v

LEARNTEC

2. – 4. Februar 2027
Messe Karlsruhe

„Sich nicht sofort vom KI-Tsunami mitreißen lassen“

LEARNTEC 2027: Interview mit Dr. Constanze Kurz, Informatikerin und Sprecherin des Chaos Computer Club

„Ohne KI is nich“. So könnte man die derzeitige Haltung beschreiben, die bei vielen Menschen im Alltag vorherrscht. Da werden Reisen geplant, Krankheiten recherchiert, Tipps eingeholt und das System dabei mit Daten gefüttert – Sicherheit und Datenschutz sind oft zweitrangig. Für Unternehmen wäre ein ähnliches Laisser-faire nicht möglich oder sogar bedrohlich. Dennoch lässt der KI-Hype vielen Firmen kaum Zeit, sich intensiv mit deren Risiken auseinanderzusetzen. Zu groß die Angst, abgehängt zu werden, wenn man nicht auf den KI-Zug aufspringt. Wir haben mit der Informatikerin Dr. Constanze Kurz über Sicherheitslücken bei der Nutzung von KI gesprochen und sie gefragt, wie Unternehmen vorgehen sollten, wenn sie die Technologie sicher einführen möchten. Dr. Kurz ist Sprecherin des Chaos Computer Club und wird auf dem LEARNTEC Kongress mit ihrem Vortrag „KI und IT-Sicherheit - Keine Panik?!“ genau jene Themen aufgreifen, die viele Unternehmen in Sachen IT-Sicherheit aktuell umtreiben.

Im September warnten KI-Entwickler von Anthropic und Open AI vor den Gefahren künstlicher Intelligenz. Für manche Panik-PR, für andere durchaus ernstzunehmend. Wie ordnen Sie das ein?
Dr. Constanze Kurz: Aus meiner Sicht tendiert das Pendel auch eher in die Richtung Panik-PR. Ich finde die Beschreibungen, welche Gefahren uns drohen, massiv übertrieben. Natürlich sind die großen Sprachmodelle, die von Anthropic und OpenAI angeboten werden, aus technischer Perspektive sehr interessant. Aber sie sind nun sicherlich nicht der Sargnagel der Menschheit. Hier werden die Fähigkeiten dieser großen Sprachmodelle überschätzt.

Unternehmen, die KI einsetzen, denken natürlich weniger an den Untergang der Menschheit, sondern an ganz konkrete Sicherheitslücken: Was passiert mit meinen Daten? Bin ich verwundbarer, selbst wenn ich ein Private LLM nutze?
Dr. Constanze Kurz: Man muss hier unterscheiden zwischen der sogenannten Frontier AI – also den ganz großen Sprachmodellen – und der Technik generell. Wenn ich Sprachmodelle in kleinerem Maße selbst betreibe, dann kann ich auch die Risiken anders beherrschen. Wenn wir aber über die großen generativen Sprachmodelle, diese Allrounder, reden, dann ist die eigentliche Gefahr nicht so sehr der Datenschutz, sondern die Wirtschaftsspionage.

Es geht nicht nur um Daten, sondern eben auch um strukturelles Wissen aus Unternehmen. Da stellt sich die Frage: Wer wertet eigentlich diese

Ansprechpartnerin Katrin Wagner
tel +49 721 3720-2308 | katrin.wagner@messe-karlsruhe.de

Karlsruher Messe- und Kongress GmbH
Festplatz 9
76137 Karlsruhe
tel +49 721 3720-0
fax +49 721 3720-99-2116
info@messe-karlsruhe.de
messe-karlsruhe.de

Messe Karlsruhe
Messeallee 1
76287 Rheinstetten

Kongresszentrum
Festplatz 9
76137 Karlsruhe

Geschäftsführerin
Britta Wirtz

Vorsitzende des Aufsichtsrats
Bürgermeisterin
Gabriele Luczak-Schwarz

Reg.-Ger. Mannheim
HRB 100147

Mitglied
AUMA | FKM | GCB
IDFA | EVVC | ICCA

learntec.de

messe karlsruhe

Informationen aus, wenn ich solche Modelle benutze? Darauf gibt es keine einheitliche Antwort, da die einzelnen Anbieter das ganz unterschiedlich handhaben.

