Praxistipps

- **Schaffen Sie Awareness für KI:** Schulen Sie Ihre Mitarbeitenden zu den Fähigkeiten und Risiken von KI und wie sie KI-basierte Angriffe wie Deepfakes erkennen können. Für Early Adopter sollte die Sicherheit bei der Entwicklung, Implementierung und Wartung von KI-Technologien an oberster Stelle stehen.
- **Definieren Sie KI-Zuständigkeiten:** Etablieren Sie einen Governance-Ausschuss und Verwaltungsprozesse für alle KI-Lösungen innerhalb Ihrer Organisation. Führen Sie Inventar zu Ihren KI-Tools, bestimmen Sie Verantwortliche, bewerten Sie Risiken und arbeiten Sie Recovery-Pläne für mögliche Zwischenfälle aus. Etablieren Sie Mechanismen zur Überwachung neuer Risiken bei der Nutzung von KI in Ihrer Organisation. Nutzen Sie Richtlinien wie ISO 420001 als Ausgangspunkt.
- **Vermeiden Sie die Nutzung einer Standard-KI:** Eine einzige KI, die Zugriff auf alle Daten hat, kann zwar die Nutzererfahrung verbessern, sie birgt jedoch auch massive Risiken. Isolieren Sie Trainings-Datensätze, um zu vermeiden, dass beispielsweise Lagerarbeiter Zugang zum Netzwerkdesign haben oder ein Entwickler versehentlich HR-Daten freilegt. Nutzen Sie spezialisierte KIs, anstatt eines allgemeinen Systems.
- **Stärken Sie Ihre Sicherheits-Basics:** Optimieren Sie Ihre grundlegenden Schutzmechanismen, wie Least-Privilege-Zugriff, Trennung von Verantwortlichkeiten, regelmäßige Prüfungen von Zugriffsrechten, MFA und Patching. Stellen Sie sicher, dass Sie einen soliden Incident Response Plan haben, der regelmäßig überarbeitet wird.
- **Wenden Sie bestehende Richtlinien auf KI an:** Behandeln Sie KI-Outputs und KI-bezogene Entscheidungen aus dem Gesichtspunkt bewährter Richtlinien. Stellen Sie sicher, dass Ihre KI-Systeme DSGVO-Vorgaben und andere Frameworks erfüllen, indem Sie Audit-fähige Aufzeichnungen führen und Zuständigkeiten klar definieren.

Welche Aspekte KI-getriebener Angriffe beunruhigen Sie am meisten, falls überhaupt?

	Alle	DACH	AUS	FR	GB	BENELUX
Erschwerte Zurückverfolgung von Angriffen	50,8 %	54 %	52 %	52 %	55 %	41 %
Aufkommen völlig neuer Angriffsmethoden	44,8 %	38 %	43 %	56 %	45 %	42 %
Täuschungskraft KI-generierter Inhalte	41,6 %	36 %	44 %	40 %	45 %	43 %
Präzision der Zielsetzung	41,4 %	48 %	49 %	33 %	46 %	31 %
Schlechte Vorbereitung und fehlende KI-Bedrohungserkennungstools	38,8 %	41 %	48 %	37 %	29 %	39 %
Umfang und Schnelligkeit automatisierter Angriffe	38 %	32 %	43 %	38 %	38 %	39 %