Sicher. Digital. Zukunftsfähig.

Cyberrisiken erkennen. Verantwortung übernehmen. Handlungsfähig bleiben.

eccyber

ECCLESIA GRUPPE

SCHUNCK GROUP

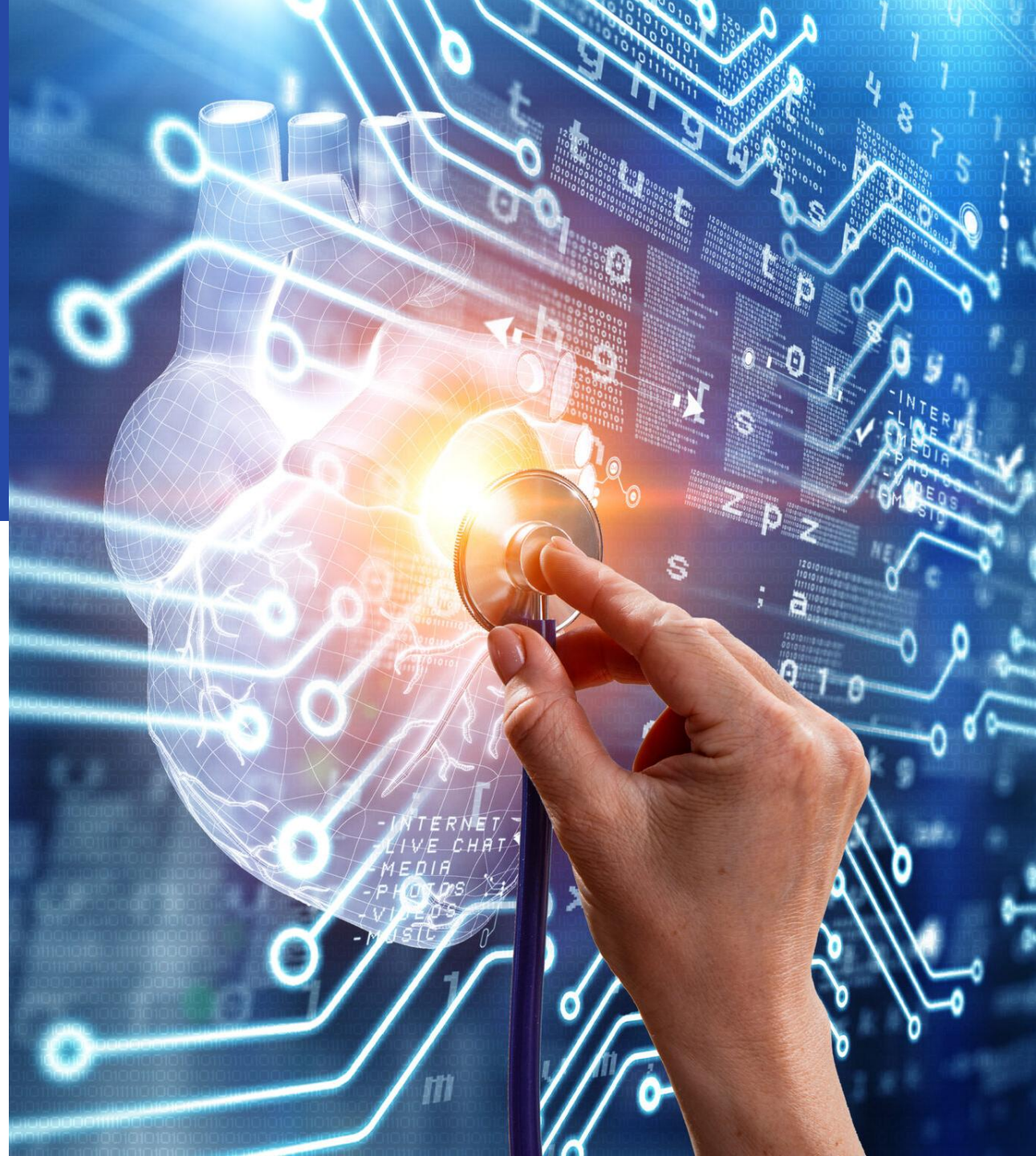
deas ASSEKURANZMAKLER

08. April 2026

ECCLESIA
GRUPPE

RISIKOLAGE – AKTUELLE INFORMATIONEN UND EINSCHÄTZUNGEN

08. April 2026



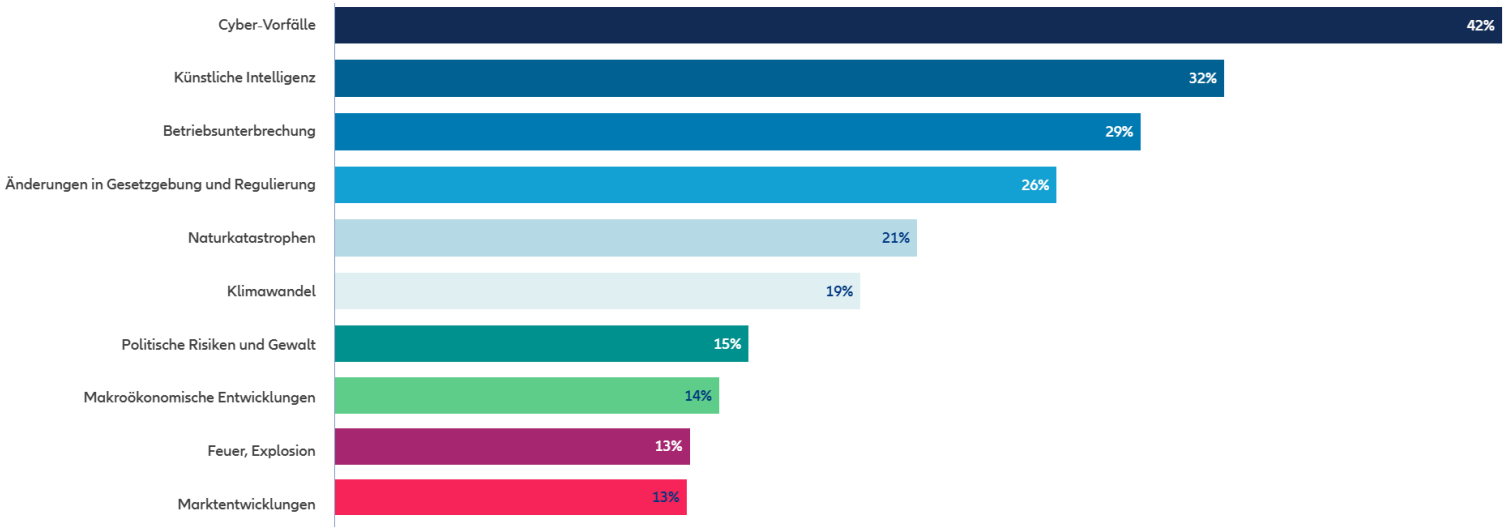
Cybervorfälle und KI in 2026 das Toprisiko

Allianz

Top 10 Geschäftsrisiken weltweit im Jahr 2026

Allianz Risiko Barometer 2026

Basierend auf den Antworten von 3,338 Risikomanagement-Experten aus 97 Ländern und Gebieten (% der Antworten). Die Zahlen ergeben nicht 100%, da jeweils bis zu drei Risiken ausgewählt werden konnten.



Allianz Commercial News & Insights

Quelle: Allianz Commercial

Am 14. Januar 2026 veröffentlichte die Allianz das aktuelle Risk Barometer, und die Ergebnisse könnten kaum einsichtiger sein:

Zum fünften Mal in Folge stehen **Cybervorfälle** wie Datenschutzverletzungen, Ransomware-Angriffe und IT-Ausfälle an der Spitze der größten Geschäftsrisken **weltweit**.

