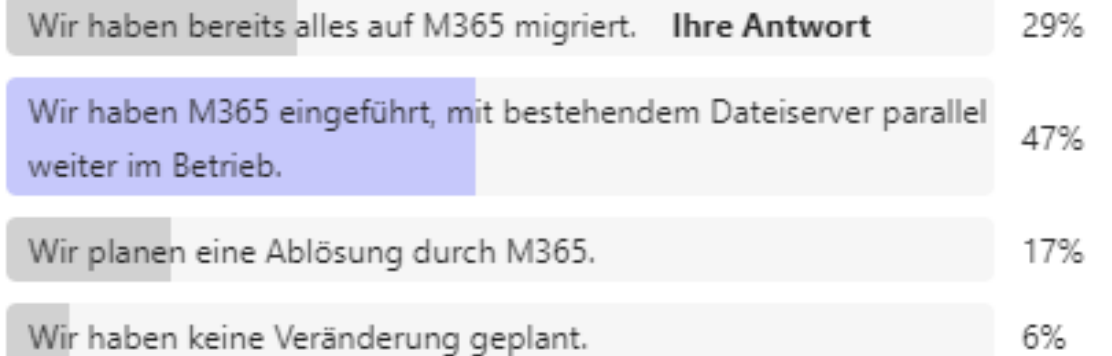




Datei-Server im Einsatz?

Umfrage unter den Teilnehmenden

Haben Sie einen Datei-Server im Einsatz und/oder planen...



78 Antworten

Unterschiedliche Interessen unter einem Hut

Geschäftsleitung



- Compliance
- Wie arbeiten wir sinnvoll mit M365?
- **Kosten & Nutzen & Risiken**

Alles im Griff?

ICT



- Governance & Control
- Nutzende-Unterstützung und Nutzende Self-Service
- **Hardware & Software Zyklen**

Mehr mit weniger!

Nutzende



- Modernes Arbeiten
- Produktivität + Fun
- Individualität ist möglich
- **Zeit und Ortsunabhängig**

Get my job done.

Sicherheit

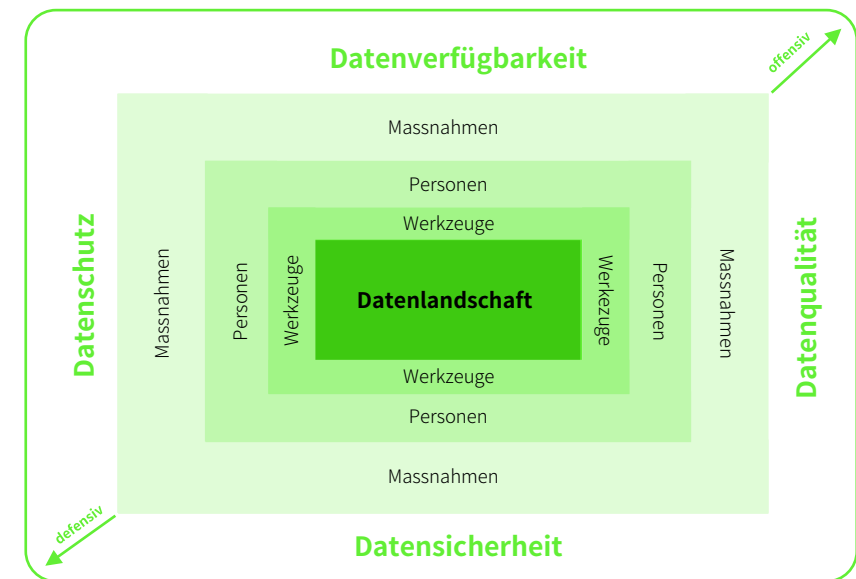
- **Cyber-Pandemie**
- Zunahme der **Schatten-IT**
- **65 %** mehr Cyberattacken in der Schweiz in 2021 vs. 2020
- **70%** und mehr der Hacking Vorfälle werden mithilfe gestohlener Anmeldeinformationen verursacht.



