BR-Systems

MODERN WORKPLACE SECURITY 2026

Microsoft 365 sicher betreiben

Identitäten, Berechtigungen, Endgeräte, Daten und Wiederherstellung als zusammenhängendes Betriebsmodell

Dokument-ID	BR-WP-M365-003
Version	1.0
Fachstand	24. März 2026
Veröffentlicht	7. April 2026
Klassifizierung	Öffentlich – kostenfreier Fachbeitrag
Autor	Benjamin Raulf, BR-Systems
Herausgeber	BR-Systems · IT-Systemhaus · Unterlüß
Standort zum Fachstand	Unterlüß
Kontakt	info@br-systems.eu · https://br-systems.eu · +49 179 1601700

Executive Summary

Dieses Whitepaper übersetzt aktuelle Anforderungen und technische Entwicklungen in einen umsetzbaren Betriebsansatz. Im Mittelpunkt stehen nicht einzelne Produkte, sondern Verantwortlichkeiten, überprüfbare Kontrollen und ein realistischer Weg vom heutigen Zustand zu einer belastbaren Zielarchitektur.

Die vier wichtigsten Aussagen

- Phishing-resistente MFA und saubere Administratorrollen etablieren
- Conditional Access, Gerätevertrauen und Gastzugriffe strukturieren
- SharePoint, Teams, Copilot und Datenfreigaben kontrollierbar halten
- Backup, Protokollierung und Reaktion vor einem Vorfall klären

Inhalt

1. Der Tenant ist ein produktives Rechenzentrum
2. Identitäten zuerst schützen
3. Geräte und Anwendungen einbeziehen
4. Teams, SharePoint und Copilot verantwortbar nutzen
5. E-Mail, Protokolle und Reaktion
6. Backup, Wiederherstellung und laufender Betrieb
7. Vom Konzept zum belastbaren Betrieb

Praxis-Checkliste

Quellen und weiterführende Informationen

1. Der Tenant ist ein produktives Rechenzentrum

Microsoft 365 wird im Alltag gern als Paket aus E-Mail, Office und Teams betrachtet. Technisch ist der Tenant jedoch eine zentrale Betriebsplattform für Identitäten, Kommunikation, Dateien, Geräte, Berechtigungen und Anwendungen. Wer den Tenant kompromittiert, erhält unter Umständen Zugriff auf weit mehr als ein Postfach. Deshalb reicht es nicht, Lizenzen zu bestellen und Benutzer anzulegen. Die Umgebung benötigt ein Betriebsmodell mit Rollen, Standards, Änderungen, Monitoring, Backup und Notfallverfahren.

Microsoft beschreibt im Digital Defense Report 2025 eine Bedrohungslage, in der finanziell motivierte Akteure, Infostealer, Phishing, ungepatchte Systeme und exponierte Dienste eine große Rolle spielen [1]. Identitätsangriffe sind besonders attraktiv, weil ein gültiges Konto Sicherheitsgrenzen scheinbar legitim passiert. Zugleich verändern Cloud und KI die Geschwindigkeit von Angriff und Verteidigung. Für kleinere Unternehmen folgt daraus keine Pflicht zu maximaler Komplexität. Es folgt die Pflicht zu einer klaren Basis, die konsequent betrieben wird.

Die Verantwortung ist geteilt. Microsoft schützt die Plattform und stellt Sicherheitsfunktionen bereit. Das Unternehmen bleibt für Benutzer, Rollen, Freigaben, Geräte, Datenklassifizierung, Konfiguration und Wiederherstellungsanforderungen verantwortlich. Ein sicherer Standard entsteht nicht automatisch aus dem Produktnamen. Er entsteht aus Entscheidungen, die zur tatsächlichen Nutzung passen.

