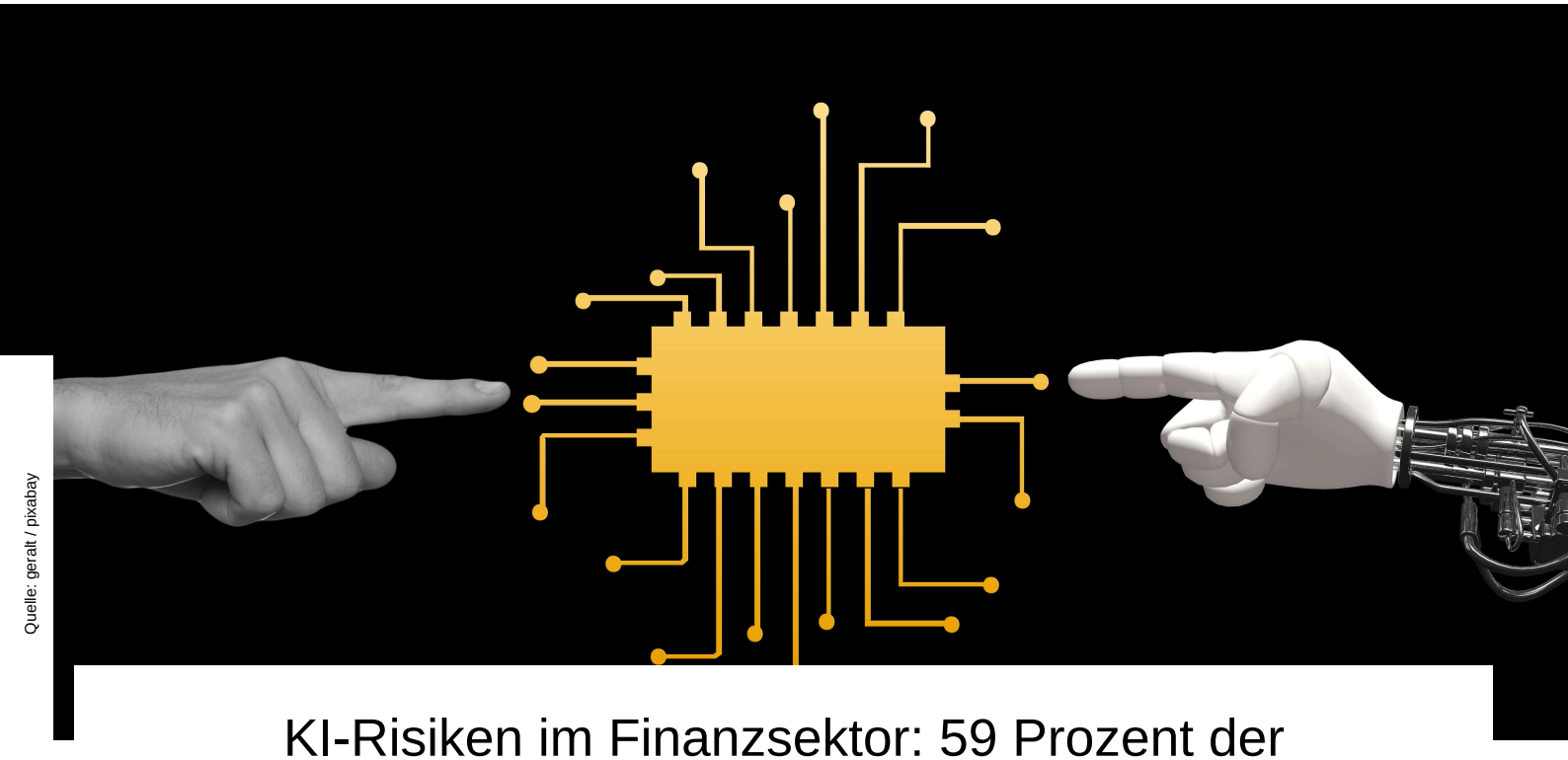
expertenReport



Quelle: geralt / pixabay

KI-Risiken im Finanzsektor: 59 Prozent der Datenverstöße betreffen regulierte Daten

Michael Fiedler

Die Nutzung generativer KI hat in der Finanzbranche stark zugenommen – doch mit der Verbreitung wachsen auch die Risiken. Eine aktuelle Analyse zeigt: Besonders betroffen sind sensible, regulatorisch geschützte Finanzdaten.

