HORNETSECURITY | infinigate

# MICROSOFT 365

## DER ULTIMATIVE LEITFADEN

## Vorwort von Michele Guida von infinigate

Sehr geehrte Leserinnen und Leser

Als Distribution für Cybersecurity-Lösungen ist es uns eine Freude, Ihnen dieses Werk von Hornetsecurity ans Herz legen zu dürfen: «Microsoft 365: Der ultimative Leitfaden". In einer Ära, in der die digitale Transformation unsere Geschäftswelt unaufhaltsam vorantreibt, wird die Sicherheit von Endkunden zu einem immer zentraleren Faktor für den Erfolg von Unternehmen.

Unsere Partnerschaft mit Hornetsecurity ermöglicht es uns, umfassende Leitfäden und Ressourcen bereitzustellen, welche IT-Dienstleister dabei unterstützen, ihre Endkunden optimal zu schützen. Durch den Austausch von Best Practices und die Zusammenarbeit mit IT-Dienstleistern streben wir danach, Vertrauen aufzubauen und langfristige Partnerschaften zu schaffen.

Das vorliegende Buch bietet Ihnen nicht nur technische Lösungen, sondern auch wertvolle Einblicke und Ratschläge, wie Sie die Sicherheit Ihrer Endkunden optimieren können. Es ist eine Ressource für Administratoren und IT-Mitarbeiter, die eine Microsoft 365-Umgebung verwalten, sowie für Business-Entscheider, die sich auf die Cloud-Migration vorbereiten.

Unser Ziel ist es, IT-Dienstleister zu Managed Service Providern (MSP) weiterzuentwickeln, um eine kooperative Zusammenarbeit zu fördern und die Sicherheit von Endkunden auf höchstem Niveau zu gewährleisten. Wir sind fest davon überzeugt, dass nur durch eine enge Zusammenarbeit und gegenseitiges Vertrauen ein nachhaltiger Schutz vor den immer raffinierteren Bedrohungen der digitalen Welt erreicht werden kann.

Ich lade Sie herzlich ein, dieses Buch zu studieren und von den wertvollen Erkenntnissen zu profitieren, die Ihnen dabei helfen werden, die Sicherheit Ihrer Endkunden zu optimieren und Ihre Reise mit Microsoft 365 erfolgreich zu gestalten.

Mit freundlichen Grüssen

**Michele Guida**
Business Development Manager bei Infinigate (Schweiz) AG

# EINLEITUNG

WILLKOMMEN ZU DIESEM KOSTENLOSEN E-BOOK ÜBER MICROSOFT 365 VON HORNETSECURITY. WIR ZEIGEN IHNEN, WIE SIE DIESE CLOUD SERVICES NUTZEN KÖNNEN, UM DAS BESTE AUS DER NUTZUNG VON MICROSOFT 365 FÜR IHR UNTERNEHMEN HERAUSZUHOLEN. DIES IST DIE DRITTE VERSION DIESES E-BOOKS MIT STAND VOM JULI 2023.

MICROSOFT 365
DER ULTIMATIVE
LEITFADEN

## WER SOLLTE DIESES E-BOOK LESEN?

Die Zielgruppe dieses Buches sind Administratoren und IT-Mitarbeiter, die eine Microsoft 365-Umgebung verwalten. Es behandelt Best Practices und optimale Konfigurationen der wichtigsten Anwendungen und Funktionen, gibt aber auch einen Überblick über die gesamte Suite, was besonders für diejenigen nützlich ist, die sich entweder auf die Migration zu Microsoft 365 vorbereiten oder bereits migriert haben und sich einen Überblick verschaffen möchten. Wenn Sie ein Entwickler sind, der Anwendungen und Services für die Microsoft 365-Plattform erstellen möchte, ist dieses Buch nicht das Richtige für Sie.

Wenn Sie eher ein Business-Entscheider als ein technischer Implementierer sind, gibt Ihnen dieses Buch eine gute Einführung in das, was Sie erwarten können, wenn Ihr Unternehmen in die Cloud migriert ist und wie Sie die verschiedenen Dienste von Microsoft 365 nutzen können, um die Effizienz Ihres Unternehmens zu verbessern. Wenn Sie ein Microsoft-Partner sind, der die Deployments anderer Unternehmen verwaltet und Microsoft 365 Lighthouse als Möglichkeit nutzt, mehrere Tenants in einer Konsole zu verwalten, sind die Inhalte dieses E-Books für Sie absolut relevant.

## AUFBAU DIESES E-BOOKS

Das Buch ist in drei Teile gegliedert. Teil 1 (Kapitel 1-6) ist eine Einführung in Microsoft 365. Wenn Sie bereits mit den Grundlagen vertraut sind, können Sie zu Teil 2 (Kapitel 7-13) übergehen, um mehr über die alltägliche Verwaltung und das Management, bewährte Verfahren und die Wartung zu erfahren. Der letzte Teil (Kapitel 14-16) konzentriert sich auf drei kritische M365-Themen, die alle Microsoft 365-Umgebungen berücksichtigen müssen, nämlich Security, Backup und Compliance.

Wir werden die Unterschiede im weiteren Verlauf des Buches näher erläutern, aber an dieser Stelle sollte klargestellt werden, dass es sich bei Office 365 (im Folgenden als O365 bezeichnet) um E-Mail- und Office-Anwendungen für die Zusammenarbeit und eine Vielzahl anderer Services handelt, die als Software as a Service (SaaS) bereitgestellt werden, während es sich bei Microsoft 365 (M365) um Office 365 plus Azure Active Directory Premium, Endpoint Manager (Intune) – eine Cloud-basierte Verwaltung von Endgeräten und deren Security - sowie Windows 11 Enterprise handelt. Bei beiden handelt es sich um benutzerbasierte Abonnement-Services, die keine (oder nur eine sehr geringe) Infrastrukturbereitstellung bei Ihnen vor Ort bzw. on-premises erfordern. Für die kleineren Business Pläne (bis zu 300 Benutzer) ist nur Microsoft 365 verfügbar, und während beide als Enterprise Pläne verfügbar sind, bedeuten die enormen Vorteile der zusätzlichen Services in Microsoft 365, dass es ungewöhnlich wäre, nur Office 365 Pläne zu haben. Daher werden wir uns von nun an hauptsächlich auf Microsoft 365 beziehen.

Dies ist die dritte Version dieses E-Books mit Stand vom Juli 2023.

# INHALTSVERZEICHNIS


Teil 1

# OFFICE & MICROSOFT 365 GRUNDLAGEN

MICROSOFT 365
DER ULTIMATIVE
LEITFADEN



In diesem Abschnitt werden M365, die grundlegende Verwaltung, die Migration zu M365, Support-Optionen, die von Ihnen zu unterstützenden und zu verwaltenden Client-Anwendungen sowie Windows 10/11 vorgestellt. Wenn Sie bereits mit M365 vertraut sind und einen tieferen Einblick in die M365-Administration wünschen, können Sie **direkt zu Teil 2 übergehen.**

## WERFEN SIE ÜBERHOLTE VORSTELLUNGEN ÜBER BORD!

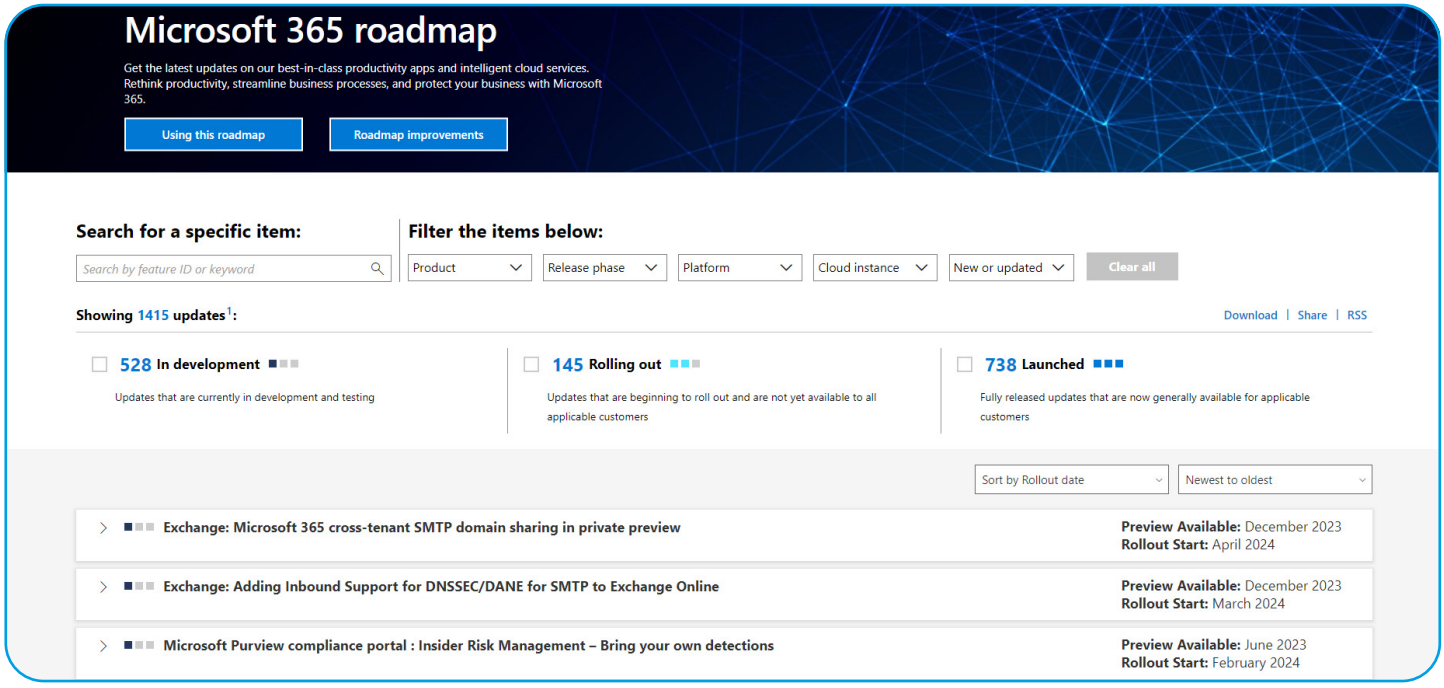
Eines der wichtigsten Dinge, die Sie tun sollten, wenn Sie bereits mit Exchange- oder SharePoint-Servern on-premises Erfahrung haben, ist, sich von der Vorstellung zu lösen, dass M365 nur ein gehostetes Exchange oder SharePoint ist. Vor einigen Jahren war dies der Fall, und O365 war einfach ein Microsoft-Hosting von Exchange-, SharePoint- und Lync-Servern in ihren Rechenzentren, aber das stimmt nicht mehr. M365 ist jetzt eine umfassende Plattform, wobei Exchange und SharePoint einige grundlegende Bausteine für diese Plattform bilden, aber es gibt viele andere darauf aufbauende Dienste, die Sie übersehen (oder missverstehen) werden, wenn Sie immer noch an gehostete Mailserver denken. Ein Beispiel dafür ist Microsoft Teams, ein Service für die Zusammenarbeit, der Exchange zum Speichern von Daten und Chats nutzt, SharePoint zum Speichern von Dokumenten, Planner für ein einfaches Projektmanagement sowie Azure AD für die Verwaltung von Identitäten. All diese Komplexität wird von Microsoft gemanagt, und Sie verwalten Teams einfach wie einen weiteren Dienst. Und das bedeutet auch, dass es nie einen "Teams-Server" on-premises geben wird. Die erforderlichen Komponenten dafür wären für die meisten Unternehmen einfach zu komplex, um sie bereitstellen zu können.

Ein weiterer Punkt, von dem Sie sich verabschieden müssen, wenn Sie aus einer On-Premises-Umgebung kommen, ist die Planung von Software-Upgrades alle paar Jahre. Ein Upgrade vom Exchange-Server kann beispielsweise ein größeres Projekt sein (je nach Größe Ihrer Umgebung), dessen Planung und Durchführung Monate in Anspruch nimmt. M365 ist eine andere Welt, in der jeden Tag oder jede Woche kleinere Updates verfügbar sind, und Ihre Aufgabe besteht nun darin, diese Neuerungen zu bewerten, ihre Auswirkungen auf die Benutzer zu beurteilen und den Wandel im Unternehmen zu managen.

## SO BLEIBEN SIE AUF DEM LAUFENDEN

Ich habe seit Version 5.5 (1997) mit Exchange Server gearbeitet und mich an die Regelmäßigkeit einer neuen Version alle 2-3 Jahre gewöhnt. Ich kaufte Bücher und informierte mich über alle neuen Funktionen und Änderungen, um mich auf die nächste Iteration vorzubereiten. Dieser Ansatz der Softwareentwicklung ist nun vorbei.

Fast alle Softwareprojekte (und ganz sicher die in M365) zielen jetzt auf häufigere, inkrementelle Änderungen ab. Dies bringt mehrere Vorteile mit sich: Erstens ist jede Neuerung eher geringfügig und es ist kein großer Projektplan für das "Upgrade" erforderlich. Zweitens können die Entwickler den Kurs anpassen und auf der Grundlage des Feedbacks der Benutzer viel schneller kontinuierlich neue Funktionen hinzufügen.




*Die Microsoft 365 Roadmap*

Für Sie als M365-Administrator stellt dies jedoch eine große Herausforderung dar. Anstatt eine große Anzahl neuer Funktionen für die nächste große Version zu planen und zu lernen, werden täglich neue Funktionen veröffentlicht, die Sie verstehen und Ihrem Unternehmen helfen müssen, sie zu nutzen. Es gibt verschiedene Möglichkeiten, dies zu bewältigen - je nach Lernstil. Manche Menschen lernen durch Lesen, andere durch Zuhören, wieder andere durch das Anschauen von Videos und manche lernen nur, indem sie Aufgaben selbst erledigen (und die meisten von uns lernen am besten mit einer Mischung aus diesen Methoden).

Hier finden Sie einige Ressourcen, die Sie in Ihren Werkzeugkasten legen können, um mit den Änderungen in M365 Schritt zu halten:

Die offizielle **Microsoft 365 roadmap** (microsoft.com) ermöglicht es Ihnen, nach vielen verschiedenen Komponenten von M365 zu filtern.

**Staying on top of Office 365 Updates** (techcommunity.microsoft.com) ist ein großartiger Blog mit Links zu verschiedenen Ressourcen für die Bewältigung der Flut von Updates, für verschiedene Zielgruppen.

**Neuerungen in Azure Active Directory** umfassen die monatlichen Updates für Entra ID (früher Azure AD) **(siehe Kapitel 7).**

**Azure AD Connect: Verlauf der Versionsveröffentlichungen** umfasst Updates für AAD Connect **(siehe Kapitel 7).**

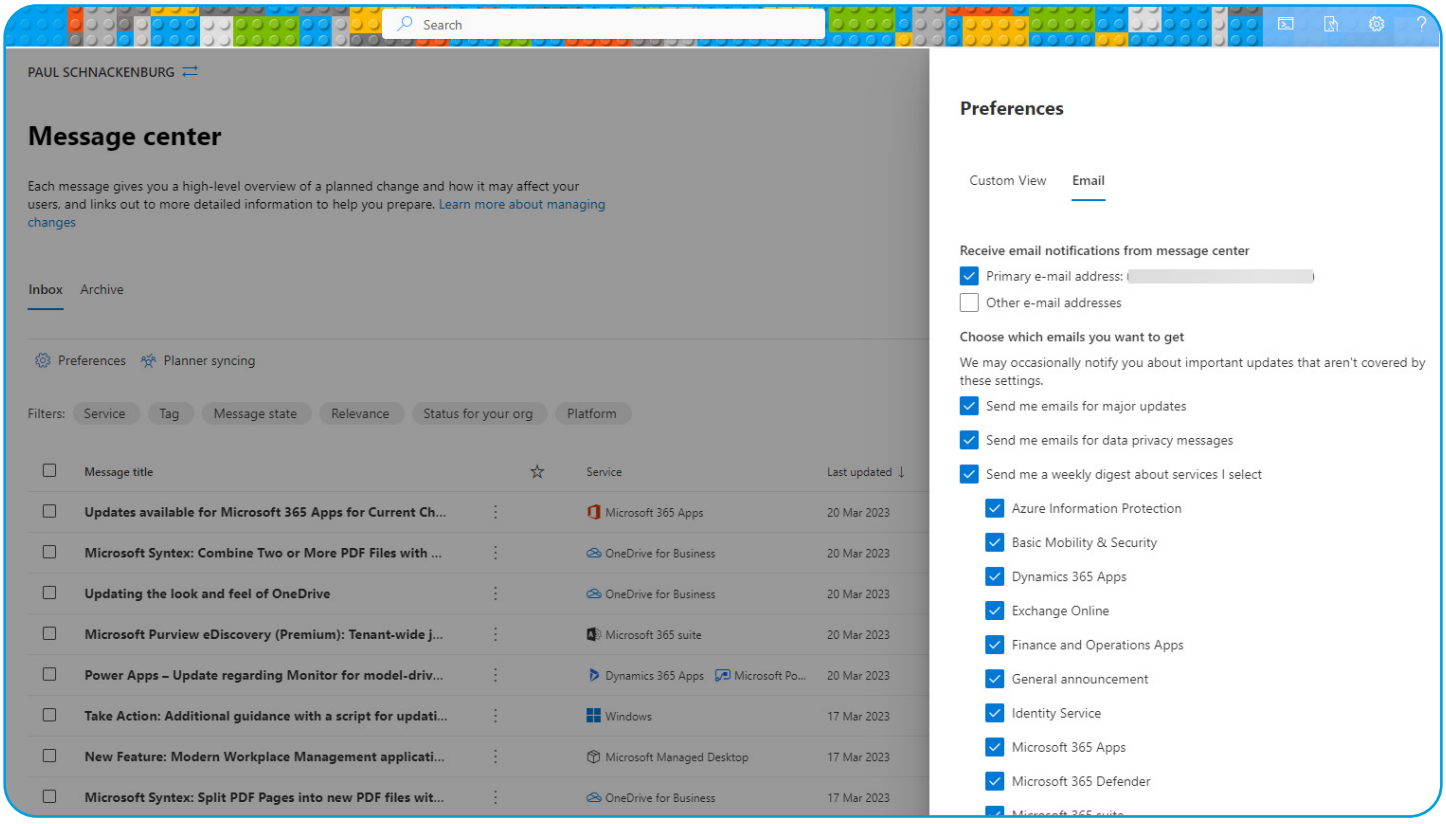
**Microsoft Mechanics** ist ein YouTube-Kanal mit Interviews und Demos zu kommenden Funktionen sowie Playlists zu Office und Azure.

Und schließlich zeigt das **Message Center** im Portal (Kapitel 2) eine Reihe von Änderungen und neuen Funktionen an - klicken Sie auf den Preferences-Link, um festzulegen, für welche Services Sie Updates erhalten und wer die wöchentliche E-Mail-Zusammenfassung erhalten soll - am besten richten Sie einen E-Mail-Verteiler ein, damit Mitarbeiter, die keinen Zugang zum Message Center haben, wöchentliche E-Mail-Updates erhalten können.

## SEIEN SIE IHR EIGENES VERSUCHSKANINCHEN

Es ist wichtig, dass Sie als Administrator neue Funktionen testen, sobald sie herauskommen oder idealerweise, wenn sie sich in der Preview-Phase befinden. Es gibt zwei Arten von Updates für O365: **„Standard" und „Zielversion"** (Targeted Release). Ersteres ist der normale Rollout-Turnus, während letzteres sicherstellt, dass Sie neue Funktionen erhalten, sobald sie zur Verfügung stehen.

In der Vergangenheit wurde empfohlen, dafür einen kleinen, separaten Test-Tenant einzurichten, in dem der gesamte Tenant in **Targeted** war - falls Sie über




*Benachrichtigungen im Message Center verwalten*

das entsprechende Budget verfügen, kann dies sinnvoll sein. Heute ist es üblicher, Mitglieder des IT-Teams und Power-User in Ihrem Unternehmen mit **Targeted Release für ausgewählte Benutzer** zu definieren. Es gibt auch **eine Option**, mit der Sie sicherstellen können, dass Ihre lokalen Office Apps für Enterprise-Installationen Updates vor den anderen Benutzern erhalten.

### ADAPTION

Wenn Ihre Herausforderung darin besteht, anderen in Ihrem Unternehmen zu helfen, auf den M365-Zug aufzuspringen, bietet Microsoft eine **großartige Community** und zahlreiche **Ressourcen**, die Ihnen dabei helfen können. Wenn Sie Hilfe benötigen, um die Einführung von M365-Workloads weiter voranzutreiben, nehmen Sie am kostenlosen Champions Programm teil.

Eine weitere hervorragende Ressource ist **Fasttrack**, das Migrationsanleitungen für jeden M365 Tenant (und Dynamics 365 und Azure) bereitstellt. Wenn Sie M365 nutzen und mehr als 150 Arbeitsplätze haben, können Sie sich online mit einem Migrations-Experten beraten, und wenn Sie mehr als 500 Arbeitsplätze haben, kann Ihnen ein Experte bei der Migration und bei nachfolgenden Adaptions-Projekten **per Fernzugriff zur Seite stehen.**

# KAPITEL 1:

# WILLKOMMEN BEI MICROSOFT (UND OFFICE) 365

**IN DIESEM KAPITEL WERDEN WIR UNS DIE VERSCHIEDENEN VARIANTEN VON M365 ANSEHEN, WIE SIE ZWISCHEN IHNEN WÄHLEN KÖNNEN UND WELCHEN WERT SIE FÜR IHR UNTERNEHMEN BIETEN. WIE BEREITS ERWÄHNT, FAHREN SIE DIREKT MIT TEIL 2 FORT, WENN SIE IHRE M365-UMGEBUNG BEREITS EINGERICHTET HABEN ODER EINEN TIEFEREN EINBLICK ERHALTEN MÖCHTEN.**

**EIN KORREKT IMPLEMENTIERTES MICROSOFT 365 IST EIN KATALYSATOR FÜR IHR UNTERNEHMEN, DER ES IHREN MITARBEITERN ERLEICHTERT, IN TEAMS ZU ARBEITEN UND SOWOHL INTERN ALS AUCH MIT EXTERNEN PERSONEN AUF SICHERE WEISE ZUSAMMENZUARBEITEN. AUSSERDEM ERMÖGLICHT ES IHREN MITARBEITERN EIN SICHERES ARBEITEN VON ZU HAUSE/ÜBERALL. ABGESEHEN VON DER AUSWAHL DER RICHTIGEN M365-VARIANTE LIEGT DER SCHLÜSSEL ZU EINER ERFOLGREICHEN ADAPTION IN DER PLANUNG, DER SCHULUNG DER BENUTZER UND DER GEWÄHRLEISTUNG, DASS IHRE IT-MITARBEITER IHRE NEUE ROLLE VERSTEHEN.**

## 1.1: OFFICE 365

Microsoft hat seinen Fokus auf Office 365 seit einigen Jahren verringert und wird dies auch weiterhin tun. Für Unternehmen mit weniger als 300 Mitarbeitern ist es keine Option mehr, und für größere Unternehmen empfiehlt sich ein Blick auf die Microsoft 365-Pläne (siehe unten).

Auf einige der in diesem Kapitel erwähnten Services wird in späteren Kapiteln näher eingegangen. Wir werden den Begriff SKU verwenden; er steht für Stock Keeping Unit und ist ein Begriff, der verschiedene Lizenzstufen beschreibt.

Die erste Entscheidung, die Sie treffen müssen, ist die zwischen den Business- und Enterprise-SKUs. Erstere ist auf 300 Benutzer begrenzt. Wenn Sie also ein größeres Unternehmen haben (oder ein Wachstum erwarten), sollten Sie bei den Enterprise-Varianten bleiben.

Zur Klarstellung: **Microsoft 365 Apps für Unternehmen** (**früher Office ProPlus genannt**) ist der neue Name für die Desktop-Anwendungen wie Word, Excel usw., die für Windows und Mac verfügbar sind - einige SKUs enthalten sie, andere nicht. Andererseits enthalten alle Pläne Office Online (umbenannt in einfach "Office" - überhaupt nicht verwirrend), also Word, PowerPoint usw., die in einem Browser laufen.

Beachten Sie, dass diese Online-Versionen von Office im Vergleich zu ihren Desktop-Versionen nur über einen eingeschränkten Funktionsumfang verfügen, aber für schnelle Änderungen sehr nützlich sind.

Auf der Enterprise-Seite (was nur ein Name ist, es muss nicht für ein großes Unternehmen stehen - Sie könnten z.B. fünf Anwälte haben, die in einem KMU mit sehr sensiblen Daten arbeiten und Enterprise E5 verwenden) gibt es Apps for Enterprise, das Ihnen nur die Apps for Enterprise und OneDrive-Dateispeicher bietet, aber keine anderen Cloud-Services. Mit E1 erhalten Sie Office (Online) und Exchange, OneDrive, SharePoint, Teams, Yammer und Stream, mit E3 erhalten Sie Microsoft 365 Apps for Enterprise zusätzlich zu den Cloud-Services von E1 und mit E5 kommt PowerBI als Cloud-Service hinzu, zusammen mit verschiedenen Security-Features (siehe Kapitel 15).

Werfen Sie einen Blick auf den **offiziellen Vergleich**, der die Unterschiede zwischen diesen Plänen anschaulich darstellt.

Die **Plan-Optionen für Microsoft 365 und Office 365** decken alle Pläne ab, einschließlich spezieller Versionen für das Bildungswesen, Behörden und länderspezifischer Varianten für China und Deutschland.

Der wichtigste Punkt ist, dass sich die verschiedenen SKUs innerhalb jeder Familie nicht gegenseitig ausschließen. In einem kleinen Produktionsbetrieb können Sie die Fabrikarbeiter mit Business Essentials, die Büroangestellten mit Business und die Führungskräfte mit Business Premium ausstatten. In einem größeren Unternehmen könnten die Benutzer auf E1-, E3- und E5-Lizenzen verteilt sein.

Die **Service-Beschreibung von Microsoft 365 und der Office 365-Plattform** beschreibt genau, was die Plattform bietet.

### 1.2: MICROSOFT 365

M365 baut auf den oben genannten O365-Plänen auf und fügt Windows 10 Enterprise, Endpoint Manager (Intune) und Azure Active Directory Premium hinzu.

Für Unternehmen (bis zu 300 Benutzer) gibt es drei Optionen: **M365 Business Basic**, das Ihnen Office (nur online), E-Mail, Filesharing, Teams und Security-Funktionen bietet. **M365 Business Standard** fügt die Desktop-Version von Office „Microsoft 365 Apps for Business" hinzu, während **M365 Business Premium** die Verwaltung von iOS-, Android- und Windows 10/11-Geräten und die Durchsetzung von Richtlinien mit Intune sowie viele erweiterte Security-Funktionen bietet. Mehr dazu finden Sie **hier**.

Auf der **Enterprise-Seite** gibt es **F3** (für „Frontline"-Mitarbeiter, früher F1 genannt), das Ihnen Office (Online), Windows 10 Enterprise, Active Directory Premium P1, Azure Information Protection P1 und Intune zusätzlich zu O365 E1 bietet. **E3** fügt Active Directory Premium P1, Advanced Threat Analytics (ATA), Azure Information Protection P1, Windows 10 Enterprise und Intune zusätzlich zu O365 E3 hinzu. **E5** schließlich fügt Active Directory Premium P2, Microsoft 365 Defender, Microsoft Defender for Endpoint, Microsoft Defender for Office 365, Microsoft Defender for Identity und Azure Information Protection P2, Windows 10 Enterprise, eine Reihe von Security-Funktionen und Intune zusätzlich zu O365 E5 hinzu.

Es mag verlockend sein zu denken: „Ich bin ein kleines Unternehmen, also kann ich mit Business SKUs ein wenig Geld sparen", aber Sie müssen sich

einiger Einschränkungen bewusst sein. Ihr OneDrive for Business ist in Business auf 1 TB pro Benutzer begrenzt, während Sie dies in Enterprise durch einen Anruf beim Support erhöhen können. Microsoft hat erhebliche Änderungen am Business Premium Plan vorgenommen und bietet nun alle Funktionen von **Azure AD Premium Plan 1**. Zusätzlich zu den bereits enthaltenen Security-Features (Conditional Access, Self-Service-Passwort-Reset und MFA) kommen also Cloud App Discovery, Azure AD Application Proxy, dynamische Gruppen und passwortlose Authentifizierung hinzu. In den Enterprise-Plänen, insbesondere M365 E5, sind viele wertvolle Security-Funktionen enthalten (siehe Kapitel 15).

Beachten Sie, dass Sie Lizenzen zwischen verschiedenen SKUs verschieben können (sowohl Upgrade als auch Downgrade) und dass Sie Business SKUs auf Enterprise SKUs upgraden können. Hier ging es um die kompletten SKUs und die darin enthaltenen Funktionen, aber es ist auch möglich, einzelne Funktionen zu erwerben, wie z.B. Azure Active Directory Premium P1 als eigenständige Funktion. Je nach den Bedürfnissen (einiger) Benutzer in Ihrem Unternehmen können Sie ein Paket mit genau den Funktionen zusammenstellen, die sie benötigen.

Eine gute Möglichkeit, all die verschiedenen Teile von M365 zu verstehen, wie sie zusammenpassen, und eine kurze Beschreibung der einzelnen Services ist das **Periodensystem von Microsoft 365.**

Das Wichtigste, was Sie aus diesem Kapitel mitnehmen sollten, ist, nicht davon auszugehen, dass Sie sich als kleines Unternehmen automatisch für eine Business-SKU entscheiden sollten, sondern genau zu prüfen, welche Funktionen für Ihr Unternehmen geeignet sind, und sich nicht davor zu scheuen, verschiedene SKUs für unterschiedliche Mitarbeiterrollen zu kombinieren.

# KAPITEL 2:

# MANAGING O365 AND M365

**SOBALD SIE IHREN TENANT IN M365 EINGERICHTET HABEN, MÜSSEN SIE IHN VERWALTEN. IN DIESEM KAPITEL GEHEN WIR AUF DIE VERSCHIEDENEN SCHNITTSTELLEN EIN, DIE SIE VERWENDEN KÖNNEN.**

**WENN SIE NOCH KEINEN O365 / M365 TENANT HABEN, KÖNNEN SIE SICH FÜR EINEN PROBE-TENANT ANMELDEN - KLICKEN SIE EINFACH AUF „KOSTENLOS TESTEN" UNTER E3 ODER E5. DIESE TENANTS HABEN EINE LAUFZEIT VON 30 TAGEN. SIE KÖNNEN DIE TESTPHASE UM WEITERE 30 TAGE VERLÄNGERN, INDEM SIE DEN SUPPORT KONTAKTIEREN.**

## 2.1: WEB-PORTALE

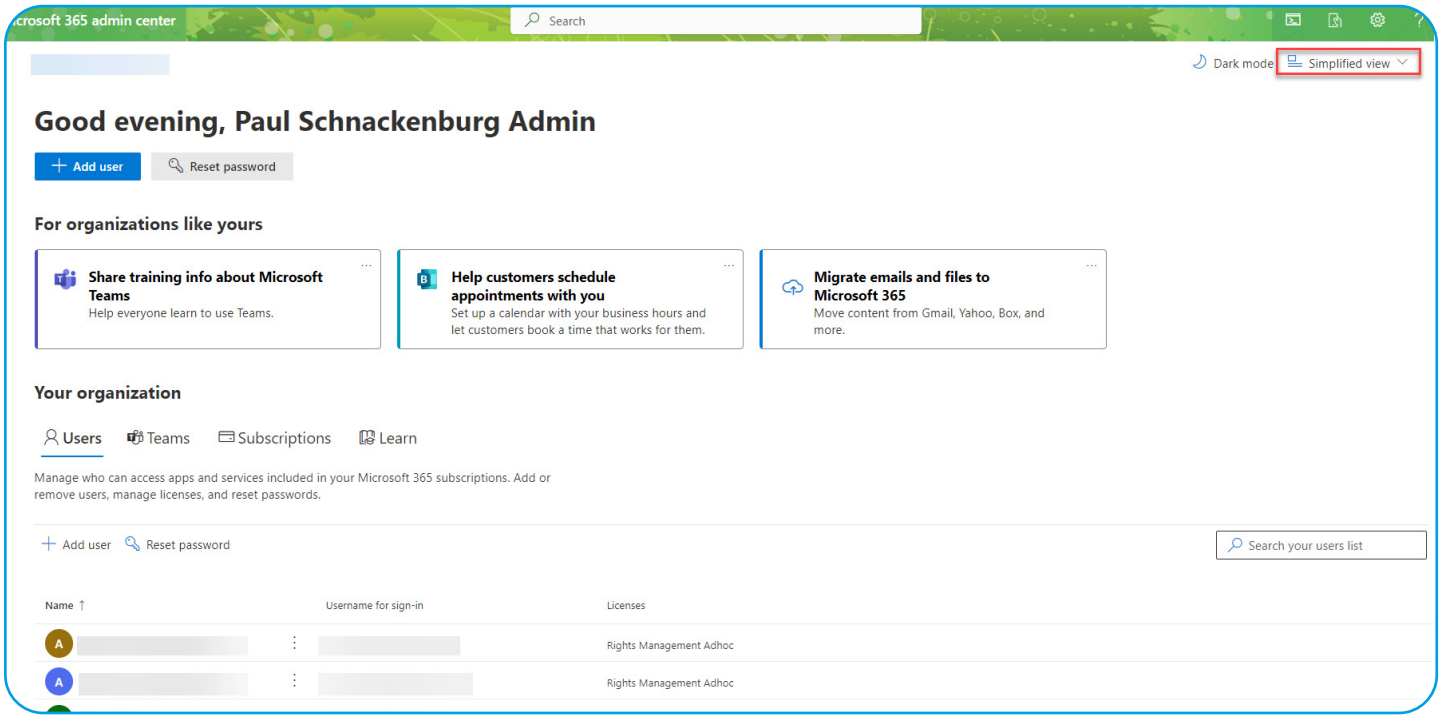
Das Hauptportal ist **admin.microsoft.com**, das Sie auch über **www.office.com** erreichen können. Auf der linken Seite finden Sie Links zur Verwaltung von Benutzern, Gruppen, Abrechnung und Einstellungen usw. und weiter unten unterhalb von Admin Center finden Sie Links zu den einzelnen Portalen für Exchange, Teams, SharePoint, OneDrive und andere. Abhängig von Ihrer SKU werden Ihnen eventuell unterschiedliche Links angezeigt.

Zu den Highlights für die tägliche Arbeit gehört die Möglichkeit, Benutzer mehrfach auszuwählen ("Users - Active users") und z.B. deren Lizenzierung zu ändern. Unter "Users - Guest users" können Sie eingeladene externe Benutzer verwalten, denen Dokumente von OneDrive oder SharePoint zur Verfügung gestellt wurden. Sie können auch einen kürzlich (vor 30 Tagen oder weniger) gelöschten Benutzer wiederherstellen.

Sie können Gruppen und gemeinsam genutzte Postfächer verwalten, z.B. "sales@mycompany.com", auf die mehrere Personen Zugriff haben, sowie Ressourcen wie Räume und Geräte (Buchung von Konferenzräumen oder Firmenwagen). Im Bereich Abrechnung können Sie zusätzliche Lizenzen erwerben, Ihre Abonnements und Zahlungsmethoden verwalten und im Bereich Support können Sie Service-Anfragen stellen. Unter Einstellungen finden Sie einen Bereich, in dem Sie verschiedene Services und Add-Ins konfigurieren können, während Sie unter Setup Ihre E-Mail-Domänen verwalten können. Berichte enthält sowohl Nutzungs- als auch Sicherheitsberichte, während Integrität zwei wichtige Bereiche enthält: Dienststatus zeigt Ihnen, ob es in der Cloud Probleme mit Ihren Ressourcen gibt, und Nachrichtencenter enthält eine Liste der kommenden Updates und Änderungen.

Mit jedem einzelnen Admin Center können Sie einen einzelnen Service wie Azure Active Directory oder Teams verwalten. Unter **Msportals.io** finden Sie alle Links zu den verschiedenen Portalen, auf die Sie direkt zugreifen können, ohne über das Hauptportal zu gehen.

