Microsoft 365 sicher einführen und betreiben

Leitfaden für den Mittelstand

Datenstandort, Zugriffsschutz, Datensicherung, E-Mail-Sicherheit und KI: die Punkte, die Sie vor und nach der Umstellung klären sollten.

Stand: Oktober 2026

conpro IT Solutions GmbH, Kurfürstendamm 30, 10719 Berlin

Inhalt

Kurzfassung 3
1 Ausgangslage 2026 3
2 Cloud, eigener Server oder beides 4
3 Datenstandort und Pflichten 5
4 Identität und Zugriff 5
5 Datensicherung und Archivierung 6
6 E-Mail-Sicherheit 7
7 KI und Copilot vorbereiten 7
8 Migration in Phasen 8
9 Checkliste 9
10 So unterstützt conpro 10
11 Quellen 11
Kontakt 12

Über diesen Leitfaden

Der Leitfaden richtet sich an Geschäftsführung und IT-Leitung in Unternehmen mit 20 bis 200 Arbeitsplätzen sowie an Informationssicherheits- und Datenschutzbeauftragte. Die Kurzfassung auf der nächsten Seite gibt den Überblick für Entscheidungen. Die Kapitel 1 bis 8 erläutern die Einzelheiten, Kapitel 9 fasst alles in einer Checkliste zusammen.

Rechtliche Themen werden allgemein dargestellt. Der Leitfaden ersetzt keine Rechtsberatung. Produktnamen, Funktionen und Rechtslage ändern sich, maßgeblich ist der Stand auf der Titelseite.

Kurzfassung

Für viele mittelständische Unternehmen ist Microsoft 365 heute der zentrale Arbeitsplatz: E-Mail, Dateien, Besprechungen und zunehmend auch KI laufen über denselben Dienst. Die Frage lautet deshalb selten noch, ob Sie Microsoft 365 nutzen, sondern wie sicher, nachweisbar und wirtschaftlich Ihre Umgebung eingerichtet ist. Sieben Punkte entscheiden darüber.

- **Eigenen Exchange-Server ablösen.** Exchange Server 2016 und 2019 erhalten seit dem 14.10.2025 keine Sicherheitsupdates mehr. Wer sie weiter betreibt, lässt ein Kernsystem mit bekannten Lücken am Netz. Das Ziel ist Exchange Online in Microsoft 365 (Kapitel 1 und 2).
- **Pflichten klären.** Mit dem NIS-2-Umsetzungsgesetz gelten für deutlich mehr Unternehmen Pflichten zu Risikomanagement, Meldung von Vorfällen und Schulung der Geschäftsleitung. Prüfen Sie, ob Sie betroffen sind, auch mittelbar als Lieferant (Kapitel 3).
- **Anmeldungen absichern.** Mehr-Faktor-Authentifizierung für alle Konten ist der wirksamste einzelne Schritt gegen gestohlene Zugangsdaten (Kapitel 4).
- **Daten selbst sichern.** Microsoft hält die Dienste verfügbar. Einen unabhängigen, wiederherstellbaren Stand Ihrer Daten organisieren Sie selbst. Die Archivierung von E-Mails ist eine eigene Aufgabe (Kapitel 5).
- **Das Postfach schützen.** Eine Prüfung vor dem Postfach, SPF, DKIM und DMARC für Ihre Domain und aufmerksame Mitarbeitende greifen ineinander (Kapitel 6).
- **Vor KI die Berechtigungen ordnen.** Copilot findet alles, worauf eine Person Zugriff hat. Zu weit gefasste Freigaben werden damit sichtbar (Kapitel 7).
- **Geordnet umziehen.** Eine Migration in drei Phasen mit Prüfung am Ende vermeidet Datenverluste und Überraschungen im Betrieb (Kapitel 8).

Die Checkliste in Kapitel 9 übersetzt diese Punkte in Prüffragen, die Sie mit Ihrer IT-Leitung oder Ihrem Dienstleister durchgehen können.

1 Ausgangslage 2026

Drei Entwicklungen haben die Anforderungen an eine Microsoft-365-Umgebung seit 2025 verändert.

