NIS2-Selbstcheck für Unternehmen

Wie nah sind Sie an der NIS2-Konformität?

www.michael-wessel.de

michael wessel
THINK DIGITAL

Inhaltsübersicht

Diese Checkliste hilft Unternehmen dabei, in wenigen Minuten einzuschätzen, wie nah sie bereits an der Erfüllung der NIS2-Anforderungen sind. Sie deckt sowohl technische als auch organisatorische Aspekte ab und zeigt transparent auf, wo bereits ein gutes Sicherheitsniveau besteht und wo noch Handlungsbedarf besteht.

Die Checkliste dient damit als praktischer erster Schritt, um Risiken sichtbar zu machen, Prioritäten zu setzen und den eigenen Weg zu einer auditfähigen und widerstandsfähigen IT-Sicherheitsstruktur zu planen.

1. Infrastruktur & Verfügbarkeit

NIS2 bewertet die tatsächliche Belastbarkeit der IT-Infrastruktur – nicht den stabilen Tagesbetrieb. Unzureichende Redundanzen, veraltete Systeme oder fehlende Wiederanlaufkonzepte gehören zu den häufigsten kritischen Befunden in Assessments.

ja	nein	
☐	☐	Unsere Server laufen auf unterstützter Hardware und aktuellen Betriebssystemen.
☐	☐	Wir verfügen über Redundanzen (Cluster, Storage, Netzwerk), um Ausfälle abzufangen.
☐	☐	Alle kritischen Systeme haben definierte Wiederanlaufzeiten (RTO/RPO).
☐	☐	Unsere IT-Infrastruktur ist dokumentiert und aktuell.

2. Netzwerk- & Zugriffssicherheit

Netzwerksegmentierung ist eines der zentralen technischen Anforderungen von NIS2. Flache Netze und weit gefasste Firewall-Regeln führen in der Praxis regelmäßig zu hohen Risiken.

ja	nein	
☐	☐	Unser Netzwerk ist segmentiert (Server, Clients, OT/IoT, Gäste, externe Partner).
☐	☐	Firewall-Regeln sind restriktiv, aktuell und frei von „ANY-Regeln“.
☐	☐	Externe Zugänge (VPN etc.) sind durch MFA und Rollenmodelle abgesichert.
☐	☐	Bewegungen im Netzwerk können nachvollzogen und kontrolliert werden.

3. Identitäten, Rechte & Zugriffskontrolle

Die meisten Angriffe beginnen heute über kompromittierte Identitäten. NIS2 verlangt deshalb eine klare Kontrolle privilegierter Konten und nachvollziehbare Berechtigungsstrukturen.

ja	nein	
☐	☐	MFA ist für alle sensiblen und administrativen Zugänge verpflichtend.
☐	☐	Administratorrechte sind klar getrennt (Admin-Konten / Standard-Konten).
☐	☐	Es gibt regelmäßige Überprüfungen aller Accounts und Berechtigungen.
☐	☐	Verwaiste Benutzer- oder Gerätekonten existieren nicht mehr.

4. Backup & Wiederherstellbarkeit

Ein Backup gilt erst dann als sicher, wenn die Wiederherstellung getestet und dokumentiert ist. Genau hier zeigen Assessments in vielen Unternehmen die größten Abweichungen zu NIS2.

ja	nein	
☐	☐	Alle produktiven Systeme sind vollständig im Backup enthalten.
☐	☐	Backups werden verschlüsselt und mindestens an einem zweiten Ort gespeichert.
☐	☐	Wiederherstellungstests werden regelmäßig durchgeführt und dokumentiert.
☐	☐	Backup-Prozesse werden überwacht und Fehler zeitnah behoben.

5. Prozesse, Rollen & organisatorische Vorgaben

NIS2 fordert gelebte und überprüfbare Prozesse – nicht nur definierte. Unklare Rollen oder ungeübte Abläufe führen im Ernstfall zu Sicherheits- und Compliance-Verlusten.

ja	nein	
☐	☐	Es gibt klar definierte Rollen (z. B. IT-Sicherheitsverantwortliche).
☐	☐	Sicherheitsvorfälle, Änderungen und Risiken folgen dokumentierten Prozessen.
☐	☐	Alle Mitarbeitenden sind regelmäßig geschult und sensibilisiert.
☐	☐	Richtlinien (Passwörter, BYOD, Backup, Cloud, Netzwerk, Incident Response) sind aktuell und werden gelebt.

6. Endpoint-, Client- & Cloud-Sicherheit

Endpoints und Cloud-Dienste sind heute primäre Angriffsflächen. NIS2 verlangt hier konsistente Sicherheitsrichtlinien, zentrale Kontrolle und vollständige Patch- und Compliance-Prozesse.

ja	nein	
☐	☐	Alle Endgeräte werden zentral verwaltet, geschützt und gepatcht.
☐	☐	Auch Drittsoftware (Browser, PDF, Java etc.) wird automatisiert aktualisiert.
☐	☐	Cloud-Dienste wie Microsoft 365 sind nach Best Practices abgesichert.
☐	☐	Mobile Geräte sind über MDM und klare Richtlinien kontrolliert.

