ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Liebe Cybersicherheitsinteressierte,

in den letzten Wochen ist wieder so einiges bei ATHENE passiert.
Ein Forschungsteam hat einen schwerwiegenden Design-Fehler im DNSSEC aufgedeckt, der ohne Fehlerbehebung zu einem Internet-Ausfall für Millionen von Nutzenden hätte führen können.
Ein weiteres Forschungsteam der TU-Darmstadt beschäftigte sich mit der Frage, wie man Jugendliche auf TikTok besser bei der Erkennung von Desinformation unterstützen kann. Ihre Studienergebnisse dazu stellen sie demnächst auf der führenden Konferenz für Mensch-Maschine-Interaktionen vor.
Unsere Datenschutzexpertinnen am Fraunhofer SIT haben einen Ergänzungsvorschlag für die DSGVO – die Datenschutz-Vorsorge. Was sie darunter verstehen und warum sie diese Ergänzung für notwendig halten, erklären sie in einem Positionspapier.
Und natürlich gibt es auch in den kommenden Wochen wieder spannende und informative Veranstaltungen zu den unterschiedlichsten Cyberthemen, etwa unsere Lunch Lectures zum Cyber-Resiliance-Act der EU.
Bestimmt ist auch etwas für Sie dabei.

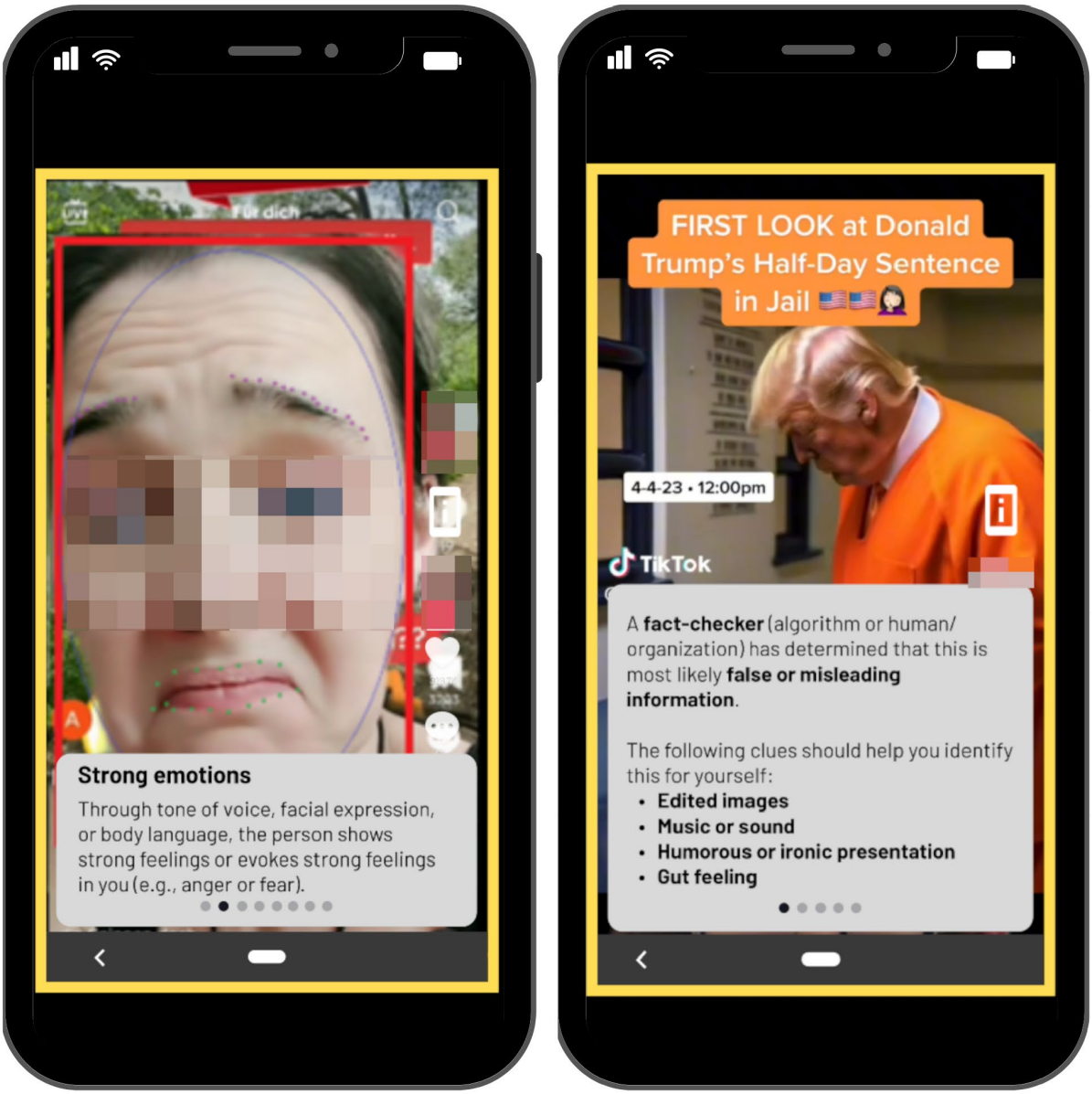
Jetzt wünschen wir Ihnen viel Freude beim Lesen unseres Newsletters.

