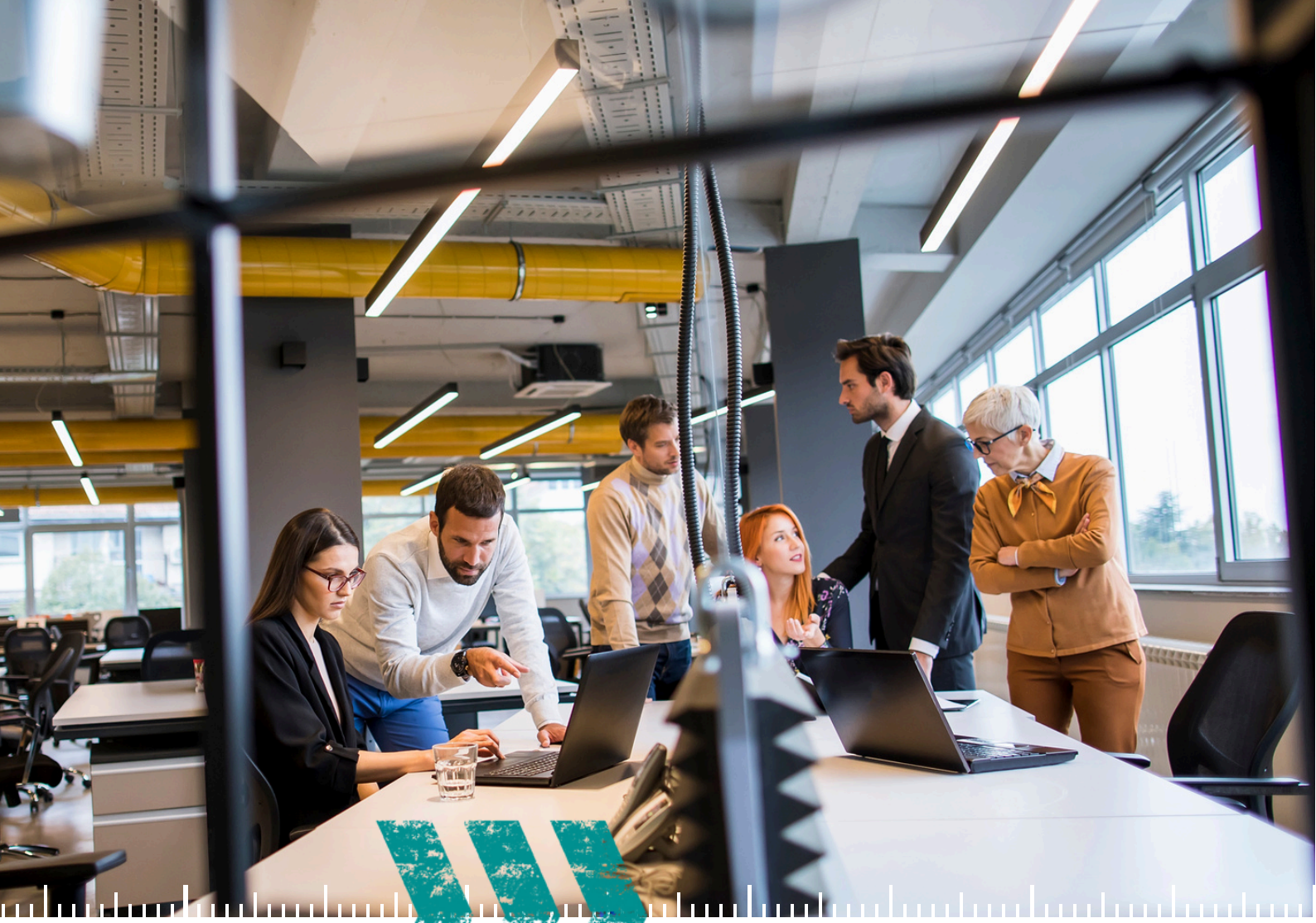


NIS2 Readiness Assessment

Wie Unternehmen ihre IT-Infrastruktur, Prozesse und Sicherheitsorganisation auf ein auditfähiges Niveau bringen

www.michael-wessel.de

michael wessel
THINK DIGITAL

Inhaltsübersicht

1. Einleitung - NIS2 als Prüfstein für die tatsächliche Belastbarkeit der IT

Die NIS2-Richtlinie verändert die Anforderungen an IT-Sicherheit grundlegend. Sie fordert nicht das bloße Vorhandensein von Policies, sondern den nachweisbaren Betrieb einer widerstandsfähigen, aktuellen und nachvollziehbaren IT-Architektur. Unternehmen müssen zeigen, dass ihre Sicherheitsmechanismen im Alltag funktionieren, dass Prozesse eingehalten werden und dass kritische Systeme jederzeit kontrolliert betrieben werden können.