Lokale Exchange-Server ohne Updates

Microsoft hat den Support für Exchange Server 2016 und Exchange Server 2019 am 14.10.2025 beendet. Seitdem erscheinen für diese Versionen keine Sicherheitsupdates mehr [6, 7]. Ein E-Mail-Server ist aus dem Internet erreichbar und verarbeitet täglich Inhalte von außen. Schwachstellen, die jetzt noch entdeckt werden, bleiben auf diesen Systemen dauerhaft offen. Für Unternehmen mit Pflichten nach NIS-2 ist ein solcher Betrieb kaum mit dem geforderten Stand der Technik zu vereinbaren.

NIS-2 erweitert den Kreis der Pflichtigen

Die europäische NIS-2-Richtlinie ist in Deutschland mit dem Gesetz zur Umsetzung der NIS-2-Richtlinie (NIS-2-Umsetzungsgesetz) umgesetzt. Es ist am 6. Dezember 2025 in Kraft getreten, die Pflichten gelten seitdem ohne Übergangsfrist [2]. Betroffen sind deutlich mehr Unternehmen als unter den früheren KRITIS-Regeln. Sie müssen sich beim BSI registrieren, Maßnahmen zum Risikomanagement umsetzen und erhebliche Sicherheitsvorfälle melden. Die Geschäftsleitung muss die Maßnahmen billigen, ihre Umsetzung überwachen und an Schulungen teilnehmen [1].

KI-Assistenten arbeiten mit vorhandenen Daten

Mit Microsoft Copilot (bisher Microsoft 365 Copilot) arbeitet ein KI-Assistent direkt mit E-Mails, Dateien, Chats und Besprechungen. Er zeigt nur Inhalte, für die eine Person mindestens Leserechte hat [5]. Das ist Schutz und Prüfstein zugleich: Wo Freigaben über Jahre gewachsen sind, macht Copilot sichtbar, was nie für alle gedacht war.

2 Cloud, eigener Server oder beides

Für die meisten Unternehmen ist nicht die Frage, ob alles in die Cloud wandert, sondern was wohin gehört. Häufig ist eine Kombination sinnvoll: E-Mail, Dateien und Zusammenarbeit in Microsoft 365, Fachanwendungen oder Datenbanken auf Servern im eigenen Haus oder in einem Rechenzentrum.

Kriterien für Ihre Entscheidung

- **Anwendungen:** Welche Programme brauchen einen eigenen Server, welche gibt es als Clouddienst?
- **Datenarten:** Welche Daten sind besonders schutzbedürftig, und welche Vorgaben machen Auftraggeber, Verbände oder Aufsichtsbehörden?
- **Funktionen:** Die Lösung sollte eine zentrale Ablage, E-Mail und Kalender, Zusammenarbeit im Team, eine zentrale Verwaltung der Benutzer und eine Anmeldung mit zweitem Faktor bieten.
- **Kosten über mehrere Jahre:** Lizenzen, Betrieb, Hardware, Datensicherung und der Aufwand für Updates gehören in eine gemeinsame Rechnung.
- **Zuständigkeit:** Wer betreut die Umgebung im Alltag, wer vertritt im Urlaub, wer reagiert im Notfall?

Exchange: der Weg zu Exchange Online

Für Unternehmen, die noch Exchange Server 2016 oder 2019 betreiben, empfiehlt conpro den Wechsel zu Exchange Online in Microsoft 365. Updates, Verfügbarkeit und Weiterentwicklung des Dienstes liegen dann bei Microsoft, Ihr Team arbeitet mit Outlook weiter. Microsoft bietet für den lokalen Betrieb zwar eine Nachfolgeversion im Abonnement an, die Exchange Server Subscription Edition [7]. Sie verlangt aber weiterhin eigene Server, regelmäßige Updates und Fachwissen im Haus.

Zugriffsschutz, Datensicherung, Archivierung und Berechtigungen bleiben auch nach dem Umzug Ihre Aufgabe (Kapitel 4 bis 7).

