

NIS-2-Richtlinie: ***Ihr strategischer*** ***Wettbewerbsvorteil***

**Sieben Handlungsfelder, ein klarer Fahrplan:
Die neue EU-Richtlinie zur Cybersicherheit –
und was sie für Ihr Unternehmen bedeutet.**

NIS-2 als Chance – früh handeln, sichtbar vorne sein

Was die Zahlen sagen – und was das für Sie bedeutet

Platz 1

Cyberisiko
weltweit –
4 Jahre in Folge¹

¹Allianz Risk Barometer 2026

202 Mrd. €

Schäden jährlich
in Deutschland²

²Bitkom Studie „Wirtschaftsschutz 2025“

+39,5%

Wachstum der
Cyberschäden
in 2 Jahren

81%

der Angriffe ohne
sichtbare Schad-
software

NIS-2 setzt verbindliche Anforderungen – und wer früh handelt, hat einen echten Vorsprung. Der Gesetzgeber kalkuliert mit rund **87.000 €** Einmalaufwand für ein mittleres Unternehmen – überschaubar im Vergleich zu den **50.000 – 500.000 €**, die ein Ransomware-Angriff im Schnitt kostet. Dabei gilt ausdrücklich Verhältnismäßigkeit: Was für Ihr Unternehmen gilt, richtet sich nach Größe und Sektor.

88% der betroffenen Unternehmen stehen noch am Anfang – das ist Ihr Fenster. Als Geschäftsführung tragen Sie dabei persönliche Verantwortung. Wer jetzt handelt, wird für Kunden und Auftraggeber zur verlässlichen Wahl und entscheidet selbst, wie sein Unternehmen wahrgenommen wird.

Betroffenheitsprüfung: Bin ich betroffen?

1 Ist Ihr Unternehmen in einem dieser Bereiche tätig?

- Energie Transport & Verkehr Finanzwesen Gesundheit Wasser Digitale Infrastruktur
- Weltraum Maschinenbau Medizintechnik Chemie Lebensmittel iT-Dienstleistungen
- Abfallbewirtschaftung Post & Kurierdienste Forschung

2 Wie groß ist Ihr Unternehmen?

Mittleres Unternehmen: ≥ 50 Mitarbeitende oder > 10 Mio. € Umsatz/Bilanz

Großes Unternehmen: ≥ 250 Mitarbeitende oder > 50 Mio. € Umsatz und > 43 Mio. € Bilanz

3 Liefern Sie an Unternehmen, die selbst unter NIS-2 fallen?

Kein Sektor-Treffer? Wer Leistungen an betroffene Unternehmen liefert, kann trotzdem **vertraglich zu Nachweisen verpflichtet** werden.

→ Ihr Ergebnis

Sektor ✓ + Größe ✓ = direkt betroffen
Als Geschäftsführung sind Sie nun
persönlich verantwortlich

Unsicher über Ihr Ergebnis?

Nutzen Sie den **NIS-2-Check** auf unserer Website für eine detaillierte Prüfung oder nehmen Sie direkt Kontakt mit uns auf (erste Orientierung, keine Rechtsberatung). Wir beraten Sie gerne.



Sieben Handlungsfelder im Überblick

Was NIS-2 fordert – und was es Ihnen als Geschäftsführer konkret bringt

1 Risikomanagement einführen

- iT-Risiken systematisch erfassen, bewerten, steuern (ISMS nach ISO 27001/BSI iT-Grundschutz)
- Welche Prozesse dürfen wann wie lange ausfallen?

Ihr Nutzen: Sie investieren gezielt – nicht nach Bauchgefühl, sondern nach tatsächlichem Risiko. Kein Geld mehr für Maßnahmen, die nichts bewegen.