Für viele Organisationen bedeutet das einen Paradigmenwechsel:
IT-Sicherheit ist nicht länger ein begleitendes Thema – sie wird zu einer Voraussetzung für Geschäfts- und Betriebsfähigkeit. Die Richtlinie macht sichtbar, was im Tagesbetrieb oft nicht auffällt: ungetestete Backups, gewachsene Netzwerke ohne Segmentierung, veraltete Systeme, unklare Rollen oder unzureichend dokumentierte Prozesse.

NIS2 verlangt ein Sicherheitsniveau, das nicht auf Vertrauen basiert, sondern auf Fakten. Und diese Fakten entstehen nur, wenn der tatsächliche Zustand der I T präzise analysiert wird. **Ein Readiness Assessment bildet dafür die Grundlage: Es zeigt nicht nur, wo Risiken liegen – sondern auch, wie reif und belastbar die bestehende Sicherheits-architektur wirklich ist.**

TIPP

Ihnen ist unklar, ob Ihr Unternehmen betroffen ist? Machen Sie jetzt den Test des BSI:

Zum Test

2. Warum der technische und organisatorische Reifegrad oft überschätzt wird

In den meisten Unternehmen ist die IT über Jahre gewachsen, angepasst, erweitert – aber nur selten konsequent modernisiert oder durchgängig dokumentiert worden. Systeme funktionieren im Alltag, Ausfälle werden pragmatisch kompensiert, und Sicherheitsmechanismen greifen punktuell. Solange der Betrieb stabil bleibt, entsteht leicht der Eindruck, dass die Umgebung robust ist.

Doch genau diese Alltagsperspektive führt zu einer gefährlichen Fehleinschätzung. NIS2 betrachtet nicht, wie „gefühlt sicher" eine Umgebung ist, sondern wie **nachweisbar widerstandsfähig sie im Ernstfall bleibt**. Es prüft nicht die Funktionstüchtigkeit, sondern **Struktur, Prozessesicherheit, Wiederherstellbarkeit und Kontrollmechanismen**.

Typische Beispiele aus Assessments zeigen diese Diskrepanz deutlich:

- Server laufen seit Jahren stabil, aber ohne Redundanz oder Support.
- Backups existieren, aber Wiederherstellungen wurden nie getestet.
- Netzwerke funktionieren, aber sie trennen kritische Systeme nicht voneinander.
- Identitäten sind nutzbar, aber nicht kontrolliert oder regelmäßig bereinigt.
- Prozesse sind beschrieben, aber im Alltag nicht verankert.
- Richtlinien existieren, aber sie sind weder operationalisiert noch nachweisbar.

Das Problem ist selten die fehlende Absicht — sondern die fehlende Transparenz über die tatsächliche Belastbarkeit der eigenen IT. Unter NIS2 reicht „es funktioniert bislang" nicht mehr aus. Gefordert ist ein Sicherheitsniveau, das strukturiert, geprüft und dokumentiert ist.
Die zentrale Frage lautet also nicht: „Läuft unsere IT?"
Sondern: „Wäre unsere IT im Ernstfall nachweislich in der Lage, ihre Aufgaben sicher zu erfüllen?"

Genau dieses Delta zwischen gefühlter Stabilität und realer Resilienz macht ein Readiness Assessment sichtbar – und schafft die Grundlage für eine zielgerichtete, priorisierte Modernisierung.

