

NIS2 in 20 Tagen

Ein Praxisleitfaden für
Organisation & Management



MANAGEMENT SUMMARY

NIS2 ist kein IT-Projekt. NIS2 ist eine Management- und Organisationsaufgabe.

Unternehmen scheitern nicht an fehlender Technik, sondern an unklaren Verantwortlichkeiten, fehlender Steuerung, nicht dokumentierten Entscheidungen und fehlender Nachweisbarkeit.

Dieses Whitepaper zeigt, wie Unternehmen innerhalb von 20 Tagen organisatorisch NIS2-fähig werden: pragmatisch, nachvollziehbar und prüfbar. Der Fokus liegt bewusst auf Struktur, Organisation und Management. Wenn diese Basis steht, lassen sich technische Maßnahmen gezielt und risikobasiert umsetzen.

In der Praxis zeigt sich, dass viele Unternehmen NIS2 zunächst als rein technisches Thema betrachten. Firewalls, Endpoint-Security oder Monitoring-Lösungen stehen früh im Fokus, während organisatorische Fragen vertagt werden. Genau hier liegt jedoch das größte Risiko. NIS2 adressiert explizit die Verantwortung des Managements und verlangt, dass Sicherheitsmaßnahmen geplant, gesteuert und überwacht werden.

Dieses Whitepaper setzt daher bewusst vor der Technik, wie Firewalls oder Endpoint-Security, an. Es zeigt, wie Unternehmen zunächst Ordnung in Verantwortlichkeiten, Entscheidungsprozesse und Nachweise bringen. Ziel ist es, eine belastbare organisatorische Grundlage zu schaffen, auf der technische Maßnahmen sinnvoll priorisiert und später erweitert werden können.

DIE 5 ORGANISATORISCHEN KERNPFLICHTEN AUS NIS2

Unabhängig von Branche oder Größe lassen sich die Anforderungen der NIS2 auf fünf zentrale Pflichten reduzieren:

- 1. Klar definierte Verantwortlichkeiten und Rollen**
- 2. Risikobasierte Maßnahmenplanung**
- 3. Dokumentierte und aktive Prozesse sowie Richtlinien**
- 4. Nachweisbare Awareness- und Schulungsmaßnahmen**
- 5. Fortlaufende Überwachung und Aktualisierung**

Diese fünf Pflichten ziehen sich konsistent durch die gesamte NIS2-Richtlinie und sind unabhängig davon, in welchem Sektor oder mit welcher technischen Reife ein Unternehmen startet. Sie machen deutlich, dass es nicht um Einzelmaßnahmen geht, sondern um ein steuerbares Gesamtsystem.

Besonders wichtig ist dabei das Zusammenspiel der Punkte: Verantwortlichkeiten ohne Maßnahmenplanung bleiben wirkungslos, Prozesse ohne Schulungen werden nicht gelebt und Maßnahmen ohne regelmäßige Überprüfung verlieren schnell ihre Aktualität. Erst wenn alle fünf Pflichten gemeinsam betrachtet werden, entsteht eine belastbare und prüfbare NIS2-Umsetzung.

ORGANISATIONSORIENTIERTER EINSTIEG

Ein Einstieg in NIS2 beginnt in der Regel nicht mit Technik, sondern mit Organisation, Zuständigkeiten und Nachweisen. Ziel ist es, die Anforderungen der Richtlinie in konkrete, überprüfbare Arbeitsergebnisse zu übersetzen, ohne Interpretationsspielräume durch abstrakte Gesetzestexte.

Bewährt hat sich ein organisationszentriertes Vorgehen mit folgenden Prinzipien:

- ✓ **Anforderungen operationalisieren:** Gesetzliche Pflichten werden in klare Aufgaben, Verantwortlichkeiten und Nachweise überführt.
- ✓ **Schrittweise Umsetzung:** Statt umfangreicher Konzeptarbeit werden Maßnahmen in einer sinnvollen Reihenfolge aufgebaut.
- ✓ **Erprobte Grundstrukturen nutzen:** Vorgefertigte Rollenmodelle, Checklisten und Dokumentationsbausteine beschleunigen den Start und reduzieren Leerlauf.
- ✓ **Organisation entlasten und Reifegrad erhöhen:** Durch klare Zuständigkeiten, zentrale Maßnahmenübersichten und feste Prüfzyklen wird die Umsetzung handhabbar und dauerhaft steuerbar.

