A quick guide to secure Office 365

V2.0

About the author

Nicki Borell is a Microsoft Reginal Director & MVP, Co-founder of Experts Inside, founder of the label *"Xperts at Work"* and partner of atwork GmbH. As a team, we successfully implement IT and strategy projects for mid-sized companies and large enterprise customers. Take advantage of the expertise, competence and specialized knowledge we bring to each of our projects.

Contact: www.xpertsatwork.com | nb@atwork-it.com | nb@expertsinside.com

Inhalt

Sicherheitsstrategie mit Office 365

Die Default Einstellungen in Office 365 erlauben einen Zugriff auf die Services durch die Eingabe von Benutzername und Passwort. Es erfolgt keine weitere Evaluierung des Zugriffs. Abhängig von den Lizenzen und den Rollen, die dem Benutzer zugewiesen sind, hat er dann Zugriff auf den Office 365 Tenant. Um zu verhindern, dass unbefugte Zugriffe stattfinden oder dass Benutzer Aktionen durchführen die nicht erlaubt sind, stehen mehrere Lösungen zur Verfügung. Die folgende Matrix veranschaulicht ein Sicherheitssetup basierend auf 5 Stufen und nennt die jeweiligen Auswirkungen und benötigten Lizenzen:

Stufe	Erläuterung	Auswirkung auf Usability	Auswirkung auf Security	Lizensierung
Default	Standard Einstellungen von Office 365	• Dem Benutzer stehen alle Funktionen gemäß seiner Lizenz zur Verfügung. • Er kann mit internen und externen Personen zusammenarbeiten und beliebige Inhalte teilen. • E-Mails können mit beliebigen Anhängen an beliebige Empfänger verschickt werden. • Der Zugriff kann von jedem beliebigen Gerät aus durch die Eingabe von Benutzername und Passwort stattfinden.	Eine Sicherheitsmaßnahme zusätzlich zur Eingabe von Benutzername und Passwort findet nicht statt.	Keine zusätzliche Lizenz erforderlich
Mittel	Anpassungen der Default Office 365 Einstellungen ohne die Verwendung zusätzlicher Funktionen / Lizenzen. Konfigurieren von Office 365 MFA Office 365 MDM	**Maßnahmen:** • Dem Benutzer stehen alle Funktionen gemäß seiner Lizenz zur Verfügung. • Er kann mit internen und externen Personen gemäß den Einstellungen zur Freigabe von Dateien in OneDrive for Business und SharePoint Online zusammenarbeiten. • E-Mails können mit beliebigen Anhängen an beliebige Empfänger verschickt werden. • Benutzer müssen bei jedem Anmeldevorgang zusätzlich zu Benutzername und Passwort einen weiteren Faktor angeben (SMS, App Auth, etc.) Details dazu siehe: Azure AD Premium & Office 365 MFA • Zugriffe auf die Office 365 Umgebung können nur von verwalteten Geräten erfolgen. Verwaltete	• Durch die Aktivierung von O365 MFA und O365 MDM wird die Sicherheit deutlich erhöht. • Die Umsetzung der Vorgabe zu OneDrive for Business und SharePoint erhöht die Sicherheit und das ungewollte Abfließen von Daten.	Keine zusätzliche Lizenz erforderlich

