



Quelle: Quelle: links: Bafin/Matthias Sandmann und rechts: Bundesbank/ Gaby Gerster

BaFin warnt vor KI-Risiken: Cybersicherheit wird zur Belastungsprobe für den Finanzsektor

Dirk Stein

Knapp 900 gemeldete IT-Vorfälle innerhalb von vier Quartalen, neue Risiken durch künstliche Intelligenz und wachsende Abhängigkeiten von internationalen Technologieanbietern: Auf der Digital Finance Conference 2026 (DigiFin26) in Berlin haben BaFin-Präsident Mark Branson und Bundesbank-Vorständin Fritzi Köhler-Geib vor den Herausforderungen für die Sicherheit und Stabilität des europäischen Finanzsystems gewarnt. Während die BaFin ihre Cyberaufsicht ausbauen will, verweist die Bundesbank auf die wirtschaftlichen Folgen technologischer Abhängigkeiten.

BaFin registriert knapp 900 IT-Vorfälle

„Jetzt ist nicht die Zeit für Naivität“, erklärte BaFin-Präsident Mark Branson auf der DigiFin26 am 10. November 2026. Seine Warnung richtete sich insbesondere auf die Risiken, die mit dem zunehmenden Einsatz künstlicher Intelligenz und der Entwicklung leistungsfähiger Quantencomputer verbunden sind.

Innerhalb von vier Quartalen wurden der Finanzaufsicht knapp 900 IT-Vorfälle gemeldet. Lediglich 14 Prozent davon waren direkte Cyberangriffe. Der überwiegende Teil entfiel somit auf andere IT-Störungen, die den Geschäftsbetrieb ebenfalls erheblich beeinträchtigen können.

Für Banken und Versicherer ist diese Unterscheidung wesentlich. Die Sicherheit digitaler Geschäftsprozesse hängt nicht allein vom Schutz vor kriminellen Angriffen ab. Auch technische Fehler, Systemausfälle und Störungen bei externen Dienstleistern können die Verfügbarkeit wichtiger Anwendungen gefährden. Die gemeldeten Vorfälle lassen allerdings keinen Rückschluss auf die Gesamtzahl sämtlicher Cyberangriffe zu, da die Statistik nur meldepflichtige Ereignisse erfasst.

Die BaFin will deshalb ihre Cyberaufsicht ausbauen und künftig verstärkt kürzere, gezielte Prüfungen durchführen. Damit soll schneller auf neue Risiken und technische Entwicklungen reagiert werden können.

Branson kritisiert die Prioritäten bei IT-Investitionen

Besonders deutlich wurde Branson bei der Frage, welchen Stellenwert die Absicherung neuer Technologien innerhalb der Investitionsentscheidungen einnimmt.

„Wenn nur ein Bruchteil der gigantischen Investitionen in KI-Kapazitäten für Cybersicherheit aufgewendet würde, wäre die Finanzwelt ein viel sichererer Ort“, erklärte der BaFin-Präsident.

Seine Kritik betrifft das Verhältnis zwischen dem Ausbau technologischer Leistungsfähigkeit und den dafür erforderlichen Sicherheitsmaßnahmen. Finanzunternehmen integrieren zunehmend KI-Anwendungen in ihre Geschäftsprozesse, während gleichzeitig neue Abhängigkeiten und Angriffsflächen entstehen.

Für Versicherer betrifft dies insbesondere die Bestandsverwaltung, die Verarbeitung sensibler Kundendaten und automatisierte Entscheidungen. Die Einführung neuer Technologien muss dabei mit bestehenden Sicherheitsanforderungen und häufig über Jahrzehnte gewachsenen IT-Systemen vereinbart werden.

Bundesbank sieht wachsende Risiken durch beschleunigte Cyberangriffe

Bundesbank-Vorständin Prof. Dr. Fritzi Köhler-Geib ergänzte Bransons Warnungen um die Entwicklung der Cyberbedrohung und die wirtschaftlichen Abhängigkeiten des europäischen Finanzsektors.

Dabei verwies sie auf die zunehmende Geschwindigkeit, mit der Sicherheitslücken ausgenutzt werden können. Für Finanzunternehmen verkürzt sich damit die Zeit, in der sie auf neu erkannte Schwachstellen reagieren müssen. Die Entwicklung stellt insbesondere Unternehmen mit komplexen IT-Landschaften und zahlreichen externen Schnittstellen vor zusätzliche Herausforderungen.

