FMA/OeNB-DORA-Dialog:

KI-basierte Schwachstellensuche und -ausnutzung

Stand der Hinweise ist 3.6.2026.

FMA/OeNB-Antworten sind in dieser Form dargestellt.

Die Hinweise zu den während des Webinars erhaltenen Fragen stellen keine verbindliche Auslegung und insbesondere auch keine Auslegungen im Rahmen der Fragen- und Antwort-Prozesse (Q&As) der drei Europäischen Aufsichtsbehörden (EBA – European Banking Authority, ESMA – European Securities and Markets Authority und EIOPA – European Insurance and Occupational Pensions Authority) dar. Alle Angaben erfolgen trotz sorgfältiger Bearbeitung, insbesondere hinsichtlich Aktualität, Vollständigkeit und Richtigkeit ohne Gewähr und es wird keinerlei Haftung für die Inhalte übernommen. Fragstellungen wurden gs. unformatiert übernommen.

1. Werden FMA bzw. EZB auch die nach DORA direkt beaufsichtigten IT-Service Provider auffordern entsprechende Aktionspläne zu entwickeln?
   Die federführenden Überwachungsbehörden stehen in laufendem Kontakt mit kritischen IKT-Drittdienstleistern. Die FMA ist in diesen Prozess eingebunden, wird aber selbst keine Aufforderung zur Entwicklung entsprechender Aktionspläne an diese richten.

2. Gibt es konkrete Empfehlungen abseits von Claude Mythos zur Nutzung von KI-Modellen zur zeitnahen Integration in bestehende Prozesse?

   Sollten hier ausschließlich selbst/lokal betriebene Modelle eingesetzt werden? Wenn nein, wie kann beim Einsatz von extern durch IKT-DDL betriebenen Modellen die datenschutzrechtliche Compliance und die Überwachung dieser IKT-DDL gemäß DORA gewährleistet werden? Große externe Modellanbieter widmen sich diesen Anforderungen regelmäßig nicht bzw. unzureichend.
   Diese Frage muss jedes Finanzunternehmen selbst evaluieren.
   Beispielsweise verbindet ein risikoadäquater Hybridansatz die Vorteile beider Welten: Externe Frontier-Modelle werden ausschließlich für die Analyse öffentlicher Open-Source-Bibliotheken eingesetzt (nach Prüfung und Pseudonymisierung etwaiger Bank-spezifischer Konfigurationsanteile). Für die Analyse des Closed-Source-Codes wird ein selbst gehostetes Modell oder eine dedizierte, isolierte private Cloud-Instanz mit vertraglich gesicherter Vertraulichkeit (z. B. Confidential Computing, Single-Tenant-Garantien) genutzt.

3. In einer der ersten Folien war es bei der empfohlenen Vorgehensweise erwähnt: Was Organisationen nach CERT-EU jetzt tun sollen - sich an aufkommenden Frameworks orientieren? Welche aufkommenden Frameworks gibt es?
   Im CERT-EU-Artikel ‚AI is changing the economics of vulnerability discovery. Defenders should adapt now' sind zum Beispiel ENISA Multilayer Framework for Good Cybersecurity Practices for AI oder der EU AI Act angeführt.

4. Sie haben erwähnt, dass davon auszugehen ist, dass derartige Tools mittelfristig die Sicherheit erhöhen. Der Firefox-CTO hat ähnliches erwähnt: Die Schwachstellen in einem Codeteil sind logisch betrachtet endlich, KI könnte die Möglichkeit sein, sie alle zu finden. Wenn das schon während der Entwicklung passiert, würde das bedeuten, dass nachträglich "nie wieder" ein Security-Update notwendig ist, weil man alle Schwachstellen bereits während der Entwicklung gefunden hat. Für wie realistisch halten Sie das & wie lange glauben Sie braucht die Transformation, bis wir an diesen Punkt kommen?

Wie bereits präsentiert, halten wir eine Steigerung der Softwarequalität für die unbedingt notwendige Voraussetzung, um diese Welle an neu gefundenen Schwachstellen zu beenden. Es ist aber nicht anzunehmen, dass alle Softwarehersteller weltweit dieses nun notwendige Niveau liefern werden. Vorabanalysen von Third Party Software und Anbietern kommt damit in der Zukunft noch mehr Bedeutung zu. Zusätzlich ist aber zu erwarten, dass die KI-Entwicklung sich fortsetzt und damit eine kontinuierliche Weiterentwicklung der Schwachstellenanalyse bei Anbietern und Betreibern langfristig erforderlich ist.