Regulierte Daten besonders gefährdet

Die zentrale Erkenntnis des Reports: 59 Prozent aller Datenschutzverstöße im Zusammenhang mit generativer KI betreffen regulierte Finanzdaten. Damit sind genau jene Informationen betroffen, die unter Aufsicht von Regulierungsbehörden wie BaFin, EBA oder im Rahmen von DORA besonders geschützt werden müssen. Weitere Verstöße entfallen auf geistiges Eigentum (20 Prozent), Quellcode (11 Prozent) sowie Zugangsdaten wie Passwörter oder API-Keys (9 Prozent). Besonders kritisch: 94 Prozent der Nutzenden greifen auf GenAI-Anwendungen zurück, die eingegebene Daten potenziell für das Training von Modellen verwenden.

Neue Risikozone durch parallele Nutzung

Während die Branche Fortschritte beim Eindämmen sogenannter „Shadow AI“ erzielt hat, entsteht gleichzeitig eine neue Herausforderung. Der Anteil der Beschäftigten, die ausschließlich private GenAI-Accounts nutzen, ist deutlich gesunken – von 76 auf 36 Prozent. Gleichzeitig stieg die Nutzung unternehmenseigener Lösungen auf 79 Prozent. Doch genau hier entsteht eine neue Grauzone: Immer mehr Mitarbeitende wechseln regelmäßig zwischen privaten und unternehmenseigenen Anwendungen. Dieser Anteil stieg von 9 auf 15 Prozent. Damit bewegen sich sensible Daten potenziell zwischen kontrollierten und unkontrollierten Umgebungen – ein Risiko, das mit klassischen Sicherheitsmechanismen nur schwer zu adressieren ist.

KI-Tools: Nutzung und Sperrungen

Bei den eingesetzten Anwendungen dominiert weiterhin ChatGPT mit einer Organisationsreichweite von 76 Prozent, gefolgt von Google Gemini mit 68 Prozent. Gleichzeitig greifen viele Institute aktiv in die Tool-Nutzung ein: Anwendungen wie ZeroGPT (46 Prozent), DeepSeek (44 Prozent) und PolitePost (43 Prozent) werden häufig blockiert. Die vergleichsweise hohe Blockquote von DeepSeek deutet darauf hin, dass Finanzinstitute geopolitische Risiken bei KI-

Anbietern zunehmend eigenständig bewerten – noch bevor regulatorische Vorgaben greifen.

Cloud-Dienste als Angriffspunkt

Neben GenAI-Risiken rückt auch die Nutzung von Cloud-Plattformen in den Fokus. Angreifer nutzen zunehmend etablierte Dienste zur Verbreitung von Schadsoftware. So ist GitHub bei 11 Prozent der betroffenen Organisationen die am häufigsten missbrauchte Plattform, gefolgt von Microsoft OneDrive mit 8 Prozent. Schadsoftware wird dabei gezielt in legitime Infrastrukturen eingebettet, um im regulären Datenverkehr unauffällig zu bleiben.

Mehrschichtige Sicherheitsstrategien erforderlich

Ray Canzanese, Director der Netskope Threat Labs, sieht insbesondere die Überschneidung zwischen privater und geschäftlicher Nutzung als kritischen Faktor: „Da Finanzinstitute den Einsatz generativer KI vorantreiben, vergrößern sie gleichzeitig die Anzahl der Wege, über die sensible Daten offengelegt werden können.“ Der Umstieg auf unternehmenseigene Lösungen sei zwar ein wichtiger Schritt, reiche jedoch allein nicht aus. Entscheidend sei ein mehrschichtiger Ansatz, der sowohl Datenverkehr überwacht als auch Anwendungen kontrolliert und gezielt Maßnahmen zur Verhinderung von Datenverlust einsetzt.

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4949172/KI-Risiken-im-Finanzsektor-59-Prozent-der-Datenverstoesse-betreffen-regulierte-Daten/