Beachten Sie, dass Sie als kleines Unternehmen die Möglichkeit haben, das Admin Center in der vereinfachten Ansicht (anstelle der Dashboard-Ansicht) zu nutzen, die den Großteil der Komplexität ausblendet und einen einfachen Zugriff auf die grundlegenden Aufgaben der Benutzer-, Gruppen-, Team- und Geräteverwaltung ermöglicht. Klicken Sie einfach auf „Vereinfachte Ansicht" (Simplified View) oben rechts auf der Startseite im Admin Center.




*M365 Admin Center Simplified view*

## 2.2: POWERSHELL

Für kleine Tenants werden Sie wahrscheinlich nie über das Webportal hinausgehen müssen, aber wenn Sie eine große Anzahl von Benutzern haben, werden Sie häufige Aufgaben in der PowerShell automatisieren wollen, indem Sie das neuere **Azure AD-Modul** verwenden.

Um das Modul zu installieren, führen Sie in einem erweiterten PowerShell-Fenster einfach aus:
`Install-Module -Name AzureAD`

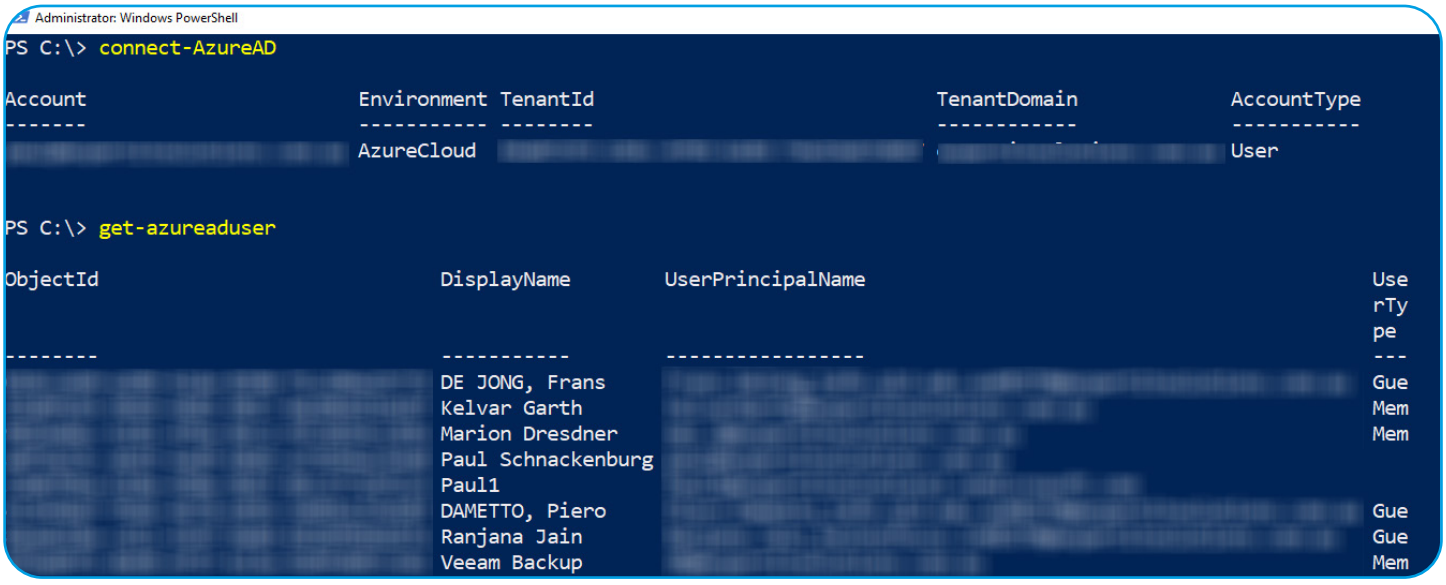
Um sich zu verbinden (und optional mit MFA zu authentifizieren) verwenden Sie:
`Connect-AzureAD`

Um zu überprüfen, ob alles funktioniert, verwenden Sie:
`Get-AzureADUser`

Damit erhalten Sie eine Liste der Benutzer in Ihrem Tenant. Lesen Sie die **ausführliche Anleitung**, auch wenn Sie eine Verbindung zu Regierungs- oder chinesischen/deutschen Tenants herstellen wollen.

Sobald Sie verbunden sind, gibt es viele Aufgaben, die Sie erledigen und vielleicht automatisieren möchten, z.B. die **Verwaltung von Benutzerkonten und Lizenzen**, die **Erstellung von SharePoint Sites und die Verwaltung von Benutzern und Gruppen**, die **Konfiguration von Exchange-Einstellungen**, die **Verwaltung von E-Mail-Migrationen** (Kapitel 3) oder das **Verwalten von Teams-Informationen**. Beachten Sie, dass für einige dieser Aufgaben zusätzliche Module installiert werden müssen.

Microsoft hat schließlich einen offiziellen, skriptbasierten **Weg dokumentiert**, um eine einzige PowerShell-Sitzung auszuführen, die mit allen verschiedenen Diensten verbunden ist, unabhängig davon, ob Sie MFA (Kapitel 7) verwenden oder nicht.



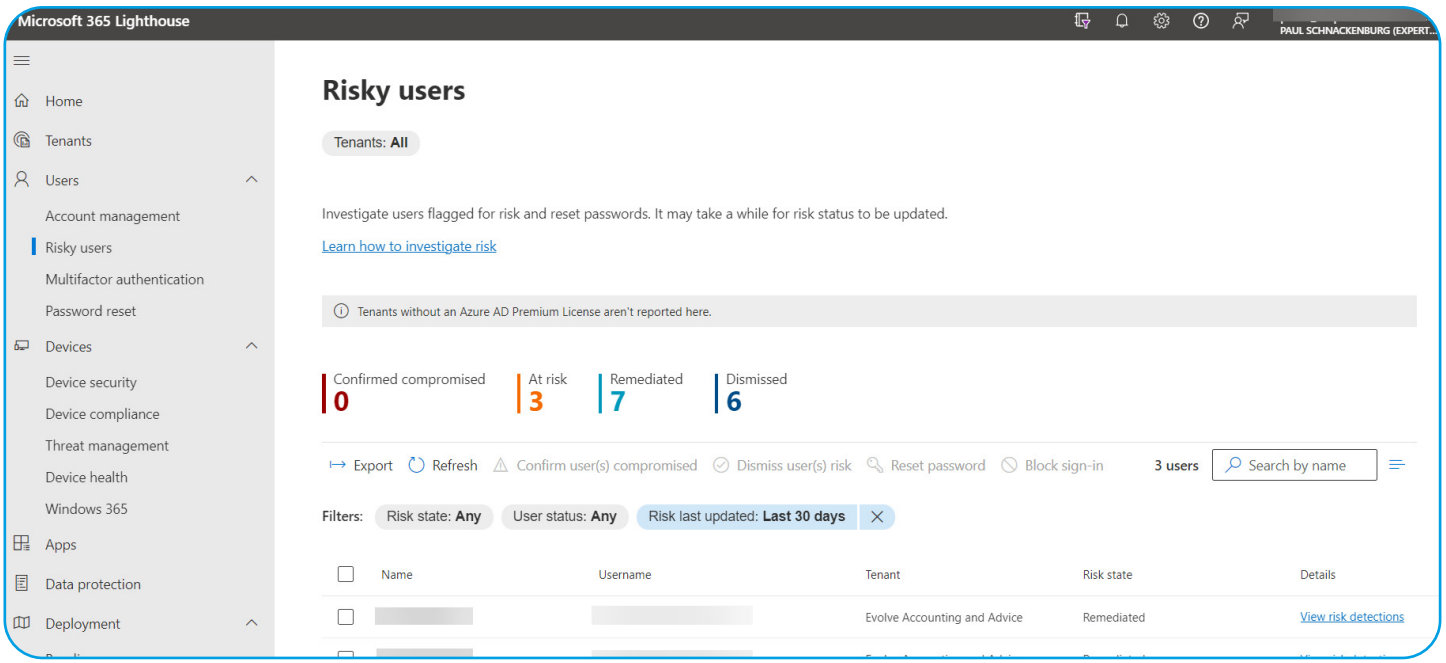

*Connecting with PowerShell*

Für SharePoint (sowohl Online als auch on-premises 2013/2016/2019) gibt es eine Open-Source-Alternative / Ergänzung namens **PnP PowerShell** zum offiziellen SharePoint-Modul des Patterns and Practices (PnP)-Teams. Die offiziellen SharePoint Online-Cmdlets konzentrieren sich auf die Erstellung/Verwaltung von Sites und Benutzern, während die PnP-Cmdlets für die Arbeit mit Artefakten innerhalb von Sites nützlich sind, die bereits erstellt wurden.

Wenn Sie M365 Tenant-Einstellungen oder SharePoint Framework (SPFX)-Erweiterungen verwalten müssen, werfen Sie einen Blick auf **CLI for Microsoft 365**, ebenfalls vom PnP-Team, das auf **Windows, macOS und Linux läuft**. Und wenn Sie keine Lust haben, CLI auf Ihrem Rechner zu installieren, können Sie es **direkt in Azure Cloud Shell ausführen.**

## 2.3: MICROSOFT 365 LIGHTHOUSE

Wenn Sie als Managed Service Provider (MSP) mehrere M365 Tenants betreuen, sollten Sie Microsoft 365 Lighthouse verwenden, nicht zu verwechseln mit Azure Lighthouse. Beides sind Technologien, die es Service Providern ermöglichen, mehrere Tenant-Clients zu verwalten. Doch während die Azure-Variante den Nutzern des Service Providers einen eingeschränkten Zugriff auf Azure-Ressourcen ermöglicht, ist M365 Lighthouse ein Portal, über das Sie mehrere Tenants einbinden, die Anwendung von Richtlinien und die Verwaltung (einschließlich dem Zurücksetzen von Passwörtern für jeden Benutzer in jedem Tenant) in einer einzigen Konsole vornehmen können.




*Microsoft 365 Lighthouse*

# KAPITEL 3:

# MIGRIEREN NACH O365

**WENN SIE MIT IHREM UNTERNEHMEN GERADE ERST AUF DER "GRÜNEN WIESE" BEGINNEN, IST DIESES KAPITEL FÜR SIE NICHT RELEVANT. ERSTELLEN SIE EINFACH BENUTZERKONTEN IN DER CLOUD, VERBINDEN SIE IHRE WINDOWS 10/11-GERÄTE MIT ENTRA ID UND VERWALTEN SIE IHRE IOS- UND ANDROID-GERÄTE MIT ENDPOINT MANAGER UND SIE KÖNNEN LOSLEGEN.**

## 3.1: MIGRATION

Die meisten Unternehmen haben jedoch in bestehende On-Premise-Technologien investiert und müssen nun **nach M365 migrieren**. Dieses Kapitel befasst sich mit Ihren verschiedenen Optionen:

- Übernahmemigration (Cutover Migration)
- Mehrstufige Migration (Staged Migration)
- Express Hybrid Migration
- Minimal Hybrid Migration
- Hybrid Migration
- PST-basierte Migration
- IMAP-Migration
- Drittanbieter-Tools

Wenn Sie Exchange nicht on-premises betreiben, d.h. Sie verwenden **Lotus Notes** / Domino, ein anderes E-Mail-System, **Google Workspace** oder eine andere Cloud-E-Mail-Lösung, müssen Sie entweder eine IMAP-Migration oder Migrationsdienste von Drittanbietern in Betracht ziehen.



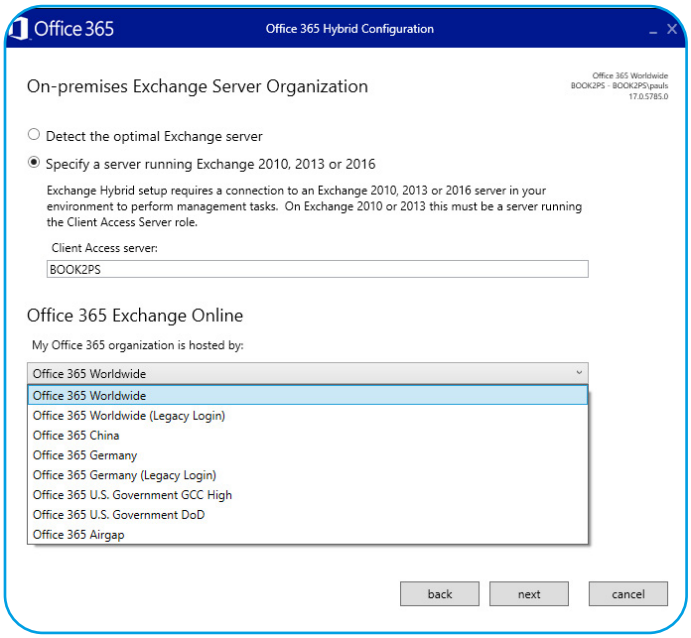
Die meisten anderen Migrationsmethoden beruhen auf einer Verzeichnissynchronisierung, bei der Ihre lokalen bzw. on-premises AD-Konten mit Azure AD synchronisiert werden, was wir in Kapitel 7 behandeln werden.

Wenn Sie noch mit Exchange 2007, 2010 oder 2013 arbeiten (die alle nicht mehr unterstützt werden), können Sie mit einer **mehrstufigen Migration Postfächer stapelweise migrieren**, sobald Sie die Verzeichnissynchronisierung konfiguriert haben. Beachten Sie, dass Sie das Outlook-Profil jedes Benutzers manuell neu konfigurieren müssen, damit es auf O365 verweist, wenn dessen Postfach migriert wurde.

Für kleinere Umgebungen ist die **Übernahme-migration** bzw. der Cutover-Ansatz am einfachsten. Microsoft empfiehlt **diese Methode** für weniger als 2000 Postfächer (Exchange 2003+), aber in der Praxis ist sie wahrscheinlich eher für 100-150 Postfächer geeignet, je nach Internet-Bandbreite. Die Idee ist, dass Sie die Postfächer aller Benutzer an einem Wochenende oder während einer anderen geeigneten Ausfallzeit vom lokalen System in die Cloud verschieben.

Wenn Sie mit Exchange 2010+ arbeiten und planen, alle Postfächer innerhalb weniger Wochen in die Cloud zu verlagern, sollten Sie die **Hybridoption Express** in Betracht ziehen. Wenn Sie eine größere Umgebung haben und mit einigen Monaten Migrationszeit rechnen, sollten Sie sich die **Minimal-Hybrid-Alternative** ansehen. Wenn Sie eine größere Umgebung haben (Exchange 2010+) und davon ausgehen, dass Sie sich für längere Zeit in einem hybriden Zustand befinden werden und die Möglichkeit benötigen, Postfächer aus der Cloud zurück nach on-premise zu verschieben (Offboarding), sollten Sie **Full Hybrid** in Betracht ziehen. Eine vollständige Aufschlüsselung der verschiedenen **Hybrid-Varianten finden Sie hier.** Die verschiedenen Hybridbereitstellungen **bieten eine reichhaltige Koexistenz** mit einer vereinheitlichten globalen Adressliste, gemeinsamer Nutzung von Frei/Gebucht-Kalenderinformationen und Postfachverschiebungen, die für Endbenutzer reibungslos ablaufen. Wenn ihr Postfach verschoben wurde, werden sie lediglich aufgefordert, Outlook neu zu starten.

Wenn Sie einen (oder mehrere) Exchange-Server vor Ort bzw. on-premises behalten müssen, sollten Sie ihn **auf dem neuesten Stand halten, um nicht beeinträchtigt zu werden**. Wenn möglich, **sollten Sie ihn ausmustern** und stattdessen PowerShell-Cmdlets zur Verwaltung von Exchange-Attributen im AD verwenden.




*Hybrid Configuration Wizard*



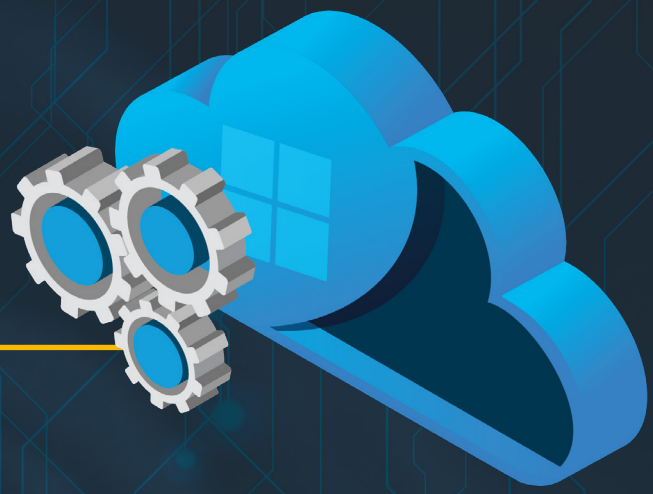
In der **Dokumentation von Microsoft** werden Sie auf den **Mail-Migrationsratgeber** verwiesen, der Sie - je nach Ihrer Auswahl - zum Assistenten für die Hybridkonfiguration (Hybrid Configuration Wizard bzw. kurz: HCW) weiterleitet. Der HCW führt Sie Schritt für Schritt durch die einzelnen Schritte, die Sie unternehmen müssen, je nachdem, welchen Weg Sie einschlagen, einschließlich der Hybrid-Migrations-Varianten sowie der mehrstufigen und der Übernahmemigration.

Mit **IMAP-Migrationen** können Sie von Nicht-Exchange-Systemen umziehen, die IMAP mit einem Limit von 500.000 Objekten pro Postfach und einer maximalen E-Mail-Größe von 35 MB unterstützen.
Wenn Sie E-Mail PST-Dateien on-premise haben, können Sie diese zu Office 365 migrieren. Es gibt sogar ein PST-Sammel-Tool, mit dem Sie diese Dateien in Ihrem Netzwerk aufspüren und zusammentragen können. Wenn Sie viele davon haben, können Sie sie sogar **auf Disks an Microsoft schicken.**

Sobald Sie die Migration abgeschlossen haben, müssen Sie Ihren **Mail Exchanger (MX) DNS-Eintrag** überprüfen, der auf Ihren lokalen E-Mail-Server verweist und nun geändert werden muss, damit er auf Exchange Online verweist. Außerdem müssen Sie Ihre **Autodiscover-DNS-Einträge** überprüfen, mit denen Outlook und andere E-Mail-Clients automatisch den richtigen Exchange-Server finden.

Wenn Sie auf der Suche nach einer einfachen Mailbox-Migration sind, bietet Hornetsecurity das Mailbox Migration Tool (MMT) als Teil seiner **365 Total Protection Enterprise** Lösung an.

# KAPITEL 4:

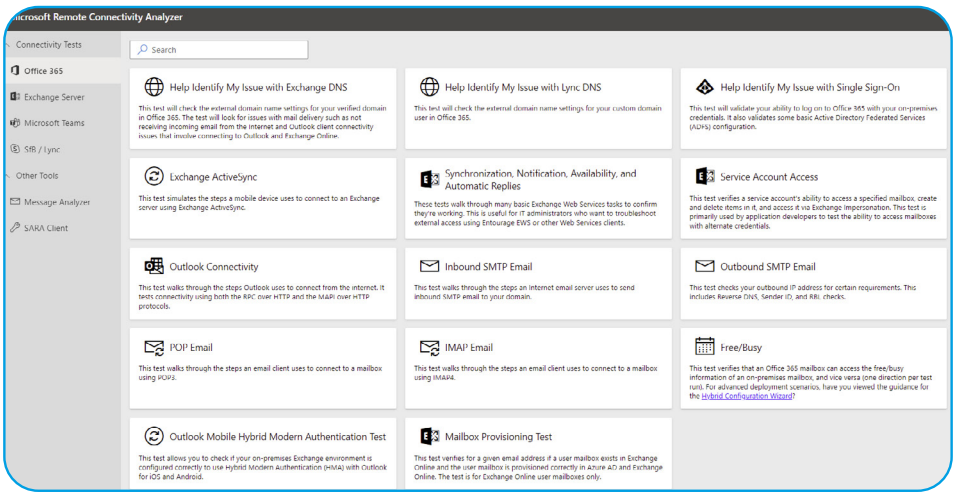


# SUPPORT-UNTERSTÜTZUNG FÜR M365

**EINE GROSSE HERAUSFORDERUNG FÜR UNS IN DER IT, ZUMINDEST ANFANGS, IST DER VERLUST AN KONTROLLE, DEN DIE CLOUD MIT SICH BRINGT. WENN SIE ON-PREMISE EIN PROBLEM MIT DER E-MAIL-ZUSTELLUNG HABEN, KÖNNEN SIE JEDES GLIED DER KETTE ÜBERPRÜFEN, UM ZU SEHEN, WO DAS PROBLEM LIEGT. SOBALD SIE AUF M365 MIGRIERT SIND, TEILEN SIE SICH DIE VERANTWORTUNG MIT MICROSOFT. IN DIESEM KAPITEL SEHEN WIR UNS ZWEI SELBSTHILFETOOLS AN, DIE ICH BEI PROBLEMEN VERWENDE, UND DANN SEHEN WIR UNS AN, WIE SIE EINEN SUPPORTFALL BEI MICROSOFT ERÖFFNEN UND BEARBEITEN.**

### 4.1: VERBINDUNGEN TESTEN

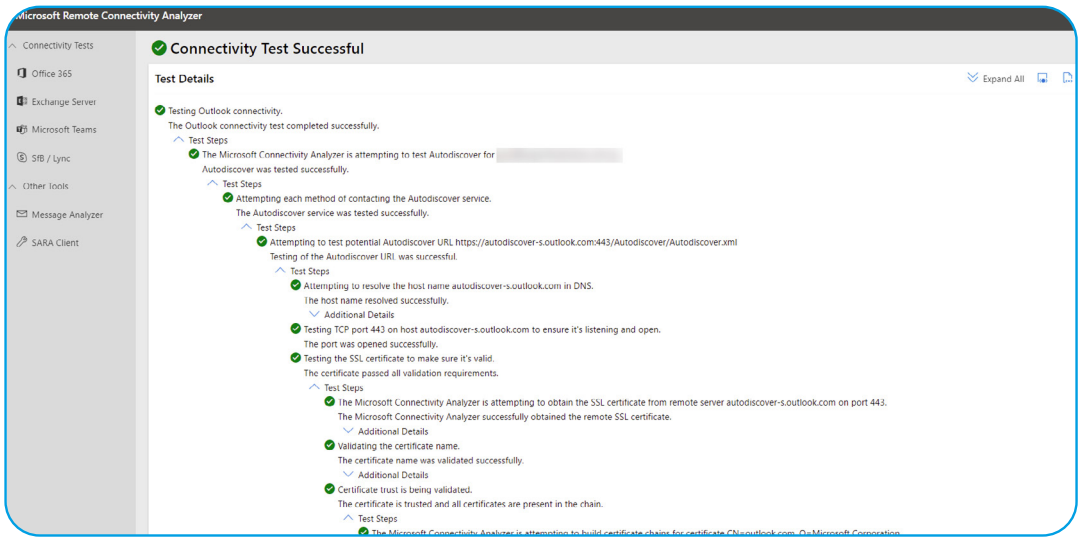
Bei E-Mail und Teams ist die Verbindung eine häufige Ursache für Probleme. Microsoft bietet ein nützliches Tool an: Microsoft Remote Connectivity Analyzer (MRCA oder RCA) unter **https://testconnectivity.microsoft.com/**.




*Remote Connectivity Analyzer*

Hier können Sie verschiedene Dinge testen: DNS-Einträge, ActiveSync-Konnektivität zu Exchange, Outlook und Outlook Autodiscover-Funktionalität sowie eingehende und ausgehende SMTP-E-Mails usw. Wählen Sie den Test, den Sie durchführen möchten, und geben Sie die erforderlichen Informationen ein. Je nach Test müssen Sie einen gültigen Benutzerkonto-Namen und ein gültiges Kennwort eingeben - ich empfehle, das Kennwort dieses Kontos zurückzusetzen, nachdem Sie die Fehlerbehebung abgeschlossen haben. Die Captcha-Verifizierung gilt für 30 Minuten. Wenn Sie also mehrere Durchläufe machen, während Sie Ihre Werte ändern, müssen Sie nicht jedes Mal bestätigen, dass Sie ein Mensch sind.

Die Testberichte sind ausführlich und sollten Ihnen helfen, das Problem recht schnell zu lokalisieren.

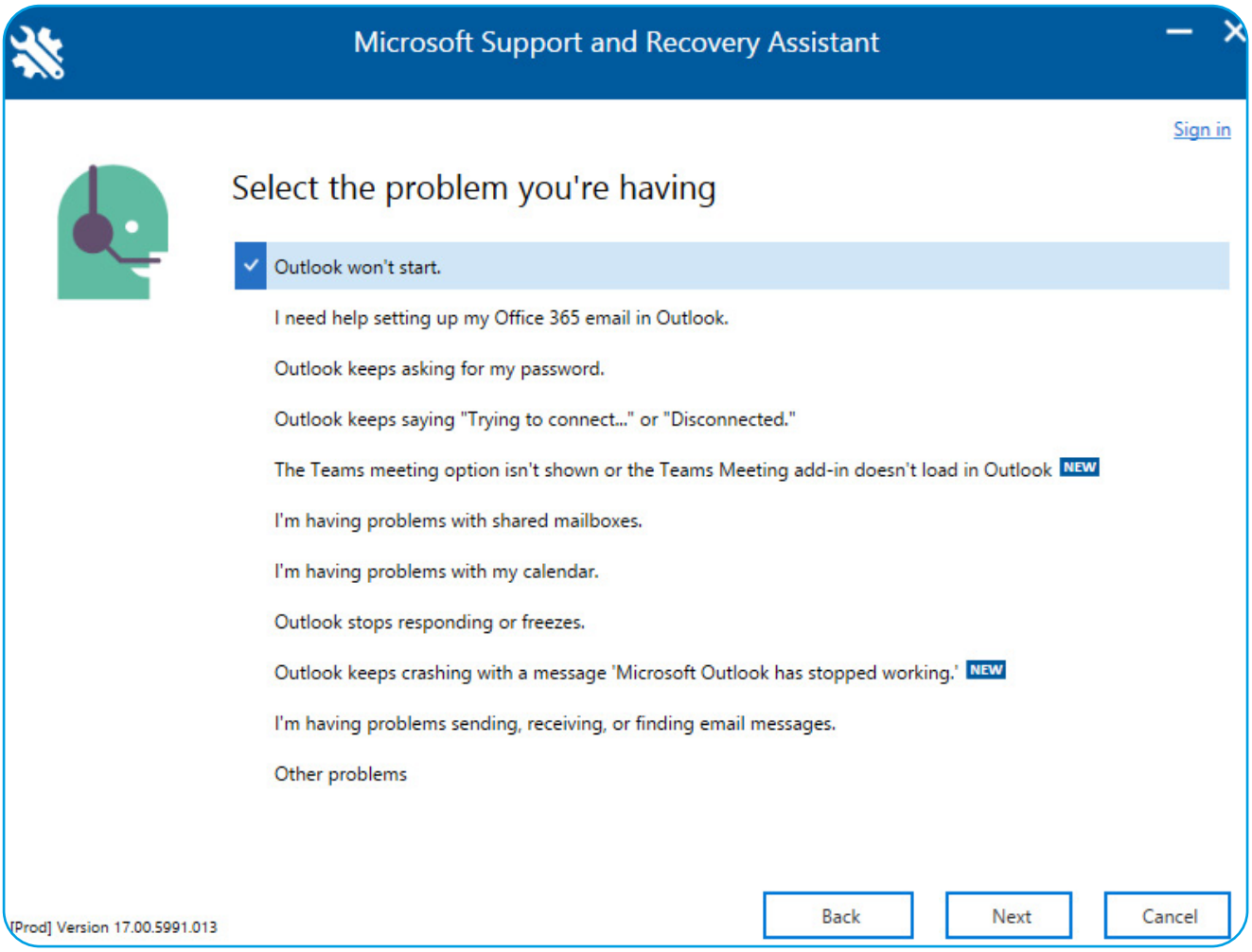



*Connectivity test report*

## 4.2: CLIENT-SEITIGE TOOLS

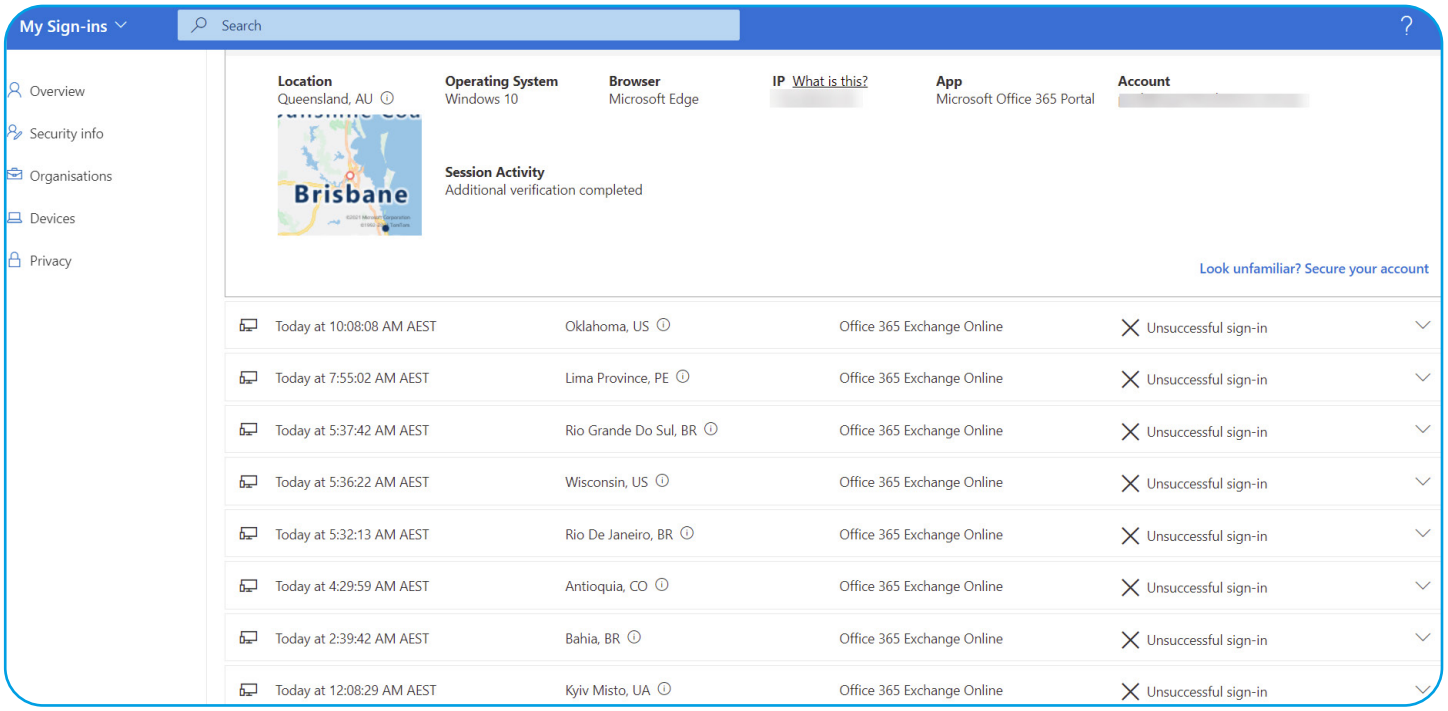
Wenn das Problem nicht mit der Konnektivität zusammenhängt und Sie stattdessen ein Problem auf einem bestimmten Client-Gerät vermuten, sollten Sie den **Support- und Wiederherstellungs-Assistenten für Office 365 (SARA)** verwenden, der bei der Identifizierung von Outlook-, Dynamics 365- und OneDrive for Business-Problemen sowie von Problemen mit Apps for Enterprise hilft. Es handelt sich dabei um einen einfachen Download, den Sie auf dem betroffenen Gerät ausführen.

Meiner Erfahrung nach ist SARA ziemlich gut darin, die Ursache für Profil- oder zeitweilige Verbindungsprobleme (die nicht auf eine Fehlkonfiguration auf der Service-Seite zurückzuführen sind - siehe RCA) aufzuspüren, wenn Sie damit zu kämpfen haben.




*Support- und Wiederherstellungs-Assistent*

Eine weitere Hilfe zur Selbsthilfe für Endbenutzer sind die Sites "**My Sign-ins**", "**My Groups**" und "**My Access**", die zusammen mit "**My Applications**" den Benutzern eine gute Möglichkeit bieten, ihren Zugriff auf die M365 Services zu verwalten. „My Sign-ins" ist auch ein hervorragendes Schulungsinstrument, da es sowohl erfolgreiche als auch fehlgeschlagene Anmeldungen von Angreifern auflistet. Hier sehen Sie eine Liste, wie mein Konto an einem typischen Tag aussieht (MFA ist für dieses Konto aktiviert):




*My Sign-Ins mit den Anmeldeversuchen der Angreifer*

## 4.3: SERVICE-ANFRAGEN

Wenn Sie die Selbstbedienungsoptionen ausgeschöpft haben, klicken Sie auf die Schaltfläche "Brauchen Sie Hilfe?" in der unteren rechten Ecke des Portals. Beginnen Sie damit, eine Beschreibung Ihres Problems einzugeben, die Ihnen einige Ergebnisse zu häufigen Problemen und deren Lösung liefern kann. Sobald Sie Enter drücken, leuchtet unten die Option Support kontaktieren auf. Geben Sie Ihre Kontaktinformationen ein und wählen Sie zwischen Telefon und E-Mail. Sie können auch Screenshots oder Protokolldateien anhängen (bis zu fünf, jeweils mit einer Größe von maximal 25 MB), eine Zeitzone und eine Sprache für die Kommunikation wählen.

Meiner Erfahrung nach ist der Support für M365 gut und kommt dem Problem in der Regel viel schneller auf die Spur, als wenn ich auf eigene Faust in Foren suchen und verschiedene Lösungen ausprobieren würde.

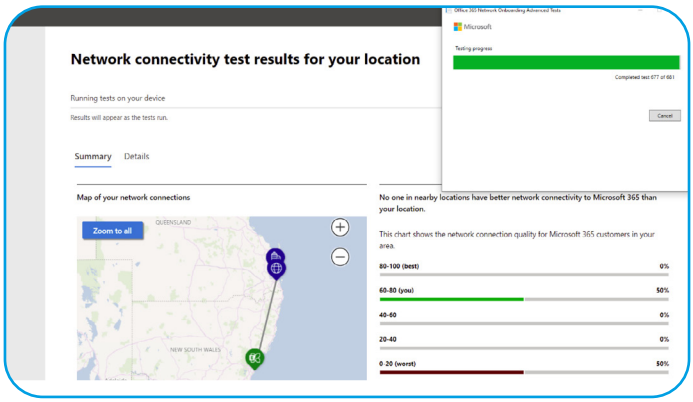
Hinter den Kulissen - in dem seltenen Fall, dass der Support-Techniker Zugriff auf einen Server benötigt, auf dem Ihre Daten liegen, verwendet er ein "Lockbox-System", bei dem er den Zugriff beantragt und ein Vorgesetzter die Anfrage für eine begrenzte Zeit genehmigt. Wenn Sie mit O365 / M365 E5 arbeiten, haben Sie möglicherweise die **Kunden-Lockbox** aktiviert, die Sie in diesen Prozess einbezieht, und Sie müssen die Anfrage ebenfalls genehmigen.

Liegt das Problem hingegen auf Ihrer Seite, verwenden die Support-Techniker Quick Assist in Windows, um sich mit Ihrem Server oder Client-PC zu verbinden und das Problem gemeinsam mit Ihnen zu lösen.

## 4.4: SERVICE HEALTH STATUS

Der Bereich „Integrität" des Admin Centers gibt Auskunft über den allgemeinen Betriebszustand der verschiedenen Services in M365 und darüber, ob es Ausfälle/Vorfälle gibt, die Ihren Tenant betreffen, sofern Sie auf das Portal zugreifen können. Wenn der Ausfall das Portal oder den Health-Teil davon betrifft, versuchen Sie **https://status.office365.com/.** Folgen Sie auch @Office365Health und @MSFT365Status auf "X", dem früheren Twitter.

