CUBIC SOLUTIONS

BEISPIELAUSWERTUNG · MUSTER

NIS2 Readiness Report

Standortbestimmung der Cybersicherheit nach NIS2 für Ihre Microsoft-365-Umgebung. Organisatorischer Self-Check kombiniert mit technischem Read-only-Scan.

ERSTELLT FÜR	**Muster GmbH (Beispielunternehmen)**
BERICHTSART	**NIS2 Readiness Report**
BERICHTSDATUM	**31. Mai 2026**
ERSTELLT VON	**cubic solutions GmbH**
BERICHTSSTAND	**Version 1.0 · Muster**
VERTRAULICHKEIT	**Vertraulich**

HINWEIS: MUSTERBERICHT

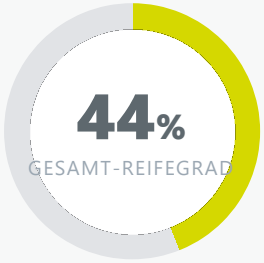
Dies ist eine fiktive Beispielauswertung zu Demonstrationszwecken. Unternehmensname, Kennzahlen und Befunde sind frei erfunden und beziehen sich auf kein reales Unternehmen. Ein echter Report wird ausschließlich auf Basis Ihres eigenen Self-Checks und Ihres eigenen Microsoft-365-Scans erstellt. Vertraulich, nur für den internen Gebrauch des Empfängers bestimmt.

BEISPIEL / MUSTER GMBH

FÜR DIE GESCHÄFTSFÜHRUNG

Management Summary

Die Muster GmbH steht bei NIS2 noch am Anfang. Wichtige organisatorische Grundlagen fehlen, technisch ist die Microsoft-365-Umgebung teils gut, teils lückenhaft abgesichert. Das größte Problem ist nicht ein einzelnes technisches Detail, sondern dass die Verantwortung nicht klar bei der Leitung verankert ist.



Grundlegend

Ampel Gelb: grundlegend aufgestellt, aber nicht NIS2-konform

Ein Gesamtwert von 44 Prozent bedeutet: Es ist bereits etwas vorhanden, aber zentrale Pflichten sind nicht erfüllt. Vier von elf Themenfeldern liegen im roten Bereich. Ohne Nachsteuern besteht ein konkretes Haftungs- und Ausfallrisiko. Die gute Nachricht: Die größten Lücken lassen sich mit überschaubarem Aufwand schließen.

4	5	2
Themenfelder im roten Bereich (kritisch, sofort handeln)	Themenfelder im gelben Bereich (grundlegend, ausbauen)	Themenfelder im grünen Bereich (gut aufgestellt)

Die größten Risiken im Klartext

1. **Niemand ist klar verantwortlich, die Leitung ist nicht geschult**
   Es gibt keine benannte verantwortliche Person und keine dokumentierte Schulung der Geschäftsführung. Genau das verlangt NIS2 aber ausdrücklich von der Leitung.
2. **Kein eigenes Backup von Microsoft 365**
   Mails, Dateien und Teams-Inhalte werden nicht zusätzlich gesichert. Microsoft sichert diese Daten nicht dauerhaft. Bei Ransomware oder Löschung können sie unwiederbringlich verloren gehen.
3. **Kein Notfallplan für den Ernstfall**
   Es ist nicht geregelt, wer bei einem Angriff was tut. Auch die gesetzliche Meldepflicht ans BSI binnen 24 bzw. 72 Stunden ist nicht vorbereitet, im Krisenfall geht so wertvolle Zeit verloren.
4. **Anmeldesicherheit mit Lücken**
   Die Zwei-Faktor-Anmeldung deckt nur 72 Prozent der Konten ab, veraltete Anmeldeverfahren sind noch aktiv und es gibt zu viele Administratorrechte. Das sind bevorzugte Einfallstore für Angreifer.

Haftungsfokus: Es geht um die persönliche Verantwortung der Leitung

NIS2 macht die Geschäftsführung **persönlich verantwortlich**. Die Leitung muss die Sicherheitsmaßnahmen genehmigen, ihre Umsetzung überwachen und selbst geschult sein. Diese Pflicht ist nicht an die IT oder einen Dienstleister delegierbar. Wird sie verletzt, drohen Bußgelder und im Schadensfall die persönliche Inanspruchnahme der Leitung. Bei der Muster GmbH ist dieser Bereich aktuell der schwächste Punkt.