Und zum Thema Datenschutz: Es ist natürlich ein Problem, wenn Sie sich über höchstpersönliche Inhalte mit einem Chatbot unterhalten. Dann müssen Sie davon ausgehen, dass diese Daten auch ausgewertet werden – das sichern die Anbieter in der Regel auch über ihre Allgemeinen Geschäftsbedingungen ab.

Prinzipiell ist es ein vielschichtiges Problem – im Bereich Datenschutz, im Bereich Wirtschaftsspionage oder Compliance. Damit müssen sich Unternehmen wirklich auseinandersetzen. Das müssen sie aber bei jeder Software, die sie in ihr Unternehmen integrieren möchten.

Bei der LEARNTEC konnten wir in den vergangenen Jahren sehen, dass KI auch vermehrt im HR-Bereich genutzt wird, bei der Skill-Gap-Analyse oder bei Beurteilungen – mit dem Ziel, Mitarbeitende entsprechend zielgerichteter zu schulen und Lücken aufzuzeigen. Was müssen Unternehmen hier beachten?
Dr. Constanze Kurz: Wenn man Mitarbeitende oder Bewerber hat, ist man natürlich erst einmal verantwortlich für die personenbezogenen Daten, die an das Unternehmen weitergegeben werden oder die man zu schützen hat, – auch rechtlich.

Personal, Weiterbildung – das sind strukturelle Daten über Unternehmen, die sensibel sein können. Hier muss ich natürlich mit Vorsicht vorgehen und diese schützen, nicht unbedingt spezifisch für KI oder Sprachmodelle, sondern auch bei anderer Software. Wenn ich Software in mein Unternehmen hole und Daten abfließen können, dann ist das ein rechtliches, ein Datenschutz- und ein IT-Sicherheitsproblem.

Mein Eindruck ist aber, dass durch die Schnelligkeit, mit der sich viele Unternehmen KI-Anwendungen ins Haus geholt haben, diese Fragen am Anfang gar nicht betrachtet wurden. Jetzt sind wir im vierten Jahr dieser großen KI-Welle und plötzlich lassen sich diese Fragen eben nicht mehr länger ignorieren.

Das große Problem ist, dass viele der großen Sprachmodellanbieter über ihre Geschäftsbedingungen kein Modell offerieren, das mit personenbezogenen Daten nach der europäischen Datenschutzlage wirklich in Ordnung wäre. Es muss aber niemand auf die großen Anbieter setzen: Unternehmen können auch eigene Modelle betreiben oder sich Anbieter suchen, die eine bessere

Karlsruher Messe- und Kongress GmbH
Festplatz 9
76137 Karlsruhe
tel +49 721 3720-0
fax +49 721 3720-99-2116
info@messe-karlsruhe.de
messe-karlsruhe.de

Messe Karlsruhe
Messeallee 1
76287 Rheinstetten

Kongresszentrum
Festplatz 9
76137 Karlsruhe

Geschäftsführerin
Britta Wirtz

Vorsitzende des Aufsichtsrats
Bürgermeisterin
Gabriele Luczak-Schwarz

Reg.-Ger. Mannheim
HRB 100147

Mitglied
AUMA | FKM | GCB
IDFA | EVVC | ICCA

learntec.de

Datenschutzlage haben – oder zumindest im europäischen Datenschutzraum bessere Bedingungen bieten.

