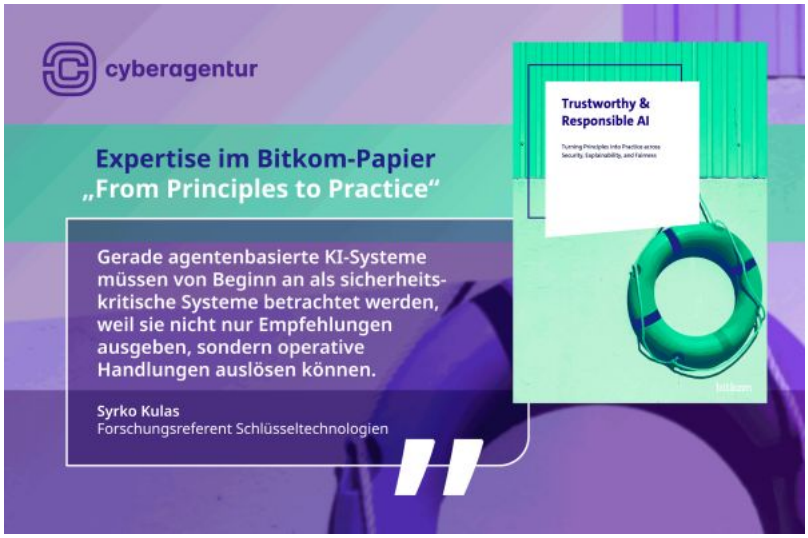
Cyberagentur im neuen Bitkom-Papier

02.06.2026, 11:51 | Wissenschaft, Forschung, Bildung

Pressemitteilung von: *idw - Informationsdienst Wissenschaft*



Die Cyberagentur ist mit einem Fachbeitrag im neuen Bitkom-Papier „From Principles to Practice: Implementing Trustworthy & Responsible AI in the dimensions Security, Explainability, Fairness“ vertreten. Syrko Kulas und Philippe Krajsic, Forschungsreferenten in der Abteilung Schlüsseltechnologien der Cyberagentur, haben Inhalte zum Kapitel „Security“ beigetragen. Das Whitepaper liefert praxisnahe Leitlinien für Unternehmen und richtet sich an Entscheider, Entwickler sowie Governance- und Compliance-Verantwortliche. Es zeigt, wie regulatorische Anforderungen in konkrete Maßnahmen übersetzt und KI-Systeme sicher, fair, nachvollziehbar und nachhaltig betrieben werden können.
Der Beitrag der Cyberagentur: KI-Systeme eröffnen entlang ihres gesamten Lebenszyklus neue Angriffsflächen – von manipulierten Trainingsdaten über unsichere Lieferketten bis hin zu Angriffen im Betrieb. Besonders kritisch sind Prompt-Injections und Jailbreaks sowie Risiken wie Datenvergiftung, Datenlecks und Modell-Extraktion, verstärkt durch externe Datenquellen und APIs. Diese Bedrohungen lassen sich nur durch ganzheitliche Sicherheitsstrategien, kontinuierliches Monitoring und zentrale Governance wirksam begrenzen.
„Mit jeder neuen Fähigkeit von KI wächst nicht nur ihr Nutzen, sondern auch die Angriffsfläche: Sicherheit muss daher genauso dynamisch sein wie die Systeme selbst und ganzheitlich gedacht werden.“, sagt Syrko Kulas, Forschungsreferent in der Abteilung Schlüsseltechnologien der Cyberagentur. „Gerade agentenbasierte KI-Systeme müssen von Beginn an als sicherheitskritische Systeme betrachtet werden, weil sie nicht nur Empfehlungen ausgeben, sondern operative Handlungen auslösen können.“
Ein zentrales Anliegen ist der Wechsel von punktuellen Schutzmaßnahmen hin zu einer systemischen Sicherheitsarchitektur. Einzelne Tools reichen nicht aus – erforderlich sind integrierte Konzepte mit Zero-Trust-Prinzipien, minimalen Zugriffsrechten, kontinuierlicher Überwachung sowie klaren Eskalationsmechanismen.
„KI-Sicherheit ist keine Eigenschaft, die man einmal prüft und dann abhakt. Sie ist eine dauerhafte Kontrollaufgabe über den gesamten Lebenszyklus eines Systems“, sagt Philippe Krajsic, Forschungsreferent in der Abteilung Schlüsseltechnologien der Cyberagentur. „Entscheidend ist, Risiken nicht isoliert zu betrachten, sondern ihre Wechselwirkungen im Gesamtsystem zu verstehen.“
Im Bitkom-Papier wird Security als eine von drei zentralen Dimensionen vertrauenswürdiger KI neben Erklärbarkeit und Fairness eingeordnet. Für die Cyberagentur ist die Security-Perspektive dabei eine Grundvoraussetzung: Nur wenn KI-Systeme gegen gezielte Manipulationen, Datenverfälschung, Modellmissbrauch und unkontrollierte Systemwirkungen abgesichert sind, können sie belastbar in Wirtschaft, Verwaltung und sicherheitsrelevanten Anwendungen eingesetzt werden.
Mit ihrem Beitrag unterstreicht die Cyberagentur ihre Rolle an der Schnittstelle von Sicherheitsforschung,

technologischer Vorausschau und digitaler Souveränität – und die Bedeutung sicherer KI als strategische Voraussetzung für die Zukunft.

Weitere Informationen:
Link zum Paper: https://www.bitkom.org/EN/List-and-detailpages/Publications/Trustworthy-Responsible-AI

Kontakt:

Agentur für Innovation in der Cybersicherheit GmbH
Große Steinstraße 19
06108 Halle (Saale)
Michael Lindner
Pressesprecher
Tel.: +49 151 44150 645
E-Mail:

Hintergrund: Cyberagentur

Die Agentur für Innovation in der Cybersicherheit GmbH (Cyberagentur) wurde im Jahr 2020 als vollständige Inhouse-Gesellschaft des Bundes unter der gemeinsamen Federführung des Bundesministeriums der Verteidigung und des Bundesministeriums des Inneren und für Heimat durch die Bundesregierung mit dem Ziel gegründet, einen im Bereich der Cybersicherheit anwendungsstrategiebezogenen und ressortübergreifenden Blick auf die Innere und Äußere Sicherheit einzunehmen. Vor diesem Hintergrund bezweckt die Arbeit der Cyberagentur maßgeblich eine institutionalisierte Durchführung von hochinnovativen Vorhaben, die mit einem hohen Risiko bezüglich der Zielerreichung behaftet sind, gleichzeitig aber ein sehr hohes Disruptionspotenzial bei Erfolg innehaben können.

Die Cyberagentur ist Bestandteil der Nationalen Sicherheitsstrategie der Bundesrepublik Deutschland.

Der Cyberagentur stehen als Geschäftsführung Prof. Dr. Christian Hummert als Forschungsdirektor und Bettina Bubnys als kaufmännische Geschäftsführung vor.

wissenschaftliche Ansprechpartner:
Syrko Kulas und Philippe Krajsic, Forschungsreferenten Künstliche Abteilung Schlüsseltechnologien

Originalpublikation:
https://www.cyberagentur.de/presse/cyberagentur-im-neuen-bitkom-papier/

Agentur für Innovation in der Cybersicherheit GmbH

MichaelLindner (Mitarbeiter in der Presse- und Öffentlichkeitsarbeit)

+49 151 44150645

lindner@cyberagentur.de

News-ID: 1313517 • Views: 80 (Stand: 07.06.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/1313517/Cyberagentur-im-neuen-Bitkom-Papier-idw.html