

SIMEDIA-Innovationsforum

Künstliche Intelligenz in der Unternehmenssicherheit

– Chancen, Risiken und Herausforderungen –

Neues
Zukunftsforum



4. Juni 2024 in Eschborn bei Frankfurt

Vorwort

Sicherer Umgang mit KI

Steigende Rechenleistung, neue Algorithmen und wachsende Datenmengen haben dazu geführt, dass sich Künstliche Intelligenz (KI) und KI-Systeme durchgesetzt haben, bereits eingeführt wurden oder im Prozess der Etablierung stehen und somit aus der Zukunft der Unternehmenssicherheit nicht mehr wegzudenken sind. In Folge investieren diverse Firmen weltweit mit steigender Tendenz in KI. Doch wie sicher ist der Einsatz von KI neben all den Chancen, die sie bietet?

„Das Risiko der Auslöschung durch KI zu entschärfen, sollte weltweit die Priorität anderer gesamtgesellschaftlicher Risiken wie Pandemien und Nuklearkrieg haben.“ Mit der im Mai vergangenen Jahres veröffentlichten Aussage auf der Website des Thinktanks Center for AI Safety (CAIS) aus San Francisco warnten Führungsebenen vor der Künstlichen Intelligenz als Gefährdung der Menschheit. Unterscriben worden war der Aufruf von Chefs namhafter KI-Unternehmen, unter anderem von OpenAI. Trotz der Warnung blicken laut einer Studie von Forbes die meisten Unternehmer der Entwicklung von KI positiv entgegen. Über die Hälfte der befragten Firmen sehen Potenzial zur Steigerung der Produktivität, Verbesserung der Kundenbeziehungen sowie Vorantreiben des Umsatzwachstums. So wird KI oft mit dem Ziel eingesetzt, zum Beispiel Abläufe und Prozesse zu optimieren, Kommunikation mit Kunden zu verbessern, Cybersicherheit zu gewähren, für Personalbeschaffung, Lieferketten, Zeit- und Kosteneinsparungen, Vermeidung menschlicher Fehler u.v.a.

Damit das Zusammenspiel Mensch und Maschine effizient funktionieren kann, spielen Richtlinien, Ethik & Moral, Mitarbeiter und vor allem Sicherheitsvorkehrungen eine bedeutende Rolle. So verabschiedete im Juni 2023 das Europäische Parlament seine Verhandlungsposition zum Gesetz über Künstliche Intelligenz, dem weltweit ersten umfassenden Regelwerk zur Bewältigung von KI-Risiken.

Das neue Zukunftsforum „KI in der Unternehmenssicherheit“ der SIMEDIA Akademie widmet sich in erster Linie der Frage der Sicherheit beim Einsatz von KI sowie dem Einsatz KI zur Steigerung der Sicherheit von Unternehmen.

Zielgruppe:

Sicherheitsverantwortliche, Bauabteilungen/Facility Management, Planer und Projektsteuerer in Unternehmen, Revision, Mitarbeiter Corporate Security, Betreiber und Mitarbeiter von Leitzentralen, Videoüberwachung, Zutrittskontrollanlagen, Rechenzentren und IT

Programm 4. Juni 2024

- 09:00 Uhr** **Begrüßung, Einführung und Moderation**
Peter Loibl, VON ZUR MÜHLEN'SCHE GmbH
- 09:15 Uhr** **KI, alles nur ein Hype? Visuelle KI in der Videotechnik – Möglichkeiten und Grenzen**
Robert Schwerdtner, Rola Security Solutions GmbH
- ▶ allgemeiner Einstieg in die Welt der KI
 - ▶ was bedeuten Large Language Models (LLMs) wie ChatGPT oder ist alles nur ein Hype?
 - ▶ Fokus auf die Visuelle KI – Interpretation von Signalen und keine Generierung
 - ▶ ein Blick auf echte Usecases und der zielgerichtete Weg zu einem echten Nutzen
- 10:00 Uhr** **KI gegen KI: Wie Deepfakes mit Hilfe maschinellen Lernens erkannt werden können**
Dr. Nicolas Müller, Fraunhofer Institut
- ▶ Was sind Deepfakes, und wie werden sie erstellt?
 - ▶ Überblick Bedrohungslage: Wie werden Deepfakes für Betrug, Meinungsmache und Desinformation eingesetzt?
 - ▶ Wie kann man sich schützen? Überblick über die Gegenmaßnahmen Medienkompetenz, KI-basierte Deepfake-Erkennung, und Content Authenticity.
 - ▶ Kann man Deepfakes überhaupt zuverlässig erkennen?
 - ▶ Wie wird sich die Technologie weiterentwickeln?
 - ▶ Erklärbare KI: Wie können wir verstehen, was KI lernt, und lernt sie das „Richtige“?
 - ▶ Hands-On: Welche Tools kann man nutzen, um Deepfakes zu erkennen, Inhalte zu verifizieren, oder auch sein Gehör in der Erkennung zu schulen?
 - ▶ Die andere Seite der Medaille: Der ethische Einsatz von KI-Deepfakes
- 10:45 Uhr** **Kaffeepause**
- 11:15 Uhr** **KI-Einsatz im globalen Sicherheitslagezentrum**
Karl-Peter Becker, DHL Group
- ▶ Problem der Datenflut im Lagezentrum
 - ▶ Wo kann Maschinelles Lernen und KI unterstützen?
 - ▶ Wege zur Implementierung
 - ▶ Risiken und Chancen generativer KI im Sicherheitslagezentrum
 - ▶ Zukunft des Analysten in Zeiten generativer KI