Sie haben das Thema Schnelligkeit angesprochen: Mir scheint, die Gesetzgebung kann mit dem technologischen Fortschritt nicht recht mithalten. Wo sehen Sie da auch strukturelle Grenzen staatlicher Regulierung in Sachen IT-Sicherheit bei KI? Wo muss ein Unternehmen einfach in Eigenverantwortung handeln?
Dr. Constanze Kurz: Natürlich steht die gesetzliche Regulierung in Deutschland, aber auch in Europa, immer hinter den technologischen Entwicklungen. Aber ich halte das nicht für eine große Gefahr. Besser ist es, sich auch Zeit zum Nachdenken zu nehmen und zu überlegen, wie man es richtig macht. Eine sehr schnelle Gesetzgebung ist nicht immer eine gute. Im Gegenteil: Meine Erfahrung zumindest bei technischen Themen ist, dass es in der Regel Murks wird, wenn der Gesetzgeber eilig handelt. Daher sehe ich es nicht unbedingt als Nachteil, wenn die Gesetzgebung hinterherhinkt.

Wir haben bereits eine ganze Reihe an Regularien: Wir haben eine KI-Verordnung, die in Europa gültig ist, wir haben die Datenschutzgrund-verordnung und wir haben nationale Gesetze. Wir haben nur leider sehr viele Rechtsbrüche. Viele dieser Normen sind im alltäglichen Gebrauch plötzlich gar nicht mehr so wichtig. Daher geht es nicht darum, dass der Gesetzgeber in Europa oder auch in Berlin mehr Gesetze macht, solange das geltende Recht nicht endlich durchgesetzt wird.

Anders als beim Datenschutz gibt es bei der IT-Sicherheit aus meiner Sicht noch Lücken, die der Gesetzgeber schließen sollte – zum Beispiel bei der Haftung oder auch bei der Frage, welche Sicherheitsmaßnahmen in Unternehmen vorgeschrieben sind. Da hängt die Gesetzgebung noch sehr hinterher. Das sieht man auch an der allgemeinen Nachrichtenlage. Sie können eine beliebige Webseite oder Zeitung aufklappen – und finden direkt Berichte von Sicherheitsvorfällen.

Die passieren in der Regel nicht einfach so. In der Regel gibt es Verantwortliche, die bei der IT-Sicherheit geschlampt haben. Das ist leider ein Zustand, den wir wahrscheinlich noch ein paar Jahre beibehalten werden. Das ist sehr bedauerlich und schlecht.

Das heißt, die Unternehmen müssen viel stärker in die Eigenverantwortung gehen, weil die staatliche Kontrolle oder die Einhaltung der Vorschriften einfach auch Grenzen hat?
Dr. Constanze Kurz: Das ist auf jeden Fall sehr wichtig. Insofern sehe ich die aktuelle Lage auch ein bisschen positiv, weil sie zur Sensibilisierung beiträgt. Gerade diese große Menge an Vorfällen in Zusammenhang mit KI und IT-

Karlsruher Messe- und Kongress GmbH
Festplatz 9
76137 Karlsruhe
tel +49 721 3720-0
fax +49 721 3720-99-2116
info@messe-karlsruhe.de
messe-karlsruhe.de

Messe Karlsruhe
Messeallee 1
76287 Rheinstetten

Kongresszentrum
Festplatz 9
76137 Karlsruhe

Geschäftsführerin
Britta Wirtz

Vorsitzende des Aufsichtsrats
Bürgermeisterin
Gabriele Luczak-Schwarz

Reg.-Ger. Mannheim
HRB 100147

Mitglied
AUMA | FKM | GCB
IDFA | EVVC | ICCA

learntec.de

Sicherheit führt nämlich dazu, dass sich die Menschen in den Unternehmen zusammensetzen und sagen: Was müssen wir eigentlich ändern, damit wir nicht die Nächsten sind?

Natürlich ist die IT-Sicherheit zunächst einmal die Verantwortung derjenigen, die die Software betreiben. Aber auch derjenigen, die die Software herstellen, stehen in der Pflicht. Bei den KI-Anbietern machen sich manche natürlich schon seit Langem einen schlanken Fuß, indem sie behaupten: Unsere KI handelt quasi selbstständig. Das ist aus technischer Sicht Nonsens. Das sollten wir ihnen dauerhaft nicht durchgehen lassen – wie übrigens allen Anbietern.