2. Identitäten zuerst schützen

MFA ist unverzichtbar, aber nicht jede Methode bietet denselben Schutz. SMS, Einmalcodes und einfache Push-Bestätigungen können durch Social Engineering, Adversary-in-the-Middle-Techniken oder MFA-Fatigue umgangen werden. Microsoft bezeichnet phishing-resistente MFA als neue Baseline und nennt Passkeys, FIDO2-Sicherheitsschlüssel, Windows Hello for Business und geeignete Plattformverfahren [2]. Besonders privilegierte Rollen sollten zuerst umgestellt werden.

Administrationskonten dürfen nicht gleichzeitig normale E-Mail- und Browsingkonten sein. Rollen werden nach Aufgabe vergeben und möglichst zeitlich begrenzt. Mindestens zwei kontrollierte Notfallkonten schützen vor Fehlkonfigurationen, müssen aber besonders überwacht und sicher verwahrt werden. Dienstkonten und Anwendungen benötigen einen eigenen Lebenszyklus. Ein Zertifikat, Secret oder API-Schlüssel ohne Ablaufverantwortlichen ist eine zukünftige Sicherheitslücke.

Conditional Access verbindet Identität mit Kontext. Standort, Gerätezustand, Risiko, Anwendung und Authentisierungsmethode können in Entscheidungen einfließen. Die Einführung sollte mit Bericht- oder Pilotmodus beginnen, damit legitime Prozesse nicht versehentlich ausgesperrt werden. Ausnahmen werden dokumentiert, befristet und regelmäßig geprüft. Eine lange Liste dauerhafter Ausnahmen ist kein flexibles Konzept, sondern schleichender Kontrollverlust.

3. Geräte und Anwendungen einbeziehen

Ein sicherer Login auf einem unbekannten oder kompromittierten Gerät bleibt riskant. Deshalb sollten Gerätekonformität, Festplattenverschlüsselung, Patchstand, Endpoint-Schutz und lokale Administratorrechte Teil des Arbeitsplatzmodells sein. Nicht jedes Unternehmen benötigt sofort die maximal mögliche Geräteverwaltung. Es sollte aber wissen, welche Geräte auf Unternehmensdaten zugreifen und wie ein verlorenes oder ausgeschiedenes Gerät behandelt wird.

OAuth-Anwendungen und Drittanbieterintegrationen verdienen besondere Aufmerksamkeit. Benutzer können Anwendungen Berechtigungen auf Postfächer, Dateien oder Verzeichnisse erteilen. Ein seriöser Freigabeprozess prüft Herausgeber, benötigte Rechte, Datenfluss, Vertragsgrundlage und Widerruf. Administratorzustimmungen werden nicht beiläufig erteilt. Bestehende Enterprise Applications und App Registrations sollten regelmäßig inventarisiert werden.

Microsoft beobachtete 2025 unter anderem Device-Code-Phishing, bei dem Opfer zur Eingabe eines Codes auf einer legitimen Microsoft-Seite bewegt werden [3]. Awareness muss deshalb über gefälschte Loginseiten hinausgehen. Mitarbeitende sollten unerwartete Gerätecodes, Supportanfragen, Freigabeaufforderungen und MFA-Prompts melden können. Technische Richtlinien und verständliche Meldewege verstärken sich gegenseitig.

4. Teams, SharePoint und Copilot verantwortbar nutzen

Zusammenarbeit erzeugt Berechtigungen. Teams, Microsoft-365-Gruppen, SharePoint-Sites, OneDrive-Freigaben und Gäste wachsen schnell. Ohne Eigentümer und Ablaufregeln bleiben alte Projekte, externe Benutzer und anonyme Links bestehen. Jede Arbeitsfläche braucht einen verantwortlichen Owner, einen verständlichen Zweck und eine regelmäßige Überprüfung. Sensible Daten dürfen nicht allein durch gute Absichten geschützt sein.

Vor der Einführung von Copilot sollten Datenzugriffe aufgeräumt werden. Copilot erzeugt keine neuen Berechtigungen, kann vorhandene Zugriffe aber wesentlich leichter nutzbar machen. Überberechtigte Benutzer finden dadurch Informationen schneller, die sie bereits technisch lesen durften, obwohl dies organisatorisch nicht beabsichtigt war. Ein Copilot-Readiness-Check betrachtet deshalb SharePoint-Berechtigungen, externe Freigaben, Sensitivity Labels, Aufbewahrung, Datenqualität und Verantwortlichkeiten.