Quelle:
Computerworld Januar 2022 <https://www.computerworld.ch/security/hacking/65-prozent-cyberattacken-in-schweiz-2730544.html>
Verizon 2021 Data Breach Investigations Report

Datenlandschaft

- Mehr Daten, mehr Geräte, mehr Vorschriften
- Reuters: 2020 in 190 Ländern **jeden Tag durchschnittlich 257 Aktualisierungen von regulatorischen Vorgaben.**¹



Wenn der Fileshare wird zum Problem

1. Fehlender **Überblick** über bestehendes Wissen
2. Frustration bei der **Suche** nach Unternehmensdokumenten
3. **Unsicherheit** bei der Ablage von Unternehmens-Dokumenten
4. Datenleichen und **Speicherplatz**
5. **Hardware** Ablösung und "end of support" von Systemen
6. Schritthalten mit **Regulatorien** (DSVGO, HIPAA, ISO, ...)



Kollaboration mit M365

Ist wie Arbeiten mit Datei-Servern,
einfach in der Cloud?



Kollaboration & Informations-Ablage



Logische
Strukturierung



Physische
Strukturierung



Physisch versus logisch strukturierte Daten

Physische Strukturierung

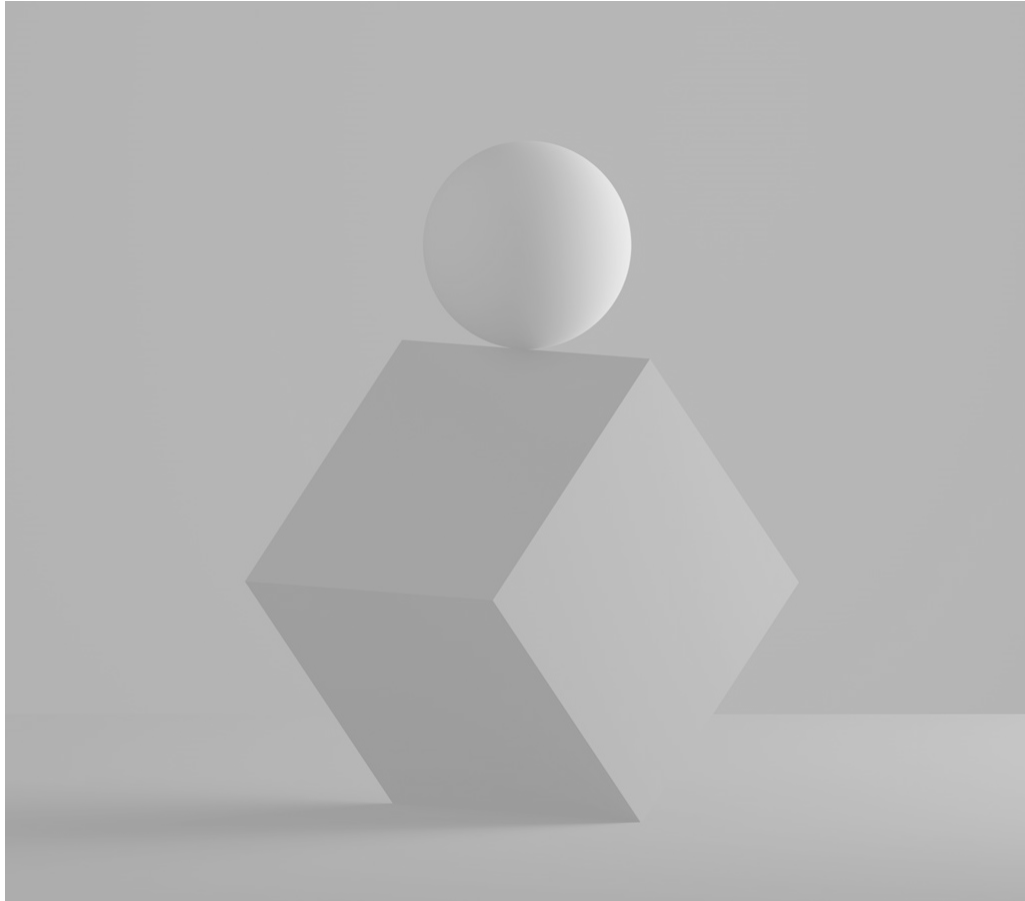
- Namensgebung
- Hierarchische Ablage und Zugriff über Ordner
- Objekt-funktionsorientierte Gliederung

Schwachstellen

- eingeschränkte **Suchfunktionen**
- die **Regeln** zur Ablage sind teilweise unbekannt
- **Unübersichtlich** bei grossen Datenmengen
- Inkonsistenzen und **Redundanzen**