Ziel ist organisatorische Compliance in 20 Tagen. Wenn die Organisation steht, ist der Rest einfach. Statt Unternehmen mit abstrakten Richtlinien texten oder umfangreichen Methodiken zu konfrontieren, wird der Fokus auf konkrete organisatorische Ergebnisse gelegt. Jede Aktivität zielt darauf ab, Klarheit zu schaffen: Wer ist verantwortlich? Welche Entscheidungen wurden getroffen? Welche Maßnahmen sind geplant oder umgesetzt?

Der Ansatz folgt einer klaren Logik: Erst Struktur, dann Steuerung, dann Nachweis. Dadurch entsteht bereits nach kurzer Zeit ein messbarer Reifegrad, ohne die Organisation zu überfordern oder den laufenden Betrieb zu beeinträchtigen.



Tobias Frank,
Gründer und CEO

Als **Head of IT und Verantwortlicher für Informationssicherheit** in Handelsunternehmen und Fertigungsindustrie und habe ich in allen Facetten erlebt, wie aufwändig Informationssicherheit für CxO und Teams im Alltag ist. 20 Jahre lang.

Aus diesem persönlichen Antrieb heraus entwickelten wir VantarIS und gründeten Vantarion.

VantarIS nimmt die Bürokratie aus Normen wie NIS2 und bringt kompetente Sicherheit.

The logo for VANTARIS, with "VANTAR" in white and "IS" in green, all in a bold, sans-serif font.

DER 20-TAGE-PLAN

WOCHE 1 - BETROFFENHEIT & SCOPE

Ziel ist Klarheit. Am Ende der ersten Woche sind Betroffenheit, Scope und Verantwortlichkeiten dokumentiert. In dieser Phase geht es nicht um Maßnahmen, sondern um Orientierung. Unternehmen verschaffen sich einen strukturierten Überblick darüber, ob und warum sie unter NIS2 fallen und welche Teile der Organisation betroffen sind. Gleichzeitig wird festgelegt, welche organisatorischen Einheiten, Prozesse oder Dienstleistungen in den Geltungsbereich fallen.

Diese Klarheit verhindert spätere Diskussionen und unnötige Ausweitungen des Scopes, die Aufwand und Komplexität deutlich erhöhen würden.

- ✓ **Betroffenheitsprüfung durchgeführt**
- ✓ **Organisatorischer Scope definiert**
- ✓ **Verantwortliche Rollen benannt**
- ✓ **Management-Entscheidungen dokumentiert**

WOCHE 2 - VERANTWORTUNG & STEUERUNG

Jetzt wird die Organisation arbeitsfähig gemacht. Verantwortung wird nicht nur benannt, sondern steuerbar. In Woche zwei wird aus formaler Zuständigkeit tatsächliche Steuerung. Durch klare Rollenmodelle und eine zentrale Maßnahmenübersicht wird Transparenz geschaffen: Was ist zu tun, wer ist verantwortlich und bis wann muss es erledigt sein?

Besonders wichtig ist hier die Festlegung von Entscheidungs- und Eskalationswegen. NIS2 verlangt nicht, dass jede Entscheidung auf Management-Ebene getroffen wird – wohl aber, dass klar ist, wann und wie Entscheidungen eskaliert werden.

- ✓ **RACI-Modell für die Organisationsstruktur festgelegt**
- ✓ **Zentrale Maßnahmenliste angelegt**
- ✓ **Verantwortlichkeiten je Maßnahme definiert**
- ✓ **Eskalations- und Entscheidungswege festgelegt**

WOCHE 3 - PROZESSE, RICHTLINIEN & AWARENESS

NIS2 wird sichtbar gelebt. Es geht nicht um Vollständigkeit, sondern um Wirksamkeit. Der Fokus liegt bewusst auf wenigen, zentralen Prozessen und Richtlinien. Diese müssen verständlich, kommuniziert und im Alltag anwendbar sein. Eine kleine Anzahl klar definierter Regeln ist deutlich wirksamer als ein umfangreicher Richtlinienkatalog, der nicht gelebt wird.

Awareness-Maßnahmen sorgen dafür, dass Mitarbeitende ihre Rolle verstehen und sicherheitsrelevante Situationen erkennen können. Entscheidend ist dabei nicht die Form der Schulung, sondern die Nachweisbarkeit.