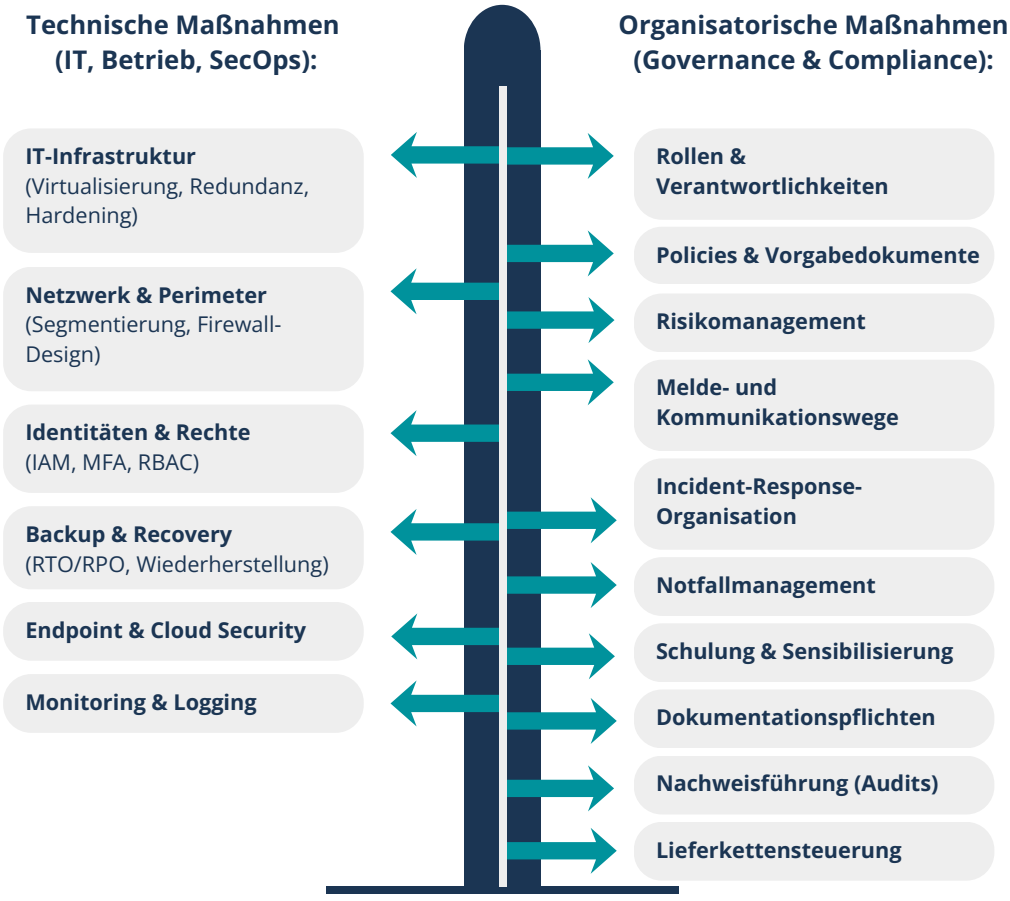
3. NIS2 verlangt nachgewiesene operative Sicherheit

NIS2 unterscheidet sich von bisherigen Sicherheitsvorgaben in einem entscheidenden Punkt: Die Richtlinie bewertet nicht nur, welche technischen Maßnahmen vorgesehen sind, sondern ob sie i**m täglichen Betrieb nachweislich funktionieren**. Damit rückt die operative Sicherheit in den Mittelpunkt — also die Fähigkeit einer Organisation, kritische IT-Systeme stabil, kontrolliert und nachvollziehbar zu betreiben.

Technische Schutzmaßnahmen müssen deshalb nicht nur existieren, sondern **systematisch überprüft**, **dokumentiert** und **im Ernstfall belastbar sein**. Ein Backup gilt erst dann als sicher, wenn die Wiederherstellung erfolgreich getestet wurde. Eine Segmentierung schützt erst dann, wenn ihre Regeln konsequent durchgesetzt und überwacht werden. Und Identitäten sind nur dann „gesichert", wenn Berechtigungen regelmäßig überprüft, gepflegt und minimal gehalten werden.

NIS2 macht IT-Sicherheit messbar. Die Richtlinie verlangt Strukturen, die nicht auf Annahmen oder Vertrauen basieren, sondern auf klaren technischen Belegen. Unternehmen müssen zeigen können, dass **Systeme widerstandsfähig** sind, dass **Sicherheitsprozesse greifen** und dass die Organisation in der Lage ist, **Störungen kontrolliert zu erkennen und zu behandeln**.

