ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Liebe Cybersicherheitsinteressierte,

im aktuellen ATHENE-Newsletter berichten wir über neue ATHENE-Forschungsprojekte und aktuelle Ergebnisse: Mit dem Start von CYNTRA zur KI-gestützten Erkennung von Hassrede und dem neuen Projekt HAICC zur Verbesserung der Mensch-KI-Kollaboration in der Cybersicherheit bündelt ATHENE seine Forschungsaktivitäten im Bereich Künstliche Intelligenz; hinzu kommen Erfolge auf den renommierten Konferenzen ACM CHI und der Eurocrypt 2026 sowie ein neues Trainingsformat zur Stärkung der Cyberresilienz im Gesundheitssektor. Neu vorgestellt werden außerdem das Projekt VAMPIR zur Identifikation von Fehlinformationen in Videoformaten sowie ein praxisorientierter Leitfaden zur Umstellung auf Post-Quanten-Kryptografie für Kommunen und Behörden. Für Cyber-Startups haben wir eine wichtige Information: der ATHENE Startup Award UP@it-sa geht in die nächste Runde, die Bewerbungsphase startet in wenigen Tagen! Im Veranstaltungskalender finden Sie aktuelle Terminankündigungen und am Ende eine Auswahl der jüngsten Medienberichte zu aktuellen ATHENE-Forschungsaktivitäten.
Wir wünschen Ihnen eine informative Lektüre!

Ihr ATHENE-Redaktionsteam

Neues ATHENE-Projekt stärkt Mensch-KI-Kollaboration

Künstliche Intelligenz zeigt beeindruckende Leistungen – doch die Zusammenarbeit von KI-Systemen und menschlichen Expertinnen und Experten führt nicht automatisch zu besseren Ergebnissen. Das neue ATHENE-Projekt „Human-AI Collaboration for Cybersecurity" (HAICC), koordiniert von Prof. Dr. Iryna Gurevych an der TU Darmstadt, setzt genau hier an: Es entwickelt Methoden, die eine gleichberechtigte, iterative Zusammenarbeit zwischen Fachkräften und KI-Agenten ermöglichen – unter anderem bei der Analyse von Sicherheitslücken und Protokollen. Dabei adressiert das Projekt zentrale Herausforderungen wie den sogenannten Automation Bias, also die unkritische Übernahme von KI-Empfehlungen, sowie den Mangel an verfügbaren Trainingsdaten im Cybersicherheitsbereich.

Mehr Informationen

Quantensicher: Neuer Leitfaden für Kommunen und Behörden

Quantencomputer werden künftig in der Lage sein, viele aktuelle Verschlüsselungsverfahren zu brechen – Angreifer speichern bereits heute verschlüsselte Daten, um sie zu einem späteren Zeitpunkt zu entschlüsseln. ATHENE-Forschende des Fraunhofer SIT haben daher gemeinsam mit dem Hessischen Ministerium des Innern, für Sicherheit und Heimatschutz den Leitfaden „Post-Quanten-Kryptografie in Umsetzung" entwickelt, der Kommunen und Landesbehörden konkrete Handlungsempfehlungen für den Übergang zu quantensicheren IT-Systemen bietet: von der Bestandsaufnahme kryptografischer Verfahren bis hin zu behördenspezifischen Vergabekriterien. Der Leitfaden orientiert sich am EU-Umsetzungsfahrplan vom Juni 2025 und steht kostenlos zum Download bereit.

Zum Download

Wenn Effizienz zur Schwachstelle wird: ATHENE deckt Lücke in kryptografischen Protokollen auf