Unsere Handlungsempfehlung

Starten Sie mit den Sofortmaßnahmen aus der Roadmap (Seite 7): verantwortliche Person benennen, Leitung schulen, Microsoft-365-Backup einrichten, Zwei-Faktor-Anmeldung verpflichtend ausrollen und einen Notfallplan erstellen. Schon damit verlässt die Muster GmbH den roten Bereich und senkt ihr Haftungsrisiko spürbar.

WIE DIESER REPORT ENTSTEHT

Methodik

Der NIS2 Readiness Report kombiniert zwei Perspektiven: was Ihre Organisation geregelt hat und was Ihre Technik tatsächlich zeigt. So entsteht ein ehrliches Gesamtbild statt einer reinen Selbsteinschätzung.

1

Organisatorischer Self-Check

Ein strukturierter Fragebogen mit **30 Fragen in 11 Themenfeldern**, ausgerichtet an den Sicherheitspflichten der NIS2-Richtlinie. Beantwortet von Geschäftsführung und IT-Verantwortlichen, in verständlicher Sprache ohne Fachjargon.

- Antwortskala: Ja / Teilweise / Nein
- Fokus auf Prozesse, Verantwortung, Dokumentation
- Auswertung je Themenfeld als Prozentwert

2

Technischer Read-only-Scan

Eine **rein lesende** Auswertung Ihrer Microsoft-365-Umgebung. Wir lesen ausschließlich **Konfiguration und Metadaten** aus, niemals Inhalte wie E-Mails, Dateien oder Chats.

- Keine Software-Installation, keine Änderung am System
- Konfiguration zu MFA, Anmeldung, Freigaben, Admin-Rollen
- Indikatoren zu Update-Stand und Backup-Status

Vom Rohbefund zur Ampel

1 **Erheben.** Self-Check-Antworten und technische Konfigurationsdaten werden zusammengeführt. Antworten ergeben Punkte (Ja = 2, Teilweise = 1, Nein = 0).

2 **Bewerten.** Je Themenfeld wird der Anteil erreichter Punkte an den möglichen Punkten berechnet und als Prozentwert dargestellt. Technische Befunde fließen in die zugehörigen Themenfelder ein.

3 **Einordnen.** Jeder Prozentwert erhält eine Ampelfarbe. Der Gesamt-Reifegrad ist der Mittelwert über alle bewerteten Themenfelder.

4 **Priorisieren.** Aus den Lücken leiten wir eine konkrete Maßnahmen-Roadmap ab, sortiert nach Aufwand und Wirkung.

Die Ampel-Logik

Ampel	Wertebereich	Bedeutung
◆ Kritisch	0 - 39 %	Wesentliche Anforderungen sind nicht erfüllt. Hier besteht akuter Handlungsbedarf.
■ Grundlegend	40 - 70 %	Grundlagen sind vorhanden, aber es bestehen relevante Lücken, die geschlossen werden sollten.
● Gut	71 - 100 %	Das Themenfeld ist solide aufgestellt. Es bleibt im Wesentlichen, den Stand zu halten.

Datenschutz und Sicherheit beim Scan

Der technische Scan erfolgt über die offiziellen, abgesicherten Microsoft-Schnittstellen mit eng begrenzten Leserechten. Es werden keine Postfach-, Datei- oder Chat-Inhalte gelesen, kopiert oder gespeichert. Nach Erstellung des Reports werden die ausgelesenen Konfigurationsdaten gemäß Vereinbarung wieder gelöscht.

ERGEBNIS IM ÜBERBLICK

Reifegrad je NIS2-Themenfeld

NIS2 wird in elf Themenfeldern bewertet. Die Übersicht zeigt je Feld den Reifegrad als Balken, die Ampel und eine kurze Einordnung.

#	NIS2-Themenfeld	Reifegrad	Ampel	Einordnung in einem Satz
1	Governance & Leitungspflichten	25%	Kritisch	Verantwortung nicht verankert, Leitung nicht geschult.
2	Risikoanalyse & Sicherheitsrichtlinien	33%	Kritisch	Keine schriftliche, beschlossene Sicherheitsrichtlinie vorhanden.
3	Umgang mit Sicherheitsvorfällen	33%	Kritisch	Kein Notfallplan, Meldefristen ans BSI nicht vorbereitet.
4	Notbetrieb, Backup & Krisenmanagement	25%	Kritisch	Kein eigenes Microsoft-365-Backup, kein getesteter Notbetrieb.
5	Sicherheit bei Lieferanten & Dienstleistern	50%	Grundlegend	Wichtige Dienstleister bekannt, aber vertraglich nicht abgesichert.
6	Sichere Beschaffung & Updates	50%	Grundlegend	Updates laufen, aber ohne feste Regeln und Fristen.
7	Kontrolle der Wirksamkeit	25%	Kritisch	Wirksamkeit der Maßnahmen wird nicht überprüft oder gemessen.
8	Schulung & gesundes IT-Verhalten	50%	Grundlegend	Erste Schulungen vorhanden, aber unregelmäßig und ohne Phishing-Tests.
9	Verschlüsselung	50%	Grundlegend	Verschlüsselung teils im Einsatz, aber ohne verbindliche Regelung.
10	Personal, Zugriffe & Geräte	67%	Grundlegend	Prozesse vorhanden, aber Berechtigungen werden selten überprüft.
11	Anmeldung & sichere Kommunikation	75%	Gut	Zwei-Faktor-Vorgabe vorhanden, technische Restlücken bleiben.