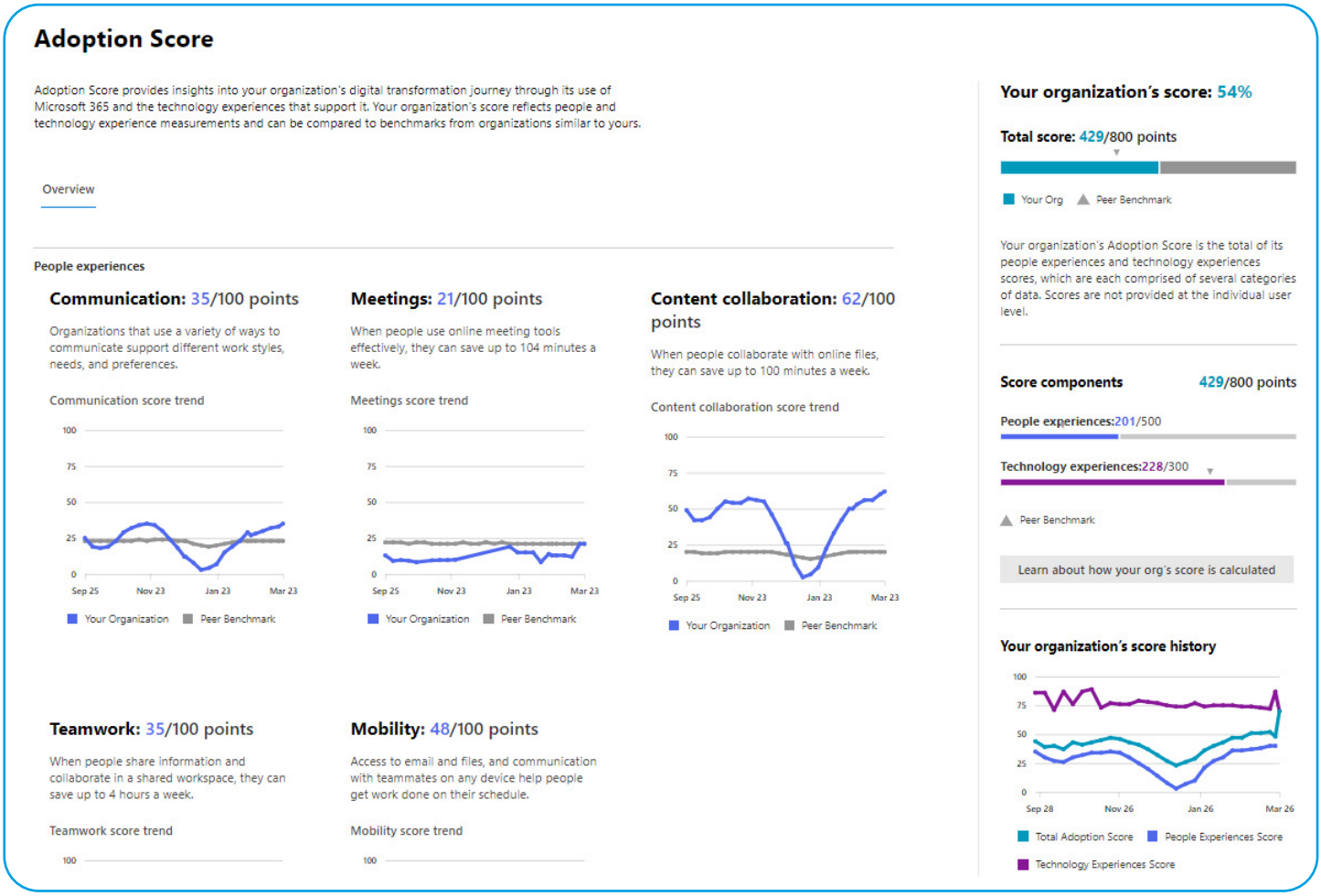
Der Bereich Integrität bietet auch ein interessantes neues Tool namens **Netzwerkkonnektivität**, das den OD4B-Client zusammen mit dem Windows Location Service und optionalen manuellen Tests zur Datenerfassung verwendet, um die **Verbindungsqualität der einzelnen Clients zu Office 365** zu ermitteln. Es hat sogar ein **eigenes Portal**.



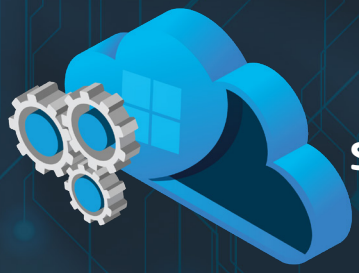

*Manual Network Connectivity test to Office 365*

### 4.5: NETZWERK-KONNEKTIVITÄT

Viele Unternehmen bieten ihren Benutzern ein unterdurchschnittliches Erlebnis, indem sie sie zwingen, VPN-Verbindungen zurück ins Büro und dann weiter zu Office 365 zu nutzen (insgesamt ein langsameres Nutzererlebnis, aber ein Killer für die Sprach- und Videoanrufe von Teams) oder sogar den gesamten ausgehenden Datenverkehr aus "Sicherheitsgründen" über einen Proxy umzuleiten. Letzteres basiert auf der irrtümlichen Annahme, dass alle Webservices/Internetsites "gefährlich" sind und der gesamte Datenverkehr überprüft werden muss, anstatt zwischen vertrauenswürdigen Business Services von Microsoft und anderen und fragwürdigen Websites zu unterscheiden und den Datenverkehr entsprechend zu behandeln. Hier ist ein **ausgezeichneter Artikel**, der die erforderlichen und optionalen Optimierungstechniken für M365 beschreibt.




*Microsoft 365 Adoption Score*





Microsoft ist außerdem Partnerschaften mit vielen ISPs, Internet Exchange Partners (IXPs) und Software-defined Cloud Interconnect (SDCI) Anbietern eingegangen, um über den **Azure Peering Service** eine optimale Konnektivität zu M365, Dynamics 365 und Azure zu gewährleisten.

Wenn Ihr Unternehmen ein Software Defined WAN (SD-WAN) verwendet, gibt es eine Funktion namens "**Informiertes Netzwerk-Routing**", die Ihre Konnektivität weiter optimiert, indem sie den Datenaustausch zwischen Microsoft und dem SD-WAN-Anbieter ermöglicht, um den Datenverkehr gegebenenfalls automatisch umzuleiten. Derzeit wird nur Ciscos IOS XE SD-WAN unterstützt, aber es ist zu erwarten, dass mit dem Fortschreiten der Preview weitere SD-WANs hinzugefügt werden.

Der neue **Adoption Score** soll Ihnen dabei helfen, zu verstehen, wo Ihr Unternehmen auf dem Weg der digitalen Transformation steht. Er erfasst Metriken in zwei Kategorien: Erfahrungen der Mitarbeiter und Technologieerfahrung.

### 4.6: MICROSOFT 365 DESIRED STATE CONFIGURATION

PowerShell verfügt seit langem über eine Funktion namens Desired State Configuration (DSC) - Sie definieren, wie ein System (VM, Anwendung usw.) aussehen soll, wenden die Richtlinie an und der Local Configuration Manager sorgt dafür, dass das System die richtigen Einstellungen hat, wobei er regelmäßig auf Abweichungen überprüft.

Dies wird als „Infrastructure as Code" bezeichnet und ist **jetzt auch für M365 verfügbar**. So können Sie einen Test-Tenant haben, in dem Sie neue Konfigurationen und Einstellungen testen, die Sie dann exportieren und auf Ihren Produktions-Tenant anwenden können. Sie können damit auch alle Ihre Konfigurationen als "Backup" exportieren, regelmäßig Berichte über Konfigurationsänderungen erstellen und die Einstellungen Ihres Tenants mit bewährten Vorgehensweisen vergleichen.

# KAPITEL 5:

# CLIENTS

**ES GIBT ZAHLREICHE SOFTWARE, DIE SIE FÜR EINE VERBINDUNG ZU M365 VERWENDEN KÖNNEN - IN DIESEM KAPITEL WERDEN WIR UNS DIESE ANSEHEN UND ERLÄUTERN, WIE SIE SIE UNTER GOVERNANCE-GESICHTSPUNKTEN MANAGEN.**

## 5.1: DESKTOP-OPTIONEN

Microsoft empfiehlt die neueste Version von Chrome, Edge, Firefox oder Safari oder Internet Explorer 11 für den Zugriff auf M365.

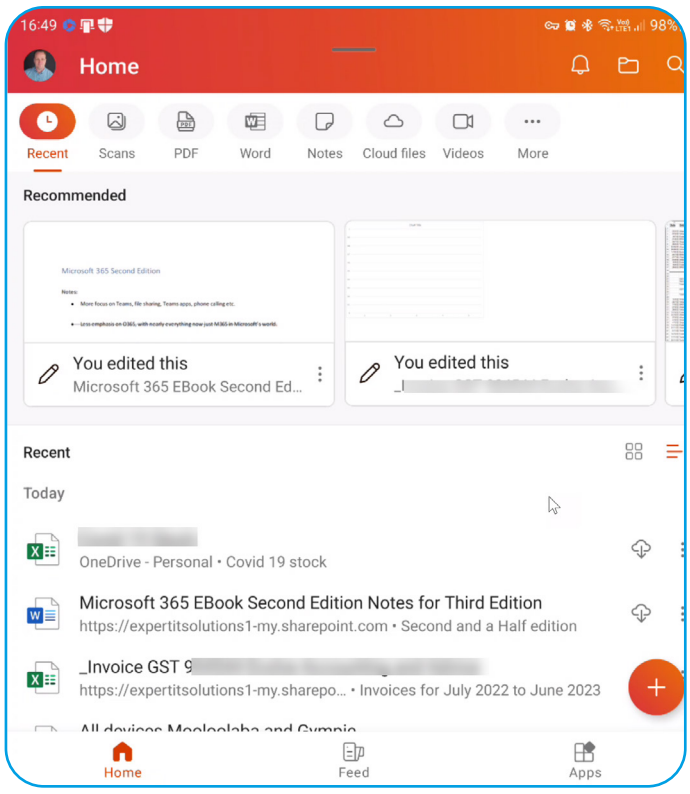
Wenn Sie den Office-Desktop-Client installiert haben, sollten alle unterstützten Versionen mit M365 funktionieren, aber es empfiehlt sich, die Apps for Enterprise-Version für Windows und Mac zu verwenden, die in Business Premium und E3+ enthalten ist. Sie können festlegen, **welche Benutzer den empfohlenen "Aktueller Kanal" erhalten** und wer den monatlichen oder die halbjährliche Variante des "Enterprise-Kanal" erhält. Wenn Sie ganz vorne mit dabei sein wollen, können Sie sich für das **Office Insider Programm** anmelden, um neue Funktionen zu testen.

Outlook Web App (OWA) oder Outlook für das Web verdient eine besondere Erwähnung, da es extrem leistungsfähig und keine "verwässerte" Version von Outlook ist, die in einem Browser läuft. Tatsächlich testet Microsoft neue Funktionen und Ansätze oft im Web-Client, weil so Änderungen viel schneller umgesetzt werden können. Mit **OWA-Richtlinien können Sie steuern**, welche Funktionen Ihren Benutzern zur Verfügung stehen.

Mit den **Client-Zugriffsregeln** können Sie steuern, welche Protokolle Benutzer verwenden können, um sich mit Exchange zu verbinden.

## 5.2: MOBIL-OPTIONEN

Viele Jahre lang war die bevorzugte Methode für die Online-Verbindung mit Exchange die Verwendung von ActiveSync, einem Protokoll, das sowohl der Mail-Client von iOS als auch von Android unterstützt (sozusagen - nicht alle Funktionen wurden von jedem Anbieter unterstützt). Microsoft empfiehlt jetzt die Verwendung der kostenlosen Outlook-Client-App, mit der Microsoft neue Funktionen viel schneller einführen kann, ohne darauf warten zu müssen, dass Apple oder Google nachziehen. Der Funktionsumfang dieser App ist stetig gewachsen, einschließlich der Möglichkeit, sich mit Gmail und anderen E-Mail-Diensten zu verbinden, und sie wird inzwischen von weit über 100 Millionen Menschen genutzt.




*M365 App (Office) auf einem Mobilgerät*

Früher gab es separate Word-, Excel- usw. Apps für Mobilgeräte, aber jetzt sind sie alle unter der Microsoft 365 (Office) App zusammengefasst, mit der Sie die verschiedenen Office-Dokumenttypen öffnen und auf dem Mobilgerät bearbeiten können. Die Installation ist kostenlos, aber die Funktionalität hängt davon ab, mit welchem Konto Sie sich bei der App anmelden.

## 5.3: ONEDRIVE FOR BUSINESS

Der Sync-Client wird automatisch auf Windows oder Mac OS installiert, wenn Apps for Enterprise installiert wird, und Sie können sein Verhalten mit dieser **Gruppenrichtlinien-Vorlage** steuern. Bitte schulen Sie Ihre Benutzer in der Verwendung von OneDrive for Business - die Möglichkeit, Ihre Dateien auf jedem beliebigen Gerät zur Verfügung zu haben, sollte nicht unterschätzt werden, insbesondere die Möglichkeit, sich auf jedem beliebigen Gerät (wenn Sie Ihre eigenen Geräte nicht zur Hand haben) bei **www.office.com** in einem beliebigen Browser anzumelden und dieselben Dateien zu bearbeiten.

## 5.4: TEAMS

Die Teams-Anwendung (Kapitel 11) ist Microsofts All-in-One-Collaboration-Client mit Unterstützung für Instant-Messaging-Chats, Gruppenchats, Sprachanrufe, Videoanrufe und, wenn Sie die entsprechende Lizenz haben, PSTN-Anrufe zu und von normalen Telefonen. Teams ersetzt Skype for Business und ab Anfang 2019 wird der Client automatisch installiert, wenn Sie Apps for Enterprise installieren.

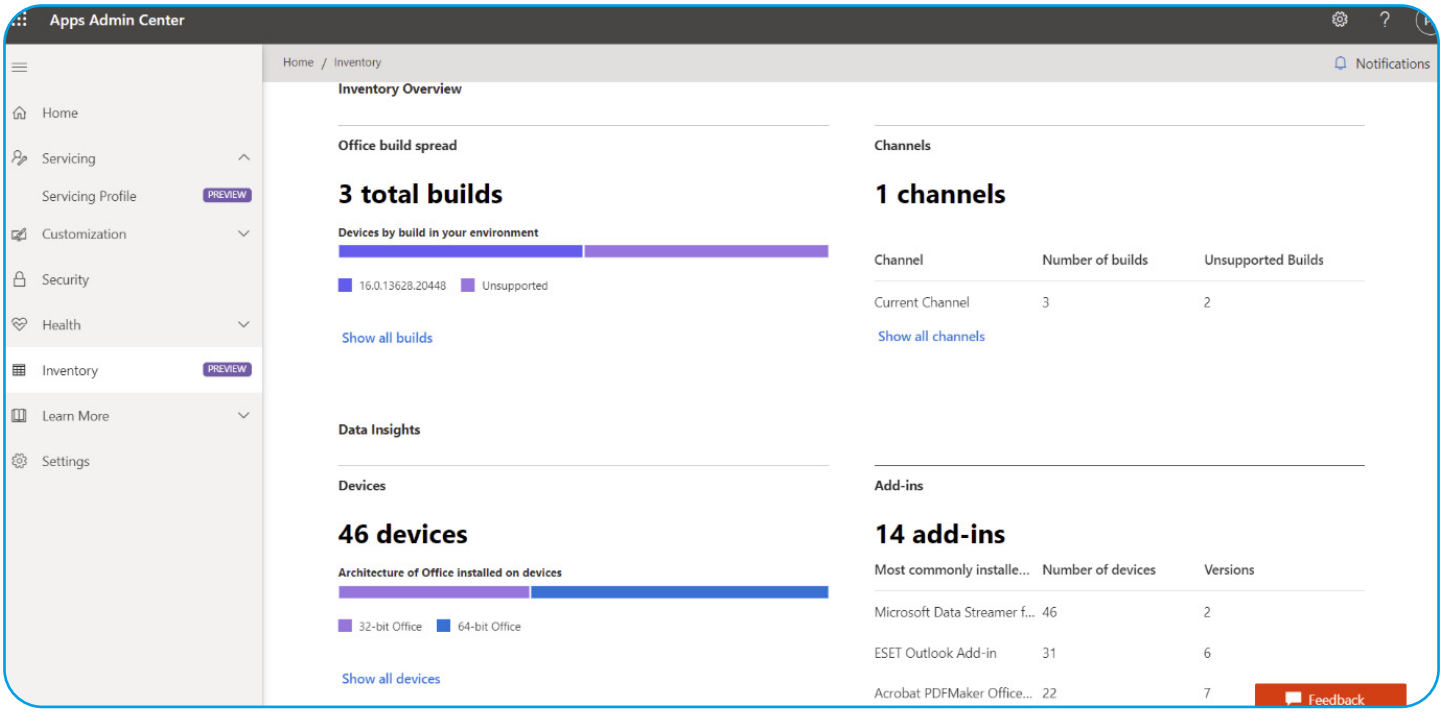
Wenn Sie ihn mit Ihrem bevorzugten Softwareverteilungswerkzeug bereitstellen müssen, verwenden Sie das **MSI**.

Zum jetzigen Zeitpunkt befindet sich eine neue Team's Client-App in der Public Preview, die die beiden größten Probleme mit dem aktuellen Client beheben soll: die Performance (der Client ist eine Electron-App und verbraucht viel CPU und Speicher) und das Swappen zwischen verschiedenen Tenants.

### 5.5: APPS ADMIN CENTER

Das **Microsoft 365 Apps Admin Center** ist eine sehr interessante Variante des Cloud-Managements für Apps for Enterprise (Office auf dem Windows-Desktop). Anstatt die Anpassungseinstellungen mit dem **Office-Bereitstellungstool** (ODT: Office Deployment Tool) zu verwalten, verwenden Sie das Cloud-Portal, um die erforderlichen XML-Dateien zu erstellen. Das Apps Admin Center kann jedoch noch viel mehr. Es inventarisiert Ihre Office-Installationen im gesamten Tenant, verfolgt, welche Versionen und Build-Nummern installiert sind, welche nicht mehr unterstützt werden und ermöglicht Ihnen die Erstellung von Wartungsprofilen für die Bereitstellung neuerer Office-Versionen. Mit Security Policy Advisor können Sie außerdem die aktuelle Nutzung der Apps analysieren und Richtlinienkonfigurationen für alle Apps for Enterprise-Installationen erstellen und bereitstellen (ohne auf GPOs oder MDM zurückgreifen zu müssen) und verfolgen, welche Add-Ins auf allen Ihren Geräten verwendet werden.

Wenn Sie eine große Anzahl von Benutzern haben, sollten Sie die Option zum Herunterladen von Apps for enterprise von **www.office.com** (M365 Portal - Einstellungen - Dienste & Add-Ins - Einstellungen für das Herunterladen von Office-Software) deaktivieren und stattdessen Ihre bevorzugte Methode für die Bereitstellung verwenden.




*Apps Admin Center*



Wenn Ihr Unternehmen den System Center Configuration Manager verwendet, können Sie **Apps for Enterprise damit bereitstellen und aktualisieren**.

Da für das Apps Admin Center keine zusätzliche Lizenzierung erforderlich ist, sollten Sie prüfen, ob es Ihnen das Leben als Office 365-Administrator erleichtern kann.

Wenn Sie Ihren Benutzern eine moderne Druckumgebung zur Verfügung stellen möchten, ohne sich mit Druckservern oder der Installation von individuellen Treibern für jeden Drucker auf jedem Gerät herumschlagen zu müssen, sollten Sie **Universal Print** in Betracht ziehen.

Eine weitere Möglichkeit, die Integration der verschiedenen Komponenten von M365 zu verdeutlichen, ist **Microsoft Search**. Damit können Sie an verschiedenen Stellen in M365 suchen und sich relevante Inhalte anzeigen lassen. Dabei werden Ihnen nur Inhalte angezeigt, auf die Sie von Ihrem Tenant aus Zugriff haben.

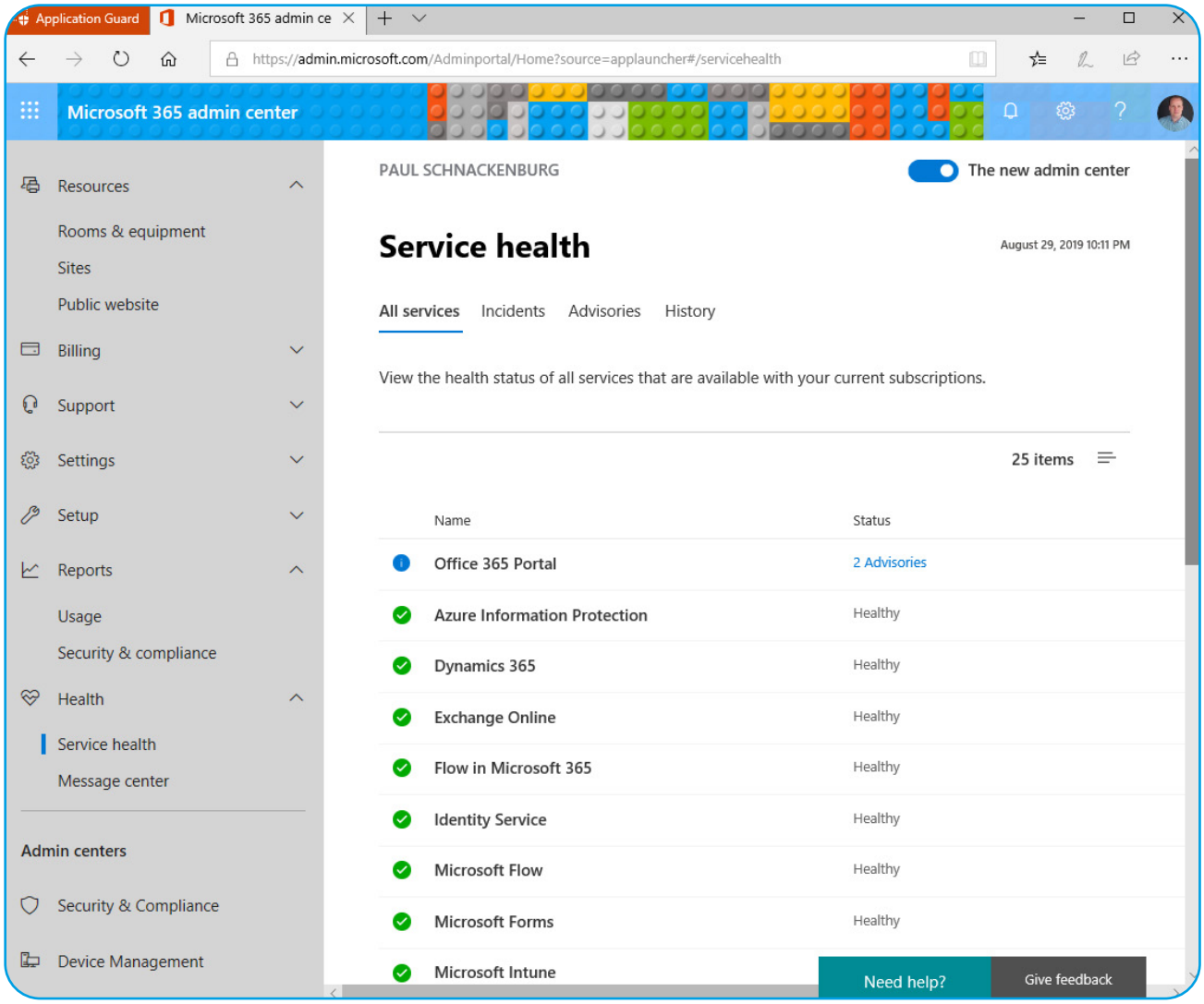
# KAPITEL 6:

# WINDOWS 11 ENTERPRISE

**DIE LETZTE SÄULE VON M365 IST WINDOWS 11 ENTERPRISE, FÜNF GERÄTE FÜR JEDEN LIZENZIERTEN BENUTZER, DIE AUTOMATISCH EIN UPGRADE VON WINDOWS 11 PRO AUF ENTERPRISE DURCHFÜHREN, SOBALD SICH EIN BENUTZER ANMELDET. IN DIESEM KAPITEL GEHEN WIR DARAUF EIN, WELCHE ZUSÄTZLICHEN SECURITY-FUNKTIONEN DIES FÜR IHR UNTERNEHMEN MIT SICH BRINGT.**

## 6.1: WINDOWS 11 ENTERPRISE

Enterprise fügt **Defender Application Guard** und **Defender Application Control** zusätzlich zu den Sicherheitsfunktionen von Windows 11 Pro hinzu. **Application Guard** schützt Ihre Benutzer beim Surfen auf potenziell bösartigen Sites mit Edge auf eine hardwareisolierte Weise. Diese Technologie wurde auch auf **Word, Excel und PowerPoint ausgeweitet**. **Application Control** hingegen baut auf früheren Versionen von AppLocker auf und blockiert die Ausführung nicht vertrauenswürdiger Anwendungen, einschließlich Plug-ins und Add-ins.




*Browsen in einem Application Guard-Fenster*

**Always On VPN** erfordert kein Windows 11 Enterprise und ist der Nachfolger von **DirectAccess**, wenn Sie in Ihrem Unternehmen weiterhin Client-VPN nutzen. Auch wenn es nicht exklusiv für Windows 11 Enterprise ist, sollten Sie sich **Windows Hello for Business** ansehen, um die Anmeldeerfahrung Ihrer Benutzer und Ihre Security zu verbessern (ein seltener Fall, bei dem jeder in Sachen Security gewinnt), indem Sie sich von Passwörtern lösen.

Wenn Sie eine große Anzahl von Windows 11-Geräten bereitstellen und den Aufwand für die Löschung jedes neuen Geräts und die Installation Ihres benutzerdefinierten Images reduzieren möchten, sollten Sie **Windows Autopilot in Betracht ziehen**. Es ist eine leistungsstarke Möglichkeit, Windows 11 "bereitzustellen", indem Sie einfach das von Ihrem OEM gelieferte vorinstallierte Image transformieren.

Teil 2

# VERWALTUNG, WARTUNG UND SUPPORT FÜR MICROSOFT 365

**Hier werden wir uns fortgeschrittene M365-Funktionen und -Konfigurationen ansehen, wie z.B. Entra zur Sicherung Ihrer Benutzer- und Workload-Identitäten, die Verwaltung von Exchange und SharePoint Online, Teams und die zentrale Konfiguration aller Ihrer Geräte mit Intune.**

# KAPITEL 7 :

# ENTRA ID

**HINTER M365 VERBIRGT SICH EIN VERZEICHNIS, DAS BENUTZERKONTEN, GRUPPEN UND ANDERE SECURITY-OBJEKTE ENTHÄLT. VIELE JAHRE LANG WAR DIESES VERZEICHNIS ALS AZURE ACTIVE DIRECTORY BEKANNT, OBWOHL ES NUR SEHR WENIG MIT DEM ON-PREMISE ACTIVE DIRECTORY GEMEIN HATTE. AZURE AD WURDE IM JULI 2023 IN ENTRA ID UMBENANNT. IN DIESEM KAPITEL SEHEN WIR UNS ENTRA ID AN UND WIE SIE DAMIT FÜR M365 INTERAGIEREN.**

## 7.1: ENTRA, PRIVA AND PURVIEW

Bevor wir uns mit Entra ID befassen, werfen wir einen Blick auf das neue Portal, auf das Sie zugreifen werden: **entra.microsoft.com**. Alle identitätsbezogenen Services sind hier untergebracht, während alle Funktionen im Zusammenhang mit Information Governance unter **compliance.microsoft.com** zu finden sind, dem sogenannten Purview-Portal (Kapitel 14), und es gibt einen Abschnitt mit allen datenschutzbezogenen Funktionen namens Priva.

Neben Entra ID enthält das Entra-Portal auch **Entra Permissions Management**, das administrative Berechtigungen in Azure, AWS und GCP (IaaS und PaaS) inventarisiert und entsprechend zuteilt - unabhängig von Microsoft 365-Berechtigungen. Außerdem gibt es Verified ID, das in Zukunft bei Neueinstellungen und der Verwaltung externer Identitäten helfen wird, sowie Global Secure Access - diese Funktionen liegen jedoch außerhalb des Umfangs dieses Buches.



## 7.2: BEGRÜSSEN SIE ENTRA ID & HYBRID IDENTITY

AD verwendet Kerberos und Group Policy, hat eine hierarchische Struktur und basiert auf LDAP, was alles nicht besonders Cloud-freundlich ist. Entra ID arbeitet über HTTPS, kann über eine REST-API angesprochen werden und unterstützt moderne Authentifizierungsprotokolle wie Security Assertion Markup Language (SAML), WS-Federation und OpenID Connect für die Authentifizierung und OAuth für die Autorisierung. Es unterstützt auch Federation, so dass Sie es mit anderen Authentifizierungssystemen verbinden können.

In Entra ID werden drei Arten von Authentifizierungen unterstützt: **Cloud-basiert, Verzeichnis-Synchronisierung** und **Single Sign On (SSO) mit AD FS**. Die erste Variante eignet sich, wenn Sie kein AD on-premises haben (oder es abschaffen wollen) und Sie nur Konten in der Cloud erstellen. Sie ist definitiv am einfachsten zu konfigurieren. Bei den beiden anderen müssen Sie Ihr on-premises AD über das kostenlose **AAD Connect-Tool** mit Ihrem Entra ID Tenant verknüpfen.

## 7.3: AAD CONNECT – DIE NABELSCHNUR

AAD Connect (wird vermutlich in Entra ID Connect umbenannt) hatte im Laufe der Jahre mehrere Vorgänger mit unterschiedlichen Namen - wenn Sie eine Installation von DirSync oder AAD Sync vorfinden, sollten Sie ein Upgrade auf AAD Connect durchführen, da diese Tools nicht mehr unterstützt werden. AAD Connect **unterstützt die Verbindung mehrerer on-premises Verzeichnisse mit AAD**. Es gab auch eine Version 1 Generation von AAD Connect, die veraltet ist. Sie sollten die Version 2 verwenden, die sich automatisch aktualisiert.

Sie können das Tool direkt auf einem DC oder auf einem Member Server installieren. Es gibt keine echte Aktiv/Aktiv-HA-Option, aber Sie können eine zweite Installation von **AAD Connect** auf einem separaten Server im **Staging-Modus** einrichten und ein manuelles Failover durchführen, wenn der primäre Server für einige Zeit offline sein sollte.

AAD Connect synchronisiert Benutzer- und Gruppenkonten in den von Ihnen ausgewählten OUs (oder das gesamte Verzeichnis - nicht empfohlen) mit Entra ID. Anschließend weisen Sie diesen Benutzerkonten Lizenzen zu, und sie können anfangen, die Cloud Services zu nutzen. Beachten Sie, dass dies auch bedeutet, dass On-premises immer der Ort ist, an dem Sie neue Konten erstellen und bestehende Konten aktualisieren, deaktivieren oder löschen können.

Es gibt **einige Möglichkeiten**, wie Sie Passwörter in AD verwalten können. Die einfachste ist die **Kennwort-Hash-Synchronisierung**, die on-premises Kennwort-Hashes nimmt, sie mit einem modernen Algorithmus erneut hasht und den Hash des Hashes in der Cloud speichert. Dadurch erhalten Ihre Benutzer SSO (auch wenn es sich technisch gesehen um " dieselben Anmeldedaten " handelt, da sich die beiden Benutzerkonten in zwei verschiedenen Verzeichnissen befinden). Ein weiterer Vorteil dieser Methode ist, dass Microsoft Sie warnen kann, wenn es im Internet / Dark Web Anmeldedaten mit Konten Ihres Tenants findet, bei denen die Passwörter übereinstimmen.

Wenn Sie darauf bestehen, dass die Passwörter Ihrer Benutzer nicht in der Cloud gespeichert werden dürfen (**nicht einmal als Hash eines Hashs**), ist die **Pass-Through-Authentifizierung (PTA)** eine weitere Option.



Sie **richten Agenten** auf mehreren (mindestens 3, maximal 40) Windows Server 2012 R2+ Servern ein (keine eingehenden Ports erforderlich), und wenn sich ein Benutzer z.B. auf **www.office.com** anmeldet, überprüft Entra ID, ob das richtige Passwort eingegeben wurde, indem es über die PTA-Agenten mit Ihrem on-premises AD kommuniziert.

Sowohl mit PTA als auch mit der Passwort-Hash-Synchronisierung können Sie optional **Seamless Single Sign On** (Seamless SSO) aktivieren, bei dem sich der Benutzer bei AD anmeldet und beim Zugriff auf **www.office.com** automatisch eingeloggt wird.

Eine Ergänzung ist **AAD Connect Cloud Sync,** das über die Cloud konfiguriert wird und nur auf schlanke Agenten on-premises angewiesen ist. Das bedeutet auch, dass Sie über eine integrierte Hochverfügbarkeit verfügen, sofern Sie mehrere Agenten einsetzen. Cloud Sync gewinnt langsam an **Funktionsgleichheit** mit AAD Connect. Die wichtigsten Funktionen, die heute noch fehlen, sind die Unterstützung von Geräte-Objekten, die Möglichkeit der Synchronisierung von Non-AD-LDAP-Verzeichnissen, PTA-Unterstützung, einige Filteroptionen und große Gruppen mit über 250.000 Mitgliedern. Das Hindernis für viele wird jedoch sein, dass es keine Unterstützung für Exchange Hybrid Writeback gibt. Ich erwarte, dass Cloud Sync irgendwann AAD Connect ersetzen wird.

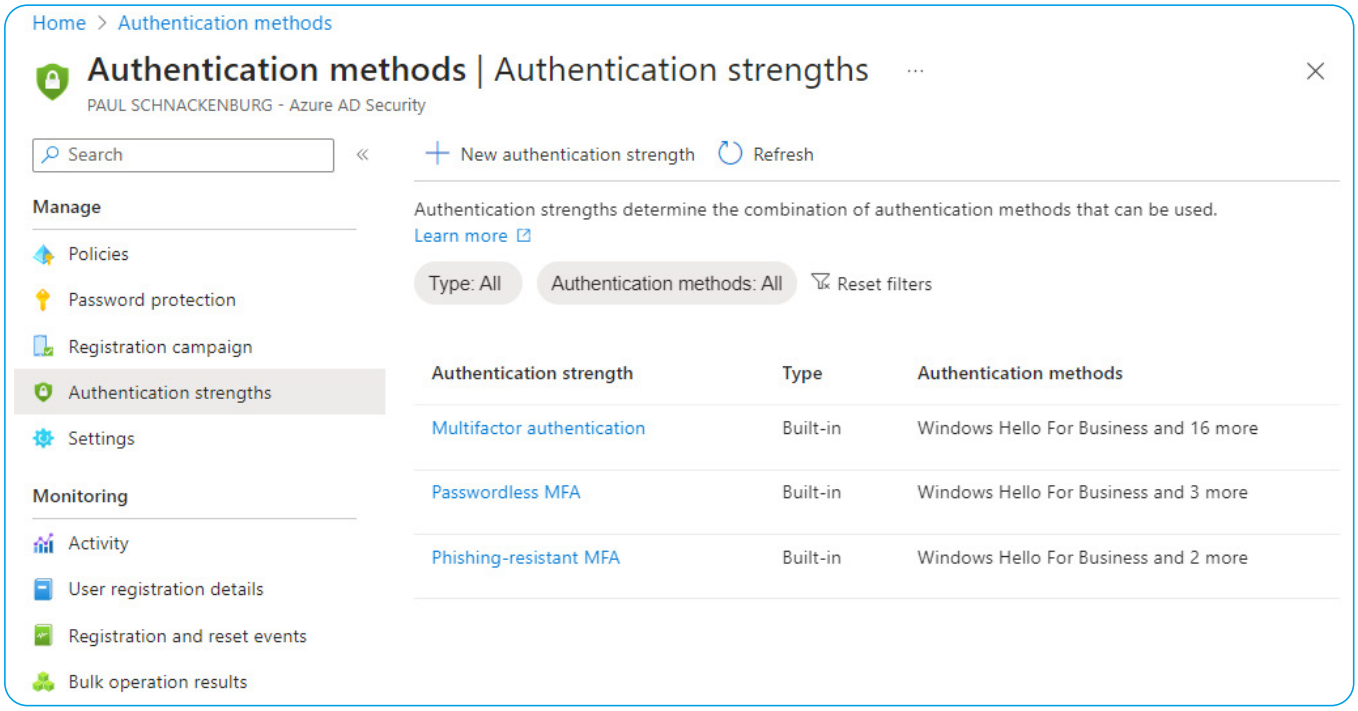
Die traditionelle Methode, Kennwort-Hashes nicht in der Cloud zu speichern, ist die Verwendung von **AD Federation Services (ADFS)**. Dies ist **wesentlich komplexer und erfordert die Einrichtung mehrerer Server** on-premises (oder als VMs in Azure), bietet aber mehr Flexibilität. Wenn Ihr Unternehmen AD FS bereits für andere Zwecke eingesetzt hat, ist die Einrichtung der Federation mit O365 kein großes Projekt, aber meine Empfehlung (und die von Microsoft) ist, bei PTA oder Passwort-Hash-Sync zu bleiben. In Anbetracht des Einbruchs in die Lieferketten von Solarwinds und des anschließenden Eindringens in verschiedene Organisationen, die ADFS verwenden, sowie der Empfehlung von Microsoft in den letzten Jahren, von ADFS zu Azure AD zu migrieren, **ist es an der Zeit**, auf Azure AD umzusteigen, wenn Sie ADFS im Einsatz haben.