KI-Nutzung braucht zusätzlich klare Regeln: Welche Daten dürfen in Prompts verwendet werden? Welche Ergebnisse müssen geprüft werden? Wie werden personenbezogene oder vertrauliche Inhalte behandelt? Wer darf Agenten oder Automatisierungen veröffentlichen? Diese Regeln sollten kurz, verständlich und mit realen Beispielen formuliert sein. Verbote ohne praktikable Alternativen fördern Schatten-IT.

5. E-Mail, Protokolle und Reaktion

E-Mail bleibt ein wichtiger Angriffsweg. Schutzmechanismen wie SPF, DKIM und DMARC, sichere Standardrichtlinien, Link- und Anhangprüfung sowie ein Meldebutton reduzieren Risiken. Sie müssen jedoch korrekt eingeführt werden. Eine harte DMARC-Richtlinie ohne Inventar legitimer Versender kann Geschäftsprozesse stören. Umgekehrt liefert eine dauerhaft lockere Richtlinie wenig Schutz. Die Umstellung erfolgt deshalb schrittweise mit Auswertung.

Protokolle sind nur nützlich, wenn klar ist, welche Ereignisse beobachtet und wie lange sie aufbewahrt werden. Verdächtige Anmeldungen, neue Administratorrollen, geänderte Weiterleitungen, OAuth-Zustimmungen, ungewöhnliche Downloads und Manipulationen an Sicherheitsrichtlinien gehören zu den wichtigen Signalen. Servicezeiten und Eskalation müssen realistisch beschrieben werden. Ein Alarm außerhalb vereinbarter Zeiten ist nicht automatisch bearbeitet.

Für Kontenübernahmen braucht es ein kurzes Playbook: Konto sperren, aktive Sitzungen widerrufen, Authentisierungsmethoden prüfen, Passwort und Geheimnisse erneuern, Weiterleitungen und Regeln untersuchen, betroffene Daten bewerten, weitere Konten suchen und Kommunikation koordinieren. Bei einem Vorfall darf nicht erst diskutiert werden, wer Entscheidungen treffen kann.

6. Backup, Wiederherstellung und laufender Betrieb

Aufbewahrung, Papierkorb und Versionierung sind wertvolle Plattformfunktionen, aber nicht automatisch ein unabhängiges Backup. Das Unternehmen muss definieren, welche Daten wie lange wiederherstellbar sein sollen, wie versehentliche oder böswillige Löschung behandelt wird und ob eine getrennte Sicherung erforderlich ist. Die Entscheidung betrifft Exchange Online, SharePoint, OneDrive, Teams-Inhalte und relevante Konfigurationen.

Ein laufender Microsoft-365-Service umfasst Benutzeränderungen, Lizenzverwaltung, Rollen, Sicherheitsbaseline, Geräte, Freigaben, Dokumentation, Alarmbewertung und regelmäßige Reviews. Der Serviceanteil ist deshalb von der reinen Lizenzgebühr zu unterscheiden. Transparenz entsteht, wenn Angebot und Bericht zeigen, welche Aufgaben enthalten sind, welche Reaktionszeiten gelten und welche Tätigkeiten separat beauftragt werden.

Ein 90-Tage-Programm beginnt mit privilegierten Konten, MFA, Notfallzugängen und Inventar. Danach folgen Conditional Access, Gerätebasis, App-Berechtigungen und externe Freigaben. Im dritten Schritt werden Backup, Protokollierung, Incident-Playbook und ein Management-Review etabliert. Sicherheit bleibt anschließend ein Prozess: monatliche Änderungen, quartalsweise Rechte- und Freigabeprüfungen sowie eine jährliche Neubewertung.

