

DACH-Region

KI und Cybersicherheit: Das nächste Schlachtfeld für digitales Vertrauen

PECB REGIONAL WEBINARS

Agenda

1. Einleitung und Kontext
2. Bedrohungslage im Wandel durch KI
3. Agents
4. Zero Trust und Vertrauenskrise
5. Defensive Nutzung von KI
6. Regulatorische Rahmenbedingungen
7. Handlungsempfehlungen & Roadmap
8. Fazit & Ausblick
9. Q&A

1. Einleitung und Kontext

1. Einleitung und Kontext

Artikel 3

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „KI-System“ ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können;

1. Einleitung und Kontext

- Aktuelle Entwicklung: Rolle von KI in der Cybersicherheit (Angriff vs. Verteidigung)
- Deepfake-Anrufe, gefälschte E-Mails, etc.
- Bedeutung von „Digital Trust“ in einer von KI geprägten Welt

2. Bedrohungslage im Wandel durch KI

2. Bedrohungslage im Wandel durch KI

- Phishing und Social Engineering auf neuem Level (generative KI für täuschend echte E-Mails)
- Deepfakes (Audio, Video, Bilder) als Werkzeug für Betrug, Desinformation, Erpressung
- Beispiele realer Vorfälle (u. a. CEO-Fraud, Deepfake-Video-Konferenzen)
- Automatisiertes Vulnerability Scanning und Exploit-Anpassung durch KI
- Model Extraction Angriffe

3. Agents

3. Agents

- Definition von KI-Agents und ihre Fähigkeit, Aufgaben eigenständig auszuführen
- Agents auf Angreiferseite (Reconnaissance, Weaponization, Exploitation ohne menschliches Zutun)
- Agents auf Verteidigungsseite (Automatisierte Angriffs- und Anomalieerkennung)
- Risiken wie Data Poisoning und manipulative Trainingsdaten

4. Zero Trust und Vertrauenskrise

4. Zero Trust und Vertrauenskrise

- Paradigmenwechsel vom perimeterbasierten Modell zu Zero Trust
- Prinzipien: Explizite Verifizierung, Minimale Rechtevergabe, Segmentierung
- Auswirkungen von KI auf digitale Identitäten, Authentifizierung und Inhalte

4. Zero Trust und Vertrauenskrise

1. Explizite Verifizierung
2. Minimale Rechtevergabe
3. Segmentierung und Mikro-Isolierung

4. Zero Trust und Vertrauenskrise

- Continuous Verification, Schutz vor Deepfakes und synthetischen Inhalten
- Strategisches, organisationsweites Modell

4. Zero Trust und Vertrauenskrise

1. Authentifizierung & Zugangskontrolle
2. Content Integrity
3. Netzwerksegmentierung und Asset-Isolation
4. Continuous Evaluation von LLMs und Agents
5. Example

5. Defensive Nutzung von KI

5. Defensive Nutzung von KI

- Anomalieerkennung in Echtzeit (Erkennung unbekannter Angriffsmuster)
- SOAR-Systeme (Security Orchestration, Automation and Response) zur automatisierten Reaktion
- Threat Intelligence durch KI (Analyse von großen Datenmengen in Darknet, Foren, Social Media)
- Risiken bei KI-generiertem Code (fehlende Eingabevalidierung, Sicherheitslücken)
- Maßnahmen zur Code-Prüfung und -Validierung (Security-Reviews, automatisierte Scanner)

5. Defensive Nutzung von KI

1. Standardmäßig potenziell unsicher
2. Automatischen statischen Analysetools
3. Entwicklung und Integration von spezialisierten Scannern
4. Schulungen
5. AI validating AI

Beispiel: KI und Echtzeitüberweisungen



6. Regulatorische Rahmenbedingungen

6. Regulatorische Rahmenbedingungen

- EU-Verordnung über Künstliche Intelligenz (KI-VO) und Einstufung als Hochrisiko-Anwendungen
- Pflichten von Betreibern vs. Anbietern, Art. 4 KI-VO und KI-Kompetenzanforderungen
- Menschliche Kontrolle, Transparenz, Erklärbarkeit (Explainable AI)

6. Regulatorische Rahmenbedingungen

Artikel 4

KI-Kompetenz

Die Anbieter und Betreiber von KI-Systemen ergreifen Maßnahmen, um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen sind.