7. Monitoring, Logging & Angriffserkennung

NIS2 verlangt die Fähigkeit, sicherheitsrelevante Ereignisse zuverlässig zu erkennen und nachweisbar darauf zu reagieren. Fehlende oder unvollständige Logs, unklare Alarmierungswege und nicht korrelierte Ereignisdaten gehören zu den häufigsten Ursachen dafür, dass Angriffe zu spät bemerkt werden.

ja	nein	
☐	☐	Sicherheitsrelevante Ereignisse werden zentral gesammelt und ausgewertet.
☐	☐	Alarmmeldungen werden aktiv überwacht und nicht nur passiv geloggt.
☐	☐	Es existiert ein definiertes Verfahren zur Reaktion auf sicherheitsrelevante Ereignisse.
☐	☐	Die Angriffserkennung deckt sowohl Netzwerk als auch Endpoints ab.

8. Physische Sicherheit & Betriebsumgebung

NIS2 bewertet auch die physische Integrität der IT-Umgebung. Fehlende Zutrittskontrollen, ungesicherte Technikräume oder unzureichende Umgebungsüberwachung führen schnell zu Risiken, die weder durch Software noch durch organisatorische Maßnahmen kompensiert werden können.

ja	nein	
☐	☐	Serverräume sind abschließbar, überwacht und ausschließlich für IT vorgesehen.
☐	☐	Serverschränke sind geschlossen und gegen unbefugten Zugriff geschützt.
☐	☐	Netzwerk- und Technikräume werden nicht als Abstellflächen genutzt.
☐	☐	Klimatisierung, Stromversorgung und USV sind funktional und getestet.

9. Dokumentation & Nachweisbarkeit

NIS2 fordert nicht nur die Umsetzung technischer und organisatorischer Maßnahmen, sondern deren nachweisbare Wirksamkeit. Fehlende, veraltete oder verstreute Dokumentation gehört zu den häufigsten Gründen, warum Sicherheitsmaßnahmen im Audit nicht anerkannt werden.

ja	nein	
☐	☐	Alle sicherheitsrelevanten Prozesse sind dokumentiert und aktuell.
☐	☐	Nachweise über Tests, Schulungen und Prüfungen liegen vor.
☐	☐	Es existiert ein Risikomanagement mit regelmäßigen Bewertungen.
☐	☐	Die Dokumentation ist auditfähig und vollständig.

10. Lieferkette & externe Dienstleister

NIS2 bezieht die gesamte IT-Lieferkette in die Sicherheitsverantwortung ein. Fehlende Nachweise, unklare Zuständigkeiten oder ungesicherte Dienstleisterzugänge führen dazu, dass Risiken außerhalb des eigenen Unternehmens entstehen – aber dennoch vollständig auf Ihre Organisation zurückfallen.

ja	nein	
☐	☐	Externe IT-Dienstleister werden vertraglich und technisch kontrolliert.
☐	☐	Sicherheitsanforderungen sind Bestandteil aller Dienstleisterbeziehungen.
☐	☐	Externe Systeme und Partnerzugänge sind klar definiert und begrenzt.
☐	☐	Risiken in der Lieferkette werden regelmäßig bewertet.

Auswertung

- **80–100 % erfüllt** → Sehr gute Basis. NIS2 kann mit gezielten Maßnahmen erreicht werden.
- **50–80 % erfüllt** → Gute Grundstrukturen vorhanden, aber deutliche technische und organisatorische Lücken.
- **30-50 % erfüllt** → NIS2 nur durch umfangreichere Modernisierungsmaßnahmen erreichbar.
- **unter 30 % erfüllt** → kritisches Risiko. NIS2-Konformität im aktuellen Zustand nicht realisierbar.

Fazit: Wann Sie Unterstützung brauchen

Wenn Sie in mehreren Bereichen ‚nein' angekreuzt haben oder unter 80 % Erfüllung liegen, ist eine strukturierte Ursachenanalyse erforderlich.
Ein NIS2 Readiness Assessment liefert die technische und organisatorische Klarheit, die notwendig ist, um Risiken zu priorisieren, Handlungsfelder zu definieren und eine auditfähige Sicherheitsarchitektur aufzubauen.

Ihr nächster Schritt

Gerne unterstützen wir Sie dabei, Ihre NIS2-Anforderungen strukturiert umzusetzen und Ihre IT-Sicherheit nachhaltig zu stärken.

+49 (0)511 999 79 – 201

kontakt@michael-wessel.de

www.michael-wessel.de

michael wessel
THINK DIGITAL