## 7.4: AZURE MFA

Eines der besten Dinge, die Entra ID ermöglicht, ist die einfache Einrichtung der Multi-Faktor-Authentifizierung (MFA) für Benutzer. Kennwörter sind eines der schwächsten Glieder in der heutigen IT-Landschaft, und die meisten Sicherheitsverletzungen, die wir beobachten, sind darauf zurückzuführen, dass die Anmeldedaten einer Person kompromittiert wurden. Eine Lösung für dieses Problem ist die Verwendung von MFA (manchmal auch als 2FA oder zweistufige Authentifizierung bekannt), bei der für die Authentifizierung nicht nur ein Benutzername und ein Passwort, sondern auch ein Gerät oder eine biometrische Geste erforderlich sind. Dadurch wird der Erfolg von Angriffen auf Zugangsdaten drastisch reduziert (**laut Microsoft um 99%**).

MFA kann ein Telefon anrufen, eine SMS mit einem Code senden oder eine Benachrichtigung senden bzw. einen Code von der kostenlosen **Microsoft Authenticator-App** anfordern. Wenn es nicht unbedingt erforderlich ist, sollten Sie keine Anrufe oder SMS verwenden, da diese unsicherer sind als die App-Optionen.

Grundsätzlich gilt: Alle Ihre privilegierten Konten (Global / Exchange / SharePoint / Compliance-Administratoren usw.) MÜSSEN MFA verwenden. **Dies ist auf allen Ebenen von O365 kostenlos** und lässt sich **einfach einrichten**.




*Stärken der MFA-Authentifizierung*

Die Benutzererfahrung ist relativ nahtlos, wenn Sie die App auf Ihrem Smartphone installieren. Wenn Sie ein IT-Entscheidungsträger sind, müssen Sie damit rechnen, dass Ihre Administratoren diesen Punkt ablehnen, aber um eine akzeptable IT-Sicherheit zu gewährleisten, ist dieser Schritt nicht verhandelbar - alle Administratoren MÜSSEN MFA verwenden. Nebenbei bemerkt verwende ich Azure MFA für meinen eigenen geschäftlichen Tenant und alle Tenants meiner Kunden, die ich seit vielen Jahren verwalte, ohne Probleme.

Sie müssen jedoch auch für Zeiten planen, **in denen Azure MFA nicht verfügbar ist**. Dazu gehört die Einrichtung eines (vorzugsweise zwei) Global Admin Cloud-Konten, die von MFA und allen CA-Richtlinien ausgenommen sind. Diese Konten sollten mit sehr langen und komplexen Passwörtern versehen sein, die nur hochrangigen Administratoren zur Verfügung stehen, und sie sollten überwacht werden, so dass im Falle ihrer Verwendung ein Alarm ausgelöst wird. Diese Konten für den Notfall sollten nur verwendet werden, um den Benutzerzugang wiederherzustellen. Wenn z.B. Entra ID MFA ausgefallen ist, können Sie die MFA-Anforderungen für die Dauer des Ausfalls deaktivieren, damit sich die Benutzer anmelden und produktiv arbeiten können.

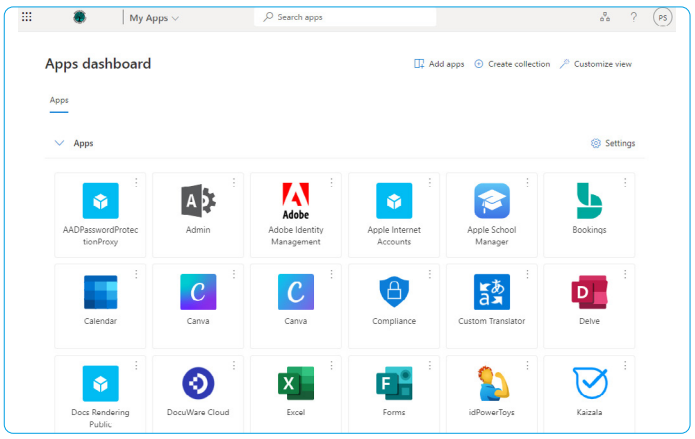
Die Aktivierung von MFA für Ihre Endbenutzer erfordert eine gewisse Planung und Schulung der Benutzer. Wie Sie MFA implementieren, hängt davon ab, wie gut Ihre Benutzer mit der Technik vertraut sind und ob sie normalerweise von einem Firmensitz aus arbeiten. Administratoren erhalten MFA immer kostenlos, bei den Business SKUs ist MFA bereits integriert, aber in beiden Fällen fehlen die erweiterten Funktionen, die Entra ID Premium P1 (M365 E3) oder Entra ID Premium P2 (M365 E5) bieten.

Dazu gehören die einmalige Umgehung, vertrauenswürdige IPs/**benannte Standorte**, mit denen Sie IP-Adressbereiche des Firmensitzes definieren können, in denen Benutzer nicht zur MFA aufgefordert werden. Beachten Sie, dass alle MFA-Stufen es Ihnen ermöglichen (wenn Sie diese Funktion zulassen), MFA auf einem vertrauenswürdigen Gerät für eine bestimmte Anzahl von Tagen (7-60) zu speichern. Wenn sich ein Benutzer an einem Gerät angemeldet und MFA erfolgreich durchgeführt hat, wird er für diesen Zeitraum nicht mehr auf dem Gerät gefragt und wenn das Gerät verloren geht oder gestohlen wird, können entweder der Benutzer oder Sie das Vertrauen in diese Geräte einfach „aufheben". Ab Mai 2023 hat Microsoft den Nummernabgleich für alle Microsoft Authenticator-Genehmigungen aktiviert. Anstatt also einfach auf Genehmigen oder Ablehnen zu drücken, müssen Sie einen zweistelligen Code eingeben, der auf Ihrem Computerbildschirm angezeigt wird. Die App zeigt Ihnen auch den geografischen Standort an, von dem die MFA-Anfrage kommt. Beide Funktionen wurden entwickelt, um MFA-Ermüdungsangriffe zu bekämpfen, bei denen der Angreifer wiederholt versucht, sich anzumelden und dabei so viele Anfragen auf Ihrem Telefon generiert, dass manche Benutzer am Ende einfach auf Genehmigen drücken, damit es aufhört.

Microsoft aktiviert jetzt **Sicherheitsstandards** für alle neuen Tenants, und Sie können sie für Ihre bestehenden Tenants **manuell aktivieren**. Dies erzwingt MFA für alle Benutzer und Administratoren, wobei nur die Microsoft Authenticator-App verwendet und ältere Authentifizierungsverfahren blockiert werden (siehe Kapitel 15) sowie der Zugriff auf das Azure AD-Portal kontrolliert wird. Während diese Sicherheitsmaßnahmen ein guter Ausgangspunkt für ein kleines Unternehmen mit begrenzten Anforderungen sind, rate ich bei komplexeren Organisationen zur Vorsicht, da es keine Möglichkeit gibt, Notfall-User (so genannte „Break Glass Accounts") oder Service-Konten von MFA auszuschließen oder mit Benutzern umzugehen, die nicht über die Authenticator-App auf einem Telefon verfügen bzw. nicht darauf zugreifen können.

## 7.5: PUBLISHING APPLICATIONS

Eine der leistungsstärksten Funktionen von Entra ID ist die Möglichkeit, Anwendungen (von Drittanbietern und **on-premises**) für Ihre Benutzer **zu veröffentlichen**. Diese werden direkt neben den normalen Office-Anwendungen unter **myapplications.microsoft.com** oder **www.office.com** angezeigt und können von den Benutzern mit inem einzigen Klick gestartet werden.




*MyApps portal*

Nehmen Sie zum Beispiel das Twitter-Konto Ihres Unternehmens, bei dem mehrere Benutzer den Benutzernamen und das Kennwort haben, um Tweets im Namen des Unternehmens zu versenden. Sie müssen nicht nur das Kennwort zurücksetzen, sobald jemand das Unternehmen verlässt (Sie möchten schließlich nicht, dass er weiterhin im Namen Ihres Unternehmens twittert, nachdem



er das Unternehmen verlassen hat), sondern Sie haben auch kaum Kontrolle darüber, wem das Kennwort sonst noch mitgeteilt wird. Wenn Sie Twitter über Entra ID veröffentlichen und eine AD-Gruppe erstellen, in die Benutzer aufgenommen werden, die Zugriff haben sollen, fügen Sie einfach ein Benutzerkonto zu dieser Gruppe hinzu. Der Benutzer hat dann automatisch Single-Sign-On-Zugriff auf Twitter im My Apps-Portal, ohne jemals das Passwort zu kennen. Für einige der mehr als 2400 Anwendungen, die standardmäßig unterstützt werden, können Sie sogar eine **automatische Bereitstellung** konfigurieren, so dass beim Hinzufügen eines Benutzers zur AD Salesforce-Gruppe automatisch ein Konto für ihn in Salesforce erstellt wird - wiederum ohne dass er das Kennwort dafür kennt.

Eine beliebte Option ist die Verwendung der AWS Single Sign-On App zur **Integration von AAD und AWS.**

### 7.6: PREMIUM-FUNKTIONEN

Entra ID Premium P1 schaltet nicht nur mehr MFA-Funktionen frei, sondern ermöglicht es Ihnen auch, häufig verwendete Passwörter in Ihrem on-premises AD **zu sperren** (einschließlich einer **benutzerdefinierten Wortliste**), Benutzern die Möglichkeit zu geben, **ihre eigenen Passwörter zurückzusetzen**, wenn sie sie vergessen haben, **MFA mit bedingtem Zugriff** zu integrieren und Benutzern gleichzeitig die Möglichkeit zu geben, sich sowohl für MFA als auch für das **Zurücksetzen von Passwörtern per Self-Service** (SSPR) zu registrieren.

Der P2-Level bietet den vollen Funktionsumfang von Entra Identity Protection, bei dem Sie **Berichte erhalten, und Authentifizierungen** auf der Grundlage der Risikostufe des Benutzerkontos und der Anmeldung blockieren oder sogar eine **"zusätzliche" MFA-Aufforderung** auf der Grundlage des Risikoprofils des Authentifizierungsversuchs auslösen können. P2 bietet auch **Privileged Identity Management (PIM)**, bei dem Sie alle administrativen Konten in berechtigte Konten umwandeln und die Benutzer eine Erhöhung beantragen müssen, wenn sie administrative Aufgaben durchführen müssen (bekannt als "Just in Time Administration").

Anstatt einzelnen Benutzer-Konten in Entra ID administrative Rollen zuzuweisen, können Sie jetzt **Gruppen verwenden, um Admin-Zugriff zu gewähren**. Die Gruppen müssen ein bestimmtes Attribut (isAssignableToRole) haben, das auf true gesetzt ist, und eine statische Mitgliedschaft im Benutzerkonto (keine dynamische - automatische Zuweisung von Benutzerkonten zu einer Gruppe auf der Grundlage eines Attributs wie "Abteilung" im Verzeichnis).

Während AD eine hierarchische Struktur hat, die sich auf Organisationseinheiten (Organizational Units, kurz: OUs) stützt, um Ihre Benutzer-, Rechner- und Gruppenkonten auf der Grundlage von Abteilungen, Geografie oder anderen Ansätzen zu strukturieren, hat Entra ID eine flache Struktur. **Mit Hilfe von Verwaltungseinheiten** (Administrative Units, kurz: AUs) können Sie Benutzer- und Gruppenkonten strukturieren und dann **administrative Berechtigungen an eine oder mehrere AUs delegieren.** Die AU-Administratoren benötigen eine Entra ID Premium-Lizenz. Beachten Sie, dass im Gegensatz zu OUs, bei denen ein Konto nur in einer einzigen OU sein kann, ein Gruppen- oder Benutzerkonto Mitglied mehrerer AUs (bis zu 30) sein kann.

Wenn Sie über eine große Umgebung und Premium P2-Lizenzen verfügen, sollten Sie die **Berechtigungsverwaltung** (engl. Entitlement Management) in Betracht ziehen, mit der Sie den Zugriff auf Anwendungen und Sites sowie Gruppenmitgliedschaften (einschließlich Teams) in einem einzigen Zugriffspaket zusammenfassen können. Diese sind für interne Benutzer nützlich ("Sie sind ein neuer Mitarbeiter im Marketing - hier ist Ihr Paket, mit dem Sie alle benötigten Zugriffsrechte erhalten") und können auch für die Vergabe von Zugriffsrechten an externe Benutzer verwendet werden. Für Partnerorganisationen, mit denen Sie häufig zusammenarbeiten, können Sie es sogar so einrichten, dass deren Benutzer Pakete im Self-Service-Modus beantragen können. Die Berechtigungsverwaltung kann auch die IT-Abteilung aus der Rolle der Rechtevergabe herausnehmen, indem sie die Zuweisung von Paketen an Benutzer im Unternehmen delegiert.

## 7.7: RICHTLINIEN FÜR DEN BEDINGTEN ZUGRIFF

Sowohl P1 als auch P2 schalten eine weitere leistungsstarke Funktion in Entra ID frei: **Bedingter Zugriff** (Conditional Access, kurz: CA). Damit können Sie Richtlinien für den Anwendungszugriff (sowohl für Cloud- als auch für On-Premises-Anwendungen) auf der Grundlage des Benutzerkontos und der Gruppen, in denen der Benutzer Mitglied ist, der Anwendung, auf die er zugreift, dem Zustand seines Endgeräts, seinem Standort, dem Anmeldungsrisiko und der Art der Client-Anwendung, von der aus er zugreift, erstellen. Diese "wenn dies - dann das"-Regeln erhöhen die Sicherheit Ihrer Daten erheblich, indem die Risikofaktoren, die die Identität und den Zugriff in M365 beeinflussen, gemanagt werden.

Um die Einrichtung guter CA-Richtlinien noch einfacher zu machen, gibt es **Vorlagen** (zum Zeitpunkt der Erstellung dieses eBooks noch in der Preview), die die Themen Sichere Grundlage (engl. Secure Foundation), Zero Trust, Remote-Arbeit, Schutz der Administratoren und Neu auftretende Bedrohungen abdecken.

Um sicherzustellen, dass Sie nicht aus Versehen eine Richtlinie erstellen, die den CEO fünf Minuten vor seiner Vorstandspräsentation aussperrt, können Sie mit der Option, CA-Richtlinien im **reinen Berichtsmodus** einzusetzen, die Auswirkungen der Richtlinien bewerten, ohne sie tatsächlich durchzusetzen.

Es gibt eine **API für den Zugriff auf CA-Richtlinien**. Damit können Sie (z.B. mit PowerShell) ein Backup Ihrer CA-Richtlinien erstellen, sie wiederherstellen, Änderungen überwachen und sie als Code behandeln, anstatt sie manuell im Portal zu verwalten. Sie können die Richtlinien auch in einem Test-Tenant testen, bevor Sie sie von dort aus exportieren und in Ihren Produktions-Tenant importieren, nachdem sie die Überprüfung bestanden haben.

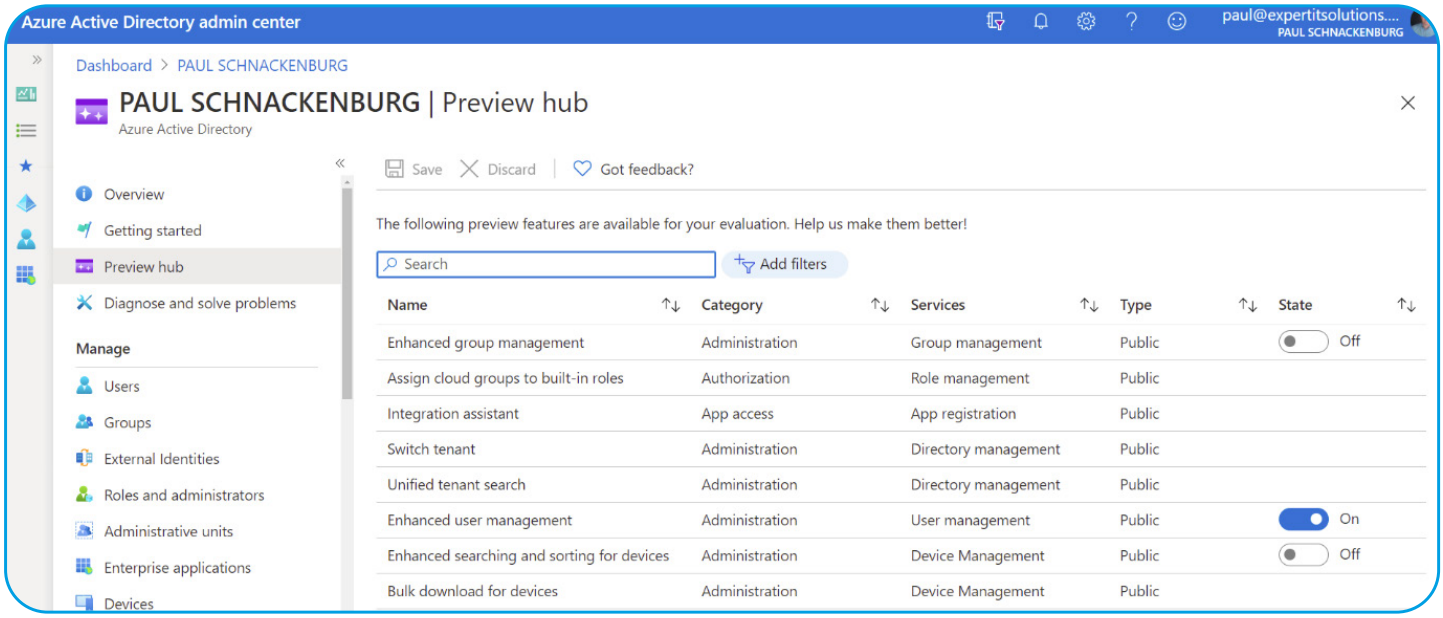
## 7.8: DEN LEBENSZYKLUS VON KONTEN MANAGEN

Sobald Sie AAD Connect implementiert haben, sollten Sie Ihre Prozessdokumentation aktualisieren, um den gesamten Lebenszyklus von Benutzerkonten zu berücksichtigen, z. B. um sicherzustellen, dass sie die richtigen Lizenzen erhalten, den richtigen Gruppen hinzugefügt werden und dass bei der Deaktivierung des Kontos die **richtigen Schritte** befolgt werden.

Um sicherzustellen, dass Benutzer (und Gäste) keine Zugriffsrechte ansammeln, die sie nicht mehr benötigen, verwenden Sie die **Zugriffsüberprüfung** (Premium P2), mit der Sie jetzt **alle Gastkonten in einem Arbeitsgang überprüfen können**, statt auf Basis der einzelnen Teams/M365 Gruppen.

Bei einem kleineren O365- oder M365-Tenant ist es wahrscheinlich, dass Sie das vollständige Azure AD-Portal gar nicht benötigen und stattdessen Ihre Benutzer nur im M365-Portal verwalten (Kapitel 2). Es ist jedoch eine gute Idee, das "vollständige" Entra-Portal unter **https://entra.microsoft.com** zu erkunden.

Wenn Sie die neuen Funktionen von Entra ID ausprobieren möchten, nutzen Sie den Preview Hub, um sich über die Public Preview-Funktionen zu informieren und diese zu aktivieren.




*Azure AD Preview hub*

# KAPITEL 8:

# EXCHANGE ONLINE

**E-MAIL IST DIE LEBENSADER DER GESCHÄFTLICHEN KOMMUNIKATION, SELBST IM ZEITALTER VON TEAMS UND SLACK UND ZAHLREICHEN ANDEREN KOMMUNIKATIONSTOOLS. E-MAIL IST DER KLEINSTE GEMEINSAME NENNER - DAS EINZIGE TOOL, MIT DEM SIE IMMER JEMANDEN ERREICHEN KÖNNEN, WENN SIE SEINE E-MAIL-ADRESSE HABEN. UND E-MAIL IST EINE COMMODITY - JEDES UNTERNEHMEN BRAUCHT SIE, ABER KEIN UNTERNEHMEN WIRD WETTBEWERBSFÄHIGER SEIN, WENN ES SIE "EFFIZIENTER" EINSETZT ALS EIN ANDERES.**

## 8.1: WIR LEBEN IN EINER HYBRIDEN WELT

Eine der Stärken von M365 gegenüber Google Workplace ist zum Beispiel der klare Migrationspfad von dem, was Sie heute haben, in die Cloud, da Microsoft über eine große Präsenz in den Rechenzentren von Unternehmen auf der ganzen Welt verfügt.

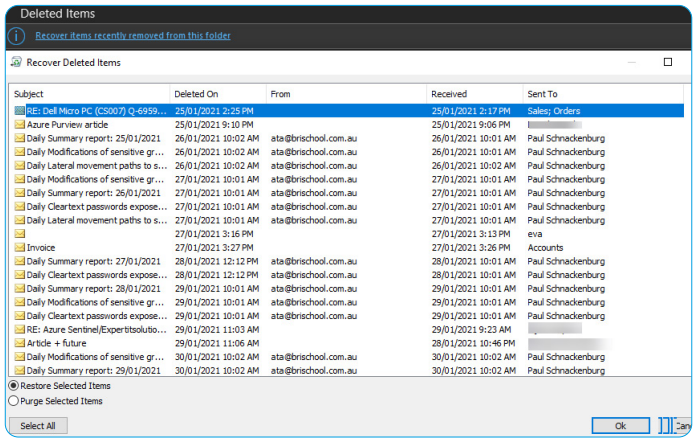
Wenn Sie Exchange 2013+ on-premises haben, können Sie eine der Migrationsmethoden wählen, die wir uns in Kapitel 3 angesehen haben, von denen einige eine hybride Koexistenz ermöglichen. Bei der vollständig hybriden Option können Sie Ihre on-premises Infrastruktur so lange weiter betreiben, wie Sie möchten, und Postfächer nach Ihrem eigenen Zeitplan stapelweise in die Cloud verschieben. Sie können sogar Postfächer zurück nach on-premises verlagern, wenn dies erforderlich ist. Wie zu erwarten, gibt es bei einem **hybriden Setup** viele Details zu verwalten, darunter **Voraussetzungen**, **ActiveSync-Konnektivität** und **Postfachberechtigungen** - insbesondere wenn ein Benutzer on-premises über Berechtigungen für ein Postfach in der Cloud verfügt oder umgekehrt.

Wenn Sie nur einen einfachen Weg suchen, um Postfächer von Exchange zu Exchange Online zu verschieben - dann hat Hornetsecurity ein hervorragendes **Mailbox Migration Tool**.

## 8.2: BACKUP UND NATIVER DATENSCHUTZ

Eine Sache, die Sie bei O365 wissen sollten, ist, dass Microsoft sicherstellt, dass Sie Ihre Postfachdaten nicht verlieren. Dies geschieht durch den nativen Datenschutz in Exchange, indem drei Kopien Ihrer Postfachdaten auf separaten Servern aufbewahrt werden, zusammen mit einer "verzögerten Kopie" (zeitlich verzögert, für Fälle, in denen die Daten beschädigt sind und nicht verloren gehen) auf einem vierten Server.

Sie bewahren jedoch KEINE Backup-Kopien Ihrer Daten auf, die bis in die Vergangenheit zurückreichen, was für Ihr Unternehmen je nach Ihren gesetzlichen Anforderungen ein Problem darstellen kann oder auch nicht. Es gibt mehrere Services von Drittanbietern auf dem Markt, die Backups Ihrer Exchange- und SharePoint-Online-Daten erstellen. **365 Total Backup** von Hornetsecurity ist eine hervorragende Backup-Lösung für Postfächer, Teams, OneDrive for Business, SharePoint und Dateien auf Endgeräten (**siehe Kapitel 16**).




*Gelöschte Elemente in Outlook wiederherstellen*

Ein gelöschtes Benutzerkonto und Postfach **kann wiederhergestellt werden**, wenn nicht länger als 30 Tage vergangen sind.

## 8.3: AUTODISCOVER

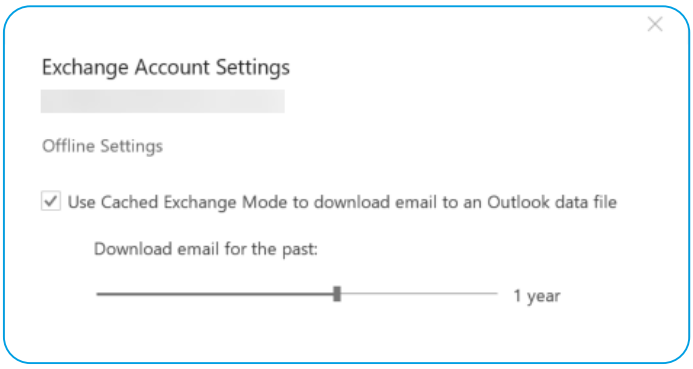
Unabhängig davon, ob sich Ihr Exchange-Server in der Cloud oder on-premises befindet, ist es wichtig, dass Client-Anwendungen ihn finden können - dafür sind die Autodiscover-Einträge im DNS zuständig. Es gibt noch eine Reihe weiterer DNS-Einträge, die für M365 erforderlich sind - Sie finden sie **in diesem Artikel.**

Wenn Sie eine hybride Exchange-Bereitstellung haben, müssen die Autodiscover-Einträge auf Ihren on-premises Exchange 2016/2019 Mailbox Server verweisen.

## 8.4: POSTFÄCHER VERWALTEN

Mit der Verwaltung von Postfächern sind viele Aufgaben verbunden, eine davon ist die **Verwaltung von Kontigent-Grenzwerten**. F3-Lizenzen erhalten 2-GB-Kontingente, E1 ist auf 50 GB (mit einem 50-GB-Archiv) festgelegt und E3+ haben 100-GB-Kontingente mit Archivpostfächern, die maximal 1,5 TB groß sein können. Der Unterschied zwischen einer Mailbox und einem Archiv-Postfach besteht darin, dass das Archiv nur verfügbar ist, wenn Sie online sind. Sie können mit einem Schieberegler in Outlook steuern, wie viele Postfachdaten auf jedem Gerät offline gespeichert werden.

Wenn Sie große Postfächer zu Office 365 migrieren, stellen Sie sicher, dass diese kleiner als 100 GB sind und kein Element größer als 150 MB ist, bevor Sie mit der Migration beginnen.




*Outlook offline cache setting*

In der Exchange-Konsole können Sie die Einstellungen für ein Postfach konfigurieren, z.B. E-Mail-Aliase hinzufügen, die Kontingentauslastung einsehen, steuern, welche Clients (OWA, Unified Messaging) und Protokolle (EAS, MAPI, IMAP und POP) ein Benutzer verwenden kann, sowie die Aufbewahrung von Nachrichten und die Delegation von Postfächern. Mit der letztgenannten Option können Sie Benutzer so konfigurieren, dass sie E-Mails im Namen eines anderen Benutzers senden, oder in seinem Auftrag senden, wobei der Empfänger dann sehen kann, dass die E-Mail im Namen des anderen Benutzers gesendet wird. Sie können anderen Benutzern auch den vollen Zugriff auf das Postfach eines bestimmten Benutzers einräumen.

## 8.5: POSTFACH-ARCHIVE

Wie bereits erwähnt, können Sie ein Archivpostfach für Postfachinhalte aktivieren, das im Wesentlichen als "bodenloser" Speicherbereich für ältere Inhalte dient und hoffentlich Benutzer davon abhält, PST-Dateien als Archivierungslösung zu adaptieren. Der mobile Outlook-Client (iOS und Android) kann nicht auf Archiv-Postfächer zugreifen. Sie können die **automatisch erweiterte Archivierung für E3- und E5-lizenzierte Benutzer** mit PowerShell aktivieren:

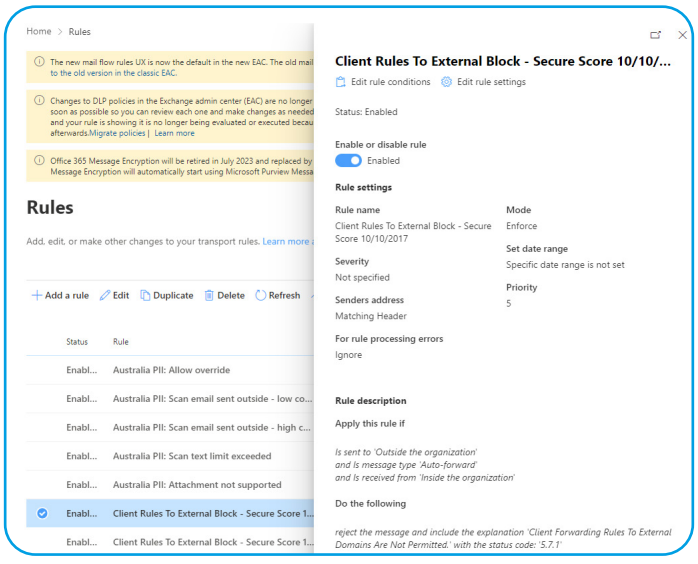
```
Set-OrganizationConfig -AutoExpandingArchive
```

Sie können Archivpostfächer auch pro Benutzer aktivieren. Beachten Sie, dass der Archivordner, der in einem Postfach erstellt wird, wenn Sie mit der rechten Maustaste auf ein Element klicken und Archiv wählen, nicht mit dem Archivpostfach verbunden ist.

## 8.6: E-MAIL-WEITERLEITUNGEN

Beachten Sie, dass Benutzer ihre Postfächer so einrichten können, dass sie E-Mails an eine externe E-Mail-Adresse weiterleiten (optional an beide Postfächer). Dies sollten Sie im Auge behalten, denn obwohl es legitime geschäftliche Gründe für die Weiterleitung von E-Mails geben kann, ist dies auch ein beliebter Angriffsvektor für Hacker, die E-Mails unbemerkt lesen und dann für verschiedene schändliche Zwecke nutzen.

Im Mail Flow Dashboard finden Sie einen Bericht, der Ihnen zeigt, welche Weiterleitungsregeln existieren. Sie können die **Weiterleitung von E-Mails durch Benutzer auch auf verschiedene Weise blockieren**.




*Mail Flow Regel zum Blockieren externer E-Mail-Weiterleitungen*



## 8.7: FREIGEGEBENE / GEMEINSAM GENUTZTE POSTFÄCHER

Es kommt vor, dass Sie ein Postfach haben möchten, das nicht einem bestimmten Benutzer "gehört", wie beispielsweise sales@ oder support@, wo mehrere Benutzer auf denselben Alias zugreifen. Solange das **Gemeinsame Postfach** kein größeres Kontingent als 50 GB umfasst oder ein Archiv-Postfach verwendet, wird keine Lizenz dafür benötigt. Dies ist auch eine Möglichkeit, um Mitarbeiter zu verwalten, die Ihr Unternehmen verlassen haben, deren E-Mails Sie aber weiterhin überwachen müssen. Durch die Umwandlung ihres Postfachs in ein gemeinsames Postfach und die Zuweisung des Zugriffs an den entsprechenden Mitarbeiter wird die Lizenz für einen neuen Benutzer frei. Stellen Sie aus Sicherheitsgründen sicher, dass die direkte Anmeldung bei gemeinsamen Postfächern blockiert ist - Benutzer sollten nur auf gemeinsame Postfächer zugreifen, indem sie diese als zusätzliches Postfach in Outlook hinzufügen.

## 8.8: E-MAIL-KONTAKTE UND BENUTZER

Sowohl **E-Mail-Kontakte** als auch **Benutzer** werden in Alle Kontakte, der Globalen Adressliste (GAL) und dem Offline-Adressbuch (OAB) angezeigt. Ein **Kontakt** ist ein Verweis auf eine E-Mail-Adresse in einem externen System, während ein **Benutzer** ebenfalls ein Verweis auf eine externe Adresse ist, aber der Benutzer verfügt über O365-Anmeldeinformationen, um auf SharePoint Online oder OneDrive for Business zugreifen zu können. Letzteres ist ein Überbleibsel von on-premises Exchange, moderne externe Freigaben wie Teams, Planner und andere nutzen **Azure Business to Business** (B2B) Zusammenarbeit für den Gastzugang.

## 8.9: VERTEILERGRUPPEN

Die Gruppierung von E-Mail-Adressen zur Erleichterung der Kommunikation mit Teams von Mitarbeitern ist etwas, was E-Mail-Systeme schon seit Jahrzehnten tun - im Exchange Online Admin Center (EAC) können Sie Verteilergruppen erstellen. Beachten Sie, dass die Standardeinstellung darin besteht, stattdessen eine **M365-Gruppe** zu erstellen, und Microsoft in der Tat darauf drängt, **Verteilergruppen durch Gruppen zu ersetzen**. **Dynamische Gruppen** erleichtern die Verwaltung der Mitgliedschaft, da sie auf einem Entra ID-Attribut wie z.B. "Abteilung" basieren. Wenn dieses Attribut z.B. auf Marketing eingestellt ist, wird der Benutzer automatisch in die richtige Gruppe aufgenommen.

# KAPITEL 9:

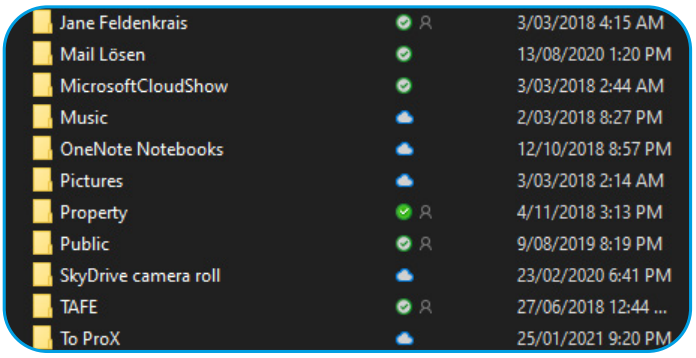
# ONEDRIVE FOR BUSINESS UND SHAREPOINT

**DIE GEMEINSAME NUTZUNG VON DATEIEN UND DIE BEREITSTELLUNG EINER INTRANET-PLATTFORM IST EIN ZENTRALER BESTANDTEIL VON M365. IN DIESEM KAPITEL BEFASSEN WIR UNS MIT ONEDRIVE FOR BUSINESS (OD4B) FÜR DIE PERSÖNLICHE SPEICHERUNG UND GEMEINSAME NUTZUNG VON DATEIEN SOWIE DIE WEBBASIERTE ZUSAMMENARBEIT IN SHAREPOINT.**

## 9.1: ONEDRIVE FOR BUSINESS

OD4B baut auf SharePoint Online auf und bietet jedem lizenzierten Benutzer einen eigenen Dokumentenspeicher; 1 TB für die meisten SKUs. Dieses Kontingent kann für bestimmte Lizenzen **auf 5 TB erhöht werden.**

Wie bereits erwähnt, können Sie, sobald Sie Dateien in OD4B gespeichert haben, von jedem Gerät aus darauf zugreifen, über Clients für Android, iOS, Windows, MacOS und eine Weboberfläche. Es gibt **einige Einschränkungen** bei Dateinamen, -typen und -größen, die Sie beachten sollten. Mit dem Sync-Client von OD4B können Sie **alle Dateien auf einem Gerät sehen**, die Sie synchronisiert haben. Sie können sich in einem **reinen Online-Status** befinden, in dem Sie sie zwar sehen, sie aber nicht tatsächlich auf dem Gerät vorhanden sind. Wenn Sie eine solche Datei öffnen, wird sie heruntergeladen und zwischengespeichert und ist somit **lokal verfügbar**. Der Benutzer kann auch eine oder mehrere Dateien auswählen, die er **immer auf diesem Gerät behalten möchte**.




*Nur Cloud, lokale und angeheftete Dateien in OD4B*

Sie können die Synchronisierung nur auf Geräte beschränken, die in **einer Domäne eingebunden** sind. Um Benutzern die Verwaltung der Inhalte von gemeinsamen Ordnern zu erleichtern, können Sie das **Verschieben bekannter Ordner** (engl.: Known Folder Move) verwenden, um den Inhalt der Ordner Desktop, Dokumente und Bilder mit OD4B und damit zwischen den Geräten zu synchronisieren.