7. Vom Konzept zum belastbaren Betrieb

Technische Maßnahmen entfalten ihren Wert erst in einem geregelten Betrieb. Dazu gehören ein benannter Service Owner, eine aktuelle Systemdokumentation, ein Änderungsprozess und ein fester Kontrollrhythmus. Der Umfang darf zur Organisation passen. Ein kleiner Betrieb benötigt keine Sitzungsbürokratie wie ein Konzern. Er benötigt jedoch Klarheit darüber, wer entscheidet, wer umsetzt, wer prüft und wie Abweichungen behandelt werden.

Bei jeder Maßnahme sollten vier Fragen beantwortet werden: Welches konkrete Risiko wird reduziert? Woran erkennen wir, dass die Maßnahme aktiv ist? Wer reagiert auf Fehler oder Alarme? Wie verlassen oder ersetzen wir die Lösung später? Diese Fragen schützen vor Scheinsicherheit und unnötiger Herstellerbindung. Sie machen Angebote vergleichbarer und erleichtern die Übergabe zwischen internen und externen Verantwortlichen.

Dokumentation ist kein Selbstzweck. Sie verkürzt Störungen, macht Änderungen sicherer und verhindert, dass kritisches Wissen ausschließlich bei einer Person liegt. Gute Dokumentation ist knapp genug, um gepflegt zu werden, und konkret genug, um in einer Störung zu helfen. Dazu gehören Übersichten, Abhängigkeiten, Verantwortliche, Zugangsverfahren, Wiederanlaufhinweise und der Stand der letzten Prüfung.

Ein Management-Review sollte Risiken nicht in technischen Einzelmeldungen verstecken. Sinnvoll sind wenige verständliche Kennzahlen: ungeklärte kritische Schwachstellen, Abdeckung starker Authentisierung, erfolgreiche Restore-Tests, überfällige Offboardings, nicht unterstützte Systeme und offene Maßnahmen nach Priorität. Die Kennzahlen dienen Entscheidungen, nicht dem Schönrechnen eines Ampelstatus.

Die beste Roadmap ist umsetzbar. Maßnahmen werden in kleine, prüfbare Pakete geschnitten und mit Termin sowie Verantwortlichem versehen. Kritische Sofortmaßnahmen stehen vor Komfortprojekten. Nach jedem Abschnitt wird geprüft, ob das Risiko tatsächlich gesunken ist. So entsteht über Monate ein belastbarer Betrieb, ohne das Tagesgeschäft durch einen unrealistischen Komplettumbau zu blockieren.

Beschaffung und Betrieb sollten getrennt bewertet werden. Ein günstiger Einstieg kann durch aufwendige Administration, unklare Lizenzbedingungen, fehlende Exportmöglichkeiten oder schwachen Support später teuer werden. Umgekehrt ist eine umfangreiche Plattform nicht automatisch die bessere Wahl. Vor einer Entscheidung werden deshalb fünf Jahre Betrieb, interne Zeit, notwendige Kompetenzen, Ausfallfolgen, Datenmigration und Rückbau betrachtet. Diese Gesamtsicht verhindert, dass ein kurzfristiger Preisvergleich die langfristige Handlungsfähigkeit bestimmt.

Auch Kommunikation ist eine Sicherheits- und Qualitätskontrolle. Mitarbeitende müssen wissen, wo sie Störungen, verdächtige Nachrichten oder Fehlbedienungen ohne Angst vor Schuldzuweisung melden können. Führungskräfte benötigen eine verständliche Lage, keine Sammlung unbewerteter Warnungen. Dienstleister brauchen eindeutige Freigaben und erreichbare Ansprechpartner. Ein kurzer, regelmäßig geübter Kommunikationsweg reduziert im Ernstfall Verzögerungen und Fehlentscheidungen deutlich.

Vor dem Produktivstart gehört eine unabhängige Abnahme in den Plan. Dabei wird nicht nur geprüft, ob Funktionen vorhanden sind, sondern ob Berechtigungen, Protokollierung, Sicherung, Alarmierung, Dokumentation und Rückfallweg tatsächlich funktionieren. Festgestellte Abweichungen werden mit Risiko, Verantwortlichem und Zieltermin protokolliert. Eine bewusste Rest-Risikoentscheidung ist legitim; eine unbemerkte Lücke ist es nicht. Diese Abnahme schafft eine belastbare Ausgangslage für den späteren Regelbetrieb.

