Deloitte.

Together makes progress

Resilient, reguliert, souverän

Die drei Gesichter der KI in der Security

IT-SECX | St. Pölten, Oktober 2026





Ilyas Demirtas

Application Security Lead

Kai Starik

OT Security Lead

Inhalt

01 | Die Ausgangslage

02 | Cybersecurity im KI-Zeitalter

03 | Drei strategische Perspektiven

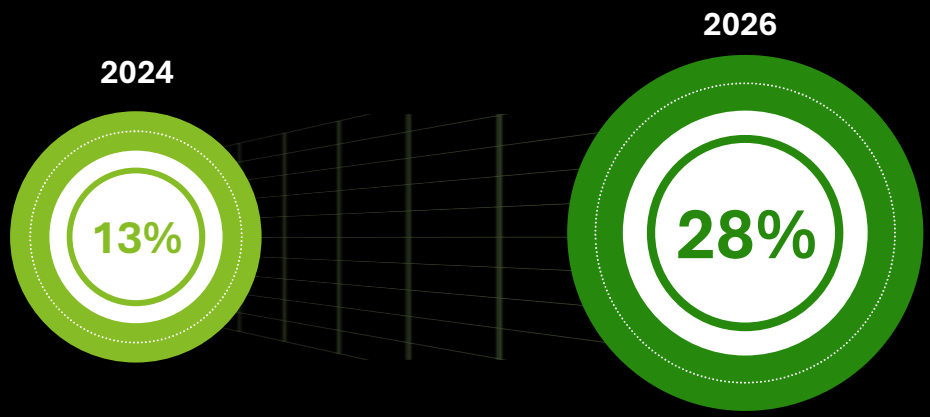
04 | Ausblick & Key Takeaway



01 | Die Ausgangslage

Die internationale Bedrohung spitzt sich zu





Der ***Deloitte Cyber Report 2026*** stellte fest, dass der Anteil jener österreichischen Unternehmen, welche *tägliche Angriffsversuche* verzeichnen von **13 %** (2024) **auf 28 %** (2026) **gestiegen ist.** [6]

Unternehmen sind gefordert sich dieser Herausforderung zu stellen & müssen aufrüsten

KI wird zu einem Beschleuniger für Angreifer

KI-gesteuerte Schwachstellenerkennung und -ausnutzung erhöhen die Geschwindigkeit und das Ausmaß von Angriffen erheblich und damit die daraus resultierenden Cyberrisiken



~7 Tage

Durschnittliche Zeit bis zur Ausnutzung einer Schwachstelle[7]



134%

Anstieg in der Ausführung von KI-Skripten bei Angriffen[8]



88%

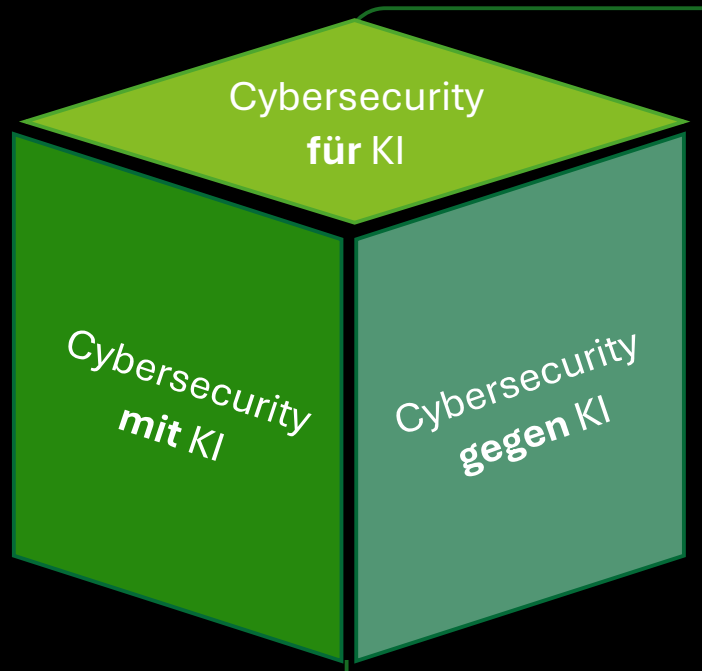
Anstieg bei KI-gestützter Aufklärung und Datensammlung[9]

KI ist kein weiteres IT-Thema, sondern verändert die gesamte Bedrohungslandschaft von Grund auf



02 | Cybersecurity im KI-Zeitalter

Cyberrisiko und stategische Chance



Schutz von KI-Systemen vor Cybersecurity Bedrohungen durch **Sicherung** implementierter oder geplanter KI-Anwendungsfälle