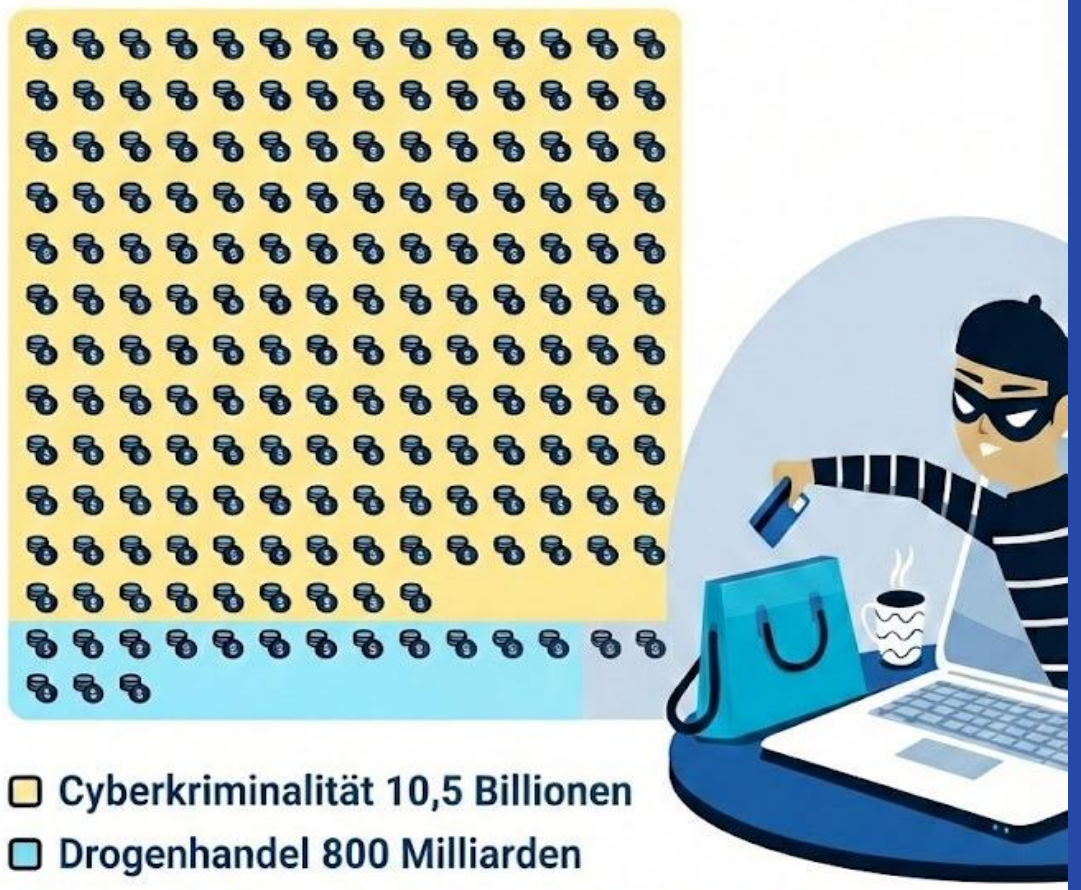
Von Platz 10 auf Platz 2 gesprungen:
Künstliche Intelligenz

Größte Volkswirtschaften (BIP) weltweit Jahr 2025*

- **USA**: 30,6 Billionen USD
- **China**: 19,4 Billionen USD