Im Rahmen des ATHENE-Projekts PriDA deckten ATHENE-Wissenschaftler Prof. Dr. Thomas Schneider und Andreas Brüggemann eine Sicherheitslücke in mehreren Protokollen für sichere Mehrparteienberechnungen (Secure Multi-Party Computation, MPC) auf. MPC sind Verfahren, die es mehreren Parteien ermöglichen, gemeinsam Berechnungen durchzuführen, ohne ihre vertraulichen Daten gegenseitig preiszugeben. Die Schwachstelle betrifft Protokolle, bei denen bestimmte Sicherheitsprüfungen aus Effizienzgründen ans Ende des Berechnungsprozesses verschoben werden – ein Vorgehen, das es einer unehrlichen Partei ermöglicht, die geheimen Eingaben der anderen zu rekonstruieren. Als Lösung entwickelten die Forschenden einen Reparaturmechanismus, der alle Sicherheitsprüfungen bündelt und nur das Endergebnis sichtbar macht, ohne dabei neue Angriffsflächen zu schaffen. Diese und weitere Arbeiten aus der ATHENE-Forschung wurden auf der hochrangigen Annual International Conference on the Theory and Applications of Cryptographic Techniques, kurz Eurocrypt, präsentiert.

Mehr Informationen

Von AR-Memes bis Faktencheck: ATHENE-Forschung im Bereich der Mensch-Computer-Interaktion

Im ATHENE-Projekt XRGuard untersuchten ATHENE-Wissenschaftler Prof. Dr. Jan Gugenheimer und Prof. Dr. Florian Müller von der TU Darmstadt wie Internet-Memes mithilfe von Augmented Reality in direkte Gespräche

integriert werden können – mit dem Ergebnis, dass AR-Memes die Gesprächsqualität nicht beeinträchtigen und von Nutzenden als attraktiv bewertet werden. In einem weiteren Beitrag, der in das ATHENE-Projekt CYNTRA einfließt, analysierten Forschende aus der von Prof. Dr. Dr. Christian Reuter an der TU Darmstadt geleiteten Forschungsgruppe PEASEC in einem Online-Experiment mit 1.004 Teilnehmenden, wie fünf verbreitete Gegenmaßnahmen gegen Falschinformationen auf TikTok, Telegram und X wirken – mit dem zentralen Befund, dass professionelle Faktenprüfungen und Indikatoren die Glaubwürdigkeitswahrnehmung von Falschinformationen plattformübergreifend signifikant reduzieren, sofern sie fehlerfrei arbeiten. Diese und weitere Arbeiten stellten die Wissenschaftler auf der ACM CHI Conference on Human Factors in Computing Systems vor – der weltweit führenden Konferenz zur Mensch-Computer-Interaktion und zentralen Plattform für den Austausch zwischen Forschung, Praxis und Industrie.

Mehr erfahren

Neue Projekte, neue Forschende: Dr. Thea Riebe forscht über KI gegen Hassrede

Hassrede im Internet nimmt zu und stellt Strafverfolgungsbehörden sowie Plattformbetreiber vor wachsende Herausforderungen. Neue KI-basierte Ansätze sollen hier Abhilfe schaffen: Im ATHENE-Forschungsbereich REVISE

startet im Juli 2026 das Projekt CYNTRA mit dem Ziel, effizientere KI-Methoden zur Erkennung und Bekämpfung von Hassrede zu entwickeln. Koordiniert wird das Projekt gemeinsam von Dr. Thea Riebe und Dr. Marc-André Kaufhold, zwei Forschenden der TU Darmstadt aus der Forschungsgruppe PEASEC – Science and Technology for Peace and Security. Im Interview stellt sich Dr. Riebe vor und gibt Einblicke in den Forschungsansatz und die Praxisrelevanz des Projekts.

Interview mit Dr. rer. nat. Thea Riebe

Neues Forschungsprojekt: Falschinformationen in Videos erkennen

Videoplattformen wie TikTok sind bei Jugendlichen weit verbreitet und stellen ein bevorzugtes Ziel für Desinformationskampagnen dar. Kurze Videos gehen innerhalb kürzester Zeit viral. Falsche oder irreführende Informationen erreichen so ein junges Publikum, das traditionelle Nachrichtenkanäle zunehmend weniger nutzt. Genau hier setzt das interdisziplinäre Forschungsprojekt VAMPIR an, an dem sich ATHENE-Forschende um Prof. Dr. Martin Steinebach beteiligen. Das Projekt entwickelt automatisierte Methoden zur Erkennung und Einordnung von Fehlinformationen in Videoformaten und adressiert damit eine der drängendsten Herausforderungen unserer Gesellschaft.