6. Regulatorische Rahmenbedingungen

Artikel 3

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

4. „Betreiber“ eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet;

6. Regulatorische Rahmenbedingungen

- Relevante Gesetze und Standards in der DACH-Region
  - DSGVO
  - NIS2
  - DORA

7. Handlungsempfehlungen & Roadmap

7. Handlungsempfehlungen & Roadmap

- KI als sicherheitsrelevante Schlüsseltechnologie begreifen (Zusammenarbeit CISO–CTO)
- Governance & interne Richtlinien für den KI-Einsatz (Risikobewertung, Ethische Leitplanken)
- Transparenz & Auditierbarkeit sicherstellen (Explainable AI, Nachvollziehbare Entscheidungen)
- Kompetenzaufbau im Unternehmen (Data-Science-Skills, Schulungen für Security-Teams)
- Standards & Best Practices (z. B. ISO/IEC 27001:2024, ISO/IEC 42001:2023)

7. Handlungsempfehlungen & Roadmap

Blick in die Norm



NORM [AKTUELL]

DIN EN ISO/IEC 27001:2024-01

Informationssicherheit, Cybersicherheit und Datenschutz - Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27001:2022); Deutsche Fassung EN ISO/IEC 27001:2023

Englischer Titel:
Information security, cybersecurity and privacy protection - Information security management systems - Requirements (ISO/IEC 27001:2022); German version EN ISO/IEC 27001:2023

Ausgabedatum:
2024-01

Originalsprachen:
Deutsch

Seiten:
31

7. Handlungsempfehlungen & Roadmap



NORM [AKTUELL]

ISO/IEC 42001:2023-12

Informationstechnik – Künstliche Intelligenz - Managementsystem

Englischer Titel:
Information technology - Artificial intelligence - Management system

Ausgabedatum:
2023-12

Originalsprachen:
Englisch

Seiten:
51

7. Handlungsempfehlungen & Roadmap



AI RISK MANAGEMENT

The **PECB Certified AI Risk Manager** course teaches professionals how to identify, assess, and mitigate AI-related risks. It focuses on compliance with frameworks like the NIST AI Risk Management Framework and the EU AI Act, while providing practical insights into real-world AI challenges, such as bias and security risks. Participants will learn to integrate AI risk management into business strategies and ensure ethical AI governance.

8. Fazit & Ausblick

8. Fazit & Ausblick

- KI als Chance und Risiko in der Cybersicherheit
- Bedeutung von Vertrauen und Souveränität in einer digitalisierten Welt
- Schnelle Entwicklung erfordert kontinuierliche Anpassung und Investition

9. Q&A

Q&A Session



Contact

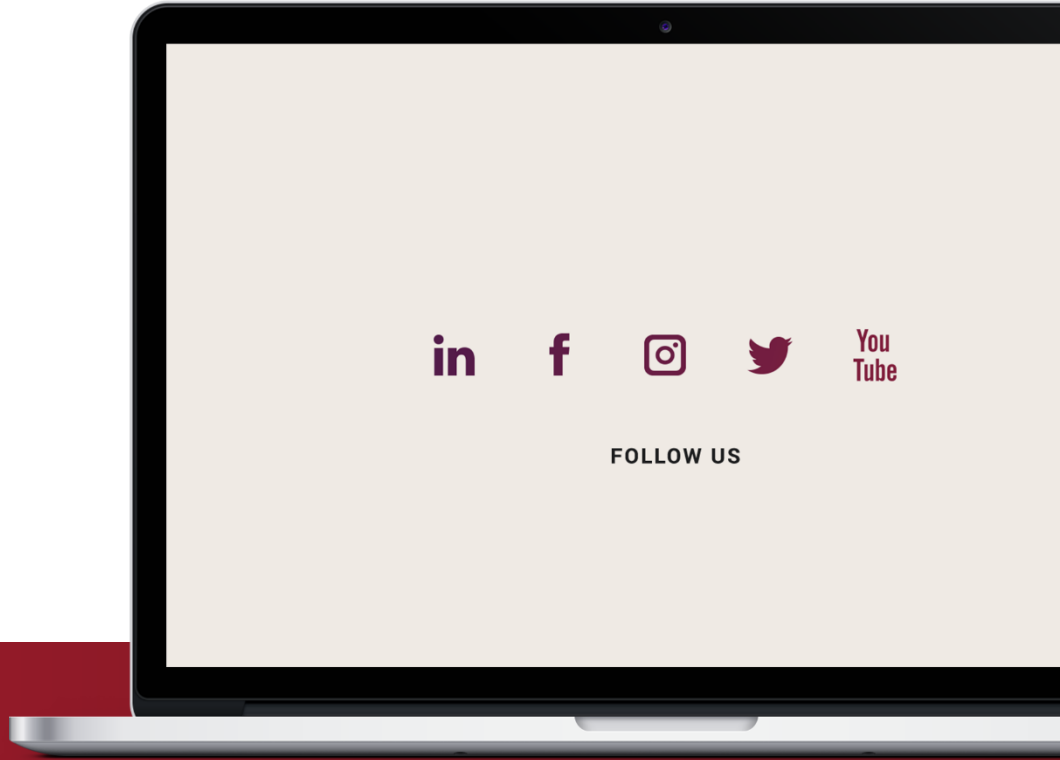
- Referent: Viktor Jahn

- Website: www.msdd.net
- Phone: +49 155 61820514
- Email: vj@msdd.net

- LinkedIn.com/in/viktor-jahn

For any questions or comments you can contact us below:

- support@pecb.com



PECB REGIONAL WEBINARS