2 Technische Schutzmaßnahmen umsetzen

SOFORT UMSETZBAR

- Multi-Faktor-Authentifizierung einführen
- Backup-Strategie erstellen
- Software und Systeme stets aktuell halten
- Netzwerkbereiche voneinander trennen

MITTELFRISTIG

- Intelligente Erkennung von Angriffen auf Endgeräten statt klassischem Virenschutz
- Verschlüsselung sensibler Daten
- Regelmäßige Überprüfung auf Sicherheitslücken
- Zugriffsrechte auf das Nötigste beschränken

LANGFRISTIG

- Automatisierte Angriffserkennung – von NIS-2 explizit gefordert
- Regelmäßige Sicherheitstests durch externe Spezialisten

Ihr Nutzen: Jede umgesetzte Maßnahme senkt messbar Ihr Angriffsrisiko – und verbessert Ihre Konditionen bei der Cyber-Versicherung.

3 Vorfälle erkennen, bewältigen und melden

- Sicherheitsvorfälle systematisch erkennen und bewerten
- Klare Abläufe zur Eindämmung und Analyse
- Meldepflichten: Erstmeldung 24 h · Vollbericht 72 h

Ihr Nutzen: Wer strukturiert reagiert, begrenzt den Schaden – und reduziert Kosten für Notfalldienstleister, Rechtsberatung und Reputationsschäden erheblich.

4 Lieferkette absichern

- Kritische Lieferanten mit iT-Zugang oder Ausfallrisiko identifizieren
- Sicherheitsanforderungen vertraglich verankern
- Zugriffsrechte regelmäßig bewerten und dokumentieren

Ihr Nutzen: Sie schützen sich vor Angriffen über Dritte – und öffnen gleichzeitig Türen bei Großkunden, die NIS-2-Nachweise von ihren Zulieferern fordern.

5 Geschäftskontinuität sicherstellen (BCM)

- iT-Notfallhandbuch mit Wiederanlaufplänen
- Krisenorganisation und Kommunikationswege festlegen
- Regelmäßig üben – vom Planspiel bis zur Vollübung

Ihr Nutzen: Im Ernstfall entscheiden Stunden. Wer einen erprobten Plan hat, ist in Tagen wieder operativ – und hält Vertragsstrafen sowie Lieferverpflichtungen ein.

6 Beim BSI registrieren

- Über Mein Unternehmenskonto via ELSTER



Link
zum BSI

Ihr Nutzen: Ihrer gesetzlichen Meldepflicht nachkommen und Bußgelder vermeiden.