		Geräte können remote bereinigt werden. Details dazu siehe unter: Intune & Office 365 MDM **Auswirkungen:** • Die Maßnahmen führen zu einem Mehraufwand bei jedem Anmeldevorgang. • Die Möglichkeiten der Zusammenarbeit mit Externen sind eingeschränkt. • Der Zugriff auf Office 365 kann nur noch von verwalteten Geräten aus stattfinden.		
Hoch	**wie „Mittel“ plus:** Einsatz von Cloud App Security um Aktionen in Office 365 zu überwachen und Maßnahmen zu konfigurieren. Verwendung von Azure AD Premium um MFA und Conditional Access Regel auch für externe Benutzer, Apps und Geräte durchzusetzen.	**Maßnahmen:** • Cloud App Security ermöglicht es, Aktionen innerhalb von Office 365 zu überwachen und Maßnahmen automatisch anzuwenden. Details dazu siehe unter: Cloud App Security Diese Maßnahmen werden ohne ein Zutun des Anwenders automatisch angewendet. • MFA und Conditinal Access als Teil von Azure AD Premium stellt erweiterte Funktionen wie z.B. das Erstellen von Richtlinien für den Zugriff (Sichere IP Adresse-Bereiche, Vertrauenswürdige Apps etc.) zur Verfügung. Details dazu siehe unter: Azure AD Premium & Office 365 MFA **Auswirkungen:** Die Maßnahmen führen zu keinem Mehraufwand bei den Anwendern. Ganz im Gegenteil reduziert die Umsetzung von MFA und Anmelderegeln mit Azure AD Premium den Aufwand bei den Anwendern deutlich. Anmeldungen von z.B. aus dem Firmennetzwerk oder von verwalteten Geräten und Apps aus kann dann ohne MFA geschehen etc.	• Durch den Einsatz von Cloud App Security wird die Sicherheit deutlich erhöht. Reports und automatische Maßnahmen für z.B. ungewöhnliche Anmeldeaktivitäten stehen nun zur Verfügung. • MFA und Conditinal Access als Teil von Azure AD ermöglichen erweiterte Szenarien und erhöhen dadurch die Sicherheit weiter.	• CAS • Azure AD Premium P1 oder P2 Beide Lizenzen sind z.B. Teil von EMS oder M365 und können auch jeweils separat erworben werden.

Sehr Hoch	**Wie „Hoch“ plus:** verwenden von Intune um Zugriffe von Geräten und Zugriffe auf Anwendungen zu steuern und Geräte zu verwalten.	**Maßnahmen:** • Es kann ganz explizit geregelt werden, welche Anwendung von wo aus und von welchem Gerät aus wie auf welche Daten zugreifen darf. Und welche Daten z.B. kopiert oder mit welchen Apps weiterverarbeitet werden dürfen. Stichwort „Copy & Past“ oder Download in private Dropbox Ordner etc. • Geräte und Anwendungen können verwaltet werden. **Auswirkungen:** Die Sicherheitsanforderungen können explizit und granular auf die Anforderungen der Anwender abgestimmt werden.	• Durch die Möglichkeiten granulare und explizite Regeln für den Zugriff auf Office 365 / Azure und Daten zu konfigurieren wird die Sicherheit noch einmal erhöht. • Es können auch Regeln für nicht-Office 365 Apps umgesetzt werden	Intune ist z.B. Teil von EMS oder M365 und kann auch separat erworben werden.
Deaktivieren aller externen Zugriffe		**Maßnahmen:** • Ein Zugriff auf Office 365 ist nur noch für Mitarbeiter möglich. • Der Zugriff ist nur aus dem Firmennetzwerk möglich • Eine Zusammenarbeit mit externen Personen ist nicht mehr möglich **Auswirkungen:** Die Usability von Office 365 ist sehr stark eingeschränkt. Der Service ist nur noch bedingt nutzbar.	Maximale Sicherheit	Keine zusätzliche Lizenz erforderlich

OneDrive for Business und SharePoint Online

OneDrive for Business und SharePoint Zugriffs- und Freigabeeinstellungen können im Admin-Center konfiguriert werden. Die folgende Matrix zeigt die relevanten Einstellungen um OneDrive for Business und SharePoint basierend auf Ihren Anforderungen zu konfigurieren:

	Einstellung	**Optionen**
OneDrive for Business Sharing Einstellungen	Standardlinktyp	*jeder mit diesem Link *nur Intern *Bestimmte Personen
Verwalten der Freigabe in OneDrive	Erweiterte Einstellungen für Links	*Ablaufdatum der Links *Berechtigung zum Bearbeiten von freigegebenen Dateien und Ordner
	externen Freigabe	*Alle Benutzer *Neue und vorhandene externe Benutzer *Vorhandene externe Benutzer *Nur Personen in Ihrer Organisation
	erweiterte Einstellungen für externe Freigaben	*Zulassen oder Blockieren der Freigabe für Personen in bestimmten Domänen *Externe Benutzer müssen Freigabeeinladungen mit demselben Konto akzeptieren, an das die Einladung gesendet wurde *Zulassen, dass externe Benutzer Elemente freigeben, die sie nicht selbst besitzen
	weitere Einstellungen	Anzeige auf Besitzer die Namen aller Personen, die ihre Dateien angezeigt
	Schaltfläche zum Synchronisieren in OneDrive anzeigen	
Synchronisieren	Synchronisieren nur auf PC´s erlauben die Mitglied einer bestimmten Domäne sind	
	Synchronisieren für bestimmte Dateitypen blockieren	
	Standard Speicher pro Benutzer	
Speicher	Tage die Datei aufbewahrt werden, wenn ein Benutzer gelöscht wurde	
	Zugriff aufgrund der IP Adresse steuern	Zugriff nur von bestimmten IP Adresse zulassen
Zugriffe auf OneDrive for Business	Zugriff von Geräten die kein modern Auth unterstützen	Zulassen JA oder NEIN
	Benutzern Benachrichtigungen anzeigen wenn Dateien mit ihnen geteilt werden	Zulassen JA oder NEIN
Benachrichtigungen	E-Mails an OneDrive Besitzer schicken, wenn…:	*Ein andere Benutzer lädt zusätzlich externe Benutzer zu meinen Datei ein *Ein externen Benutzer akzeptiert die Einladung *Ein anonymer Zugriffslink wird erstellt oder geändert

SharePoint Online Sharing Einstellungen	Freigeben außerhalb der Organisation	*Freigabe außerhalb Ihrer Organisation nicht zulassen *Freigabe nur für externe Benutzer erlauben, die bereits im Verzeichnis Ihrer Organisation vorhanden sind *Benutzern das Einladen von und Freigeben für authentifizierte externe Benutzer gestatten *Freigabe für authentifizierte externe Benutzer und Verwendung anonymer Zugriffslinks zulassen *Anonyme Zugriffslinks laufen nach folgender Anzahl von Tagen ab:
	Anonyme Zugrifflinks gestatten Empfängern	Berechtigung zum Bearbeiten von freigegebenen Dateien und Ordner
	Wer außerhalb der Organisation teilen kann	*Nur Benutzer in ausgewählten Sicherheitsgruppen dürfen mit authentifizierten externen Benutzern teilen *Nur Benutzer in ausgewählten Sicherheitsgruppen dürfen mit authentifizierten externen Benutzern und mittels anonymer Links teilen
	Standardlinktyp	*Direkt – bestimmte Personen *Intern – nur Personen in Ihrer Organisation *Anonymer Zugriff – jeder mit dem Link
	Standardlinkberechtigung	*Anzeigen *Bearbeiten
	Zusätzliche Einstellungen	*Externe Freigaben mithilfe von Domänen einschränken *Externe Benutzer daran hindern, Dateien, Ordner und Websites zu teilen, die sie nicht besitzen *Externe Benutzer müssen Freigabeeinladungen mit demselben Konto annehmen, wie dem, an das die Einladungen gesendet wurden *Empfänger müssen fortwährend den Besitz des Kontos nachweisen, wenn sie auf geteilte Elemente zugreifen
	Apps, die keine moderne Authentifizierung verwenden	*Zulassen *Sperren
	Zugriff je nach Netzwerkadresse steuern	Zugriff nur von bestimmten IP-Adressstandorten aus zulassen
Nützliche Einstellung per PowerShell	BccExternalSharingInvitations	
	BccExternalSharingInvitationsList	
	DisallowInfectedFileDownload	
	NotificationsInSharePointEnabled	
	ODBAccessRequests	
	UserVoiceForFeedbackEnabled	