Model Theft
Supply Chain
Prompt Injection
Excessive Agency
Data Leakage/Poisoning

Verbesserung der Cybersicherheitsfähigkeiten und Förderung von Cybersicherheitsprozessen durch **Einbeziehung von KI**

Alert Triage
SOC Copilots
Incident Response
Threat Intelligence
Detection Engineering

Veränderung der Bedrohungslandschaft durch die Einführung ausgefeilterer und neuer Arten von **Cyberangriffen**

Phishing
Deepfakes
Agentic Attacks
Automated Recon
Malware Assistance

KI ist sowohl ein Angriffswerkzeug und ein Angriffsziel, allerdings auch eine neue Verteidigungstechnologie

03 | Drei strategische Perspektiven

Vorbereitung für die neue Realität



Ziel ist es, regulatorische Anforderungen zu erfüllen, die Widerstandsfähigkeit gegen neue Angriffe zu stärken und zugleich Kontrolle über kritische Abhängigkeiten zu behalten

KI-Resilienz

Was bedeutet sie und welche Handlungsfelder daraus entstehen

Die Fähigkeit eines Unternehmens, KI-Systeme **sicher, robust und kontrolliert** zu betreiben, auch wenn sie durch Angriffe, Fehlfunktionen, Datenprobleme, regulatorische Änderungen oder externe Abhängigkeiten unter Druck geraten

Handlungsfelder

- Awareness
- SIEM- Monitoring
- AI Red Teaming
- Recovery
- IDS/IPS - SOAR – XDR
- Tabletop Exercises

[10]

PRAXISBEISPIEL: Ein Angreifer imitiert mithilfe eines Deepfakes die Stimme einer Führungsperson und fordert eine dringende Überweisung



Resilienz bedeutet nicht, Angriffe vollständig zu verhindern, sondern den Geschäftsbetrieb trotz Angriffen aufrechtzuerhalten

KI-Regulation

Was bedeutet sie und welche Handlungsfelder daraus entstehen

Der Rahmen aus externen **gesetzlichen Anforderungen** und internen Governance-Vorgaben, nach dem KI-Systeme entwickelt, eingesetzt, überwacht und verantwortet werden

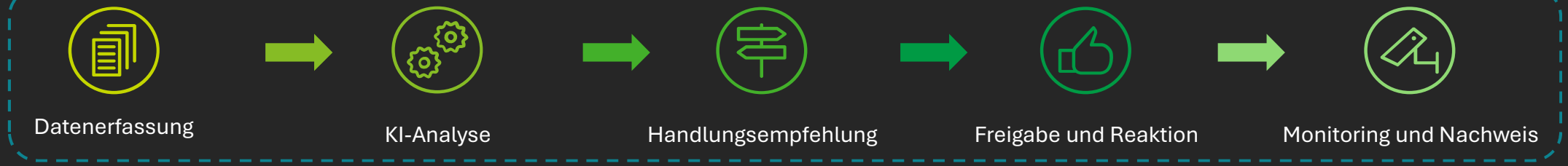
Handlungsfelder

- KI-Inventarisierung
- Risko Assessments
- Governance
- Dokumentation
- Security by Design
- Continuous Monitoring

EU AI ACT
DORA
NIS2
DSGVO

[11]

PRAXISBEISPIEL: Ein cloudbasierter SOC-Copilot, der Security Logs analysiert, Alerts priorisiert und Maßnahmen zur Eindämmung eines Angriffs empfiehlt



Mit zunehmender Nutzung wird KI selbst zum regulatorischen Objekt mit neuen Anforderungen an Sicherheit, Transparenz und Verantwortung

KI-Souveränität

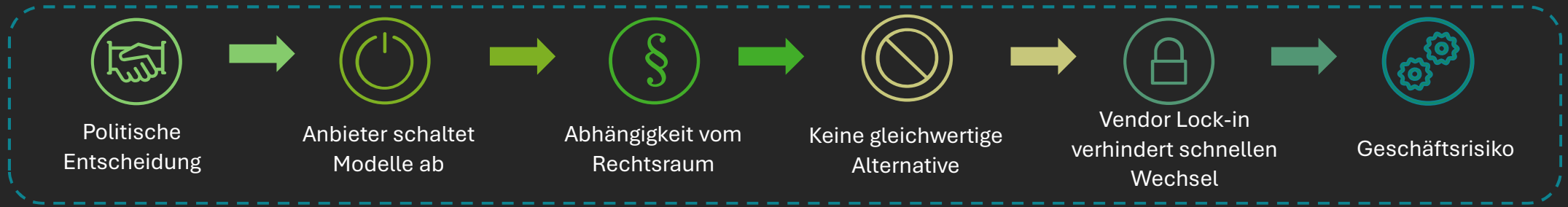
Was bedeutet sie und welche Handlungsfelder daraus entstehen

Die Fähigkeit eines Unternehmens, den Einsatz von KI **selbstbestimmt zu steuern** und dabei Kontrolle über Daten, Modelle, Infrastruktur, Anbieterabhängigkeiten und kritische Entscheidungsprozesse zu behalten.