Wo ein Sicherheitsbruch passiert, ist vielleicht ein Mitarbeiter involviert, der gar nicht die Befähigung hatte. Umfragen sprechen von bis zu 70 Prozent der Mitarbeitenden, die noch gar kein Schulungsangebote zu KI erhalten haben. Gleichzeitig nutzen viele fleißig KI im Privatgebrauch. Was müssen Unternehmen tun, um diese Lücke zu schließen?
Dr. Constanze Kurz: Ein wichtiger Aspekt ist zunächst natürlich die Sensibilisierung. Mein Eindruck ist aber, dass KI, im Unterschied zu anderer Software, sich insbesondere dort verbreitet, wo sehr wenig technisches Vorwissen vorhanden ist. Denn man muss keine technischen Voraussetzungen haben, um KI zu nutzen. Die KI zieht direkt in den Alltag ein, und man muss sich klarmachen, dass über solche Anwendungen Daten abfließen können.

Der zweite Schritt ist, dass Unternehmen und Mitarbeitende überhaupt wahrnehmen, dass sich Sicherheitsmaßnahmen in einer Firma durch die KI-Nutzung unterminieren lassen. Mitarbeitende können die Konzepte, die ein Unternehmen erstellt hat, um eine ordentliche IT-Sicherheit zu gewährleisten, sozusagen von hinten umgehen. Das ist zwar nicht unbedingt ein Alleinstellungsmerkmal der KI – aber ich habe oft den Eindruck, dass durch die Vermenschlichung der KI eine gewisse Vertrauensseligkeit entstanden ist. Das liegt auch an diesem merkwürdig devoten Tonfall, den Chatbots anschlagen. Man hat den Eindruck, man sitzt vor einer sehr fähigen Software, der man vertrauen kann. Wenn man sich aber mit der Technik beschäftigt, ist eigentlich das Gegenteil der Fall. Sie ist fehlerbehaftet, und sie ist ein Sicherheitsrisiko.

Hinzu kommt, dass die KI-Welle für Unternehmen oft nicht ganz freiwillig ist, weil KI-Anwendungen in viele Betriebssysteme und Smartphones integriert werden, ohne dass die Nutzer das wollen. Manchen ist gar nicht klar, was da eigentlich in ihre Betriebssysteme oder Smartphones einzieht und wo Gefahren entstehen. Und sie konnten es sich gar nicht erst aussuchen:

Karlsruher Messe- und Kongress GmbH
Festplatz 9
76137 Karlsruhe
tel +49 721 3720-0
fax +49 721 3720-99-2116
info@messe-karlsruhe.de
messe-karlsruhe.de

Messe Karlsruhe
Messeallee 1
76287 Rheinstetten

Kongresszentrum
Festplatz 9
76137 Karlsruhe

Geschäftsführerin
Britta Wirtz

Vorsitzende des Aufsichtsrats
Bürgermeisterin
Gabriele Luczak-Schwarz

Reg.-Ger. Mannheim
HRB 100147

Mitglied
AUMA | FKM | GCB
IDFA | EVVC | ICCA

learntec.de

Plötzlich ist diese Anwendung im Betriebssystem, im Messenger oder in der Software vorhanden.

Insofern gibt es hier auch eine Verantwortung der Anbieter, die diese Technik pushen – und das stärker als Techniken, die wir in der Vergangenheit gesehen haben.

Unternehmen müssen sehr klare Regeln aufstellen und festlegen: Was ist inakzeptabel? Wie können Mitarbeitende KI benutzen und unter welchen Bedingungen?

Dann sollte man sich für die Zukunft überlegen, wie man eigene Angebote schaffen kann – also selbst betriebene Anwendungen, bei denen keine Daten nach außen dringen und die man wirklich kontrollieren kann.