Physisch versus logisch strukturierte Daten



Logische Strukturierung

- Definierte Eigenschaften der Inhalte (Metadaten)
- Inhalte werden dort angezeigt wo sie Relevanz haben
- Alle Inhalte werden in die Suche eingebunden

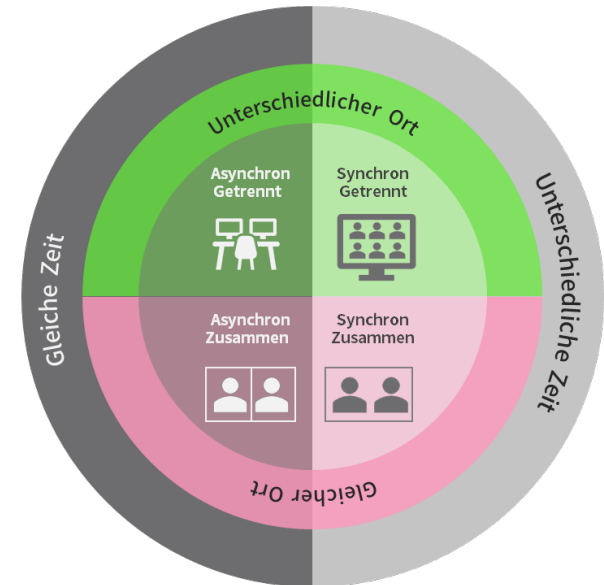
Vorteile

- Eindeutige **Volltext-Suche**
- Verschlagwortung mit **Metadaten** ermöglicht das gezielte Filtern und verbesserte Suchergebnisse
- Daten sind physisch nur einmal vorhanden, werden aber angezeigt, wo sie **Relevanz** besitzen
- **Nutzende** müssen nicht wissen, wo die Daten physisch liegen



Hybrid Work

- Arbeiten von überall
(1.4 Tage Home-Office im Schnitt in Deutschland)
- Synchrones und asynchrones Arbeiten
- Management von Dokumenten **Versionen**
- **Kontextinformationen** (Chats, Calls, Kommentare)



1: Quelle Grafik: Microsoft

2: Homeoffice etabliert sich in Deutschland mit 1,4 Tagen pro Woche | ifo Institut

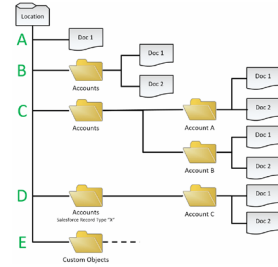
(<https://www.ifo.de/pressemitteilung/2022-09-16/homeoffice-etabliert-sich-deutschland-mit-14-tagen-pro-woche>)

Vorgehen

1

Verschaffen Sie sich einen Überblick über die bestehende Ordnerstruktur

- Analyse der Daten auf Fileshares (X-Drives)
- Typen, Grössen, Alter, Ablagelogik, Eigentümer
- Manuel oder Automatisiert (Datei-Parser)



2

Finden von sinnvollen Gruppierungen von Dateien

- Normalisieren Eigenschaften
- Themen, Organisations-Einheiten, Anwendungs-Bereiche - Datei-Typen
- Datenklassifizierung
- Externer Zugang



3

Entwerfen einer übersichtlichen Ablagestruktur

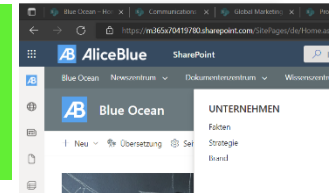
- Organisations-Ablagen
- Anwendungen
- Projekte / Prozesse / Themen
- Holistische Sicht:
FileServer, SharePoint, OneDrive, Chats, Apps,



4

Erstellen Sie die digitale Site- und Ordnerstruktur

- Berücksichtigung der SharePoint Eigenheiten
- Berechtigungen, Performance-Optimierung, Dokumentenanzahl
- Speicherort



Datenmigration

- Wer migriert (IT oder User)?
- Wieviel wird migriert?
- Automatisierungsgrad
- Werden auch Metainformationen und Berechtigungen migriert?
- Wann wird migriert (vor oder nach Go Live)
- Soll aufgeräumt werden?

