Auditing Microsoft 365

Too big to (be) secure!?

Agenda

Microsoft Teams oder wie arbeite ich zusammen?

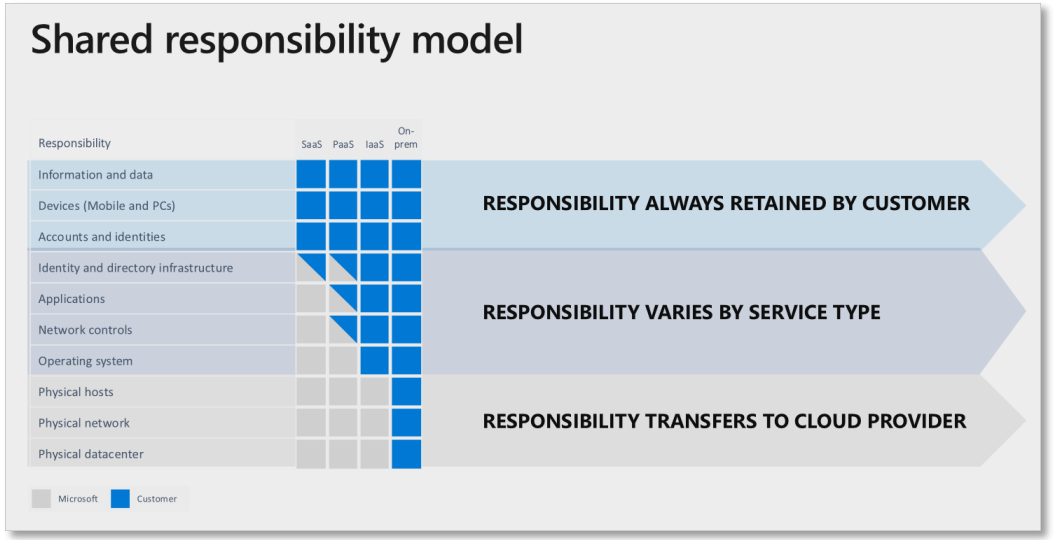
Microsoft Entra ID oder wie identifiziere ich mich?

Microsoft Power Platform oder wie verbessere ich IDV?

Was lässt sich am Schreibtisch prüfen?

Warum nicht nur ein Besuch in Redmond viele Risiken abdeckt…

- blaue Kästchen – Kontrollen müssen vom eigenen Unternehmen implementiert und damit von Internal Audit geprüft werden
- geteilte Kästchen – Kontrollen müssen vom eigenen Unternehmen implementiert und damit von Internal Audit geprüft werden; zusätzlich bestehen Kontrollen von Microsoft, die innerhalb von Zertifizierungen geprüft werden
- graue Kästchen – Kontrollen werden von Microsoft implementiert und werden im Rahmen von Zertifizierungen geprüft

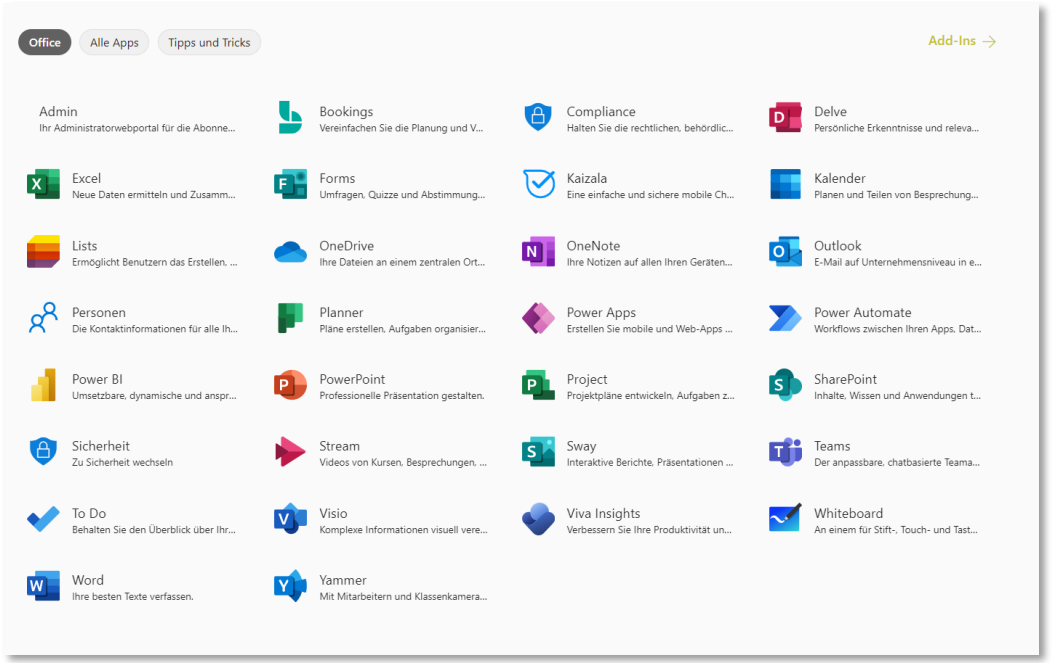


Quelle: https://docs.microsoft.com/de-de/azure/security/fundamentals/shared-responsibility

Was ist Microsoft 365? (1/2)

Namensverwirrungen und Unklarheiten…

- „Microsoft 365-Abonnements umfassen vertraute Office-Anwendungen, intelligente Clouddienste und erstklassige Sicherheitsmerkmale – alles an einem Ort.“
- Sammlung von Software-as-a-Service-Diensten (SaaS), die stetig erweitert wird – Überblick über den (Enterprise-)-Lizenzumfang hier
- Früher (Lizenzen weiterhin erwerbbar) stärker unter dem Namen Office 365 vermarktet



Quelle: https://www.microsoft365.com/apps?auth=2

Was ist Microsoft 365? (2/2)

