Cybersecurity & KI

Sicherheit - Pflicht und Chance

Webinar | 22. Juli 2025 | 17:00 - 18:00 Uhr

Arno Schimmelpfennig

Unabhängiger Experte für Cybersecurity & KI

SELBSTÄNDIGE IN BAYERN BDS

Agenda

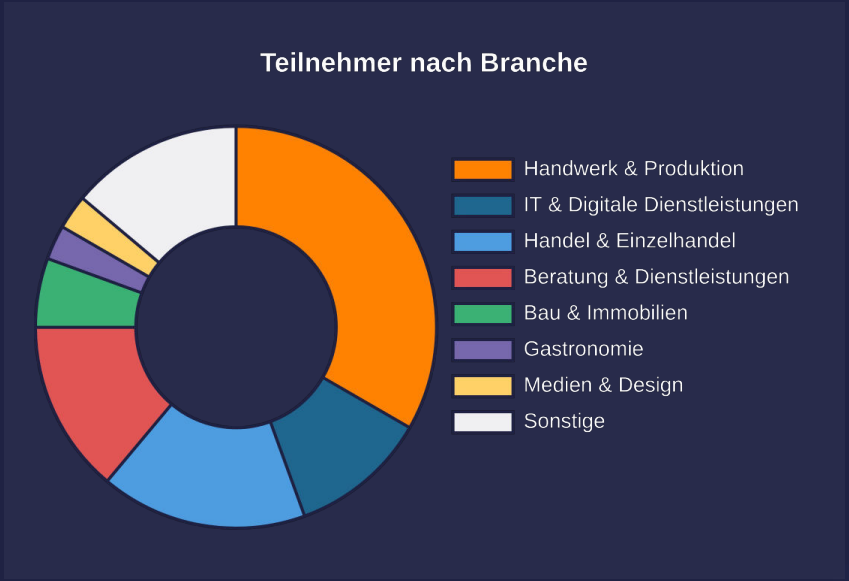
- **NIS-2 Richtlinie: Neue Anforderungen für KMU**
  Verstehen & Anwenden
- **AI Act: Compliance als Wettbewerbsvorteil**
  Analysieren & Evaluieren
- **Ransomware-Angriffe: Aktuelle Bedrohungen**
  Analysieren & Evaluieren
- **Zero Trust: Moderne Sicherheitsarchitektur**
  Anwenden & Erschaffen
- **Interaktives Mini-Selbstaudit**
  Erschaffen & Evaluieren

Jedes Thema wird mit einem konkreten Praxisbeispiel veranschaulicht

SELBSTÄNDIGE IN BAYERN BDS

Unsere Teilnehmer heute

Branchenverteilung und spezifische Herausforderungen



Handwerk & Produktion (12)
IoT-Sicherheit, Produktionsanlagen-Schutz, NIS-2 Compliance

IT & Digitale Dienstleistungen (4)
AI Act Compliance, Supply Chain Security, Zero Trust

Handel & Einzelhandel (6)
PCI-DSS, E-Commerce Sicherheit, Kundendatenschutz

Beratung & Dienstleistungen (5)
Beraterhaftung, sichere Kommunikation, Compliance-Beratung

Datenschutzexpertin unter den Teilnehmern

Herausforderung 1: NIS-2 Richtlinie

Neue Anforderungen für deutsche KMU

Was ist NIS-2?

EU-Richtlinie zur Netzwerk- und Informationssicherheit mit erheblich erweiterten Anforderungen für Unternehmen.

Januar 2023

Inkrafttreten der NIS-2-Richtlinie

Oktober 2024

Umsetzung in deutsches Recht

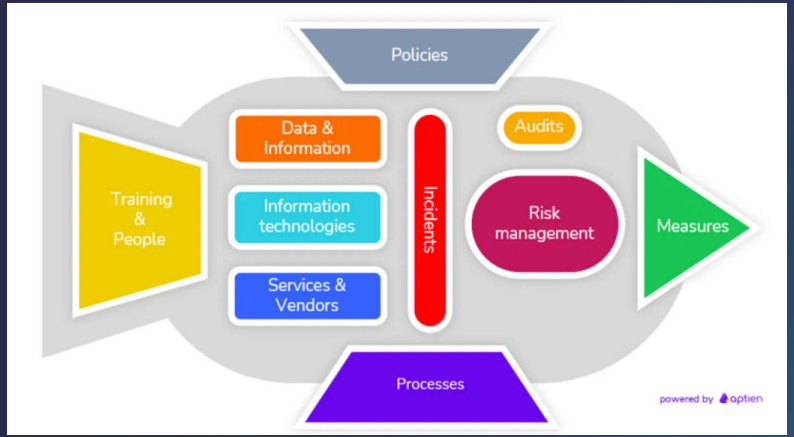
Februar 2025

Pflicht zur Umsetzung für betroffene Unternehmen

Betroffene Branchen

- 18 kritische Sektoren, darunter Energie, Verkehr, Gesundheit
- Auch viele KMU als Zulieferer oder Dienstleister betroffen