Hybride Ablage:

Was kann oder soll im Datei-Server bleiben

- **Fachapplikationen mit eigener Ablage**
ERP, CAD, QM, PIM, ...
- **Datei "Archive"**
- Erfolgreiche **Ablage-Systeme** für einen spezialisierten Nutzendenkreis

Modernisierungs- Plan der Datenablage

Wahl des Cloud Daten Speicherortes

- Hyperscaler: Schweiz, EU
- Schweizer Anbieter (CH-Private Clouds)

Tipps Daten-Ablage-Strukturen

Flache Strukturen

- **Normalisierte Strukturen**
- Maximale Skalierbarkeit
- Minimale Verschachtelung
- **Grösste Flexibilität bei Berechtigungsvergabe**
- Minimaler Verwaltungsaufwand

Meta-Daten vererben

- **Darstellung der Inhalte in mehrdimensionalen Sichten**
- Grundlage für die Kontextsuche
- Minimierung der Verwaltungsaufwandes
- *"So viele wie nötig, so wenig wie möglich"*

Anwendungs-orientierter Aktenplan

- Flexible Struktur basierend auf den tatsächlichen Anwendungsfällen
- **Kontextorientierte Einhaltung von Richtlinien**

Maximale Offenheit

Offenheit als Maxime:

- Minimierung des Verwaltungsaufwands und der Komplexität
- Maximierung und Transparenz

