Wie sicher ist Microsoft 365 für Unternehmen? Schutz, Risiken und wichtige Einstellungen

Ein verständlicher Sicherheitsleitfaden für kleine und mittlere Unternehmen

Titel	Wie sicher ist Microsoft 365 für Unternehmen? Schutz, Risiken und wichtige Einstellungen
Kategorie	IT-Sicherheit
Tags	Microsoft 365, IT-Sicherheit, KMU, MFA, Phishing-Schutz, Microsoft Defender, Entra ID, Intune, Cloud-Sicherheit
Geschätzte Lesezeit	7 Minuten
Kurze Beschreibung	Microsoft 365 bietet eine solide technische Sicherheitsbasis, ist aber nicht automatisch vollständig abgesichert. Der Artikel erklärt verständlich, welche Schutzmechanismen vorhanden sind, welche Aufgaben beim Unternehmen bleiben und welche Einstellungen für kleine und mittlere Unternehmen besonders wichtig sind.

URL-Vorschlag	/news/microsoft-365-sicherheit-unternehmen
Meta Description	Wie sicher ist Microsoft 365? Erfahren Sie, welche Schutzfunktionen es bietet und was KMU bei Konten, Geräten und Daten beachten sollten.

> **Microsoft 365 wird in vielen kleinen und mittleren Unternehmen für E-Mail, Dateien, Besprechungen und die tägliche Zusammenarbeit eingesetzt. Dabei entsteht schnell die Frage: Sind Unternehmensdaten in der Cloud wirklich sicher?**
> Die ehrliche Antwort lautet: Microsoft 365 bietet umfangreiche Sicherheitsfunktionen und eine professionelle technische Infrastruktur. Die tatsächliche Sicherheit hängt jedoch auch davon ab, wie Benutzerkonten, Geräte, Berechtigungen und Sicherheitsrichtlinien eingerichtet und regelmäßig kontrolliert werden. Eine Cloud-Plattform kann viele Risiken reduzieren, sie ersetzt aber keine klare Sicherheitsorganisation im Unternehmen.

1. Welche Sicherheitsbasis bietet Microsoft 365?

Microsoft schützt die zugrunde liegende Cloud-Infrastruktur, Rechenzentren und zentralen Dienste. Daten in Microsoft 365 werden nach Angaben des Herstellers sowohl bei der Speicherung als auch während der Übertragung verschlüsselt. Dadurch sollen Informationen beispielsweise beim Zugriff auf Exchange Online, OneDrive oder SharePoint vor unbefugtem Mitlesen geschützt werden.

Für Benutzerkonten steht die Multi-Faktor-Authentifizierung, kurz MFA, zur Verfügung. Zusätzlich zum Passwort wird dabei eine zweite Bestätigung verlangt, beispielsweise über die Microsoft Authenticator App. Selbst wenn ein Passwort durch Phishing oder ein Datenleck bekannt wird, reicht es allein normalerweise nicht für die Anmeldung aus.

Je nach Microsoft-365-Plan stehen weitere Funktionen zur Verfügung. Microsoft 365 Business Premium umfasst unter anderem erweiterten Identitäts- und Zugriffsschutz, zentrale Geräteverwaltung mit Microsoft Intune sowie Schutzfunktionen von Microsoft Defender. Diese Werkzeuge können verdächtige Anmeldungen, schädliche E-Mail-Anhänge oder unsichere Geräte besser erkennen und begrenzen.

Wichtig ist jedoch: Das Vorhandensein einer Funktion bedeutet noch nicht, dass sie passend konfiguriert, überwacht und im Arbeitsalltag konsequent genutzt wird.

2. Welche Sicherheitsrisiken bleiben beim Unternehmen?

Microsoft 365 folgt dem Prinzip der gemeinsamen Verantwortung. Microsoft ist für den sicheren Betrieb der Cloud-Plattform zuständig. Das Unternehmen selbst bleibt unter anderem für Benutzerkonten, Zugriffsrechte, Endgeräte, interne Abläufe und den korrekten Umgang mit Daten verantwortlich.

Ein häufiges Risiko sind schwach geschützte Konten. Wird MFA nicht konsequent genutzt, können gestohlene Passwörter weiterhin zu einem erfolgreichen Angriff führen. Besonders kritisch sind Administratorenkonten, weil sie weitreichende Änderungen an Benutzern, E-Mails und Sicherheitseinstellungen ermöglichen.

Auch zu viele Berechtigungen erhöhen das Risiko. Ehemalige Mitarbeiter, alte Gastkonten oder unnötige Administratorrechte bleiben in kleineren Unternehmen häufig länger aktiv als geplant. Ein regelmäßiger Benutzer- und Rechtecheck ist daher wichtiger als eine einmalige Einrichtung.

Weitere Risiken entstehen durch unverwaltete private Geräte, fehlende Sicherheitsupdates, unkontrollierte externe Dateifreigaben und Phishing-E-Mails. Außerdem sollte Synchronisation nicht mit Backup verwechselt werden: OneDrive und SharePoint bieten Wiederherstellungsfunktionen, eine unabhängige Backup-Strategie kann für geschäftskritische Daten dennoch sinnvoll sein.

