Wenn Gefahren im IT-System lauern

26.08.2026, 11:16 | IT, New Media & Software

Pressemitteilung von: *idw - Informationsdienst Wissenschaft*

Bedrohungen für IT-Systeme entstehen nicht nur durch Angriffe von außen. Innentäterinnen und Innentäter verfügen häufig bereits über legitime Zugriffsrechte und können sich deshalb vergleichsweise unauffällig innerhalb von IT-Infrastrukturen bewegen. Sie können Systeme erkunden, Informationen missbrauchen oder Schäden verursachen. Insiderbedrohungen können dabei böswillig, fahrlässig oder kollusiv entstehen. Auch kompromittierte Nutzerkonten können Angreifern die Rolle eines vermeintlich legitimen Insiders verschaffen.

Mit dem geplanten Forschungsprogramm „Negative-Trust-Architekturen“ (Ne-Trust) will die Agentur für Innovation in der Cybersicherheit GmbH (Cyberagentur) untersuchen, wie sich solche Bedrohungen zuverlässiger erkennen und wirksamer abwehren lassen.

Am Dienstag, 22. September 2026, von 14:00 bis 17:00 Uhr veranstaltet die Cyberagentur dazu ein virtuelles Partnering Event. Es richtet sich an Unternehmen, Start-ups, Hochschulen und Forschungseinrichtungen, die sich mit IT-Sicherheitsarchitekturen, Cyberabwehr oder angrenzenden technischen, sozialen und rechtlichen Fragestellungen beschäftigen.

Wenn legitimer Zugriff zum Sicherheitsrisiko wird

Etablierte Sicherheitskonzepte wie Zero Trust gehen grundsätzlich davon aus, dass keinem Zugriff automatisch vertraut werden sollte. Identitäten und Berechtigungen werden kontinuierlich geprüft, Zugriffsrechte begrenzt und IT-Systeme stärker segmentiert. Diese Prinzipien können die Widerstandsfähigkeit digitaler Infrastrukturen erheblich erhöhen.

Bei Insiderbedrohungen bestehen jedoch besondere Herausforderungen. Personen oder kompromittierte Konten können bereits über gültige Berechtigungen verfügen und damit zunächst regelkonform erscheinen. Auch zentrale Grundlagenwerke wie die NIST-Leitlinie SP 800-207 weisen auf verbleibende Lücken und weiteren Forschungsbedarf hin.

Zusätzlich verändert Künstliche Intelligenz die Bedrohungslage. KI-gestützte Methoden können Angriffe automatisieren, Täuschungen glaubwürdiger gestalten und Schwachstellen gezielter ausnutzen. Solche Entwicklungen betreffen auch IT-Systeme in Verwaltung, Verteidigung und Sicherheitsbehörden.

Negative Trust als eigenständiger Forschungsansatz

Ne-Trust setzt an diesen Grenzen bestehender Sicherheitskonzepte an. Technologieoffen und interdisziplinär sollen eigenständige Negative-Trust-Paradigmen sowie entsprechende Referenzarchitekturen für IT-Systeme untersucht und entwickelt werden. Dabei geht es nicht allein darum, Zugriffe stärker zu kontrollieren. Erforscht werden soll vielmehr, wie Systeme verdächtiges Verhalten innerhalb ihrer eigenen Strukturen erkennen und darauf proaktiver reagieren können.

Die Wirksamkeit solcher Ansätze gegen unterschiedliche Formen von Insiderbedrohungen soll untersucht, messbar gemacht und anhand technischer Umsetzungen demonstriert werden. Neben technischen Fragen sollen auch soziale Auswirkungen und rechtliche Rahmenbedingungen berücksichtigt werden.

Negative Trust ist bislang kein wissenschaftlich etabliertes IT-Sicherheitsparadigma. Erste begriffliche Ansätze bestehen beispielsweise in Richtung sogenannter Deception Technology. Diese arbeitet gezielt mit Täuschungselementen, um Angreifer zu erkennen, ihr Verhalten zu beobachten oder sie von relevanten Systembereichen abzulenken. Eine umfassende wissenschaftliche und interdisziplinäre Auseinandersetzung mit Negative Trust als eigenständigem Sicherheitsparadigma steht jedoch noch aus.

Ne-Trust soll diese Forschungslücke adressieren. „Das Forschungsprogramm überträgt den Negative-Trust-Begriff in diesem Kontext erstmalig in den wissenschaftlichen Diskurs“, erklärt Felix Dotzauer, Programmleiter und Forschungsreferent in der Abteilung Cybersicherheit komplexer Systeme. „Somit können frühzeitig neue Ansätze für IT-Sicherheitsarchitekturen untersucht werden, die Insiderbedrohungen effektiver adressieren, Abwehrfähigkeiten von IT-Systemen weiterdenken und über heutige Schutzkonzepte hinausreichen“.

Partnering Event bringt unterschiedliche Kompetenzen zusammen

Die fachliche Breite des Programms erfordert unterschiedliche Perspektiven. Das Partnering Event soll deshalb potenzielle Forschungspartner miteinander in Kontakt bringen und die Bildung interdisziplinärer Konsortien unterstützen.

Nach einer Vorstellung der Cyberagentur und des Forschungsprogramms Ne-Trust erhalten die Teilnehmenden die Möglichkeit, ihre fachlichen Schwerpunkte in jeweils zweiminütigen Kurzpräsentationen vorzustellen. Auf diese Weise können Kompetenzen sichtbar gemacht, Schnittstellen identifiziert und mögliche Partnerschaften für spätere Forschungsprojekte angebahnt werden.

Die Anmeldung zum Partnering Event ist bis einschließlich 16. September 2026 ist unter folgendem Link möglich. Teilnehmende, die sich während der Veranstaltung vorstellen möchten, senden ihre Präsentationsfolie bis spätestens 18. September 2026 an ne-trust@cyberagentur.de.

Weitere Informationen:
https://www.cyberagentur.de/programme/ne-trust/

Pressekontakt:

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 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:
Felix Dotzauer, Programmleiter und Forschungsreferent in der Abteilung Cybersicherheit komplexer Systeme

Originalpublikation:
https://www.cyberagentur.de/presse/wenn-gefahren-im-it-system-lauern/

Agentur für Innovation in der Cybersicherheit GmbH

MichaelLindner (Mitarbeiter in der Presse- und Öffentlichkeitsarbeit)

+49 151 44150645

lindner@cyberagentur.de

News-ID: 1321626 • Views: 68 (Stand: 27.08.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/1321626/Wenn-Gefahren-im-IT-System-lauern-idw.html