> **Und Google Workspace?**
> Google Workspace bündelt E-Mail, Kalender, Dokumente und Videokonferenzen ebenfalls in einem Clouddienst. Es kann passen, wenn Ihr Team bereits damit arbeitet oder überwiegend im Browser arbeitet. Prüfen Sie vor einer Entscheidung vor allem, ob Ihre Fachanwendungen mit der Plattform zusammenarbeiten, wie Sie Datensicherung und Archivierung lösen und welche Kenntnisse Ihr Team mitbringt.
> conpro richtet beide Plattformen ein und betreut sie. Migriert werden E-Mails, Kontakte und Kalender von einem Exchange-Server, von E-Mail-Anbietern mit IMAP-Zugang, aus Google Workspace oder aus einem anderen Microsoft-365-Mandanten, jeweils zu Microsoft 365 oder Google Workspace. E-Mail Security und E-Mail-Archivierung von conpro arbeiten mit beiden Plattformen. Dieser Leitfaden behandelt Microsoft 365, viele Prüfpunkte gelten für Google Workspace sinngemäß.

3 Datenstandort und Pflichten

Wo Microsoft Ihre Daten verarbeitet

Microsoft hat die EU Data Boundary im Februar 2025 abgeschlossen. Kundendaten und pseudonymisierte personenbezogene Daten der Kerndienste, darunter Microsoft 365, werden seitdem in der EU und der EFTA gespeichert und verarbeitet, ebenso Daten aus dem technischen Support [4]. Für Copilot gilt: Anfragen von Nutzern in der EU bleiben innerhalb der EU Data Boundary [5].

Es gibt Ausnahmen, die Sie kennen sollten. Ist die Websuche in Copilot aktiviert, gehen daraus abgeleitete Suchanfragen an den Dienst Bing. Außerdem lassen sich KI-Modelle von Drittanbietern zuschalten. Modelle von Anthropic sind nach Angaben von Microsoft derzeit von der EU Data Boundary ausgenommen [5]. Ob diese Funktionen genutzt werden, entscheiden Sie als Administrator.

Ihre Verantwortung nach der DSGVO

Der Ort der Verarbeitung ändert nichts daran, dass Ihr Unternehmen für personenbezogene Daten verantwortlich bleibt. Dazu gehören der Vertrag zur Auftragsverarbeitung, ein Eintrag im Verzeichnis der Verarbeitungstätigkeiten, ein Löschkonzept und die Abstimmung mit Ihrer Datenschutzbeauftragten oder Ihrem Datenschutzbeauftragten.

NIS-2: was das für Microsoft 365 bedeutet

Ob Ihr Unternehmen unter NIS-2 fällt, hängt vor allem von Sektor und Größe ab. Einen ersten Anhaltspunkt gibt die Betroffenheitsprüfung des BSI. Betroffene Unternehmen müssen sich beim BSI registrieren. Die gesetzliche Frist dafür ist abgelaufen, wer noch nicht registriert ist, soll das nach Hinweis des BSI sofort nachholen [1]. Auch wer nicht selbst betroffen ist, erhält oft Sicherheitsanforderungen von Kunden, die unter NIS-2 fallen.

Die Richtlinie nennt Mindestmaßnahmen, die Microsoft 365 direkt betreffen, darunter die Aufrechterhaltung des Betriebs mit Backup-Management sowie Mehr-Faktor-Authentifizierung [3]. Erhebliche Vorfälle sind gestuft zu melden: eine frühe Warnung innerhalb von 24 Stunden, eine Meldung innerhalb von 72 Stunden und ein Abschlussbericht spätestens einen Monat nach der Meldung [3]. Die Verantwortung bleibt bei der Geschäftsleitung und lässt sich nicht an einen Dienstleister abgeben.

> **Hinweis**
> Dieses Kapitel gibt einen allgemeinen Überblick und ersetzt keine Rechtsberatung. Die verbindliche Einordnung Ihres Unternehmens nehmen Sie mit Ihrer Rechtsberatung vor.

4 Identität und Zugriff

Viele Angriffe auf Microsoft 365 beginnen nicht mit einer technischen Lücke, sondern mit einem gestohlenen Passwort, etwa aus einer Phishing-E-Mail. Der Zugriffsschutz ist deshalb der erste Baustein einer sicheren Umgebung.

Mehr-Faktor-Authentifizierung für alle Konten

Microsoft empfiehlt eine Grundregel, die für alle Benutzer und alle Anwendungen einen zweiten Faktor verlangt. Ausgenommen werden nur Notfallkonten, die gesondert geschützt sind [8]. Bevorzugen Sie Verfahren, die gegen Phishing widerstandsfähig sind, etwa Passkeys oder Sicherheitsschlüssel nach FIDO2, gegenüber Codes per SMS.