Kritisch (0 - 39 %) Grundlegend (40 - 70 %) Gut (71 - 100 %)

Vier Felder liegen im roten Bereich, sie betreffen vor allem Governance, Notfall und Backup. Fünf Felder sind grundlegend aufgestellt, zwei bereits gut. Die Roadmap ab Seite 7 setzt zuerst an den roten Feldern an.

AUSZUG AUS DEN DETAILBEFUNDEN

Detailbefunde der kritischen Felder

Für die Felder mit dem größten Handlungsbedarf zeigen wir hier die konkreten Befunde aus Self-Check (organisatorisch) und Scan (technisch).

1 · Governance & Leitungspflichten

◆ 25 %

ORGANISATORISCH (SELF-CHECK)

- Keine namentlich **verantwortliche Person** für Informationssicherheit benannt.
- Keine **Cyber-Schulung der Geschäftsführung** dokumentiert.
- IT-Sicherheit ist **kein fester Punkt** in der Geschäftsführungs-Runde.
- Betroffenheit durch NIS2 und BSI-Registrierungspflicht noch ungeklärt.

TECHNISCH (SCAN)

- **5 globale Administratoren** aktiv, üblich wären 2 bis 3.
- Für Administratoren ist **kein gesondertes Notfallkonto** hinterlegt.
- Aktivitäten privilegierter Konten werden **nicht regelmäßig ausgewertet**.

Warum kritisch: Dies ist der Haftungsblock. NIS2 verlangt, dass die Leitung Maßnahmen genehmigt, überwacht und selbst geschult ist. Diese Pflicht ist nicht delegierbar und aktuell nicht erfüllt.

4 · Notbetrieb, Backup & Krisenmanagement

◆ 25 %

ORGANISATORISCH (SELF-CHECK)

- Kein Plan für den **Notbetrieb** bei längerem IT-Ausfall.
- Wiederherstellung von Daten wurde im letzten Jahr **nicht getestet**.
- Kein **Plan B** für Kommunikation, falls Microsoft 365 ausfällt.

TECHNISCH (SCAN)

- **Kein dediziertes Microsoft-365-Backup** erkennbar (Mail, OneDrive, SharePoint, Teams).
- Papierkorb-Aufbewahrung auf **Standardwerten**, kein Schutz vor Löschung.
- Keine unveränderliche Sicherung gegen Ransomware vorhanden.

Warum kritisch: Microsoft sichert Ihre Inhalte nicht dauerhaft. Ohne eigenes Backup können Daten nach Ransomware oder Löschung endgültig verloren sein. Das ist die häufigste und teuerste Lücke im Mittelstand.

11 · Anmeldung & sichere Kommunikation

● 75 %

ORGANISATORISCH (SELF-CHECK)

- Verbindliche **Zwei-Faktor-Vorgabe** ist beschlossen und kommuniziert.
- Sichere Wege für **Notfallkommunikation** sind nur teilweise definiert.

TECHNISCH (SCAN)

- **MFA-Abdeckung 72 %**, Lücken vor allem bei **Dienst- und Funktionskonten**.
- **Legacy-Authentifizierung noch aktiv** (z. B. ältere Mailprotokolle).
- Conditional-Access-Richtlinien vorhanden, aber **unvollständig** (Lücken bei Gastkonten).

Naheliegender Hebel: Trotz grüner Ampel bleiben technische Restlücken. Werden Dienstkonten in die MFA aufgenommen und veraltete Anmeldeverfahren abgeschaltet, steigt die Sicherheit hier deutlich.

