ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Liebe Cybersicherheitsinteressierte,

der Energiesektor ist besonders wichtig für das Funktionieren einer Gesellschaft und deshalb wird dieser Bereich auch verstärkt Ziel von Cyberangriffen: ATHENE und das israelische Ministerium für Energie und Infrastruktur haben jetzt ein dreijähriges kooperatives Forschungsprogramm zum Schutz des Energiesektors gestartet. Internationale Beachtung fanden auch kritische Schwachstellen, die ATHENE-Forschende in der RPKI-Software entdeckten. Mit der Software wird das Internet Routing abgesichert, eine Ausnutzung der Sicherheitslücken hätte schwerwiegende Folgen haben können. Die Forschenden hatten deshalb die Hersteller bereits vor der Veröffentlichung informiert, sodass entsprechende Sicherheitsupdates verfügbar waren. Eine große Ehre wurde ATHENE-Forscherin Prof. Iryna Gurevych zuteil, die in die Leopoldina berufen wurde, eine hohe wissenschaftliche Auszeichnung. Außerdem gibt es ein neues ATHENE-Whitepaper zum Cyber Resilience Act und wir informieren über aktuelle Veröffentlichungen von ATHENE-Forschenden auf internationalen Spitzenkonferenzen sowie über Berichte zu ATHENE-Forschungsaktivitäten in den Medien. Zudem möchten wir nicht versäumen, Sie auf die diesjährige Tour der MS Wissenshaft, dem „schwimmenden Science Center“, hinzuweisen: Mit an Board ist ein ATHENE-Exponat zum Thema "Darknet". Am Ende gibt es wie gewohnt unsere Veranstaltungstipps.
Jetzt wünschen wir Ihnen viel Freude beim Lesen unseres Newsletters.

Ihr ATHENE-Redaktionsteam

Start einer deutsch-israelischen Forschungskooperation zur Cybersicherheit im Energiesektor

ATHENE und das israelische Ministerium für Energie und Infrastruktur starten ein dreijähriges kooperatives Forschungsprogramm, bei dem Forschende israelischer Universitäten gemeinsam mit ATHENE-Forschenden Lösungen für Cybersicherheitsprobleme im Energiesektor entwickeln. Zur Eröffnung der Forschungskooperation fand vor wenigen Tagen unter Leitung von Prof. Haya Schulmann ein gemeinsamer Workshop der beteiligten Forschenden aus Israel und Deutschland statt, bei dem über 40 Personen aus der deutschen und israelischen Forschung, Wirtschaft und Politik zusammenkamen, um Probleme und Lösungsansätze zu diskutieren.

Mehr über die Forschungskooperation

Whitepaper zum Cyber Resilience Act

Vernetzte Produkte sollen EU-weit sicherer werden – das ist das Ziel des Cyber Resilience Act (CRA), einer in Abstimmung befindlichen EU-Verordnung, die voraussichtlich dieses Jahr in Kraft treten wird. Doch welche Produkte werden davon betroffen sein, welche Anforderungen und Verpflichtungen kommen auf Unternehmen zu? Unser Whitepaper greift die neueste Version des CRA-Entwurfs auf und erklärt, welche Produkte voraussichtlich betroffen sind und wie sich Unternehmen auf die Veränderungen vorbereiten können.

