ZUKUNFTS
ZENTRUM
NORD

Zukunfts-
Zentren

Quartal Insights

2. Quartal / 2026

Cybersicherheit in Zeiten von KI

KI-Agenten: Hype vs. Realität

Im Rückblick:

KI.Compliance.Sicherheit

Neu in dieser Ausgabe:

Zahlen, Daten, Trends

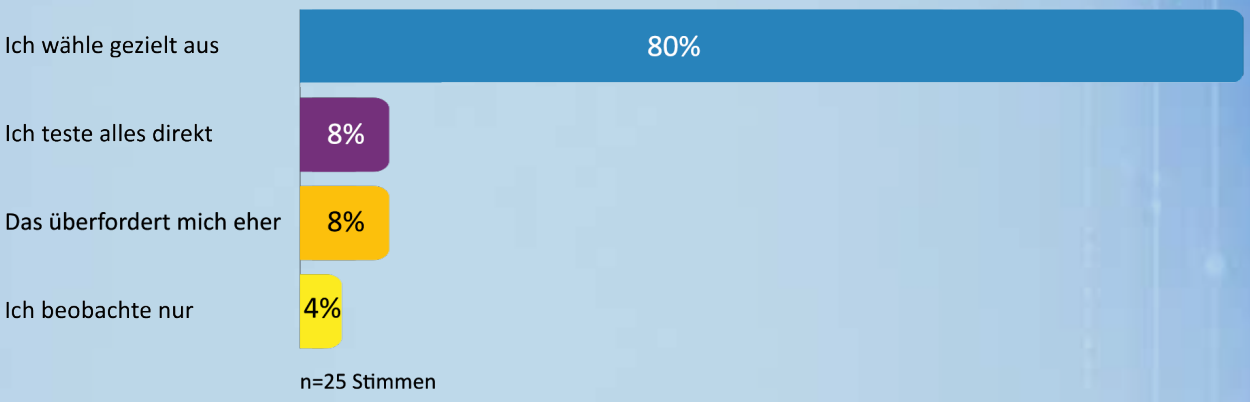
Was Unternehmen bewegt. Was Studien zeigen. Was morgen wichtig wird.

Inhalte

Sie haben Anmerkungen, Anregungen oder Fragen zum Magazin?
Schreiben Sie uns gerne an:
beratung@zukunftszentrumnord.de

Zahlen, Daten, Trends

Auf LinkedIn haben wir neulich eine kurze Umfrage gestartet, um zu verstehen, wie mit der rasanten Entwicklung neuer KI-Tools umgegangen wird. Die Ergebnisse sind in der folgenden Grafik dargestellt.



Die Antworten zeigen ein klares Bild: **Die Mehrheit setzt auf eine gezielte Auswahl** statt auf das Testen jedes neuen KI-Tools. Das macht deutlich, dass das Thema „KI-Strategie“ zunehmend in den Fokus rückt.

Künstliche Intelligenz in Deutschland

Ein aktueller Studienbericht von Bitkom „Künstliche Intelligenz in Deutschland“ (Februar 2026) zeigt: Künstliche Intelligenz (KI) wird als wichtigste Zukunftstechnologie eingestuft. **KI ist längst keine Zukunftsvision mehr**, sondern Realität in Wirtschaft, Verwaltung und Alltag.

Zunehmender Einsatz von KI in deutschen Unternehmen:

36 Prozent der Unternehmen setzen bereits KI ein. Das sind mehr als jedes dritte Unternehmen. Im Vergleich zum Vorjahr 2024 (20 Prozent) entspricht dies einer Verdopplung der KI-Nutzung binnen eines Jahres.

Der Weiterbildungsbedarf ist groß:

43 Prozent der Unternehmen bieten bislang keine Schulungen zu KI an. Das heißt, in knapp jedem zweiten Unternehmen fehlen somit die gezielte Qualifizierung der Mitarbeitenden im Umgang mit KI.

Der EU AI Act wird als erheblicher Aufwandstreiber wahrgenommen:

93 Prozent der vom EU AI Act betroffenen Unternehmen sehen mit seiner Umsetzung einen eher oder sogar sehr hohen Aufwand verbunden. 56 Prozent der befragten Unternehmen stimmen zudem der Aussage zu, dass der EU AI Act mehr Nachteile als Vorteile für deutsche Unternehmen schaffe.

