KOOPERATIONS PARTNER TÜV HESSEN

CARMAO 20 JAHRE
INTELLIGENT. EINFACH. PREMIUM.

KI und IT-Sicherheit – Partner oder Feinde?

KOOPERATIONS PARTNER TÜV HESSEN

CARMAO 20 JAHRE
INTELLIGENT. EINFACH. PREMIUM.

Unser **Unternehmenssitz**

Tradition trifft **Hightech**

- Im denkmalgeschützten Walderdorffer Hof in **Limburg an der Lahn**
- **Ideale Anbindung** (Bahn, Flug, PKW) im Drehkreuz zwischen Frankfurt am Main und Köln

KOOPERATIONS PARTNER TÜV HESSEN

CARMAO 20 JAHRE
INTELLIGENT. EINFACH. PREMIUM.

Wir verhelfen seit 20 Jahren jeder Organisation zu Resilienz, Sicherheit und Wirtschaftlichkeit für nachhaltigen Erfolg!

Schwerpunkte

Unsere Expertise ist Ihre Sicherheit!

Unternehmensresilienz

- **Informationssicherheit**
- **Risikomanagement**
- **Business-** und **IT-Service-Continuity-Management**
- **Datenschutz** & Compliance

Academy for Organizational Resilience

- Personen-Zertifizierungen – in Präsenzkursen und im eLearning
- Gezielte Entwicklung von Fach- und Führungskräften
- Maßgeschneiderte Programme zum Aufbau fachlicher, methodischer und sozialer Kompetenzen
- Academy for Organizational Resilience ist Partner der **PECB University** im Rahmen des Executive MBA Programms.

Kompetenz-Netzwerk

Gemeinsam noch stärker

- **Strategische Partner**
  - bits&vision eG
  - TÜV Hessen
  - PECB
  - PECB University
- **Verbandsmitgliedschaften**
  - Allianz für Cyber-Sicherheit (BSI)
- **Lösungspartner**
  - SerNet, Avedos, CONTECHNET, Compliance Aspekte, RSA, WMC, CISS, …

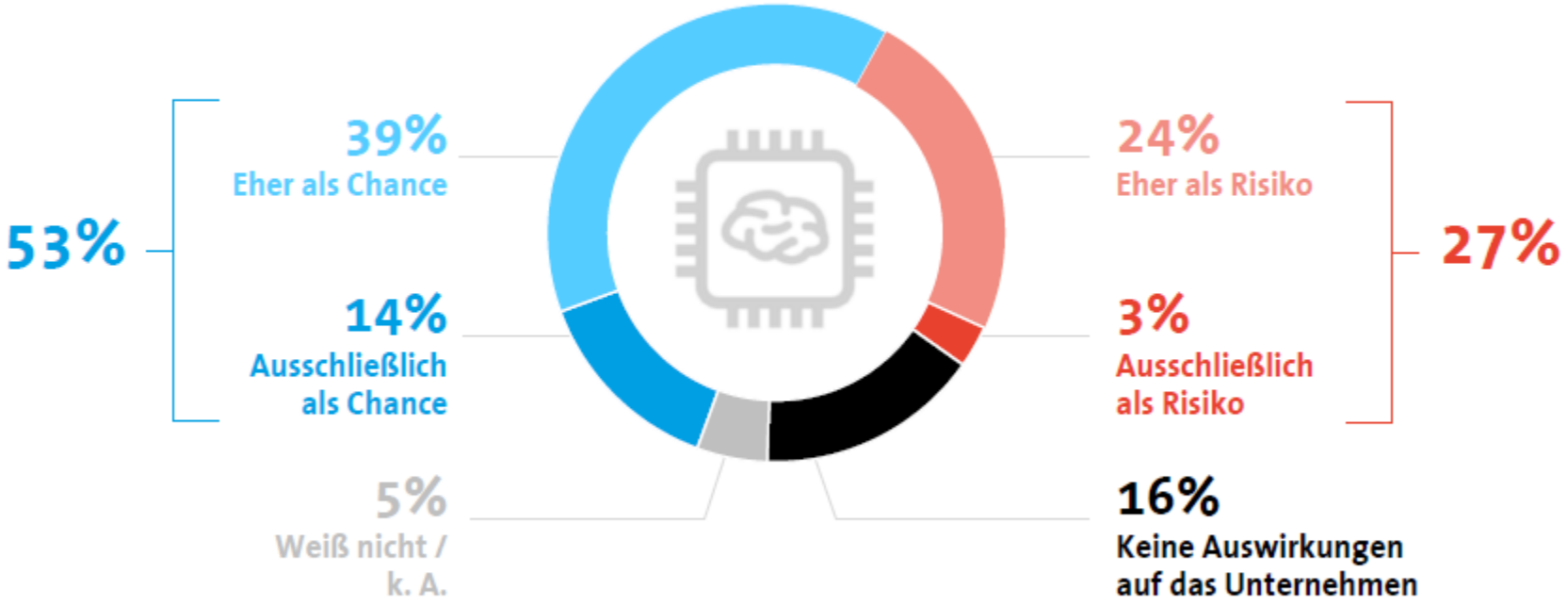
KOOPERATIONS PARTNER TÜV HESSEN

CARMAO 20 JAHRE
INTELLIGENT. EINFACH. PREMIUM.

KI und IT-Sicherheit

Mehrheit sieht Künstliche Intelligenz als Chance

Sehen sie Künstliche Intelligenz eher als Chance oder eher als Risiko für ihr Unternehmen?