Ist es für kleine und mittlere Unternehmen überhaupt machbar, sich souverän aufzustellen mit einer betriebseigenen KI? Gibt es eine Zwischenlösung? Denn keine KI scheint heutzutage keine Lösung mehr zu sein.
Dr. Constanze Kurz: Oftmals ist KI nur *eine* Form, mit der man Prozesse automatisieren kann – und genau das ist das Ziel. Dafür ist KI technologisch gesehen nicht die einzige Lösung. Sie ist jetzt nur gerade der neueste Schrei. Das wird sich auch wieder legen.

Wenn Sie auf die großen Frontier-AI-Modelle setzen, setzen Sie nicht unbedingt auf das beste Pferd. Es gibt mittlerweile eine ganze Reihe an Alternativen. Diese Modelle sind in der Regel etwas kleiner, aber auch konkret geschaffen für den jeweiligen Anwendungszweck. Insofern entwickelt sich schon seit einer ganzen Weile ein Markt mit kleineren Modellen und spezifischeren Anwendungen.

Schon aus Kostengründen lohnt es sich nicht, dem allerneuesten großen Sprachmodell hinterherzulaufen. Wenn man auf ein bestimmtes Modell setzt und sich davon abhängig macht, ist die Preisschraube, die folgt, natürlich unangenehm. Ein etwas kleineres Modell anzuwenden, ist nicht unbedingt die schlechtere Alternative, denn der technologische Abstand ist nämlich gar nicht so groß.

Wenn sich ein Unternehmen ganz neu in diesem Bereich aufstellen will, also noch ein völlig unbeschriebenes Blatt ist, was würden Sie diesem Unternehmen mitgeben?
Dr. Constanze Kurz: Das Erste, was ich jedem empfehlen würde, ist, sich nicht von dieser FOMO – Fear of Missing Out – ergreifen zu lassen, sondern mit Verstand und Skepsis zu prüfen: Was brauche ich wirklich? Was will ich

Karlsruher Messe- und Kongress GmbH
Festplatz 9
76137 Karlsruhe
tel +49 721 3720-0
fax +49 721 3720-99-2116
info@messe-karlsruhe.de
messe-karlsruhe.de

Messe Karlsruhe
Messeallee 1
76287 Rheinstetten

Kongresszentrum
Festplatz 9
76137 Karlsruhe

Geschäftsführerin
Britta Wirtz

Vorsitzende des Aufsichtsrats
Bürgermeisterin
Gabriele Luczak-Schwarz

Reg.-Ger. Mannheim
HRB 100147

Mitglied
AUMA | FKM | GCB
IDFA | EVVC | ICCA

learntec.de

sinnvoll automatisieren und womit? Wo liegen meine Effizienz- und Optimierungspotenziale und womit kann ich diese erschließen? Diese Fragen vorab zu klären, ist manchmal schwer, weil gerade alle der KI hinterherlaufen.

Wenn man ein ordentliches Konzept hat, kann man gar nicht viel falsch machen. KI kann ein Teil davon sein, aber es kann auch sein, dass man andere Automatisierungslösungen oder eine andere Software findet.

Das Zweite ist: Wenn man sich für solche Anwendungen entscheidet, gerade von großen Anbietern, muss man dringend eine IT-Sicherheitsanalyse durchführen. Man muss sich fragen: Werden meine IT-Sicherheitskonzepte unterlaufen? Kann ich die rechtlich bestehenden Datenschutzanforderungen gegenüber meinen Mitarbeitenden oder auch Bewerbern erfüllen? Das ist nicht neu – denn das muss man auch bei anderer Software machen.

Das Letzte, was ich noch empfehlen würde, ist: offen zu sein. Die Technik ist spannend und neu. Man kann sie ausprobieren, sollte aber mit Vorsicht vorgehen. Denn KI führt eben auch dazu, dass es mehr Angriffe geben wird. Auch Kriminelle setzen KI ein – und zwar massiv.