Für seine Verwaltungsportale setzt Microsoft die Mehr-Faktor-Authentifizierung inzwischen selbst durch: für das Azure-Portal, das Microsoft Entra Admin Center und das Intune Admin Center seit Oktober 2024, für das Microsoft 365 Admin Center seit Februar 2025, jeweils schrittweise [9]. Für die Konten Ihrer Mitarbeitenden gilt das nicht automatisch.

Bedingter Zugriff und Lizenzen

Mit Regeln für den bedingten Zugriff (Conditional Access) legen Sie fest, unter welchen Bedingungen eine Anmeldung erlaubt ist, zum Beispiel nur mit zweitem Faktor oder nur von verwalteten Geräten. Diese Funktion setzt eine Lizenz mit Microsoft Entra ID P1 oder P2 voraus. Ohne sie bieten die Sicherheitsstandards von Microsoft (Security Defaults) einen einfacheren Grundschutz [9].

Die Microsoft-365-Tarife unterscheiden sich deutlich in ihren Sicherheitsfunktionen. Welcher Tarif passt, hängt von der Zahl der Arbeitsplätze, Ihren Geräten und Ihren Pflichten ab. conpro berät Sie bei der Auswahl im Rahmen des Cloud-Lizenzmanagements.

Konten und Rechte ordnen

- // Eigene Konten für die Administration, die nicht für E-Mail und Alltagsarbeit genutzt werden.
- // Mindestens ein Notfallzugang, sicher hinterlegt und dokumentiert, falls die normale Anmeldung ausfällt.
- // Regelmäßige Prüfung, wer welche Rechte hat, besonders nach Austritten und Wechseln der Abteilung.
- // Gastzugänge für Externe mit Ablaufdatum und regelmäßiger Durchsicht.
- // Zentral verwaltete, aktuelle und verschlüsselte Endgeräte, denn eine sichere Anmeldung nützt wenig auf einem kompromittierten Gerät.

5 Datensicherung und Archivierung

Verfügbarkeit ist keine Datensicherung

Microsoft betreibt Microsoft 365 mit mehrfach vorgehaltenen Daten in redundanten Rechenzentren. Das schützt vor dem Ausfall von Technik. Gegen versehentliches Löschen, Überschreiben oder die Verschlüsselung durch Schadsoftware im eigenen Mandanten brauchen Sie dagegen einen früheren, unabhängigen Stand Ihrer Daten.

Microsoft bietet dafür mit Microsoft 365 Backup ein eigenes Produkt an, das SharePoint, OneDrive und Exchange Online sichert und zusätzlich nach Verbrauch abgerechnet wird. Als Einsatzfälle nennt Microsoft unter anderem Ransomware sowie versehentliches oder böswilliges Löschen [10]. Eine Datensicherung in diesem Sinn gehört also nicht zum Standardumfang von Microsoft 365.

Worauf Sie bei einer Sicherung achten sollten

- // **Umfang:** Postfächer einschließlich freigegebener Postfächer, OneDrive, SharePoint und Teams.
- // **Häufigkeit:** mehrmals täglich, damit im Ernstfall wenig Arbeit verloren geht.
- // **Schutz der Sicherung:** verschlüsselt, mit bekanntem Speicherort und geschützt gegen Veränderung durch Angreifer.
- // **Überwachung:** Jemand prüft, ob jede Sicherung erfolgreich war, und reagiert auf Fehler.
- // **Wiederherstellung:** Sie wissen, wer sie auslöst und wie lange sie dauert, und Sie haben sie getestet.

Archivierung ist eine eigene Aufgabe

Ein Backup schützt vor Verlust. Es hält Stände für eine begrenzte Zeit vor und ersetzt sie später durch neuere. Geschäftliche E-Mails müssen Sie dagegen je nach Inhalt über Jahre vollständig und unveränderbar aufbewahren, wie es die GoBD verlangen. Das leistet eine Archivierung, die jede ein- und ausgehende E-Mail ab dem Zeitpunkt der Aktivierung erfasst. Für den Datenschutz ist ebenso wichtig, dass sie E-Mails nach Ablauf der Fristen wieder löschen kann.