Download des Whitepapers

Schwere Sicherheitslücken in Software zum Schutz von Internet Routing entdeckt

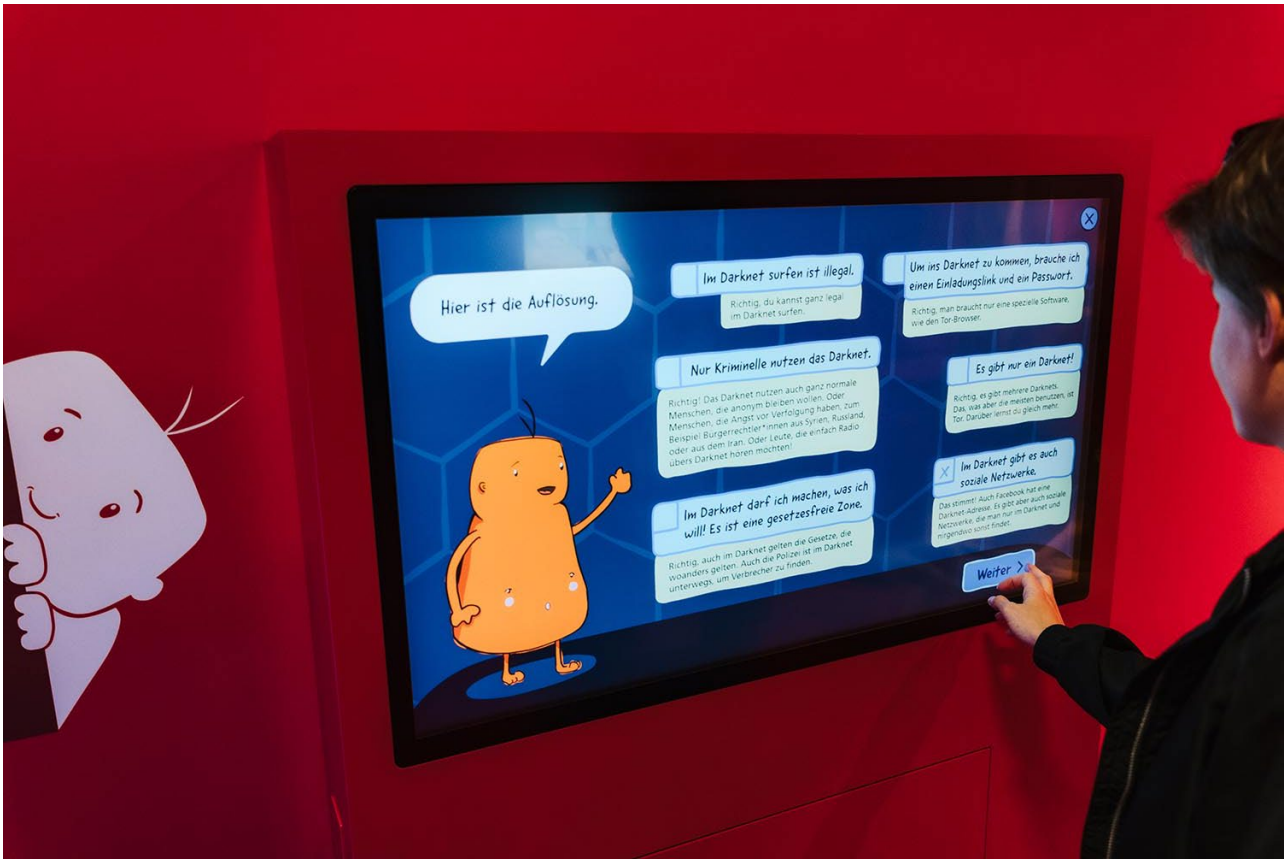
Ein Team von ATHENE-Forschenden unter der Leitung von Prof. Haya Schulmann hat kürzlich 18 Schwachstellen in wichtigen Softwarekomponenten der Resource Public Key Infrastructure (RPKI) entdeckt. Diese Sicherheitslücken hätten schwerwiegende Auswirkungen haben können, darunter Datenlecks, betrügerische Zertifikatsausstellungen und Malware-Verbreitung. Die gute Nachricht: allen betroffenen Hersteller wurden bereits Patches bereitgestellt, um diese Risiken zu beheben. Durch diese rasche Reaktion wurde die potenzielle Gefahr für die Online-Sicherheit minimiert. Das wissenschaftliche Paper zu der Forschungsarbeit ”The CURE To Vulnerabilities in RPKI Validation”, erschien im Februar 2024 auf dem "The Network and Distributed System Security (NDSS) Symposium 2024", einer akademischen Spitzenkonferenz. Im August 2024 wird das Forschungsprojekt auch auf der Black Hat USA 2024 vorgestellt, der führenden technischen Anwender-und-Hacking Konferenz für Cybersicherheit.