- **Cyberkriminalität: 10,5 Billionen USD**
- **Deutschland**: 5,1 Billionen USD
- **Österreich: 512 Milliarden USD**

*(Quelle: Statista)

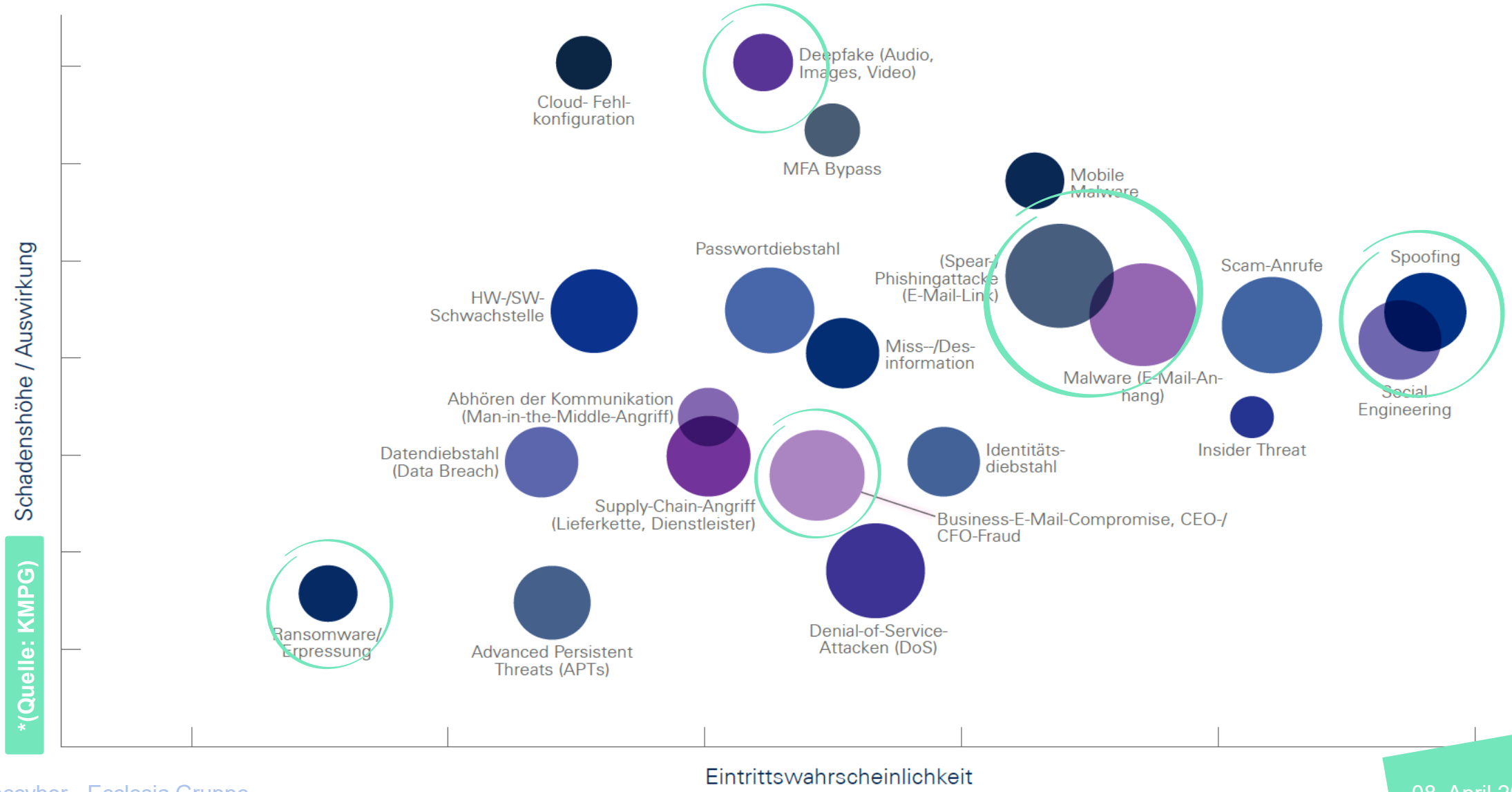
Cyberkriminalität global lukrativste kriminelle Einnahmequelle* 2025