3. Welche Maßnahmen sind für KMU besonders wichtig?

Für ein Unternehmen mit 5 bis 30 Benutzern muss Sicherheit nicht unnötig kompliziert sein. Entscheidend sind wenige, konsequent umgesetzte Grundlagen:

- MFA für alle Benutzer und besonders für Administratoren
- separate Administratorkonten statt dauerhafter Arbeit mit Global-Admin-Rechten
- regelmäßige Kontrolle aktiver Benutzer, Gastkonten und Lizenzen
- klare Rollen und möglichst geringe Berechtigungen
- sichere Gerätekonfiguration, Updates und Verschlüsselung
- Prüfung auffälliger Anmeldungen und wichtiger Sicherheitswarnungen
- Schutz vor Phishing und schädlichen E-Mail-Anhängen
- geregeltes Onboarding und Offboarding von Mitarbeitern
- nachvollziehbare Freigaben in Teams, SharePoint und OneDrive
- eine passende Backup- und Wiederherstellungsplanung

Welche Funktionen dafür eingesetzt werden können, hängt vom gebuchten Lizenzplan ab. Business Basic und Business Standard bieten grundlegende Kontosicherheit. Für strengere Zugriffsregeln, zentrale Geräteverwaltung und erweiterten Bedrohungsschutz ist Business Premium häufig besser geeignet. Die richtige Wahl sollte sich an Arbeitsweise, Geräten, Daten und Risiken des Unternehmens orientieren.

4. Praktisches Beispiel aus einem kleinen Unternehmen

Ein deutsches Beratungsunternehmen mit zwölf Mitarbeitern nutzt Outlook, Teams und OneDrive. Mehrere Beschäftigte arbeiten teilweise im Homeoffice. Anfangs wurden Konten nur mit Passwörtern geschützt. Zwei ehemalige Gastbenutzer hatten noch Zugriff auf Projektordner, und private Notebooks konnten ohne einheitliche Sicherheitsprüfung verwendet werden.

Nach einer strukturierten Überprüfung führte das Unternehmen MFA für alle Benutzer ein, reduzierte Administratorrechte, entfernte nicht mehr benötigte Konten und definierte Regeln für externe Freigaben. Firmenlaptops wurden zentral erfasst und Sicherheitsupdates kontrolliert. Zusätzlich wurde festgelegt, welche Daten gesichert und wie Wiederherstellungen getestet werden.

Microsoft 365 war bereits vor diesen Maßnahmen technisch leistungsfähig. Erst durch die passende Konfiguration und klare Prozesse wurde die Umgebung jedoch übersichtlicher und deutlich besser kontrollierbar.

5. Wie unterstützt Remote IT Cloud?

Remote IT Cloud unterstützt kleine und mittlere Unternehmen bei der strukturierten Absicherung bestehender Microsoft-365-Umgebungen. Die Betreuung erfolgt überwiegend remote und kann beispielsweise die Prüfung

von Benutzerkonten, MFA-Status, Administratorrollen, Anmeldeaktivitäten, Gerätestatus und wichtigen Sicherheitsmeldungen umfassen.

Je nach Ausgangslage können außerdem Conditional Access, Microsoft Intune, Microsoft Defender, geregelte Onboarding- und Offboarding-Prozesse sowie eine passende Backup-Strategie geplant oder eingerichtet werden. Ziel ist keine überladene Sicherheitsarchitektur, sondern eine nachvollziehbare Lösung, die zur Größe und Arbeitsweise des Unternehmens passt.

Fazit

Microsoft 365 kann für Unternehmen eine sichere und moderne Arbeitsplattform sein. Verschlüsselung, MFA, Identitätsverwaltung und optionale Schutzfunktionen schaffen eine gute Grundlage. Vollständig automatisch entsteht Sicherheit jedoch nicht.

Entscheidend sind passende Lizenzen, saubere Konfigurationen, kontrollierte Benutzerrechte, geschützte Geräte und regelmäßige Überprüfungen. Gerade kleine Unternehmen profitieren davon, ihre Microsoft-365-Umgebung nicht nur einzurichten, sondern dauerhaft strukturiert zu betreuen.

Sie möchten wissen, wie sicher Ihre aktuelle Microsoft-365-Umgebung eingerichtet ist? Remote IT Cloud prüft gemeinsam mit Ihnen Benutzer, Zugriffe, Geräte und zentrale Sicherheitseinstellungen und zeigt verständlich, welche Maßnahmen sinnvoll sind.

Offizielle Quellen

Stand der fachlichen Prüfung: Juli 2026. Die Sicherheitsfunktionen können je nach Lizenz, Mandantenkonfiguration und späteren Produktänderungen abweichen.

- Microsoft Learn: Verschlüsselung in Microsoft 365: https://learn.microsoft.com/de-de/purview/encryption
- Microsoft Learn: Einrichten der Multi-Faktor-Authentifizierung: https://learn.microsoft.com/de-de/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide
- Microsoft Learn: Sicherheits-Best-Practices für Microsoft 365 Business: https://learn.microsoft.com/de-de/microsoft-365/admin/security-and-compliance/m365b-security-best-practices?view=o365-worldwide
- Microsoft Learn: Gemeinsame Verantwortung in der Cloud: https://learn.microsoft.com/de-de/azure/security/fundamentals/shared-responsibility
- Microsoft: Microsoft 365 Business Premium Security: https://www.microsoft.com/de-de/security/business/microsoft365-business-premium

Artikelumfang: ca. 774 Wörter