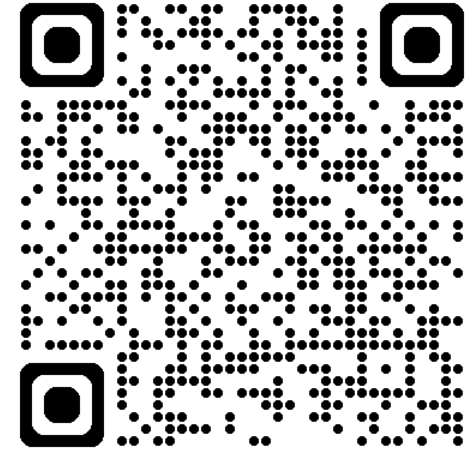




Webinar IHK Spezial

NIS-2-Compliance durch risikobasiertes
Schwachstellenmanagement

BIHK-Reihe "Umsetzen statt Abwarten: Neue Spielregeln für die Cybersicherheit"



<https://www.bihk.de/themen/digitalisierung/reihe-it-sicherheit>

Kooperation



Bayerisches Staatsministerium
für Digitales



- Digitalimpulse im Rahmen des bayerischen Pakts für berufliche Weiterbildung
- <https://www.kommweiter.bayern.de/mit-unterstuetzung/pakt-fuer-berufliche-weiterbildung/>
- <https://www.bihk.de/themen/digitalisierung/reihe-it-sicherheit>

Aktuelle Zahlen



Digital-Report 2026:

26 % der Unternehmen im letzten
Jahr Cyberangriffen ausgesetzt

Zum vollständigen Report:



Die NIS-2-Richtlinie



- 18 betroffene Sektoren
(u. a. Energie, Gesundheit, digitale Infrastruktur)
- Neue Unternehmenspflichten:
 - Meldepflichten
 - Risikomanagement
 - Lieferkettensicherheit
 - Management-Verantwortung

Hinweis: Nachholen der Registrierung im BSI-Portal **bis spätestens 31.07.2026!**

Wie geht es für betroffene Unternehmen weiter?



Christopher Proske

Geschäftsführer
initSecurity.Red GmbH

NIS-2 Compliance durch risikobasiertes Schwachstellenmanagement

- initSecurity.Red GmbH
- 10+ Jahre Erfahrung in der IT-Security
- Gerichtlich bestellter Gutachter & CISSP
- Penetrationtests & Red Teaming
- Schwachstellenmanagement Service & Beratung (PlenaSec.)
- **christopher.proske@initsecurity.red**
- +4916094800816

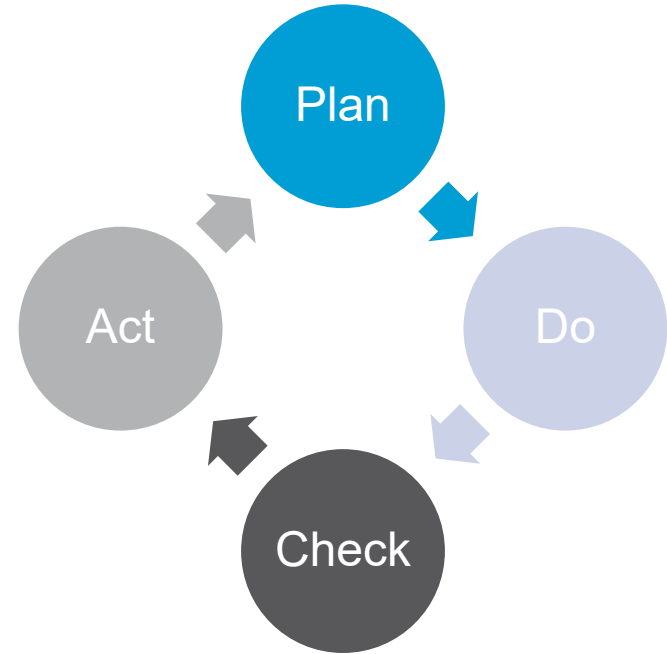
1. Einordnung
2. Interpretation
3. Konkretisierung
4. Umsetzung + Schmankerl

- Art. 20: Governance
- Art. 21: **Risikomanagementmaßnahmen**
- Art. 22: Lieferkettenrisiken
- Art. 23: Berichtspflichten