AUSZUG AUS DEN DETAILBEFUNDEN (FORTSETZUNG)

Weitere ausgewählte Befunde

3 · Umgang mit Sicherheitsvorfällen

◆ 33 %

ORGANISATORISCH (SELF-CHECK)

- **Kein dokumentierter Incident-Plan** (wer macht im Ernstfall was).
- Meldepflicht ans BSI binnen **24 / 72 Stunden** nicht bekannt und nicht vorbereitet.
- Notfall wurde im letzten Jahr **nie durchgespielt**.

TECHNISCH (SCAN)

- Erweiterte **Protokollierung nur teilweise** aktiviert.
- Keine zentralen **Warnregeln** für verdächtige Anmeldungen konfiguriert.
- Aufbewahrungsdauer der Anmeldeprotokolle auf Standard begrenzt.

Warum kritisch: Ohne Plan und ohne Kenntnis der Meldefristen drohen im Ernstfall Zeitverlust und zusätzlich ein Verstoß gegen die gesetzliche Meldepflicht.

5 · Sicherheit bei Lieferanten & Dienstleistern

■ 50 %

ORGANISATORISCH (SELF-CHECK)

- Kritische Dienstleister sind grob bekannt, aber **nicht in einer Liste erfasst**.
- Verträge enthalten **keine verbindlichen Sicherheitsanforderungen**.
- Keine Pflicht der Dienstleister, eigene Vorfälle zu melden.

TECHNISCH (SCAN)

- **Externe Freigaben unbeschränkt**: Teilen mit beliebigen externen Adressen möglich.
- Mehrere **Drittanbieter-Apps** mit weitreichenden Berechtigungen verbunden.
- Gastkonten ohne **Ablaufdatum** und ohne regelmäßige Prüfung.

Hebel: Angriffe laufen oft über Dienstleister und zu weit geöffnete Freigaben. Eine Lieferantenliste plus Begrenzung externer Freigaben senkt das Risiko schnell.

8 · Schulung & gesundes IT-Verhalten

■ 50 %

ORGANISATORISCH (SELF-CHECK)

- Schulungen finden statt, aber **nicht regelmäßig** und nicht für alle.
- **Keine simulierten Phishing-Tests** im Einsatz.
- Einfache Verhaltensregeln existieren, sind aber **nicht schriftlich** festgehalten.

TECHNISCH (SCAN)

- Phishing- und Schadsoftware-Schutz **aktiv**, aber nicht auf empfohlenem Niveau.
- **Keine Auswertung** zu Schulungsabdeckung im System hinterlegt.

Hebel: Regelmäßige Kurzschulungen und Phishing-Simulationen gehören zu den wirksamsten Maßnahmen überhaupt und sind günstig umzusetzen.

WAS ZUERST, WAS DANACH

Priorisierte Maßnahmen-Roadmap

Wir trennen Sofortmaßnahmen mit hoher Wirkung bei geringem Aufwand von strategischen Maßnahmen, die mehr Zeit brauchen. So bringen Sie zuerst die größten Risiken aus dem roten Bereich.

Quick Wins · sofort, geringer Aufwand, hohe Wirkung

#	Maßnahme	Aufwand	Wirkung	Feld
1	**Verantwortliche Person** für Informationssicherheit benennen (intern oder extern).	Gering	Hoch	1
2	**Geschäftsführung schulen** (halbtägiger Cyber-Workshop) und dokumentieren.	Gering	Hoch	1
3	**Microsoft-365-Backup** einrichten (Mail, OneDrive, SharePoint, Teams).	Mittel	Hoch	4
4	**MFA verpflichtend** ausrollen, Dienstkonten einschließen, Legacy-Auth abschalten.	Mittel	Hoch	11
5	**Einseitiger Notfallplan** inkl. BSI-Meldefristen (24 / 72 h) und Kontaktliste.	Gering	Hoch	3
6	**Externe Freigaben begrenzen** und Gastkonten mit Ablaufdatum versehen.	Gering	Mittel	5

Strategische Maßnahmen · mittelfristig, höherer Aufwand, nachhaltige Wirkung

#	Maßnahme	Aufwand	Wirkung	Feld
7	**Schriftliche IT-Sicherheitsrichtlinie** erstellen und von der Leitung beschließen lassen.	Mittel	Hoch	2
8	**Jährliche Risikoanalyse** einführen, inklusive Maßnahmenliste mit Verantwortlichen.	Mittel	Mittel	2
9	**Lieferanten-Governance**: kritische Dienstleister listen, Sicherheits- und Meldeklauseln vereinbaren.	Mittel	Mittel	5
10	**Schulungsprogramm** mit jährlichen Pflichtschulungen und Phishing-Simulationen aufsetzen.	Mittel	Hoch	8
11	**Patch- und Update-Regeln** festlegen (Fristen) und Wirksamkeit regelmäßig prüfen.	Mittel	Mittel	6 / 7
12	**Notfallplan testen** und Wiederherstellung aus dem Backup mindestens jährlich üben.	Mittel	Hoch	3 / 4

Erwartete Wirkung

Allein mit den sechs Quick Wins verlassen die vier roten Felder voraussichtlich den kritischen Bereich. Der Gesamt-Reifegrad steigt nach Erfahrung aus vergleichbaren Projekten von rund 44 auf über 65 Prozent, noch bevor die strategischen Maßnahmen abgeschlossen sind.