Umfangreiche Schnittstellen zwischen den Backends

- Diverse übergreifende Dienste, die nicht direkt für den Endbenutzer sichtbar sind
- Beispiele:
  - Aufbewahrungsrichtlinien, die auf Dateien in SharePoint, Anhänge in Outlook, Nachrichten in Teams etc. wirken können
  - Geräteverwaltung, um Clients sicher für die Verbindung zu Microsoft 365 einschränken
  - …
- Empfehlung: Der Scope der Microsoft-365-Prüfung sollte eher „kleiner“ gewählt werden

Complianceverwaltung
Compliance-Risiken bewerten, vertrauliche Daten kontrollieren und schützen sowie gesetzliche Anforderungen umsetzen
Manuelle Aufbewahrungsbezeichnungen, Inhaltssuche, Standardüberwachung
Standardrichtlinien zur unternehmens- und standortweiten Aufbewahrung, Aufbewahrungsrichtlinien in Teams, zentrale eDiscovery, Aufbewahrung für juristische Zwecke
Regelbasierte Richtlinien für die automatische Aufbewahrung, Machine Learning-basierte Aufbewahrung, Datensatzverwaltung
Advanced eDiscovery, Erweiterte Überwachung
Insider-Risikomanagement, Regeln für gute Kommunikation, Informationsbarrieren, Kunden-Lockbox, Privileged Access Management
Integrierte Drittanbieter-Verbindungen

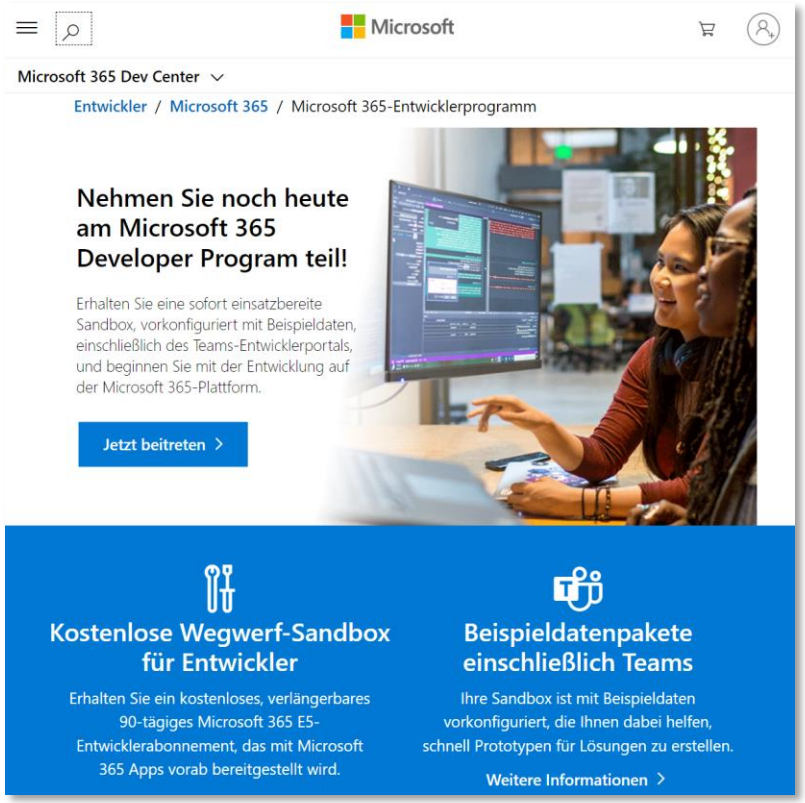
Quelle: https://www.microsoft.com/de-de/microsoft-365/compare-microsoft-365-enterprise-plans?market=de

Was findet sich in Prüfungen?

Einige Live Demos zu bad practices…

- Microsoft 365 Developer Program – eigener Tenant, mit nahezu allen Lizenzen, Funktionalitäten und Testbenutzern

- Halb-fiktive Ausgangslage: „Wir haben für unsere rund 15.000 Mitarbeiter eine dezentrale Benutzerverwaltung und Verantwortung bei den Teameigentümern, damit diese im Sinne ihres Bedarfs arbeiten können.“

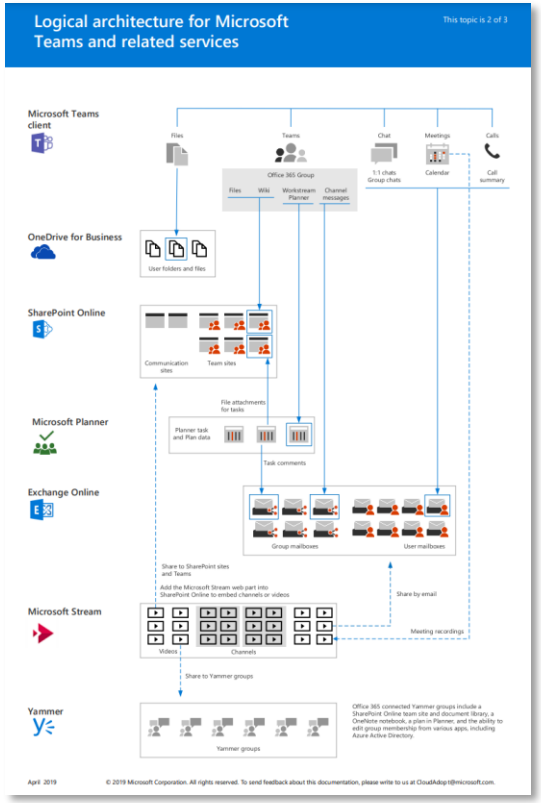


Quelle: https://developer.microsoft.com/en-us/microsoft-365/dev-program

Microsoft Teams

Frontend für viele Backends

- Bei Anlage eines Teams wird u.a. folgendes angelegt:
  - „eine neue Microsoft 365-Gruppe
  - eine SharePoint Online-Website und eine SharePoint Online-Dokumentbibliothek zum Speichern von Teamdateien
  - ein freigegebenes Exchange Online-Postfach und ein Exchange Online-Kalender
  - ein OneNote-Notizbuch
  - Verbindungen mit anderen Microsoft 365- und Office 365-Apps wie beispielsweise Planner und Power BI“

