Automazing Works

SICHERHEITSREIFEGRAD · MANAGEMENT-KURZFASSUNG

Reifegrad 1,9 von 4 — Basis erreicht, Pflicht nicht.

Hartmann Anlagenbau GmbH & Co. KG · Konzern-Reifegrad nach NIST CSF 2.0

BEWERTUNGSZEITRAUM	BERICHTSSTAND	METHODIK	ADRESSAT
Mai 2026	**2026-06-17**	**NIST CSF 2.0 · CIS v8.1 · NIS-2**	**Geschäftsführung · IT-Leitung**

Vorschlagsdokument auf Basis von Selbstauskünften. Ersetzt weder Audit nach ISO/IEC 27001 oder BSI IT-Grundschutz noch Penetrationstest oder verbindliche NIS-2-Compliance-Bewertung.

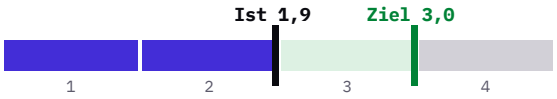
Basis erreicht, Pflicht offen — Erwartungswert ~2,1 Mio. €/Jahr, das schlechte Jahr ~8,6 Mio. €.

Die drei Zahlen, die heute zählen

REIFEGRAD HEUTE

1,9 / 4

Basis erreicht · gewichtet 1,88 / 4



RISIKO IN EURO (FAIR)

≈ 2,1 Mio. €

Erwartungswert/Jahr · Maßnahmen → ROI ≈ 13×

NIS-2 · BUSSGELDRISIKO

bis 7 Mio. €

Wichtige einrichtung nach BSIG-neu §28

Einstufung: wichtige Einrichtung (wE)

Registrierung 76 Tage überfällig

Rahmen: 7 Mio. € oder 1,4 % Umsatz

Quelle: Report § 2.1 · § 3.1 · § 4.3 (FAIR)

Drei Lücken halten den Risikoanker — alle drei sind NIS-2-pflichtige Bereiche.

Identity · Data Protection · Modern Connectivity

IDENTITY & ACCESS MANAGEMENT

Identitäten nicht durchgängig geschützt.

2,0 / 4 · Basis

- MFA fehlt für privilegierte/Admin-Konten, VPN und Backup-Konsole.
- Berechtigungen werden vergeben, aber nicht systematisch rezertifiziert.
- Gated Scoring: Mindestanker MFA für privilegierte Konten verletzt.

Report § 5.3 · NIS-2 §30 Nr. 9/10 · Versich.-Kontrolle 1

DATA PROTECTION, BACKUP & RECOVERY

Wiederherstellung ungetestet.

2,0 / 4 · Basis

- Kein geplanter Restore-Test — Wiederanlauf im Ernstfall unbelegt.
- Kein Immutability-Mechanismus · Backup-Konsole löschbar.
- RTO/RPO ohne abgestimmte Zielwerte je System.

Report § 5.6 · NIS-2 §30 Nr. 3 · Versich.-Kontrolle 3

MODERN CONNECTIVITY & CLOUD SECURITY

Netz nicht durchgesetzt segmentiert.

2,0 / 4 · Basis

- Grobe VLAN-Trennung ohne durchgesetzte Filter dazwischen.
- Server/Anwendungen erreichen sich untereinander ohne Mikrosegmentierung.
- Gated Scoring: flaches Netz an einem Standort verletzt Mindestanker.

Report § 5.5 · NIS-2 §30 Nr. 8/10

Quelle: Report § 5.8 · § 5.9 · § 5.11

Handeln kostet 700–950 T€ über 12 Monate — Nicht-Handeln mehr.

Investition vs. Erwartungsschaden · drei Beschluss-Themen

Handeln

12-Monats-Programm · NIS-2-konform · versicherbar

Sofort (0–8 W)	**55–110 T€**
90-Tage-Plan	**200–300 T€**
6–12-Monats-Pfad	**450–750 T€**
Gesamt 12 Monate	**700–950 T€**

Nicht-Handeln

Ohne Aktion · jährlicher Erwartungsschaden

Bußgeldrahmen NIS-2 wE	**bis 7 Mio. €**
Ransomware-Erwartungsschaden	**2–8 Mio. € Median**
Cyber-Versicherung	**+30–80 % Prämie**
Erwartungswert / Jahr schlechtes Jahr (P90) ≈ 8,6 Mio. €	**≈ 2,1 Mio. €**

BESCHLUSS 1
Drei Sofortmaßnahmen freigeben — MFA, Backup-Immutabilität, NIS-2-Registrierung.

BESCHLUSS 2
90-Tage-Plan beauftragen mit Pflicht-Gate W4 und Versicherungs-Gate W8.

BESCHLUSS 3
Informationssicherheits-Verantwortlichen benennen (intern oder vCISO).

Quelle: Report § 8 (Prioritätenplan) · § 4.3 (FAIR) · NIS-2 §28

Vier Termine in den nächsten 14 Tagen — jeder mit dokumentiertem Output.

Operative Termin-Tabelle

Tag	Wer	Was	Output
T + 3 01.06.2026	**Geschäftsführung**	Beschluss-Sitzung: drei Sofortmaßnahmen freigeben, ISB benennen.	**→ Beschluss-Protokoll**
T + 7 05.06.2026	**IT-Leitung**	Detailplan MFA + Restore-Test + MUK-Portal-Registrierung erstellen.	**→ Maßnahmen-Plan v1**
T + 10 08.06.2026	**Geschäftsführung · IT-Leitung**	Cyber-Schulung GF nach NIS-2 Art. 20 durchführen (mind. 90 Min).	**→ Teilnahme-Nachweis**
T + 14 12.06.2026	**Geschäftsführung · IT-Leitung · HR-Leitung**	Tabletop Ransomware mit Krisenteam · Q4-Police-Abgleich mit Makler.	**→ IR-Übungs-Bericht**