5. Laut heise.de kooperieren BNP Paribas mit Mistral AI zum Thema Cybersicherheit. Gibt es hier Bestrebungen von Seiten FMA/OeNB Kontakt zu den beiden Unternehmen herzustellen, bzw. gab es bereits eine Kontaktaufnahme?
   OeNB und FMA stehen über die europäischen Aufsichtsgremien der ESAs und der EZB in laufendem internationalen Austausch. Neue Erkenntnisse werden, wenn aufsichtsbehördlich indiziert und in Abstimmung mit den jeweiligen Unternehmen, gerne weitergegeben. Aktuell haben wir keine weitergehenden Informationen über dieses Projekt zwischen diesem Kreditinstitut und diesem KI-Anbieter.

6. Im Kontext von NIS2, DORA und CRA stellt sich zunehmend die Frage nach verifizierbarer Datenintegrität — also kryptografische Signaturen und Provenance-Nachweisen entlang der Datenverarbeitung, nicht nur Transportverschlüsselung oder Zugriffskontrolle. Wie ordnet die FMA bzw. die internationale Aufsichtspraxis das ein — eher als organisatorische Maßnahme im Risikomanagement, oder zeichnet sich eine konkrete technische Erwartungshaltung ab?
   Es kann hierzu keine generelle Aussage bzw. aufsichtliche Erwartungshaltung getroffen werden, da es sich bei der konkreten technischen Ausgestaltung immer um eine Einzelfallentscheidung handelt. Wir möchten diesbezüglich jedoch auf die Anforderungen gemäß Art 6 Abs. 4 Delegierte Verordnung (EU) 2024/1774 (IKT-Risikomanagement) verweisen.

7. Werden auch die kritischen IKT-Dienstleister in diesem Falle Zugriff zu Mythos erhalten (Anthropic öffnet Mythos: EU-Cyberagentur soll Zugriff erhalten | heise online)? Können Sie bereits sagen, was der Stand und Ausblick hierzu ist?
   Der Zugriff auf kommerzielle Modelle wie Mythos wird rein durch die individuellen privaten Anbieter gesteuert. Es ist nicht anzunehmen, dass ein zukünftiger Zugang der ENISA weitergegeben werden kann.

8. Angesichts der zunehmenden geopolitischen Spannungen und der starken Abhängigkeit von außereuropäischen Cybersecurity-Anbietern stellt sich die Frage: Welche konkreten Initiativen verfolgt Österreich, um eigene Sicherheitslösungen zu fördern und die digitale Souveränität zu stärken?
   Das Community Event des Nationalen Koordinierungszentrums für Cybersicherheit in Österreich (NCC-AT) am 30.06.2026 (Registrierung unter https://www.ffg.at/europa/veranstaltung/ncc-community-event_2026-06-30) stellt die zentrale Bedeutung von Kooperation und Vernetzung im Bereich der Cybersicherheit in den Mittelpunkt – mit besonderem Fokus auf den Bank- und Finanzsektor. In einem zunehmend komplexen, dynamischen Umfeld, und vor dem Hintergrund aktueller geopolitischer Entwicklungen, wird deutlich: Wirksame Cybersicherheit ist nur gemeinsam zu erreichen.
   Wir unterstützen die europäischen Entwicklungen im Hinblick auf die europäische technische Souveränität (Strengthening Europe's Tech Sovereignty | Shaping Europe's digital future).

9. Wie weit nimmt die Gesetzgebung der EU im Kontext der aktuellen Entwicklungen die großen KI-Dienstleister in die Pflicht, Ihre Modelle gegen Missbrauch von Cyber-Kriminellen (z.B. durch Jailbreaking) zu härten? Wie haben sich in dem Kontext die Sicherheitsmechanismen bekannter Modelle verbessert? Gibt es Empfehlungen zu belastbaren Studien & Statistiken?
   DORA sieht die Letztverantwortung bei den Finanzunternehmen, welche die Entscheidung hinsichtlich des Einsatzes von IKT-Systemen treffen.