§ Das ist keine Rechtsberatung §

- Assets und Schwachstellen kennen
- Risiken bewerten
- Meldewege etablieren
- Lieferketten einbeziehen
- Dokumentieren, Berichten und Überprüfen

- Assets kennen und bewerten
- Schwachstellen erkennen
- Risiken ermitteln
- Reaktionszeiten festlegen
- Schwachstellen beheben
- Regelmäßige Überprüfungen
- Sichere Beschaffung
- Integration von Lieferanten



1. Alle **wichtigen** und **besonders wichtigen** Assets
2. **Verantwortlichkeiten** definieren
3. Automatisierte und manuelle **Erkennung**
4. Zentrale **Datenbank**
5. **Bewertung** der Systeme
6. Kontinuierliche **Aktualisierung**

1. **Automatisierte** Erkennung
2. Bewerten und **Anreichern**
3. Scan-**Strategie**

1. Auswirkung **X** Wahrscheinlichkeit
2. NIS-2 **relevante** Prozesse

1. Definition von Reaktionszeiten und **Priorisierung**
2. Definition von **Eskalationswegen**
3. Integration in den **Incident Response Prozess** für kritische Schwachstellen
4. **Meldung** an Behörden bei Bedarf

1. Einspielen von Security Patches **nach Risiko**
2. Einführen von **kompensierenden Maßnahmen** bei Bedarf
3. Dokumentation und **Überprüfung** der Behebung

1. Definition und Erhebung von **KPIs**
2. Erzeugung von **Reports**
3. Berichtsweg an die **Geschäftsführung**

1. Durchführung von **Penetrationstests**
2. Durchführung von **Red Teaming**
3. Durchführung von **Audits**
4. Prozesses zur **Offenlegung** von Schwachstellen

1. IT-Security **Anforderungen** an Lieferanten
2. Umsetzung der Anforderungen bei der **Beschaffung**

1. **Schwachstellenquellen** von Lieferanten
2. **Kommunikationslinien** zu Herstellern
3. **SLAs**

1. Fundament & Asset-Bewertung
2. Kontinuierliche Schwachstellen-Erkennung
3. Risikofusion & Reaktionszeiten
4. Effektive Behebung & Verifikation
5. Governance, Lieferkette & Überprüfung

- **Confidentiality**
- **Integrity**
- **Availability**
- **System Dependency**
- **Recovery Complexity**
- **Compliance Impact**
- **Exposure**



Wie fit ist Ihr Team in Sachen Cyber Security?



 **IHK** Schwaben

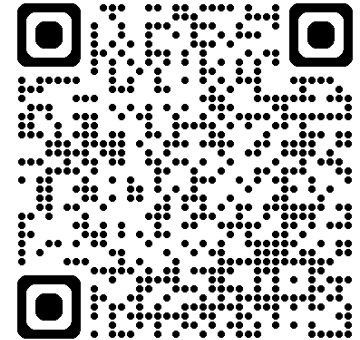
Jetzt kostenlos mitmachen!

Member Login
Username
Password
Login

Cyber-Security-Awareness-Test

Wie fit sind Sie und Ihre Mitarbeiter in Sachen Cybersicherheit?

kostenfrei
anmelden:





Unsere nächsten Webinare im Themenfeld Digitalisierung und KI

**IT-Beschaffungen der Bundeswehr
– Worauf interessierte
Unternehmen achten müssen**

Montag, 29.06.2026 | 14:00 - 15:00 Uhr

Anne Müller | Dr. Thomas Kirch

Leinemann Partner Rechtsanwälte mbB



**KI-Kennzeichnungspflicht nach dem
AI Act: Was Unternehmen jetzt konkret
umsetzen müssen**

Donnerstag, 09.07.2026 | 15:00 - 16:00 Uhr

Julian Modi

Sonntag & Partner





Business Continuity Management | 1.-2. Juli 2026



Jetzt anmelden!



Kommen Sie bei Fragen gerne auf mich zu!

Luzia Ghoggal



Digitale Innovation und Künstliche
Intelligenz



luzia.ghoggal@schwaben.ihk.de



0821/3162-230





**Vielen Dank für
Ihre
Aufmerksamkeit!**

Weitere Informationen unter
 [ihk.de/schwaben/ihkspezial](https://www.ihk.de/schwaben/ihkspezial)