## 9.2: SHAREPOINT

Wenn Sie ein on-premises SharePoint-Administrator sind, sind Sie mit der Verwaltung der zugrunde liegenden Infrastruktur Ihrer Server sowie des komplexen Geflechts von Sites und Dokumenten-Workflows vertraut, die Endbenutzer auf dieser Basis nutzen. Wenn Sie SharePoint in der Cloud erst jetzt zum ersten Mal kennenlernen, werden Sie wahrscheinlich eine ganz andere Erfahrung machen, bei der Sie SharePoint lediglich als zugrundeliegenden Dokumentenspeicher für andere Anwendungen (Teams, Gruppen, Planner) und vielleicht als Plattform für das Intranet Ihres Unternehmens sehen.

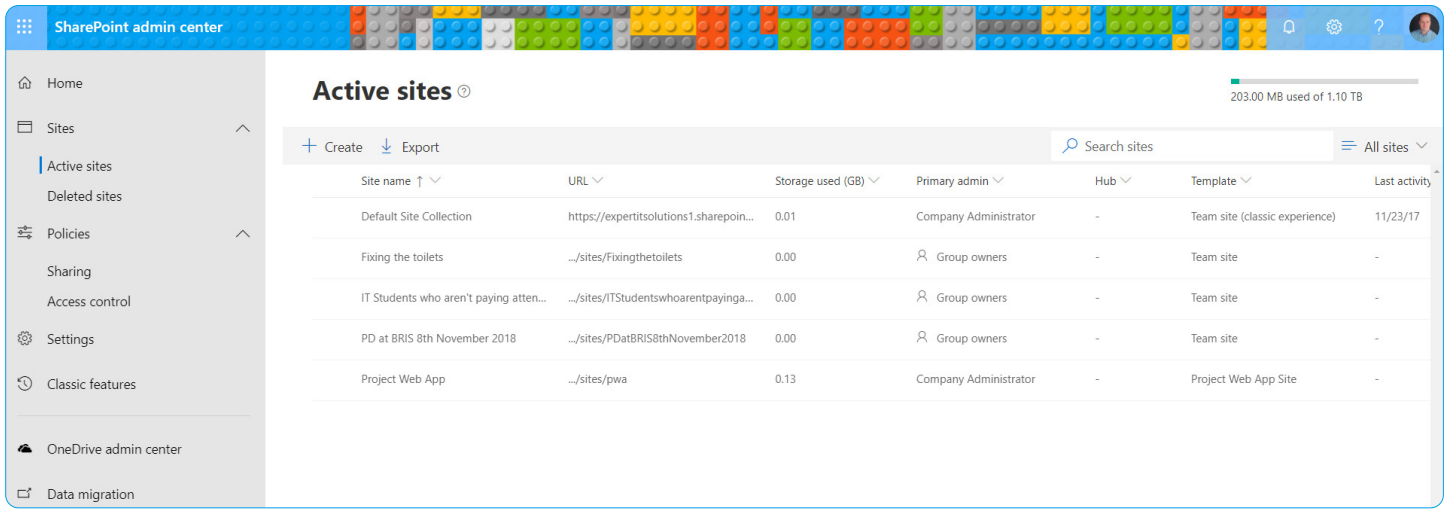
Die Bausteine in SharePoint sind **Sites**, auf denen Inhalte gespeichert werden. Sie können das Layout, das Thema, die Navigation und die Security sowohl mit den klassischen als auch mit den modernen Alternativen steuern. Wenn Sie neu anfangen oder neue Sites erstellen, sind moderne Websites **das Mittel der Wahl**. Es gibt einige verschiedene Typen wie **Kommunikationswebsites**, **Teamwebsites** und **Hub-Websites**. Als Teil einer größeren Vision für SharePoint sind die modernen Sites und Seiten sehr nützlich, da sie sich an Bildschirmauflösungen von Smartphones und unterschiedlich großen Computerbildschirmen anpassen.

Mit der **Suche** können Sie Sites, Dateien (einschließlich OneDrive for Business-Dateien), Personen und Nachrichteninhalte finden. Wenn der Inhalt Bilder enthält, extrahiert die Künstliche Intelligenz (KI) Metadaten und (falls vorhanden) Textinhalte aus diesen Bildern. Wenn Sie eine **hybride Bereitstellung** konfiguriert haben, werden Ihre on-premises Dokumente ebenfalls in den Suchergebnissen angezeigt.

**Apps** sind Add-Ins/Webparts, die die Funktionalität von Sites erweitern, und **Site-Sammlungen** sind eine Möglichkeit, Sites mit einem ähnlichen Zweck zusammenzufassen.

Um verschiedene Sites einzurichten, verwenden Sie **Website-Vorlagen**, die Ihnen den Einstieg erleichtern. Wenn Sie eine Intranet-Site erstellen, gibt es einen ausgezeichneten **Lookbook-Service** mit schönen Sites, die moderne Benutzeroberflächen bieten.

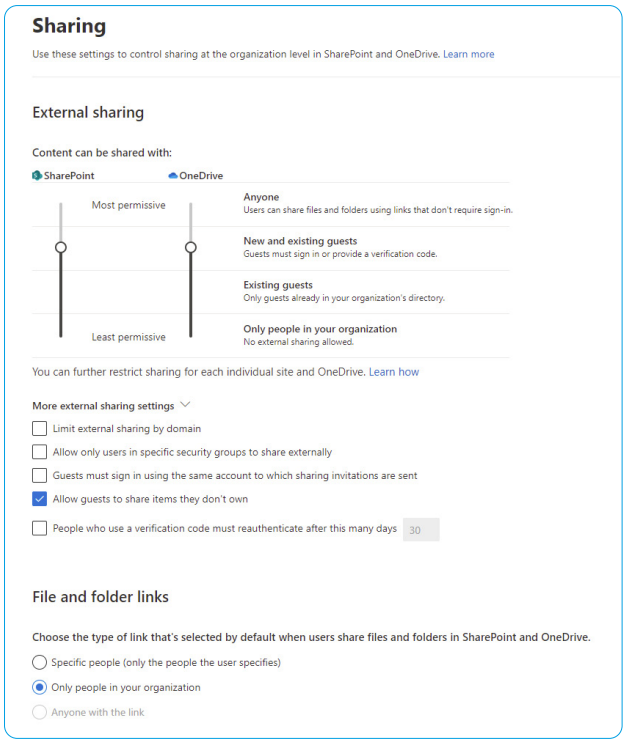
**SharePoint Syntex** ist eine Technologie, die KI und ML nutzt, um die Verarbeitung von Inhalten zu automatisieren und Inhalte in Wissen zu verwandeln. Sie versteht Ihre Dokumente, verarbeitet Formulare und ist für große Organisationen mit komplexen Workflows und Prozessen geeignet.




*SharePoint Online Admin Center*

Beachten Sie die **Beschränkungen von SharePoint Online**, insbesondere den verfügbaren Gesamtspeicherplatz, der 1 TB + 10 GB pro erworbener Lizenz beträgt. Die Suche ist ein Bereich, in dem Sie **einige Zeit mit Anpassungen verbringen sollten**, damit Ihre Benutzer eine gute Nutzererfahrung haben. Und auch die Freigabe von Inhalten ist ein Bereich, den Sie kontrollieren sollten, denn die Art und Weise, **wie Benutzer Inhalte intern und (kritisch) extern freigeben können**, hat direkten Einfluss auf das Gleichgewicht zwischen Zusammenarbeit und Sicherheit.

Die Migration von Inhalten von on-premises SharePoint Server und Netzwerk-Dateifreigaben nach M365 ist die **Aufgabe des SharePoint-Migrationstools** sowie zahlreicher Services von Drittanbietern. Wenn Benutzer versehentlich Dateien löschen oder Ransomware gespeicherte Dateien verschlüsselt hat, können Sie die Option **Dateien wiederherstellen** nutzen, um Dateien und Ordner oder ganze Bibliotheken aus der Vergangenheit (bis zu 30 Tage) wiederherzustellen. Außerdem gibt es den **Papierkorb** (93 Tage Aufbewahrungsfrist) für die Wiederherstellung einzelner Dateien und die **Wiederherstellung von Dateien für OneDrive.**




*SharePoint und OD4B externe Freigabekontrolle*

# KAPITEL 10:

# MICROSOFT 365-GRUPPEN

**M365-GRUPPEN SIND EIN GRUNDLEGENDER BAUSTEIN FÜR VERSCHIEDENE SERVICES. IN DIESEM KAPITEL WERDEN WIR UNS DIE VERSCHIEDENEN VERWENDUNGSMÖGLICHKEITEN DIESER GRUPPEN ANSEHEN.**

## 10.1: GRUPPENTYPEN

Ein Bereich, der neue O365-Administratoren oft verwirrt, sind die verschiedenen Arten von Gruppen. Hier eine kurze Übersicht:

- **Microsoft 365-Gruppen** (der in diesem Kapitel behandelte Typ)
- **Verteilergruppen** (Kapitel 8)
- **Sicherheitsgruppen** werden verwendet, um Zugriff auf Ressourcen zu gewähren
- **E-Mail-aktivierte Sicherheitsgruppen** werden ebenfalls verwendet, um Zugriff zu gewähren und können auch per E-Mail verschickt werden, so dass alle Mitglieder eine Kopie der E-Mail erhalten
- **Freigegebene Postfächer** (Kapitel 8)

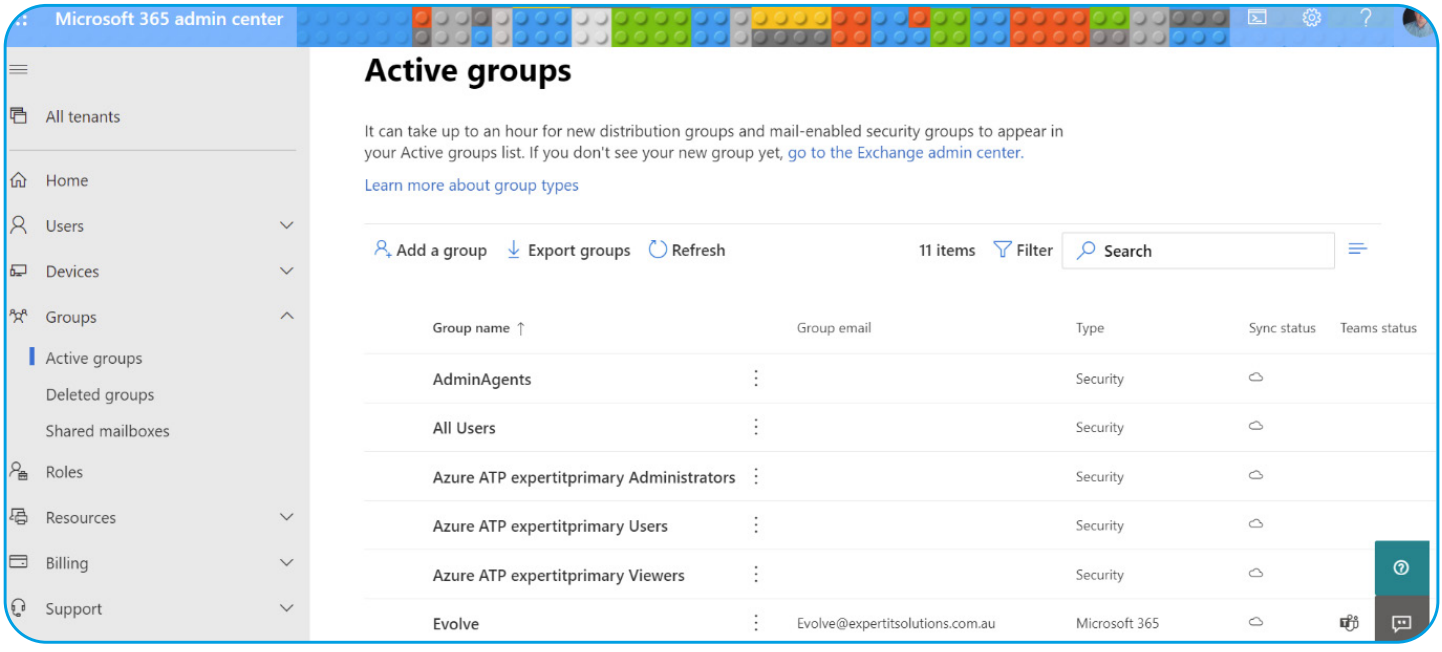
Sie können zwar direkt Microsoft 365-Gruppen erstellen, aber Sie werden eher mit ihnen als Grundbaustein interagieren, der eine zentrale Identität für ganz M365 bereitstellt, die Dienste wie Teams, Yammer und andere nutzen. Darüber hinaus kann Outlook M365-Gruppen verwenden, moderne SharePoint Teamwebsites bauen auf ihnen auf und Stream und PowerBI nutzen sie zur Zugriffskontrolle.



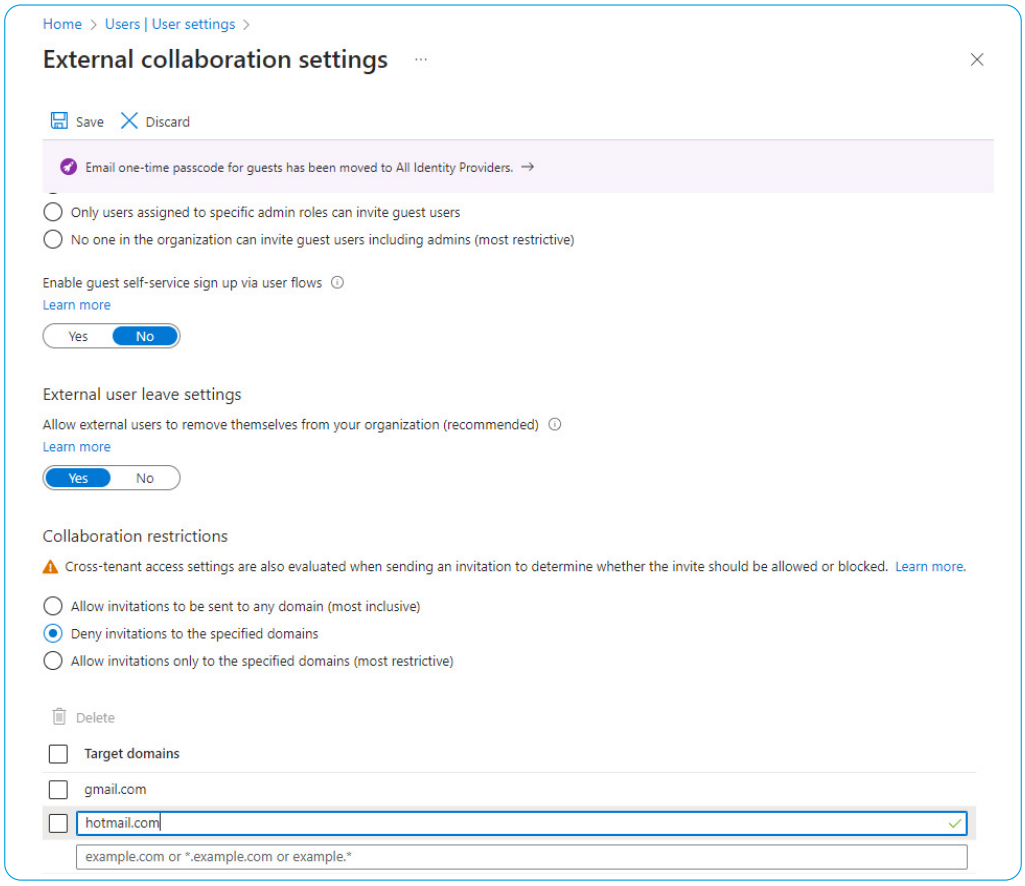
Wenn sie entsprechend konfiguriert sind, können Sie M365-Gruppen in Ihr on-premises AD zurückschreiben, wo sie sich als Verteilergruppen manifestieren. M365-Gruppen können nicht in andere Gruppen verschachtelt werden und sie können nur echte M365-Benutzerkonten enthalten, während Exchange-Verteilergruppen Benutzerkonten, E-Mail-Benutzer und Kontakte enthalten können (siehe Kapitel 8). Sofern Sie die Standardeinstellungen nicht geändert haben, kann jeder Benutzer in Ihrem Tenant eine M365-Gruppe erstellen, was zu **Problemen mit der Governance** führen kann. Sie können stattdessen **Benutzer bestimmen**, die Gruppen erstellen können. Sie können auch verschiedene **Richtlinien-Einstellungen** verwenden, um das Verhalten von O365-Gruppen in Ihrem Tenant zu steuern, z. B. **Ablaufrichtlinien** zur Verwaltung des Lebenszyklus von Gruppen, und Sie können die **Benennung von Gruppen** über Richtlinien steuern.

Es ist einfach, Inhalte aus einer M365-Gruppe für externe Benutzer freizugeben, und M365-Gruppen sind auch ein gemeinsames Repository für historische Inhalte, da jeder, der Mitglied ist, alle Inhalte sehen kann, die bis zum Zeitpunkt der ersten Erstellung der Gruppe zurückreichen. Früher gab es für jeden lizenzierten Benutzer in Ihrem Tenant fünf **B2B-Gastlizenzen**, und Sie konnten **Einmalkennungen** für externe Gäste verwenden, die nicht über ein Google- oder Microsoft-Konto oder ein Konto in Azure AD verfügen.

Das Lizenzierungsmodell für externe Benutzer hat sich geändert. Microsoft führt Azure B2B und B2C (Nutzung von Azure als Speicher für Consumer-Identitäten für Ihre intern entwickelte Anwendung) zusammen und das neue Lizenzmodell bedeutet, dass jeder Tenant ohne zusätzliche Kosten bis zu 50.000 externe Benutzer haben kann.




*Gruppen im M365 Admin Center*




*External Collaboration settings in Entra - blocking specified domains*

Beachten Sie, dass Gäste standardmäßig vollen Zugriff auf alle Gruppeninhalte haben. Sie können **festlegen, aus welchen Domänen** externe Benutzer kommen müssen (oder nicht kommen dürfen), um externen Zugriff zu erhalten.

Wenn Sie heute eine Gruppe erstellen, ist sie **privat**, und die Eigentümer der Gruppe müssen eine Anfrage zum Beitritt genehmigen. Sie können eine Gruppe auch öffentlich machen, so dass jeder ihr beitreten kann. Sie können den Tenant-Standard ändern, der sicherstellt, dass neue Gruppen **öffentlich** sind, oder Sie können die Einstellung für eine Gruppe ändern, nachdem Sie sie erstellt haben. Jede Gruppe kann bis zu 100 Eigentümer und über 1000 Benutzer haben; ein einzelner Benutzer kann nicht mehr als 250 Gruppen erstellen. Wie bei anderen Konstrukten in M365 haben Sie 30 Tage Zeit, **eine gelöschte Gruppe wiederherzustellen**, während einzelne Dokumente in der Gruppe 93 Tage lang im SharePoint-Papierkorb verbleiben.

**Dynamische Gruppen** sind eine gute Möglichkeit, den Verwaltungsaufwand für die manuelle Verwaltung von Gruppenmitgliedschaften auf der Grundlage von Abfragen von Entra ID-Attributen zu reduzieren. Beachten Sie jedoch, dass Sie dafür eine Entra ID Premium P1-Lizenz benötigen.

# KAPITEL 11:

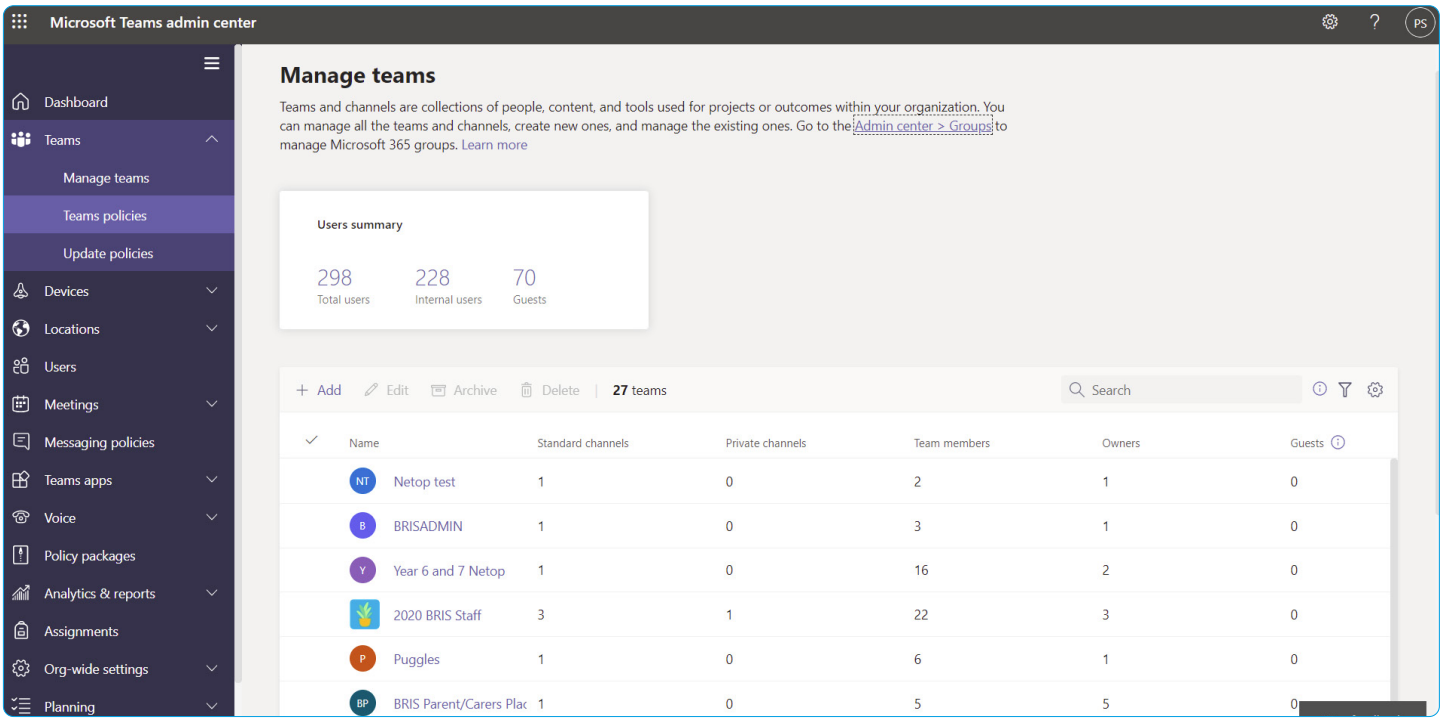
# TEAMS

**ES GAB SCHON VIELE INSTANT MESSAGING-/CHAT-ANWENDUNGEN, DIE VERSUCHT HABEN, DIE GESCHÄFTSKOMMUNIKATION ZU EROBERN, UND OHNE ZWEIFEL IST TEAMS VON MICROSOFT DIE BISHER BESTE. DAS LIEGT NICHT ZULETZT AN DER COVID-19-PANDEMIE, DIE DAZU GEFÜHRT HAT, DASS DIE NUTZUNG VON TEAMS VON 13 MILLIONEN TÄGLICH AKTIVEN BENUTZERN IM JULI 2019 AUF ÜBER 300 MILLIONEN (!) IM JAHR 2023 ANGESTIEGEN IST. IN DIESEM KAPITEL SEHEN WIR UNS AN, WAS TEAMS FÜR DIE KOMMUNIKATION UND ZUSAMMENARBEIT IN IHREM UNTERNEHMEN TUN KANN.**

## 11.1: MS TEAMS

Es wird viel an Teams gearbeitet, um sicherzustellen, dass es der beste Ort für die Zusammenarbeit von Gruppen ist. Der jüngste Beweis dafür ist die neue **Teams Client-Anwendung** (Public Preview März 2023).

Ein Team kann **bis zu 25.000 Benutzer haben**, aber meiner Erfahrung nach funktioniert es am besten mit kleineren Teams (bis zu ein paar hundert). Wenn Sie eine Veranstaltung im Stil eines Webinars veranstalten, bei der die Teilnehmer nur zuschauen, ist die Teilnehmerzahl auf 20.000 begrenzt. Es gibt Client-Anwendungen für Windows, MacOS (beide werden zweiwöchentlich aktualisiert), iOS und Android sowie eine webbasierte Benutzeroberfläche (wöchentlich aktualisiert). Wie bei vielen Dingen in M365 gibt es zwei Komponenten für eine erfolgreiche Adaption: die technische Seite und die Schulung der Benutzer.




*Teams Admin Center*

Wenn Sie über Konferenzräume verfügen, sollten Sie sich Gedanken über die Technologie machen, mit der Sie diese ausstatten. **Teams-Räume** (engl. Teams Rooms) ist eine leistungsstarke Methode, um Mitarbeiter im Büro mit Mitarbeitern, die von zu Hause aus arbeiten, zu verbinden. Teams-Räume ist unterteilt in Basic (kostenlos, bis zu 25 Systeme können diese Art von Lizenz haben) und Pro, die mit vielen Funktionen für **Sicherheit, Komfort und weiteren Funktionen für die Zusammenarbeit** ausgestattet ist. Die alte Teams-Räume Premium-Lizenzierung wurde abgeschafft.

Bis vor kurzem gab es nur die Teams-Lizenzierung (als Teil der M365-Lizenzierung) und ein kostenloses Teams für kleinere Teams (das jetzt eingestellt wird). Im Februar 2023 wurde eine neue, kostenpflichtige Lizenzierungsstufe namens Teams Premium verfügbar. Wie bei allen M365-Funktionen müssen Sie sorgfältig abwägen, ob die zusätzlichen Funktionen für die Benutzer, für die Sie sie lizenzieren, geschäftlich sinnvoll sind (nicht jeder muss Teams Premium haben). Zu den **Premium-Funktionen** gehören geschützte Meetings mit Wasserzeichen auf den Aufzeichnungen (mit der E-Mail-Adresse der aufzeichnenden Person), Kennzeichnung der Vertraulichkeit von Meetings und End-to-End-Verschlüsselung sowie benutzerdefinierte Meeting-Vorlagen und Themen. Für Webinare gibt es eine Menge zusätzlicher Funktionen, die das Gesamterlebnis verbessern, und schließlich werden mit Virtuellen Terminen diese Arten von Meetings gemanagt, einschließlich SMS-Benachrichtigungen.

## 11.2: TEAMS TELEFON

Ein großer Vorteil von Teams ist, dass Sie es **mit dem öffentlichen Telefonnetz verbinden** können, so dass Ihre Benutzer von ihrem Teams-Client aus (auf jeder Plattform) jeden in der Welt anrufen können und eine Telefonnummer haben, unter der sie jeder anrufen kann. Diese Kombination aus externen Telefongesprächen, internen VOIP-/Videoanrufen und Videokonferenzen oder Webinaren, einfacher **Dateifreigabe und Co-Authoring** sowie asynchronem Instant Messaging und Chat hat Teams in vielen Unternehmen zum De-facto-Zentrum für Zusammenarbeit und Kommunikation gemacht.

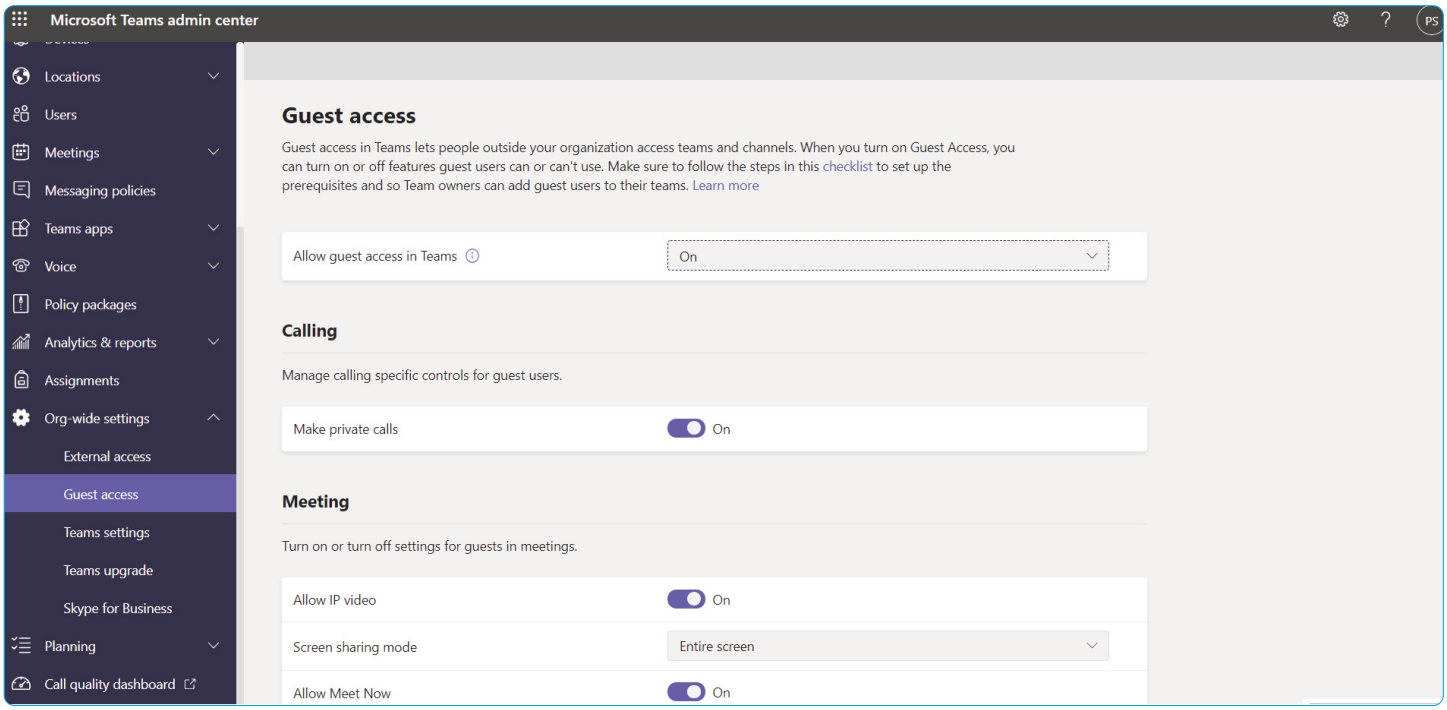
Es gibt einige Optionen für die Verbindung, und je nach Ihrem geografischen Standort in der Welt sind nicht alle verfügbar. Sie können einen **Anrufplan** verwenden, bei denen Microsoft quasi Ihr Telekommunikationsanbieter ist, oder **Operator Connect**, wenn Ihr bestehendes Telekommunikationsunternehmen an dem Programm teilnimmt und die Verbindung herstellen kann. Es gibt auch **Phone Mobile**, bei dem eine bestehende Telefongesellschaft SIM-fähige Mobiltelefonnummern mit Teams verwendet, und schließlich **Direct Routing**, bei dem Sie die on-premises Infrastruktur mit Teams verbinden. Und in größeren Umgebungen können Sie mehrere dieser Möglichkeiten in Kombination nutzen.

## 11.3: TEAMS VERWALTEN

Ihre Hauptschnittstelle ist das **Teams Admin-Portal,** und es steht ein **PowerShell-Modul** zur Verfügung. Unter jedem Team befindet sich eine M365-Gruppe (Kapitel 10), in der die Chat-Nachrichten im Azure-Tabellenspeicher, die gemeinsamen Dateien in der SharePoint-Bibliothek des Teams und die persönlichen Dateien in der OD4B jedes Benutzers gespeichert sind. Voicemail und Kalender werden in den Exchange-Postfächern der Benutzer gespeichert und die Aufzeichnungen von Meetings in den Azure Media Services. Wenn Sie in einem größeren Unternehmen tätig sind, sollten Sie die **Governance von Teams** bereits in der Anfangsphase Ihrer Implementierung einplanen. Sehen Sie sich die Einstellungen für den Gastzugang Ihres Tenants zu Teams an, um sicherzustellen, dass Sie ein ausgewogenes Verhältnis zwischen Sicherheit und Zusammenarbeit für Ihr Unternehmen finden. Eine weitere praktische Funktion ist die Möglichkeit, **Vorlagen für die Erstellung von Teams** zu verwenden, einschließlich der Erstellung Ihrer eigenen Vorlagen.

Jedes Team verfügt über einen allgemeinen Standardkanal und Sie können weitere Kanäle erstellen, um die Kommunikation zu organisieren. Innerhalb jedes Kanals können Sie Registerkarten für Planner, OneNote, PowerBI, Stream, Wiki, Websites und Drittanbieteranwendungen hinzufügen. Um die Wucherung von Teams in Ihrem Unternehmen zu unterbinden, können Sie **einschränken, wer Teams erstellen darf** (standardmäßig können das alle Benutzer), und Sie können auch **private Kanäle in einem Team** verwenden. Sie könnten ein Team für die Vertriebsabteilung mit einem privaten Kanal einrichten, in dem beispielsweise allein die Vertriebsleiter vertrauliche Informationen besprechen können.

Es gibt auch die Möglichkeit, einen **Kanal für einen externen Benutzer freizugeben**, anstatt ein ganzes Team freizugeben. Der Hauptvorteil für den eingeladenen Benutzer besteht darin, dass er mit seinem eigenen Tenant-Konto angemeldet sein kann und auf den Chat und die Dokumente des freigegebenen Kanals zugreifen kann, ohne dass er sich abmelden und mit seinem Gastkonto wieder bei Teams anmelden muss.

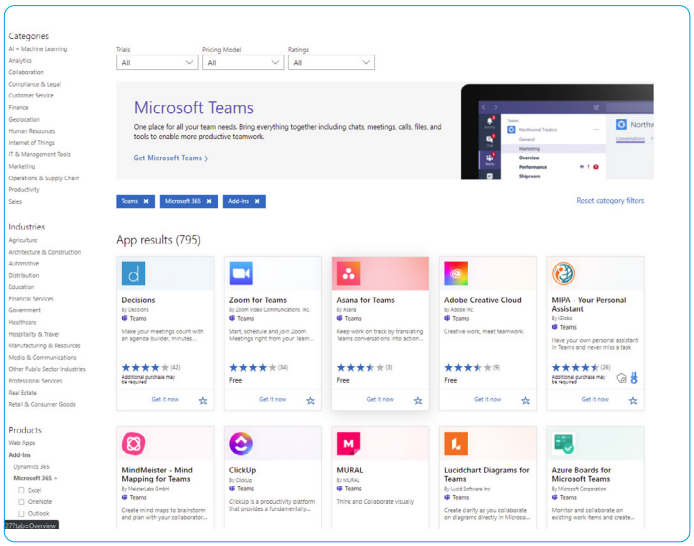



*Teams Gastzugang Einstellungen*

Sie können nur einen neuen Kanal als freigegebenen Kanal erstellen, Sie können einen normalen Kanal nicht in einen freigegebenen Kanal umwandeln.

Es ist durchaus üblich, Präsentationen mit Hilfe von Teams zu halten. Die **PowerPoint Live-Funktion** macht dies interaktiver, da die Teilnehmer in ihrem eigenen Tempo mit der Präsentation interagieren können, und der **Referentenmodus** gibt Ihnen mehr Kontrolle darüber, wie Ihre Präsentation beim Publikum ankommt. Um Ihren Vortrag (generell in PowerPoint) zu üben, verwenden Sie **Speaker Coach**.

Eine großartige Funktion sind **Gruppenräume** (engl. Breakout Rooms). Damit können Sie Benutzer in "Räume" schicken oder sie bitten, dorthin auszuweichen, damit sie während einer Besprechung mit einer Untergruppe eines Teams zusammenarbeiten können, um später zur Hauptbesprechung zurückzukehren.




*Teams Add-Ins von Drittanbietern*

Aufzeichnungen von Teams-Besprechungen (einschließlich **Transkriptionen**) wurden früher in Stream gespeichert, jetzt werden sie in **OD4B / SharePoint gespeichert**, wo sie auf einfache Weise geteilt werden können (auch mit externen Teilnehmern). Beachten Sie bitte die standardmäßige Ablauffrist für Besprechungsaufzeichnungen: 120 Tage. Sie können dies (für Aufzeichnungen in Ihrem Tenant) im Teams Admin Center - Meetings - Meeting-Richtlinien - Aufzeichnung & Transkription ändern. Apropos Transkription: Wenn Sie über Teams Premium verfügen, können Sie **übersetzte Untertitel** aktivieren, so dass ein in Englisch gehaltenes Meeting von einem deutschen Teilnehmer mit deutschen Untertiteln und von einem anderen Teilnehmer mit chinesischen Untertiteln angesehen werden kann.