Technische Standards müssen außerdem mit dem Arbeitsalltag vereinbar sein. Eine Kontrolle, die regelmäßig umgangen wird, schützt schlechter als eine etwas einfachere Lösung, die zuverlässig genutzt und überwacht wird. Pilotgruppen helfen, Nebenwirkungen früh zu erkennen. Rückmeldungen aus Fachabteilungen werden dokumentiert, ohne die Schutzziele aus dem Blick zu verlieren. So entsteht Akzeptanz nicht durch Marketing, sondern durch nachvollziehbare Entscheidungen und funktionierende Abläufe.

Mindestens einmal jährlich sollte die Organisation ihre Annahmen neu prüfen. Geschäftsprozesse, Mitarbeiterzahl, Standorte, Anwendungen, Bedrohungen und gesetzliche Rahmenbedingungen verändern sich. Ein früher sinnvoller Schwellenwert oder Vertrag kann später unpassend sein. Das Review betrachtet neue Abhängigkeiten, abgeschaltete Systeme, offene Ausnahmen, Wirksamkeitsnachweise und geplante Veränderungen. Daraus entsteht die nächste überschaubare Roadmap statt eines jahrelang unveränderten Dokuments.

Praxis-Checkliste

- Separate Administrationskonten und phishing-resistente MFA einführen
- Notfallkonten kontrolliert anlegen, testen und überwachen
- Conditional Access schrittweise und mit dokumentierten Ausnahmen ausrollen
- Geräte, OAuth-Anwendungen, Gäste und externe Freigaben inventarisieren
- Copilot erst nach Berechtigungs- und Datenprüfung freigeben
- E-Mail-Authentisierung, Meldeweg und Incident-Playbook etablieren
- Backup- und Wiederherstellungsziele unabhängig von Lizenzannahmen definieren

Fazit

Die Qualität einer IT-Entscheidung zeigt sich nicht am Prospekt, sondern im Betrieb: an klaren Rollen, nachvollziehbaren Änderungen, getesteter Wiederherstellung und einer realistischen Exit-Option. BR-Systems unterstützt bei Bestandsaufnahme, Konzeption, Migration, Umsetzung und laufendem Betrieb - herstellerbewusst, aber nicht verkaufsgetrieben.

Quellen und weiterführende Informationen

[1] Microsoft: Digital Defense Report 2025
https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2025

[2] Microsoft Learn: Phishing-resistant MFA
https://learn.microsoft.com/en-us/security/zero-trust/sfi/phishing-resistant-mfa

[3] Microsoft Security Blog: Device Code Phishing 2025
https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/

[4] Microsoft Learn: Baseline Security Mode
https://learn.microsoft.com/en-us/microsoft-365/baseline-security-mode/baseline-security-mode-settings

Historischer bzw. fachlicher Bezugsstand: 24. März 2026. Veröffentlicht: 7. April 2026. Online-Quellen zuletzt geprüft: 24. März 2026. Der Fachstand ist kein vorgetäuschtes Veröffentlichungsdatum. Dokument-ID BR-WP-M365-003, Version 1.0.

Über BR-Systems

- Herstellerunabhängige Beratung mit Blick auf Nutzen, Betrieb und Exit-Fähigkeit
- Umsetzung und Betreuung für Microsoft 365, Security, Proxmox, Backup, Netzwerk und Open Source
- Ein fester Ansprechpartner, nachvollziehbare Dokumentation und transparente Leistungsgrenzen

Nächster Schritt

Sie möchten das Thema auf Ihre Umgebung übertragen? BR-Systems beginnt mit einer Bestandsaufnahme und einem klar begrenzten Maßnahmenplan. Kontakt: info@br-systems.eu oder +49 179 1601700.