

DER PRAXISNAHE LEITFADEN

Microsoft 365 Security für KMU

Mehr Sicherheit.
Weniger Risiko.
Ein sorgenfreier
IT-Alltag.



KLARE ANLEITUNGEN

Speziell für
KMU entwickelt



KONKRETE UMSETZUNG

Schritt für Schritt
erklärt



REALISTISCHE BEISPIELE

Aus dem
Unternehmensalltag



CHECKLISTEN & VORLAGEN

Direkt
einsetzbar

Über diesen Guide

Dieser Guide richtet sich an kleine Unternehmen und IT-Verantwortliche, die Microsoft 365 strukturiert absichern möchten - ohne aus der Sicherheitsarbeit ein Großprojekt zu machen.

Die acht Teile führen von der Standortbestimmung über Identitäten, E-Mail, Daten und Geräte bis zu Benutzer-Lifecycle, Monitoring und Incident Response. Der Abschluss übersetzt die Ergebnisse in einen wiederholbaren Security-Betrieb und eine 90-Tage-Roadmap.

Empfohlene Verwendung:

1. Teil 1 als Bestandsaufnahme durchführen.
2. Kritische Lücken zuerst schließen.
3. Die Fachkapitel 2 bis 7 nacheinander bearbeiten.
4. Mit Teil 8 Maßnahmen, Verantwortliche und Review-Intervalle festlegen.

Der Guide ist als Arbeitsunterlage gedacht. Checklisten dürfen direkt im PDF bzw. in einer ausgedruckten Arbeitskopie verwendet werden.

ITSO PRAXISPRINZIP

Sichtbarkeit schaffen · Basisschutz umsetzen · Zugriffe begrenzen ·
Ereignisse erkennen · Vorfälle beherrschen · regelmäßig verbessern.

Inhaltsverzeichnis

Teil 1 · Standortbestimmung	5
Prüfen · Absichern · Dokumentieren	
Teil 2 · Identitäten & Zugriff	17
MFA · Conditional Access · Admins · Emergency Access	
Teil 3 · E-Mail & Phishing	28
Anti-Phishing · Safe Links · Safe Attachments · SPF · DKIM · DMARC	
Teil 4 · Daten & Zusammenarbeit	39
SharePoint · OneDrive · Teams · Gäste · externe Freigaben	
Teil 5 · Geräte & Endpoints	51
Intune · Defender for Business · Windows · Smartphones · BYOD	
Teil 6 · Benutzer-Lifecycle	66
Onboarding · Rollenwechsel · Offboarding · Dienstleister	
Teil 7 · Monitoring & Incident Response	81
Alerts · Sign-ins · Audit · kompromittierte Konten · Notfallplan	
Teil 8 · Abschluss & Security-Betrieb	96
Baseline · Routinen · Verantwortlichkeiten · 90-Tage-Roadmap	

Gesamtumfang: 106 Inhaltsseiten plus Einleitung und Hinweise.

Hinweise, Nutzung & Versionsstand

Fachlicher Hinweis

Dieser Guide ist eine praxisorientierte Sicherheits- und Arbeitsunterlage. Er ersetzt keine individuelle technische, rechtliche oder datenschutzrechtliche Beratung. Microsoft 365, Microsoft Entra, Defender, Intune und Purview werden laufend weiterentwickelt. Vor produktiven Änderungen sind die aktuelle Microsoft-Dokumentation, die tatsächlich eingesetzte Lizenzierung und die Anforderungen der eigenen Organisation zu prüfen.

Versionsstand

Gesamtausgabe v1.0 · Technischer Stand: September 2026

Urheberrecht und Nutzung

© 2026 ITSO - IT Security Otte. Alle Rechte vorbehalten.

Die erworbene Ausgabe ist für die interne Nutzung des Käufers bzw. der kaufenden Organisation bestimmt. Eine Weitergabe, Veröffentlichung oder ein Weiterverkauf des vollständigen Werks oder wesentlicher Teile davon ist ohne Zustimmung von ITSO nicht gestattet.