Einschränkungen wo nötig

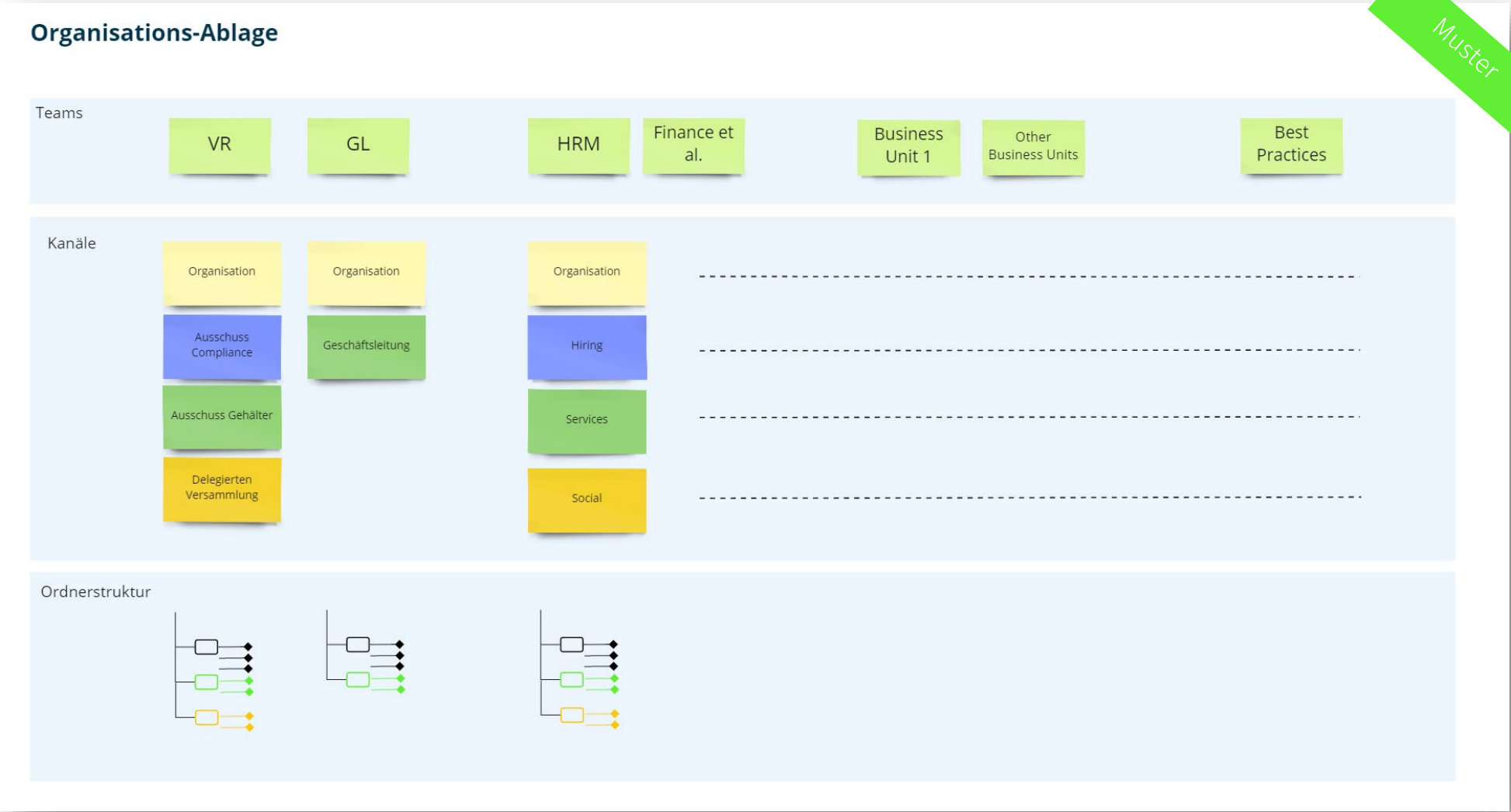
- Eingeschränkte Use-Cases definieren

Datenmanagement automatisieren

- **Automatisieren Sie die Datenklassifizierung**
- Datenschutz in Ihre täglichen Workflows integrieren
- Unternehmens-Richtlinien regelmässig aktualisieren
- **Überlassen Sie das Versions-Management M365**