Mehr Informationen

Planspiele stärken Cyberresilienz im Gesundheitssektor

Wie reagiert ein Krankenhaus, wenn Ransomware zuschlägt und die Telefonanlage ausfällt? Um Krankenhäuser gezielt auf einen solchen Ernstfall vorbereiten zu können, haben ATHENE-Forschende des Fraunhofer SIT ein Übungsformat entwickelt: In realitätsnahen Cyber-Krisen-Planspielen trainieren interdisziplinäre Teams aus IT, Medizin und Verwaltung, einen Cyberangriff zu erkennen, zu kommunizieren und zu bewältigen – und tragen damit zur systematischen Stärkung der Cyberresilienz im Gesundheitssektor bei.

Weitere Informationen

Die Bewerbungsphase für den ATHENE Startup Award UP26@it-sa startet in Kürze. Ab Anfang Juni können sich Cybersecurity-Startups aus der DACH-Region für Deutschlands wichtigsten Gründungspreis für Cybersicherheit und Datenschutz bewerben.
Der Award wird gemeinsam vom ATHENE Digital Hub Cybersecurity und der NürnbergMesse mit der it-sa Expo&Congress ausgerichtet. Ziel ist es, innovative Cybersecurity-Gründungen aus dem deutschsprachigen Raum sichtbar zu machen und aktiv zu fördern.

Mehr Informationen

In einer Spezialfolge von "House of Nerds" – dem Podcast zu Cybersicherheitsthemen aus Darmstadt – spricht Claudia Plattner, Präsidentin des Bundesamts für Sicherheit in der Informationstechnik (BSI), über Deutschland auf dem Weg zur Cybernation, was noch fehlt, um eine solche zu werden, und was man sich überhaupt darunter vorstellen kann.

Zum Podcast auf Podigee

Im Gastbeitrag in der Wochenzeitung DIE ZEIT ordnen ATHENE-CEO Prof. Dr. Michael Waidner und ATHENE-Direktoriumsmitglied Prof. Dr. Haya Schulmann den Deutschland-Stack kritisch ein und entdecken in der aktuellen Planung Parallelen zu früheren Fehlern in der Verwaltungsdigitalisierung. ATHENE-Studien belegen: Altsysteme werden nicht abgeschaltet, Lösungen an Nutzenden vorbei entwickelt und Aufwände systematisch unterschätzt. Die Forschenden fordern konkrete Querschnittsdienste, ergebnisorientierte Leitlinien und eine faktenbasierte Modernisierungsstrategie mit realistischen Zeitplänen.
Zum Bericht (Paywall): https://www.zeit.de/digital/2026-05/digitalisierung-deutschland-stack-informatik-cybersicherheit-bundesregierung

Prof. Dr. Michael Waidner und Prof. Dr. Haya Schulmann analysieren in einem Gastbeitrag in der Frankfurter Allgemeinen Zeitung FAZ den Einsatz von KI durch Cyberangreifer und konstatieren: Der Heilige Gral eines vollautonomen Angriffssystems ist erst zur Hälfte erreicht. Zwei der fünf Bausteine autonomer Angriffe – maßgeschneiderter Erstzugang und durchgängige Angriffskette ohne Menschen – fehlen noch weitgehend. Die Forschenden fordern als Gegenstrategie konsequente IT-Modernisierung, Cyberhygiene und Security by Design, denn KI verschärft bestehende Sicherheitslücken, verursacht sie aber nicht.
Zum Beitrag (Paywall):
https://www.faz.net/aktuell/wirtschaft/unternehmen/mythos-gemini-und-co-der-heilige-gral-der-cyberangreifer-accg-200828004.html

Unsere KI-Forscherin Prof. Dr. Iryna Gurevych erklärt in einem Beitrag in der FAZ, wie KI verantwortungsbewusst in der Diagnostik psychischer Erkrankungen eingesetzt werden kann. Datenschutz ist laut Professorin Gurevych der zentrale Engpass für KI-Entwicklung im Bereich mentaler Gesundheit. Ihr Team entwickelt daher Methoden mit synthetischen