Kontakt

itso.at · office@itso.at

Teil 1 - Wo steht deine Microsoft-365-Umgebung heute?

Bevor wir Sicherheitsrichtlinien verändern, MFA konfigurieren oder Geräte absichern, brauchen wir einen Ausgangspunkt. Eine Microsoft-365-Umgebung wächst: Mitarbeiter werden angelegt, Administratorrechte vergeben, Geräte hinzugefügt, Dateien geteilt und externe Benutzer eingeladen. Gleichzeitig verändern sich Microsoft 365 und die verfügbaren Sicherheitsfunktionen laufend.

ITSO GRUNDPRINZIP

Wir beginnen nicht mit der Frage: Welche Security-Funktion können wir noch aktivieren?

Sondern mit: Welche Risiken bestehen in unserer Umgebung und welche Schutzmaßnahmen sind bereits vorhanden?

Nach Teil 1 kennst du

- ☐ deine eingesetzten Microsoft-365-Lizenzen
- ☐ die wichtigsten verfügbaren Sicherheitsfunktionen
- ☐ den aktuellen Microsoft Secure Score
- ☐ erste auffällige Bereiche deiner Umgebung
- ☐ deine ersten priorisierten Maßnahmen

Kapitel 1

Microsoft 365 ist eine Plattform - kein fertiges Sicherheitskonzept

Microsoft 365 stellt bereits zahlreiche Sicherheitsmechanismen bereit. Dazu gehören - abhängig von der Lizenz - Schutz vor Spam, Malware und Phishing, Identitäts- und Zugriffssteuerung, Gerätemanagement sowie weiterführender Schutz für Endgeräte, E-Mail und Unternehmensdaten.

Das bedeutet jedoch nicht, dass eine neu eingerichtete Umgebung automatisch optimal zu deinem Unternehmen passt. Sicherheit entsteht aus mehreren Ebenen, die ineinandergreifen.

Identitäten

Wer darf sich anmelden? Wie wird überprüft, dass diese Person tatsächlich der Benutzer ist? Welche zusätzlichen Anforderungen gelten für Administratoren?

Berechtigungen

Welche Benutzer besitzen administrative Rechte? Welche Daten dürfen sie sehen? Welche externen Benutzer besitzen noch Zugriff?

E-Mail

Wie werden Phishing, schädliche Links und Anhänge behandelt? Kann ein Angreifer glaubwürdig einen Geschäftsführer oder Geschäftspartner imitieren?

Daten

Wer darf Daten aus OneDrive oder SharePoint extern freigeben? Existieren alte Freigaben? Welche Informationen benötigen besonderen Schutz?

Geräte

Von welchen Computern und Smartphones darf auf Unternehmensdaten zugegriffen werden? Wie werden verlorene oder kompromittierte Geräte behandelt?

Überwachung

Wer bemerkt eine verdächtige Anmeldung? Wer reagiert auf einen Security Alert? Was passiert, wenn ein Konto kompromittiert wurde?

ERKLÄRT - SECURITY IST EIN SYSTEM

1. Was wollen wir schützen?
2. Wer oder was darf darauf zugreifen?
3. Welche Schutzmaßnahmen existieren?
4. Wie erkennen wir einen Sicherheitsvorfall?
5. Was tun wir, wenn eine Schutzmaßnahme versagt?

Häufige Fehlannahmen

„Wir verwenden Microsoft 365. Microsoft kümmert sich um die Sicherheit.“

Microsoft schützt die zugrunde liegende Plattform und stellt Sicherheitsfunktionen bereit. Die Konfiguration der eigenen Benutzer, Rollen, Geräte, Datenfreigaben und Richtlinien bleibt jedoch ein wesentlicher Teil der Verantwortung des Unternehmens.

„Wir haben MFA aktiviert. Damit sind unsere Konten sicher.“

MFA reduziert wichtige Risiken erheblich. Zusätzlich müssen wir wissen, für wen MFA tatsächlich verlangt wird, welche Authentifizierungsmethoden erlaubt sind, wie Administratoren geschützt sind und ob Ausnahmen oder Notfallzugänge existieren.

