© **FM Forum Business Solutions GmbH**
A-1200 Wien, Dresdner Straße 45
E-Mail: kundenservice@forum-media.at

Projektziele für ein NISG 2026-Umsetzungsprojekt

Die Projektziele für ein KMU (kleines oder mittleres Unternehmen), das als wichtige Einrichtung gilt, sollten auf die spezifischen Anforderungen der NIS-2-Richtlinie und des NISG 2026 zugeschnitten sein und gleichzeitig den begrenzten Ressourcen und Kapazitäten eines KMU Rechnung tragen. Nachstehend ein Vorschlag für präzise und erreichbare Projektziele:

Projektziele für ein NIS-2-Umsetzungsprojekt in einem KMU

1. Erfüllung gesetzlicher Anforderungen

- Ziel: Sicherstellen, dass das Unternehmen die Vorgaben der NIS-2-Richtlinie und des NISG 2026 vollständig erfüllt
- Ergebnis: Nachweis der Compliance durch eine interne Prüfung oder ein Audit sowie die Bereitstellung der erforderlichen Dokumentationen und Berichte für Behörden

2. Aufbau eines Risikomanagementsystems

- Ziel: Etablieren eines strukturierten Risikomanagementsystems, das Risiken für IT-Systeme und Geschäftsprozesse identifiziert, bewertet und minimiert
- Ergebnis: Erstellung eines Risikoregisters mit priorisierten Maßnahmen zur Risikominderung und kontinuierlicher Überwachung

3. Implementierung grundlegender Sicherheitsmaßnahmen

- Ziel: Einführung von praktikablen und skalierbaren technischen und organisatorischen Sicherheitsmaßnahmen
- Technisch: Implementierung von Multi-Faktor-Authentifizierung (MFA), Verschlüsselung und Sicherheitsupdates
- Organisatorisch: Entwicklung eines Notfallplans und Schulung der Mitarbeiter
- Ergebnis: Erfüllung der Mindestanforderungen der NIS2-Richtlinie, um die Sicherheit der Netz- und Informationssysteme zu gewährleisten

4. Aufbau eines Vorfallsmanagements

- Ziel: Einführung eines Systems zur Erkennung, Analyse und Meldung von Sicherheitsvorfällen gemäß den gesetzlichen Anforderungen
- Ergebnis: Meldung von Sicherheitsvorfällen innerhalb der gesetzlich vorgegebenen Fristen, einschließlich Frühwarnung binnen 24 Stunden, Meldung binnen 72 Stunden und Abschlussbericht binnen eines Monats

5. Etablierung einer Lieferkettensicherheit

- Ziel: Sicherstellen, dass Lieferanten und Dienstleister, die Zugriff auf kritische Systeme oder Daten haben, ebenfalls angemessene Sicherheitsstandards einhalten
- Ergebnis: Überprüfung bestehender Lieferantenverträge und Einführung klarer Sicherheitsanforderungen

6. Aufbau einer Sicherheitskultur

- Ziel: Sensibilisierung der Mitarbeiter für Cybersicherheitsrisiken und Einführung eines Bewusstseins für die Bedeutung von Sicherheitsrichtlinien
- Ergebnis: Durchführung von Schulungen und Sensibilisierungskampagnen sowie Förderung der Mitarbeitermotivation zur Einhaltung der Sicherheitsstandards

7. Effiziente Nutzung von Ressourcen

- Ziel: Sicherstellen, dass die Umsetzung der NIS-2-Anforderungen im Rahmen der bestehenden finanziellen und personellen Ressourcen erfolgt, ohne Registrierung, Governance, Nachweisführung und Kernprozesse zu gefährden
- Ergebnis: Identifikation von kosteneffizienten Lösungen, die den Sicherheitsanforderungen entsprechen, ohne die Kernprozesse des Unternehmens zu beeinträchtigen

8. Schaffung von Dokumentationsstandards

- Ziel: Aufbau einer zentralen und revisionssicheren Dokumentation der Sicherheitsmaßnahmen und -prozesse
- Ergebnis: Bereitstellung von Compliance-Dokumentationen, Registerdaten, Selbstdeklaration, Risikobewertungen Auditberichten und Notfallplänen für interne Zwecke und behördliche Anforderungen

9. Vorbereitung auf Audits

- Ziel: Sicherstellen, dass das Unternehmen jederzeit bereit ist, interne Audits sowie behördlich angeforderte externe Nachweise zu bestehen
- Ergebnis: Abschluss eines internen Audits mit einem Maßnahmenkatalog und Vorbereitung auf behördliche Überprüfungen

10. Sicherstellung der Nachhaltigkeit

- Ziel: Aufbau eines Prozesses, der die kontinuierliche Verbesserung der Cybersicherheit auch nach Abschluss des Projekts gewährleistet
- Ergebnis: Einführung eines Mechanismus zur regelmäßigen Überprüfung und Aktualisierung der Sicherheitsmaßnahmen

Beispiel für SMART-Projektziele

SMART (Spezifisch, Messbar, Akzeptiert, Realistisch, Terminiert) formulierte Ziele für ein KMU könnten wie folgt aussehen:

1. Risikomanagementsystem einführen:
   Bis zum Ende des Projekts wird ein Risikoregister erstellt, das mindestens 90 % der identifizierten Risiken priorisiert und geeignete Maßnahmen definiert.
2. Sicherheitsmaßnahmen implementieren:
   Innerhalb von 6 Monaten wird in allen kritischen Systemen eine MFA und eine regelmäßige Backup-Strategie implementiert.
3. Vorfallsmanagement einführen:
   Bis zum Projektabschluss wird ein Vorfallsmanagementsystem etabliert, das die Meldung erheblicher Cybersicherheitsvorfälle binnen 24 Stunden anstößt, die 72-Stunden-Meldung vorbereitet und den Abschlussbericht binnen eines Monats ermöglicht.
4. Mitarbeiterschulungen durchführen:
   80 % der Mitarbeiter nehmen innerhalb von 3 Monaten an einem Cybersicherheitsschulungsprogramm teil.
5. Dokumentation bereitstellen:
   Alle erforderlichen Dokumentationen (zB Sicherheitsrichtlinien, Auditberichte) werden spätestens 2 Wochen vor

der geplanten internen Prüfung fertiggestellt.

Ergebnisse der Phase

Nach Abschluss der Projektvorbereitung und Zieldefinition sollte das KMU über folgende Ergebnisse verfügen:

1. Klar formulierte und priorisierte Projektziele
2. Ein genehmigter Projektauftrag mit klar definiertem Umfang
3. Ein zugewiesenes Projektteam mit klaren Rollen und Verantwortlichkeiten
4. Ein erster Maßnahmenplan zur Erreichung der Ziele
5. Sicherstellung von Ressourcen für die Umsetzung der Ziele