



Microsoft 365

Security Quick Check

10 Kontrollen, die jedes
kleine Unternehmen
durchführen sollte

Prüfen · Priorisieren · Absichern



SICHERHEITS-
STATUS PRÜFEN



RISIKEN
PRIORISIEREN



MASSNAHMEN
ABLEITEN



IHR UNTERNEHMEN
BESSER ABSICHERN

So funktioniert der Quick Check

Microsoft 365 stellt zahlreiche Sicherheitsfunktionen bereit. Entscheidend ist jedoch, ob die für dein Unternehmen relevanten Schutzmaßnahmen tatsächlich eingerichtet, wirksam und dokumentiert sind.

Bewerte jeden Kontrollpunkt mit JA, NEIN oder UNKLAR. Ein unklarer Punkt gilt nicht automatisch als sicher und sollte anschließend überprüft werden.

JA geprüft und umgesetzt	NEIN nicht umgesetzt	UNKLAR noch zu prüfen
-----------------------------	-------------------------	--------------------------

Wichtiger Hinweis

Dieser Quick Check ist eine strukturierte Bestandsaufnahme, kein Penetrationstest oder vollständiges Security-Audit. Änderungen an produktiven Microsoft-365-Umgebungen sollten geplant, getestet und an Lizenzierung, Risiko und Geschäftsanforderungen angepasst werden.

01 Ist MFA für alle Benutzer wirksam?

☐ JA	☐ NEIN	☐ UNKLAR
-----------------------------	-------------------------------	---------------------------------

Multifaktor-Authentifizierung ergänzt das Passwort um einen weiteren Faktor. Prüfe nicht nur, ob Benutzer eine Methode registriert haben, sondern ob MFA durch Security Defaults oder geeignete Conditional-Access-Richtlinien tatsächlich wirksam verlangt wird.

SECURITY CHECK

- MFA-Status und Durchsetzung prüfen
- Administratoren besonders berücksichtigen
- Legacy per-user MFA nicht als Zielarchitektur verwenden

02 Sind administrative Konten besonders geschützt?

☐ JA	☐ NEIN	☐ UNKLAR
-----------------------------	-------------------------------	---------------------------------

Administratorkonten besitzen weitreichende Rechte und sind attraktive Angriffsziele. Für alltägliche Aufgaben sollte ein normales Benutzerkonto verwendet werden; privilegierte Konten dienen nur der Administration.

SECURITY CHECK

- getrennte Admin-Nutzung
- starke bzw. phishing-resistente Authentifizierung
- keine unnötigen Privilegien

03 Gibt es nur so viele Administratoren wie notwendig?

☐ JA☐ NEIN☐ UNKLAR

Nicht jede administrative Aufgabe benötigt Global Administrator. Das Least-Privilege-Prinzip bedeutet: nur die Berechtigungen vergeben, die für die jeweilige Aufgabe tatsächlich erforderlich sind.

SECURITY CHECK

- alle Adminrollen inventarisieren
- Begründung je Rollenzuweisung dokumentieren
- nicht benötigte Rechte kontrolliert entfernen

04 Werden Security Defaults oder Conditional Access eingesetzt?

☐ JA☐ NEIN☐ UNKLAR

Security Defaults liefern eine einfache Baseline. Conditional Access ermöglicht mit geeigneter Entra-Lizenzierung deutlich granularere Regeln. Beide Ansätze sollten bewusst gewählt und dokumentiert werden.

SECURITY CHECK

- aktuellen Ansatz feststellen
- Lizenzvoraussetzungen prüfen
- Änderungen zuerst testen

05 Existieren funktionierende Notfallkonten?

☐ JA☐ NEIN☐ UNKLAR

Für den Fall, dass reguläre Administratoren ausgesperrt sind, empfiehlt Microsoft mindestens zwei cloudbasierte Emergency-Access-Konten. Sie sollten nur für Notfälle verwendet, überwacht und regelmäßig getestet werden.

SECURITY CHECK

- mindestens zwei Cloud-only-Konten
- phishing-resistente Authentifizierung
- Nutzung alarmieren und Funktion mindestens alle 90 Tage prüfen

06 Werden verdächtige Anmeldungen kontrolliert?

☐ JA☐ NEIN☐ UNKLAR

Ein erfolgreicher Login beweist nicht automatisch, dass der legitime Benutzer angemeldet ist. Sicherheitsrelevante Anmeldungen und Warnmeldungen brauchen einen klaren Verantwortlichen und einen definierten Kontrollprozess.

SECURITY CHECK

- Verantwortlichen benennen
- Kontrollintervall festlegen
- Auffälligkeiten dokumentieren

07 Sind externe Freigaben unter Kontrolle?

☐ JA☐ NEIN☐ UNKLAR

SharePoint, OneDrive und Teams erleichtern externe Zusammenarbeit. Gleichzeitig können Daten langfristig außerhalb der Organisation zugänglich bleiben, wenn Freigaben und Gäste nicht regelmäßig überprüft werden.