Programm 4. Juni 2024

- 12:00 Uhr** **SPELL – Die Zukunft der Leitstelle mit KI beginnt 2024**
Dr. Eric Rietzke, Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI)
- ▶ Das Überwinden sektoraler Grenzen
 - ▶ ein gemeinsames Lagebild zwischen Leitstellen
 - ▶ KI zur Bewältigung der Informationsflut
 - ▶ KI als Entscheidungsunterstützung
- 12:45 Uhr** **Mittagessen**
- 14:00 Uhr** **Logistik in der Krise: Und nun? Mit KI-Unterstützung zu mehr Krisenresilienz**
Dr. Jan-Ole Berndt, Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI)
- ▶ Wissen ist Resilienz: Die Rolle von KI zur Entscheidungsunterstützung im Krisenmanagement
 - ▶ Tun, was getan werden muss: Entscheidungsprozesse mit KI-Unterstützung gestalten
 - ▶ Was-wäre-wenn-Szenarien: Die Macht der KI und die Ohnmacht der Vernunft
 - ▶ Daten und Modelle in der Krise: Über die Ohnmacht der KI
 - ▶ Krisenreaktion und Erklärung: Warum es trotzdem funktioniert
- 14:45 Uhr** **KI als Sicherheitsgarant der Zukunft? Szenarien, Technologien, Entwicklungspotenziale**
Peter Loibl, VON ZUR MÜHLEN'SCHE GmbH
- ▶ Grundsätze von KI-Anwendungen
 - ▶ Einsatzszenarien von KI in der Sicherheit – 360° Rundumblick
 - ▶ Operativ – neue Formen bei Überwachung, Detektion, Alarmmanagement
 - ▶ Planung, Konzeption, Betrieb
 - ▶ Veränderte Aufgabenbereiche
 - ▶ Risiko- und Restriktionsfaktoren – Einschätzung
 - ▶ KI- Responsibility: Welche Leitplanken braucht es?
- 15:30 Uhr** **Kaffeepause**

Programm 4. Juni 2024

- 16:00 Uhr** **Rechtssichere KI in der Sicherheit: Potenziale und Herausforderungen**
Prof. Dr. Johannes Berens, Studiengangsleiter General Management der Rheinischen Hochschule Köln, Research Associate Bergische Universität Wuppertal, Consultant und Partner Concepture GmbH
- ▶ Verfahren von KI ein „eigenes Wesen“?
 - ▶ Handeln innerhalb definierter Grenzen: Automatisierung versus Autonomie
 - ▶ Prüfung rechtskonformer künstlicher Intelligenzen
 - ▶ Merkmale künstlicher Intelligenzen
 - ▶ Was sind die wichtigsten Anwendungsgebiete und wesentlichen Konflikte von KI mit geltendem Recht?
 - ▶ Rechtsentwicklung in der Zukunft: Wie soll ein Spezialrecht für künstliche Intelligenzen aussehen?
- 17:00 Uhr** **KI und Intelligence Analysis – ein praktisches Deepdive**
Matt Kish, Siemens AG
- ▶ Die Geschichte hinter unserem intern-entwickelt KI-Bot (AthenaBot)
 - ▶ Warum wir unseren AthenaBot entwickelt haben
 - ▶ Unter der Haube unseres AthenaBots
 - ▶ Was unsere wichtigsten gewonnenen Erkenntnisse sind
 - ▶ Was könnten die nächsten Schritte sein
- 17:45 Uhr** **Abschließende Diskussion**
- 18:00 Uhr** **Abschluss und Ende des Forums**
-

Referenten



Becker, Klaus-Peter

Betreut als Senior Security Expert die Themen Digitalisierung, Automatisierung und KI in der Konzernsicherheit der DHL Group. Zuvor war er dort als Lageanalyst im globalen Sicherheitslagezentrum tätig. Er hat einen Master of Science in Security Risk Management der Universität Kopenhagen.