Quelle: https://www.bitkom.org/sites/main/files/2026-02/bitkom-studienbericht-ki.pdf

Projekt-Spotlight

Veranstaltungsrückblick „KI.Compliance. Sicherheit – Orientierung und Umsetzung für KMU in Bremen und Bremerhaven“

Cybersicherheit, verantwortungsvolle KI-Nutzung und regulatorische Entwicklungen standen am in Bremen am 24. April 2026 im Mittelpunkt der Veranstaltung „KI.Compliance.Sicherheit – Orientierung und Umsetzung für kleine und mittlere Unternehmen“. Das vom Regionalen Zukunftszentrum Nord in Kooperation mit den senatorischen Behörden für Arbeit und Wirtschaft der Freien Hansestadt Bremen organisierte Event zog **über 120 Teilnehmende** an und brachte Expert:innen, Vertreter:innen aus Wirtschaft und Politik sowie KMU zusammen, um aktuelle Herausforderungen und praxisnahe Lösungen im Umgang mit Künstlicher Intelligenz zu diskutieren.

Aktuelle Entwicklungen und regionale Perspektiven

Auftakt der Veranstaltung war die Keynote von Jens Mühlner (Vorstandsvorsitzender, Charta digitale Vernetzung e.V. und Head of Digital Sustainability Solutions, T-Systems International), der die vielschichtigen Aspekte des KI-Einsatzes als Treiber von Innovation und zugleich als Risikofaktor aufzeigte.

Wie gelingt der sichere Einsatz von KI in KMU?

Wie diese Risiken heute aussehen, machte der Praxis-Impuls von Patrick Jung (ISB Plus) deutlich. Anhand aktueller Beispiele aus der Realität von Cyberangriffen zeigte er, mit welchen Herausforderungen insbesondere KMU konfrontiert sind und welche Maßnahmen zum Schutz vor Angriffen beitragen können. Mehr dazu lesen Sie auf den Seite 6-9 im Interview mit Patrick Jung.

In der anschließenden Paneldiskussion wurde aus unterschiedlichen Perspektiven diskutiert, wo Bremen und Bremerhaven derzeit in den Bereichen Regulierung und Compliance stehen und welche Bedeutung dies für kleine und mittlere Unternehmen hat.

Austausch und Vernetzung im Fokus

Ergänzt wurde das Programm durch konkrete Beispiele aus der Unternehmenspraxis, die verdeutlichten, wie KI und Cybersicherheit bereits heute erfolgreich eingesetzt werden.

In drei parallelen Workshops hatten die Teilnehmenden zudem die Möglichkeit, sich interaktiv mit Themen wie verantwortungsvollem KI-Einsatz, Skill-Gaps und konkreten KI-Anwendungsfällen auseinanderzusetzen.

Neben den inhaltlichen Impulsen boten insbesondere der Markt der Möglichkeiten sowie die Round Tables zu den Themen Handel und Handwerk viel Raum für Austausch, Vernetzung und vertiefende Gespräche.

Die Veranstaltung wurde gemeinsam durchgeführt vom Regionalen Zukunftszentrum Nord, der Senatorin für Arbeit, Soziales, Jugend und Integration sowie der Senatorin für Wirtschaft, Häfen und Transformation der Freien Hansestadt Bremen.

Mit freundlicher Unterstützung von:

BAB – Die Förderbank für Bremen und Bremerhaven, BIS Bremerhavener Gesellschaft für Investitionsförderung und Stadtentwicklung, Gemeinsamer Arbeitgeber-Service mit der Agentur für Arbeit Bremen-Bremerhaven und dem Jobcenter Bremen, Handelskammer Bremen – IHK für Bremen und Bremerhaven, Handwerkskammer Bremen, Initiative Neue Qualität der Arbeit (INQA), Landesagentur für berufliche Weiterbildung und Transformation – LABEW+, Mittelstand-Digital Zentrum Bremen-Oldenburg, WFB Wirtschaftsförderung Bremen/Digitallotsen, Wirtschafts- und Strukturrat Bremen-Nord (WIR)

Das Event zog über 120 Teilnehmende an

Future Sneak Peek

Cybersicherheit für KMU

Wir haben mit Patrick Jung, dem Gründer und Inhaber von ISB Plus gesprochen, einem echten Experten für IT-Sicherheit. Im Gespräch gibt er spannende Einblicke in moderne Cyberangriffe, typische Schwachstellen von KMU und wirksame Schutzmaßnahmen für Unternehmen.