Patientendaten, die klinisch relevant sind, aber keine persönlichen Daten preisgeben.
Zum Beitrag (Paywall): https://www.faz.net/aktuell/rhein-main/region-und-hessen/behandlung-psychisch-kranker-wie-ki-ihnen-helfen-koennte-200737594.html

Digitale Altersverifikation ist ein zentrales Instrument zum Schutz Minderjähriger vor ungeeigneten Inhalten – und gewinnt im Spannungsfeld von Jugendschutz und Datenschutz zunehmend an gesellschaftlicher Bedeutung. Unsere IT-Forensik-Experten Prof. Dr. Martin Steinebach und York Yannikos beleuchten das Thema in zwei aktuellen Beiträgen:
In einem Aufsatz in Datenschutz und Datensicherheit unterscheiden sie zwischen Altersbestätigung durch Dritte und KI-basierter Altersfeststellung durch den Diensteanbieter selbst. Ihr kryptografisches Protokoll ermöglicht datenschutzkonforme Altersverifikation, ohne dass Diensteanbieter personenbezogene Daten der nutzenden Person erhalten.
Zum Beitrag: https://rdcu.be/fhbV3
In einem Gastbeitrag im Tagesspiegel Background Cybersecurity räumen sie mit zentralen Missverständnissen rund um die EU-Wallet auf: Die Mini-Wallet prüft ausschließlich die Volljährigkeit – sie stellt kein Alter fest, sondern vermittelt lediglich zwischen prüfender und bestätigender Instanz. Außerdem bedeutet Zero-Knowledge-Technologie nicht automatisch Anonymität: Gerätedaten können Nutzende trotzdem identifizierbar machen.
Zum Beitrag (Paywall): https://background.tagesspiegel.de/it-und-cybersicherheit/briefing/die-missverstaendnisse-rund-um-die-eu-wallets

Wachsende Unsicherheit über die Echtheit von Videos eröffnet Akteuren neue Möglichkeiten zur gezielten Manipulation der öffentlichen Meinung. Prof. Dr. Martin Steinebach erklärt auf br24.de, dass selbst Experten KI-Fakes kaum noch sicher erkennen können. Er selbst könne nicht mehr spontan entscheiden, ob ein Video echt oder KI-generiert sei. Auffälligkeiten in Videos ließen sich oft auch durch verlustbehaftete Kompression erklären – nicht zwingend durch KI.
Zum Beitrag: https://www.br.de/nachrichten/netzwelt/ausrede-ki-wie-deepfakes-vertrauen-in-echte-inhalte-zerstoeren-faktenfuchs,VK3TQvH

Europas wachsendes Regulierungsgeflecht aus Datenschutz-, Datennutzungs- und Cybersicherheitsrecht stellt Organisationen vor zunehmende Herausforderungen. In einem Aufsatz in Datenschutz und Datensicherheit analysieren die ATHENE-Forschenden Dr. Michael Kreutzer, Dr. Dr. Annika Selzer und Sarah Stummer das wachsende Regulierungsdickicht in Datenschutz, Datennutzung und Cybersicherheit. Sie warnen unter anderem, dass die Vielzahl der Rechtsakte europäische Organisationen überfordern und

den Innovationsstandort Europa gefährden. Als Lösung fordern sie einen interdisziplinären Dialog zwischen Recht und Technik sowie eine systematische Konsolidierung bestehender Rechtsakte.
Zum Beitrag: https://rdcu.be/fhbV9

Deepfake-Videos auf Plattformen wie TikTok und Instagram gefährden zunehmend die Medienkompetenz von Jugendlichen. Im Gespräch mit br24.de erklärt Prof. Dr. Martin Steinebach, wie Deepfake-Videos Jugendliche durch Widersprüche zwischen Bild und Text manipulieren. Im Forschungsprojekt VAMPIR untersucht er Diskrepanzen zwischen emotionalisierenden Bildern und sachlichen Texten als Indikatoren für Desinformation. Ziel ist ein Detektor, der Alarm schlägt, sobald Bildinhalt und Ton nicht zum gesprochenen Text passen.
Zum Beitrag: https://www.br.de/nachrichten/wissen/deepfake-videos-schneller-erkennen-und-entlarven,VIAWWcU