Erhöhung der Sicherheit durch weiter Services und Feature

Die Sicherheit von Office 365 kann durch proaktive und reaktive Monitoring weiter gesteigert werden. Siehe dazu Security & Complinace Reports und Office 365 Advanced Threat Protection & Office 365 Threat Intelligence sowie Office 365 Secure Score. Darüber hinaus bietet Microsoft die Lösungen „Microsoft Advanced Threat Analytics“, „Windows Defender Advanced Threat Protection“ und „Windows Information Protection“ an, um eine umfassende Absicherung der gesamten IT Infrastruktur umzusetzen. Diese Funktionen sind in der neuen Lösung Microsoft Threat Protection zusammengefasst die nicht Bestandteil dieses Dokuments sind.

Office 365 Secure Score

Office 365 Secure Score analysiert, welche Office 365-Dienste wie z.B. OneDrive, SharePoint oder Exchange genutzt werden und prüft deren Einstellungen. Die Einstellungen werden dann mit einer von Microsoft aufgestellten Baseline verglichen. Anschließend wird ein Report und Empfehlungen zur Steigerung der Sicherheit generiert. Details dazu siehe: https://support.office.com/de-de/article/einf%C3%BChrung-in-office-365-secure-score-c9e7160f-2c34-4bd0-a548-5ddcc862eaef

Cloud App Security

Cloud App Security stellt Zugriffssicherheit und Auditing auf Applikationsebene zur Verfügung. Der Service generiert einen Report zu den genutzten Cloud-Apps und Diensten. Die erweiterten Analysen ermöglichen es, ungewöhnliche Anmeldeverhalten, untypische Aktionen wie hohe Downloadraten und Cyberbedrohungen aller Art zu erkennen und abzuwehren. Durch die Integration mit DLP und AIP ist eine weitreichende Kontrolle über Daten möglich.

Typische Szenarien:

- **Erkennen von Bedrohungen und automatisches Anwenden von Maßnahmen:**
  z.B.: Identifizieren von riskanten Nutzeraktivitäten und ungewöhnliche Zugriffsverhalten.
- **Daten schützen:**
  z.B.: Detaillierte Kontrolle über Daten und erzwingen von integrierten oder benutzerdefinierten Richtlinien für die gemeinsame Nutzung von Daten zur Vermeidung von Datenverlust.
- **Zugriff in Echtzeit steuern:**
  z.B.: Verwalten und begrenzen von Zugriffen auf Cloud-Apps anhand von Bedingungen und dem Sessionkontext, einschließlich der Benutzeridentität, Geräte und Standort.
- **Entdecken und bewerten von Risiken:**
  z.B.: Identifizieren von Cloud-Apps die im Netzwerk genutzt werden. Einblick in genutzte Anwendungen, Risikobewertungen und fortlaufende Analysen.

Details dazu siehe auch: https://www.microsoft.com/de-de/cloud-platform/cloud-app-security

Richtlinientypen und Details:

Richtlinientyp	Verwendung
Zugriffsrichtlinie	Zugriffsrichtlinien ermöglichen die Echtzeitüberwachung und das Steuern der Benutzeranmeldungen für Cloud-Apps.
Aktivitätsrichtlinie	Aktivitätsrichtlinien ermöglichen es, automatisierte Prozesse zu erzwingen. Mit diesen Richtlinien können Aktivitäten überwacht werden, die von Benutzern durchgeführt werden. Unerwartet hohe Raten eines bestimmten Aktivitätstyps werden erkannt.
Richtlinie zur Anomalieerkennung	Mit Richtlinien zur Anomalieerkennung werden, basierend auf Risikofaktoren, ungewöhnliche Aktivitäten erkannt.
App Discovery-Richtlinie	Mit App Discovery-Richtlinien werden Warnungen festgelegt, mit denen Administratoren benachrichtigt werden, wenn neue Apps erkannt werden.