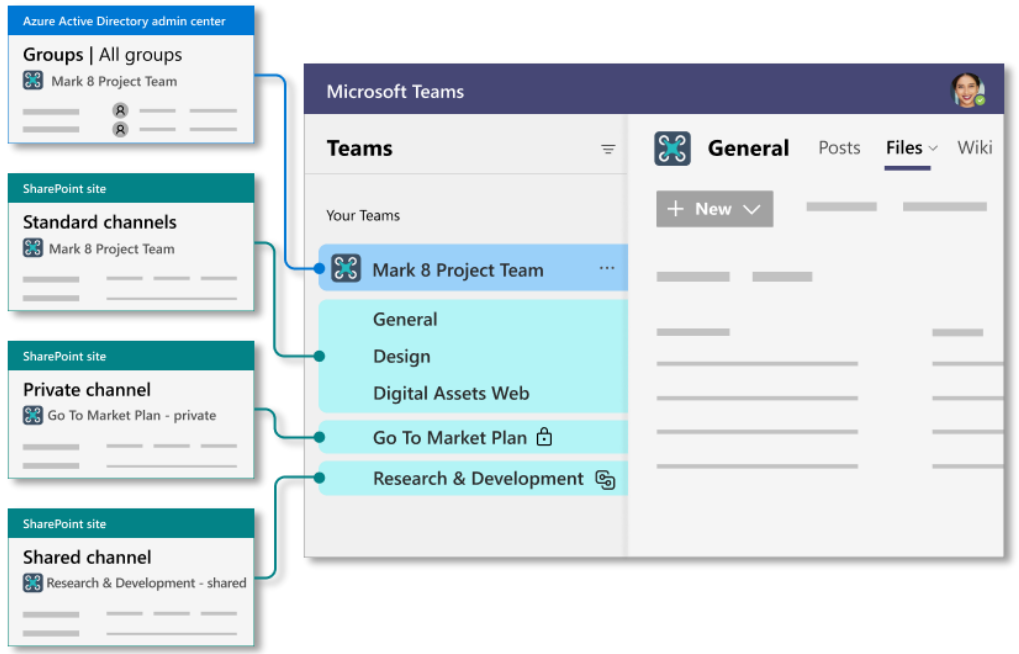


Quelle: https://docs.microsoft.com/de-de/microsoftteams/teams-architecture-solutions-posters#teams-as-part-of-microsoft-365

Microsoft Teams & SharePoint Online

Zusammenspiel der beiden Dienste

- SharePoint Online ist integriert in Teams und eine neue Seite wird automatisch bei Anlage eines Teams erstellt
- Die Kanalarten führen zu unterschiedlichen Anlagen von SharePoint Sites
- Das Teilen von Dateien ist mittels SharePoint Online möglich – übrigens OneDrive ist auch nur eine SharePoint Seite

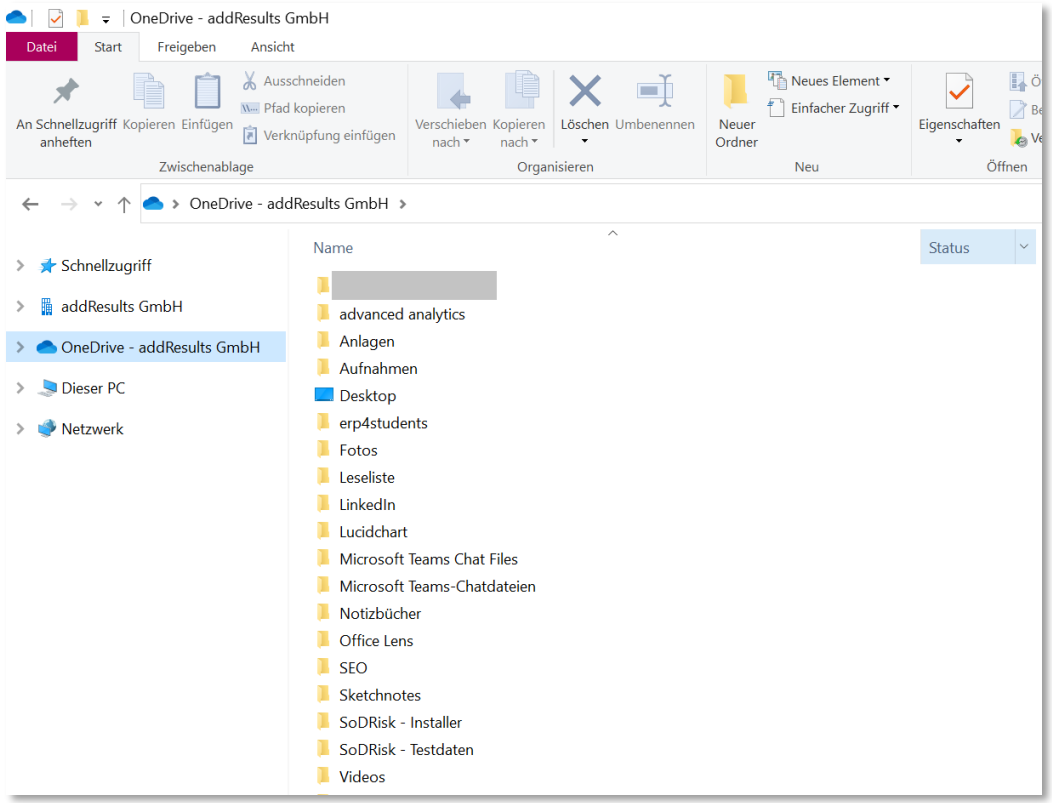


Quelle: https://docs.microsoft.com/de-de/sharepoint/teams-connected-sites

SharePoint Online & OneDrive

Offline-Verfügbarkeit der Daten

- Die Benutzer können ebenfalls SharePoint-Websites offline verfügbar machen
- Standardordner, wie ein Desktop oder Profilordner können ebenfalls automatisch synchronisiert und damit versioniert werden
- Synchronisierung kann auf AD-Domänen eingeschränkt werden