03.06.2026: ATHENE Distinguished Lecture mit HUANG Yiyang, Generalkonsul der Volksrepublik China in Frankfurt am Main
In seiner Keynote spricht er über Chinas aktuelle Entwicklung und die Perspektiven der deutsch-chinesischen Zusammenarbeit.
Mehr Informationen und Anmeldung: https://www.athene-center.de/dls

08.06.2026: Wirtschaft meets angewandte KI-Forschung | Heilbronn
Fraunhofer HNFIZ und IHK Heilbronn laden Führungskräfte ein, Forschung hautnah zu erleben – von aktueller KI bis zu konkreten Unternehmensanwendungen. Als Teil des Fraunhofer HNFIZ Cybersecurity bringt ATHENE seine Expertise in angewandter Cybersicherheitsforschung in die Veranstaltung ein. Gezeigt wird ein Demonstrator aus dem Projekt Smart-ID zum Schutz vor Produktfälschungen sowie die ATHENE Cyber Range. Eine Anmeldung ist nur noch bis 29.05. möglich.

Mehr Informationen: https://veranstaltungen.heilbronn.ihk.de/b?p=wmki

12.06.2026: ATHENE auf der Night of Science an der Goethe-Universität Frankfurt
Die Night of Science feiert ihr 20-jähriges Jubiläum auf dem Campus Riedberg der Goethe-Universität Frankfurt am Main. Das zentrale Thema des Jubiläumsjahres ist die Informatik; als Leitfigur wurde die Informatikpionierin Grace Hopper gewählt. Prof. Dr. Haya Schulmann gibt in ihrem Vortrag einen Überblick über aktuelle Angriffsvektoren in der Cybersicherheit und beleuchtet die spezifische Bedrohungslage in Deutschland. ATHENE ist mit einem eigenen Stand vertreten; der Eintritt ist frei.
Mehr Informationen: https://www.athene-center.de/aktuelles/veranstaltungen/night-of-science-an-der-goethe-universitaet-frankf-1938

23.–25.06.2026: ACM CODASPY 2026 | Frankfurt
Die 16. ACM Conference on Data and Application Security and Privacy (CODASPY 2026) findet auf dem Campus Westend der Goethe-Universität Frankfurt am Main statt. Die Konferenz ist eines der führenden Foren für Forschung zu Sicherheit und Datenschutz auf Daten- und Anwendungsebene. ATHENE unterstützt die Organisation und Durchführung.
Mehr Informationen: https://www.athene-center.de/aktuelles/veranstaltungen/acm-codaspy-2026-1920

Lunch Lectures CRA: CRA, KI-VO und DSGVO im Vergleich | Online
10.08.2026 | 12:00–12:30 Uhr: Gemeinsamkeiten und Unterschiede zwischen CRA, KI-VO und DSGVO: Ein Überblick
mit Sarah Stummer, ATHENE | Fraunhofer SIT | HNFIZ7

07.09.2026 | 12.00-12.30 Uhr: Gemeinsame technische Dokumentation nach CRA, KI-VO und DSGVO?
mit Sarah Stummer, ATHENE | Fraunhofer SIT | HNFIZ7

Die Lunch Lectures finden online statt. Die Teilnahme ist kostenfrei.
Mehr Informationen: https://www.athene-center.de/angebote/lunch-lectures-cra

---

ATHENE ist ein Forschungszentrum der Fraunhofer-Gesellschaft unter Mitwirkung von

Impressum

Fraunhofer-Institut für Sichere Informationstechnologie
Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE
Rheinstraße 75
64295 Darmstadt
Telefon +49 6151 869-368
Fax +49 6151 869-224
E-Mail: pr@athene-center.de

Fraunhofer SIT und ATHENE sind rechtlich nicht selbstständige Einrichtungen der Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V.
Hansastraße 27 c
80686 München
Telefon +49 89 1205- 0

Vereinsregister: Amtsgericht München, VR 4461
Empfangsberechtigt: Prof. Dr.-Ing. Holger Hanselka (Präsident)

Verantwortliche Redakteurin:
Cornelia Reitz
Telefon +49 6151 869 368