11 Basis: Alle befragten Unternehmen (n=606) | Abweichungen zu 100 Prozent rundungsbedingt | Quelle: Bitkom Research

bitkom

Zwischen Wunsch und Wirklichkeit

- Unsichere Begriffsverwendungen
- Stochastik vs. Muster vs. Kreativität
- Mangelnde Transparenz
- Marketing-Aussagen von Herstellern

Intelligenz?

- **Oxford English Dictionary**

  KI ist die Theorie und Entwicklung von Computer-systemen, die in der Lage sind, Aufgaben durchzuführen, die in der Regel menschliche Intelligenz erfordern, wie z.B. die visuelle Wahrnehmung, Spracherkennung, Entscheidungsfindung, Übersetzungen zwischen Sprachen

- **Entscheidend ist Problemlösungsfähigkeit bei nicht standardisierten Aufgabenstellungen**

Betrachtungsebenen

- Angriffe durch KI
- IT-Sicherheit durch KI
- IT-Sicherheit für KI
- Informationssicherheit durch KI
- Datenschutz und KI

Angriffe durch KI

- **Angriffssteuerung**
  - Koordination bei DDOS-Angriffen
  - Adaptive Malware-Angriffe (inkl. Re-Programmierung der Software), bspw lernende Phishing-Attacken
  - Data Poisening (Lerndatenbestände, Bilddaten, Eingabe-/Steuerungsdaten)
- **Seitenkanal-Attacken gegen kryptografische Algorithmen**
  - Rechenzeitangriff, Gemeinsame Speichernutzung, Simple Power Analysis, Diffential Power Analysis, elektomagnetische Abstrahlung, Schallanalyse, etc
- **Deep Fake / Audio Deepfake**
  - Generative Adversarial Network (GAN) [Generator Net + Diskiminator Net]
- **Fake News / Rufmord**

KOOPERATIONS PARTNER TÜV HESSEN

CARMAO 20 JAHRE
INTELLIGENT. EINFACH. PREMIUM.

IT-Sicherheit durch KI

- **Analysen zur Anomalie-Erkennung**
  - **Erkennung von Advanced Persistent Threads**
  - Verdächtige Event-Sequenzen in Logfiles (SIEM-UseCases)
  - Anomalien im Netzwerk-Traffic
  - Anomalien in Konfigurationsdateien
  - Netzwerk-Routing-Analysen bei Angriffen
- **Analyse von Deep Fake / Audio Deep Fake Angriffen**
  - Herausforderung: Echtzeit-Analyse während des Gesprächs
- **Software-Entwicklung / Security-by-Design**
  - Code Optimierung, Threat Modelling

Informationssicherheit durch KI

- **Generierung von Informationssicherheitsrichtlinien und Verfahrensanleitungen**
  - Analog zur Generierung von Gesetzestexten
- **Unterstützung bei Risikoanalyse**
  - Ermittlung Eintrittswahrscheinlichkeiten und Schadensauswirkungen
- **Unterstützung bei Ermittlung von Risikobehandlung**
  - Identifikation von Schutzmaßnahmen zu Risikoszenarien
- **Unterstützung bei System-Audits**
  - Analyse Dokumentation, Logfiles, Systemkonfigurationen, IKS-Kontrollen

Informationssicherheit durch KI

- **Analyse / Überwachung von Berechtigungsvergaben für Access Management Governance**
  - Passen Berechtigungen zu den Aufgaben / Stellenbeschreibungen

Datenschutz und KI

- **Internet**
  - Social Media Recherchen
  - Bilderkennung
- **Automatisierte Entscheidungen**
  - Rechtssichere Fallbearbeitungen bspw. bei Sachschäden (Versicherungen)
  - Vorqualifizierung / Selektion von Bewerbern
- **Identitätsdiebstahl**
  - Missbrauch Bilder / Audioaufnahmen für den illegalen Einsatz von Deep Fake, Audio Deep Fake

Hauptfaktor bleibt der Mensch

- KI kann schneller reagieren als der Mensch und die IT-Sicherheit verbessern
  - Dennoch **kann sie den Menschen nicht ersetzen**. Auf der einen Seite braucht es **ausgebildete IT-Sicherheitsfachkräfte**, um aus den Ergebnissen und Funden des Systems die richtigen Schlüsse zu ziehen.
  - KI-Systeme sind bislang nicht universell einsetzbar, sondern auf bestimmte Bereiche spezialisiert. KI bleibt nach aktuellem Stand ein **Mittel zum Zweck** zur Unterstützung von Entscheidungen.
- Auch ein KI-System kann gehackt werden, wenn Mitarbeitende Opfer von Cyberattacken werden und unwissentlich oder unabsichtlich Zugänge rausgeben. Einer der wichtigsten Faktoren ist und bleibt deshalb die Sensibilisierung und entsprechende Schulung aller Mitarbeitenden, um die Sicherheitssysteme zu schützen.

Vielen Dank für Ihre Aufmerksamkeit

Sie haben noch Fragen?

Wir stehen Ihnen gerne zur Verfügung.

Ulrich HEUN

Geschäftsführender Gesellschafter

Telefon: +49 6431 2196-0

E-Mail: ulrich.heun@carmao.de

CARMAO GmbH | Walderdorffer Hof | Fahrgasse 5 | 65549 Limburg