Damit verändert NIS2 die Perspektive: Sicherheit wird nicht mehr als Projektergebnis verstanden, sondern als operativer Zustand, den Unternehmen dauerhaft nachweisen müssen. Diese Anforderung ist nur erfüllbar, wenn der aktuelle Stand der IT transparent ist — **und genau diese Transparenz schafft ein Readiness Assessment.**



4. Erkenntnisse aus realen Readiness Assessments – Muster, die sich durch alle Branchen ziehen

Unabhängig von Branche oder Unternehmensgröße zeigt sich in Assessments ein konsistentes Muster: Die IT funktioniert, aber sie ist nicht resilient, nicht dokumentiert und nicht auditfähig.

4.1 Infrastruktur: Stabilität ist kein Zufallsprodukt

Serverlandschaften sind häufig historisch gewachsen. Sie laufen im Alltag zuverlässig, aber ohne Redundanz, ohne Lifecycle-Plan und ohne klaren Wiederanlaufmechanismus. NIS2 bewertet nicht den stabilen Alltag, sondern die Fähigkeit, einen Ausfall strukturiert zu kontrollieren.

4.2 Netzwerk: Segmentierung ist die Voraussetzung für Kontrolle

Viele Netzwerke sind groß, flach und schwer kontrollierbar. Sie bündeln Systeme unterschiedlichster Kritikalität in einem Segment. Eine Angriffsbewegung ließe sich kaum begrenzen. Segmentierung ist deshalb kein Firewall-Thema, sondern ein Architekturprinzip.

4.3 Backup & Recovery: Sicherheit entsteht erst bei der Wiederherstellung

Backups gelten als gesetzt — bis sie getestet werden. Erst wenn Wiederherstellungen reproduzierbar und dokumentiert funktionieren, entsteht das Sicherheitsniveau, das NIS2 verlangt.

4.4 Identitäten: Der wichtigste Verteidigungsraum der IT

Verwaiste Konten, breite Administratorrechte, fehlende MFA oder ungepflegte Berechtigungen sind typische Probleme. Identitätskontrolle ist heute das zentrale Sicherheitsprinzip — und NIS2 macht es zur Pflicht.

4.5 Prozesse: Sicherheitswirkung entsteht nur im gelebten Alltag

Viele Prozesse existieren schriftlich, aber nicht im Betrieb. Incident Response ist beschrieben, aber nicht geübt. Rollen sind formuliert, aber nicht verankert. Dokumentation existiert, aber ist nicht konsistent.

Die größte Schwachstelle entsteht selten durch Technik — sie entsteht durch das Zusammenspiel von Technik, Betrieb und fehlender Prozessreife.

5. Vom Assessment zur Roadmap – NIS2 planbar, wirtschaftlich und realistisch umsetzen

Das Readiness Assessment liefert die Diagnose. Die Roadmap ist der daraus abgeleitete, verbindliche Maßnahmenplan.

Eine wirksame Roadmap priorisiert nach:

- Sicherheitswirkung
- Kritikalität
- Aufwand
- Abhängigkeiten

und gliedert die Umsetzung in drei logisch aufeinander aufbauende Phasen.

Damit wird NIS2 von einem unübersichtlichen Regulierungsthema zu einem planbaren Sicherheits- und IT-Modernisierungsprojekt.

6. Technische Kernanforderungen aus NIS2 – und was sie in der Praxis bedeuten

NIS2 ist eine Richtlinie, die aus technischer Sicht sehr konkrete Anforderungen stellt. Viele dieser Anforderungen sind nicht neu, aber erstmals verbindlich formuliert und auditierbar. Unternehmen müssen nicht nur Maßnahmen umsetzen, sondern nachweisen können, dass diese Maßnahmen im laufenden Betrieb zuverlässig funktionieren.

Im Folgenden werden die zentralen technischen Pflichtbereiche beschrieben – jeweils mit Fokus darauf, was NIS2 tatsächlich verlangt und wie diese Anforderungen in realen IT-Umgebungen bewertet werden.

6.1 Infrastruktursicherheit: Verfügbarkeit, Redundanz und Lifecycle

Die Richtlinie verlangt eine Infrastruktur, die nachweislich:

- aktuell,
- unterstützt,
- redundant,
- härtbar,
- und wiederanlaufbar ist.

In der Praxis bedeutet das:
Virtualisierung ohne Cluster genügt NIS2 nicht.
Server ohne Support- oder Security-Patches gelten als hohes Risiko. Betriebsrelevante Systeme benötigen definierte RTO/RPO.
Storage, Netzwerk und Compute müssen konsistent auf Redundanz ausgelegt sein.

