# NIS2-Implementierungs-Fahrplan

## Vom Assessment zur Compliance mit Microsoft 365

Ein Leitfaden für den deutschen Mittelstand

Erstellt von

Rashad Bakirov

Microsoft 365 Cloud Security & Compliance Architekt

linkedin.com/in/rashadbakirov

# NIS2 auf einen Blick

| ~29.500 | 06.03.2026 | 10 Mio. EUR | §38 |
|---|---|---|---|
| Betroffene Unternehmen | BSI-Registrierungsfrist | Maximales Bußgeld | Geschäftsführerhaftung |

- NIS2UmsuCG in Kraft seit 06.12.2025
- ~29.500 betroffene Unternehmen (50–250 Mitarbeiter)
- BSI-Registrierungsfrist: 06.03.2026
- Bußgelder bis zu 10 Mio. EUR oder 2 % des Jahresumsatzes
- Persönliche Haftung der Geschäftsführung (§38)

## Was ist NIS2UmsuCG?

Die nationale Umsetzung der EU-Richtlinie NIS2 (EU 2022/2555). Das Gesetz definiert Mindeststandards für Risikomanagement, Meldepflichten und Governance in der Cybersicherheit.

## Wer ist betroffen?

Unternehmen mit 50–250 Mitarbeitern oder mehr als 10 Mio. EUR Jahresumsatz in betroffenen Sektoren: Energie, Transport, Gesundheit, Digitale Infrastruktur, Verarbeitendes Gewerbe, Lebensmittel, Chemie und weitere.

## Geschäftsführerhaftung (§38)

Die Geschäftsleitung ist persönlich für die Umsetzung verantwortlich. Pflichtverletzung = Haftung mit Privatvermögen. Schulungen zur Cybersicherheit sind verpflichtend.

© 2026 Rashad Bakirov — linkedin.com/in/rashadbakirov

# Die 10 Maßnahmen nach §30

| Nr | NIS2-Maßnahme (§30 Abs. 2) | Microsoft 365 Lösung |
|---|---|---|
| 1 | Risikoanalyse und Sicherheitskonzepte | Microsoft Purview Compliance Manager, Secure Score, Defender Vulnerability Mgmt |
| 2 | Bewältigung von Sicherheitsvorfällen | Microsoft Sentinel, Defender XDR, Automated Investigation & Response |
| 3 | Business Continuity & Krisenmanagement | SharePoint Disaster Recovery, OneDrive Versionierung, Azure Backup |
| 4 | Sicherheit der Lieferkette | Microsoft Defender for Cloud Apps, Conditional Access für Externe |
| 5 | Sicherheit bei Erwerb/Entwicklung/Wartung | Microsoft Intune, Defender for Endpoint, Windows Autopatch |
| 6 | Bewertung der Wirksamkeit | Compliance Manager Assessments, Secure Score Trending, Audit Logs |
| 7 | Cyberhygiene und Schulungen | Microsoft Viva Learning, Attack Simulation Training |
| 8 | Kryptografie und Verschlüsselung | Microsoft Purview Information Protection, BitLocker, Azure Information Protection |
| 9 | Personalsicherheit und Zugriffskontrolle | Entra ID (Conditional Access, PIM, MFA), Identity Governance |
| 10 | Multi-Faktor-Authentifizierung (MFA) | Entra ID MFA, Passwordless Auth, FIDO2, Windows Hello for Business |

© 2026 Rashad Bakirov — linkedin.com/in/rashadbakirov

# Der 4-Stufen-Implementierungsansatz

## 01 Readiness Assessment (1–2 Wochen)

- Betroffenheitsanalyse
- Gap-Analyse gegen §30
- Reifegradmessung (0–5)
- M365 Lizenz-Audit
- Secure Score Baseline

## 02 Security Hardening (4–6 Wochen)

- Entra ID (Conditional Access, MFA, PIM)
- Defender XDR
- Purview (DLP, Sensitivity Labels)
- Intune (Device Compliance)
- Sentinel (SIEM-Integration)

## 03 Dokumentation & Audit (1–2 Wochen)

- Sicherheitsrichtlinien
- Incident-Response-Plan
- BSI-Registrierung
- Compliance-Evidence
- Schulungsnachweise

## 04 Managed Compliance (Monatlich)

- Secure Score Reviews
- Compliance Manager Assessments
- Threat-Landscape-Monitoring
- Richtlinien-Updates
- Quartalsweise Berichte

 Jede Stufe baut auf der vorherigen auf. Der gesamte Prozess ist in 8–12 Wochen umsetzbar.