6 E-Mail-Sicherheit

Das Postfach bleibt ein häufiges Einfallstor. Phishing zielt auf Zugangsdaten, Anhänge und Links bringen Schadsoftware ins Netz, gefälschte Absender veranlassen Überweisungen. Mit KI geschriebene Phishing-E-Mails sind sprachlich oft kaum noch von echten zu unterscheiden. Wirksam ist ein Schutz in drei Schichten.

- **Prüfung vor dem Postfach:** Microsoft 365 bringt einen eigenen Schutz mit. Eine vorgeschaltete Prüfung mit weiteren Virenscannern, Spamfilter und Linkprüfung ergänzt ihn und fängt E-Mails ab, bevor sie das Postfach erreichen.
- **Schutz Ihrer Domain:** Drei DNS-Einträge regeln, wer in Ihrem Namen E-Mails senden darf. SPF legt die berechtigten Server fest, DKIM versieht ausgehende E-Mails mit einer digitalen Signatur, und DMARC teilt empfangenden Servern mit, wie sie mit E-Mails umgehen sollen, die diese Prüfungen nicht bestehen. Zusammen erschweren sie es Angreifern, Ihre Domain zu fälschen.
- **Aufmerksame Mitarbeitende:** Kein Filter erkennt jede Phishing-E-Mail. Kurze, regelmäßige Schulungen und ein einfacher Weg, verdächtige E-Mails zu melden, schließen die verbleibende Lücke.

> **Praxistipp DMARC**
> Führen Sie DMARC schrittweise ein: zunächst nur beobachten und die Berichte auswerten, dann verdächtige E-Mails in die Quarantäne leiten und erst zuletzt abweisen. So vermeiden Sie, dass legitime E-Mails verloren gehen, etwa aus einem Newsletter-Dienst oder einer Fachanwendung, die in Ihrem Namen sendet.

7 KI und Copilot vorbereiten

Microsoft Copilot arbeitet mit den Daten, auf die die angemeldete Person zugreifen darf [5]. Copilot umgeht keine Berechtigungen, kann aber finden, was über Jahre zu weit freigegeben wurde: die Gehaltsliste in einer offenen Teamablage oder das Vertragsarchiv mit einem Link für alle im Unternehmen. Vor der Einführung lohnt deshalb eine Bestandsaufnahme.

Vor der Einführung

- **Berechtigungen prüfen:** Wer hat Zugriff auf welche Teams, SharePoint-Seiten und freigegebenen Ordner? Links für alle Personen im Unternehmen verdienen besondere Aufmerksamkeit.
- **Datenablage ordnen:** Veraltete Ablagen archivieren oder löschen, für jede Ablage eine verantwortliche Person festlegen.
- **Vertraulichkeit kennzeichnen:** Vertraulichkeitsstufen für besonders schutzbedürftige Inhalte festlegen. Bei verschlüsselten Inhalten beachtet Copilot die Nutzungsrechte der jeweiligen Person [5].
- **KI-Richtlinie beschließen:** Welche Dienste sind erlaubt, welche Daten dürfen eingegeben werden, und wer prüft Ergebnisse, bevor sie das Haus verlassen?

- **Einstellungen festlegen:** Websuche, Modelle von Drittanbietern und Agenten bewusst freigeben oder sperren (siehe Kapitel 3).
- **Klein beginnen:** Mit einer Pilotgruppe starten und die Erfahrungen auswerten, bevor Copilot für alle freigegeben wird.

Datenschutz und Schulung

Microsoft sagt zu, dass Eingaben, Antworten und die über Microsoft Graph abgerufenen Daten nicht zum Training der zugrunde liegenden Sprachmodelle verwendet werden [5]. Welche Lizenzen Sie für Copilot brauchen, hängt von Ihrem bestehenden Microsoft-365-Tarif ab.

Art. 4 der EU-KI-Verordnung verpflichtet Unternehmen, die KI-Systeme einsetzen, seit dem 2. Februar 2025 zu Maßnahmen für die KI-Kompetenz ihrer Beschäftigten. Seit dem 27. Juli 2026 gilt eine geänderte Fassung: Sie müssen Maßnahmen ergreifen, um die Entwicklung der KI-Kompetenz zu unterstützen, ein bestimmtes Kompetenzniveau müssen Sie nicht garantieren [11]. Unabhängig davon sollten Beschäftigte wissen, wo KI-Werkzeuge Fehler machen und welche Daten nicht eingegeben werden dürfen. Dokumentieren Sie die Schulungen.