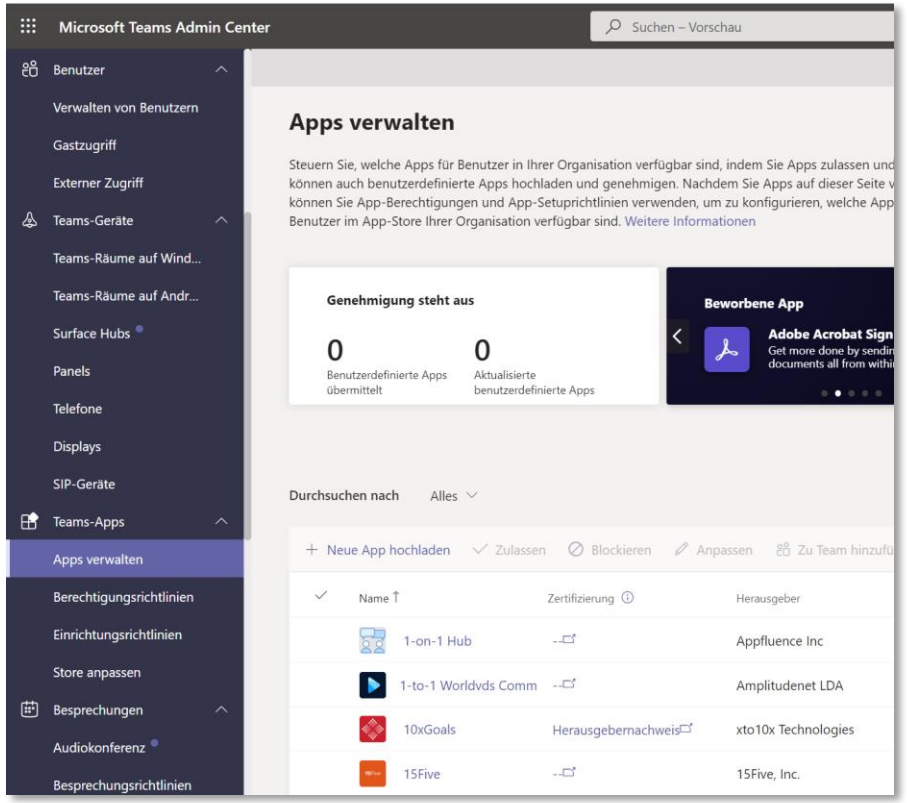
Quelle: https://docs.microsoft.com/de-de/onedrive/allow-syncing-only-on-specific-domains

Microsoft Teams & die Erweiterungen

Integration (unbekannter) Drittdienste

- Mit Apps kann Drittanbietersoftware in Microsoft Teams integriert werden – dadurch können die Benutzer mit weniger Medienbrüchen ihrer Arbeit nachgehen

- In der Grundeinstellung sind „alle“ Apps zugänglich und von Benutzern hinzufügbar

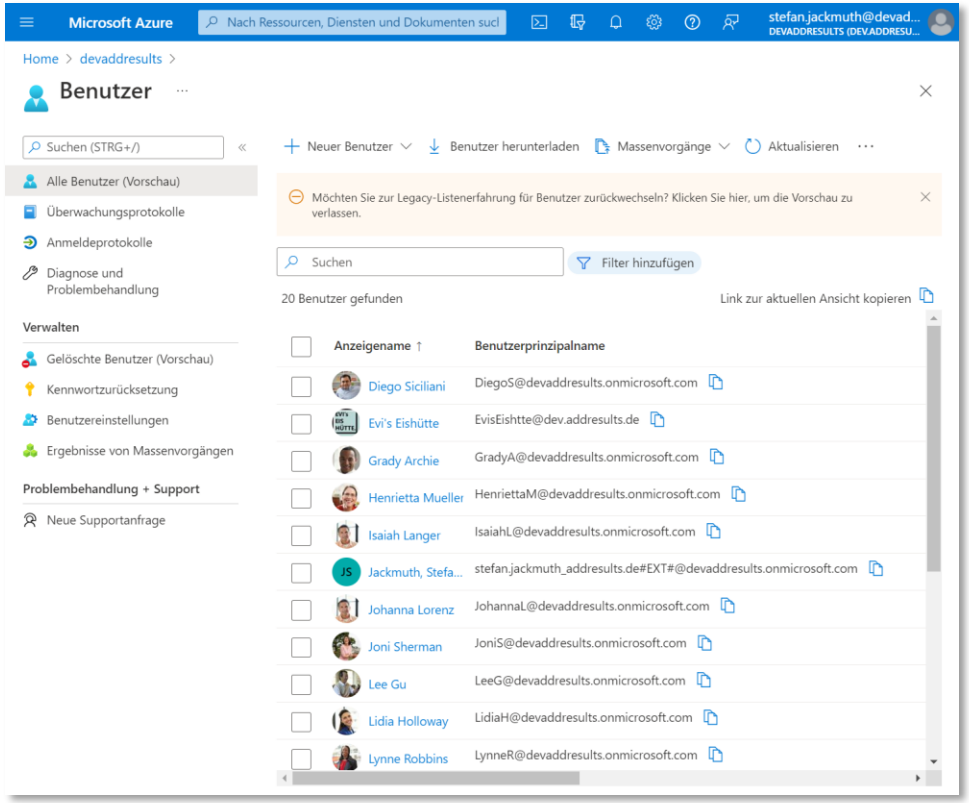


Quelle: https://docs.microsoft.com/de-de/microsoftteams/deploy-apps-microsoft-teams-landing-page

Microsoft Entra ID (1/2)

Grundsätzliches zu Benutzern

- (interaktive) Benutzertypen
  - Mitgliedsbenutzer
  - Gastbenutzer
- Unterschiedliche Standardberechtigungen für Gäste und Mitglieder
- Die Standardberechtigungen für Mitglieder sind weitreichend, z. B.
  - Einladung von Gästen
  - Erstellung von Sicherheits- und Microsoft 365-Gruppen
  - Registrierung von Applikationen
  - …