Organisations-Ablage | Arbeitsräume

Organisationsablage



Muster

Arbeitsräume



Arbeitsräume

Vorlagen

Projekte

Objekte

Prozesse

Teams

Projekt A

Projekt B

Objekt A

Objekt B

Prozess A

Prozess B

Kanäle

Organisation

01 ... NAME

02 ... NAME

ARCHIV

Organisation

01 ... NAME

02 ... NAME

ARCHIV

Organisation

01 ... NAME

02 ... NAME

ARCHIV

Ordnerstruktur

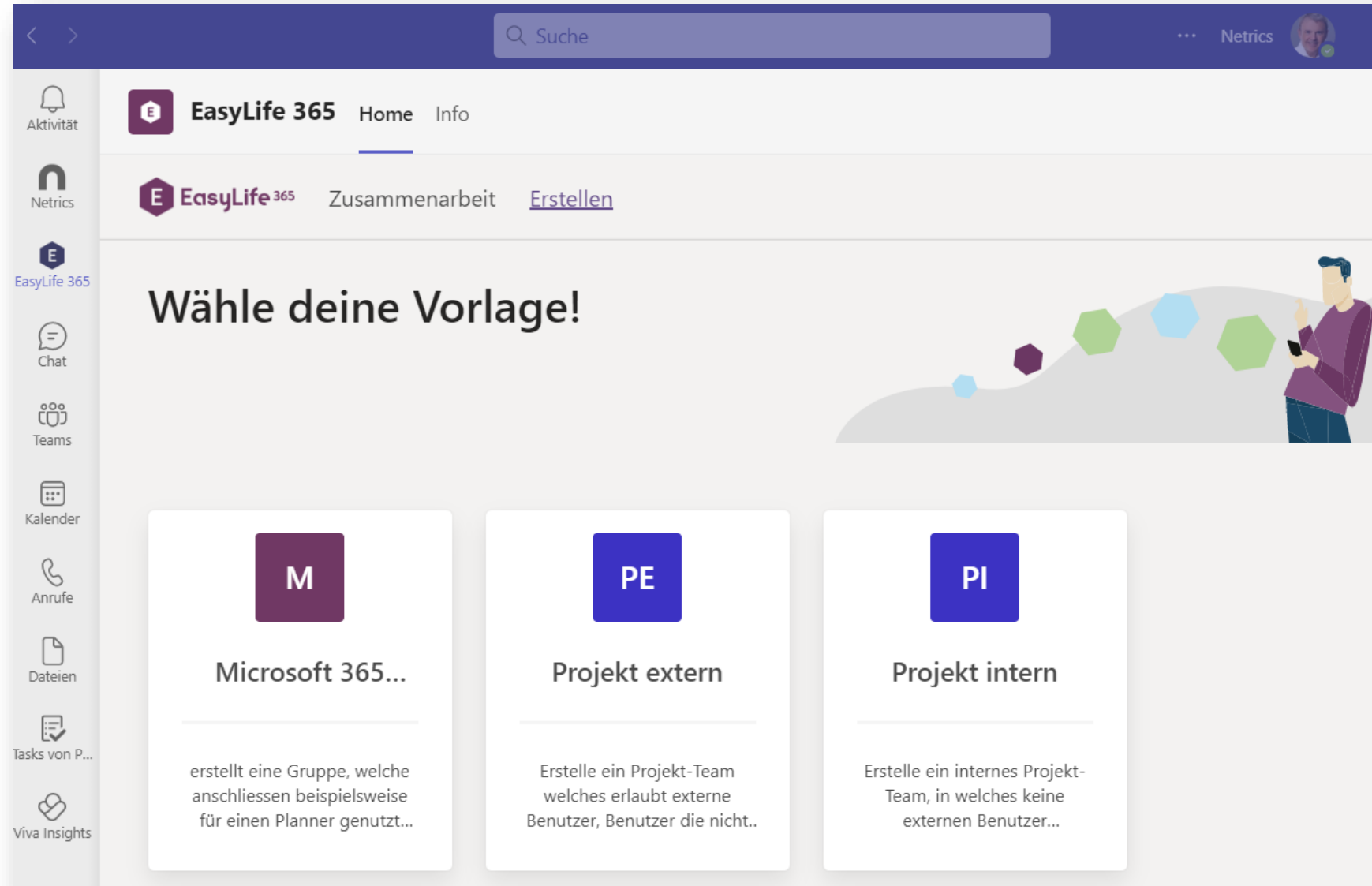


Muster

Delegation von Governance an Nutzende

EasyLife 365

- Automatisierte Provisionierung von Arbeitsräumen in MS (Teams, Channels, Tabs)
- Interne/Externe Nutzende
- Automatische Checks: Mitglieder, Zugang, De-Kommissionierung, Archivierung



Daten Klassifizierungen

- Identifizieren von **sensiblen Dateien**, geistigem Eigentum und Geschäftsgeheimnissen
- **Sichern** (und Sperren) kritischer Daten
- **Nachverfolgen** regulierter Daten, um die Anforderungen von Vorschriften wie HIPAA der DSGVO zu erfüllen
- Optimieren von **Suchmöglichkeiten** durch Datenindexierung
- Erkennen signifikanter **Muster oder Trends** im Datenbestand

- **Personenbezogene Daten:** Kreditkartennummern, Reisepassnummern, Führerscheinnnummern, Sozialversicherungsnummern, IBAN und weitere
- **Finanzunterlagen**
- **Sicherheitsdateitypen** (.cer, crt, p7b usw.)
- **Regulierte Daten** (DSGVO, HIPAA, PII, PHI, PCI, Sabanes Oxley, GLBA usw.)

Chief Information Security Officer (CISO)

Daten Klassifizierung

Klassifizierung	Beschreibung	Zugänglichkeit/Weitergabe	Ablagen & Systeme	Aufbewahrung und Vernichtung	Beispiele
Unklassifiziert	Sämtliche unklassifizierten Informationen werden als "Intern" behandelt.				
Öffentlich	Sämtliche der Öffentlichkeit legal zugänglichen Informationen	Die Informationen sind allen zugänglich.	Alle Ablagen-Systeme		
Intern	Alle Unternehmensdaten, die nicht für die Öffentlichkeit bestimmt sind, aber nicht vertraulich oder geheim klassifiziert sind.	- Nur den internen Mitarbeitenden und dedizierten, extern beauftragen Partnern zugänglich. - Als "intern" klassifizierte Dokumente dürfen im Rahmen der gesetzlichen Vorgaben bearbeitet, übermittelt, und aufbewahrt werden.	Ablage-Systeme mit einer Klassifizierungsmöglichkeit oder einer adequaten Einschränkung des Zugriffs (interne Rollen, externe Gast-Zugänge mit Bewilligungs-Verfahren)		
Vertraulich <i>besonders schützenswert</i>	Informationen mit besonderem Schutzbedarf, welche - Verwaltungs- oder Beschwerdeverfahren betreffen, - aufgrund gesetzlicher oder vertraglicher Geheimhaltungspflichten dieser Kategorie zugewiesen sind, 	Der Personenkreis, welcher auf als vertraulich klassifizierte Informationen Zugang hat, ist möglichst klein zu halten.			
besonders schützenswert	Informationen mit besonderem Schutzbedarf, welche - besonders schützenswerte Personendaten nach Artikel 3 Schweizer DSG enthalten, - besonderen Kategorien personenbezogener Daten nach Artikel 9 EU-DSVG0 enthalten, - schützenswerte Angaben über familiäre oder finanzielle Verhältnisse Einzelner enthalten, - Kreditkartendaten enthalten,	Die Erstellung, Die Bekanntgabe und das Zugänglichmachen von als "Vertraulich" klassifizierten Dokumenten sind auf ein Minimum zu beschränken. Ein Mitglied der Geschäftsleitung entscheidet über eine Weitergabe.			
Geheim	Informationen mit besonderem Schutzbedarf, welche - bei Kenntnisnahme das Unternehmen schädigen könnten - börsenkursrelevante Informationen über ein Unternehmen enthalten,	Ein Mitglied der Geschäftsleitung entscheide über eine Weitergabe.			