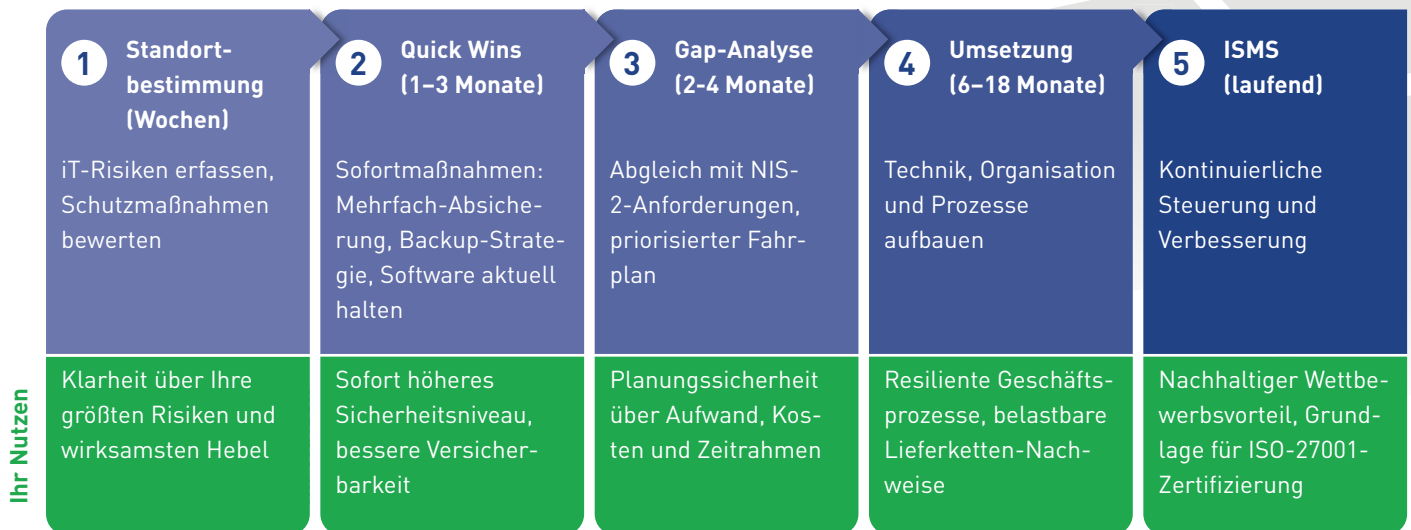
7 Geschäftsleitung schulen

- iT-Sicherheit ist Chefsache – auch nachweislich
- Regelmäßige Schulungen sind verpflichtend

Ihr Nutzen: Wer Verantwortung nachweislich übernimmt und dokumentiert, schützt sich persönlich – und signalisiert Kunden, Partnern und Versicherern: Hier ist jemand, dem man vertrauen kann.

Ihr Weg zur NIS-2-Konformität

Schritt für Schritt – jede Phase bringt eigenständigen Nutzen



Ihr Einstieg: **die Betroffenheitsprüfung**. Bevor Sie planen, brauchen Sie Klarheit. Branche, Unternehmensgröße und Lieferkettenrolle entscheiden – wir zeigen Ihnen in einem kurzen Gespräch, wo Sie stehen.

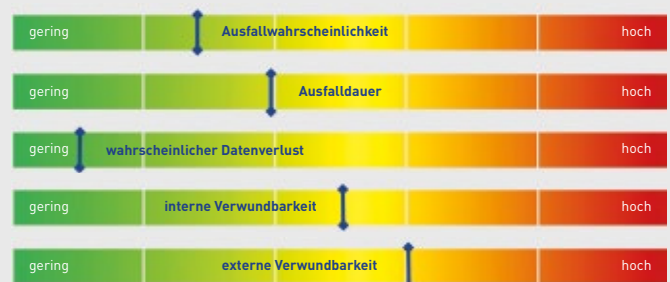
- Erstnachweis gegenüber dem BSI: bis Ende 2028
- Kein Big-Bang-Projekt – jede Phase bringt eigenständigen Nutzen

Ihr Anteil – eine Orientierung

NIS-2 lässt sich aufteilen: Vieles können Sie selbst leisten, für den Rest gibt es Spezialisten. Je nach Ausgangslage übernehmen Sie **20 - 70 %** selbst. Die Standortbestimmung zeigt präzise, wo Sie aktuell stehen und welche Aufgaben bei Ihnen liegen.

Ihr Einstieg: das RIT® iT-Risk-Assessment

Unser Werkzeug für die Standortbestimmung: **das RIT® iT-Risk Assessment (iTRA)** – seit über 20 Jahren im Mittelstand erprobt, ausgezeichnet mit dem Label „Cybersecurity Made in Europe“. In wenigen Wochen wissen Sie, wo Sie stehen – mit Executive Summary für die Geschäftsleitung, priorisiertem Maßnahmenplan und belastbaren Zahlen für Ihre Cyberversicherung.