„Unser IT-Dienstleister macht das.“

Das kann stimmen. Trotzdem sollte die Geschäftsführung zumindest wissen, welche Sicherheitsmaßnahmen umgesetzt wurden und wer dafür verantwortlich ist. Security darf nicht ausschließlich von implizitem Vertrauen abhängen.

SECURITY CHECK 1

Kannst du heute eindeutig beantworten?

- ☐ Wer besitzt Global-Administrator-Rechte?
- ☐ Ist MFA für alle relevanten Benutzer wirksam?
- ☐ Wer kontrolliert Security Alerts?
- ☐ Wer darf Unternehmensdaten extern freigeben?
- ☐ Was passiert bei einem kompromittierten Microsoft-365-Konto?

Mehrere unklare Antworten bedeuten: Diese Bereiche müssen untersucht werden.

Kapitel 2

Welche Microsoft-365-Lizenz verwenden wir?

Bevor wir eine Sicherheitsfunktion konfigurieren, müssen wir prüfen, ob sie mit der vorhandenen Lizenz verfügbar ist. Für kleine und mittlere Unternehmen sind besonders Business Basic, Business Standard und Business Premium relevant.

Bereich	Basic / Standard	Business Premium
Identität	Microsoft Entra ID Free	Microsoft Entra ID P1
Conditional Access	-	enthalten
E-Mail Basisschutz	enthalten	enthalten
Defender for Office 365	-	Plan 1
Gerätemanagement	Basisfunktionen	Intune Plan 1
Endpoint Security	-	Defender for Business

LIZENZHINWEIS

Im Guide kennzeichnen wir Funktionen als BASIS, PREMIUM oder PRÜFEN. Wichtig: lizenziert, konfiguriert und wirksam sind drei unterschiedliche Zustände.

Lizenzbestand aufnehmen

Unternehmen

Microsoft-365-Tenant

Datum

Business Basic - Benutzer

Business Standard - Benutzer

Business Premium - Benutzer

Andere Microsoft-Lizenzen

Zusätzliche Security-Produkte

Kapitel 3

Der 15-Minuten-Security-Quick-Check

Dieser Check ersetzt kein vollständiges Security-Audit. Er zeigt dir, wo du zuerst genauer hinsehen solltest. Bewerte jeden Punkt mit JA, NEIN oder UNKLAR.

Kontrolle	JA	NEIN	UNKLAR
1. Ist MFA für alle Benutzer wirksam?	☐	☐	☐
2. Sind administrative Konten besonders geschützt?	☐	☐	☐
3. Gibt es nur so viele Administratoren wie notwendig?	☐	☐	☐
4. Werden Security Defaults oder Conditional Access eingesetzt?	☐	☐	☐
5. Existieren funktionierende Notfallzugänge?	☐	☐	☐
6. Werden verdächtige Anmeldungen und Security Alerts kontrolliert?	☐	☐	☐
7. Sind externe Freigaben unter Kontrolle?	☐	☐	☐
8. Gibt es einen definierten Offboarding-Prozess?	☐	☐	☐
9. Gibt es einen dokumentierten Cybersecurity-Notfallplan?	☐	☐	☐
10. Wird Microsoft 365 regelmäßig überprüft?	☐	☐	☐

Das war die Leseprobe.

Die Vollversion umfasst 110 Seiten und führt den Security-Check Schritt für Schritt durch alle zentralen Bereiche einer Microsoft-365-Umgebung:

Identitäten & Zugriff · E-Mail & Phishing · Daten & Zusammenarbeit
Geräte & Endpoints · Benutzer-Lifecycle · Monitoring & Incident Response
sowie eine 90-Tage-Roadmap für den laufenden Security-Betrieb.

MICROSOFT 365 SECURITY FÜR KMU

Gesamtausgabe v1.1 · ITSO - IT Security Otte

itso.at

office@itso.at