- ✓ **Incident-Response-Prozess dokumentiert**
- ✓ **Zugriffs- und Backup-Regeln festgelegt**
- ✓ **Kernrichtlinien verabschiedet**
- ✓ **Awareness-Schulung durchgeführt und dokumentiert**

WOCHE 4 - NACHWEIS & REGELBETRIEB

Auditfähigkeit wird hergestellt. In der letzten Phase werden alle organisatorischen Bausteine zusammengeführt. Maßnahmenstatus, Verantwortlichkeiten und Dokumentationen werden so aufbereitet, dass sie intern gesteuert und extern nachvollzogen werden können.

Gleichzeitig wird der Übergang vom Projekt in den Regelbetrieb vorbereitet. NIS2 endet nicht mit der Erstumsetzung, sondern verlangt eine kontinuierliche Pflege und Überwachung der getroffenen Maßnahmen.

- ✓ **Maßnahmenstatus aktuell**
- ✓ **Reporting vorbereitet**
- ✓ **Regelmäßige Überprüfung terminiert**
- ✓ **Verantwortlichkeiten für den Betrieb festgelegt**

RISIKOMANAGEMENT & BIA - EINORDNUNG

NIS2 verlangt eine risikobasierte Maßnahmenplanung. Die anerkannte Grundlage dafür ist eine Business Impact Analysis (BIA). Die risikobasierte Herleitung von Maßnahmen ist ein zentrales Element der NIS2. Sie stellt sicher, dass Sicherheitsmaßnahmen nicht pauschal, sondern gezielt dort umgesetzt werden, wo sie den größten Beitrag zur Stabilität des Unternehmens leisten.

Um die Komplexität in der Startphase gering zu halten, wird die vollständige BIA bewusst ausgelagert. Stattdessen werden in den ersten 20 Tagen alle organisatorischen Voraussetzungen geschaffen, um eine strukturierte und auditfähige Risikoanalyse im nächsten Schritt durchführen zu können.

Checkliste BIA-Readiness:

- Kritische Prozesse identifiziert
- Prozessverantwortliche benannt
- Abhängigkeiten grob erfasst
- Struktur für Maßnahmenpriorisierung vorhanden

CHECKLISTE: ÜBLICHE RICHTLINIEN

Diese Richtlinien stellen ein bewährtes Minimal-Set dar, das für die meisten Unternehmen ausreicht, um die organisatorischen Anforderungen der NIS2 abzudecken. Entscheidend ist nicht der Umfang der Dokumente, sondern deren Anwendung im Alltag.

Richtlinien sollten regelmäßig überprüft, bei Bedarf angepasst und den Mitarbeitenden bekannt gemacht werden. Nur so werden sie vom formalen Dokument zum wirksamen Steuerungsinstrument.

Governance:

- Informationssicherheitsleitlinie
- Rollen & Verantwortlichkeiten
- Dokumentenlenkung

Zugriffe & IT-Betrieb:

- ✓ Zugriffskontrollrichtlinie
- ✓ Passwort- und MFA-Regeln
- ✓ Patch- und Vulnerability-Management
- ✓ Backup- und Restore-Richtlinie
- ✓ Logging & Monitoring

Incident & Continuity:

- ✓ Incident-Response-Richtlinie
- ✓ Notfall- / Business-Continuity-Grundkonzept

Lieferkette & Menschen:

- ✓ Supplier-Security-Richtlinie
- ✓ Awareness- & Schulungsrichtlinie

NIS2 ist kein Mammutprojekt.

Wer Organisation, Verantwortung und Steuerung sauber aufsetzt, ist innerhalb von 20 Tagen organisatorisch NIS2-fähig.

Wenn die Organisation steht, ist der Rest einfach. Ein strukturierter Einstieg reduziert nicht nur Risiken, sondern auch langfristigen Aufwand. Unternehmen schaffen Transparenz, stärken ihre Entscheidungsfähigkeit und legen den Grundstein für weitere Standards wie ISO 27001 oder TISAX.

NIS2 wird so vom Pflichtprogramm zu einem steuerbaren Bestandteil der Unternehmensorganisation.

Noch einfacher? Geht auch!

Man muss nicht alles selbst machen. Sie als Entscheider in einem KMU wissen, welche Kompetenzen Sie wo am sinnvollsten nutzen. Wir bei Vantarion wissen um Informationssicherheit, gesetzliche Anforderungen und wie auch Ihr Unternehmen beides vereinen kann.

Weitere Informationen auf unserer Website <https://www.vantarion.de>