Handlungsfelder

- KI Governance
- Datenklassifizierung
- Private LLMs
- EU-/On-Prem-Hosting
- Hybrid-KI
- Zero Trust

PRAXISBEISPIEL: Ein US-Exportverbot zwingt Anthropic, zwei leistungsstarke KI-Modelle weltweit vom Netz zu nehmen [12]



Souveränität bedeutet Kontrolle über Daten, Modelle und Infrastruktur

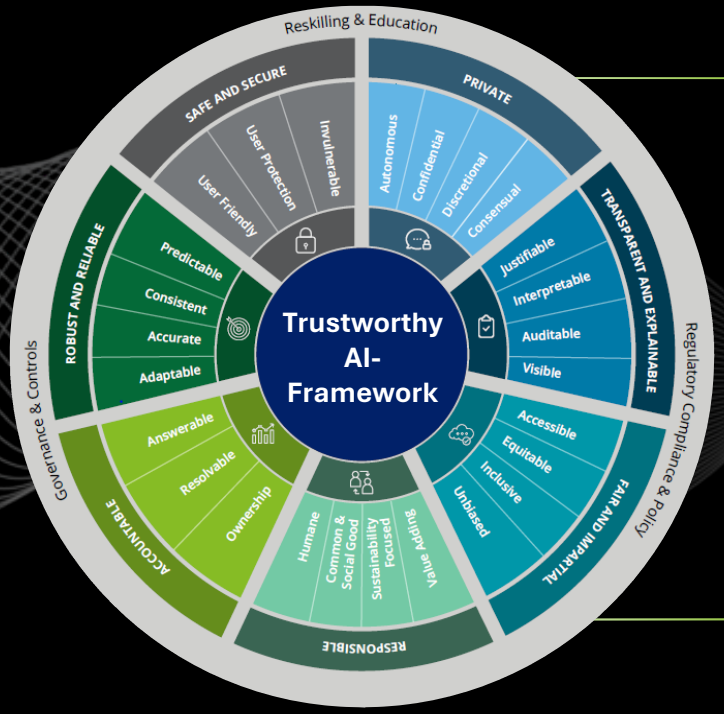
04 | Ausblick & Key Takeaway

Vertrauenswürdige KI für eine BESSERE ZUKUNFT

RESILIENZ

REGULATION

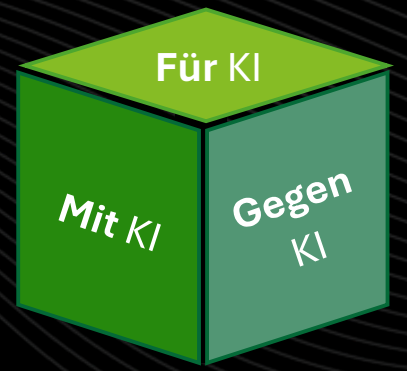
SOUVERÄNITÄT



KI-Systeme schützen und wiederherstellungsfähig gestalten

Regulatorische Anforderungen in wirksame Governance übersetzen

Kontrolle über kritische KI-Ressourcen & Abhängigkeiten sichern



Resilienz, Regulation und Souveränität für eine transparente, sichere und menschenzentrierte KI



Fragen & Diskussion

Deloitte.

Together makes progress

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/de/UeberUns for a more detailed description of DTTL and its member firms.

Deloitte provides audit, risk advisory, tax, financial advisory and consulting services to public and private clients spanning multiple industries; legal advisory services in Germany are provided by Deloitte Legal. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte’s approximately 312,000 professionals are committed to making an impact that matters.

This presentation contains general information only, and none of Deloitte Consulting GmbH or Deloitte Touche Tohmatsu Limited (“DTTL”), any of DTTL’s member firms, or any of the foregoing’s affiliates (collectively, the “Deloitte Network”) are, by means of this presentation, rendering professional advice or services. In particular this presentation cannot be used as a substitute for such professional advice. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this presentation. This presentation is to be treated confidential. Any disclosure to third parties – in whole or in part – is subject to our prior written consent.

For further information please contact Deloitte Consulting GmbH .

Gesellschaftssitz Wien | Handelsgericht Wien | FN 212552 b

© 2026 Deloitte Consulting GmbH