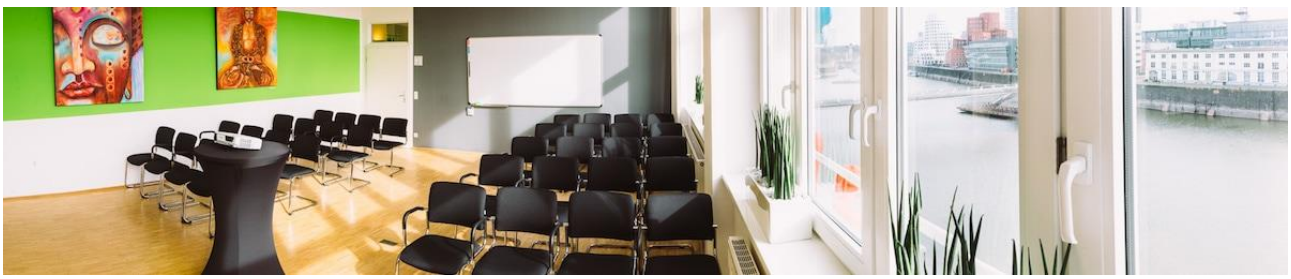
Agenda CCV-Arbeitskreis AI & Robotics 19.06.2024 in Düsseldorf

Die CCV-Arbeitskreisleiter AI & Robotics Rainer Wilmers, Ralf Mühlenhöver und Sascha Poggemann laden unter dem Motto **„KI im Kundenservice: Praxisnahe Einblicke, Erfolgsgeschichten, Lernen und (Er-)Arbeiten"** zum ersten Präsenz-Event des Arbeitskreises nach Düsseldorf ein.

Hinweis: Mitglieder des CCV-Arbeitskreises nehmen kostenfrei teil, für CCV-Mitglieder erheben wir eine Teilnahmegebühr in Höhe von 99€, für CCV-Interessenten in Höhe von 199€. Sollten sich nicht ausreichend Teilnehmende anmelden, behalten wir uns die Absage der Veranstaltung bis 14 Tage vor dem Termin vor.

Ab 11:30 Uhr Get together und Networking bei Snacks und Getränken

Startplatz Düsseldorf GmbH
Speditionstr. 15 · 40221 Düsseldorf
www.startplatz.de



13:00 Uhr **Begrüßung**

Leiter des CCV-Arbeitskreises Ai & Robotics: Rainer Wilmers, Ralf Mühlenhöver und Sascha Poggemann

CCV-Präsident: Dirk Egelseer


13:10 Uhr **Aktuelles aus dem Verband**

Dirk Egelseer

13:20 Uhr **Kennenlernen der Teilnehmer – 20 mal 2 - Methode!**

14:00 Uhr **Vortrag: „Gezieltes Kompromittieren von Sprachmodellen“ - Wie man Generative KI ganz einfach hacken kann**

Dr. Christoph Endres, Geschäftsführer der sequire technology GmbH

Große Sprachmodelle (LLMs) werden aktuell vielfältig und intensiv genutzt, aber sind anfällig für Angriffe. Bisher wird diese Möglichkeit sehr wenig, bzw. rein aus der Perspektive des Datenschutzes betrachtet. Das reicht aber bei weitem nicht aus; die wirklich relevanten Bedrohungen sind ganz woanders, und es ist nur eine Frage der Zeit, bis sie real werden.

Indirect Prompt Injection ermöglicht eine ferngesteuerte Übernahme von LLM-Anwendungen im großen Stil. Dabei schmuggelt ein Angreifer über externe Quellen (Webseiten, Dokumente, etc.) versteckte Anweisungen in den Dialogkontext eines Sprachmodells, und bringt den Dialog unter seine Kontrolle. Der Nutzer bekommt davon nichts mit.

Diese Schwachstelle wurde von sequire technology im Februar 2023 veröffentlicht und demonstriert. Dazu gab es ausführliche Gespräche mit betroffenen Anbietern, wie beispielsweise Microsoft, OpenAI und Google. Im Ranking der gefährlichsten Schwachstellen von Sprachmodellen (OWASP Top 10) wurde Prompt Injection als Top 1 Bedrohung gelistet; das Bundesamt für Sicherheit in der Informationstechnik veröffentlichet ein Warnung basierend auf der Arbeit von sequire.