NIS2 betrachtet Infrastruktur als Gesamtsystem – nicht als Sammlung einzelner Komponenten

6.2 Netzwerksicherheit: Segmentierung und Minimierung der Angriffsfläche

Technisch erwartet NIS2:

- kontrollierte Segmentierung,
- eingeschränkte Bewegungsmöglichkeiten für Angreifer,
- präzise Firewall-Regeln,
- getrennte Zonen für Server, Clients, OT, IoT und externe Partner.

In realen Umgebungen sind diese Anforderungen oft nicht erfüllt:

- VLANs dienen der Organisation – nicht der Sicherheit.
- Firewalls erlauben mehr, als sie sollten.
- OT-/Produktionssysteme hängen im gleichen Netz wie Clients.

NIS2 macht daraus eine klare Pflicht: Systeme müssen isoliert sein, wenn sie nicht direkt voneinander abhängen.

Verwaiste Konten, lokale Admin-rechte oder selten geprüfte AD-Gruppen widersprechen den Anforderungen.
NIS2 definiert Identitäten als kritische Infrastruktur innerhalb der Infrastruktur.

6.3 Identitäten & Berechtigungen: Schutz des wichtigsten Angriffsvektors

Die Richtlinie stärkt den Identitätsschutz erheblich. Sie verlangt:

- MFA für alle sensiblen Zugänge,
- minimal vergebene Rechte,
- klare Administratorrollen,
- regelmäßige Account-Reviews,
- Trennung von Admin- und Standardkonten.

Die operative Umsetzung ist oft das größte Defizit.

6.4 Endpoint Security & Patchmanagement

Technisch fordert NIS2:

- aktuelle Betriebssysteme,
- automatisierte Patchprozesse,
- Schutzmechanismen mit zentraler Auswertung,
- Monitoring von Abweichungen,
- vollständige Abdeckung aller Endgeräte.

Ein Office-Patch genügt nicht, wenn Browser, PDF-Reader oder Java veraltet sind.

Besonders wichtig:
Auch Third-Party-Software fällt unter NIS2-Pflichten.

6.5 Backup & Recovery: Ein System ist nur so sicher wie sein Wiederanlaufment

NIS2 verlangt:

- vollständige Backups
- verschlüsselte Speicherung
- geografisch getrennte Aufbewahrung
- regelmäßige Wiederherstellungstests
- dokumentierte RTO/RPO
- Überwachung und Alarmierung

In Assessments zeigt sich häufig:

- kritische Systeme sind nicht vollständig gesichert
- Daily/Weekly/Monthly sind unzureichend
- Offsite fehlt
- Wiederherstellung ist nie getestet

Für NIS2 zählt nicht das Backup – sondern der erfolgreich getestete Wiederanlauf.

6.6 Logging, Monitoring & Angriffserkennung

Die Richtlinie fordert:

- zentrale Logsammlung
- korrelierte Ereignisauswertung
- Alarmierung bei sicherheitsrelevanten Ereignissen
- dokumentierte Reaktion

Operativ bedeutet das:

- Firewalls müssen loggen
- Server müssen überwacht werden
- Endpoints müssen Ereignisse melden
- M365 muss mit Security-Baselines betrieben werden

NIS2 bewertet nicht die Tools, sondern die Fähigkeit zur tatsächlichen Angriffserkennung.

6.7 Physische Sicherheit & Betriebsprozesse

Technisch verlangt NIS2:

- gesicherte Technikräume
- Zutrittskontrolle
- dokumentierte Betriebsmittel
- definierte Notfallprozesse
- Umgebungsüberwachung (Strom, Klima, Hardwarestatus)

Viele Umgebungen erfüllen diese Anforderungen teilweise – aber nicht systematisch. NIS2 zwingt Unternehmen dazu, physische Sicherheit als Teil der IT-Sicherheitsarchitektur zu verstehen.

7. Ergebnis des NIS2 Readiness Assessments

Das NIS2 Readiness Assessment endet nicht mit einer Auflistung von Feststellungen. Unternehmen erhalten ein vollständig ausgearbeitetes, technisch fundiertes und priorisiertes Ergebnisdokument, das als direkte Grundlage für die NIS2-Umsetzung und die Modernisierung der IT-Sicherheitsarchitektur dient.