Richtlinie zur Anomalieerkennung von Cloud Discovery	Richtlinien zur Anomalieerkennung von Cloud Discovery untersuchen die Protokolle um Apps zu ermitteln und auf Ungewöhnliches hin zu durchsuchen. Wenn beispielsweise ein Benutzer, der vorher nie Dropbox verwendet hat, plötzlich 600 GB hochlädt, oder wenn viel mehr Transaktionen als üblich bei einer bestimmten App verzeichnen werden.
„Dateirichtlinie“	Mit Dateirichtlinien werden Cloud-Apps auf angegebene Dateien oder Dateitypen freigegeben, (freigegeben mit externen Domänen) sowie Daten (proprietäre Informationen, Kreditkartendaten usw.) überprüft und Governanceaktionen auf die Dateien angewendet.
Sitzungsrichtlinie	Sitzungsrichtlinien ermöglichen die Echtzeitüberwachung und das Steuern der Benutzeraktivitäten.

Details dazu siehe auch: https://docs.microsoft.com/de-de/cloud-app-security/control-cloud-apps-with-policies

Office 365 Cloud App Security:

Office 365 E5 beinhaltet ebenfalls das Feature Cloud App Security jedoch in einer stark eingeschränkten Version. Unterschiede zwischen Cloud App Security und Office 365 Cloud App Security sind:

Funktion	**Feature**	**Microsoft Cloud App Security**	**Office 365 Cloud App Security**
Cloud Discovery	Ermittelte Apps	Über 16.000 Cloud-Apps	Über 750 Cloud-Apps mit ähnlichen Funktionen wie Office 365
	Bereitstellung für die Ermittlungsanalyse	Manueller und automatischer Protokollupload	Manueller Protokollupload
	Protokollanonymisierung für Datenschutz	●	
	Zugriff auf den vollständigen Cloud-App-Katalog	●	
	Risikobewertung für Cloud-Apps	●	
	Cloud-Nutzungsanalyse pro App, Benutzer, IP-Adresse	●	
	Laufende Analyse und Berichterstellung	●	
	Anomalieerkennung für ermittelte Apps	●	
Datenschutz	Unterstützung der Verhinderung von Datenverlust (Data Loss Prevention, DLP)	SaaS-DLP (übergreifend) und Datenfreigabesteuerung	Verwendet die bestehende Office-DLP (verfügbar in Office E3 und höher)
	App-Berechtigungen und die Möglichkeit, den Zugriff zu widerrufen	●	●
	Richtlinieneinstellung und -durchsetzung	●	
	Integration in Azure Information Protection	●	
	Integration in DLP-Lösungen von Drittanbietern	●	
Erkennung von Bedrohungen	Anomalieerkennung und Verhaltensanalysen	Für SaaS-übergreifende Apps inklusive Office 365	Für Office 365-Apps
	Manuelle und automatische Warnungsbehandlung	●	●
	SIEM-Connector	Ja. Warnungen und Aktivitätsprotokolle für SaaS-übergreifende Apps	Ja. Nur Office 365-Warnungen

	Integration von Microsoft Intelligent Security Graph	•	•
	Aktivitätsrichtlinien	•	•

Details dazu siehe: https://docs.microsoft.com/de-de/cloud-app-security/editions-cloud-app-security-o365

Intune & Office 365 MDM

Per Default bringt Office 365 eigenständige und in den Benutzerlizenzen inkludierte Optionen für das Verwalten mobiler Geräte und mobiler Zugriffe mit. Diese sind in ihrem Funktionsumfang reduziert und decken nur Grundfunktionen ab.