Mehr über die aufgedeckten Sicherheitslücken

Hohe Auszeichnung für Prof. Iryna Gurevych

Vor wenigen Wochen wurde Prof. Iryna Gurevych in die Deutsche Akademie der Naturforscher Leopoldina berufen. Diese Berufung stellt eine der höchsten wissenschaftlichen Auszeichnungen dar, die von einer deutschen Institution vergeben wird. Als älteste dauerhaft existierende naturforschende Akademie der Welt vereint die Leopoldina unter ihrem Dach Forschende mit herausragenden wissenschaftlichen Leistungen.
Prof. Gurevych leitet an der TU Darmstadt das Arbeitsgebiet "Ubiquitäre Wissensverarbeitung". Ihre Forschungen auf dem Gebiet der automatischen Sprachverarbeitung und Künstlichen Intelligenz sind wegweisend und sorgen international für Forschungsimpulse. In ATHENE fließen ihre Forschungen in die Forschungsbereiche Automatic Vulnerability Scanning and Verification (AVSV), Security and Privacy in Artificial Intelligence (SENPAI) und Secure Digital Transformation in Health Care (SeDiTraH) ein.

Mehr über diese Auszeichnung



ATHENE auf der MS Wissenschaft

Rund 30 interaktive Exponate sind in diesem Jahr an Bord der MS Wissenschaft und laden zum Anfassen und Mitforschen ein. Mit dabei ist auch ein Exponat von ATHENE zum Thema Darknet. Bei der Tour durch das "Darknet - heller als gedacht" erfahren die Besucherinnen und Besucher, was genau sich hinter dem "Darknet" verbirgt und dass sich nicht nur Kriminelle dort bewegen. Denn zum Beispiel wird das Darknet auch von Menschen genutzt, die in ihren Heimatländern politisch verfolgt werden oder Repressionen fürchten, um unzensierte Nachrichten zu lesen oder sich anonym zu organisieren. Zwischen Mai und September steuert die MS Wissenschaft rund 30 größere und kleinere Städte in Deutschland an und kommt damit vielleicht auch in Ihre Nähe - schauen Sie gerne vorbei!

Mehr über unser Darknet-Exponat auf der MS Wissenschaft

Neue Folgen im House of Nerds

Im ATHENE-Podcast „House of Nerds" gibt es neue Folgen: Prof. Martin Steinebach gibt ein KI-Update und erläutert den aktuellen Stand zu Deep Fakes, und Prof. Sebastian Schinzel erzählt, wie er mit seinem Team vor einigen Jahren die spektakuläre Efail-Sicherheitslücke gefunden hat, mit der sich die E-Mail-Verschlüsselung bei S/MIME und PGP aushebeln ließ. Auf die Veröffentlichung von Efail hin gab es viele für die Wissenschaftler überraschend emotionale Reaktionen, sowohl aus der Community als auch aus der Presse, woraus Sebastian Schinzel Lehren für seine Wissenschaftskommunikation gezogen hat.
Diese und weitere Folgen unseres Podcasts „House of Nerds" finden Sie hier: https://www.athene-center.de/aktuelles/houseofnerds

---

Paper accepted - ATHENE-Paper auf internationalen Spitzenkonferenzen

Texte klassifizieren mit KI – Schädliche Inhalte automatisiert erkennen

Textklassifizierung ist ein wichtiges Werkzeug für Expertinnen und Experten der natürlichen Sprachverarbeitung. Leistungsfähige Systeme sind jedoch entweder zu langsam, zu umständlich oder zu unvorhersehbar, was ihre zuverlässige Anwendung erschwert. In ihrem Paper „Like a Good Nearest Neighbour: Practical Content Moderation and Text Classification" stellen die ATHENE-Forschenden Prof. Iryna Gurevych und Luke Bates einen von ihnen entwickelten Textklassifikator vor, der nicht nur unerwünschte Inhalte erkennt, sondern auch einfacher und leistungsfähiger ist als teurere Systeme. Dieses und weitere Paper zu computergestützten Ansätzen für natürliche Sprachverarbeitung stellten die Forschenden jüngst auf der 8th Conference of the European Chapter of the Associations for Computational Linguistics, kurz EACL, vor.

