#008 KI als Chance

KI gegen Cybercrime

Sehr geehrte Kolleginnen und Kollegen,

Cybercrime zählt zu den größten Bedrohungen für Banken und Finanzdienstleister. Die wirtschaftlichen Schäden gehen jährlich in die Milliarden. Entsprechend entwickelt die Finanzbranche ihre Präventions- und Abwehrstrategien konsequent weiter.

Dabei kommt zunehmend KI zum Einsatz: Sie bietet erhebliche Chancen, Cybercrime zu erkennen und Gegenmaßnahmen zielgerichtet einzuleiten. Typische Einsatzfelder sind

- das Erkennen von Anomalien und Mustern,
- die Identifikation von Phishing und Malware ,
- die Analyse (auffälligen) Benutzerverhaltens.
- die Aufklärung von Cyber-Bedrohungen sowie
- die Reaktion auf Sicherheitsvorfälle.

Um Cyber-Angriffen wirksam vorzubeugen, setzt auch die Atruvia AG auf KI. Dabei ist klar: **Der sichere und rechtskonforme Einsatz von KI erfordert eine belastbare Governance-Architektur, in der sowohl Atruvia als auch die nutzende Bank eingebunden sind.**

Ohne definierte Verantwortlichkeiten, Kontrollen und Dokumentationsstandards **auf beiden Ebenen** kann KI selbst zu einem Risiko werden und im ungünstigsten Fall neue Angriffsflächen eröffnen.

Besonderheit genossenschaftliche FinanzGruppe

Die KI-VO unterscheidet, wer das **KI-System entwickelt, bereitstellt bzw. herstellt.** Wichtig ist hierbei die Begriffsdefinition gem. Art. 3 KI-VO. Danach könnte auch die Bank in die Anbieterrolle wechseln, weil sich z. B. die Atruvia in der Entwicklerrolle und nicht in der Anbieterrolle sieht. In den meisten Fällen ist jedoch davon auszugehen, dass die **Bank die Betreiberrolle** einnimmt.

Voraussetzung ist, dass die von Atruvia entwickelte KI-Anwendung nicht Dritten angeboten und lediglich zu internen Zwecken verwendet wird. Dies trifft i. d. R. bei den Atruvia-Lösungen zur Cybercrime-Abwehr zu. Wir empfehlen jedoch, die Unterlagen zum KI-Assetbezug genau zu prüfen und bei Bedarf direkt die Kontaktaufnahme zum Dienstleister vorzunehmen.

Betreiberpflichten bei Cybersecurity-KI-Systemen

Für die Bank impliziert die Rolle des Betreibers sogenannte Betreiberpflichten. **Diese sind insbesondere dann von hoher Relevanz, wenn ein KI-System als Hochrisiko-KI-System einzustufen ist.** Nach der KI-VO ist eine solche Einstufung nicht pauschal für jede Cybersecurity-Anwendung in Betracht zu ziehen. Wohl aber für bestimmte Anwendungsfälle mit erhöhtem Gefährdungspotenzial, beispielsweise wenn ein Zugriff auf privilegierte Benutzerkonten (z. B. Admin-Konten) eingeräumt wird. >

vertrieb@dz-cp.de
www.dz-cp.de

Betreiber von Hochrisiko-KI-Systemen sind verpflichtet, geeignete Maßnahmen zu ergreifen, u. a.:

1. **Technische und organisatorische Maßnahmen**
2. **Menschliche Aufsicht** (Human-in-the-Loop)
3. **Protokollierung in einem KI-Register**
4. **Meldung von Vorfällen**
5. **Schulung**

Die wichtigsten ToDos auf einen Blick

- Risikobewertung der eingesetzten KI-Systeme zur Cybercrime-Bekämpfung
- Prüfung der DSGVO-Rechtsgrundlage (inkl. AV-Verträge, Informationspflichten)
- Dokumentation und Protokollierung jeder sicherheitsrelevanten KI-gestützten Entscheidung
- Integration in bestehende Governance-Strukturen (z. B. ISMS-/IKT-Risikomanagement, BCM)
- Schulung von Security- und Compliance-Teams im Umgang mit KI-basierten Sicherheitssystemen

Fazit

KI bietet erhebliche Chancen, die Cyber-Abwehr in Banken wirksamer zu gestalten. Gerade in arbeitsteiligen Strukturen wie der genossenschaftlichen FinanzGruppe entbindet **der Einsatz zentral bereitgestellter KI-Lösungen die einzelne Bank jedoch nicht von ihrer eigenen regulatorischen Verantwortung**.

Entscheidend ist, den KI-Einsatz nicht nur technologisch, sondern auch organisatorisch und rechtlich sauber aufzustellen. Nur wenn Rollen, Pflichten und Kontrollen klar definiert sind, kann KI ihr Potenzial in der Cybersecurity voll entfalten, ohne selbst zum Risiko zu werden.

Weitere Fachinformationen zum sicheren Einsatz von KI im Bankenumfeld finden Sie auch online:
https://www.dz-cp.de/ki-ready

Björn Blechenberg
Marketing & Vertrieb
069 580024-172
bjoern.blechenberg@
dz-cp.de

Benjamin Wellnitz
IKT-Compliance &
Datenschutz
069 580024-246
benjamin.wellnitz@
dz-cp.de