Cyberkriminalität 10,5 Billionen
Drogenhandel 800 Milliarden
Menschenhandel und Prostitution 240 Milliarden

* (2025 in USD. Quellen: Cybersecurity Ventures, UNODC, ILO)

Schadenseintrittswahrscheinlichkeit nach Angriffsarten



*(Quelle: KMPG)

Aktuelle Übersicht Angriffsherkunft 2025

Nicht bekannte Herkunft der Angriffe

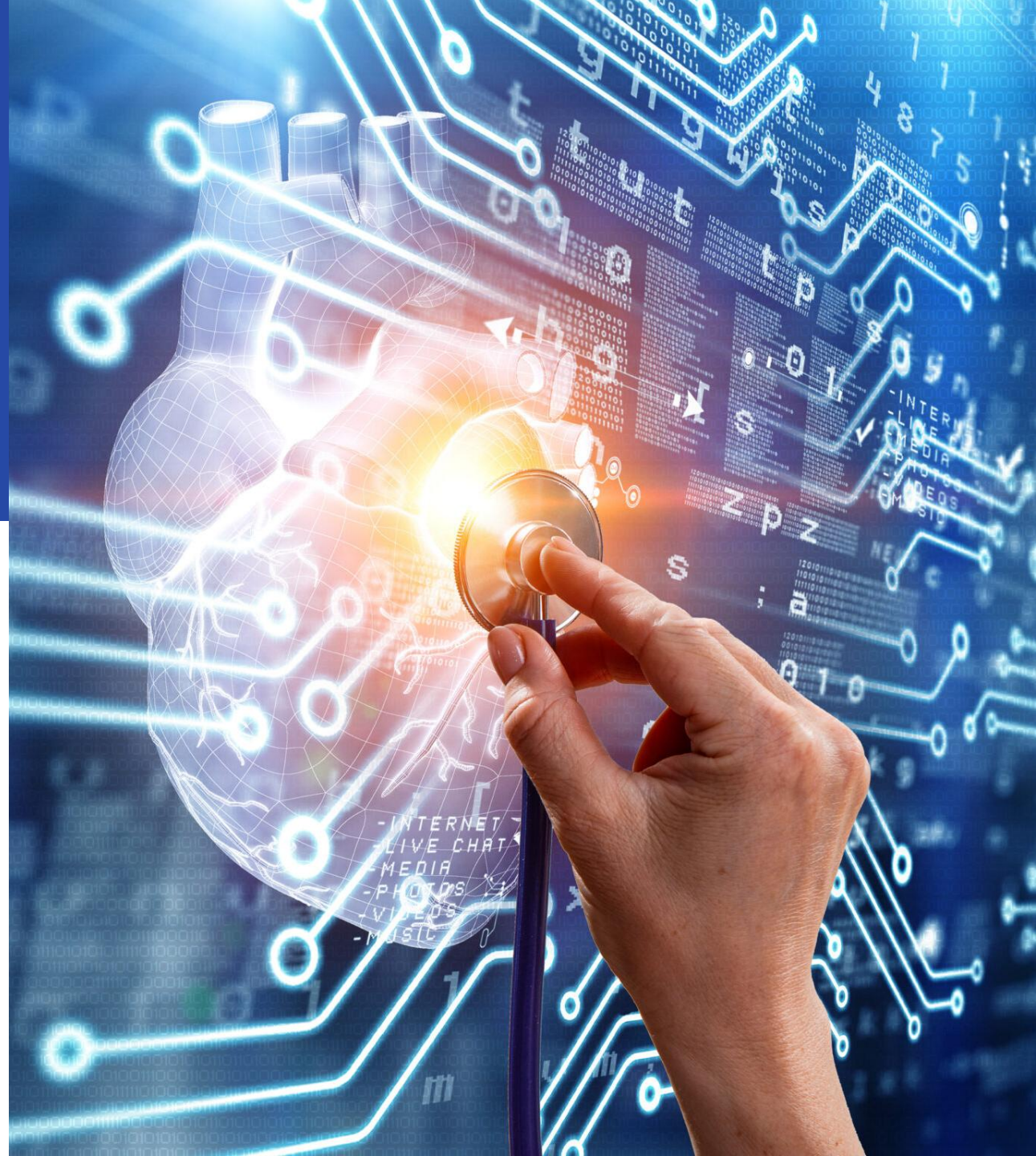
43 %

*(Quelle: KMPG)

ECCLESIA
GRUPPE

REGULATORISCHE ENTWICKLUNGEN NIS-2 (NISG 2026)

08. April 2026



NIS-2 (NISG 2026) –
Bedeutung & Relevanz für Ihr Unternehmen

Zum **Oktober 2026** tritt die **EU-Cybersicherheitsrichtlinie NIS-2 (NISG 2026)** in Österreich verbindlich in Kraft.

NIS-2 (NISG 2026) zielt darauf ab, ein *gemeinsam hohes Niveau der Cybersicherheit in der EU* zu etablieren.

Betroffen sind nicht nur klassische kritische Infrastrukturen, sondern eine breite Palette von Unternehmen aus Gesundheitswesen, Produktion, Transport und weiteren Sektoren.

Gleichzeitig wurden die Pflichten für Unternehmen ausgeweitet: von Risikomanagement über Registrierung bis hin zur Meldung relevanter Sicherheitsvorfälle.

Warum ist NIS-2 (NISG 2026) wichtig?

Regulatorisch verbindlich:
Kein freiwilliger Standard, sondern Gesetz.

Management Verantwortung:
Ihre Führungsebene trägt die Pflicht, Risiken zu verstehen, zu steuern und nachweisbar zu adressieren.

Betroffenheit nach NIS-2 (NISG 2026) – Sektoren & Größenkriterien

Was bedeutet Betroffenheit?

Ein Unternehmen fällt unter die NIS-2 (NISG 2026) - Pflichten, wenn es**:**

In einem relevanten Sektor tätig ist
und
bestimmte Größen/Umsatzschwellen erreicht

Größen- und Umsatz-Schwellen

- **Wichtige Einrichtung:**
  ≥ 50 Mitarbeitende **oder**
  Umsatz > 10 Mio. € und Bilanzsumme > 10 Mio. €
- **Besonders wichtige Einrichtung:**
  ≥ 250 Mitarbeitende **oder**
  Umsatz > 50 Mio. € und Bilanzsumme > 43 Mio. €

Relevante Sektoren (Beispiele)

- Gesundheits-/Sozialwesen (z.B. Krankenhäuser, akutmedizinische Versorgung, ambulante Versorgung)
- Transport & Logistik (z.B. Güterverkehr, Personenverkehr)
- Öffentliche Dienste & Verwaltung
- KRITIS
- …

Wer/Was ist *nicht* betroffen?

- Unternehmen, die nicht in relevanten Sektoren tätig sind
- Unternehmen in relevanten Sektoren, die unter den Schwellenwerten bleiben

Wesentlichen Firsten im NIS-2 (NISG 2026)

01.10.2026

Das NISG 2026 tritt in Kraft; zeitgleich tritt das NISG 2018 außer Kraft.