Patrick Jung

Sie beschreiben, dass Cyberangriffe früher Wochen dauerten – heute nur noch Minuten. Was hat sich technisch verändert, dass das möglich ist?

Die Angreifer unterliegen beim Einsatz von Automatisierungen oder „unfertigen“ KI-Modellen keinerlei Einschränkungen. Damit lassen sich Aufgaben, die früher manuell erledigt werden mussten, beispielsweise das Prüfen gestohlener Zugangsdaten, schnell umsetzen. Das heißt, hier wird geprüft, ob die Zugangsdaten überhaupt noch funktionieren und ob sie eventuell auch für andere Plattformen funktionieren, weil jemand das gleiche Kennwort bei der Arbeit und in einem Online-Shop benutzt.

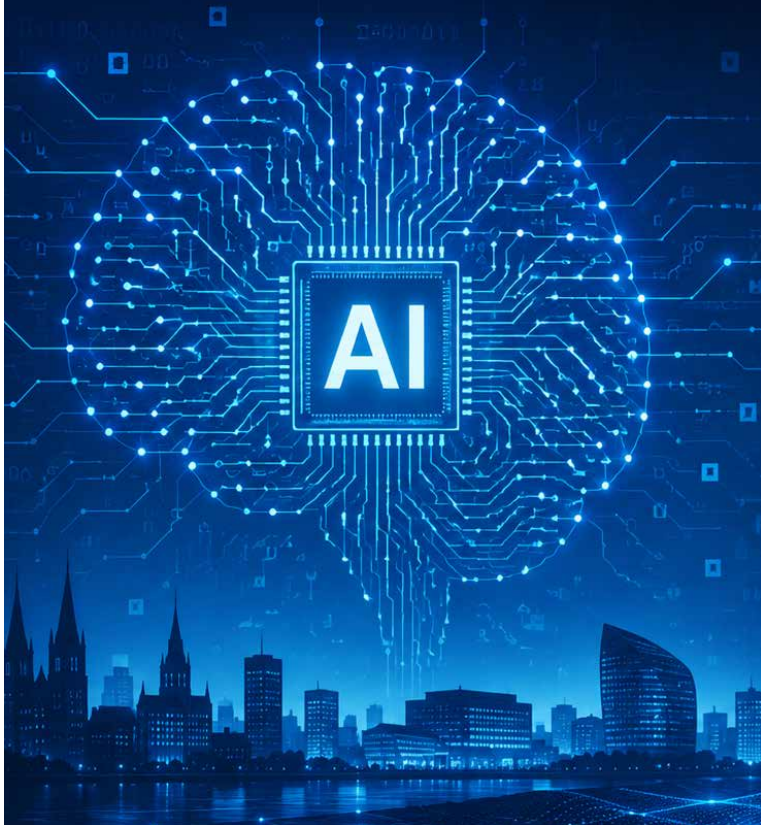
Was sich vor allem geändert hat, ist die Ausnutzung bekannter Schwachstellen. Das muss man sich so vorstellen:

Man hat ein Haus, das mit einer Alarmanlage gesichert ist. Nun kommt heraus, dass man über ein Bauteil die Alarmanlage abschalten kann. Dieses Bauteil muss aber umprogrammiert werden. Früher musste sich jemand hinsetzen und dieses Programm schreiben und immer wieder prüfen, ob die Alarmanlage nun wirklich abgeschaltet werden kann. Das dauerte Wochen. Das kann man heute mit KI-Modellen machen. Eine Schwachstelle in einer Software wird bekannt und man kann per KI, die den Programmcode schnell versteht, einen sogenannten Exploit, also das Werkzeug der Einbrecher, bauen lassen. Die Statistik von zerodayclock.com sagt aus, dass der Zeitraum von Bekanntwerden und Ausnutzung der Schwachstelle im Jahr 2025 im Durchschnitt noch bei 21,5 Tagen lag und im Jahr 2026 nur noch bei 1,9 Tagen. Das bedeutet, dass ein Teil der Angriffe schon direkt am Tag des Bekanntwerdens stattfindet.

Cyberangriffe werden immer schneller

Welche Art von Angriffen sehen Sie aktuell am häufigsten bei kleinen und mittleren Unternehmen?