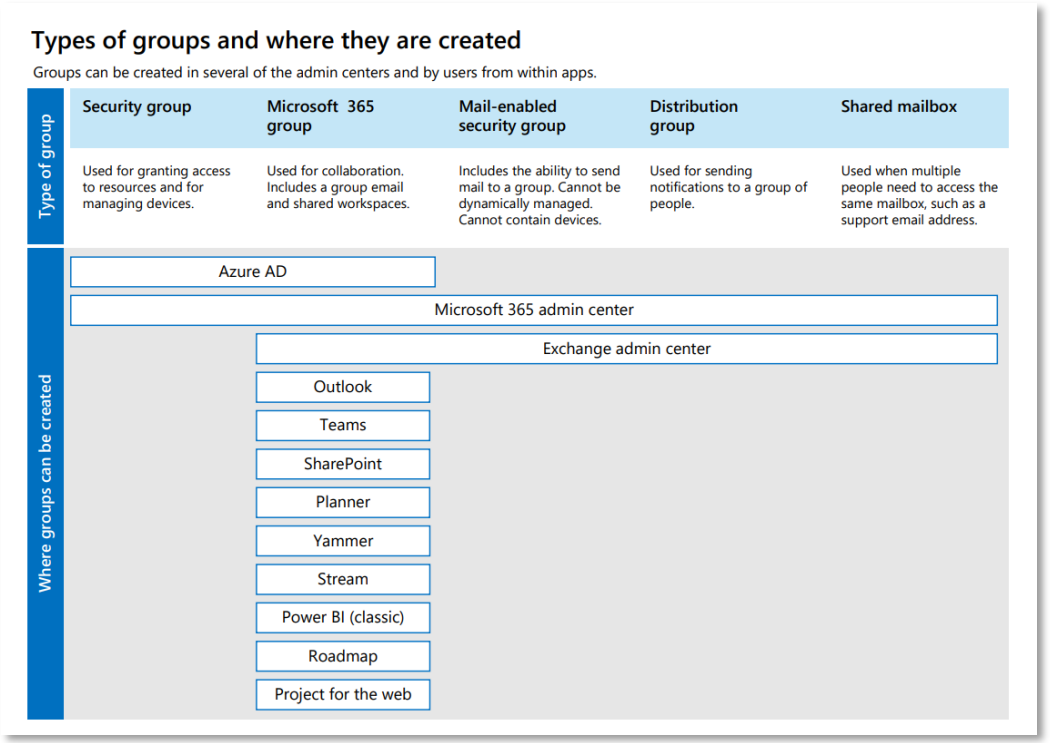


Quelle: https://docs.microsoft.com/de-de/azure/active-directory/fundamentals/users-default-permissions

Microsoft Entra ID (2/2)

Grundsätzliches zu Gruppen

- Sicherheitsgruppen
  - „nur“ eine Bündelung von Benutzern, Geräten, Gruppen und Service Principals
  - Gruppen des on-Premise AD DS
- Microsoft 365-Gruppen
  - Gruppe zur Zusammenarbeit, gleichzeitig wird ein Postfach, SharePoint-Seite, Kalender etc. erstellt
  - kann nur Benutzer aufweisen
- Zwei Arten von „Berechtigungen“:
  - Besitzer
  - Mitglieder

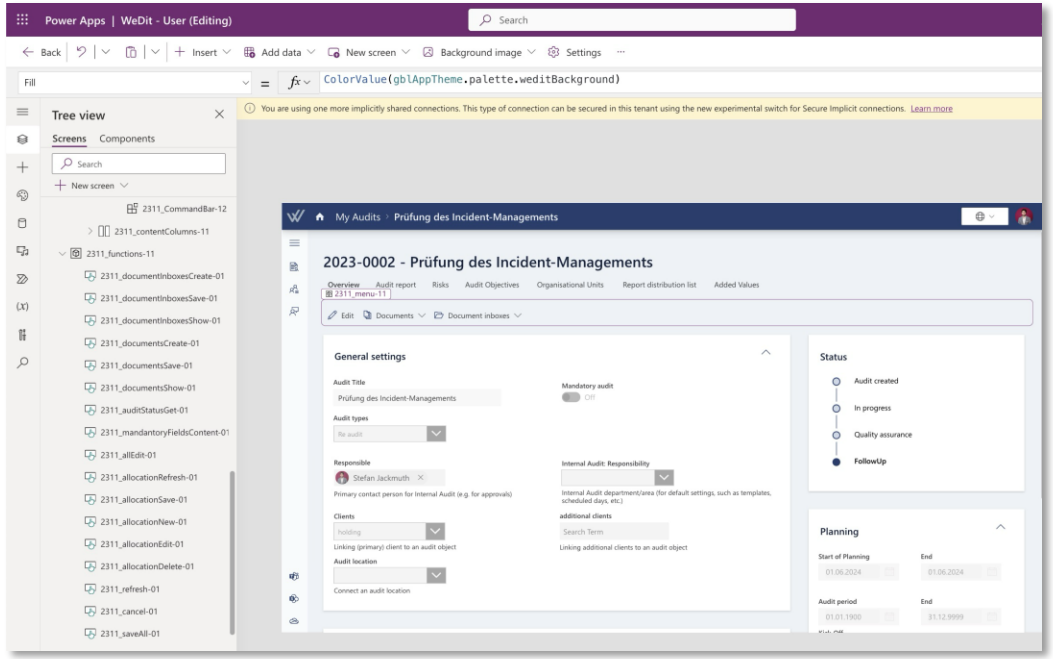


Quelle: https://docs.microsoft.com/de-de/azure/active-directory/fundamentals/users-default-permissions

Microsoft Power Platform

Low-/No-Code für die Business User

- Citizen Development via Low-Code – Fachbereiche sollen in die Lage versetzt werden, einfach Applikationen und Automatisierungen zu entwickeln
- Die IT ist potenziell an dieser dezentralen Entwicklung nur im Betrieb beteiligt
- Klarer Entwicklungsprozess möglich – IDV kann leichter prozessual begrenzt werden, aber nicht per „eingebautem“ Application Lifecycle Management

