cycura

NIS2 erfüllt.
Trotzdem angreifbar.

Warum Compliance-Checklisten keine Sicherheit garantieren – und was technisch nachweisbare NIS2-Umsetzung wirklich bedeutet

Die Realität: NIS2 verpflichtet – aber die technische Umsetzung hakt

Die NIS2-Richtlinie schreibt konkrete Sicherheitsmaßnahmen vor. Doch zwischen dem Verstehen des Gesetzestextes und einer technisch belastbaren Umsetzung in Microsoft-Umgebungen klafft eine Lücke. Viele Organisationen dokumentieren sich compliant, während die technische Realität Lücken aufweist.

Was Sie in diesem Guide erwartet

- Die 4 kritischen Umsetzungslücken bei NIS2-Projekten
- Warum Papier-Compliance vor Audits nicht schützt
- Das Framework für technisch nachweisbare Sicherheit
- Ein Selbstcheck: Ist Ihre NIS2-Umsetzung betriebswirksam?

cycura

Die 4 Lücken, die Ihre NIS2-Umsetzung angreifbar machen

1. Die Papier-Compliance-Lücke

Maßnahmen sind dokumentiert, aber technisch nicht umgesetzt. Der Audit wird bestanden – die Sicherheit bleibt Lücke.

2. Die Lizenz-Illusion

Microsoft 365 E5 ist lizenziert, aber die Security-Features sind nicht konfiguriert. Teure Lizenzen, ungenutzter Schutz.

3. Die Audit-vs-Betrieb-Lücke

Zum Audit-Zeitpunkt ist alles korrekt. Im laufenden Betrieb driften Konfigurationen ab. Die dokumentierte Sicherheit existiert nicht mehr.

4. Die Verantwortungslücke

Compliance definiert, IT setzt um – aber niemand prüft die technische Wirksamkeit. Im Ernstfall weiß niemand, wer verantwortlich ist.

cycura

1

Die Papier-Compliance-Lücke

DIE LÜCKE

Organisationen erstellen umfangreiche Policies für NIS2. Die technische Umsetzung in Microsoft 365 und Azure bleibt oberflächlich oder unvollständig. Die Dokumentation suggeriert Sicherheit, die technisch nicht existiert.

DAS KONKRETE RISIKO

Bei einem Sicherheitsvorfall oder einer behördlichen Überprüfung zeigt sich: dokumentierte Maßnahmen sind nicht aktiv oder voller Ausnahmen. Sie haften für nicht-umgesetzte Schutzmaßnahmen – obwohl Ihre Dokumentation „grün" war.

DIE KONSEQUENZ

Ihre Dokumentation schützt Sie nicht vor Haftung. Sie können nicht nachweisen, dass Ihre Maßnahmen wirken – weil sie technisch nicht vorhanden sind. Diese Lücken entstehen im Alltag, nicht im Audit. Sie sind in bestehenden Reports oft nicht sichtbar.

WAS WIR IN ASSESSMENTS FINDEN

- Dokumentierte MFA-Pflicht, aber 30% der Admins ohne MFA
- Beschriebene Zugriffskontrollen, aber keine Conditional Access-Regeln
- Vorgeschriebene Logging-Anforderungen, aber Logs werden nicht gesammelt
- Existierende DLP-Richtlinien, die auf keine sensiblen Daten angewendet werden

PRÜFPFAD

NIS2-Dokumentation → Technische Konfiguration in Entra ID/Defender → Abgleich tatsächlicher Einstellungen mit dokumentierten Maßnahmen

cycura

2

Die Lizenz-Illusion

DIE LÜCKE

Unternehmen kaufen Microsoft 365 E5, um NIS2 abzudecken. Doch Lizenzen allein erfüllen keine Vorgaben – sie müssen konfiguriert und betrieben werden. Viele Features bleiben im Default-Zustand oder deaktiviert.

DAS KONKRETE RISIKO

Sie glauben, durch den Einkauf teurer Lizenzen compliant zu sein. Tatsächlich fehlen essenzielle Schutzmechanismen: PIM ist nicht aktiv, Conditional Access deckt nicht alle Admin-Pfade ab, Defender läuft im Audit-Modus ohne Enforcement. Ein Angriff gelingt über genau die Lücken, die die Lizenz schließen sollte.

DIE KONSEQUENZ

Sie haben für Sicherheit gezahlt, erhalten sie aber nicht. Im Ernstfall zeigt sich, dass Ihre teuren Lizenzen keinen Schutz bieten – weil sie nie konfiguriert wurden. Diese Abweichungen sind ohne gezielte technische Prüfung schwer erkennbar.