ATHENE-Paper auf der EACL 2024

Mit "Cyber Threat Observatory" Sicherheitsbewusstsein im Cyberraum schaffen

Um Computer Emergency Response Teams (CERTs) und IT-Sicherheitsbeauftragte durch neue Technologien bei der Erfassung, Analyse und Kommunikation des Cyber-Lagebilds unterstützen zu können, hat das Forscherteam um ATHENE-Wissenschaftler Christian Reuter gemeinsam mit weiteren Forschungs- und Entwicklungspartnern das „Cyber Threat Observatory" entwickelt. Die neuartige, webbasierte Anwendung ermöglicht die automatisierte Sammlung öffentlicher Daten, eine interaktive Datenauswertung und die Kommunikation von Warnmeldungen. Akzeptanz und Gebrauchstauglichkeit wurden bei der Entwicklung ebenso berücksichtigt wie ethische, rechtliche und soziale Rahmenbedingungen.
In ihrer Publikation "'We Do Not Have the Capacity to Monitor All Media': A Design Case Study on Cyber Situational Awareness in Computer Emergency Response Teams" fassen die Forschenden den Designprozess des „Cyber Threat Observatory" wissenschaftlich zusammen. Dieses und weitere Paper von ATHENE Forschenden wurde vor wenigen Tagen auf der ACM CHI Conference on Human Factors in Computing Systems, kurz CHI, vorgestellt. Das Paper von Prof. Reuter wurde zudem mit dem Best-Paper-Award ausgezeichnet.

ATHENE-Paper auf der CHI 2024

Schutz kryptographischer Systeme durch Seitenkanalangriffe

In der Kryptographie wird die Sicherheit von Algorithmen typischerweise in einem Sicherheitsmodell bewiesen. Zur Sicherheitsanalyse von Maskierungsverfahren gegen Seitenkanalangriffe hat sich das sogenannte Random Probing Modell durchgesetzt, das annimmt, dass Zwischenwerte einer Berechnung mit einer bestimmten Wahrscheinlichkeit an den Angreifer preisgegeben werden. Die Wahrscheinlichkeit hängt hierbei zum einen von den verwendeten Schutzmechanismen, zum anderen von den in physikalischen Messungen vorhandenen Rauschen ab. In der Forschungsarbeit "From Random Probing to Noisy Leakages Without Field-Size Dependence" eines Autorenteams um ATHENE-Wissenschaftler Prof. Sebastian Faust konnte gezeigt werden, wie kryptographische Verfahren durch zusätzliche Randomisierungsschritte selbst dann Sicherheit gewährleisten können, wenn deutlich weniger Rauschen in der physikalischen Messung vorhanden ist. Dies ist insbesondere für kryptografische Systeme wichtig, die mit großen Feldern arbeiten, wie der AES-Verschlüsselungsstandard oder neuere Post-Quantum-Verfahren. Die Forschenden stellen dieses und ein weiteres Paper Ende Mai auf der renommierten 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, kurz Eurocrypt, vor.

ATHENE-Paper auf der Eurocrypt 2024

KI ist der Versuch, menschliches Denken und Lernen auf den Computer zu übertragen. Und an diesem Punkt setzen auch die Hacker-KI an, erläutert Prof. Haya Schulmann im SWR: https://www.swr.de/swraktuell/radio/ki-hacker-cyber-kriminalitaet-phishing-100.html

Prof. Matthias Hollick in der hessenschau über ein Warnsystem bei Stromausfall: https://www.youtube.com/watch?v=P2iWc7nMbEA

Mittels KI-Systemen lassen sich Fotos und Videos mittlerweile erschreckend gut manipulieren. Wie sich solche Fälschungen technisch erkennen lassen verrät ATHENE-Forensik-Experte Prof. Martin Steinebach in der Hessenschau: https://www.hessenschau.de/tv-sendung/neue-kriminaltechnik-wie-ein-multimedia-forensiker-faelschungen-erkennt-teil-4,video-196786.html

---

ATHENE Lunch Lectures

In kostenfreien Online-Kurzvorträgen, den sogenannten „Lunch Lectures", informieren wir über aktuelle Fragestellungen wie Datenschutz, IT-Recht oder Cyber Resilience Act (CRA und auch EU NIS2 und EU Artificial Intelligence Act.