Funktionsbereich	**MDM für Office 365**	**Microsoft Intune**
Verwaltung von Geräten	Die Verwaltung von Geräten erfolgt mit Hilfe des Security and Compliance Center in Office 365.	Intune Verwaltungskonsole in Azure oder Integration in System Center
Verwaltbare Geräte	Cloud-basierte Verwaltung iOS, Android und Windows Geräte.	Cloud-basiertes Management für iOS, Mac OS X, Android, Windows 8.1 (Telefon und Computer) und höher in Windows 10 enthalten
Wichtige Funktionen	• Sicherstellen, dass auf E-Mails und Dokumente des Unternehmens in Office 365 nur über Smartphones und Tablets zugegriffen werden kann, die vom Unternehmen verwaltet werden und den IT-Richtlinien entsprechen. • Festlegen und Verwalten von Sicherheitsrichtlinien wie PIN-Sperre auf Geräteebene und Jailbreak-Erkennung, um den Zugriff nicht autorisierter Benutzer auf E-Mails und Daten des Unternehmens über ein Gerät zu verhindern, wenn es verloren geht oder gestohlen wird. • Entfernen von Unternehmensdaten in Office 365 vom Gerät eines Mitarbeiters, während persönliche Daten erhalten bleiben.	MDM für Office 365-Funktionen und zusätzlich folgende Funktionen: • Sicherer Zugriff der Benutzer auf Unternehmensressourcen mit Zertifikaten, Wi-Fi, VPN und E-Mail-Profilen • Registrieren und Verwalten von unternehmenseigenen Geräten zur Bereitstellung von Richtlinien und Apps • Bereitstellen von Apps für Benutzer • Sichererer Zugriff auf Unternehmensdaten wobei Datensicherheit gewährleistet wird, indem Aktionen wie "Kopieren", "Ausschneiden", "Einfügen" und "Speichern unter" auf die von Intune verwalteten Apps beschränkt werden. • Verwalten von PCs, Macs, Linux- und UNIX-Server sowie mobiler Geräte

Details dazu siehe auch: https://support.office.com/en-us/article/choose-between-mdm-for-office-365-and-microsoft-intune-c93d9ab9-efb2-4349-9b93-30c30562ee22 und https://support.office.com/de-de/article/funktionen-der-integrierten-verwaltung-mobiler-ger%C3%A4te-f%C3%BCr-office-365-a1da44e5-7475-4992-be91-9ccec25905b0?ui=de-DE&rs=de-DE&ad=DE

Azure AD Premium & Office 365 MFA

Per Default bringt Office 365 eigenständige und in den Benutzerlizenzen inkludierte Optionen für Multifaktor Authentifizierung mit. Diese sind in ihrem Funktionsumfang reduziert und decken nur Grundfunktionen ab.

Feature	Multi-Factor Authentication für Office 365	Azure Multi-Factor Authentication
Schutz von Azure AD-Administratorkonten mit MFA	●	●
Mobile App als zweiter Faktor	●	●
Telefonanruf als zweiter Faktor	●	●
SMS als zweiter Faktor	●	●
App-Kennwörter für Clients, die MFA nicht unterstützen	●	●
Administrative Kontrolle über Überprüfungsmethoden	●	●
Schutz von Nicht-Administrator-Konten mit MFA	● (Nur für Office 365-Anwendungen)	●
PIN-Modus		●
Betrugswarnung		●
MFA-Berichte		●
Einmalumgehung		●
Benutzerdefinierte Begrüßungen für Telefonanrufe		●
Benutzerdefinierte Anrufer-ID für Telefonanrufe		●
Vertrauenswürdige IP-Adressen		●
Speichern der MFA für vertrauenswürdige Geräte	●	●
MFA für lokale Anwendungen		●

Details dazu siehe: https://docs.microsoft.com/de-de/azure/active-directory/authentication/concept-mfa-licensing

Weitere Funktionen von Azure AD Premium

Conditional Access:

Die Funktion Conditional Access von Azure Active Directory Premium regelt den Zugriff für Apps und Benutzer basierend auf bestimmten Bedingungen. Mit Hilfe von Richtlinien für den bedingten Zugriff wird eine anlassbezogene Zugriffssteuerung umgesetzt.