Kernelemente der NIS-2



- Risikomanagement-Maßnahmen nach Artikel 21
- Meldepflichten bei Sicherheitsvorfällen (24h/72h)
- Verantwortlichkeit der Geschäftsführung
- Lieferkettenmanagement und Drittanbieter-Sicherheit

Praxisbeispiel: NIS-2 Umsetzung

Erfolgreiche Implementierung in einem mittelständischen Unternehmen

Maschinenbau GmbH, 120 Mitarbeiter

Das Unternehmen fällt unter die NIS-2-Richtlinie als Zulieferer für kritische Infrastrukturen und musste bis Februar 2025 die Anforderungen umsetzen.

> *"Die frühzeitige Umsetzung der NIS-2-Richtlinie hat sich als Wettbewerbsvorteil erwiesen. Unsere Kunden schätzen die erhöhte Sicherheit."*

Herausforderungen:

Begrenzte IT-Ressourcen
Komplexe Produktionsumgebung
Hohe Anforderungen an Verfügbarkeit

Ergebnisse:

- 70% weniger Sicherheitsvorfälle
- Vollständige Compliance mit NIS-2
- Verbesserte Kundenzufriedenheit

Implementierungszeitplan:

1. Juli 2024
   Betroffenheitsanalyse & Team-Zusammenstellung
2. August-September 2024
   Risikobewertung & Gap-Analyse
3. Oktober-November 2024
   Implementierung technischer Maßnahmen
4. Dezember 2024
   Schulung aller Mitarbeiter
5. Januar 2025
   Dokumentation & Incident Response Plan
6. Februar 2025
   Externe Prüfung & Zertifizierung

Wichtigste Erfolgsfaktoren:

1. Frühzeitige Planung (7 Monate vor Deadline)
2. Einbindung aller Abteilungen

Herausforderung 2: AI Act Compliance

Risikoorientierter Ansatz für KMU

Aktueller Stand (Juli 2025)

46 führende Unternehmen fordern **Aufschub um 2 Jahre** für die Umsetzung des AI Acts

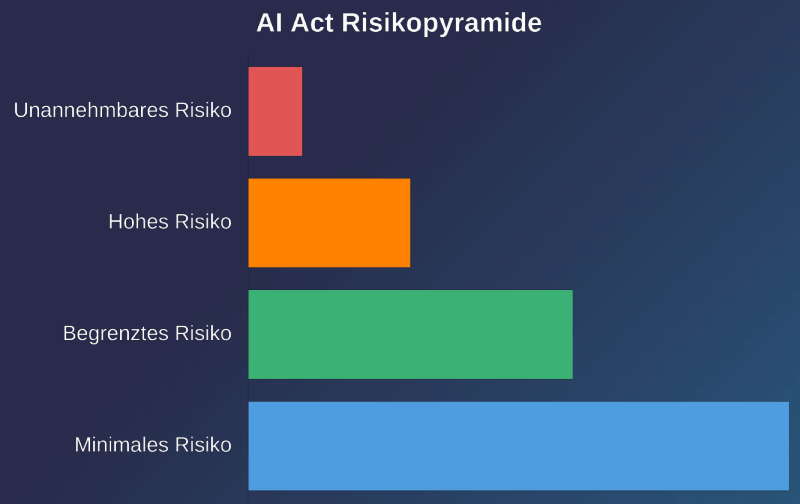
Herausforderungen für KMU

- Rechtsunsicherheit und unklare Zuständigkeiten
- Verpflichtung zur KI-Ausbildung ab 2025
- Dokumentationspflichten je nach Risikoklasse
- Menschliche Aufsicht bei automatisierten Entscheidungen

Zeitplan

- 2024: Verabschiedung des AI Acts
- 2025: Verpflichtung zur KI-Ausbildung
- 2025-2027: Stufenweise Umsetzung