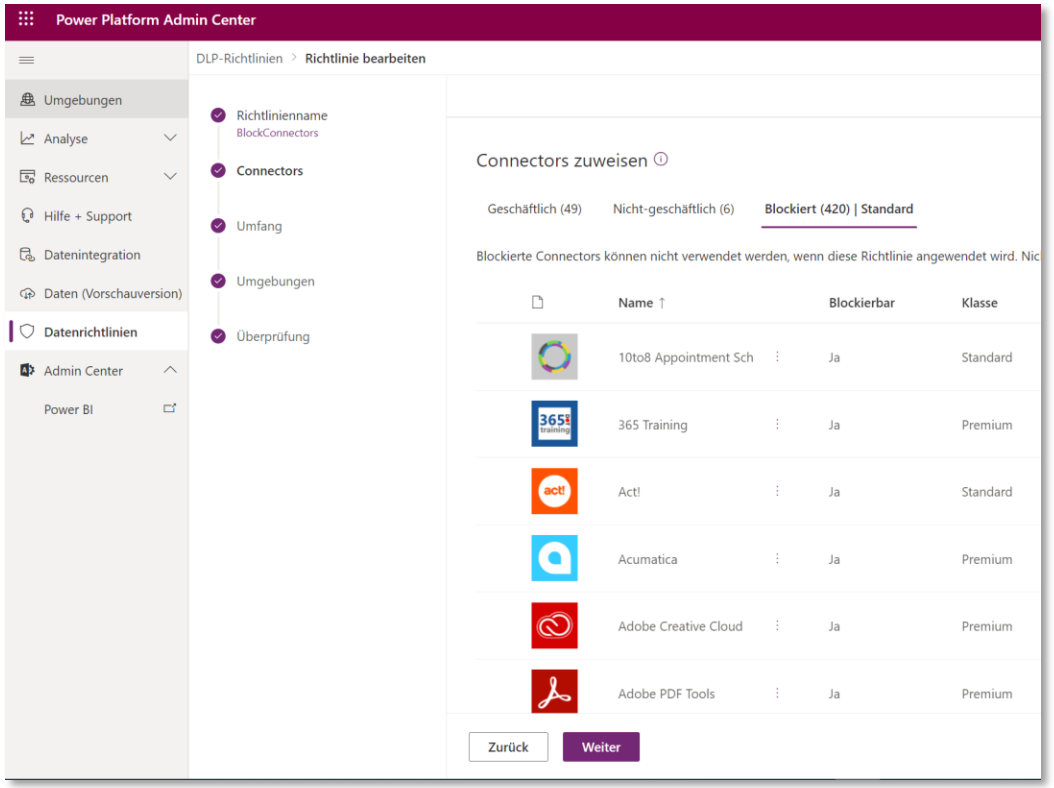


Quelle: https://docs.microsoft.com/de-de/power-platform/admin/security

Microsoft Power Automate

Automatisieren mit Vor- und Nachteilen

- Erstellung von Workflows, die APIs aufrufen und JSONs übergeben
- Die Automatisierungen können von einfachen Unterstützungen a la „lege mir Dateien ab, wenn eine Mail ankommt“ zu komplexen Programmierungen gehen
- „Lege mir jede Datei, die per Mail kommt, in meiner privaten Dropbox ab.“

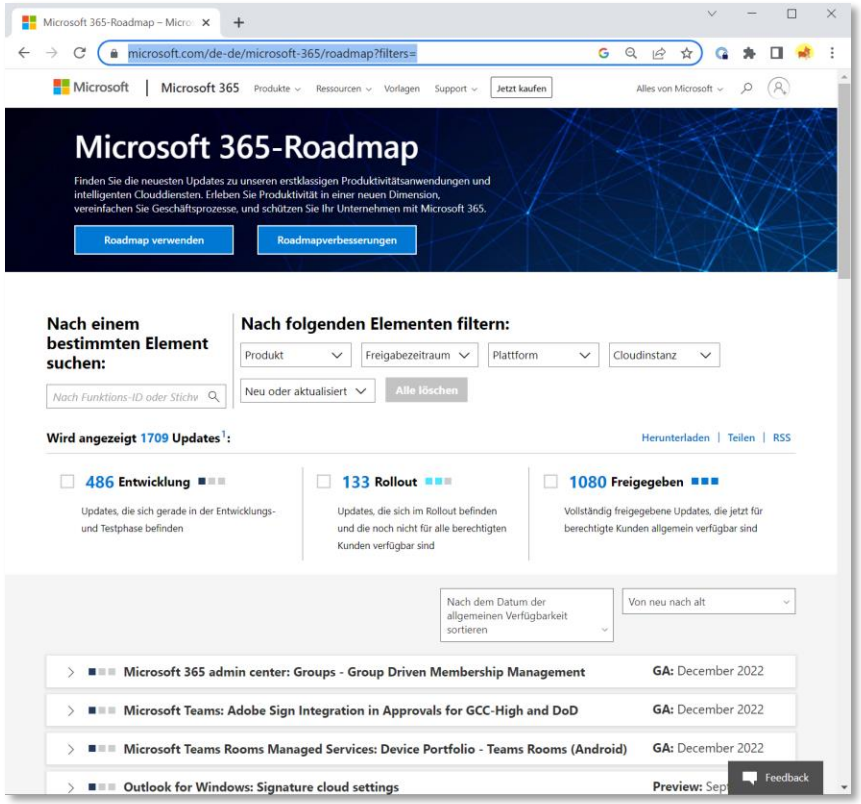


Quelle: https://docs.microsoft.com/en-us/power-platform/admin/wp-data-loss-prevention

Change Management (1/2)