## 11.4: NUTZUNG VON TEAMS

Wenn Sie es gewohnt sind, per E-Mail zu kommunizieren, finden Sie hier einige Tipps, wie Sie mit Teams effektiv arbeiten können. Verwenden Sie @-Erwähnungen, um ein bestimmtes Teammitglied, einen Kanal oder ein ganzes Team auf etwas aufmerksam zu machen. Seien Sie großzügig mit Ihrem Lob, wenn jemand etwas Gutes für das Team tut, und wenn Sie eine Nachricht anerkennen möchten, liken Sie sie einfach, anstatt mit einer textbasierten Antwort zu reagieren. Wenn Sie etwas posten möchten, prüfen Sie, ob es bereits einen Thread dazu gibt und fügen Sie stattdessen zu diesem hinzu. Verwenden Sie Textformatierungen (oder ein GIF / einen Sticker / ein Meme), wenn Sie Ihren Standpunkt deutlich machen möchten, und tragen Sie gegebenenfalls mit einer Traurig-, Wütend- oder Happy-Reaktion zur Unterhaltung bei.

Sie können den Hintergrund unscharf machen, wenn Sie in einer Videokonferenz sind, oder das **Hintergrundbild ersetzen**, und wenn Sie Außendienstmitarbeiter haben, die mit anderen auf die Schnelle kommunizieren müssen, können sie die **Walkie Talkie** Push-to-Talk-Funktion nutzen. Sie können auch **einen Avatar** einsetzen, der Sie in Ihrem Video-Feed ersetzt. Das ist praktisch für Meetings am Montagmorgen, wenn Ihre Frisur noch nicht richtig sitzt und Sie stattdessen lieber auf eine "Cartoon"-Version von sich selbst zurückgreifen wollen.

Teams **übersetzt Nachrichten** in anderen Sprachen automatisch in die Sprache, die Sie in Ihren persönlichen Einstellungen festgelegt haben. Und es gibt eine **Offline-Funktion**, die Ihre noch nicht gesendeten Nachrichten offline speichert und sie erst dann sendet, wenn Sie wieder online sind.

Wenn Sie sich in einer Besprechung befinden, können Sie den **Together Mode** verwenden, der das Videobild jedes Teilnehmers so anzeigt, als säßen sie alle zusammen in einem Hörsaal, statt der üblichen Gitter-Darstellung.

## 11.5: VIVA

Wenn Sie noch einen Beweis dafür brauchen, wie zentral Teams für Microsofts Vision und Roadmap für moderne Zusammenarbeit und Arbeit geworden ist, dann schauen Sie sich die **Viva** Employee Experience Platform (EXP) an. Viva besteht aus acht Säulen, die alle in Teams abgebildet sind: **Viva Connections** nutzt Ihre SharePoint Online Home Site, andere Fachanwendungen und weitere interne Nachrichtenquellen und ermöglicht es Ihnen, Unternehmensnachrichten und -verbindungen gezielt an die richtigen Personen weiterzuleiten. **Viva Insights** ist die Weiterentwicklung von My Analytics, um Mitarbeitern zu helfen, ihre Zeit zu managen und Burnout zu vermeiden, sowie eine Integration mit Headspace für geführte Meditationen und eine virtuelle Pendelfunktion, um den Arbeitstag abzuschließen.

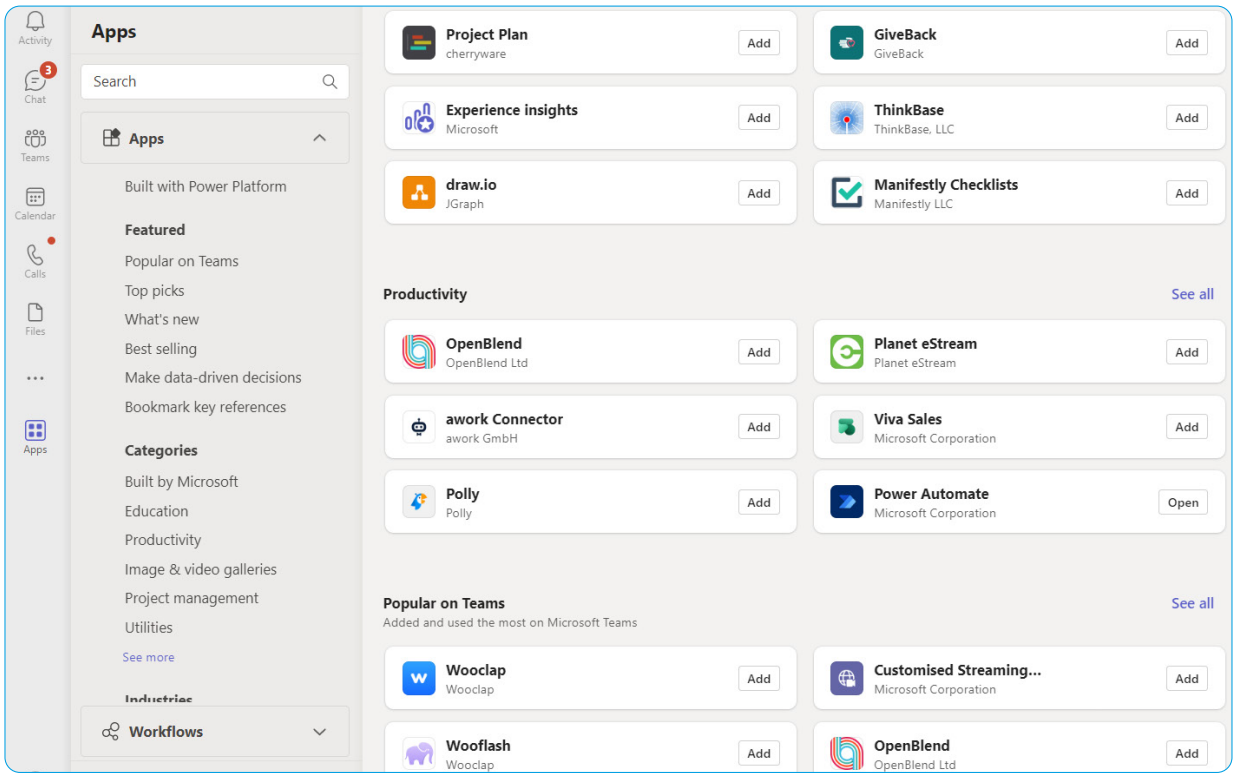
Für Führungskräfte gibt es eine anonymisierte Ansicht, mit der Sie sehen können, wie es Ihrem Team in Bezug auf Stress, psychische Gesundheit und Produktivität geht. Es gibt auch eine Ansicht für Führungskräfte, um den Gesamtstatus ihrer Mitarbeiter zu sehen. Die dritte Säule ist **Viva Learning**, das **Trainingskurse und Microlearning-Inhalte** bereitstellt und mit **anderen Lernmanagementsystemen** (Cornerstone OnDemand, Saba, SAP SuccessFactors und Workday) integriert ist, um das Lernen zu einem natürlichen Bestandteil der täglichen Arbeit zu machen. Vorgesetzte können Schulungen planen und Mitarbeiter können besonders gute Kurse untereinander austauschen und sie sind alle direkt in Teams verfügbar. **Viva Topics** baut auf Cortex / Syntex auf und nutzt KI, um unternehmensweite Inhalte (interne Projekte, Produkte, Akronyme) und das Fachwissen der Mitarbeiter zu organisieren und diese als Themenkarten / Seiten in Teams, Microsoft Search, SharePoint und Office zu präsentieren. Stellen Sie sich dies als Wikipedia für Ihr Unternehmen vor.

**Viva Goals** nutzt die Leistungsfähigkeit des Objectives and Key Results (OKR) Systems, um den Mitarbeitern zu helfen, ihre Fortschritte im Hinblick auf ihre Ziele zu verfolgen. **Viva Engage** hingegen verbindet Menschen im gesamten Unternehmen (dies ist eigentlich der neue Name für das ehemalige Yammer). Das neue **Viva Sales** lässt sich in jedes CRM integrieren (natürlich auch in Microsoft Dynamics 365), um einen besseren Einblick in die Kundenbeziehungen zu erhalten. Und schließlich hilft **Viva Pulse** (zum Zeitpunkt der Erstellung dieses E-Books in der Public Preview) Führungskräften und Managern dabei, internes Feedback in einer Organisation zu erhalten und darauf zu reagieren.

Wie Sie diesen kurzen Beschreibungen entnehmen können, werden die meisten Viva-Module wahrscheinlich in größeren Unternehmen zum Einsatz kommen, da dort die Herausforderungen des "Managements von Mitarbeitern" in großem Maßstab am stärksten zu spüren sind.

## 11.6: TEAMS ERWEITERN

Eine weitere leistungsstarke Funktion ist das **Hinzufügen von Apps** zu Teams über den Teams Store. Microsoft testet und validiert diese Apps. Es gibt Hunderte von verschiedenen Apps zur Integration mit anderen Plattformen, zur Steigerung der Produktivität, zur Verbesserung von Meetings, zur Verwaltung von Kundenbeziehungen (CRM) und viele mehr. Eine sehr beliebte App ist **Microsoft Whiteboard**, die auf allen Plattformen kostenlos ist und die Sie sowohl innerhalb von Teams als auch eigenständig zum Brainstorming und zur gemeinsamen Planung verwenden können.




*Teams Store mit Apps von Drittanbietern*

Als Administrator haben Sie die Möglichkeit, **Apps zuzulassen oder zu sperren,** die ihnen **zugewiesenen Berechtigungen zu kontrollieren**, zu verwalten, **wie die Apps den Benutzern zur Verfügung gestellt werden**, und **Berichte über die App-Nutzung** zu erstellen. Sie können auch **benutzerdefinierte Apps** einbinden.

Sie können **Teams auch mit Bots erweitern**, die mit Ihren Benutzern auf natürliche Weise durch Chats interagieren können, oder mit einem Benachrichtigungs-Bot, der Ihren Benutzern relevante Informationen zukommen lässt.

Mit dem Aufkommen von Slack (dem Hauptkonkurrenten von Teams) und Teams haben viele Leute (wieder einmal) den Tod der E-Mail verkündet. Wie üblich neigen wir dazu, eine neue Technologie als direkten Ersatz für die alte zu sehen, während die Realität etwas differenzierter ist.

Ich finde Teams effizienter für die gruppenbasierte Arbeit, das Teilen von Dateien und die Kommunikation ist besser als E-Mail, aber die Kommunikation außerhalb von Kundenprojekten, an denen ich beteiligt bin, beruht immer noch auf E-Mail. Und Sie können E-Mails verwenden, um Nachrichten an einen Kanal in einem Team zu senden.

# KAPITEL 12:

# WEITERE OFFICE 365 ANWENDUNGEN

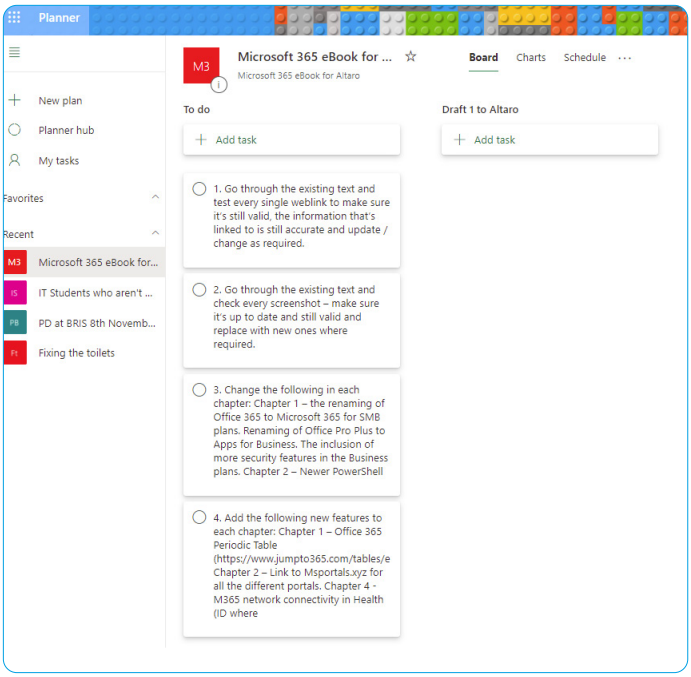

**ES GIBT NOCH VIELE WEITERE ANWENDUNGEN UND SERVICES IM O365-PORTFOLIO. IN DIESEM KAPITEL SEHEN WIR UNS EINIGE VON IHNEN MIT EINER KURZEN VORSTELLUNG AN.**

## 12.1: PLANNER

Microsoft bietet seit vielen Jahren Project für das Management großer Projekte an, aber für kleine bis mittlere Unternehmen ist es zu viel des Guten (die Lernkurve ist steil), und hier glänzt Planner. Wenn Sie schon einmal mit Trello gearbeitet haben, sollten Sie mit dem Arbeitsablauf von Planner vertraut sein.

Es gibt eine webbasierte Oberfläche sowie iOS- und Android-Clients, aber keinen PC-Client. Wenn Sie einem Team einen Planner-Reiter hinzufügen, können Sie einen neuen Projekt-Plan erstellen oder einen bestehenden Plan anhängen. Sie organisieren Aufgaben in Spalten, weisen verschiedenen Personen Aufgaben zu und verfolgen den Fortschritt dieser Aufgaben. Die Aufgaben können auch in einer Zeitplanansicht (Kalender) angezeigt werden, und Sie können einen Plan nach Excel exportieren.




*Ein Projektplan in Planner*

Zu den anderen Microsoft-Angeboten für die Aufgabenverwaltung gehört To-Do (mobile, Web- und PC-Clients sind verfügbar), das sich mit Outlook-Aufgaben integrieren lässt.

## 12.2: STREAM

Das ist der beste Weg, um **Videos** innerhalb Ihres Unternehmens zu teilen, und es ist ähnlich wie YouTube. Es gibt Clients für iOS und Android und eine Weboberfläche, aber derzeit gibt es keine Lizenz für das Teilen von Videos mit Personen außerhalb Ihres Tenants.

Wenn Sie ein Video hochladen, wird es verarbeitet und wenn die Personen darin Englisch, Chinesisch, Französisch, Deutsch, Italienisch, Japanisch, Portugiesisch oder Spanisch sprechen, werden **automatisch Untertitel generiert**, die in Stream durchsuchbar sind, so dass Sie das richtige Video oder die richtige Stelle im Video leicht finden können. Außerdem wird versucht, Personen im Video zu erkennen, und wenn dies gelingt, werden diese Personen zusammen mit den.

## 12.3: KAIZALA

Dies ist eine Anwendung wie Teams, die für Außendienst-/Zeit-Mitarbeiter mit schlechter Konnektivität entwickelt wurde. Stellen Sie sich dies als eine gemanagte Version von WhatsApp vor.

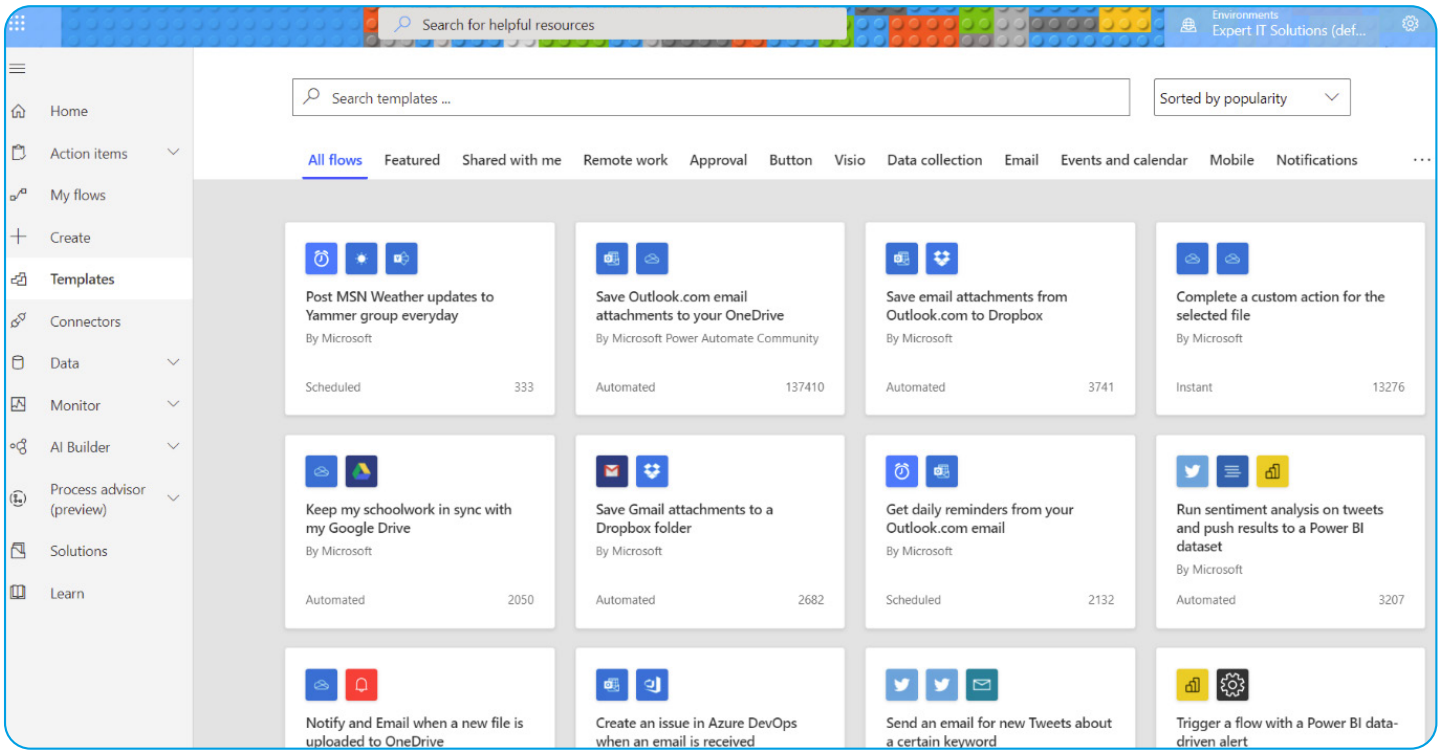
## 12.4: POWERBI

Die Visualisierung von Daten ist für jedes moderne Unternehmen wichtig, das datengesteuert arbeiten muss, und **PowerBI** ist die Antwort von Microsoft. Es gibt einen Desktop-Client, mit dem Sie Ihre Dashboards erstellen, und eine Weboberfläche. Die Lizenzierung ist **eine kleine Herausforderung**, je nachdem, was Sie erstellt haben und mit wem Sie es teilen möchten.

Es macht Spaß, es zu benutzen, und die Ergebnisse können für viele Aspekte Ihres Unternehmens äußerst nützlich sein.

## 12.5: POWER AUTOMATE

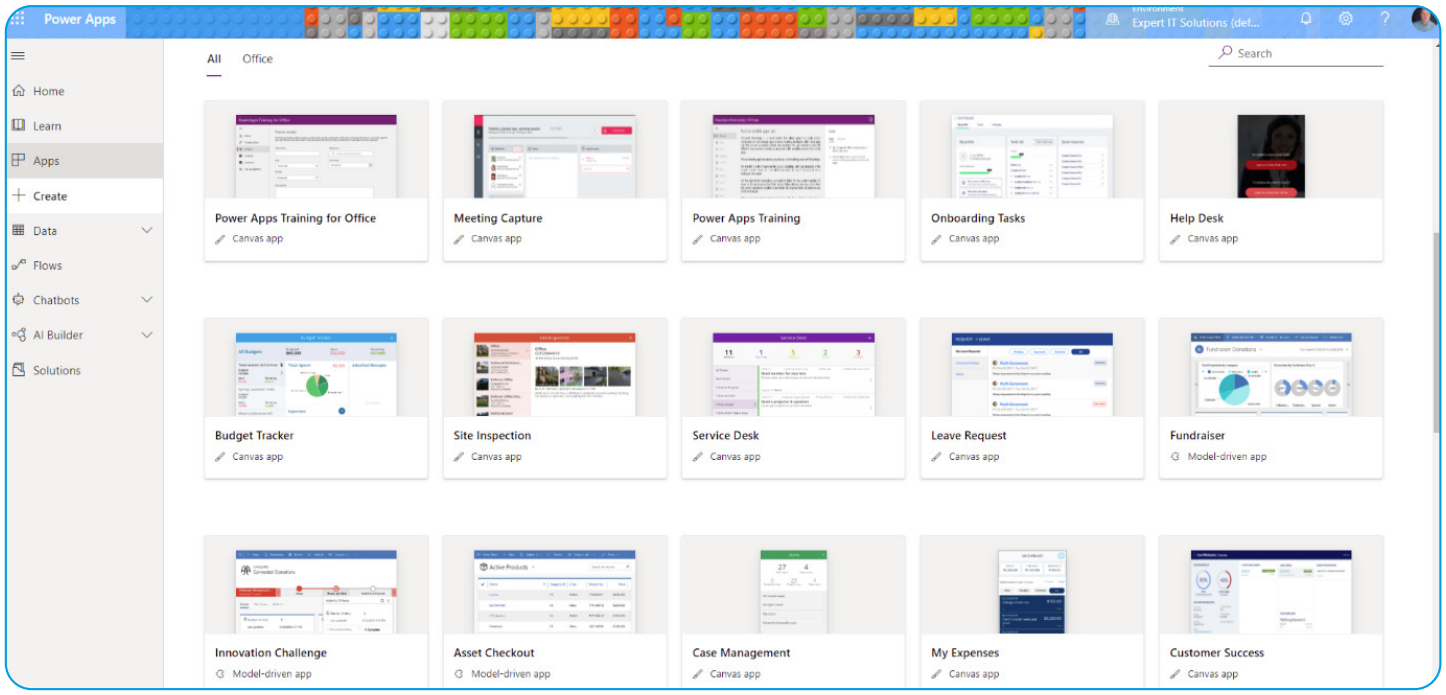
Dieses verblüffend einfache, webbasierte Tool wurde entwickelt, um Aufgaben zu automatisieren, ohne Code schreiben zu müssen (es hieß früher Flow). Ziehen Sie einfach Aktionen hinein, verbinden Sie sie mit externen Systemen und planen Sie sie so, dass sie regelmäßig ausgeführt oder durch ein Ereignis ausgelöst werden. Es gibt viele Vorlagen, die Ihnen den Einstieg erleichtern, sowie Konnektoren, mit denen Sie Microsoft- und Fremdsysteme einbinden können. Wenn Sie bereits If This Then That oder Zapier verwendet haben, ist der Einstieg in **Power Automate** ganz einfach.




*Vorlagen in Power Automate*

## 12.6: POWERAPPS

Haben Sie sich schon einmal gewünscht, Ihre Mitarbeiter mit einer maßgeschneiderten mobilen App auszustatten, um Daten vor Ort zu erfassen oder darauf zuzugreifen, aber die Entwicklungskosten waren Ihnen zu hoch? **PowerApps** ist die Lösung, denn es bietet eine Low Code / No Code-Entwicklungsumgebung zur Erstellung von Anwendungen, die mit SharePoint, Excel, O365, Dynamics 365 oder SQL Server on-premises oder in der Cloud verbunden sind; oder mit der **Dataverse-Plattform**. Die resultierende App läuft auf iOS, Android, in einem Webbrowser oder in Teams und SharePoint Online. Wenn Sie Daten in Ihren Apps verwalten müssen, gibt es **Dataverse for Teams** und die Vollversion von Dataverse.




*PowerApps Templates*




## 12.7: MICROSOFT LISTS

Ja, das alte SharePoint-Listenkonzept wurde zu neuem Leben erweckt, einschließlich einer **separaten App** und ist auch in Teams verfügbar. Nutzen Sie es, um Listen mit allen möglichen Aufgaben zu verfolgen und Informationen zu verwalten.

## 12.8: MICROSOFT LOOP

Die möglicherweise verwirrendste Technologie, die Microsoft in den letzten Jahren veröffentlicht hat (derzeit in der Public Preview), ist **Loop**. Das Konzept ist recht einfach: Sie haben Loop-Komponenten, die Sie an verschiedenen Stellen einbetten können, z. B. in Dokumente, Teams-Chats oder eine E-Mail, und diese werden an diesen verschiedenen Stellen synchron gehalten.

Mit Loop-Seiten können Sie Komponenten, Links, Aufgaben und andere Daten zusammenführen. Loop-Arbeitsbereiche schließlich sind gemeinsame Bereiche, die Seiten und Komponenten zusammenführen. Ich finde Loop in den frühen Phasen eines Projekts oder einer Idee am nützlichsten - Brainstorming, Zusammenarbeit mit anderen an einem Konzept und Synchronisierung aller Ideen mit allen, mit denen Sie zusammenarbeiten.

Die Herausforderung besteht heute darin, dass die Loop-Komponenten im persönlichen OneDrive for Business des Benutzers gespeichert werden. Daher funktioniert die gemeinsame Nutzung außerhalb eines Unternehmens nicht wirklich, und selbst innerhalb eines Tenants kann es eine Herausforderung sein. Wenn Microsoft diese Herausforderungen lösen kann, hat Loop eine interessante Zukunft.

# KAPITEL 13:

# MICROSOFT INTUNE

**M365 E3 UND E5 BIETET IHNEN MICROSOFT INTUNE, DEN CLOUD SERVICE FÜR MOBILE DEVICE MANAGEMENT (MDM) VON MICROSOFT. IN DIESEM KAPITEL SEHEN WIR UNS AN, WIE SIE DAMIT GERÄTE UND PCS SOWIE MOBILE APPS VERWALTEN, UNTERNEHMENSDATEN SCHÜTZEN UND SICHERHEITSRICHTLINIEN DURCHSETZEN KÖNNEN.**

Früher gab es ein on-premises Produkt namens System Center Configuration Manager (SCCM), das jetzt **Microsoft Configuration Manager** heißt und das Sie eng mit Intune integrieren können.

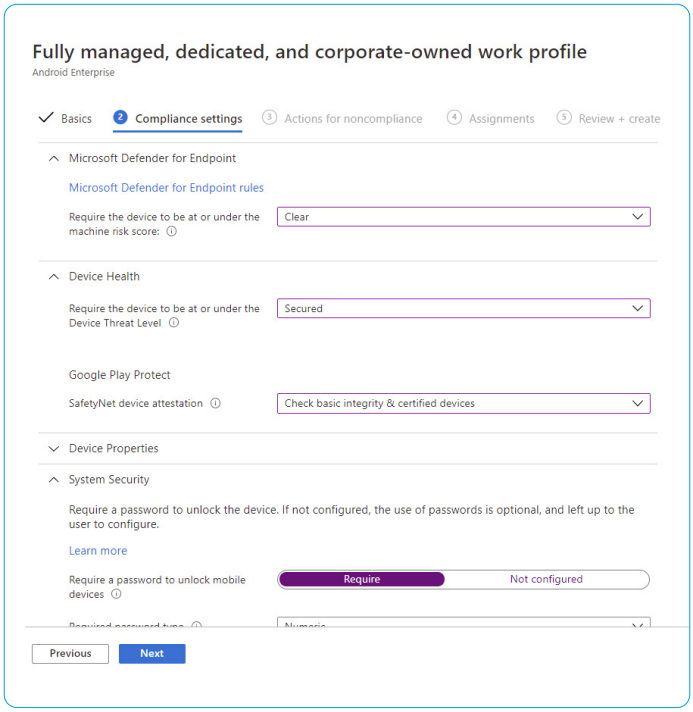
Früher war es erforderlich, dass Intune-Administratoren für Intune lizenziert waren, aber das ist jetzt **nicht mehr der Fall**. Die **Endpunkt-Analyse** ist ein interessanter Teil von Intune. Sie nutzt Signale von Ihren Geräten, um problematische oder langsame PCs zu identifizieren, und ist Teil der **Einführungsbewertung** (englisch: Adoption).

Wenn Sie Windows 10/11-Geräte haben, die bestimmte Funktionen erfüllen (z.B. in einer Fabrikhalle oder auf einer Krankenstation in einem Krankenhaus), können Sie diese mit Cloud Configuration **ganz einfach vollständig über Intune verwalten**, mit skriptgesteuerten Grundkonfigurationseinstellungen.



## 13.1: MOBILE DEVICE MANAGEMENT

Es gibt mehrere Möglichkeiten, Intune zu nutzen. Wenn Sie über Geräte (Smartphones, Tablets, Laptops) verfügen, die Ihrem Unternehmen gehören, können Sie diese **in Intune registrieren**. Dadurch erhalten Sie eine umfassende Kontrolle über das Gerät, einschließlich der Möglichkeit, Einstellungen und Anwendungen zu verwalten und das Gerät zu löschen, falls es verloren geht oder gestohlen wird. Sie können Intune auch verwenden, um Betriebssystem-Updates für Windows-Geräte zu verwalten, Anwendungen auf die Geräte zu übertragen, Wi-Fi-Profile zu konfigurieren und Zertifikate bereitzustellen sowie iOS-Geräte mit Jailbreak und gerootete Android-Geräte zu blockieren.




*Android Compliance-Richtlinie im Endpunkte-Manager*

Wenn es sich bei dem Gerät um ein persönliches Gerät handelt, das dem Mitarbeiter gehört, kann es sein, dass er das Gerät nicht registrieren möchte, so dass Sie Mobile Application Management (MAM) für diese Geräte verwenden können.

## 13.2: MOBILE APPLICATION MANAGEMENT

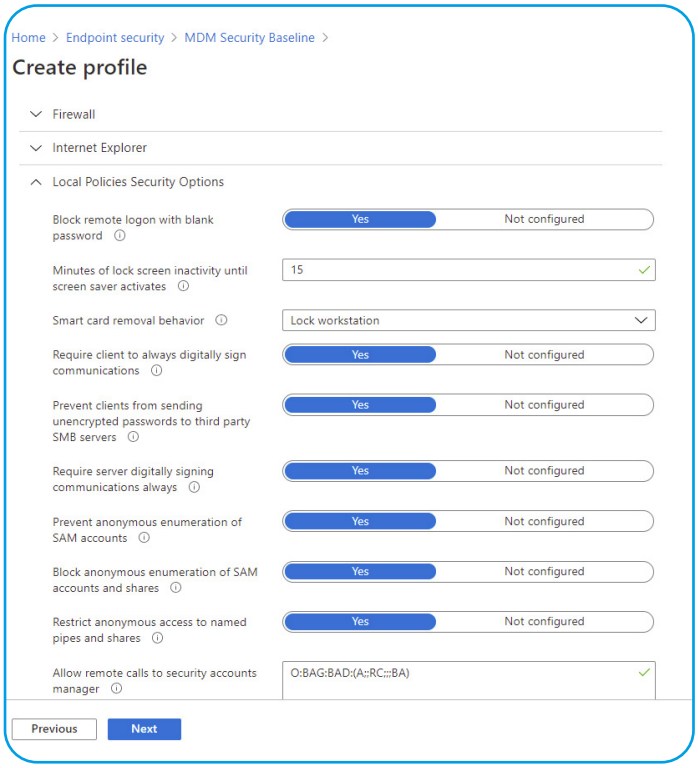
This less intrusive approach lets you create Mit diesem weniger eingreifenden Ansatz können Sie **App-Schutzrichtlinien** für bestimmte Anwendungen erstellen, wobei E-Mail das klassische Beispiel ist. Wenn Benutzer auf ihrem privaten Smartphone auf geschäftliche E-Mails zugreifen möchten, legen Sie Richtlinien fest, die vorsehen, dass sie nur Outlook (kostenlose mobile App für Android und iOS) und nicht die integrierten Mail-Apps verwenden können. Außerdem können Sie Unternehmensdaten schützen, so dass ein Benutzer keine geschäftlichen Daten in eine nicht geschäftliche App (persönliche E-Mail-App usw.) kopieren kann. Wenn das Gerät verloren geht oder gestohlen wird, können Sie die Unternehmensdaten löschen, während persönliche Fotos usw. unangetastet bleiben.

**Die Entscheidung zwischen MDM und MAM** hängt von vielen Faktoren ab, z.B. von Ihrer Nutzerbasis, Ihren Arbeitsverträgen, Ihren Geschäfts- und Sicherheitsanforderungen und vielem mehr. Nehmen Sie sich in der **Planungsphase** etwas Zeit, um die richtige Entscheidung zu treffen.

Ein weiterer Teil der Verwaltung mobiler Anwendungen könnte darin bestehen, sie sicher mit on-premises Ressourcen zu verbinden.

Microsoft bietet jetzt sein eigenes VPN für iOS und Android namens **Tunnel** an - und es ist in den Microsoft Defender for Endpoint integriert.






*MDM Security Baseline*

## 13.3: MICROSOFT CONFIGURATION MANAGER

Wenn Sie MCM on-premises eingesetzt haben, um Ihre Server und herkömmlichen Client-PCs zu verwalten, können Sie Intune **über Co-Management** in Ihren Verwaltungsablauf integrieren, um das Beste aus beiden Welten zu nutzen und Ihre Umgebung auf eine schrittweise Migration zur Cloud-Verwaltung vorzubereiten. Verwechseln Sie dies nicht mit **Hybrid MDM**, dem älteren, veralteten Ansatz zur Verbindung von SCCM und Intune.

## 13.4: INTUNE SUITE

Wie es sich für Microsoft gehört, gibt es **Add-Ons für Intune,** die Sie für Ihr Unternehmen in Betracht ziehen können, um bestimmte Aufgaben zu lösen. Es gibt eigenständige Add-ons, einen Intune P2-Plan und die komplette Intune Suite, die Folgendes umfasst: **Erweiterte Endpunktanalysen** zur Nachverfolgung und Optimierung der Benutzererfahrung, **Endpoint Privilege Management**, mit dem Endbenutzer bestimmte administrative Aufgaben auf ihrem Windows-Gerät durchführen können, ohne ein lokaler Administrator zu sein, und **Microsoft Tunnel for MAM**, das die VPN-Funktion für Android- und iOS-Apps auf MAM ausweitet. Außerdem gibt es die **Remotehilfe**, die es dem Supportteam auf sichere Weise ermöglicht, auf den Bildschirm der Mitarbeiter zuzugreifen, um sie zu unterstützen, sowie **das Verwalten von Spezialgeräten** wie AR/VR-Headsets und große Smart-Screen-Geräte.

TEIL 3

# SECURITY, BACKUP & COMPLIANCE

MICROSOFT 365
DER ULTIMATIVE LEITFADEN

# KAPITEL 14:

# SECURITY IN O365

**IN DEN ANFÄNGEN DES CLOUD COMPUTING GAB ES VIELE BEDENKEN HINSICHTLICH DER SECURITY VON DATEN, DIE IN EIN "FREMDES RECHENZENTRUM" AUSGELAGERT WURDEN. ICH DENKE, DEN MEISTEN CISOS IST HEUTE KLAR, DASS DIE GROSSEN ANBIETER EINE VIEL BESSERE ARBEIT IN SACHEN IT SECURITY LEISTEN, ALS DIE MEISTEN UNTERNEHMEN ES TUN KÖNNEN (ODER DAS BUDGET DAFÜR HABEN). SIE HABEN AUCH EIN STARKES INTERESSE DARAN, DENN EIN GROSSER SICHERHEITSVORFALL KÖNNTE VIELE TAUSENDE VON UNTERNEHMEN BETREFFEN. DESHALB GEBEN SIE VIEL GELD AUS, UM SICHERZUSTELLEN, DASS IHRE CLOUDS SO SICHER WIE MÖGLICH SIND.**

Das bedeutet jedoch nicht, dass Sie alles Microsoft überlassen können. Es gibt ein sogenanntes **Modell „der geteilten Verantwortung"** - andere Cloud-Anbieter haben ähnliche Ansätze. Es gibt einige Bereiche, für die Sie nach wie vor verantwortlich sind, z.B. die Endpunkte, die Ihre Benutzer für den Zugriff auf Cloud Services verwenden, jede on-premises Infrastruktur, die in einem Hybridmodus mit O365 betrieben wird, sowie die Bereitstellung und das Entfernen der Benutzer. Es gibt auch viele Sicherheitsvorgaben in O365, die Sie an Ihr Unternehmen anpassen müssen, wobei Sie und Microsoft die Verantwortung für die Sicherheit gemeinsam tragen. In diesem Kapitel befassen wir uns mit diesen Steuerelementen und damit, wo und wie Sie sie konfigurieren.