Lunch Lecture IT-Recht
02.07.2024: Das Gesetz zur Umsetzung von EU NIS2 und Stärkung der Cybersicherheit (NIS2UmsuCG): Eine rechtliche Einführung
04.07.2024: „EU Artificial Intelligence Act": Eine rechtliche Einführung
Mehr über die Lunch Lectures IT-Recht: https://www.athene-center.de/lunch-lectures-it-recht

Lunch Lecture zum CRA
25.06.2024: Cyber Resilience Act: Datenschutz-Grundverordnung und Cyber Resilience Act im Implementierungsprozess berücksichtigen
03.07.2024: Mindestsicherheitsanforderungen und Security by Design

04.09.2024: SBOM: Ein genauerer Blick auf die Software-Stückliste
23.10.2024: Coordinated Vulnerability Disclosure: Wie setzt man einen effizienten und effektiven Schwachstellenmeldeprozess auf?
Zu unseren CRA-Angeboten: https://www.athene-center.de/cra

Lunch Lecture zum Datenschutz
26.06.2024: Einführung in das Datenschutzrecht
27.06.2024: Pflicht zur Information betroffener Personen und Pflicht zur Dokumentation der Datenschutzumsetzung
Mehr über die Lunch Lectures zum Datenschutzrecht: https://www.athene-center.de/aktuelles/lunch-lectures

---

CyberUps Datenschutz-Grundverordnung - Ein Kurzüberblick

Bei den virtuellen, 45-minütigen CyberUps geben unsere Expertinnen und Experten KMUs Einblicke und Tipps rund um Cybersicherheitsthemen. Die nächsten Termine sind:
24.06.2024: Datenschutz-Grundverordnung - Ein Kurzüberblick
01.07.2024: Compliance im Datenschutzrecht - Informations- und Dokumentationspflichten der DSGVO
Die Teilnahme ist kostenfrei, eine Anmeldung ist erforderlich.

Anmleldung und Informationen zu weiteren CyberUps

T.I.S.P.-Vorbereitungskurs

Informationssicherheit wird immer wichtiger: Zum Schutz elektronischer Geschäftsprozesse suchen Unternehmen deshalb verstärkt qualifizierte Mitarbeitende, die beweisen können, dass sie den komplexen Herausforderungen beim Thema IT-Sicherheit gewachsen sind. Der TeleTrusT Information Security Professional (T.I.S.P.) ist der einzige effektive Nachweis dieser Art für Europa. Das in ATHENE mitwirkende Fraunhofer SIT bietet Seminare zur Vorbereitung auf die Prüfung an. Das nächste T.I.S.P.-Seminar findet vom **03. – 07. Juni** online statt.

Mehr über das T.I.S.P.-Seminar

Anwendertag IT-Forensik

19.09.2024 | hybrid

Der diesjährigeAnwendertag IT-Forensik mit Fokusthema "OSINT: Wahrheitssuche im Cyberspace" thematisiert die Möglichkeiten der Informationssammlung und Informationsauswertung durch die im Clear- und Darknet bereitgestellte Daten. Dabei ist es wichtig, die Plausibilität von Daten zu prüfen, die relevanten Daten zu erkennen und zwischen Wahrheit und Täuschung zu unterscheiden.

Mehr über den Anwendertag IT-Forensik

ATHENE ist ein Forschungszentrum der Fraunhofer-Gesellschaft unter Mitwirkung von

Fraunhofer SIT

Fraunhofer IGD

TECHNISCHE UNIVERSITÄT DARMSTADT

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

h_da HOCHSCHULE DARMSTADT UNIVERSITY OF APPLIED SCIENCES