Ihr ATHENE-Redaktionsteam

Grundlegende Design-Fehler in DNSSEC

16 Stunden ohne Internet, das hätte vielen Internetnutzenden passieren können, wenn Angreifer die Sicherheitslücke genutzt hätten, die ein ATHENE-Forschungsteam um Prof. Haya Schulmann und Prof. Michael Waidner aufgedeckt hat. Konkret fand das Team einen Design-Fehler im DNSSEC (DNS Security Extensions), der Sicherheitserweiterung des DNS (Domain Name System), die das Internet eigentlich sicherer machen soll. Die Sicherheitslücke fand große Beachtung in nationalen und internationalen Medien, unter anderem berichteten Heise, die Zeit, The Register, Dark Reading und CSO Online.
Die Forschenden arbeiteten über mehrere Monate mit allen relevanten Herstellern und großen öffentlichen DNS-Anbietern zusammen und unterstützten diese bei der Entwicklung einer Reihe von spezifischen Patches, von denen die letzten vor wenigen Tagen veröffentlicht wurden. Anbietern von DNS-Diensten wird dringend empfohlen, diese Patches sofort anzuwenden, um diese kritische Sicherheitslücke zu entschärfen.

Weitere Informationen und Q & A



Beispiel für Fehlinformation (links) und Deep Fake/manipuliertes Video (rechts)

Desinformation auf Tik Tok erkennen

Ein ATHENE-Forschungsteam der Technischen Universität Darmstadt hat erstmals untersucht, wie man Jugendliche auf der Kurzvideoplattform TikTok bei der Erkennung von Desinformation unterstützen kann. Ergebnis: Die Jugendlichen akzeptieren Warnhinweise besonders gut, wenn diese nachvollziehbar begründet werden. Anzeichen für Desinformation auf einer Videoplattform lassen sich zum Beispiel in Kommentaren oder bei den Urheber-Informationen finden, und auch emotionalisierende Musik, Mimik und Gestik können ein Hinweis auf Desinformation sein. Veröffentlicht werden die Erkenntnisse des Teams im Mai dieses Jahres auf der führenden Konferenz für Mensch-Maschine-Interaktionen, der ACM CHI Conference on Human Factors in Computing Systems, kurz CHI. Dort konnte das Team noch zwei weitere Paper platzieren.

Informationen zur Studie

Mehr Informationen zu den auf der CHI platzierten Paper

ATHENE Positionspapier fordert mehr Rechtssicherheit für Cybersicherheitsforschung

Cybersicherheitsforschende können Datenschutzvorschriften oft nicht befolgen, da sie vor Beginn einer Forschungsaktivität nicht wissen, ob und welche personenbezogenen Daten sie genau verarbeiten werden. Unsere Datenschutzexpertinnen haben deshalb einen Ergänzungsvorschlag für die DSGVO formuliert. Ihr Anliegen: Die rechtsverbindliche Einführung der Datenschutz-Vorsorge, die ungeplante Datenzugriffe berücksichtigt. Das Positionspapier, in dem sie ihr Konzept erläutern, kann unter **www.athene-center.de/datenschutz-vorsorge** kostenfrei heruntergeladen werden.