- **Anmelderisiko:** Azure AD Identity Protection erkennt Anmelderisiken und führt entsprechend der konfigurierten Regeln automatisch Maßnahmen aus. Details dazu siehe: https://docs.microsoft.com/de-de/azure/active-directory/active-directory-conditional-access-conditions#sign-in-risk
- **IP Ranges:** Über Regeln wird gestreut, dass z.B. MFA bei der Anmeldung aus einem unbekannen Netzwerk erzwungen wird. Bei der Anmeldung aus dem Unternehmensnetzwerk heraus wird dann z.B. kein MFA erzwungen. Details dazu siehe: https://docs.microsoft.com/de-de/azure/active-directory/active-directory-conditional-access-locations
- **Geräteverwaltung:** Benutzer können über eine breite Palette von Geräten, einschließlich mobiler und privater Geräte zugreifen. Über Regeln zur Geräteverwaltung wird gestreut, dass

z.B. ein Zugriff nur noch über verwaltete Geräte möglich ist. Eine weitere Option ist es, den Zugriff für bestimmte Apps nur von verwaltete Geräte aus zuzulassen etc.

Beispiel:

- Der Zugriff auf Microsoft Teams kann nur von einem verwalteten Gerät aus geschehen
- Der Zugriff auf E-Mail kann von jedem beliebigen Gerät aus geschehen. Greift das Gerät aber von außerhalb des Firmennetzwerks zu, wird MFA erzwungen.

Details dazu siehe: https://docs.microsoft.com/de-de/azure/active-directory/active-directory-conditional-access-conditions#device-platforms

- **Clientanwendung:** Mit dieser Funktion wird gestreut, mit welchen Anwendungen auf welche Ressourcen zugegriffen werden kann. So kann z.B. erzwungen werden, dass für den Zugriff auf E-Mails die Outlook App genutzt werden muss. Details dazu siehe: https://docs.microsoft.com/de-de/azure/active-directory/active-directory-conditional-access-conditions#client-apps

Weitere Information zum Thema Conditional Access: https://docs.microsoft.com/de-de/azure/active-directory/active-directory-conditional-access-azure-portal

Darüber hinaus stellt der Bereich Conditional Access von Azure Active Directory Premium die Funktion „Nutzungsbedingungen“ zur Verfügung. Weiterhin wird erzwungen, dass einem Benutzer beim Anmelden relevante Haftungsausschlüsse, rechtliche oder compliancebezogene Anforderungen oder Informationen zum Thema Datenschutz und Datensicherheit anzeigt werden und er diese bestätigen muss bevor er weitergeleitet wird. Details dazu siehe: https://docs.microsoft.com/de-de/azure/active-directory/active-directory-tou

Role-Based Access Control und Privileged Identity Management:
Mit Azure Active Directory Privileged Identity Management (PIM) kann die Funktion für die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) kombiniert werden. So müssen Administratoren nicht dauerhaft über die Rolle „global Admin“ verfügen. Anlassbezogen kann über einen Freigabeworkflow eine administrative Rolle beantragt werden.

