ÖSTERREICHISCHE FMA · FINANZMARKTAUFSICHT

OESTERREICHISCHE NATIONALBANK
EUROSYSTEM

Wien, am 10.07.2026

Umgang mit KI-gestützten Cybersicherheitsbedrohungen – aufsichtliche Erwartungen

Sehr geehrte Damen und Herren,

die Finanzmarktaufsicht (FMA) und die Oesterreichische Nationalbank (OeNB) möchten auf aktuelle Entwicklungen im Bereich KI-gestützter Cybersicherheitsbedrohungen aufmerksam machen, auf den am 07.07.2026 veröffentlichten „Dear CEO"-Letter der EZB und die am gleichen Tag veröffentlichte Warnung des ESRB zu Frontier AI Models hinweisen und ihre aufsichtliche Erwartungshaltung im Hinblick auf diese Entwicklungen darlegen.
Die raschen Fortschritte leistungsfähiger Modelle der künstlichen Intelligenz führen zu einer nachhaltigen Veränderung der Cybersicherheitslandschaft. Moderne KI-Systeme können die Identifikation von Schwachstellen, die Entwicklung von Angriffsvektoren sowie die Durchführung von Cyberangriffen erheblich beschleunigen und skalieren. Dadurch kann sich die Zeitspanne zwischen der Entdeckung einer Schwachstelle und deren möglicher Ausnutzung auf wenige Stunden verkürzen. Gleichzeitig können Angriffe komplexer, zielgerichteter und automatisierter erfolgen. Diese Entwicklungen stellen kein völlig neues Risiko dar, erhöhen jedoch Umfang und potenzielle Auswirkungen bestehender Cyberrisiken erheblich. Die Bedrohung betrifft grundsätzlich alle beaufsichtigten Unternehmen, unabhängig von Geschäftsmodell, Größe oder Sektor.
Es wird darauf hingewiesen, dass die bereits bestehenden regulatorischen Anforderungen im Bereich des IKT-Risikomanagements (DelVO 2024/1774) und der digitalen operationalen Resilienz vor dem Hintergrund dieser Entwicklungen von hoher Bedeutung sind. Insbesondere liefern die Anforderungen der Verordnung über die digitale operationale Resilienz im Finanzsektor (DORA) bereits jetzt einen geeigneten Rahmen, um Risiken aus KI-gestützten Cyberbedrohungen angemessen zu identifizieren, zu bewerten, zu steuern und zu überwachen.
Es wird daher erwartet, dass beaufsichtigte Unternehmen die Auswirkungen dieser veränderten Bedrohungslage im Rahmen ihrer bestehenden Governance-, Risiko- und Kontrollsysteme angemessen berücksichtigen. Dabei sollen Art, Umfang, Komplexität und Risikoprofil des jeweiligen Unternehmens sowie die Kritikalität der eingesetzten IKT-Systeme und Dienstleistungen berücksichtigt werden. Die konkrete Ausgestaltung entsprechender Maßnahmen bleibt den Unternehmen im Rahmen des Proportionalitätsprinzips überlassen.
Folgende Themenbereiche sollten auf Basis der veränderten Risikolandschaft reevaluiert werden:

a) die Erhöhung der Wirksamkeit bestehender Verfahren zur Schwachstellenidentifikation und zum Patch-Management (bis hin zur (Teil-)Automatisierung dieser Prozesse) und der damit verbundenen höheren Ressourcenausstattung;
b) die bestmögliche Reduktion der Angriffsfläche insb. auch in Bezug auf Altsysteme;
c) die Fähigkeit zur zeitnahen Erkennung, Analyse und Behandlung von Cybervorfällen insbesondere aufgrund von Zero-Day Sicherheitslücken;
d) die Widerstandsfähigkeit kritischer Geschäftsprozesse einschließlich aktualisierter Notfall-, Wiederherstellungs- und Krisenmanagementvorkehrungen;

e) die Überprüfung von Softwareentwicklungsprozessen unter Berücksichtigung aktueller Bedrohungen, einschließlich KI-bezogener Risiken, unter Wahrung des Schutzes vertraulichen Quellcodes;
f) die laufende Sensibilisierung von Leitungsorganen, Führungskräften und Mitarbeitenden für aktuelle Cyberbedrohungen und deren mögliche Auswirkungen auf das Unternehmen;
g) und die Sicherstellung dieser Anforderungen auch bei Übertragung von Aufgaben an IKT-Drittdienstleister innerhalb der digitalen Lieferkette.

Es wird ferner erwartet, dass Finanzunternehmen ihre Maßnahmen und Vorkehrungen regelmäßig überprüfen und dabei den aktuellen Stand der Technik sowie verfügbare Erkenntnisse der nationalen und europäischen Aufsichtsbehörden, Sicherheitsorganisationen, dem Computer Emergency Response Team Austria (CERT-AT) und einschlägiger Fachgremien berücksichtigen. Dies gilt sowohl für präventive Maßnahmen als auch für Detektions-, Reaktions- und Wiederherstellungsfähigkeiten.
Dieses Schreiben dient der Sensibilisierung für die aktuelle Bedrohungslage und der Kommunikation aufsichtlicher Erwartungen. Es wird darauf hingewiesen, dass angesichts der heterogenen Zusammensetzung des österreichischen Finanzsektors im Gegensatz zu den aktuellen Vorgaben der Europäischen Zentralbank für signifikante Kreditinstitute[1] kein einheitlicher Maßnahmenkatalog für sämtliche beaufsichtigte Unternehmen gefordert wird. Vielmehr sollten Finanzinstitute die für sie relevanten Risiken analysieren und angemessene, risikobasierte Maßnahmen festlegen, die ihrer individuellen Exponierung und ihrer Unternehmensgröße und -komplexität entsprechen. Die oben genannten Themenbereiche sollten jedoch nachweislich behandelt werden. Es wird keine explizite Meldung hinsichtlich der Umsetzung der Maßnahmen erwartet, die Nachverfolgung der Empfehlungen wird im Rahmen der laufenden Aufsicht geprüft.
FMA und OeNB werden die weitere Entwicklung KI-gestützter Cybersicherheitsrisiken sowie einschlägige europäische und internationale Initiativen laufend beobachten und die daraus gewonnenen Erkenntnisse weiterhin in ihre Aufsichtstätigkeit einfließen lassen.
Bitte beachten Sie insbesondere allfällige Informationen unter https://www.fma.gv.at/querschnittsthemen/dora/.

Mit freundlichen Grüßen

Michael Hysek
Bereichsleiter BI
Bankenaufsicht

Martina Andexlinger
Bereichsleiterin BII
Versicherungs-
Pensionskassen- und
Vorsorgekassenaufsicht

Birgit Puck
Bereichsleiterin BIII
Wertpapieraufsicht

Gabriela de Raaij
Hauptabteilung
Europäische Großbanken-
und IT-Aufsicht

Markus Schwaiger
Hauptabteilung
Finanzmarktstabilität und
Bankenaufsicht

Finanzmarktaufsichtsbehörde

Oesterreichische Nationalbank

[1] https://www.bankingsupervision.europa.eu/press/letterstobanks/shared/pdf/2026/ssm.2026_letter_on_AI_enabled_cybersecurity_threats.ro.pdf