READ-ONLY-SCAN DER MICROSOFT-365-UMGEBUNG

Technischer Scan · Beispiel-Auszug

Diese Kennzahlen liefert der technische Scan typischerweise. Alle Werte stammen aus Konfiguration und Metadaten, nicht aus Inhalten. Die folgenden Zahlen sind beispielhaft für die Muster GmbH.

MFA-Abdeckung

Lücken

72 %

28 % der Konten ohne zweiten Faktor, vor allem Dienst- und Funktionskonten.

Legacy-Authentifizierung

Aktiv

aktiv

Veraltete Anmeldeverfahren noch zugelassen. Diese umgehen die Zwei-Faktor-Pflicht.

Externe Freigaben

Unbeschränkt

offen

Teilen mit beliebigen externen Adressen möglich, ohne Ablauf oder Freigabeschranke.

Globale Administratoren

Zu viele

5

Empfehlung: 2 bis 3 globale Admins, mit gesondertem Notfallkonto und MFA.

Conditional Access

Unvollständig

teilweise

Grundrichtlinien vorhanden, aber Lücken bei Gastkonten und Altprotokollen.

Update- / Patch-Indikator

Uneinheitlich

~ 80 %

Rund 80 % der Clients auf aktuellem Stand, einzelne Geräte deutlich zurück.

Microsoft-365-Backup

Nicht erkannt

fehlt

Kein dediziertes Backup für Mail, OneDrive, SharePoint und Teams erkennbar.

Schadsoftware- / Phishing-Schutz

Aktiv

aktiv

Schutzfunktionen aktiv, Feineinstellungen noch unter dem empfohlenen Niveau.

Lesehinweis: Die Ampel je Kennzahl bezieht sich auf den jeweiligen technischen Einzelbefund und kann von der Gesamt-Ampel des zugehörigen Themenfelds abweichen, da dort auch organisatorische Antworten einfließen. Alle Werte sind fiktive Beispielwerte zur Veranschaulichung.

SO GEHT ES WEITER

Nächste Schritte & Kontakt

Dieser Musterbericht zeigt, was Sie nach Self-Check und Scan erhalten: ein klares Bild, konkrete Befunde und eine priorisierte Roadmap. Für Ihr eigenes Unternehmen ist der Weg dorthin kurz.

Ihr NIS2 Readiness Report zum Festpreis

Self-Check ausfüllen, Read-only-Scan freigeben, fertigen Report erhalten. Planbar, schnell und ohne Verpflichtung zu Folgeleistungen.

Fester Komplettpreis · transparent · Report in der Regel wenige Werktage nach Scan-Freigabe

- ✓ Geführter Self-Check (30 Fragen, 11 Themenfelder)
- ✓ Technischer Read-only-Scan Ihrer M365-Umgebung
- ✓ Auswertung je Themenfeld mit Ampel und Prozentwert
- ✓ Konkrete Detailbefunde organisatorisch und technisch
- ✓ Priorisierte Maßnahmen-Roadmap mit Quick Wins
- ✓ Verständlich für Geschäftsführung und IT

KONTAKT

cubic solutions GmbH

Ansprechpartner	Simon Scharschinger
Telefon	+49 9181 5183585
E-Mail	briefkasten@cubicsolutions.de
Web	www.cubicsolutions.de
Anschrift	Ringstraße 1, 92318 Neumarkt i.d.OPf.

In drei Schritten zu Ihrem Report

1. **Self-Check starten.** Den kostenlosen Online-Check ausfüllen, dauert nur wenige Minuten und liefert sofort einen ersten Eindruck.
2. **Scan freigeben.** Die rein lesende Verbindung zu Ihrem Microsoft 365 einmalig autorisieren. Keine Installation, kein Eingriff.
3. **Report erhalten.** Sie bekommen Ihren individuellen NIS2 Readiness Report wie diesen, mit Befunden und priorisierter Roadmap.