Köhler-Geib ordnete diese Risiken in einen größeren wirtschaftlichen Zusammenhang ein. Neben technologischen Veränderungen seien auch geopolitische Spannungen und wirtschaftspolitische Unsicherheiten entscheidende Faktoren für die Widerstandsfähigkeit des europäischen Finanzsystems.

Europas Abhängigkeit von Technologieanbietern

Ein wesentlicher Teil der digitalen Infrastruktur Europas wird von außereuropäischen Unternehmen bereitgestellt. Dazu gehören Cloud-Dienste, Rechenzentren, Softwareplattformen und zunehmend auch leistungsfähige KI-Systeme.

Köhler-Geib verwies in ihrer Rede auf die hohe Abhängigkeit Europas von internationalen Technologieanbietern. Die Konzentration auf wenige Unternehmen sei nicht allein eine Frage der technischen Sicherheit, sondern berühre auch die wirtschaftliche Handlungsfähigkeit.

Für Banken und Versicherer entstehen daraus besondere Anforderungen. Die Auslagerung von IT-Leistungen ermöglicht eine effizientere Nutzung technischer Ressourcen und kann Investitionskosten reduzieren. Gleichzeitig steigt die Abhängigkeit von der Verfügbarkeit, den Sicherheitsstandards und den vertraglichen Bedingungen der jeweiligen Dienstleister.

Störungen bei einem großen Cloud-Anbieter können zahlreiche Finanzunternehmen gleichzeitig betreffen. Hinzu kommt die Frage, in welchem Umfang sich kritische Anwendungen kurzfristig auf andere Anbieter übertragen lassen.

Die Bundesbank sieht deshalb in der Stärkung europäischer technologischer Kompetenzen einen wichtigen Bestandteil langfristiger wirtschaftlicher Resilienz. Köhler-Geib nannte in diesem Zusammenhang insbesondere Halbleiter, Cloud-Infrastrukturen, künstliche Intelligenz, Robotik und Quantencomputing.

Quantencomputing stellt langfristigen Datenschutz vor neue Aufgaben

Ein weiterer Schwerpunkt der DigiFin26 war die Entwicklung des Quantencomputings. Branson empfahl, besonders kritische Systeme bis 2030 auf quantenresistente Verschlüsselungsverfahren umzustellen.

Hintergrund ist die Möglichkeit, dass künftig ausreichend leistungsfähige Quantencomputer bestimmte heute gebräuchliche kryptografische Verfahren überwinden können. Betroffen wären insbesondere Verfahren, die zur sicheren Übertragung und Authentifizierung vertraulicher Informationen eingesetzt werden.

Auch die Bundesbank beschäftigt sich bereits mit quantensicheren Verschlüsselungsverfahren. Dabei geht es unter anderem um die Entwicklung und Erprobung neuer technischer Lösungen für die langfristig sichere Kommunikation.

Für die Versicherungswirtschaft stellt sich die Frage nach dem dauerhaften Schutz personenbezogener Daten. Gesundheitsinformationen, Vertragsunterlagen und andere sensible Angaben müssen teilweise über Jahrzehnte hinweg vertraulich bleiben. Entsprechend reicht es nicht aus, ausschließlich die gegenwärtige Sicherheit eingesetzter Verschlüsselungsverfahren zu beurteilen.

Die von Branson genannte Jahreszahl 2030 ist dabei als Empfehlung für besonders kritische Systeme einzuordnen. Eine allgemeine gesetzliche Verpflichtung, sämtliche IT-Systeme bis zu diesem Zeitpunkt umzustellen, ergibt sich daraus nicht.

DORA und KI-Aufsicht erweitern die Verantwortung der Unternehmen

Mit dem seit Januar 2025 geltenden Digital Operational Resilience Act (DORA) bestehen bereits europaweit verbindliche Anforderungen an die digitale Widerstandsfähigkeit von Finanzunternehmen. Dazu gehören das Management von IT-Risiken, die Meldung schwerwiegender Vorfälle, Resilienztests und die Überwachung externer IT-Dienstleister.