Risikobasierter Ansatz



- **Unannehmbares Risiko:** Verboten (z.B. Social Scoring)
- **Hohes Risiko:** Umfassende Compliance-Anforderungen
- **Begrenztes Risiko:** Transparenzpflichten

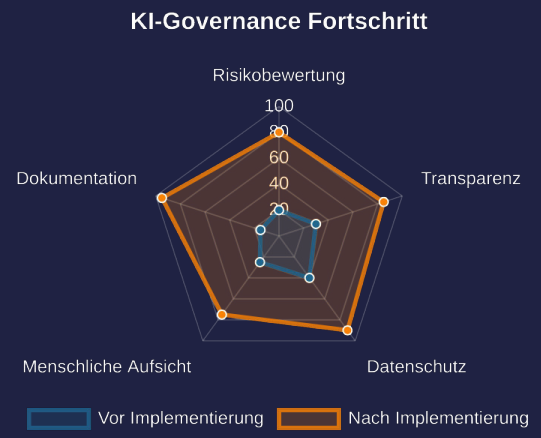
Praxisbeispiel: KI-Governance

Implementierung für ein mittelständisches Unternehmen

Softwareentwicklungsunternehmen

45 Mitarbeiter

KI-gestütztes Support-System



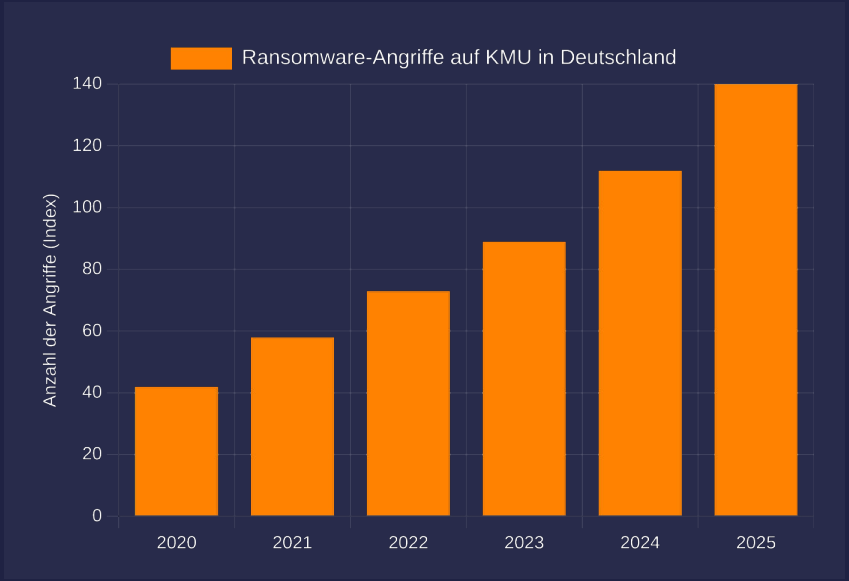
1. **KI-Inventarisierung**
   Erfassung aller KI-Systeme und Einstufung nach Risikokategorien des AI Acts
2. **Governance-Team**
   Bildung eines interdisziplinären Teams aus IT, Recht und Fachabteilungen
3. **Dokumentation & Transparenz**
   Erstellung von Datensatz-Dokumentation und Transparenzberichten
4. **Mitarbeiterschulung**
   KI-Kompetenzaufbau gemäß AI Act-Anforderungen

Ergebnis:

- Rechtssicherheit durch proaktive Compliance
- Wettbewerbsvorteil durch Transparenz
- Höhere Kundenzufriedenheit durch ethische KI

Herausforderung 3: Ransomware-Angriffe

Wachsende Bedrohung für den Mittelstand



1. Initiale Infektion

Phishing-E-Mails, kompromittierte Websites, unsichere RDP-Zugänge

2. Laterale Bewegung

Ausbreitung im Netzwerk, Rechteausweitung, Datenexfiltration

3. Verschlüsselung & Erpressung

Datenverschlüsselung, Lösegeldforderung, Drohung mit Veröffentlichung

4. Besonders gefährdete Branchen

Handwerk, Einzelhandel, Gesundheitswesen, Bildung

82%

der Ransomware-Angriffe zielen auf KMU

5,5 Mio €

durchschnittlicher Schaden pro Vorfall

⚠ Fallbeispiel: Serviettenhersteller Fasana - Insolvenz nach Ransomware-A

Praxisbeispiel: Ransomware-Abwehr

Erfolgreiche Verteidigung der Aerzener Maschinenfabrik

Aerzener Maschinenfabrik GmbH

Das Unternehmen wurde Ziel eines Ransomware-Angriffs, konnte aber durch vorbereitete Maßnahmen größere Schäden abwenden.