Im Vortrag diskutiert Dr. Christoph Endres die Bedrohungen von Großen Sprachmodellen, erläutert Indirect Prompt Injection im Detail, gibt Beispiele für aktuelle und zukünftige Angriffe und erklärt, warum die bisherigen Abwehrmaßnahmen nicht funktionieren bzw. ausreichen werden.

14:45 Uhr **Networkingpause**

15:15 Uhr **Collective Wisdom AI Workshops – Teilnehmer fragen, Teilnehmer antworten**
In einer interaktiven Session werden konkrete (auch anonym gestellte) Fragen einzelner Teilnehmer zu KI-Themen im Unternehmen von Kleingruppen beantwortet – menschliche Schwarmintelligenz in Zeiten von zunehmender Maschinenintelligenz.

15:45 Uhr **Echte-Welt-Beispiele: „Wie uns diese 10 KI-Tools im täglichen Berufsleben unterstützen können“**
Die drei Arbeitskreis-Leiter stellen ihre Lieblings-Helfer und Tipps und Tricks vor, wie KI heute ganz konkret bestimmte Aufgaben vereinfacht oder übernimmt.

16:15 Uhr **Vortrag: „Weniger messen, mehr wissen – Potenziale KI-gestützter Kontaktanalyse für das Qualitätsmanagement der Zukunft“**

Sven Ley, Abteilungsleiter Qualitätsmanagement, Deutsche Post, berichtet über die ersten Schritte einer KI-gestützten Qualitätsmessung im Kundenservice und welche Use-Cases und Änderungen im Unternehmen sich daraus ergeben.
Möglichkeiten zur Reduzierung des Prüfaufwandes, zuverlässige Identifikation von Einflussfaktoren auf Qualität, Kundenzufriedenheit und Kosten.

16:35 Uhr **Impuls: „KI und BPO - Freund oder Feind?“**

Roman Salem, Vice President bei Teleperformance, berichtet aus dem eigenen Unternehmen und stellt dar, wie den immer höher werdenden Anforderungen der Kunden mit KI-basierten Assistenz- und Automatisierungslösungen begegnet wurde. Was hat geklappt, was wurde gelernt?

16:45 Uhr **Podiumsdiskussion „AI und CC-Dienstleister: Wohl oder Wehe?“**
Unsere Experten tauschen sich unter Leitung des CCV-Präsidenten Dirk Egelseer dazu aus, wie KI ihr Business heute schon verändert – positiv und negativ. Eine offene Diskussion mit offenem Ausgang.

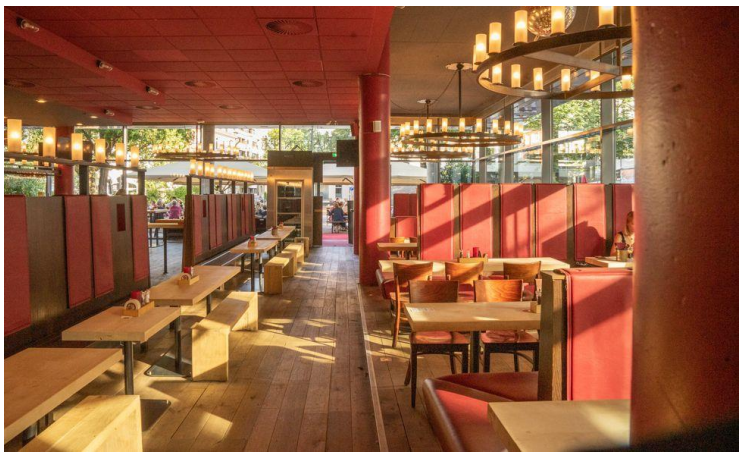
- Roman Salem, Vice President, Teleperformance
- Jürgen Thom, CSO, Snubes
- Sven Ley, Abteilungsleiter Qualitätsmanagement, Deutsche Post
- Kevin Filz, Director CX Management, Foundever

17:15 Uhr **Zusammenfassung & Feedback**

18:00 Uhr **Abschluss mit anschließendem Spaziergang zum Restaurant**

18:15 Uhr **Gemeinsames Abendessen (Selbstzahler)**

Eigelstein
Hammer Straße 17
40219 Düsseldorf



Das Fußballspiel Deutschland – Ungarn wird im Eigelstein übertragen… Das Restaurant bittet jedoch um einen Mindestverzehr in Höhe von 25€ pro Person.