WAS WIR IN ASSESSMENTS FINDEN

- PIM lizenziert, aber nur für 10% der Admin-Konten aktiv
- Conditional Access existiert, aber legale Admin-Alternativen nicht abgedeckt
- Defender für Cloud Apps lizenziert, aber keine Shadow-IT-Überwachung
- Audit-Logging aktiv, aber keine Auswertung oder Alerting

PRÜFPFAD

Microsoft 365 Admin Center → Lizenzen vs. aktivierte Features → Konfigurationsstatus von PIM, CA, Defender → tatsächliche Abdeckung

cycura

3

Die Audit-vs-Betrieb-Lücke

DIE LÜCKE

Zum Audit-Zeitpunkt sind alle Systeme korrekt konfiguriert. Doch im laufenden Betrieb entstehen Ausnahmen, Konfigurationen werden für Troubleshooting geändert und nicht zurückgesetzt. Die dokumentierte Sicherheit driftet ab.

DAS KONKRETE RISIKO

Sie weisen zum Stichtag hohe Reifegrade auf. Sechs Monate später existieren kritische Sicherheitslücken. Bei einem Vorfall stellt sich heraus: Ausnahmen von MFA wurden zur Regel, externe Zugriffe für Dienstleister nie entzogen. Die technische Kontrolle wurde aufgegeben, ohne dass es dokumentiert wurde.

DIE KONSEQUENZ

Ihre Umsetzung funktionierte einmal – aber nicht mehr. Sie können nicht nachweisen, dass Ihre Controls heute noch aktiv sind. Viele dieser Lücken bestehen, ohne dass sie intern wahrgenommen werden.

WAS WIR IN ASSESSMENTS FINDEN

- Conditional Access-Ausnahmen, die „vorübergehend" eingerichtet wurden und seit Monaten aktiv sind
- Neue App-Registrations mit hohen Rechten, die nie reviewt wurden
- Externe Gastkonten mit Zugriff auf sensible Daten, lange nach Projektende
- Änderungen an Security-Einstellungen durch Support ohne Change-Prozess

PRÜFPFAD

Entra ID Sign-Ins → Ausnahmen bei CA → Audit-Logs für Security-Änderungen → Review externer Zugriffe über letzte 6 Monate

cycura

4

Die Verantwortungslücke

DIE LÜCKE

Compliance definiert Anforderungen, IT setzt sie um – aber niemand prüft die technische Wirksamkeit im Alltag. Es fehlt ein Gremium oder Prozess, der sicherstellt, dass regulatorische Anforderungen technisch dauerhaft umgesetzt sind.

DAS KONKRETE RISIKO

Wichtige Sicherheitsentscheidungen fallen zwischen zwei Stühlen. Compliance denkt, die Technik sei umgesetzt; die Technik denkt, Compliance prüfe die Wirksamkeit. Im Ernstfall ist niemand verantwortlich. Die Haftung trägt das Unternehmen, die Verantwortung ist unklar verteilt.

DIE KONSEQUENZ

Niemand fühlt sich zuständig für die technische Qualität Ihrer NIS2-Umsetzung. Es gibt keine regelmäßige, unabhängige Prüfung. Dokumentation und tatsächliche Konfiguration weichen oft unbemerkt voneinander ab.

WAS WIR IN ASSESSMENTS FINDEN

- Kein definiertes RACI für NIS2-Technikmaßnahmen
- Compliance-Reports werden nicht mit technischen Metriken abgeglichen
- Sicherheitsincidents werden nicht auf Einhaltung dokumentierter Verfahren geprüft
- Keine regelmäßigen technischen Reviews der NIS2-Maßnahmen

PRÜFPFAD

Organigramm → Zuständigkeiten für NIS2-Technik → Meeting-Protokolle → Nachweis technischer Reviews

cycura

Die Lösung: Technisch nachweisbare Sicherheit

NIS2-Compliance ist kein Papierprojekt und kein Lizenzkauf. Sie erfordert technisch belastbare Maßnahmen, die im Betrieb überprüfbar sind – dauerhaft, nicht nur zum Audit-Zeitpunkt.

Was technisch nachweisbare Sicherheit auszeichnet

Konkrete Umsetzung: Jede dokumentierte Maßnahme hat eine technische Entsprechung in Microsoft 365/Azure, die jederzeit überprüfbar ist.

Lizenz-Optimierung: Bestehende Microsoft-Lizenzen (E5) werden vollständig für Security genutzt, nicht nur erworben.

Betriebliche Wirksamkeit: Maßnahmen sind in Betriebsprozesse eingebunden (Onboarding/Offboarding, Change Management).

Klare Verantwortung: Definierte Rollen für Umsetzung, Überprüfung und kontinuierliche Anpassung der technischen Controls.

