ContractHero

So kommen Sie Schritt für Schritt zu einem NIS2-konformen Setup

Sind Ihre Verträge auf eine Prüfung vorbereitet?

Die Anforderungen der NIS2-Richtlinie wirken auf den ersten Blick komplex. In der Praxis zeigt sich jedoch: Mit einem klaren Vorgehen lassen sich die wichtigsten Maßnahmen effizient umsetzen.

Ein sinnvoller Einstieg in die Umsetzung lässt sich in fünf zentrale Schritte gliedern:

1. Betroffenheit klären

Prüfen Sie zunächst, ob und in welchem Umfang Ihr Unternehmen unter die NIS2-Regulierung fällt. Dabei spielen insbesondere die Branche, Unternehmensgröße und die Einbindung in kritische oder regulierte Lieferketten eine zentrale Rolle.

2. Bestehende Strukturen analysieren

Verschaffen Sie sich einen Überblick über bestehende Prozesse, Verantwortlichkeiten und Sicherheitsmaßnahmen. Häufig zeigen sich hier bereits erste Lücken, insbesondere bei Dokumentation und Nachweisbarkeit.

3. Risiken und Handlungsfelder priorisieren

Bewerten Sie, wo die größten Risiken liegen, etwa bei kritischen Systemen, externen Dienstleistern oder fehlenden Governance-Strukturen.

4. Maßnahmen strukturiert umsetzen

Leiten Sie konkrete organisatorische und technische Maßnahmen ab und setzen Sie diese gezielt um. Dazu gehören insbesondere klare Zuständigkeiten, definierte Meldeprozesse und dokumentierte Sicherheitsanforderungen.

5. Transparenz und Nachweisbarkeit sicherstellen

Ein zentraler Erfolgsfaktor ist die strukturierte Dokumentation. Unternehmen sollten jederzeit nachvollziehen können, welche Anforderungen gelten, wer verantwortlich ist und wie Risiken gesteuert werden.

Wichtig: Die Umsetzung von NIS2 ist kein einmaliges Projekt, sondern ein fortlaufender Prozess. Sicherheitsanforderungen, Bedrohungslagen und regulatorische Vorgaben entwickeln sich kontinuierlich weiter und erfordern eine regelmäßige Anpassung der bestehenden Strukturen.

Wenn morgen geprüft wird: Sind Ihre Verträge strukturiert auffindbar?

Mit der NIS2-Richtlinie steigen die Anforderungen an Cybersicherheit, Risikomanagement und Dokumentation deutlich. Für viele Unternehmen wird das zunehmend zu einer Management- und Governance-Frage.

Die entscheidende Frage lautet:

Könnten Sie im Ernstfall sofort nachweisen, welche Sicherheitsanforderungen mit Ihren Dienstleistern vertraglich geregelt sind?

Der folgende 5-Minuten-Selbstcheck zeigt Ihnen schnell, ob Ihre Vertragsstruktur bereits prüfungssicher ist oder ob noch Handlungsbedarf besteht.

ContractHero

NIS2 Governance Selbstcheck

Der 5-Minuten-Check für Unternehmen

Beantworten Sie die folgenden Fragen mit **Ja oder Nein**.

Vertragsübersicht

□ Haben Sie eine vollständige Übersicht über alle IT- und Cloud-Verträge?

□ Sind Verträge zentral gespeichert und leicht auffindbar?

Fristen & Risiken

□ Sind Kündigungs- und Verlängerungsfristen zentral einsehbar?

□ Werden kritische Vertragsfristen aktiv überwacht?

Sicherheitsanforderungen

□ Können Sie Verträge mit sicherheitsrelevanten Klauseln gezielt identifizieren?

□ Wissen Sie, welche Dienstleister Zugriff auf kritische Systeme haben?

Governance

□ Gibt es klare Verantwortliche für sicherheitskritische Verträge?

□ Ist dokumentiert, wer Sicherheitsanforderungen bei neuen Verträgen prüft?

Ergebnis

0-2 x Nein

Ihre Vertragsstruktur scheint gut organisiert zu sein.

3-5 x Nein

Es bestehen erste organisatorische Risiken.

Mehr als 5 x Nein

Hier besteht ein strukturelles Risiko im Vertragsmanagement.

Unabhängig vom Ergebnis zeigt sich jedoch in der Praxis: Mit **NIS2** verschiebt sich die Verantwortung für Cybersicherheit zunehmend auf **Management- und Governance-Ebene**. Geschäftsleitungen müssen sicherstellen, dass Risiken strukturiert bewertet und Sicherheitsanforderungen auch in der Zusammenarbeit mit Dienstleistern berücksichtigt werden.

Gerade dabei spielen Verträge eine zentrale Rolle. In ihnen werden häufig Sicherheitsstandards, Meldepflichten, Verantwortlichkeiten oder Zugriffsrechte geregelt. Wenn diese Informationen jedoch nicht zentral verfügbar sind, entsteht schnell ein organisatorisches Risiko unabhängig davon, wie gut die technische IT-Sicherheit aufgestellt ist.

Vor diesem Hintergrund wird ein **strukturiertes Vertragsmanagement zu einem zentralen Bestandteil moderner Governance- und Compliance-Strukturen.** Unternehmen, die ihre Verträge zentral organisieren und sicherheitsrelevante Verpflichtungen transparent abbilden, können Risiken besser steuern und regulatorische Anforderungen nachvollziehbar umsetzen.

Wenn Sie erfahren möchten, wie eine digitale Vertragsplattform **Ihr Unternehmen dabei unterstützen kann**, regulatorische Anforderungen effizienter und transparenter in der Praxis umzusetzen, vereinbaren Sie hier eine kurze Demo mit **ContractHero**.