Die Auswertung enthält folgende Bestandteile:

7.1 Vollständige technische Analyse aller sicherheitsrelevanten Bereiche

Die Analyse umfasst Infrastruktur, Netzwerk, Identitäten, Backup, Endpoint-, Cloud- und Monitoring-Strukturen sowie physische und organisatorische Sicherheitsaspekte. Jede Feststellung wird fachlich begründet und nachvollziehbar dokumentiert.

7.2 Reifegradbewertung mit klarer Einordnung

Alle identifizierten Themen werden nach Kritikalität bewertet. Dabei wird zwischen Betriebsrisiken, Sicherheitsrisiken und regulatorischen Anforderungen unterschieden. Das Ergebnis ist ein realistisches Abbild der tatsächlichen Belastbarkeit der bestehenden IT-Architektur.

7.3 Konkrete Maßnahmenempfehlungen pro Themenbereich

Für jede Feststellung werden umsetzbare Empfehlungen formuliert — technisch sauber, priorisiert und mit klarer Wirkung. Keine generischen Aussagen, sondern konkrete, praxisnahe Maßnahmen, die sich direkt in Projekte überführen lassen.

7.4 Prioritätenliste nach Sicherheitswirkung und Aufwand

Die Maßnahmen werden in drei Kategorien gegliedert:

- kritisch - kurzfristig notwendig
- zeitnah umsetzbar - mittelfristig sinnvoll
- strategisch - langfristige Optimierungen

Diese Priorisierung bildet die Grundlage für Budgetierung und Projektplanung.

7.5 Strukturierte Roadmap für 0–3 / 3–12 / 12–36 Monate

Die Roadmap verbindet technische, organisatorische und betriebliche Maßnahmen in einer sinnvollen Reihenfolge. Sie berücksichtigt Abhängigkeiten, Ressourcenbedarf und wirtschaftliche Aspekte. Damit entsteht ein Plan, der nicht nur NIS2-konform ist, sondern im realen Betrieb umsetzbar bleibt.

7.6 Management- und Entscheidungsgrundlagen für Geschäftsführung & IT-Leitung

Das Ergebnisdokument enthält klar verständliche Zusammenfassungen für Entscheider:

- Top-Risiken der aktuellen IT
- Einschätzung der Sicherheitslage
- erforderliche Maßnahmen mit Aufwand und Wirkung
- strategische Optionen für den weiteren Modernisierungspfad

Dadurch können Geschäftsführung und IT-Leitung Entscheidungen auf Basis von Fakten treffen — nicht auf Annahmen oder Teilinformationen.

8. Ergänzende regulatorische Perspektive

Die technische Umsetzung von NIS2 ist der Kernfokus von michael wessel.
Bei datenschutzrechtlichen und regulatorischen Fragen können auf Wunsch spezialisierte Partner hinzugezogen werden — beispielsweise die Dr. Bittner Consulting GmbH & Co. KG.

9. Fazit – NIS2 als Treiber einer widerstandsfähigen IT-Landschaft

NIS2 fordert nachweisbare Sicherheit — nicht theoretische. Unternehmen sind gefordert, Strukturen zu schaffen, die Ausfälle verhindern, Angriffe begrenzen und Prozesse im Ernstfall beherrschbar machen.

Das NIS2 Readiness Assessment liefert die Basis:

- Es zeigt technische Realität, nicht vermutete Sicherheit.
- Es schafft Priorität, Struktur und Planbarkeit.
- Es ermöglicht eine Modernisierung, die wirtschaftlich sinnvoll und auditfähig ist.

Organisationen, die frühzeitig starten, gewinnen nicht nur Compliance, sondern eine belastbare, stabile und resiliente IT-Infrastruktur — und damit langfristige Betriebssicherheit.

Jetzt NIS2 Readiness Assessment anfordern

Eine NIS2-Umsetzung gelingt nur, wenn Unternehmen ihren tatsächlichen technischen und organisatorischen Reifegrad kennen. Das NIS2 Readiness Assessment liefert die Grundlage dafür: eine fundierte Analyse, klare Prioritäten und eine Roadmap, die im realen Betrieb umsetzbar ist.

Sprechen Sie mit unseren Experten und erhalten Sie:

- eine belastbare Bewertung Ihrer aktuellen Sicherheitslage,
- konkrete Maßnahmenempfehlungen mit Priorisierung,
- transparente Entscheidungsgrundlagen für IT-Leitung und Geschäftsführung.

+49 (0)511 999 79 – 201

kontakt@michael-wessel.de

www.michael-wessel.de

Jennifer Müller