Die Grundlage für die Denkweise über Sicherheit sollte Zero Trust sein. Anstatt einer Verbindung zu vertrauen, je nachdem, woher sie kommt ("wenn sie aus dem internen LAN kommt, ist sie sicher, von außen ist sie gefährlich"), wird jeder Zugriff anhand Ihrer Regeln für bedingten Zugriff überprüft, was Ihnen eine viel bessere Sicherheitslage bietet. Und stützen Sie Ihre Security auf die Identität, die die neue Firewall darstellt, und **halten Sie mit den neuen Funktionen im Bereich Security Schritt.**



Wenn Sie darüber nachdenken, wie Sie Ihre Systeme schützen können, sollten Sie nicht vergessen, dass die Angreifer ebenso **von on-premises in die Cloud wechseln**, wie wir es beim **Solarwinds-Einbruch** gesehen haben. Wenn Sie über eine M365 E5-Lizenz verfügen, können Sie mit Hilfe von Angriffssimulationen Ihre Benutzer mit vorgetäuschten Phishing-E-Mails testen und ihnen je nach ihrer Neigung, darauf hereinzufallen, automatisch ein maßgeschneidertes Training anbieten. Wenn Sie mehr Kontrolle und Optimierung wünschen, sollten Sie den **Security Awareness Service** von Hornetsecurity ausprobieren, der vollautomatisches Benchmarking, Spear-Phishing-Simulationen und E-Training bietet, um Ihre Mitarbeiter für Cyber-Bedrohungen zu sensibilisieren und zu schützen.

Denken Sie auch an Entra ID Premium P1 & P2, die Sie als Add-Ons zu O365 erwerben können (in M365 enthalten). Wir haben ihre Security-Features in Kapitel 7 behandelt.

Man könnte argumentieren, dass es einen Interessenkonflikt darstellt, wenn man sich darauf verlässt, dass Microsoft einerseits die Plattform (Office 365) bereitstellt als auch extra Geld für erweiterte Security-Funktionen aus demselben Haus verlangt. Schließlich könnte Microsoft mehr Security-Funktionen in die Basisplattform integrieren (z.B. Office 365 E3 und Microsoft 365 E3), anstatt dafür extra bezahlen zu müssen. Daher entscheiden sich viele Unternehmen für einen Dienst eines Drittanbieters für fortschrittliche Security Services zusätzlich zur Basisplattform, wie z.B. **365 Total Protection** von Hornetsecurity.

## 14.1: 365 TOTAL PROTECTION

**365 Total Protection** ist eine Cloud-basierte Sicherheitslösung, die alle wesentlichen Aspekte des Microsoft 365 Security Managements und des Datenschutzes eines Unternehmens abdeckt: E-Mail-Sicherheit, Backup und Wiederherstellung, Compliance, Rechteverwaltung und Security Awareness. Die Lösung wurde speziell für Microsoft 365 entwickelt und erfordert keine Hardware, Software oder Wartung. Gleichzeitig bietet sie die dringend benötigten zusätzlichen Sicherheits- und Datenschutzschichten gegen Spam, Malware und fortschrittliche Bedrohungen.

365 Total Protection von Hornetsecurity ist in vier verschiedenen Plänen erhältlich:

- **Plan 1: 365 Total Protection Business** bietet Ihnen erstklassige E-Mail Security, Schutz vor Spam und Malware, Signaturen und verschlüsselte E-Mails.
- **Plan 2: 365 Total Protection Enterprise** bietet zusätzlich E-Mail-Archivierung, 10-jährige Aufbewahrung, eDiscovery, Advanced Threat Protection (ATP) samt Sandboxing verdächtiger E-Mails, URL-Scanning, QR Code Analyzer
- **Plan 3: 365 Total Protection Enterprise Backup** fügt ein automatisches Backup von Postfächern, Teams, OneDrive und SharePoint hinzu und bietet eine einfache Wiederherstellung. Zusätzlich ermöglicht die Lösung die Sicherung und Wiederherstellung von Windows-Endpunkten.
- **Plan 4: 365 Total Protection Compliance & Awareness** erweitert das Angebot um Permission Manager, Security Awareness Service und AI Recipient Validation.

Diese breite Palette an Microsoft 365 Sicherheits- und Compliance-Funktionen ist **in einem Paket und in einer Lizenz** erhältlich.

## 14.2: 365 PERMISSION MANAGER

Eine der drei Säulen von Zero Trust, nämlich die Anwendung des Zugriffs mit den geringsten Rechten (englisch: least-privilege access), ist im großen Maßstab bemerkenswert schwer zu erreichen. Besonders deutlich wird dies bei SharePoint und OneDrive, wo Sie nicht nur eine komplexe Reihe von sich überschneidenden Berechtigungsoptionen haben, sondern auch die gemeinsame Nutzung von Dateien und Sites mit externen Benutzern, entweder über SharePoint, OneDrive und jetzt auch häufig über Teams.

Die Inventarisierung all dieser erteilten Berechtigungen und die Erstellung von Berichten darüber erfordert das Durchsuchen mehrerer Seiten oder die Ausführung von PowerShell-Skripten. Es gibt auch keine einfache Möglichkeit, Zugriffsrechte zu beschränken, wenn sie zu weit gefasst sind, und es gibt auch keine schnelle Möglichkeit, Zugriffsrechte schnell für alle Sites zu entziehen, wenn z.B. festgestellt wird, dass ein Benutzerkonto kompromittiert worden ist.

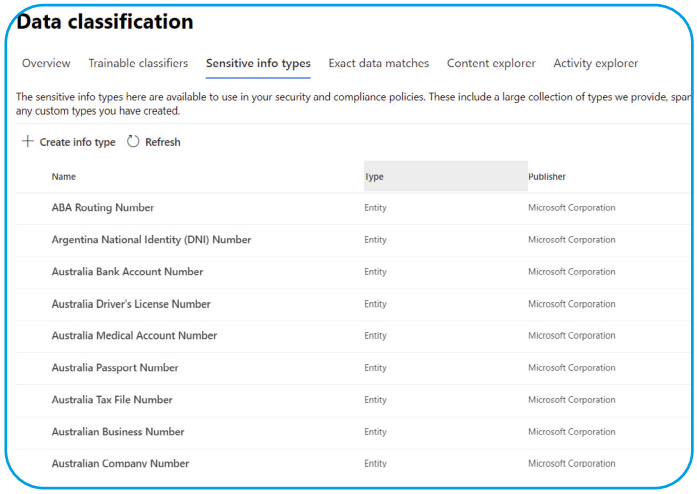
Der **365 Permission Manager,** ein einzigartiges Produkt von Hornetsecurity, beseitigt all diese Probleme und noch mehr. Ein zentrales Dashboard zeigt Ihnen alle Ihre Sites und deren Übereinstimmung mit Ihren Freigabe-Richtlinien. Um Berechtigungen anzupassen, verwenden Sie die einfache Schaltfläche Korrigieren, oder im Falle einer echten Geschäftsanforderung für eine Ausnahme von der Richtlinie, genehmigen Sie einen Sonderfall. Integrierte oder benutzerdefinierte Richtlinien, die die externe oder interne Freigabe und die damit verbundenen Einstellungen steuern, können auf einzelne SharePoint Sites oder OneDrive-Speicherorte angewendet werden, was die Governance und das Risikomanagement erheblich verbessert.

Sie können auch die Berechtigungen in SharePoint, OneDrive und Teams für einen ausgewählten Benutzer einsehen, was sehr nützlich ist, wenn Sie eine Kontokompromittierung vermuten, oder vielleicht im Falle einer Untersuchung von Insiderrisiken.

Eine weitere sehr nützliche Funktion sind Quick Actions, mit denen Sie Massenoperationen durchführen können, um Berechtigungen zu verwalten und eine konforme SharePoint-, Teams- und OneDrive-Infrastruktur zu erhalten.

## 14.3: MICROSOFT PURVIEW INFORMATION PROTECTION

Alle Funktionen für Governance, Data Loss Prevention (DLP) und den Schutz von Informationen in M365 werden unter dem Dach von Purview zusammengefasst. Das Portal befindet sich unter **compliance.microsoft.com.**




*MDM Security Baseline*



Durch die Verwendung von **Vertraulichkeitsbezeichnungen (Labels) zur Klassifizierung von Daten** entweder manuell oder automatisch durch das Crawlen von Dokumenten oder E-Mails, können Sie beginnen, Ihre Geschäftsinformationen zu kontrollieren und zu überwachen. Sobald ein Dokument gelabelt wurde, können Sie es mit MIP oder OME schützen (siehe unten) oder den Zugriff auf Windows-Endpunkte über Richtlinien kontrollieren sowie den Zugriff in Office für Mac, Windows, iOS und Android verwalten.

## 14.4 : MICROSOFT INFORMATION PROTECTION

Eine der leistungsstärksten und am wenigsten genutzten Funktionen ist die Möglichkeit, Dokumente zu schützen, unabhängig davon, wo sie sich befinden. Bei der herkömmlichen Datei- bzw. SharePoint-Dokumentenfreigabe wird der Zugriff auf Serverebene streng kontrolliert. Sobald ein Dokument jedoch an eine andere Person gemailt oder auf einem USB-Laufwerk gespeichert wird, geht diese Kontrolle verloren.

Mit Microsoft Information Protection (MIP) können Sie Kennzeichnungen und Regeln einrichten, die Dokumente verschlüsseln und deren Benutzerzugriff mit sich führen, so dass unabhängig von der Art der Weitergabe nur die richtigen Personen Zugriff haben. Wenn Sie mit MIP beginnen, werden Sie den integrierten Client in den Office-Apps auf Windows, Mac, iOS und Android verwenden. Es ist wichtig, **Superuser-Konten** zu konfigurieren, damit Sie auf Dokumente zugreifen können, wenn ein Benutzer das Unternehmen verlässt. Die Liste der sensiblen Informationstypen (SITs) wird immer länger und es ist jetzt möglich, die Vertraulichkeitsstufen der Regeln anzupassen, die eingebauten Regeln zu kopieren und anzupassen und größere Stichwortwörterbücher zu erstellen (jede Erwähnung eines Mitarbeiterausweises oder einer Patientenaktennummer zu erfassen).

Es ist möglich, **geschützte Dokumente in Echtzeit gemeinsam zu bearbeiten** (mit AutoSave-Unterstützung!) und in größeren Implementierungen können Sie Variablen in MIP-Regeln verwenden, um die Markierung von Inhalten pro Anwendung zu erleichtern. Sie können Dokumente, SharePoint Online Sites, on-premises SharePoint und Dateifreigaben mit Kennzeichnungen (und optional mit Dokumentenverschlüsselung) versehen. Sie können auch Bilder mit **OCR (Optical Character Recognition)** scannen, um sensible Informationen in Screenshots und ähnlichem zu erfassen.

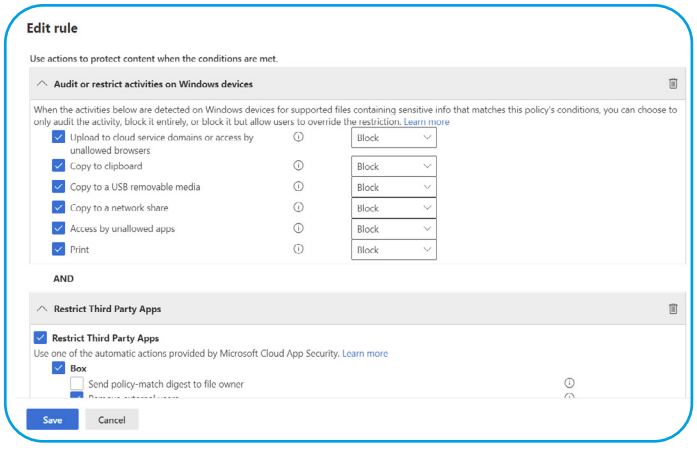
Vertraulichkeitskennzeichnungen sind jetzt auch für **SharePoint Sites, M365-Gruppen und Teams** verfügbar. Dies gilt nicht für die dort gespeicherten Inhalte, sondern verwaltet die Privatsphäre des Containers, den Zugriff externer Benutzer und kann auch in Richtlinien für bedingten Zugriff integriert werden, um z.B. den Zugriff von nicht verwalteten Geräten zu blockieren. Sie können jedoch eine **Standard-Vertraulichkeitskennzeichnung für eine SharePoint Site** konfigurieren.

## 14.5: OFFICE 365 NACHRICHTENVERSCHLÜSSELUNG

Ähnlich wie Sie mit MIP geschützte Dokumente mit jedermann teilen können, können Sie mit **O365 Nachrichtenverschlüsselung** E-Mails an jedermann senden und wissen, dass nur diese Person auf die E-Mail zugreifen kann. Wie bei MIP können Sie auch hier Regeln einrichten, damit E-Mails mit bestimmten Informationen (Kreditkartennummern, Sozialversicherungsnummern) automatisch verschlüsselt werden.

## 14.6: DATA LOSS PREVENTION

Das Ziel von **Data Loss Prevention (DLP)** ist es, Benutzern zu helfen, das Richtige zu tun, indem sie gewarnt werden, wenn sie im Begriff sind, sensible Daten über E-Mail, SharePoint Online, OD4B oder Teams weiterzugeben. Es kann auch in MIP integriert werden, da Microsoft die Vereinheitlichung der Kennzeichnung und des Schutzes in M365 weiter vorantreibt. Der DLP-Schutz wurde auf Windows 10 und 11 mit **Endpoint-DLP** ausgeweitet, das den Upload von Dokumenten mit sensiblen Inhalten in Cloud-Speicher, das Kopieren sensibler Informationen in die Zwischenablage, USB-Speicher, Netzwerkfreigaben oder das Drucken blockieren kann. Es gibt auch eine Erweiterung für Google Chrome, die den DLP-Schutz auf Browseraufgaben ausdehnt. DLP wurde auch auf **on-premises ausgeweitet**, indem der MIP-Scanner zum Auffinden sensibler Dokumente eingesetzt wird. Auch das Management von Warnungen für DLP-Verstöße wurde erheblich verbessert.

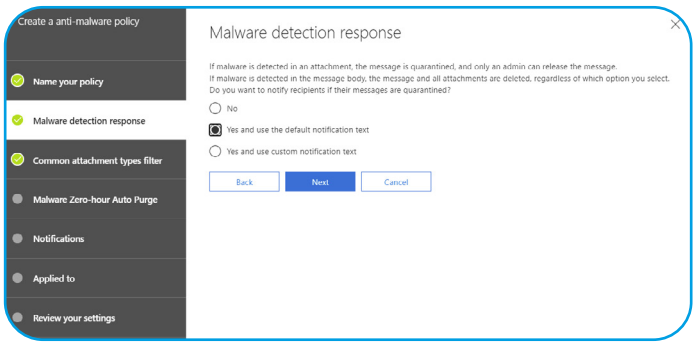



*Endpunkt DLP-Einstellungen*

## 14.7: EXCHANGE ONLINE PROTECTION

**Exchange Online Protection (EOP)** ist die E-Mail-Hygienelösung für Office 365 und kann auch Ihre on-premises Exchange-Postfächer schützen, wenn Sie sich in einer hybriden Bereitstellung befinden (Kapitel 8). Es gibt einige Einstellungen, die Sie für EOP steuern können, sowie einige zusätzliche Konfigurationen, die Sie für einen vollständigen Spamschutz in Betracht ziehen sollten, wie z.B. **Sender Policy Framework** (SPF), **Domain-based Message Authentication, Reporting, and Conformance** (DMARC) und **Domain Keys Identified Mail** (DKIM).

Wenn Sie feststellen, dass EOP nicht genug bösartige E-Mails abfängt, sollten Sie Services von Drittanbietern in Betracht ziehen. Hornetsecurity bietet ein kostenloses Tool namens **Threat Monitor** (das keine Änderungen an Ihren MX-Records erfordert), das Werbe-E-Mails (Spam), Bedrohungen und E-Mails mit fortschrittlichen Bedrohungen identifiziert und Sie diese aus den Postfächern der Benutzer löschen lässt. Threat Monitor liefert Ihrem Tenant wertvolle E-Mail-Statistiken darüber, was EOP fehlt, und erleichtert so die Entscheidung für ein Upgrade der E-Mail-Hygiene-Services.





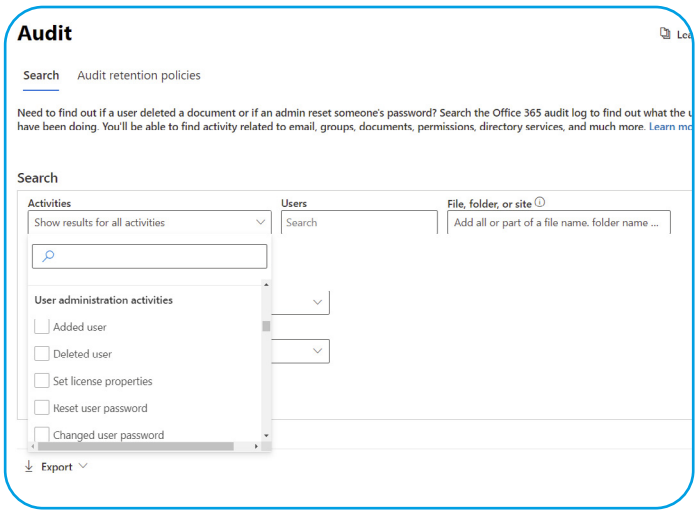
## 14.8: DEFENDER FOR OFFICE 365

Die Defender for O365-**Schutzfunktionen** (verfügbar in O365 E5 oder als eigenständiges Add-Ons) baut auf EOP auf und bietet Ihnen Sichere Anlagen, bei denen Anhänge in eingehenden E-Mails, die möglicherweise schadhaft sind, innerhalb einer VM geöffnet und überprüft werden, bevor sie an die Benutzer weitergeleitet werden. Sichere Links prüft, ob Links in E-Mails und Office-Dateien zu dem Zeitpunkt, an dem der Benutzer auf diese Links klickt, möglicherweise schadhaft sind. Anti-Phishing erkennt Versuche, sich für einen bestimmten Benutzer auszugeben. Diese Schutzmaßnahmen gelten auch für SharePoint, OD4B und Teams.

Wenn Ihnen der Defender for Office 365 zu teuer ist (er ist in M365 E5, E5 Security oder als separates Add-On enthalten), sollten Sie sich Hornetsecurity's **365 Total Protection** ansehen, das es in einer Business- und einer Enterprise-Version gibt. Business bietet Ihnen eine detaillierte Kontrolle über E-Mail-Kategorien und -Inhalte, so dass Sie unerwünschte E-Mails blockieren können. Sie können E-Mail-Signaturen mit Haftungsausschlüssen (Disclaimer) des Unternehmens festlegen und entweder PGP oder S/MIME für die E-Mail-Verschlüsselung verwenden, wobei die Handhabung von Zertifikaten integriert ist. Die Enterprise-Version bietet zusätzlich E-Mail-Archivierung/Journaling mit einer Aufbewahrungsfrist von bis zu 10 Jahren, eDiscovery und Sandbox-Analyse von Anhängen, URL-Rewriting und Scanning (sowohl in E-Mails als auch in Anhängen) und Contingency-Notfallabsicherung durch eine E-Mail-Failover-Umgebung, falls der Dienst von Microsoft 365 nicht verfügbar ist.

## 14.9: AUDITING

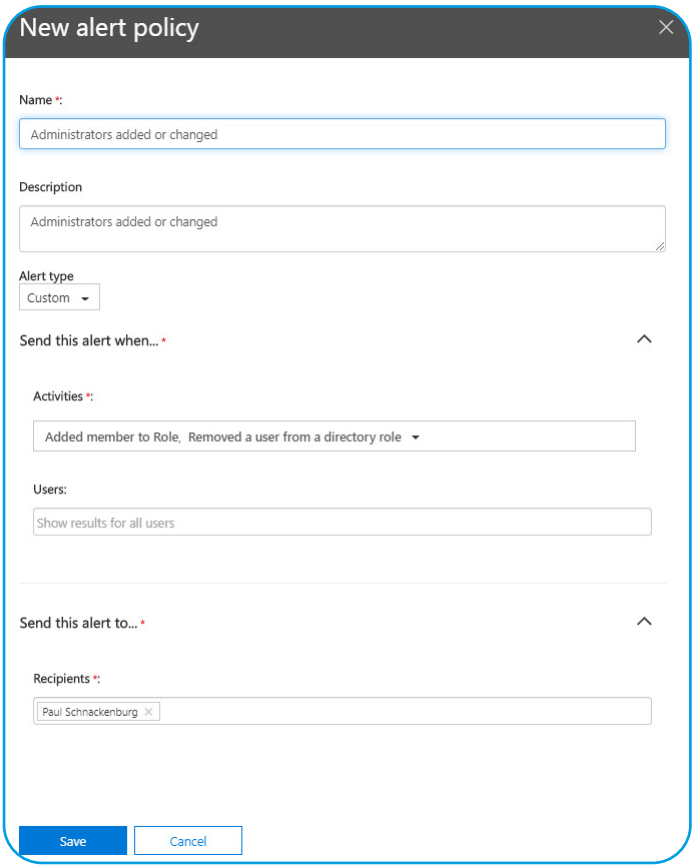
Eine der großartigen Funktionen der einheitlichen Plattform von O365 ist die Möglichkeit zur **Überwachung der Aktionen von Benutzern und Administratoren** auf der gesamten Plattform.



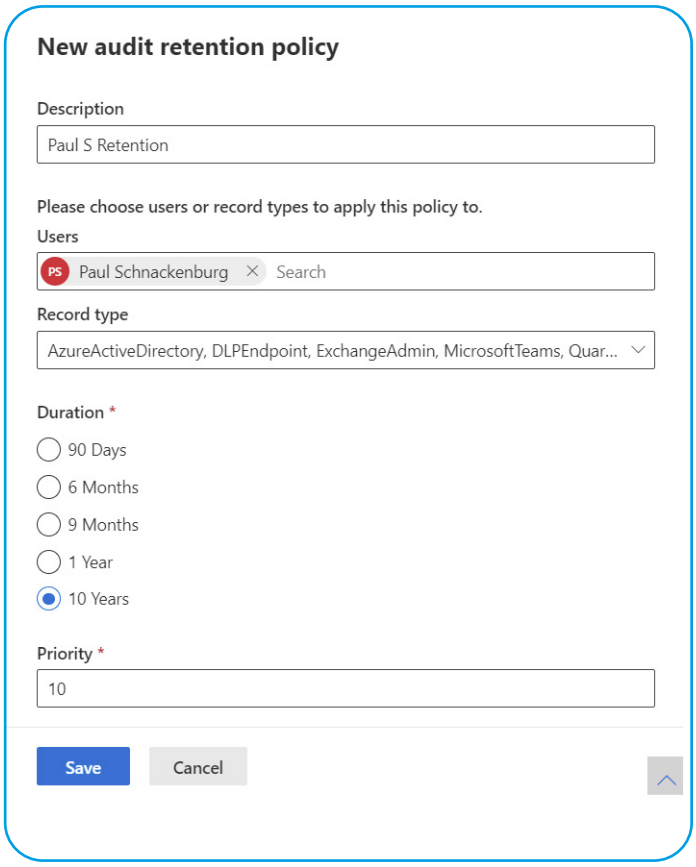

*Such-Funktion im Audit-Log*

Sie sollten zumindest die **Aktivitätswarnungen** für Entra ID konfigurieren. Gehen Sie zum Compliance-Portal - Suche - Audit Log (Überwachungsprotokollierung) Suche und sehen Sie sich all die verschiedenen Aktivitäten an, die Sie überwachen und über die Sie Berichte erhalten können, sowie **Warnrichtlinien erstellen** können.






*Erstellen von Warnrichtlinien*




*Richtlinie zur Aufbewahrung von Audits*

Standardmäßig werden Office 365 Audit-Logs 180 Tage lang aufbewahrt (Entra ID-Logs 30 Tage lang), was für Ihr Unternehmen oder die von Ihnen einzuhaltenden Vorschriften möglicherweise nicht ausreicht. Sie haben zwei Möglichkeiten: Nutzen Sie einen Service eines Drittanbieters, um die Protokolle kontinuierlich zu exportieren und für den von Ihnen gewünschten Zeitraum zu archivieren, oder weisen Sie den Benutzern, deren Protokolle Sie länger aufbewahren möchten, M365 E5 (oder M365 E5 Compliance / Discovery & Audit) Lizenzen zu. Damit können Sie die Protokolle für 1 oder 10 Jahre aufbewahren.

## 14.10: SAGEN SIE KENNWÖRTERN LEBEWOHL?

Die beste Art, Kennwörter zu verwalten, ist, erst gar keine zu verwenden oder im Verzeichnis zu speichern - das nennt man „kennwortlos". Es gibt **viele Wege zu diesem Ziel**. Heute können Sie die Authenticator App verwenden, um sich bei einem Azure AD-Konto anzumelden (nicht als zweiter Faktor, sondern als einziger Faktor), oder Windows Hello for Business oder einen FIDO 2 Hardware-USB/NFC-Schlüssel.

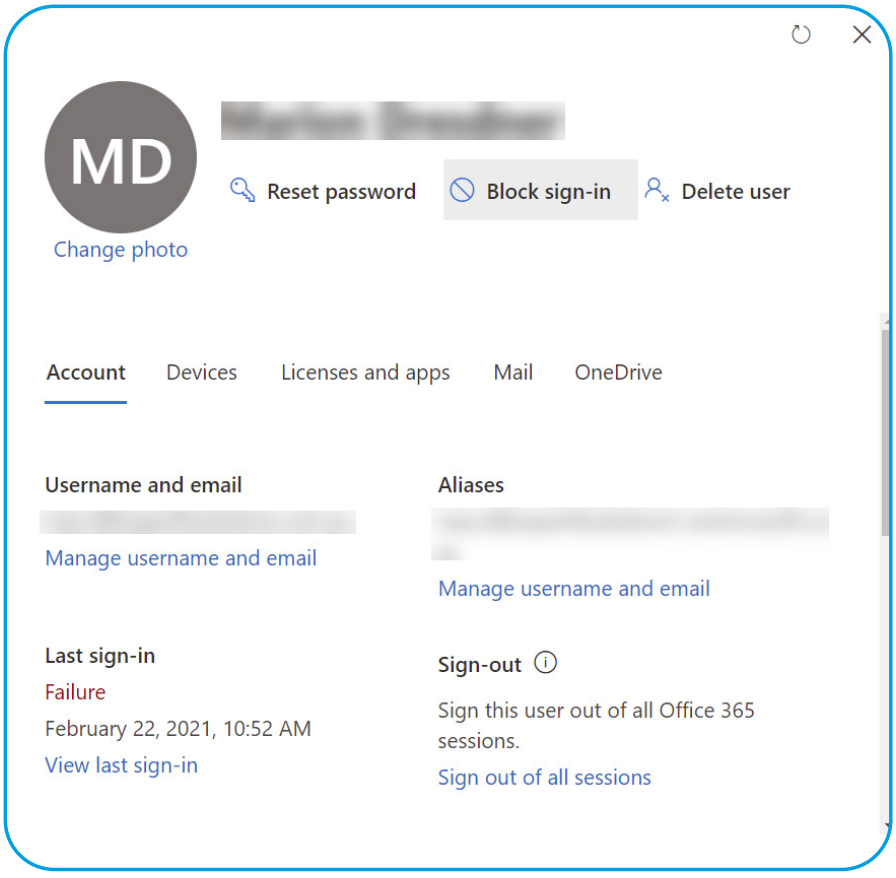
Bis dahin können Sie den **Kennwortschutz** aktivieren, um häufig verwendete Kennwörter zu unterbinden (2000 in einer von Microsoft gepflegten Liste plus bis zu 1000 benutzerdefinierte Wörter, die in Ihrem

Unternehmen/Ihrer Stadt/Ihrem Lieblings-Sportverein üblich sind). Dies funktioniert nahtlos für reine Cloud-Konten und kann **leicht auf on-premises AD ausgeweitet werden**. Wenn Sie von Ihren Benutzern verlangen, dass sie sich für MFA registrieren, werden sie auch **gleichzeitig für den Self-Service zur Kennwortrücksetzung** registriert.

### 14.11: ZUGRIFF FÜR BENUTZER SPERREN

Wenn Sie vermuten oder feststellen, dass ein Benutzer-Konto kompromittiert wurde, sollte der erste Schritt darin bestehen, die Anmeldung für das Konto im Admin Center zu deaktivieren.

Sie sollten sich jedoch darüber im Klaren sein, dass der Benutzer (oder ein Angreifer) nicht sofort von den Diensten abgemeldet wird, auf die er zugreift, und dass es aufgrund der Lebensdauer von Aktualisierungs-Tokens bis zu einer Stunde dauern kann, bis die Sperre wirksam wird. Die Lösung für dieses Problem ist die **fortlaufende Zugriffsevaluierung**, die derzeit nur für Exchange, Teams und SharePoint Online-Konnektivität gilt und den Zugriff nahezu in Echtzeit sperrt (gelegentlich mit einer Latenz von bis zu 15 Minuten aufgrund der Ereignisübermittlung).




*Block sign-in for a user account*

# KAPITEL 15:

# SECURITY IN MICROSOFT 365

**IN DER O365 PLATTFORM SIND VIELE SECURITY-TOOLS BEREITS ENTHALTEN, ABER WENN SIE AUF M365 E3 ODER E5 UMSTELLEN, ERSCHLIESSEN SIE SICH EINE GANZE REIHE NEUER, FORTSCHRITTLICHER FUNKTIONEN ZUR ABSICHERUNG IHRES UNTERNEHMENS. IN DIESEM KAPITEL WERDEN WIR UNS DIESE TOOLS ANSEHEN, MIT AUSNAHME VON ENDPOINT MANAGER, DEN WIR IM NÄCHSTEN KAPITEL BEHANDELN, UND WINDOWS 11, DAS WIR IN KAPITEL 6 BEHANDELT HABEN.**

### 15.1: MICROSOFT 365 DEFENDER

Fast alle auf M365 ausgerichteten Sicherheitsprodukte von Microsoft tragen die Marke Defender, und die zentrale Konsole dafür ist **security.microsoft.com**. Hier finden Sie einen umfassenden Extended Detection and Response (XDR) Service, der Daten von E-Mails, Identitäten, Endpunkten und Cloud-Diensten sammelt und Sie vor Eindringlingen in Ihrem gesamten digitalen M365-System warnt.



Hier finden Sie eine Übersicht über die verschiedenen Defender Services:

- **Microsoft Defender for Office 365** – Bietet Schutz für E-Mails, SharePoint Sites, OD4B und Teams
- **Microsoft Defender for Identity** – Es überwacht Ihr on-premises Active Directory (AD), lässt sich in Ihr SIEM-Tool (Security Information and Events Management) integrieren und warnt Sie vor Kontoverletzungen, Lateral-Movement-Attacken und Angriffen auf AD.
- **Microsoft Defender for Endpoint** – Zentrale Verwaltung von Anti-Malware auf allen Endgeräten in Ihrer Umgebung (Windows, Linux, macOS, Android und iOS)
- **Microsoft Defender for Cloud Apps** – Ein Cloud App Security Broker (CASB) zur **Verwaltung des Sicherheitsstatus für SaaS-Apps.**

Microsoft bietet außerdem Microsoft Sentinel - ein cloudbasiertes SIEM; Microsoft Defender for Cloud (für Azure, AWS und GCP IaaS und PaaS Workloads) und Entra für Identitätsmanagement und Schutz.

## 15.2: MICROSOFT DEFENDER FOR ENDPOINT

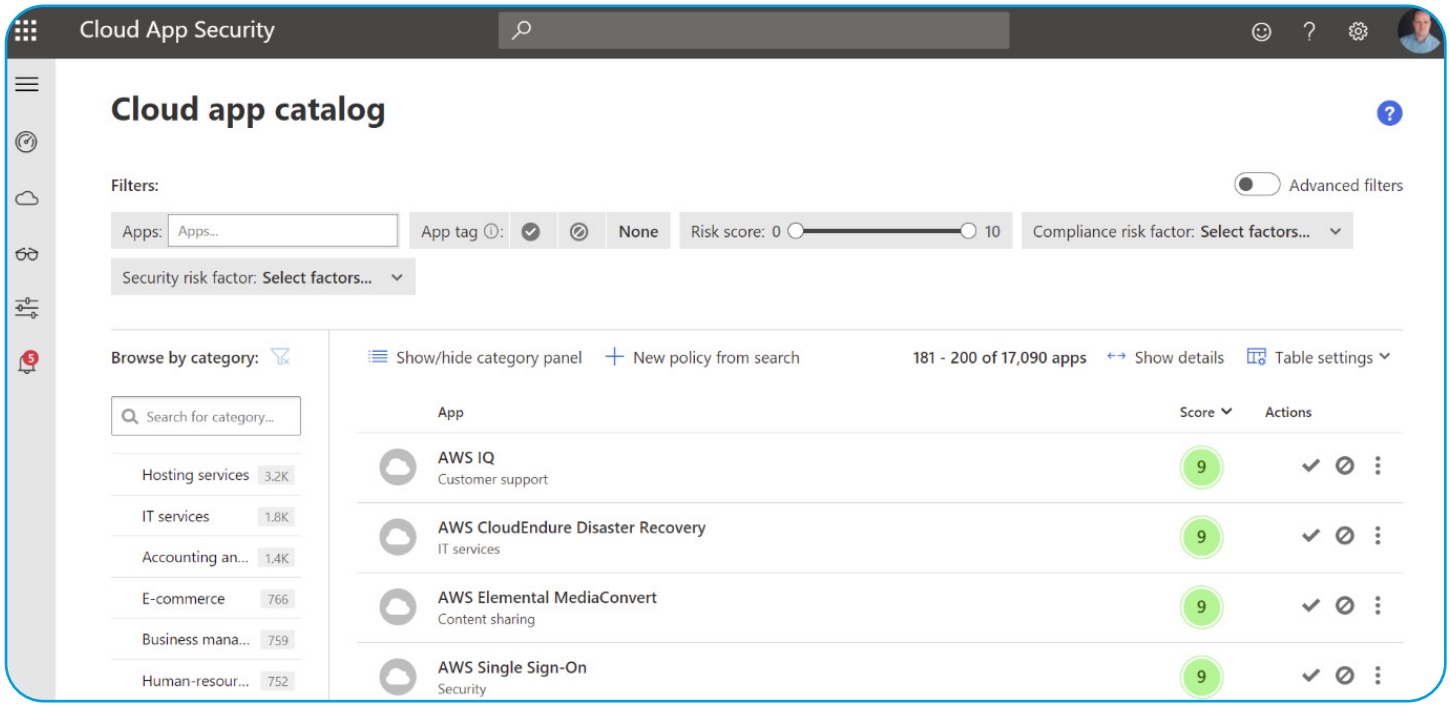
**Microsoft Defender for Endpoint (MDE)** ist eine umfassende Sicherheitslösung für Endpoint Detection and Response (EDR), die Verhaltensanalysen mit maschinellem Lernen (ML) für Windows, MacOS, Linux-Server, iOS- und Android-Geräte nutzt. Sie inventarisiert die installierten Anwendungen (Windows und MacOS) und ermittelt über **Threat and Vulnerability Management (TVM)**, welche Anwendungen die größten Risiken für Ihr Unternehmen darstellen. MDE bietet außerdem **Funktionen zur Verringerung der Angriffsfläche** und **Next-Generation-Protection** sowie viele weitere Security-Funktionen. MDE ist mit M365 E5 / E5 Security oder als eigenständige Lizenz erhältlich.

## 15.3: MICROSOFT DEFENDER FOR IDENTITY

Mit M365 E5 können Sie auf **Defender for Identity** (MDI) aufstocken, der Ihre Active Directory Domain Controller und Ihre Active Directory Federation Server mit „schlanken" Agenten überwacht, der Rest wird vom Cloud Service übernommen. Jeder Angreifer, der auf einem Gerät in Ihrem Netzwerk Fuß fasst, muss zunächst Zugang zu AD bekommen, um Seitwärtsbewegungen zur Erweiterung seiner Privilegien unternehmen zu können - MDI würde ihn dabei erwischen.