"Wir haben uns geweigert, mit den Cyberkriminellen zu verhandeln. Dank unserer Backup-Strategie konnten wir den Betrieb schnell wieder aufnehmen."

Erfolgsfaktoren:

3-2-1 Backup-Strategie

Drei Kopien der Daten auf zwei verschiedenen Medientypen, eine Kopie offline

Netzwerksegmentierung

Isolierung kritischer Systeme zur Eindämmung der Ausbreitung

Endpoint Detection and Response

Frühzeitige Erkennung verdächtiger Aktivitäten

Incident Response Plan

Vorbereiteter Notfallplan mit klaren Verantwortlichkeiten

Chronologie des Angriffs:

1. Tag 1 - 03:27 Uhr

   Erste Anzeichen: Ungewöhnlicher Netzwerkverkehr wird vom EDR-System erkannt

2. Tag 1 - 04:15 Uhr

   Automatische Isolation betroffener Systeme durch Sicherheitssoftware

3. Tag 1 - 07:30 Uhr

   IT-Team aktiviert Incident Response Plan und informiert Geschäftsführung

4. Tag 1 - 10:00 Uhr

   Erpresserschreiben wird entdeckt, Forderung: 15 Bitcoin

5. Tag 1 - 14:00 Uhr

   Entscheidung: Keine Lösegeldzahlung, Wiederherstellung aus Backups

6. Tag 2 - 18:00 Uhr

   Kritische Systeme wiederhergestellt, Produktion läuft wieder an

Chance: Zero Trust Architektur

Moderne Sicherheit für den Mittelstand

Was ist Zero Trust?

"Never Trust, Always Verify" - Ein Sicherheitsmodell, das keine automatischen Vertrauensbeziehungen gewährt, sondern jeden Zugriff kontinuierlich überprüft.

Vorteile für KMU

- Besserer Schutz bei hybriden Arbeitsmodellen
- Sichere Cloud-Migration
- Skalierbarkeit und Flexibilität

Kernprinzipien

1. Verifiziere jeden Zugriff

Jeder Zugriff wird unabhängig vom Standort oder Netzwerk überprüft

2. Minimale Berechtigungen

Zugriff nur auf benötigte Ressourcen (Least Privilege)

3. Kontinuierliche Überwachung

Ständige Analyse von Zugriffen und Verhalten

4. Mikrosegmentierung

Feine Unterteilung des Netzwerks in isolierte Segmente

Praxisbeispiel: Zero Trust Implementierung

Schrittweise Einführung in einem mittelständischen Unternehmen

Mittelständischer Maschinenbauer (50 Mitarbeiter)

Ausgangslage: VPN-basierter Fernzugriff, lokale Server, zunehmende Cyberangriffe

1. **Multi-Faktor-Authentifizierung (MFA)**
   Einführung für alle Benutzer und kritische Anwendungen

2. **Cloud-basierte Identitätsverwaltung**
   Zentralisierte Benutzerverwaltung und Single Sign-On

3. **Conditional Access Policies**
   Kontextbasierte Zugriffssteuerung nach Gerät, Standort und Risiko

4. **Netzwerksegmentierung**
   Mikrosegmentierung kritischer Bereiche und Anwendungen

"Die schrittweise Einführung von Zero Trust hat uns geholfen, die Komplexität zu bewältigen und gleichzeitig die Sicherheit deutlich zu erhöhen."