01.01.2027

Die Registrierung muss erfolgt sein (weitere Informationen folgen)

01.10.2027

Die Selbstdeklaration muss erfolgt sein.

01.10.2028

Die Cybersicherheitsbehörde kann Einrichtungen zur Prüfung auffordern

30.11.2028

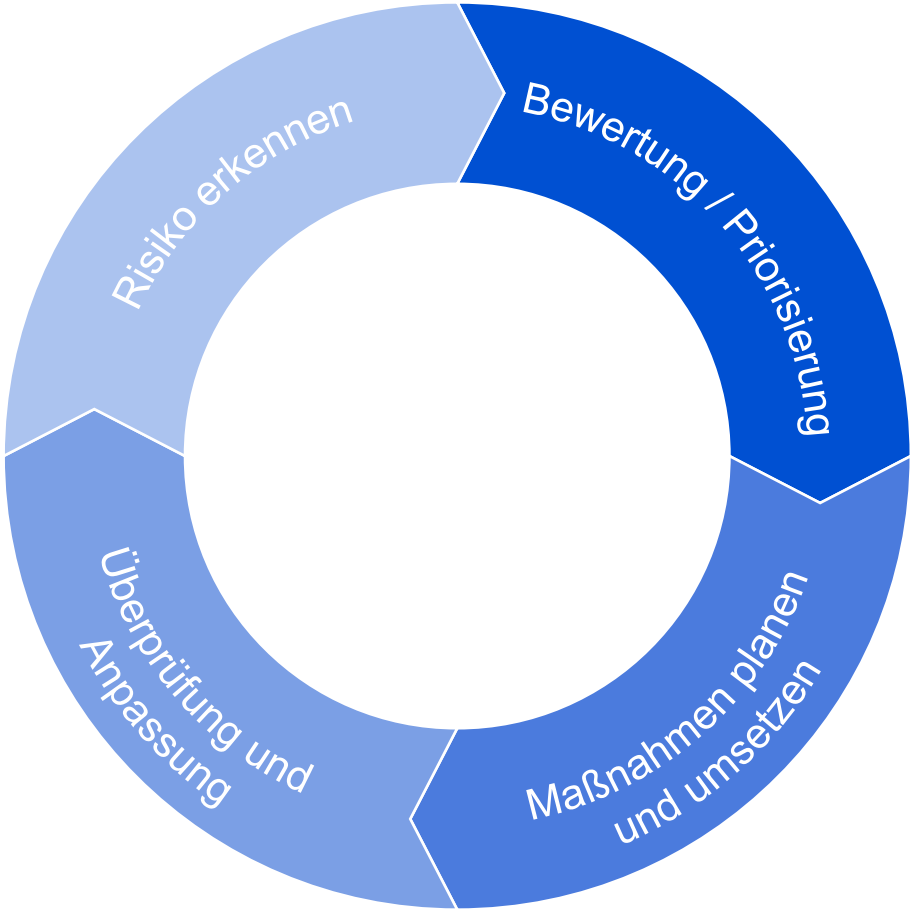
Der früheste Zeitpunkt, zu dem eine Einrichtung nach Aufforderung **die operative und organisatorische Umsetzung der Risikomanagementmaßnahmen** nachweisen muss..

Ab 30.09.2030

Muss ein Prüfbericht durch eine unabhängige Stelle nachgewiesen werden. Dies gilt jeweils nur nach Aufforderung und bei wichtigen Einrichtungen nur bei begründeten Hinweisen.

Risikomanagement nach NIS-2: Basis & Einstieg

Die Richtlinie fordert **angemessene** und **verhältnismäßige** Maßnahmen, die sich an der konkreten Risikosituation, der Größe des Unternehmens und den erwarteten Auswirkungen eines Vorfalls orientieren.



Takeaways

- **Verhältnismäßigkeit**

Maßnahmen müssen zum Risiko, zur Unternehmensgröße und zur Bedeutung für den Geschäftsbetrieb passen

- **Pragmatischer** Start

Beginnen Sie mit den wichtigsten Risiken und bauen Sie den Schutz strukturiert aus

- **Nachweisführung**

Dokumentation und regelmäßige Überprüfung sind Pflicht, auch bei „Low-Level-Maßnahmen“

- **Nicht alles sofort, sondern systematisch**

Ein stufenweiser Ansatz erzeugt Compliance-Nachweise, bevor komplexe Controls vollständig implementiert sind

Risikomanagement nach NIS-2: Grundprinzip & Ziele

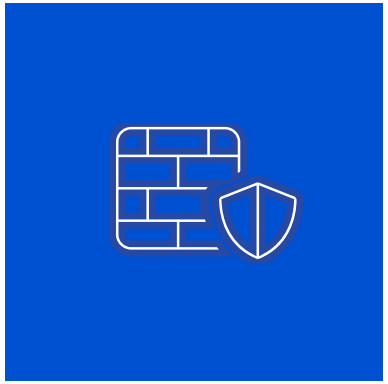
Ein wirksames Risikomanagement ist zentraler Pflichtbestandteil von NIS-2. Es sorgt dafür, dass Risiken systematisch identifiziert, bewertet, gesteuert und überprüft werden. Grundlage für Compliance, Resilienz und sichere Betriebsfähigkeit.