Prof. Dr. Berens, Johannes

Partner der concepture GmbH und Consultant für Fragestellungen des maschinellen Lernens und Sicherheitsmanagementsysteme. Seit 2016 entwickelte er an der Bergischen Universität Wuppertal in mehreren BMBF geförderten Forschungsprojekten eine KI zur Prognose drohender Studienabbrüche. Zwischen 2008 und 2015 gründete und leitete er an der Rheinischen Fachhochschule Köln gGmbH vier Außenstellen. Dort ist er bis heute Studiengangsführer für die Masterstudiengänge „Generell Management“ und „International Business Administration“.



Dr. Berndt, Jan-Ole

Diplom in Informatik mit den Schwerpunkten Robotik und Künstliche Intelligenz im Jahr 2009 sowie Promotion im Jahr 2015 von der Universität Bremen. Er ist heute stellvertretender Leiter des Themenfeldes „Kognitive Sozialsimulation“ am Deutschen Forschungszentrum für Künstliche Intelligenz (DFKI) in Trier. Seine Forschungsschwerpunkte reichen vom Einsatz Künstlicher Intelligenz in der Logistik zur automatischen Steuerung verteilter Prozesse bis zur Simulation von Prozessen, in denen Menschen im Zentrum stehen. Er leitet verschiedene anwendungsorientierte Projekte in den Bereichen des simulationsbasierten Krisenmanagements und der Gestaltung klimagerechter Transformationen in Energie und Logistik.

Referenten



Kish, Matthew

Er ist ein erfahrener Sicherheits- und Risk Intelligence Experte und war 13 Jahre lang in The Intelligence Corps der britischen Armee tätig, bevor er in zivile Positionen wechselte. Derzeit arbeitet er in München, Deutschland, als Leiter des Situation and Intelligence Analysis Teams bei Siemens und ist verantwortlich für die Bereitstellung und Analyse von sicherheitsrelevanten Informationen für Siemens' weltweite Operationen rund um die Uhr. Er ist zusätzlich Mitglied des neu einberufenen Data Hub innerhalb der globalen Unternehmenssicherheitsabteilung von Siemens. Vor seinem Eintritt bei Siemens im Jahr 2018 war Matt als Intelligence Manager für Deloitte in Großbritannien tätig und bot internen und externen Kunden eine auf soziale Medien fokussierte Risikowahrnehmungs- und Intelligence-Lösung an. Während seiner Zeit bei der britischen Armee absolvierte Matt mehrere Auslandseinsätze in Afghanistan und Irak sowie (kurzfristige) Verbindungseinsätze in Afrika und Osteuropa, bei denen er Intelligence-Unterstützung für multinationale Operationen leistete. Er hat einen Master-Abschluss in Intelligence & Security Studies von der Brunel University London und hat ein besonderes Interesse an Prognosen, künstlicher Intelligenz und Daten in der Intelligence Analysis.



Loibl, Peter

Dipl.-Ing. Nachrichtentechnik, Master of Laws (LL.M.). Geschäftsführer der VON ZUR MÜHLEN'SCHE GmbH, Bonn. ISMS ISO 27001 Lead Auditor. Seit 1993 u. a. in umfangreichen Projekten mit der Beratung und Planung von Videosystemen und Leitstellen befasst. Mitglied im Arbeitskreis Alarmempfangsstellen der DKE.



Dr. Müller, Nicolas

Promotion 2022 an der Technischen Universität München im Fachbereich Informatik mit der Dissertation über „Integrität und Korrektheit von KI-Datensätzen“. Davor absolvierte er ein Studium in Mathematik, Informatik und Theologie an der Universität Freiburg, das er 2017 mit Auszeichnung abschloss. Seit 2017 ist er als Machine Learning Scientist am Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC) tätig, speziell in der Abteilung Cognitive Security Technologies. Sein Forschungsschwerpunkt liegt auf der Zuverlässigkeit von KI-Modellen, der Identifizierung von Machine-Learning Shortcut und der KI-gestützten Erkennung von Audio-Deepfakes.