Wenn man vor der Einführung ein paar Wochen oder Monate nachdenkt, wird man nicht sofort vom KI-Tsunami mitgerissen, sondern kann vielleicht eine praktikablere und aus Compliance-, Datenschutz- und IT-Sicherheitssicht bessere Lösung finden.

Wie bei allen Softwareprodukten gilt: Den Verstand nicht ausschalten, sondern wirklich skeptisch und wohlinformiert auf die Technik schauen.

Wenn wir auf die rasanten Entwicklungen der letzten Jahre zurückblicken: Welche Prognose würden Sie wagen? Wo stehen wir in fünf Jahren?
Dr. Constanze Kurz: Klar ist, dass der gesamte Trend zur Automatisierung weitergehen wird, denn er ist absolut notwendig. Man will repetitive Aufgaben oder solche Aufgaben, die eine Maschine besser und schneller erledigen kann, abgeben.

Der Hype um diese Frontier AI – wir reden von den großen Start-ups – wird aus meiner Sicht nicht bestehen bleiben. Das liegt schlicht daran, dass die Technik fehlerbehaftet und auch zu teuer ist. Diesen speziellen Hype werden wir wieder untergehen sehen.

Bleiben wird natürlich der Bedarf, die Technik, die einen umgibt, möglichst effizient und menschenfreundlich einzusetzen. Dieser Trend hat schon begonnen, bevor die große KI-Welle losging. Aber er wird ein Teil davon sein.

Karlsruher Messe- und Kongress GmbH
Festplatz 9
76137 Karlsruhe
tel +49 721 3720-0
fax +49 721 3720-99-2116
info@messe-karlsruhe.de
messe-karlsruhe.de

Messe Karlsruhe
Messeallee 1
76287 Rheinstetten

Kongresszentrum
Festplatz 9
76137 Karlsruhe

Geschäftsführerin
Britta Wirtz

Vorsitzende des Aufsichtsrats
Bürgermeisterin
Gabriele Luczak-Schwarz

Reg.-Ger. Mannheim
HRB 100147

Mitglied
AUMA | FKM | GCB
IDFA | EVVC | ICCA

learntec.de

LEARNTEC

2. – 4. Februar 2027
Messe Karlsruhe

Wenn ich in die Zukunft schaue, werden sich aus meiner Sicht Modelle durchsetzen, die man selbst beherrschen kann. Schon jetzt bauen einige große Softwareunternehmen eigene Modelle.

Vielen Dank für das Gespräch!

Über die LEARNTEC

Die LEARNTEC ist Europas größte Veranstaltung für digitale Bildung. Jährlich kommen Entscheiderinnen und Entscheider aus Industrie, Beratung, Handel und Vertrieb sowie aus Schulen und Hochschulen nach Karlsruhe, um sich über innovative Formen des digitalen Lernens zu informieren und auszutauschen. Der dreitägige Kongress vermittelt praxisnahes Wissen und setzt auf Interaktion: Open-Space-Sessions und Diskussionsrunden fördern den direkten Austausch zwischen Referierenden und Teilnehmenden.

Die LEARNTEC findet 2027 wieder zu einem frühen Termin im Jahresverlauf statt – vom 2. bis 4. Februar 2027.

Weitere Informationen gibt es online unter www.learntec.de

Karlsruher Messe- und Kongress GmbH
Festplatz 9
76137 Karlsruhe
tel +49 721 3720-0
fax +49 721 3720-99-2116
info@messe-karlsruhe.de
messe-karlsruhe.de

Messe Karlsruhe
Messeallee 1
76287 Rheinstetten

Kongresszentrum
Festplatz 9
76137 Karlsruhe

Geschäftsführerin
Britta Wirtz

Vorsitzende des Aufsichtsrats
Bürgermeisterin
Gabriele Luczak-Schwarz

Reg.-Ger. Mannheim
HRB 100147

Mitglied
AUMA | FKM | GCB
IDFA | EVVC | ICCA

learntec.de

messe karlsruhe