Roadmap für die großen Schritte

- Laufend Entwicklung und Veröffentlichung von neuen Funktionalitäten
- Schrittweises Ausrollen der Funktionen – manchmal nicht genau erkennbar, wann das eigene Unternehmen davon profitiert
- Phasen:
  - Private Preview
  - Public Preview
  - General Availability

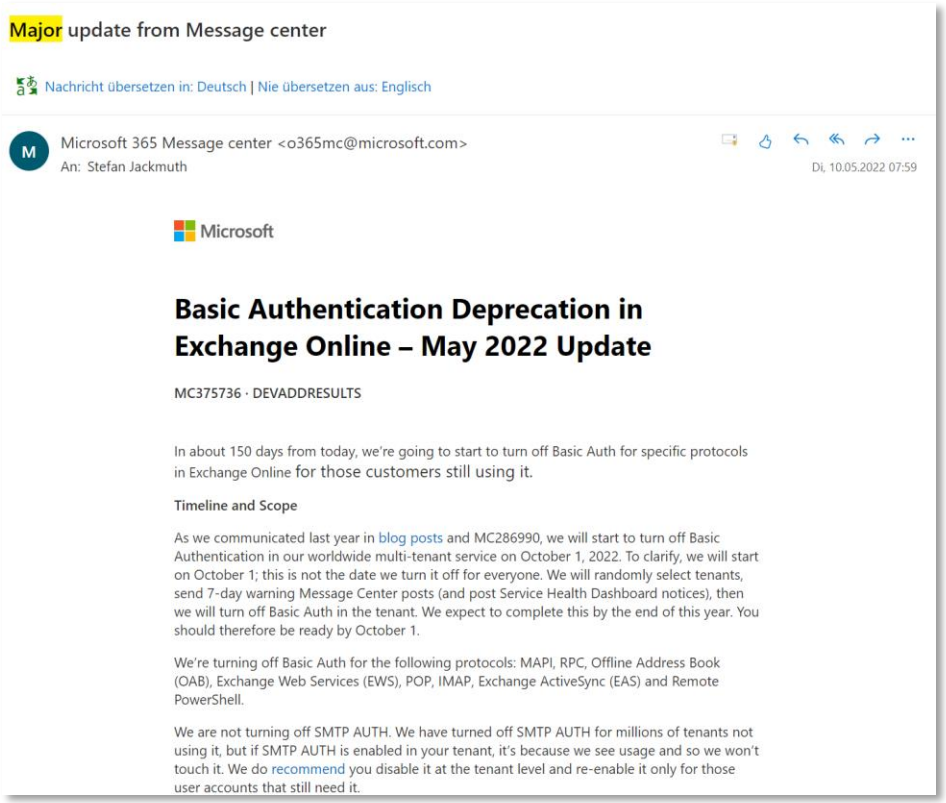


Quelle: https://docs.microsoft.com/en-us/power-platform/admin/wp-data-loss-prevention

Change Management (2/2)

Message Center für die detaillierten Änderungen

- „Um bevorstehende Änderungen, einschließlich neuer und geänderter Features, geplanter Wartung oder anderer wichtiger Ankündigungen, nachzuverfolgen, wechseln Sie zum Nachrichtencenter.“
- „das Nachrichtencenter ist die primäre Art und Weise, wie wir den Zeitpunkt einzelner Änderungen in Microsoft 365 kommunizieren“
- „Wichtige Updates werden mindestens 30 Tage im Voraus mitgeteilt, wenn eine Aktion erforderlich ist […]“



Major update from Message center

Nachricht übersetzen in: Deutsch | Nie übersetzen aus: Englisch

M Microsoft 365 Message center <o365mc@microsoft.com>
An: Stefan Jackmuth
Di, 10.05.2022 07:59

Microsoft

Basic Authentication Deprecation in Exchange Online – May 2022 Update

MC375736 · DEVADDRESULTS

In about 150 days from today, we're going to start to turn off Basic Auth for specific protocols in Exchange Online for those customers still using it.

Timeline and Scope

As we communicated last year in blog posts and MC286990, we will start to turn off Basic Authentication in our worldwide multi-tenant service on October 1, 2022. To clarify, we will start on October 1; this is not the date we turn it off for everyone. We will randomly select tenants, send 7-day warning Message Center posts (and post Service Health Dashboard notices), then we will turn off Basic Auth in the tenant. We expect to complete this by the end of this year. You should therefore be ready by October 1.

We're turning off Basic Auth for the following protocols: MAPI, RPC, Offline Address Book (OAB), Exchange Web Services (EWS), POP, IMAP, Exchange ActiveSync (EAS) and Remote PowerShell.

We are not turning off SMTP AUTH. We have turned off SMTP AUTH for millions of tenants not using it, but if SMTP AUTH is enabled in your tenant, it's because we see usage and so we won't touch it. We do recommend you disable it at the tenant level and re-enable it only for those user accounts that still need it.

Quelle: https://docs.microsoft.com/de-de/microsoft-365/admin/manage/message-center?view=o365-worldwide

Welche Berechtigungen für ein Audit?

Problem: Großer, multinationaler Tenant

- Einfachste Lösung – Zuweisung der Rolle „globaler Leser“
  - Zugang zu allen Admin Centern in Microsoft 365
  - Zugang zu allen Daten in den Admin Centern
- Mögliches Problem: Eingeschränkter Prüfungsumfang bzgl. der Gesellschaft/juristischen Person
  - Ggf. nicht möglich, da Datenbestand nicht „klar“ getrennt – ggf. über „Administrative Units“ realisiert, dann zu teilen umsetzbar

Quelle: https://blog.addresults.de/blog/microsoft-azure-welche-brauche-ich-zum-pruefen