Referenten



Dr. Rietzke, Eric

Dr. rer. nat., Business Information Systems, Diplom Informatiker (FH) – Fachrichtung Maschinenbau; Er ist Projektleiter des Deutschen Forschungszentrums für Künstliche Intelligenz (DFKI) und Geschäftsführer der LiveReader GmbH. Zuvor war er über 20 Jahre im Vorstand Silvercreations Software AG tätig. Im Zentrum seiner Forschung steht eine umfassende Wissensrepräsentation und neue KI-basierte Methoden, um aus Daten und Wissen zunächst Erkenntnisse und anschließend Handlungen ableiten zu können. Diese Form des „Knowledge Computings“ zielt darauf ab, die Menschen bei ihrer Arbeit zu unterstützen und nutzt dazu die Fähigkeiten einer symbolischen und damit auch erklärbaren KI.



Schwerdtner, Robert

Leiter SolutionDesign und Innovations bei der Rola Security Solutions GmbH, verantwortlich für den Bereich „Neue Technologien“. Zuvor Notfall- und Krisenmanager im Konzernlagezentrum der Deutschen Telekom AG, verantwortlich für die Integration verschiedenster Social Media Thematiken. Fachliche Spezialisierung unter anderem in den Bereichen Datenschutz (UDIS), Social Media Management (MC), Projektmanagement (IPMA) sowie Krisenmanagement (CECM, SIMEDIA). Experte zu den Themen Social Media Nutzung, Monitoring, KI und Recht.

Anmeldebedingungen

Veranstaltungsort

Mercure Hotel Frankfurt Eschborn Ost, Helfmann-Park 6, 65760 Eschborn, Telefon: +49 06196 901 0, E-Mail: h0491-sb@accor.com. Es steht **bis 4 Wochen** vor Veranstaltungsbeginn ein begrenztes Zimmerkontingent zur Verfügung. Bitte nehmen Sie die Reservierung unter Berufung auf Ihre Teilnahme an dem Forum selbst vor. Stichwort: SIMEDIA.

Kosten

Die Teilnahmegebühr für die Veranstaltung beträgt 850,00 €. Die Preise verstehen sich zusätzlich Mehrwertsteuer. Darin enthalten sind eine ausführliche Dokumentation, Mittagessen, Erfrischungen und Pausenverpflegung.

Anmeldung

Ihre Anmeldung und Zahlung richten Sie bitte an die SIMEDIA Akademie GmbH, Alte Heerstraße 1, 53121 Bonn. Nach Eingang Ihrer Anmeldung, die Sie telefonisch +49 228 9629370, per E-Mail anmeldung@simedia.de oder über das Internet unter www.simedia.de vornehmen können, erhalten Sie die Anmeldebestätigung und detaillierte Informationen zur gebuchten Veranstaltung sowie das Hotel. Die SIMEDIA Akademie behält sich vor, Anmeldungen ohne Angabe von Gründen abzulehnen.

Stornierung/Rücktritt

Wenn Sie bereits verbindlich zu einer Veranstaltung angemeldet sind, aber nicht teilnehmen können, stehen Ihnen folgende Möglichkeiten zur Verfügung:

Bis unmittelbar vor Beginn einer Veranstaltung können Sie einen Kollegen (Ersatzperson) benennen. Dafür entstehen Ihnen keine weiteren Kosten.

Bis 4 Wochen vor der Veranstaltung können Sie die Teilnahme kostenlos stornieren. Der Rücktritt muss immer schriftlich (per E-Mail) erfolgen.

- Erfolgt der Rücktritt zwischen 30 und 8 Tagen vor Veranstaltungsbeginn, werden wir 50% der Teilnahmegebühr berechnen
- Erfolgt der Rücktritt nach weniger als 8 Tagen vor der Veranstaltung, ist die volle Teilnahmegebühr zu entrichten

Erscheint der Teilnehmer nicht, ohne abgesagt zu haben, sind wir berechtigt, die volle Veranstaltungsgebühr in Rechnung zu stellen. Sollte die Veranstaltung seitens SIMEDIA Akademie GmbH abgesagt werden, so besteht ein Anspruch auf volle Rückerstattung der Teilnahmegebühr; Ansprüche darüber hinaus bestehen nicht.

Programmänderungen

Änderungen bleiben vorbehalten.

Wir über uns

Die SIMEDIA Akademie GmbH steht in Deutschland für hochwertige Seminare, Foren und Zertifikatslehrgänge. Ausgewählte, praxiserfahrene Referenten vermitteln umfassendes Wissen zu aktuellen Themen rund um die betriebliche Sicherheit. Darüber hinaus schätzen Nachwuchs- und Führungskräfte unsere Veranstaltungen als wertvolle Informations- und Erfahrungsbörsen. Die SIMEDIA Akademie GmbH ist eine Schwesterfirma der VON ZUR MÜHLEN'SCHE GmbH, Sicherheitsberatung – Sicherheitsplanung. Weitere Informationen erhalten Sie im Internet unter: www.simedia.de.