8 Migration in Phasen

Jede Umstellung ist anders, der Ablauf folgt aber festen Schritten. Entscheidend ist die Prüfung am Ende.

Phase 1: Analyse, Planung und Vorbereitung

Am Anfang steht die Bestandsaufnahme des Quellsystems: Postfächer, freigegebene Postfächer, Verteiler, Weiterleitungen, Regeln, Datenmengen sowie angebundene Geräte und Programme. Räumen Sie vor dem Umzug auf, denn was nicht mehr gebraucht wird, muss auch nicht migriert werden. Ziel, Reihenfolge und Zeitplan werden gemeinsam festgelegt, das Zielsystem wird samt Zugriffsschutz eingerichtet, bevor die ersten Daten umziehen.

Phase 2: Migration

E-Mails, Kontakte und Kalender werden aus dem alten in das neue System übertragen, in der Regel bei laufendem Betrieb und in Gruppen. Arbeitet Ihr Team bereits im neuen System, werden die Daten nach und nach sichtbar. Welche weiteren Daten umziehen, zum Beispiel Dateiablagen, legen Sie in der Planung fest.

Phase 3: Prüfung und Nachbereitung

Nach der Übertragung wird geprüft, ob alle Inhalte vollständig angekommen sind, kleine Fehler werden sofort behoben. Erst danach wird das alte System geordnet abgeschaltet, mit einer Aufbewahrung der Altdaten, die zu Ihren Fristen passt. Ihr Team erhält eine Einarbeitung, und die neue Umgebung wird dokumentiert.

Häufige Fehlerquellen

- vergessene freigegebene Postfächer, Verteiler, Ressourcenpostfächer, Weiterleitungen und Postfachregeln
- DNS-Einträge für E-Mail wie MX, Autodiscover und SPF, die zu früh, zu spät oder unvollständig umgestellt werden
- Smartphones und Tablets, die weiter mit dem alten Server verbunden sind
- Scanner, Drucker oder Fachanwendungen, die E-Mails direkt versenden
- fehlende Datensicherung und Archivierung ab dem ersten Tag im neuen System

9 Checkliste

Gehen Sie die Punkte mit Ihrer IT-Leitung oder Ihrem Dienstleister durch. Offene Punkte sind ein guter Ausgangspunkt für Ihre nächsten Schritte.

	Prüfpunkt	Notiz / erledigt am
Strategie und Pflichten (Kapitel 2 und 3)		
☐	Kein Exchange Server 2016 oder 2019 mehr im Betrieb, oder ein Termin für die Umstellung steht fest.	
☐	Für jede Anwendung ist entschieden, ob sie in Microsoft 365, auf einem eigenen Server oder im Rechenzentrum läuft.	
☐	NIS-2-Betroffenheit geprüft und dokumentiert, bei Bedarf Registrierung beim BSI erfolgt.	
☐	Vertrag zur Auftragsverarbeitung geprüft, Microsoft 365 im Verzeichnis der Verarbeitungstätigkeiten eingetragen.	
☐	Meldeweg für Sicherheitsvorfälle festgelegt, Zuständigkeiten und Vertretung benannt.	
Identität und Zugriff (Kapitel 4)		
☐	Mehr-Faktor-Authentifizierung für alle Konten aktiv, bevorzugt phishingresistent.	
☐	Eigene Administratorkonten und ein dokumentierter Notfallzugang vorhanden.	
☐	Regeln für den bedingten Zugriff oder die Sicherheitsstandards von Microsoft aktiv.	
☐	Berechtigungen und Gastzugänge zuletzt geprüft am:	
☐	Endgeräte zentral verwaltet, aktuell und verschlüsselt.	
Datensicherung und Archivierung (Kapitel 5)		
☐	Postfächer, OneDrive, SharePoint und Teams werden mehrmals täglich unabhängig gesichert, der Erfolg wird überwacht.	
☐	Wiederherstellung zuletzt getestet am:	
☐	E-Mails werden vollständig und unveränderbar archiviert, Löschfristen sind festgelegt.	
E-Mail-Sicherheit (Kapitel 6)		
☐	Eingehende E-Mails werden vor dem Postfach auf Schadsoftware, Spam und gefährliche Links geprüft.	
☐	SPF, DKIM und DMARC sind für alle genutzten Domains eingerichtet.	
☐	Mitarbeitende sind geschult, der Meldeweg für verdächtige E-Mails ist bekannt.	
KI und Migration (Kapitel 7 und 8)		
☐	Berechtigungen und Datenablage vor der Einführung von Copilot geprüft.	
☐	KI-Richtlinie beschlossen, Schulungen dokumentiert.	
☐	Websuche, Modelle von Drittanbietern und Agenten bewusst freigegeben oder gesperrt.	
☐	Nach der Migration Vollständigkeit geprüft und altes System geordnet abgeschaltet.	