© 2026 Rashad Bakirov — linkedin.com/in/rashadbakirov

# Reifegradmodell


| Stufe | Bezeichnung | Beschreibung |
|---|---|---|
| 0 | Nicht vorhanden | Keine Maßnahmen implementiert |
| 1 | Initial / Ad-hoc | Vereinzelte, nicht standardisierte Maßnahmen |
| 2 | Wiederholbar | Grundlegende Prozesse vorhanden, aber nicht dokumentiert |
| 3 | Definiert (NIS2-Minimum) | Dokumentierte und standardisierte Prozesse — NIS2-Mindestanforderung |
| 4 | Gesteuert | Gemessen, überwacht und kontinuierlich verbessert |
| 5 | Optimiert | Best-Practice, vollständig automatisiert und auditiert |

## Typischer Ausgangspunkt im Mittelstand

**Durchschnittlicher Reifegrad: 1,5 – 2,5**

### Größte Lücken:

- Incident Response (Maßnahme 2)
- Lieferketten-Sicherheit (Maßnahme 4)
- Wirksamkeitsbewertung (Maßnahme 6)
- Dokumentation (Maßnahme 3)

Ziel: Von Stufe 2 auf Stufe 3+ in 8–12 Wochen

© 2026 Rashad Bakirov — linkedin.com/in/rashadbakirov

# Checkliste: Erste Schritte

- [ ] **1. Betroffenheitsanalyse durchführen**
  Prüfen Sie, ob Ihr Unternehmen unter die NIS2-Richtlinie fällt
- [ ] **2. BSI-Registrierung vorbereiten**
  Registrierungsfrist 06.03.2026 einhalten
- [ ] **3. Microsoft 365 Lizenzen prüfen**
  Welche Sicherheitsfeatures sind enthalten (E3/E5/Business Premium)
- [ ] **4. Secure Score auswerten**
  Aktuellen Stand analysieren, Quick Wins identifizieren
- [ ] **5. Gap-Analyse gegen §30 durchführen**
  IST-Zustand gegen alle 10 Maßnahmen bewerten
- [ ] **6. Incident-Response-Plan erstellen**
  24h Erstmeldung, 72h Folgemeldung ans BSI
- [ ] **7. MFA für alle Benutzer aktivieren**
  Multi-Faktor-Authentifizierung über Entra ID
- [ ] **8. Geschäftsführung informieren und schulen**
  Persönliche Haftung nach §38
- [ ] **9. Dienstleister und Lieferkette bewerten**
  Cybersicherheit kritischer Zulieferer prüfen
- [ ] **10. Dokumentation starten**
  Compliance ist nur nachweisbar, wenn sie dokumentiert ist

**Nächster Schritt?**
Vereinbaren Sie ein unverbindliches Erstgespräch zur NIS2-Betroffenheitsanalyse.

© 2026 Rashad Bakirov — linkedin.com/in/rashadbakirov

# Über den Autor

## Rashad Bakirov

Microsoft 365 Cloud Security & Compliance Architekt

Spezialisiert auf NIS2-Compliance für den deutschen Mittelstand durch den bestehenden Microsoft 365 Stack.

### Schwerpunkte:

- NIS2 Gap-Analyse
- M365 Security Hardening
- Entra ID / Defender / Purview / Intune
- Compliance-Dokumentation
- Managed Compliance

LinkedIn: linkedin.com/in/rashadbakirov