Für Banken und Versicherer bedeutet dies, dass die Verantwortung für die Sicherheit ausgelagerter Geschäftsprozesse weiterhin bei den Unternehmen liegt. Die Nutzung externer Cloud-Dienste entbindet sie nicht von ihren aufsichtsrechtlichen Pflichten.

Der zunehmende Einsatz künstlicher Intelligenz erweitert zugleich die Anforderungen an Kontrollverfahren, Datenqualität und die Nachvollziehbarkeit automatisierter Entscheidungen. Das betrifft sowohl interne Anwendungen als auch KI-Systeme, die unmittelbar in Geschäftsprozesse und Kundenentscheidungen eingebunden sind.

Bitkom-Umfrage: 92 Prozent wollen einen Not-Aus-Schalter für KI

Wie die Bevölkerung die Entwicklung künstlicher Intelligenz beurteilt, zeigt eine am 10. November veröffentlichte repräsentative Bitkom-Befragung. Dafür wurden 1.006 Menschen ab 16 Jahren in Deutschland telefonisch befragt.

Demnach fordern 92 Prozent der Befragten einen Not-Aus-Schalter für sämtliche KI-Systeme. 85 Prozent wünschen sich strengere Regeln für besonders leistungsfähige künstliche Intelligenz. Gleichzeitig befürchten 49 Prozent, dass selbstständig handelnde KI die Menschheit auslöschen könnte.

Trotz dieser Sorgen betrachtet eine Mehrheit von 56 Prozent künstliche Intelligenz grundsätzlich eher als Chance denn als Risiko.

Besonders deutlich sind die Unterschiede zwischen den Generationen. Während 58 Prozent der 16- bis 29-Jährigen selbstständig handelnden KI-Systemen zuversichtlich gegenüberstehen, überwiegt bei 62 Prozent der Menschen ab 65 Jahren die Sorge.

Bitkom-Präsident Ralf Wintergerst verwies angesichts der Ergebnisse auf die Bedeutung von Sicherheitsstandards und internationaler Zusammenarbeit. Die Bundesregierung habe mit dem KI-Sicherheitsinstitut AISI Deutschland ein entsprechendes Signal gesetzt.

Die Befragung dokumentiert die Einstellungen der Bevölkerung. Aussagen über die tatsächliche Wahrscheinlichkeit der befürchteten Gefahren lassen sich daraus nicht ableiten.

Cybersicherheit wird zur Frage wirtschaftlicher Handlungsfähigkeit

Die Beiträge von Branson und Köhler-Geib auf der DigiFin26 verdeutlichen, dass die technologische Entwicklung für den Finanzsektor mit unterschiedlichen Anforderungen verbunden ist. Neue Anwendungen sollen die Produktivität erhöhen und bestehende Geschäftsprozesse verbessern. Gleichzeitig wachsen die Anforderungen an deren Sicherheit, Kontrollierbarkeit und dauerhafte Verfügbarkeit.

Für Banken, Versicherer und ihre IT-Dienstleister betrifft dies sowohl Investitionsentscheidungen als auch die Organisation des laufenden Geschäftsbetriebs. Die Abhängigkeit von wenigen Technologieanbietern, der Einsatz zunehmend autonomer KI-Systeme und die langfristige Sicherheit vertraulicher Daten lassen sich dabei nicht unabhängig voneinander betrachten.

Während die BaFin ihre Aufsicht entsprechend ausrichten will, stellt die Bundesbank die Frage nach Europas technologischer und wirtschaftlicher Handlungsfähigkeit. Beide Perspektiven treffen dort aufeinander, wo digitale Geschäftsmodelle auf Infrastrukturen angewiesen sind, deren Funktionsfähigkeit und Sicherheit die Unternehmen selbst nur begrenzt beeinflussen können.

Quellen:

Bitkom / DigiFin26: „Zwischen Innovation, Souveränität und Resilienz: Das war die DigiFin26!“ – für Bransons Aussagen und den Konferenzbericht.

Deutsche Bundesbank: Originalrede von Fritzi Köhler-Geib vom 10. November 2026.

Bitkom Research: „Deutsche wünschen sich mehr KI-Sicherheit“ vom 10. November 2026.

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4952978/bafin-cyberaufsicht-ki-risiken-digifin26/