Muster

Microsoft Compliance ("MS Purview")

←

→

↺

🔒

https://compliance.microsoft.com/datalossprevention?viewid=policies

🔊

🔖

🌟

🔖

InPrivate

⋮

⋮

AB

AliceBlue

Microsoft Purview

⚙️

?

MA

☰

Startseite

🛡️ Compliance-Manager

🔗 Datenklassifizierung

🔗 Datenconnectors

⚠️ Warnungen

📊 Berichte

🔗 Richtlinien

🔑 Berechtigungen

🧪 Testversionen

Lösungen

📁 Katalog

📁 App-Governance

📊 Überwachen

🔍 Inhaltssuche

🗨️ Kommunikationscompliance

🔒 Verhinderung von Datenverlust

📁 eDiscovery

📁 Verwaltung des Datenleben...

🔒 Informationsschutz

🔒 Informationsbarrieren

👤 Insider-Risikomanagement

📁 Datensatzverwaltung

🔒 Datenschutz-Risikomanage...

🔍 Anfragen zu Rechten betroffener ...

Verhinderung von Datenverlust

Aus der Navigation entfernen

Übersicht

Richtlinien

Warnungen

Endpoint-DLP-Einstellungen

Aktivitäten-Explorer

Verwenden Sie DLP-Richtlinien (Data Loss Prevention, Verhinderung von Datenverlust), um vertrauliche Informationen Ihrer Organisation zu identifizieren und zu schützen. Sie können beispielsweise Richtlinien einrichten, um sicherzustellen, dass Informationen in E-Mails und Dokumenten nicht mit den falschen Personen geteilt werden. [Weitere Informationen zu DLP](#)

🔔

Automatisches Konfigurieren von Teams DLP-Richtlinien zum Schützen von Dateien, die in Teamnachrichten freigegeben sind

×

Möchten Sie sicherstellen, dass alle vorhandenen und zukünftigen Richtlinien, die Teams-Chats und Kanalnachrichten schützen, auch alle Dateien schützen, die in diesen Nachrichten freigegeben sind? Wenn Sie den automatischen Dateischutz für Teams-DLP-Richtlinien aktivieren, werden zugeordnete SharePoint-Websites und OneDrive-Konten automatisch in alle Teams DLP-Richtlinien eingeschlossen.

Automatischen Dateischutz deaktivieren

+

Richtlinie erstellen

↓

Exportieren

↺

Aktualisieren

3 Elemente

🔍 Suchen

☐	Name	Reihenfolge	Zuletzt geändert	Status
☐	U.S. Financial Data	⋮ 0	31. Aug. 2022 05:36	Ein
☐	General Data Protection Regulation (GDPR)	⋮ 1	31. Aug. 2022 05:37	Ein
☐	Default policy for devices	⋮ 2	31. Aug. 2022 11:40	Ein

Schützen und Sichern von Daten

A

Identitäts- und Zugriffsverwaltung

- Zugriffsverwaltung und Sicherheit
- Mehrstufige Authentifizierung
- Bedingter Zugriff
- Erweiterte Sicherheitsberichte
- *Risikobasierter bedingter Zugriff*

B

Verwaltete mobile Produktivität

- Verwaltung mobiler Geräte
- Verwaltung mobiler Anwendungen
- Erweiterter Datenschutz in O365
- Integrierte PC-Verwaltung

C

Informations-Schutz

- Verfolgung und Sprengung von Dokumenten
- Verwaltung von Verschlüsselungsschlüsseln
- *Intelligente Klassifizierung und Kennzeichnung von Daten*