DIE ZENTRALE FRAGE

Können Sie heute, ohne großen Aufwand, nachweisen, dass alle Ihre NIS2-relevanten technischen Controls aktiv, korrekt konfiguriert und lückenlos dokumentiert sind? Wenn nicht, haben Sie ein Transparenzproblem – und damit ein Risiko. Die Bewertung erfordert tiefes Verständnis der Microsoft-Umgebung und kontinuierlichen Abgleich zwischen Dokumentation und realer Konfiguration.

cycura

Der NIS2-Reifegrad-Check

Stufe	Beschreibung
1 Ad-hoc	Keine systematische NIS2-Auseinandersetzung. „Wir wissen nicht, ob wir betroffen sind."
2 Definiert	Rechtliche Einordnung erfolgt, Maßnahmen dokumentiert, aber technisch unvollständig umgesetzt.
3 Gesteuert	Technische Basismaßnahmen aktiv, aber nicht kontinuierlich überwacht oder auf Dauerhaftigkeit geprüft.
4 Optimierend	Technische Maßnahmen vollständig, betriebsintegriert und regelmäßig auf Wirksamkeit geprüft.
5 Exzellent	Vollständige technische Umsetzung, automatisierte Compliance-Checks, Integration in Security-Operations.

Die meisten Organisationen befinden sich auf Stufe 2 oder 3. Der Sprung zu Stufe 4 ist innerhalb von 3-6 Monaten erreichbar – und bildet die belastbare Basis für Audit und Betrieb.

Wo stehen Sie? – 5 Fragen zum Selbstcheck

1. Können Sie für jede dokumentierte NIS2-Maßnahme die konkrete technische Konfiguration in Azure/365 benennen?
2. Sind alle E5-Security-Features, die Sie lizenziert haben, tatsächlich aktiv konfiguriert?
3. Gibt es einen Nachweis, dass Ihre Security-Konfigurationen der letzten 3 Monate stabil waren?
4. Ist klar definiert, wer technisch dafür verantwortlich ist, dass NIS2-Maßnahmen dauerhaft wirksam bleiben?
5. Könnten Sie morgen einem Auditor nachweisen, dass Ihre MFA, Zugriffskontrollen und Logging technisch vollständig sind?

cycura

Der 12-Punkte Risiko-Check (NIS2-Technik)

Beantworten Sie mit Ja oder Nein. Jedes „Nein" ist ein potenzielles Risiko.

Technische Umsetzung

1. Sind alle dokumentierten Zugriffsschutzmaßnahmen (MFA, CA) für 100% der relevanten Konten aktiv (ohne Ausnahmen)?
2. Sind Ihre E5-Security-Lizenzen vollständig konfiguriert (PIM, Defender, DLP) oder nur erworben?
3. Werden alle Security-relevanten Einstellungsänderungen zentral geloggt und monatlich reviewed?
4. Gibt es einen technischen Nachweis, dass Ihre Incident-Response-Verfahren funktionieren (getestet)?

Dauerhaftigkeit & Verantwortung

5. Werden neue Mitarbeiter/Admins automatisch in die NIS2-Technik-Kontrollen aufgenommen?
6. Gibt es einen dokumentierten Prozess für Security-Ausnahmen (Zeitlimit, Genehmigung, Review)?
7. Ist klar definiert, wer technisch für die Aufrechterhaltung der NIS2-Maßnahmen zuständig ist?
8. Werden externe Zugriffe technisch auf das Minimum beschränkt und quartalsweise geprüft?

cycura

Der 12-Punkte Risiko-Check (Fortsetzung)

Nachweisbarkeit

9. Können Sie die Vollständigkeit Ihrer Audit-Logs nachweisen (keine Lücken, korrekte Retention)?
10. Ist Ihre Backup-Strategie für 365/Azure technisch implementiert und getestet?
11. Gibt es einen aktuellen Bericht zum Umsetzungsstand aller NIS2-relevanten Microsoft-Controls?
12. Wurden alle technischen Abweichungen von der NIS2-Security-Baseline dokumentiert und begründet?

Auswertung

Nein-Antworten	Risikostufe	Empfohlene Maßnahmen
0-2	Niedrig	Kontinuierliche Optimierung, regelmäßige Reviews
3-5	Mittel	Technische Lücken schließen, Prozesse verankern
6-9	Hoch	Sofortige technische Umsetzung erforderlich, Audit-Risiko
10-12	Kritisch	Keine belastbare NIS2-Umsetzung, dringender Handlungsbedarf

Mehr als 3x „Nein"? Ihre NIS2-Umsetzung hat wahrscheinlich Lücken, die intern nicht vollständig sichtbar sind. Prüfen Sie, ob Ihre Umsetzung einem Audit oder Angriff standhält – und wo Risiken bestehen, die Sie selbst nicht erkennen. **www.cycura.de/termin**

cycura

Impressum

cycura GmbH

Ihr Spezialist für Microsoft-Security

Kontakt:
E-Mail: info@cycura.de
Web: www.cycura.de

Handelsregister: Amtsgericht Göttingen HRB 206706
USt-IdNr.: DE354593485