Funktionen / Szenarien:

- Bedarfsgesteuerten Just-In-Time-Zugriff mit erweiterten Rechten
- Temporär erweiterte Rechte für kurze Aufgaben oder Bereitschaftszeiten
- Erzwingen der mehrstufigen Authentifizierung beim Zugriff mit erweiterten Rechten
- Reports über Zugriffe mit erweiterten Rechten
- Benachrichtigungen, wenn Zugriff mit erweiterten Rechte angefordert wird

Details dazu: https://docs.microsoft.com/de-de/azure/active-directory/privileged-identity-management/azure-pim-resource-rbac

MAM und MDM im Kontext von Azure AD Premium:
MAM (Mobile Application Management) und MDM (Mobile Device Management) werden in der Regel miteinander kombiniert. Die beiden Lösungen lassen sich wie folgt unterscheiden:

- **MDM:** Fokussiert die Verwaltung von Unternehmens- und Privatgeräte
  - Erzwingen der Gerätekonformität durch Benutzer- und Geräteregistrierung, Konfiguration und Passwortverwaltung
  - Sichert Geräte im Netzwerk und überwacht Geräte. Melden, verfolgen und aktualisieren von Geräte sowie sperren und löschen von Geräten steht zur Verfügung.

- **MAM:** Fokussiert die Einhaltung von Datensicherheitsrichtlinien und Datenschutzanforderungen sowie Maßnahmen im Fall von Datenverlust.
    - Benutzeridentitätsrichtlinien, Single Sign-On und bedingter Zugriff nach Rolle und Gerät (mit Intune oder Active Directory on-prem oder Azure AD möglich)
    - Überwacht und pusht App Updates, einschließlich mobilem Dokumentenmanagement für SharePoint und OneDrive.

Mit Azure AD Premium besteh die Option MAM und MDM (Intune) zu kombinieren oder MAM ohne MDM (Intune) bzw. mit MDM Lösungen eines anderen Anbieters zu nutzten. Details dazu siehe: https://docs.microsoft.com/de-de/intune/mam-faq

Office 365 Advanced Threat Protection & Office 365 Threat Intelligence

Office 365 Threat Intelligence:

Office 365 Threat Intelligence ist eine Sammlung von Reports und Informationen, die im Security & Compliance Center verfügbar sind. Threat Intelligence überwacht und sammelt Daten aus mehreren Quellen, wie z. B. Benutzeraktivitäten, Authentifizierung, E-Mails etc. Das Feature ist in Office 365 Enterprise E5 enthalten.

Detail dazu siehe: https://support.office.com/de-de/article/erste-schritte-mit-office-365-bedrohungsanalyse-38e9b67f-d188-490f-bc91-a1ae4b270441?ui=de-DE&rs=de-DE&ad=DE

Office 365 Advanced Threat Protection:

Office 365 Advanced Threat Protection wird für folgenden Szenarien verwendet:

- Scannen von E-Mail-Anlagen
- Scannen von Webadressen und Office-Dokumenten in einer E-Mail-Nachricht
- Identifizieren und blockieren bösartiger Dateien in SharePoint, OneDrive, und Microsoft Teams
- Identifizieren von E-Mail-Nachrichten mit Spoofing Angriffen
- Erkennen von Phishing Angriffen

Office 365 Advanced Threat Protection ist in Office 365 Enterprise E5 enthalten. Details dazu siehe auch: https://support.office.com/de-de/article/office-365-advanced-threat-protection-e100fe7c-f2a1-4b7d-9e08-622330b83653

Security & Complinace Reports

Das Office 365 Security & Complinace Center stellt verschieden Reports und Funktionen zur Verfügung. Folgenden Themen werden unterschieden:

- Zugriffsschutz für Daten und Dienste in Office 365
- Verhindern von Datenverlust in Office 365
- Verwalten der Datenkontrolle in Office 365
- Schutz vor Bedrohungen in Office 365
- Inhaltssuche in Office 365
- Verwalten von rechtlichen Untersuchungen in Office 365
- Durchsuchen des Überwachungsprotokolls nach Benutzer- und Administratoraktivitäten
- Überwachen von Sicherheit und Compliance in Office 365

Je nach Funktion werden unterschiedliche Lizenzen benötigt.

How to deal with external Sharing Sketchnote at Microsoft Ignite 2018

Sketchnote by Luise Freese. Download Sketchnote: LINK