## 15.4: MICROSOFT DEFENDER FOR CLOUD APPS

Früher, als Ihre Benutzer noch im Firmenbüro blieben, war alles, was Sie zu ihrem Schutz brauchten, eine gute Firewall. Aber in der heutigen Welt des "Arbeitens von überall aus, auf jedem Gerät" brauchen Sie eine neue Art von Tool, um sie zu schützen, einen Cloud Access Security Broker. Microsoft Defender for Cloud Apps (MDA) ist Teil von M365 E5 und schützt Ihre Benutzer in Echtzeit, wenn sie auf Cloud Services zugreifen. Der Katalog mit über 31.000 verschiedenen Cloud Services bietet der IT-Abteilung die Möglichkeit, Schatten-IT (Cloud Services, die Benutzer ohne Wissen der IT-Abteilung nutzen) in Ihrer gesamten Benutzerbasis zu entdecken und zu verwalten.



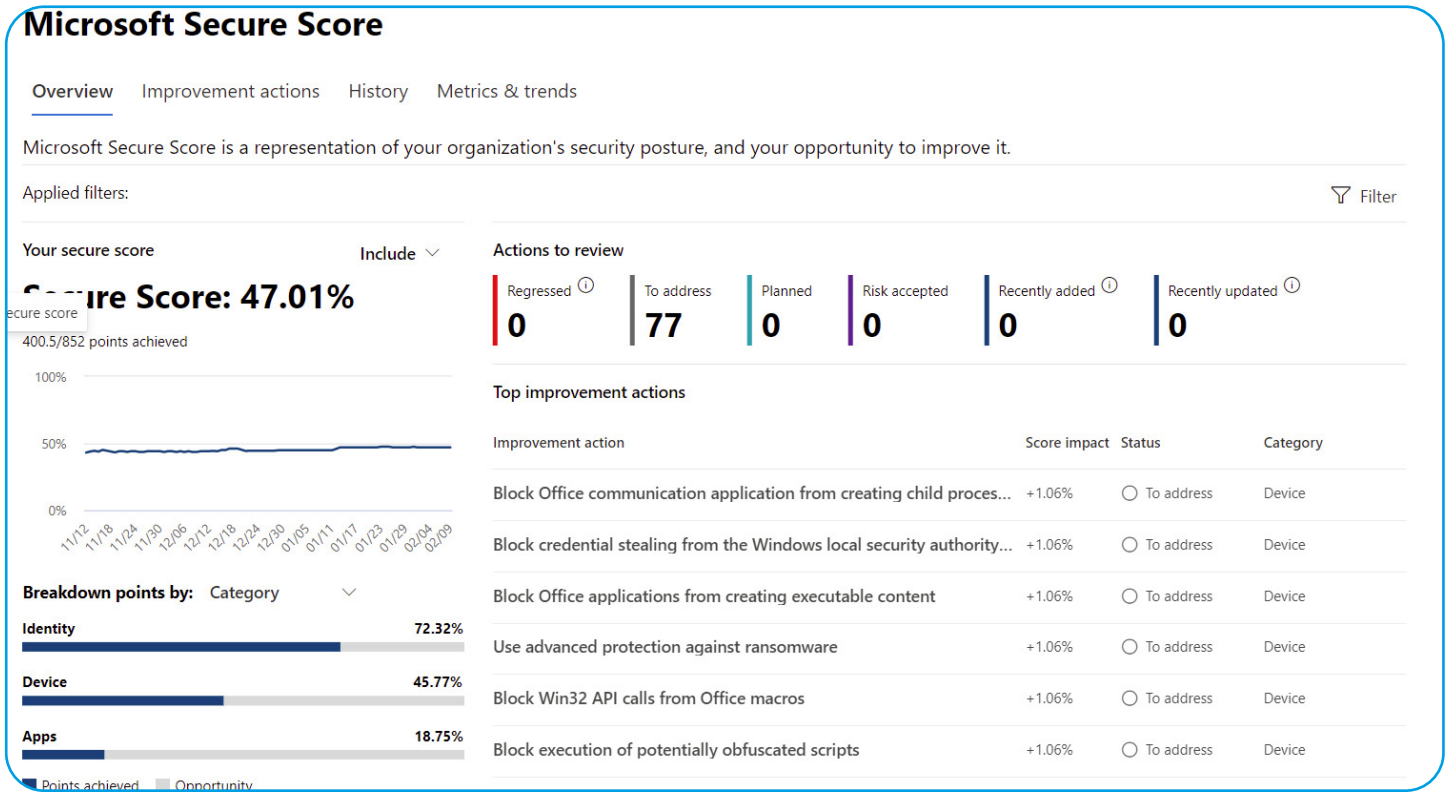

*Cloud App Security SaaS-Katalog*

## 15.5: SECURE SCORE

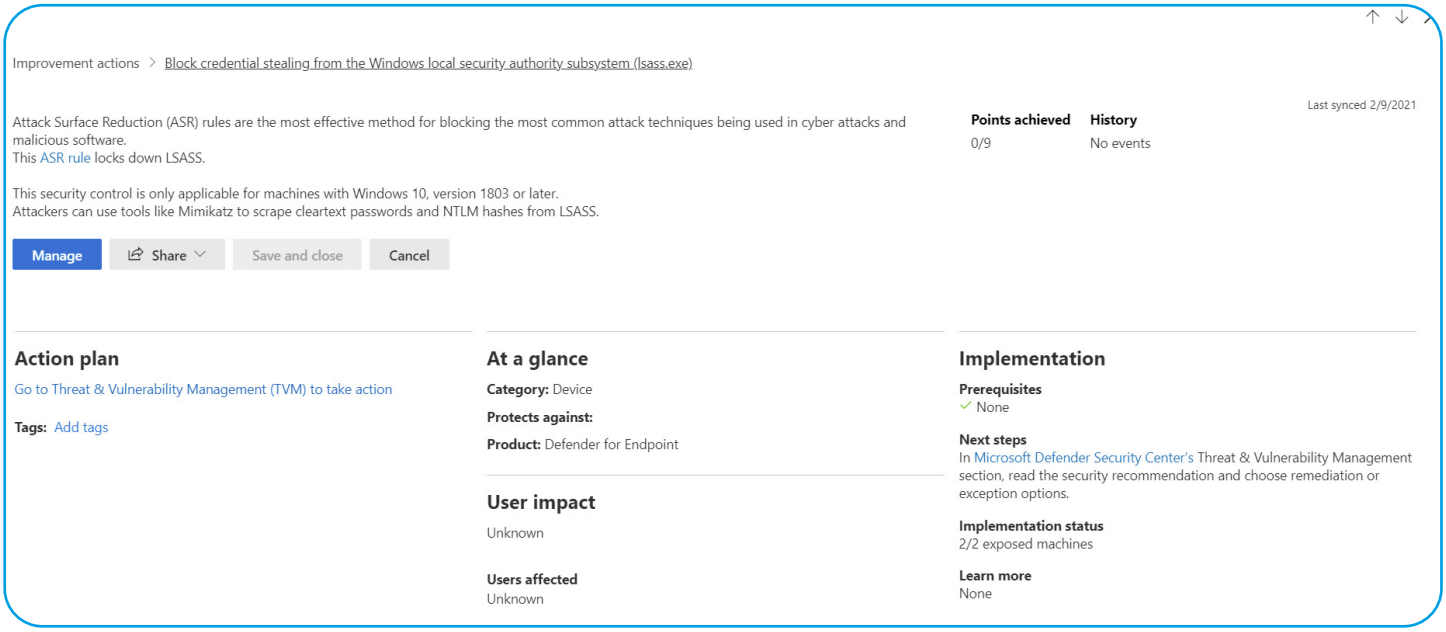
Im letzten und in diesem Kapitel haben wir uns viele der Sicherheitseinstellungen angesehen, die Sie verwenden können. Aber wo fangen Sie an? Woher wissen Sie, was am wichtigsten ist und worauf Sie achten müssen? Und wo in all den verschiedenen Portalen (oder in der PowerShell) müssen Sie die einzelnen Einstellungen konfigurieren?

Die Antworten auf diese Fragen finden Sie im Secure Score (Sicherheitsbewertung), der jetzt Teil des **Security Portals** ist. Hier sehen Sie einen Gesamtbewertung für Ihren Tenant (für Identitäts-/Daten-/Geräte-/Apps- und Infrastruktur-Kontrollsysteme) und können ihn mit dem globalen Durchschnitt von M365, dem Durchschnitt Ihrer Branche und von Unternehmen derselben Größe vergleichen. Auf der zweiten Registerkarte sehen Sie, welche Maßnahmen Sie ergreifen sollten, um Ihren Score zu verbessern, wie viele Punkte Ihnen jede Maßnahme einbringt und welche Auswirkungen auf die Benutzer und den Verwaltungsaufwand zu erwarten sind.

Wenn Sie auf eine Aktion klicken, erhalten Sie Details darüber, welche Risiken die Maßnahme abmildert, welcher Compliance-Vorschrift sie entspricht, die Möglichkeit, direkt zu der entsprechenden Stelle für die Konfiguration zu gelangen und die Option, dem System mitzuteilen, dass Sie dieses Risiko bereits mit einem Service eines Drittanbieters vermindert haben.



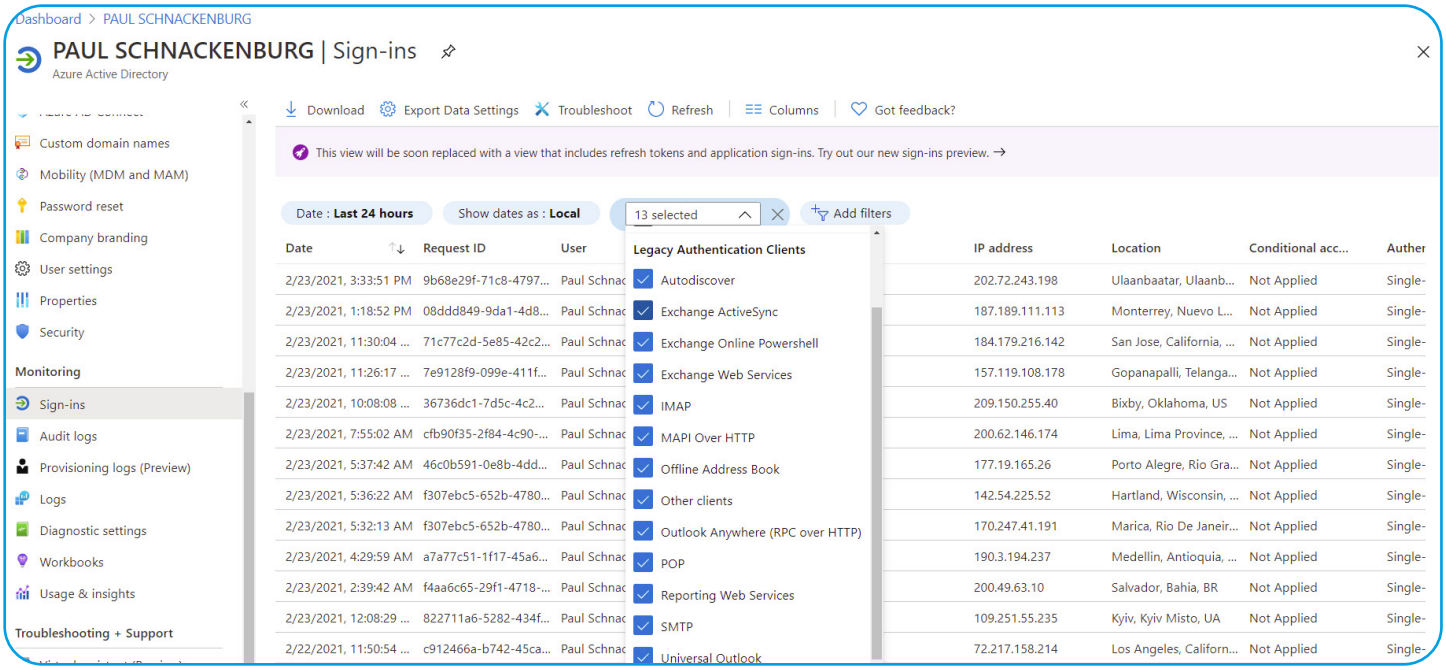

*Secure Score Überblick*




*Ein Beispiel für Maßnahmen zur Verbesserung Ihrer Security*

Je mehr Sicherheitsmaßnahmen Sie implementieren, desto höher wird Ihr Score (das kann 24-48 Stunden dauern), und Sie können Ihre Fortschritte auf der Registerkarte Verlauf verfolgen. Secure Score ist der BESTE Ort, um mit der Verbesserung der Security Ihres Tenants zu beginnen.

Ich möchte noch eine weitere Maßnahme (abgesehen von MFA) hervorheben, die Ihnen einen schnellen Erfolg bei der Verbesserung der allgemeinen Sicherheit bringt - die **Blockierung der Legacy-Authentifizierung**. Denn selbst wenn Sie MFA aktiviert haben, können Angreifer immer noch mit einem Benutzernamen und einem Kennwort über ältere Protokolle, die MFA nicht unterstützen, auf die Konten Ihrer Benutzer zugreifen. Um zu untersuchen, ob es legitime Verbindungen gibt, die diese älteren Protokolle verwenden (die aktualisiert oder von Ihrer Richtlinie zum Blockieren der Legacy-Authentifizierung ausgenommen werden müssen), gehen Sie zum Azure AD-Portal, klicken Sie unter Überwachung auf Anmeldungen, klicken Sie auf Filter hinzufügen, wählen Sie Client-App, klicken Sie dann auf "Keine ausgewählt" und fügen Sie alle 13 Legacy-Verbindungsoptionen hinzu.



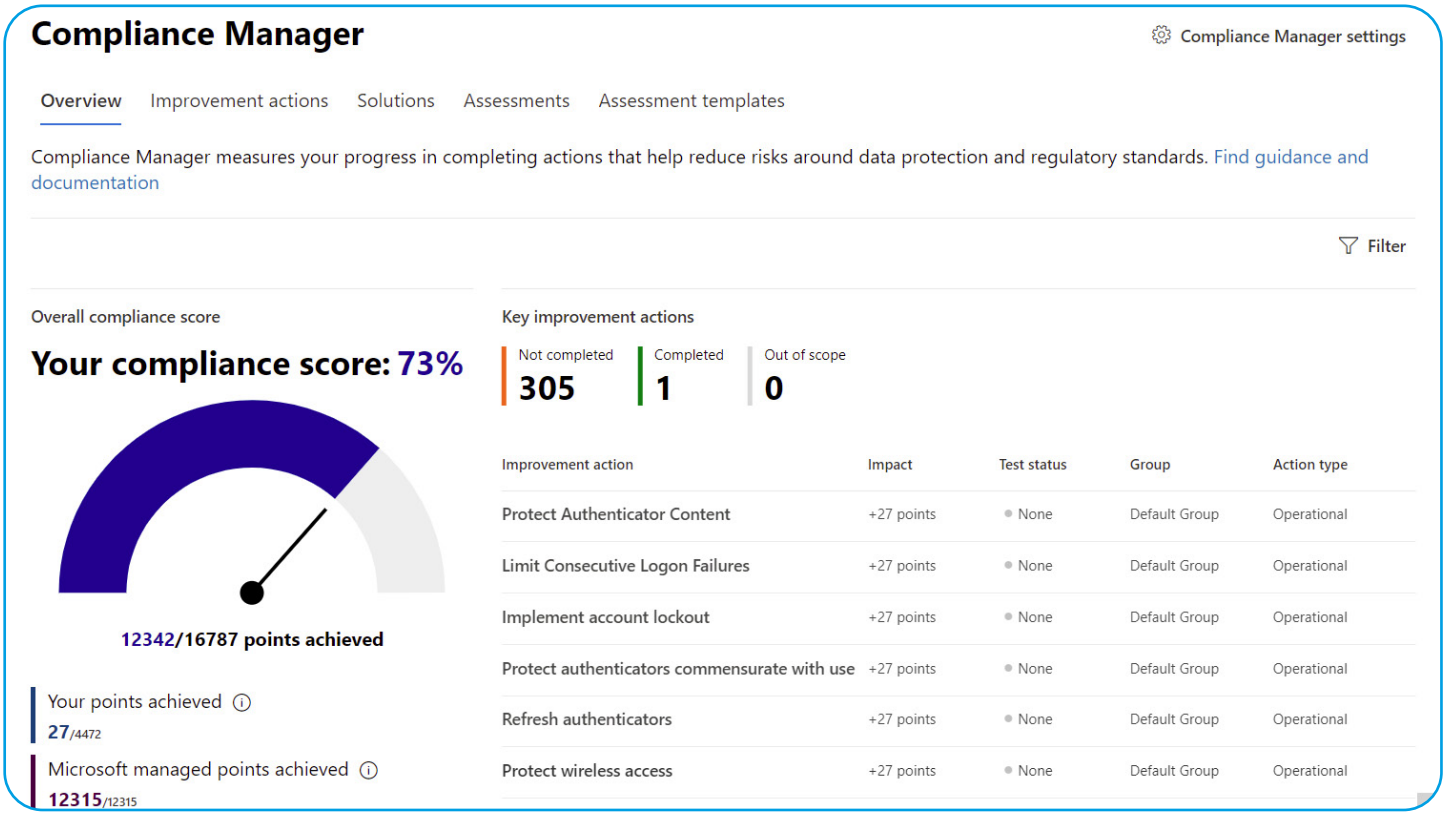

*Entra ID Anmeldeversuche mit Legacy-Authentifizierung*

Hier sehen Sie einen Tenant mit aktivierter MFA, aber noch aktivierter Legacy-Authentifizierung mit zahlreichen fehlgeschlagenen Zugriffsversuchen.

Wenn Sie sicher sind, dass es keinen legitimen Bedarf für die Legacy-Authentifizierung gibt, verwenden Sie **CA-Richtlinien, um sie zu blockieren**.

Das Konzept des Secure Score hat sich auch auf andere Teile von M365 ausgeweitet. Im **Compliance Manager** gibt es den Compliance Score, der anzeigt, wie konform Ihr Unternehmen mit regulatorischen Rahmenwerken ist, die Sie einhalten müssen.

Microsoft hat vor kurzem Hunderte von zusätzlichen Vorschriften aus der ganzen Welt hinzugefügt, um Ihnen zu helfen, Ihre Compliance zu überblicken und Benutzern Aufgaben zuzuweisen, um die Compliance zu erreichen und zu halten.




*Compliance score in Compliance Manager*

Die Verwaltung der Einhaltung von Compliance-Vorgaben für Ihre SharePoint- und OneDrive-Sites und deren Sicherheitsstatus bzw. Freigabeeinstellungen mit den integrierten Tools ist eine frustrierende Aufgabe, da sie über mehrere Portale verteilt sind. Im Gegensatz dazu bietet der **365 Permission Manager** von Hornetsecurity ein übersichtliches Dashboard mit einem Überblick über die Einstellungen für jede Site in Ihrem Tenant, der Möglichkeit zur Anwendung und Durchsetzung von Compliance-Richtlinien, die Behebung von Compliance-Verstößen, die Anzeige aller Zugriffe eines bestimmten Benutzers, die Erstellung von Berichten und vieles mehr.

## 15.6: SICHERHEIT LIEGT IN DER VERANTWORTUNG ALLER

In den letzten beiden Kapiteln haben Sie einen umfassenden Überblick über die zahlreichen Security-Funktionen von M365 erhalten. Die traurige Wahrheit ist, dass die meisten kleinen bis mittleren Unternehmen nicht annähernd genug der Funktionen implementieren, für die sie bereits bezahlt haben, und selbst große Unternehmen haben Schwierigkeiten, diese Schutzfunktionen für alle ihre Benutzer zu implementieren.



Das liegt zum Teil an der inhärenten Komplexität vieler nativer Sicherheitsfunktionen von Microsoft - erinnern Sie sich an das Sprichwort "Komplexität ist der Feind der Sicherheit". Deshalb wenden sich viele Unternehmen an Sicherheitslösungen von Drittanbietern wie Hornetsecurity, die ihnen dabei helfen, wichtige Sicherheitsfunktionen leichter zugänglich zu machen und die Komplexität zu reduzieren.

Andererseits ist die Vernachlässigung der Security auch auf eine gewisse Nachlässigkeit zurückzuführen, die daher rührt, dass in vielen Unternehmen immer noch eine Denkweise aus der On-premises-Ära vorherrscht, in der man dachte, dass (fast) alles schon mit einer Firewall erledigt sei - und die IT-Abteilungen sich schon darum kümmern würden.

Die Welt ist heute eine andere: Wir müssen verstehen, dass die Verantwortung für die Security in unser aller Händen liegt und dass unsere Cyber-Verteidigungskette nur so stark sein kann wie ihr schwächstes Glied.

Denken Sie über Security Awareness Trainings für Ihre Mitarbeiter nach, denn sie sind unerlässlich, um das Risiko von Cyberangriffen zu verringern, Datenschutzverletzungen zu verhindern und die Einhaltung von Compliance-Vorschriften zu gewährleisten. Es befähigt die Mitarbeiter, Sicherheitsbedrohungen zu erkennen und darauf zu reagieren, fördert eine starke Sicherheitskultur und schützt sowohl die Vermögenswerte als auch den Ruf des Unternehmens. Letztendlich führt die Investition in Awareness-Training zu Kosteneinsparungen und einer sichereren digitalen Umgebung.

## 15.7: ES MUSS NICHT IMMER MICROSOFT SEIN

Falls Ihnen der Gedanke nicht behagt, für die zugrundeliegende Plattform von Microsoft und dann noch einmal für die zusätzlichen Sicherheitsfunktionen von Microsoft zu zahlen, sollten Sie eine Lösung eines Drittanbieters für Ihre M365 Sicherheits- und Compliance-Anforderungen in Betracht ziehen. Hornetsecurity bietet **verschiedene Pläne** mit leistungsstarkem Advanced Threat Protection für Ihre E-Mails, Data Loss Prevention (DLP), Security Awareness Service (Phishing-Simulationen und Awareness-Training für Endbenutzer), E-Mail-Verschlüsselung, E-Mail-Archivierung und mehr.

Hornetsecurity bietet auch ein kostenloses E-Book an, das sich auf die Absicherung eines Microsoft 365 Tenants konzentriert: **The Microsoft 365 Security Checklist**. Darin werden alle Security-Einstellungen und -Konfigurationen behandelt, die Sie für jede M365-Lizenz kennen müssen, um Ihre Umgebung richtig abzusichern, und es wird ausführlicher auf die tatsächlichen Einstellungen eingegangen als hier beschrieben.

# KAPITEL 16:

# BACKUP IN MICROSOFT 365

**IN DIESEM KAPITEL BEFASSEN WIR UNS MIT DER NOTWENDIGKEIT DES DATENSCHUTZES IN MICROSOFT 365 - WOFÜR MICROSOFT VERANTWORTLICH IST - UND WOFÜR IHR UNTERNEHMEN VERANTWORTLICH IST.**

## 16.1: NATIVE DATENRESILIENZ (AUSFALLSICHERHEIT)

Wie jeder leistungsfähige Cloud Service nimmt auch Microsoft die Verfügbarkeit der Kundendaten in M365 sehr ernst. Wie bereits erwähnt, **gibt es von Exchange-Postfächern vier Kopien**, drei aktuelle und eine vierte, zeitversetzte Kopie (die bis zu 24 Stunden zurückliegt). Diese letzte Kopie wird im Falle einer systemischen Beschädigung der anderen drei Kopien verwendet. Alle vier Kopien sind auf mindestens zwei Rechenzentren verteilt. All dies wird vom System automatisch gehandhabt und ist für den Endbenutzer nicht zu bemerken.



SharePoint- und OneDrive for Business-Speicherung **beruht ebenfalls darauf, dass die Daten in zwei getrennten Azure-Regionen gespeichert werden** - ein Schreibvorgang gilt nur dann als abgeschlossen, wenn er erfolgreich in beide Regionen geschrieben wurde. Und der zugrunde liegende Datenspeicher verwendet Append-Only, um sicherzustellen, dass frühere Daten nicht von einem Angreifer beschädigt oder verschlüsselt werden können. Diese Versionierung ermöglicht auch die Wiederherstellung früherer Versionen von Dateien.

Klingt gut, oder? Microsoft unternimmt eindeutig Schritte zum Schutz meiner Daten, so dass ich mir keine Sorgen machen muss? Nicht so schnell - bei allem, was gerade beschrieben wurde, geht es um die Datenresilienz und die hohe Verfügbarkeit Ihrer Daten. Was es nicht bietet, abgesehen von einigen begrenzten Optionen, ist Backup Ihrer Daten.

Bei einem Backup handelt es sich um Kopien Ihrer Produktionsdaten in einem separaten System, die regelmäßig (stündlich, täglich) von den Produktionsdaten an den Backup-Speicherort kopiert werden. Dies bietet die folgenden Funktionen:

- Die Möglichkeit, „in der Zeit zurückzugehen" und E-Mails/Dokumente/Postfächer/Sites zu einem früheren Zeitpunkt wiederherzustellen - entweder an einem Produktionsstandort oder an einem separaten Exportstandort.

- Die Möglichkeit, auf Ihre Produktionsdaten zuzugreifen, wenn es zu einem katastrophalen Ausfall der Dienste in Microsoft 365 kommt.

Mit anderen Worten: Datenresilienz/Hochverfügbarkeit ist nicht dasselbe wie Backup. Sie sind zwar verwandt, dienen aber unterschiedlichen Zwecken. Je nach Ihren geschäftlichen Anforderungen oder den Vorschriften, die Sie einhalten müssen, benötigen Sie möglicherweise beides.

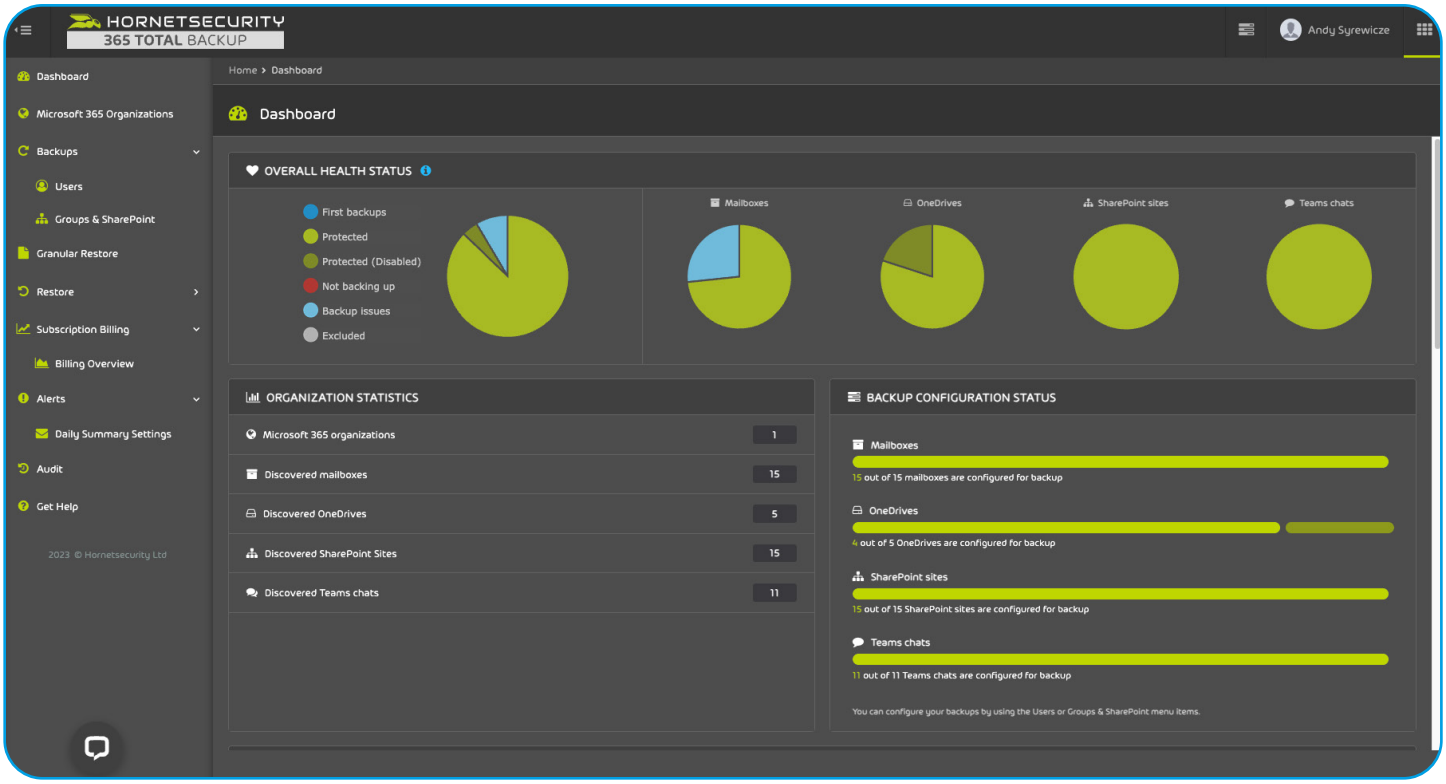
Sehen wir uns Ihre nativen Optionen zur Wiederherstellung früherer Versionen von Daten an. Gelöschte **Exchange-Elemente** (E-Mails, Kontakte, Kalendertermine) können Sie aus dem Outlook-Ordner für gelöschte Objekte wiederherstellen. Sie werden dort **auf unbestimmte Zeit aufbewahrt**, es sei denn, Sie ändern die Richtlinie in Ihrem Tenant. Wenn sie aus dem Ordner "Gelöschte Elemente" gelöscht wurden, können Sie sie bis zu 14 Tage lang aus dem versteckten Ordner "Wiederherstellbare Elemente" wiederherstellen. Sie müssen Ihren Benutzern vermitteln, wie sie dies selbst tun können, oder sicherstellen, dass Ihr Support-Team bereit ist, ihnen regelmäßig zu helfen, da die Benutzeroberfläche nicht gerade intuitiv ist.

In SharePoint / OneDrive for Business werden **gelöschte Dokumente** standardmäßig 93 Tage lang aufbewahrt, zunächst in einem für den Benutzer zugänglichen Papierkorb und, wenn sie von dort gelöscht werden, in einem für den Administrator zugänglichen Papierkorb. Auch hier ist der Wiederherstellungsprozess für ein versehentlich gelöschtes Dokument nicht ganz einfach, so dass eine gewisse Einarbeitung erforderlich ist.

Um die Standardeinstellungen zu ändern, können Sie **Aufbewahrungsrichtlinien** verwenden, um Elemente länger aufzubewahren (sie stehen zur Wiederherstellung zur Verfügung, auch wenn Benutzer sie aus dem Ordner Gelöschte Elemente löschen). Diese Richtlinien können sowohl auf Exchange- als auch auf SharePoint-Daten angewendet werden. Für Exchange können Sie auch **In-Place und Beweissicherungsverfahren** für ausgewählte Postfächer verwenden, um die Aufbewahrungsfristen zu verwalten.

## 16.2: 365 TOTAL BACKUP

Wenn Sie die Herausforderungen bei der Nutzung der eingebauten Datenschutzfunktionen als Recovery-Lösung umgehen möchten, bietet Hornetsecurity eine umfassende M365 Backup- und Recovery-Lösung **365 Total Backup** oder als Teil von **365 Total Protection Compliance & Awareness**. Diese Lösung schützt Postfächer, Teams Chats, OneDrive for Business, SharePoint Sites und Windows Endpunkte. Es ist einfach einzurichten und bietet umfassenden Schutz für Ihren gesamten Tenant.



## HÖREN SIE NIE AUF ZU LERNEN!

Wir hoffen, dass dieses Buch und die darin enthaltenen Links zu tiefer gehenden technischen Informationen Ihnen bei Ihrer Reise in die Cloud geholfen haben. Und wenn Sie erst einmal migriert haben, geht die Reise weiter, denn das Management einer sich ständig verändernden M365-Landschaft ist eine nie endende Reise.

Wie in Teil 1 erwähnt, ist es eine nie endende Aufgabe, sich über die neuesten Anwendungen und Funktionen von M365 auf dem Laufenden zu halten. Schauen Sie daher regelmäßig in den offiziellen Microsoft-Ressourcen nach, aber besuchen Sie auch den **Hornetsecurity-Blog** mit vielen interessanten Beiträgen zur Verwaltung und Sicherheit von M365.

Wenn Sie Ihre Inhalte lieber im Audio- oder Videoformat konsumieren, hören Sie sich den **Security Swarm Podcast** an - ein wöchentliches Gespräch über die kritischsten Themen, mit denen die Welt der Cybersicherheit heute konfrontiert ist, moderiert von Andy Syrewicze, Security Evangelist bei Hornetsecurity. Von der böswilligen Nutzung von KI-Tools bis hin zu Social-Engineering-Betrügereien - jede Folge befasst sich mit einem relevanten Thema, das von einem Branchenexperten analysiert und durch reale Daten direkt aus unserem Security Lab untermauert wird.

Viel Glück!

# ÜBER DEN AUTOR

**PAUL SCHNACKENBURG**
MICROSOFT CERTIFIED TRAINER

Paul begann seine Laufbahn in der IT-Branche, als DOS und 286er Prozessoren der letzte Schrei waren. Er leitet Expert IT Solutions, ein IT-Beratungsunternehmen für kleine Unternehmen an der Sunshine Coast, Australien. Außerdem arbeitet er als IT-Lehrer an einer Microsoft IT Academy. Paul ist ein angesehener Technologieautor und in der Community aktiv. Er schreibt fundierte technische Artikel mit Schwerpunkt auf Hyper-V, System Center, Private und Hybrid Cloud sowie Office 365 und Azure Public Cloud-Technologien. Er besitzt die Zertifizierungen MCSE, MCSA und MCT.

# ÜBER HORNETSECURITY GROUP

HORNETSECURITY

Hornetsecurity ist ein führender Anbieter von Cloud-basierten Sicherheits-, Compliance-, Backup- und Security-Awareness-Lösungen der nächsten Generation, die Unternehmen und Organisationen jeder Größe auf der ganzen Welt unterstützen. Das Flaggschiffprodukt 365 Total Protection ist die umfassendste Cloud-Security-Lösung für Microsoft 365 auf dem Markt. Angetrieben von Innovation und Cybersecurity-Exzellenz, sorgt Hornetsecurity mit seinem preisgekrönten Portfolio für eine sicherere digitale Zukunft und eine nachhaltige Sicherheitskultur bei seinen Kunden und Partnern.

Hornetsecurity ist über sein internationales Vertriebsnetz mit über 8.000 Channel-Partnern und MSPs in mehr als 30 Ländern aktiv. Die Lösungen des Unternehmens werden von mehr als 50.000 Kunden genutzt.

Weitere Informationen finden Sie unter **www.hornetsecurity.com**.

**Hornetsecurity GmbH, Am Listholze 78, 30177 Hannover, Germany**

HORNETSECURITY | infinigate

# 365 4 TOTAL PROTECTION

## PLAN 4 - COMPLIANCE & AWARENESS

**NEXT-GEN PROTECTION FÜR MICROSOFT 365:**
E-MAIL-SECURITY, BACKUP, COMPLIANCE & SECURITY AWARENESS

| PLAN 1 | PLAN 2 | PLAN 3 | PLAN 4 |
|---|---|---|---|
| BUSINESS | ENTERPRISE | BACKUP | COMPLIANCE & AWARENESS |
| SPAM & MALWARE PROTECTION | ADVANCED THREAT PROTECTION | BACKUP & RECOVERY OF MAILBOXES & TEAMS | PERMISSION MANAGEMENT |
| EMAIL ENCRYPTION | EMAIL ARCHIVING | BACKUP & RECOVERY OF ONEDRIVE & SHAREPOINT | PERMISSION ALERTS |
| EMAIL SIGNATURES & DISCLAIMERS | EMAIL CONTINUITY | BACKUP & RECOVERY OF ENDPOINTS | PERMISSION AUDIT |

| | | |
|---|---|---|
| PHISHING & ATTACK SIMULATION | COMMUNICATION PATTERN ANALYSIS | |
| SECURITY AWARENESS | AI RECIPIENT VALIDATION | |
| ESI® REPORTING | SENSITIVE DATA CHECK | |

365 Total Protection bringt alle Aspekte des Security- und Datenschutz-Managements von Microsoft 365 auf das nächste Level: E-Mail-Security, Backup und Recovery, Compliance, Berechtigungsmanagement und Security Awareness. Die Lösung lässt sich nahtlos in Microsoft 365 integrieren und bietet dringend erforderliche zusätzliche Sicherheits- und Datenschutzebenen gegen Spam, Malware und fortschrittlichen Bedrohungen.

**JETZT TESTEN**