Risikoanalyse & Bewertung

- Bestimmung relevanter Assets, Dienste, Prozesse
- Risikoidentifikation (Bedrohungen/Schwachstellen)
- Bewertung nach Eintrittswahrscheinlichkeit & Auswirkung
- Grundlage für Maßnahmen Priorisierung

Sicherheitsvorfall & Notfallplanung

- Incident-Response-Prozesse
- Wiederherstellungs- und BCM-Pläne
- Kommunikationswege & Eskalationsmatrix
- Tests & Simulationen



Technische & organisatorische Maßnahmen

- Zugangskontrollen (zB MFA)
- Monitoring & Logging
- Verschlüsselung, Patchmanagement
- Dokumentierte Richtlinien und Prozesse

Überprüfung & Verbesserung

- Regelmäßige Prüfungen (Audits, Tests)
- KPI-Messung & Reporting
- Lessons Learned & Anpassungen
- Dokumentation für Nachweis & Audit

Zentrale Pflichten nach NIS-2 (NISG 2026)

1

Registrierung der Unternehmen

Unternehmen müssen sich beim offiziell registrieren.
Grundvoraussetzung dafür, dass Sie als regulierte Organisation geführt werden.

Wesentliche Punkte:
- Erfassung der Betroffenheit
- Zuordnung zu Kategorie „wesentlich“ oder „wichtig“
- Grundlage für spätere Meldeprozesse

2

Meldepflichten für Vorfälle

Relevante Sicherheitsvorfälle sind innerhalb klar definierter Fristen an **CSIRT** anzuzeigen. Dies dient der Situationsfrühwarnung und ermöglicht Risiken frühzeitig zu erkennen und zu koordinieren.

Fristenbeispiele:

- 24h – Erstmeldung
- 72h – aktualisierte Meldung
- ~30 Tage - Abschlussbericht

3

Risikomanagementsystem

Kern der Pflichten ist der Aufbau eines dokumentierten RMS, das Risiken identifiziert, bewertet und steuert. Einbindung der Geschäftsleitung.

Inhaltliche Schwerpunkte:
- Risikoanalyse & Dokumentation
- Technische/organisatorische Sicherheitsmaßnahmen
- Dritt/Lieferantenrisiken

Geschäftsleitung: Verantwortung & Konsequenzen

Geschäftsleitung haftet persönlich

Cybersicherheit ist Managementaufgabe.
Die Verantwortung für Informations- und IT-Sicherheit liegt bei der Geschäftsleitung/den Leitungsorganen, nicht nur bei der IT.

→ **Entscheidungen müssen getroffen, Ressourcen bewilligt und Prozesse *überwacht* werden.**

Konsequenzen bei fehlender Sorgfalt:

- **Persönliche Haftung** von Geschäftsführern/Vorständen
- **Rechtliche Risiken** bei Pflichtverletzung
- Reputations- und Insolvenzrisiken bei großen Vorfällen

Cybersicherheit kann nicht „delegiert werden“ – sie muss *gesteuert, kontrolliert und dokumentiert* werden.

Finanzielle & regulatorische Risiken

- Bußgelder bis zu **7 Mio. € oder 1,4% des globalen Umsatzes** bei Verstößen gegen Pflichtanforderungen
- Nachweis der Prüfung durch eine unabhängige Stelle auf Aufforderung (frühestens ab 01.10.2028);
- Frist 2 Jahre ab Aufforderung für technischen Nachweis; Frist 2 Monate für operativen und organisatorischen Nachweis
- Verantwortungs- und Schadenersatzpflichten gegenüber der Gesellschaft oder Dritten möglich

- die ohnehin schon scharfe Haftung des Managements nimmt angesichts der Bedrohungslage weiter zu
- zunehmende Anforderungen an das Cyber-Risikomanagement führen zu erhöhtem Qualifikationsbedarf
- zunehmende Pflichten des Managements im Bereich Cyber engen unternehmerische Handlungs- und Ermessensspielräume zunehmend ein

ECCLESIA
GRUPPE

ECCLESIA CYBER

WELCHEN MEHRWERT BIETET EINE CYBERDECKUNG

08. April 2026

Risikotransfer

Welche Bausteine einer Cyberversicherung gibt es?