SECURITY CHECK

- externe Freigaben inventarisieren
- Gastbenutzer überprüfen
- nicht mehr benötigte Zugriffe entfernen

08 Gibt es einen definierten Offboarding-Prozess?

☐ JA☐ NEIN☐ UNKLAR

Beim Austritt eines Mitarbeiters oder Dienstleisters müssen Konten, Rollen, Geräte, Gruppen, Daten und externe Anwendungen kontrolliert behandelt werden. Eine dokumentierte Checkliste verhindert Lücken.

SECURITY CHECK

- Kontosperre und Rollen
- Daten-/Mailbox-Übergabe
- Geräte und Drittanbieterzugänge

09 Gibt es einen Cybersecurity-Notfallplan?

☐ JA☐ NEIN☐ UNKLAR

Bei einem kompromittierten Konto müssen Ansprechpartner, Verantwortlichkeiten, erste technische Schritte und Kommunikationswege bereits vor dem Vorfall feststehen.

SECURITY CHECK

- interne und externe Kontakte
- erste Maßnahmen
- Incident-Dokumentation

10 Wird Microsoft 365 regelmäßig überprüft?

☐ JA☐ NEIN☐ UNKLAR

Security ist kein einmaliges Projekt. Benutzer, Berechtigungen, Geräte und Microsoft-Funktionen verändern sich. Lege deshalb feste Kontrollintervalle passend zu Risiko und Unternehmensgröße fest.

SECURITY CHECK

- monatlich: Warnungen und relevante Ereignisse
- quartalsweise: Admins, Notfallzugänge, Gäste
- jährlich: vollständiger Review

Deine Auswertung

Dieser Quick Check erzeugt bewusst keinen vermeintlichen Sicherheits-Score. Achtmal JA bedeutet nicht, dass eine Umgebung „zu 80 % sicher“ ist. Ein einzelner kritischer Punkt kann wichtiger sein als mehrere erfolgreich geprüfte Maßnahmen.

JA	___ / 10
NEIN	___ / 10
UNKLAR	___ / 10

Priorisierung

KRITISCH - mögliche unmittelbare Sicherheitslücke; kurzfristig prüfen.

WICHTIG - Maßnahme planen und zeitnah bearbeiten.

GEPRÜFT - Umsetzung dokumentieren und regelmäßig kontrollieren.

UNKLAR - Sachverhalt untersuchen und neu bewerten.

Dein persönlicher Maßnahmenplan

Problem	Maßnahme	Verantwortlich / Termin
KRITISCH 1		
KRITISCH 2		
KRITISCH 3		
WICHTIG 1		
WICHTIG 2		
WICHTIG 3		
REGELMÄSSIG 1		
REGELMÄSSIG 2		
REGELMÄSSIG 3		

Der nächste Schritt

Dieser Quick Check zeigt, wo du genauer hinschauen solltest. Der vollständige Microsoft 365 Security für KMU - Praxis- und Security-Check führt Schritt für Schritt durch Identitäten und MFA, Administratorkonten, Conditional Access, E-Mail und Phishing, SharePoint und OneDrive, Geräte und BYOD, Onboarding und Offboarding, Monitoring, Incident Response sowie einen 30-Tage-Security-Plan.

Das Ziel ist nicht, möglichst viele Security-Funktionen zu aktivieren. Das Ziel ist eine Microsoft-365-Umgebung, deren Sicherheitsmaßnahmen verstanden, bewusst konfiguriert, dokumentiert und regelmäßig überprüft werden.

ITSO - IT Security Otte

[IT Security. Verständlich. Umsetzbar.](#)

Web: itso.at

E-Mail: office@itso.at

Hinweise & Quellen

Technische Grundlage dieser Version sind Microsoft-Learn-Empfehlungen zu Microsoft 365 Business Security, Security Defaults, Conditional Access, MFA, Administratorkonten und Emergency Access. Microsoft-Dokumentation und Produktfunktionen können sich ändern; vor produktiven Änderungen sollte die jeweils aktuelle Herstellerdokumentation geprüft werden.

Rechtlicher Hinweis

Dieser Quick Check dient der allgemeinen Information und einer strukturierten Bestandsaufnahme. Er stellt weder eine Zertifizierung noch einen Penetrationstest, ein vollständiges Security-Audit oder eine Garantie für die Sicherheit einer Microsoft-365-Umgebung dar. Sicherheitsmaßnahmen sind anhand der konkreten technischen Umgebung, der eingesetzten Lizenzen, geschäftlichen Anforderungen und des individuellen Risikoprofils zu bewerten.