10 So unterstützt conpro

conpro IT Solutions GmbH betreut mittelständische Unternehmen in Berlin und Brandenburg mit festen Ansprechpartnern und einer Regelreaktionszeit unter zwei Stunden. Rund um Microsoft 365 erhalten Sie diese Leistungen:

- **Microsoft 365 und Google Workspace:** Sie erhalten Einrichtung, Anbindung an Ihre bestehende IT und Betreuung im laufenden Betrieb. conproit.de/portfolio/cloud-services/
- **Migration:** Sie erhalten Planung, Durchführung und Nachbereitung Ihres Umzugs aus einer Hand, mit festen Ansprechpartnern vor, während und nach der Migration. conproit.de/managed-services/conpro-migration-service/
- **Zugriffsschutz:** Sie erhalten die Einrichtung von Mehr-Faktor-Authentifizierung und bedingtem Zugriff in Microsoft 365 als eigene Leistung, unabhängig davon, ob Sie unter NIS-2 fallen.
- **365 Backup:** Postfächer, freigegebene Postfächer, OneDrive, SharePoint Online und Teams werden sechsmal am Tag automatisch und verschlüsselt gesichert und von conpro überwacht. Wiederherstellungsanfragen bearbeitet der Support innerhalb von acht Arbeitsstunden während der Bürozeiten. conproit.de/managed-services/conpro-365-backup/
- **E-Mail-Archivierung:** Sie archivieren alle ein- und ausgehenden E-Mails vollständig und unveränderbar nach den Vorgaben der GoBD, auch für Microsoft 365 (Exchange Online) und Google Workspace. conproit.de/managed-services/conpro-e-mail-archive/
- **E-Mail Security:** Zwei Virenscanner, Spamfilter und Linkprüfung prüfen jede eingehende E-Mail vor dem Postfach, betrieben in einem deutschen Rechenzentrum. Die Einrichtung umfasst die Konfiguration Ihrer Domains und die nötigen DNS-Einträge (MX und SPF). Zusätzlich erhalten Sie die Einrichtung von DKIM und DMARC für Ihre Domains. conproit.de/managed-services/conpro-e-mail-security/
- **Cloud-Lizenzmanagement:** Sie erhalten den Überblick über Lizenzen und Laufzeiten, die zeitnahe Anpassung bei Ein- und Austritten und eine Empfehlung, welcher Tarif zu den Aufgaben Ihrer Mitarbeitenden passt, auch für Copilot. conproit.de/managed-services/conpro-cloud-lizenzmanagement/
- **Client Management:** Ihre Arbeitsplätze und Notebooks werden zentral verwaltet, mit Updates, Virenschutz und Festplattenverschlüsselung auf Basis von BitLocker. conproit.de/managed-services/conpro-client-management/
- **KI im Unternehmen:** Sie erhalten Beratung, die Vorbereitung von Berechtigungen und Datenbasis für Copilot, Unterstützung bei der KI-Richtlinie und Schulungen für Ihre Beschäftigten. conproit.de/ki/
- **NIS-2 und KRITIS:** Sie erfahren, ob und wie Ihr Unternehmen betroffen ist, und erhalten einen priorisierten Maßnahmenplan, die technische Umsetzung und Unterlagen für Nachweise. conproit.de/it-sicherheit/nis-2-kritis/
- **Cyber-Risiko-Check:** Sie beantworten Fragen zu sechs Bereichen Ihrer IT-Sicherheit nach DIN SPEC 27076 und erhalten im Auswertungsgespräch eine Einschätzung mit priorisierten Empfehlungen. conproit.de/it-sicherheit/cyber-risiko-check/

conpro ist Microsoft Solutions Partner für Modern Work.