Praxisbeispiel: Zero Trust Implementierung

Schrittweise Einführung in einem mittelständischen Unternehmen

Mittelständischer Maschinenbauer (50 Mitarbeiter)

Ausgangslage: VPN-basierter Fernzugriff, lokale Server, zunehmende Cyberangriffe

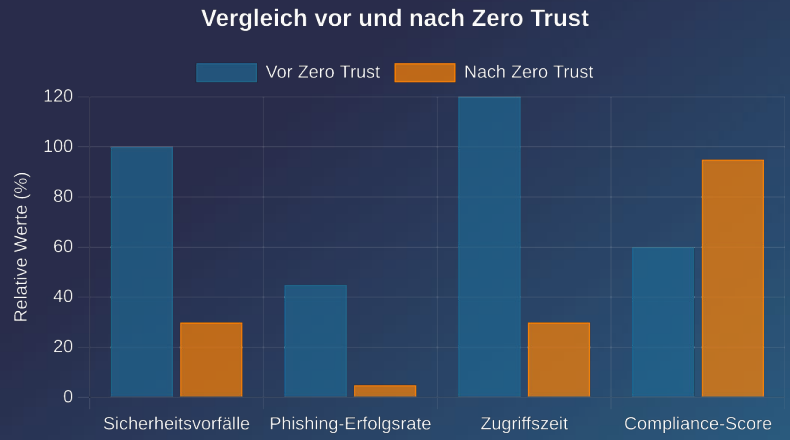
1. **Multi-Faktor-Authentifizierung (MFA)**
   Einführung für alle Benutzer und kritische Anwendungen

2. **Cloud-basierte Identitätsverwaltung**
   Zentralisierte Benutzerverwaltung und Single Sign-On

3. **Conditional Access Policies**
   Kontextbasierte Zugriffssteuerung nach Gerät, Standort und Risiko

4. **Netzwerksegmentierung**
   Mikrosegmentierung kritischer Bereiche und Anwendungen

Ergebnisse nach 12 Monaten



- 70% weniger Sicherheitsvorfälle
- Verbesserte Compliance mit NIS-2 und DSGVO
- Erhöhte Produktivität durch nahtlosen Zugriff
- ROI nach 18 Monaten durch reduzierte Vorfälle

Interaktiver Teil: Selbstaudit

Bewerten Sie Ihre Cybersecurity & KI-Readiness

1 Wie ist Ihr Unternehmen auf Ransomware-Angriffe vorbereitet?

- Keine speziellen Maßnahmen
- Grundlegende Backups und Antivirensoftware
- Umfassende Strategie mit regelmäßigen Tests

2 Wie weit sind Sie bei der NIS-2 Compliance?

- Noch nicht damit beschäftigt
- Betroffenheit geprüft, erste Schritte eingeleitet
- Umfassende Implementierung läuft oder abgeschlossen

3 Wie setzen Sie KI in Ihrem Unternehmen ein?

- Keine KI-Nutzung
- Einsatz von KI-Tools ohne spezielle Governance

Zusammenfassung & Ausblick

Ihre nächsten Schritte für mehr Cybersicherheit

1 Pflicht als Chance nutzen

NIS-2 und AI Act sind nicht nur regulatorische Pflichten, sondern bieten die Chance, Sicherheit als Wettbewerbsvorteil zu etablieren.

2 Frühzeitig handeln

Wer jetzt mit der Umsetzung beginnt, vermeidet Zeitdruck und kann Maßnahmen schrittweise implementieren.

3 Ganzheitlicher Ansatz

Erfolgreiche Cybersicherheit kombiniert technische, organisatorische und personelle Maßnahmen.

Ihr 30-Tage-Aktionsplan

- Betroffenheitsanalyse für NIS-2 und AI Act durchführen
- Verantwortlichkeiten im Unternehmen festlegen
- Basis-Schutzmaßnahmen gegen Ransomware implementieren
- Dokumentation bestehender KI-Systeme beginnen
- Schulungsplan für Mitarbeiter erstellen

Nächster Termin:

"KI in Ihrer Branche – Praxisworkshop"

12. August 2025 | 17:00 - 19:00 Uhr

Jetzt anmelden

SELBSTÄNDIGE IN BAYERN BDS

Kontakt & Fragen

Bleiben Sie mit uns in Verbindung

Arno Schimmelpfennig

Unabhängiger Experte für KI im Mittelstand

info@arno-schimmelpfennig.de

+49 172 2712600

as-digitalmarketing.de

Mitglied im Bund der Selbständigen Bayern e.V.
Zertifizierter Cybersecurity-Berater für KMU

Fragen & Antworten

Stellen Sie Ihre Fragen jetzt im Chat!

Weiterführende Ressourcen:

- Präsentationsfolien (PDF)
- NIS-2 Leitfaden für KMU
- AI Act Compliance-Checkliste
- Zero Trust Implementierungsguide

Aufzeichnung und Materialien werden im internen Bereich der BDS Bayern Akademie bereitgestellt.