D

Identitätsgeschützte Sicherheit

- Advanced Threat Analytics
- *Cloud App Security*
- *Azure Advanced Threat Protection*

Microsoft E3 und E5 Sicherheitsfunktionen

Microsoft 365				
	E3	E5	E5 Security ¹	E5 Compliance ¹
¹ Requires Microsoft 365 E3 (or Office 365 E3 and Enterprise M365)				
Information protection				
Azure Information Protection Plan 1	•	•		•
Azure Information Protection Plan 2		•		•
Manual, default, and mandatory sensitivity labeling in Office 365	•	•		
Automatic sensitivity labeling in Office 365 apps		•		•
Manual labeling with the AIP app and plugin	•	•		
Automatic labeling in the AIP plugin		•		•
Automatic sensitivity labels in Exchange, SharePoint, and OneDrive		•		•
Sensitivity labels based on Machine Learning/Trainable Classifiers		•		•
Sensitivity labeling for containers in Office 365	•	•		
Data Loss Prevention (DLP) for emails & files	•	•		
DLP for Teams chat		•		•
Endpoint DLP		•		•
Basic Message Encryption	•	•		
Advanced Message Encryption		•		•
Customer Key		•		•
Identity and access management				
Azure Active Directory Premium Plan 1	•			
Azure Active Directory Premium Plan 2		•	•	
User Provisioning	•	•	•	
Self Service Password Reset	•	•	•	
Advanced Security Reports	•	•	•	
Multi Factor Authentication	•	•	•	
Conditional Access	•	•	•	
Risk Based Conditional Access / Identity Protection		•	•	
Privileged Identity Management		•	•	
Access Reviews		•	•	
Entitlement Management		•	•	
Microsoft 365 Groups	•	•		
On-premises Active Directory sync for SSO	•	•		
DirectAccess supported	•	•		
Windows Hello for Business	•	•		
Microsoft Advanced Threat Analytics	•	•		
Windows Store Access Management	•	•		
Endpoint and app management				
Microsoft Intune	•	•		
Mobile Device Management	•	•		
Microsoft Endpoint Manager	•	•		
Mobile application management	•	•		
Windows AutoPilot	•	•		
Group Policy support	•	•		
Office cloud policy support	•	•		
Shared computer activation for M365 Apps	•	•		
Endpoint Analytics	•	•		
Cortana management	•	•		

Kollaboration mit M365

- Logische Datenstrukturen
- Überall und jederzeit
- Versions-Management
- Governance Delegation
- Datenklassifizierung up-to-date
- Schützen und Sichern
- Passender M365 Plan



M365 Konzeption Datenablage Checkliste

Richtig konzipiert	Plattform	Organisation, Prozesse	Change & Adoption
✓ Migration + Modernisierung mit M365 Fähigkeiten ✓ Prinzip der logischen Ablagen mit Klarnamen einführen ✓ Anwendungs-orientierte Ablage Strukturen (Organisations-Ablage + Arbeitsräume) ✓ Konzipieren Sie Sicherheit, Compliance + Modern Work "by Design" ✓ Überlassen Sie Versions-Management M365	✓ Passendes Cloud + Managed Workplace Model (M365 Lizenz-Pläne) ✓ Modernisierung der Geschäftsanwendungen wo möglich einbeziehen ✓ Daten-Schutz, -Sicherheit - und Verfügbarkeit über alle Ebenen, inkl. Endgeräte ✓ Operativer Betrieb mit externer + interner Kompetenz ✓ – Delegation von Compliance an Nutzende	✓ Anwendungsfälle festlegen ✓ Informations- und Datenmanagement definieren ✓ Kommunikations- und Kanalstrategie festlegen ✓ Work Smart: Arbeitsprozesse an neue Möglichkeiten anpassen ✓ Pilotierung und Einführung der neuen Prozesse und Lösungen	✓ Management-Support und Sponsoring sicherstellen ✓ Sensibilisierungsmassnahmen durchführen, um auf die Veränderungen vorzubereiten ✓ Richtlinien, Verhaltenskodex für die neue Zusammenarbeit definieren ✓ Zielgruppengerechte Schulungen durchführen ✓ Coaching und Verankerungsmassnahmen umsetzen