Ihr Einstieg: das Erstgespräch
Sie schildern Ihre Ausgangslage, wir gehen gemeinsam die offenen Punkte der Checkliste durch und legen die nächsten Schritte fest. conproit.de/erstgespraech/

11 Quellen

Die Angaben in eckigen Klammern im Text verweisen auf diese Quellen. Produktnamen, Funktionen und Rechtslage ändern sich, dieser Leitfaden wird jährlich überprüft.

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI): NIS-2-regulierte Unternehmen. https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/nis-2-regulierte-unternehmen_node.html (abgerufen am 20.10.2026)

[2] Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung vom 2. Dezember 2025, BGBl. 2025 I Nr. 301 vom 5. Dezember 2025, in Kraft seit 6. Dezember 2025. https://www.recht.bund.de/bgbl/1/2025/301/VO.html (abgerufen am 21.10.2026)

[3] Richtlinie (EU) 2022/2555 (NIS-2), Art. 21 und Art. 23, Amtsblatt der Europäischen Union. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[4] Microsoft On the Issues, 26.02.2025: Microsoft completes landmark EU Data Boundary. https://blogs.microsoft.com/on-the-issues/2025/02/26/microsoft-completes-landmark-eu-data-boundary-offering-enhanced-data-residency-and-transparency/ (abgerufen am 21.10.2026)

[5] Microsoft Learn: Data, Privacy, and Security for Microsoft Copilot, aktualisiert am 08.10.2026. https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-privacy (abgerufen am 21.10.2026)

[6] Microsoft Learn: Exchange Server 2019, Microsoft Lifecycle. https://learn.microsoft.com/en-us/lifecycle/products/exchange-server-2019 (abgerufen am 21.10.2026)

[7] CodeTwo: Exchange 2016/2019 end of life. https://www.codetwo.com/admins-blog/exchange-2016-2019-eol/ (abgerufen am 20.10.2026)

[8] Microsoft Learn: Require MFA for all users with Conditional Access, Stand 24.03.2026. https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-all-users-mfa-strength (abgerufen am 20.10.2026)

[9] Microsoft Learn: Plan for mandatory Microsoft Entra multifactor authentication. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mandatory-multifactor-authentication (abgerufen am 21.10.2026)

[10] Microsoft Learn: Overview of Microsoft 365 Backup, aktualisiert am 18.09.2026. https://learn.microsoft.com/en-us/microsoft-365/backup/backup-overview (abgerufen am 21.10.2026)

[11] Verordnung (EU) 2024/1689 (KI-Verordnung), Art. 4, in der Fassung der Verordnung (EU) 2026/1744 vom 8. Juli 2026, ABl. L 2026/1744 vom 24. Juli 2026, in Kraft seit 27. Juli 2026. https://eur-lex.europa.eu/eli/reg/2026/1744/oj (abgerufen am 21.10.2026)

Kontakt

Sie haben Fragen zu Ihrer Microsoft-365-Umgebung oder möchten die Checkliste gemeinsam durchgehen? Sprechen Sie uns an.

Dennis Eichler

Geschäftsführer
Telefon: +49 30 7675813-00 (Zentrale)
E-Mail: info@conproit.de
Erstgespräch vereinbaren: conproit.de/erstgespraech/

conpro IT Solutions GmbH
Kurfürstendamm 30
10719 Berlin
conproit.de



Stand: Oktober 2026. Dieser Leitfaden gibt einen allgemeinen Überblick und ersetzt keine Rechtsberatung. Alle Angaben ohne Gewähr, maßgeblich sind die Dokumentationen der Hersteller und die gesetzlichen Vorgaben.

Microsoft, Microsoft 365, Exchange, Outlook, OneDrive, SharePoint, Teams, Copilot, Entra und Intune sind Marken der Microsoft-Unternehmensgruppe. Google Workspace ist eine Marke von Google LLC.