ATHENE-Direktor wird Chefredakteur der ACM TOPS

Die ACM Transactions on Privacy and Security (TOPS), eine der etabliertesten und renommiertesten wissenschaftlichen Fachzeitschriften auf dem Gebiet der Cybersicherheit und Datenschutztechnologie, hat unseren Direktor Prof. Michael Waidner zum Chefredakteur ernannt. Seine Amtszeit geht vom 1. Februar 2024 bis 31. Januar 2027.

Neues Sicherheitsproblem bei Apple-IDs

Das von ATHENE-Forschenden am Fraunhofer SIT entwickelte Test Framework "Appicaptor" hilft Unternehmen sicherzustellen, dass die von ihren Mitarbeitenden genutzten Apps den eigenen IT-Sicherheitsvorschriften entsprechen. In ihrem "Appicaptor-Blog" berichten die App-Expertinnen und -Experten über aktuelle Entwicklungen und weisen auf Sicherheitsrisiken bei der Implementierung und Nutzung von Apps – sei es iOS oder Android - hin. Ihr neuester Beitrag thematisiert mögliche Sicherheitsauswirkungen beim Wechsel von einer Unternehmens Apple-ID zu einer privaten Apple-ID bei Nutzung der Keychain, mit der Apple-User ihre Kennwörter und digitale Zertifikate verwalten können. Dieser Wechsel kann dazu führen, dass die Passwörter zur privaten Apple-ID zusammengeführt werden. Unternehmenspasswörter können dann mit allen privaten Geräten synchronisiert werden, die die private Apple-ID verwenden, was eine erhebliche Herausforderung für Organisationen darstellt, die strenge Kontrolle über Unternehmensanmeldeinformationen aufrechterhalten müssen.

Zum Blogbeitrag

ATHENE Distinguished Lectures: Ransomware und Cybercrime – sind wir noch zu retten?

Cybersecurity-Profis geben Einblicke in aktuelle Cybersicherheitsthemen: Am **12. März** erwarten wir Carsten Meywirth, Leiter der Abteilung Cybercrime im Bundeskriminalamt. In seinem Vortrag spricht er über die Probleme, mit denen Privatpersonen, Unternehmen und Strafverfolgungsbehörden durch Ransomware oder Phishing-Angriffe konfrontiert sind und spricht über Lösungsmöglichkeiten.
Die Teilnahme ist kostenfrei, eine Anmeldung ist erforderlich.

Anmeldung und Informationen zu weiteren ATHENE DLS

CyberUp für KMU: Notfallpläne für den Ernstfall

Bei den virtuellen, 45-minütigen CyberUps geben unsere Expertinnen und Experten KMUs Einblicke und Tipps rund um Cybersicherheitsthemen. Bei unserem nächsten CyberUp am **18. März** stellt Henrik Rüterjans mögliche Maßnahmen vor, mit denen sich KMUs auf Notfälle im Bereich der Informationssicherheit vorbereiten können.
Die Teilnahme ist kostenfrei, eine Anmeldung ist erforderlich.

Anmleldung und Informationen zu weiteren CyberUps

Lunch Lectures zum Cyber Resilience Act (CRA) der EU

Die EU-Kommission möchte vernetzte Produkte sicherer machen. Der Cyber Resilience Act der EU sieht deshalb vor, dass Hersteller und Händler von

vernetzten Produkten angemessene Schutzmaßnahmen für ihre Angebote vorsehen müssen. Auch wenn einige Details noch unklar sind, sollten sich betroffene Unternehmen schon jetzt vorbereiten und ihre internen IT-Sicherheitsvorkehrungen und Cybersecurity-Prozesse überprüfen. Diese betreffen zum Beispiel den Umgang mit Schwachstellen, das Update-Management oder IT-Sicherheitstests von Produkten.
In zwei kostenfreien Online-Veranstaltungen informieren unsere Expertinnen und Experten über die konkreten Auswirkungen des Cyber Resilience Act und geben Handlungsempfehlungen für die Praxis:

20.03.2024 Cyber Resilience Act: Eine rechtliche Einführung
21.03.2024 Cyber Resilience Act: Ein Überblick aus technischer Sicht

Eine Anmeldung ist erforderlich.

Zu unseren CRA-Angeboten

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