Eigenschaden

Cyberdiebstahl, Cyberbetrug

Sachschäden an der IT-Hardware

Erpressung

Betriebsunterbrechung

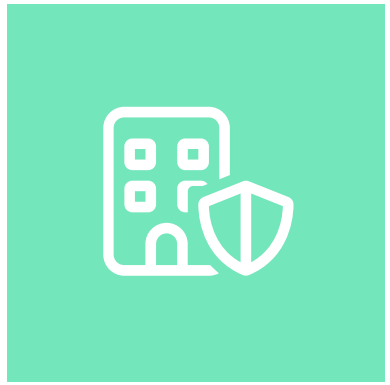
Drittschaden

Vertragsstrafen

Reputationsmanagement

Kosten bei Datenschutzverletzungen

Haftpflichtdeckung



Assistance Dienstleistungen

Soforthilfe im Cybervorfall

Kosten für Forensik

Kosten für Wiederherstellung

Leistungsübersicht einer Cyberversicherung

Ganzheitlicher Schutz für Unternehmen gegen die vielfältigen Risiken der digitalen Welt.
Die Deckungen umfassen sechs zentrale Leistungsbereiche, die speziell auf die Risiko-Anforderungen abgestimmt sind.

Cyber-Eigenschaden

Inklusive 24/7-Soforthilfe im Notfall

Betriebsunterbrechung

Absicherung finanzieller Verluste bei Umsatz- / Betriebsunterbrechung

Cyber-Erpressung

Schutz bei Lösegeldforderungen und professionelle Verhandlungsführung

Cyber-Diebstahl

Deckung von Vertrauensschäden durch digitalen Betrug und Datendiebstahl

Cyber-Haftpflicht

Umfassender Haftpflichtschutz inklusive Rechtsschutz

Cyber-Prävention

Proaktive Maßnahmen zur Risikominimierung und Mitarbeiterschulung

Nutzen einer Cyberversicherung

Schutz weit über IT-Schäden hinaus

✅ **1. Absicherung bei Betriebsunterbrechung**

- Entschädigung für **Umsatzausfälle** durch IT-Ausfälle (z. B. nach Ransomware-Angriffen, DDoS Angriffen, etc.)
- Übernahme von **Wiederherstellungskosten** für Systeme, Daten und Hardware
- Unterstützung bei der **schnellen Wiederaufnahme des Betriebes**

✅ **2. Schutz bei Reputationsschäden**

- Kostenübernahme für **Krisenkommunikation & PR-Maßnahmen**
- Unterstützung durch **Spezialisten für Reputationsmanagement**
- Vermeidung von **Vertrauensverlust bei Patienten und Partnern**

✅ **3. Weitere Vorteile**

- Zugang zu **IT-Forensikern und Incident-Response-Teams**
- Präventive Leistungen wie **Sicherheitsaudits und Awareness-Trainings**

Fazit:

Eine Cyberversicherung ist für ein Unternehmen nicht nur ein finanzieller Schutz, sondern auch ein **strategisches Instrument** zur **Krisenbewältigung und Imagewahrung**.

Übersicht eccyber Unterstützung

eccyber bietet umfassende Unterstützung im Bereich der Cyberversicherung und IT-Sicherheit.

Durch eine professionelle **Risikoevaluierung** identifizieren unsere Experten potenzielle Bedrohungen und Schwachstellen in Ihren IT-Systemen, um maßgeschneiderte Lösungen zu entwickeln.
Gemeinsam mit spezialisierten Fachbetreuern und Risikomanagern, unterstützen wir unsere Kunden auf dem **Weg zur Versicherbarkeit** und **Lösung der potenziellen Schwachstellen**.
Darüber hinaus gewährleisten wir durch eine **spezialisierte Platzierung der optimalen Versicherungslösung**, dass Sie im Falle eines Cyberangriffs bestens abgesichert sind.
Mit eccyber profitieren Sie von einer **ganzheitlichen und zukunftssicheren Absicherung** gegen digitale Bedrohungen.

Vielen Dank

eccyber

ECCLESIA GRUPPE

SCHUNCK GROUP

deas ASSEKURANZMAKLER

Weitere Informationen unter
www.ecclesia.com