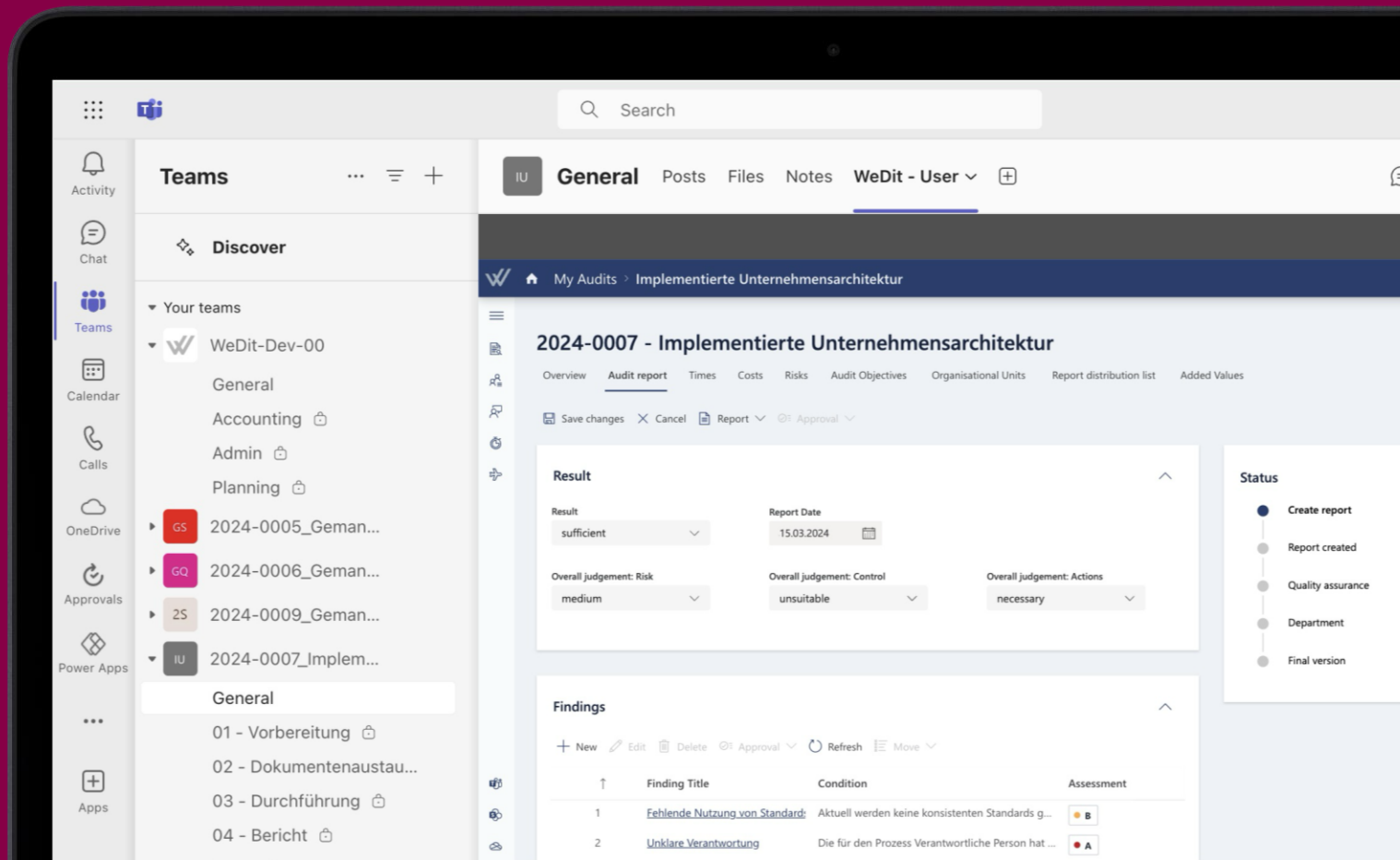
Fazit

- Dienste hängen zusammen – Scope klein halten, er vergrößert sich automatisch
- Stetige Änderungen – nur weil die Administration vor zwei Jahren gute Kontrollen erstellt hat, sind diese nicht noch immer gut
- Neugierig bleiben – irgendwelche neue Risiken ergeben sich immer – Was ist eigentlich der Microsoft Copilot?

Quelle:

WeDit

Audit... aber digital! mit Microsoft 365



Warum WeDit?

Audit Universe	Risk Assessment	Mehrjahres-planung	Prüfungs-vorbereitung	Prüfungs-durchführung	Berichte	Follow Up	Prüfungs-feedback

Planner – Prüfungsziele als Kanban-Board

OneNote – Arbeitspapiere und Notizen

Excel – Schnell Strukturen ändern

Word – Befüllte Prüfaufträge oder Berichte

Forms

Outlook – automatische Kommunikation, um Dokumente anzufordern, Berichte zu versenden oder offenen Maßnahmen Nachdruck zu geben

Approvals – Freigaben von Dokumenten, Prüfungen und Kommunikation – perfekt integriert in Microsoft Teams

Teams – Organisation und Kommunikation der Audits in automatisch erstellten Teams – der zentrale Arbeitsplatz für Auditor

Power BI – Interaktive, leicht anpassbare Berichte zur Auswertung der Audit Prozesse

Power Apps – Audit Prozesse leicht per App starten, überwachen und Microsoft 365 die Arbeit machen lassen

Power Automate – Microsoft 365 automatisiert arbeiten lassen

Graph API – um das ganze Potential von Microsoft 365 zu nutzen

SharePoint Online – Dokumente speichern, durchsuchen und per Klick teilen

OneDrive – Dokumente immer lokal dabei

Azure SQL – Stammdaten zu Prüfungen, Follow Up & Co. speichern

Wir als **WeDit-Team** – um mit Passion, Neugier, IPPF-Standards und viel Kaffee Microsoft 365 für Internal Audit zu orchestrieren

LASSEN SIE UNS REDEN

WEIL JEDER INDIVIDUELLE IDEEN BESITZT

+49 162 70 70 466
stefan.jackmuth@addResults.de

addResults GmbH
Schulweg 17a
51503 Rösrath

TERMIN BUCHEN

Stefan Jackmuth

geht den Dingen auf den Grund. Wenn es sinnvoll ist, zeigt er neuartige, kreative Lösungen auf. Aber, was im Leben gilt, gilt auch für Unternehmen: Free Jazz ist nicht für jeden Ort gedacht.