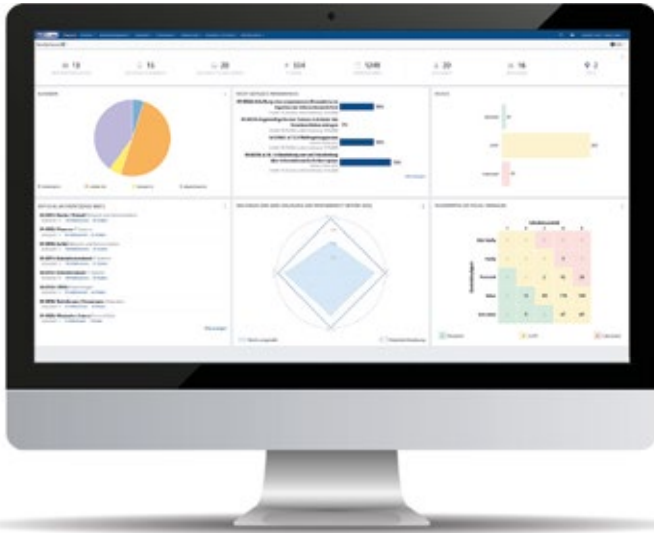
„Das Ergebnis der Beratung durch R.iT konnten wir direkt in unsere strategische Planung übernehmen und in der Kundenkommunikation nutzen.“

Frank Oelschläger, GILOG Geschäftsführer

Termin vereinbaren
in 10 Sekunden



Cyber-Sicherheit greifbar machen ISMS-Dashboard statt Excel-Chaos



Dashboard eines Informationssicherheits-Managementsystem (ISMS)

Wer IT-Sicherheit verantwortet, braucht Klarheit. Unser ISMS-Tool schafft genau das.

Auf einen Blick:

- Welche Systeme sind kritisch?
- Wo bestehen Risiken?
- Was ist umgesetzt – was nicht?
- Sind wir Audit-ready?

Ihr Nutzen:

- Kürzere Wiederanlaufzeit im Schadensfall durch klare Notfallpläne
- Bessere Cyber-Versicherungskonditionen durch nachweisbares ISMS
- Zugang zu Großkunden, die ISMS-Nachweise voraussetzen
- Nachweisbare Sorgfaltspflicht – bei Vorfällen, Versicherungsfällen und Behördenanfragen
- Kein Blindflug: Sie kennen Ihren Sicherheitsstatus, bevor es jemand anderes tut

Ihr NIS-2-Berater in Ostbayern



Über 25 Jahre Erfahrung im Bereich Cybersicherheit

Wir haben unser eigenes ISMS aufgebaut, bevor wir es empfohlen haben. Was wir Ihnen raten, haben wir selbst durchgelebt – und können es technisch auch selbst umsetzen.



Fokus auf den deutschen Mittelstand

Wir befähigen Sie, Ihre IT-Sicherheit selbst zu steuern und zu verstehen. Damit Sie langfristig unabhängig sind. Ausgezeichnet mit dem Label „Cybersecurity Made in Europe“.



Ein Ansprechpartner für Ihre Anforderungen

Von der Betroffenheitsprüfung über das iTRA-Assessment bis zum laufenden ISMS-Betrieb: kein Weitervermitteln, keine Reibungsverluste. Über 100 Mittelständler vertrauen uns ihre IT-Sicherheit an.

Ausgezeichnet



CYBERSECURITY
MADE IN EUROPE

Ihr Ansprechpartner jetzt anfragen



TOBIAS RADEMANN, M.A.

Geschäftsführer

Rademann@RiT.de

+49 (9971) 806 29-0



Termin vereinbaren
in 10 Sekunden

R.iT IN ZAHLEN & FAKTEN

Gründungsjahr: 2001

Standorte: Bochum, Cham
und Bad Schwartau

Team: 32 Mitarbeiter*innen

R.iT – DISCOVER THE SPIRIT OF EXCELLENCE

Die Digitale Transformation ist allgegenwärtig. Es gibt wohl kaum etwas, das unsere Wirtschaft und die Gesellschaft derart grundlegend verändern wird, wie dieser Prozess. Wir von R.iT beraten seit mehr als 25 Jahren Mittelstandsunternehmen auf diesem Weg und wir machen auch Sie zum **‘Digital Champion: Made in Germany’**.

R.iT GmbH – Niederlassung Süd

Rodinger Straße 15, 93413 Cham
+49 (9971) 806 29-0

info@RiT.de | www.RiT.de

DISCOVER THE SPIR.iT OF EXCELLENCE.
SURPASS YOUR SUCCESS.