Häufig handelt es sich um eine Mischung aus Identitätsdiebstahl und Betrugsfällen mit IT-Unterstützung. Die geänderte Bankverbindung ist ein klassisches Mittel, das leider immer noch sehr häufig zum Erfolg führt. Die Betrüger schaffen es nämlich auch, sich unter einer sehr ähnlich klingenden Firmenbezeichnung ein Bankkonto zu registrieren. Man sieht aber auch, dass Phishing-E-Mails sehr gezielt auf bestimmte Personen mit viel Hintergrundwissen eingesetzt werden. Hierzu werden E-Mail-Konten mit gestohlenen Passwörtern ausgenutzt, vorangegangene Konversationen kopiert bzw. fortgeführt und dann unter einer ähnlich klingenden Absenderadresse weitergeführt. Das Opfer sieht dann die bekannte Konversation im E-Mail-Verlauf und stellt die Anweisung, dass sich an der Bankverbindung etwas geändert hat, nicht in Frage bzw. überprüft sie nicht, etwa durch eine telefonische Nachfrage, besonders dann nicht, wenn die E-Mail intern an den Vorgesetzten weitergeleitet wird. Ein weiteres beliebtes Ziel ist der Diebstahl von Zugangsdaten. Hier wird ebenfalls ein gehacktes E-Mail-Postfach benutzt und bekannte Kontakte werden angeschrieben. Diese erhalten einen Link oder ein verschlüsseltes Dokument und sollen ihre Zugangsdaten eingeben. Wenn der Empfänger dies tut, wird in seinem Namen die gleiche E-Mail an die eigenen Kontakte gesendet – also ein moderner Kettenbrief, dessen Ziel es ist, Passwörter zu stehlen.



Die gefährlichsten Angriffe wirken oft völlig vertraut

Warum sind kleine und mittlere Unternehmen für Angreifer heute besonders attraktiv und wo liegen die typischen Einfallstore?

Häufig haben KMUs keine Mitarbeiter, die sich um das Thema IT-Sicherheit kümmern. Wenn der IT-Dienstleister diese Themen anspricht, haben die Unternehmen oft das Gefühl, dass er ihnen etwas verkaufen will und erkennen den Nutzen nicht. Daher ist das Schutzniveau an einigen Stellen niedriger. Man muss sich IT-Sicherheit wie einen Deich vorstellen: Er sollte überall gleich hoch sein. Wenn er an einer Stelle statt 5 m nur 3 m hoch ist, dann schwappt der Cyberangriff genau da hinein. Neben den Kosten befürchten viele auch, dass es komplizierter wird und die Arbeitszeit darunter leidet. Einige Unternehmen haben auch das Problem, dass sie eventuell IT-Dienstleister haben, die das Thema IT-Sicherheit ebenfalls nicht im Fokus haben, weil sie sich nur um die Systeme kümmern und dafür sorgen, dass alles „up and running“ ist. Dann bekommt das Unternehmen gar keine Informationen darüber, welche Maßnahmen warum umgesetzt werden müssen.

IT-Sicherheit lässt sich gut mit einem Deich vergleichen

Was sind die drei Maßnahmen, die ein KMU mit begrenztem Budget sofort umsetzen kann, um sich besser zu schützen?

Überall, wo es möglich ist, sollte ein zweiter Faktor (MFA) zusätzlich zum Passwort genutzt bzw. erzwungen werden. Zudem sollten Administratorkonten reduziert und immer als getrennte Konten genutzt werden, sodass kein Mitarbeiter unter seinem persönlichen Konto mit Mailaccount administrative Rechte besitzt. Alle Systeme sollten mit automatischen Updates konfiguriert werden, damit Lücken geschlossen werden, sobald ein Patch verfügbar ist. Dies gilt insbesondere für Arbeitsplatzrechner und Systeme, die aus dem Internet erreichbar sind. Bei Systemen, die für die Produktion genutzt werden, muss natürlich vorsichtig damit umgegangen werden. Aber auch bei solchen Systemen muss zukünftig schneller aktualisiert werden. Mein Tipp für virtuelle Systeme: Tägliche Snapshot-Sicherung durchführen und automatische Updates aktivieren. Wenn etwas schiefgeht, kann man auf die Version von gestern springen. Ein Ausfall von einigen Stunden für die Wiederherstellung nach einem fehlerhaften Update ist aus meiner Sicht besser als ein kompletter Stillstand wegen eines Cyberangriffs. Als Bonus-Tipp: Haben Sie einen Plan für den Totalausfall Ihrer IT? Stellen Sie sich die Frage: „Wie kann ich mindestens 60 % meiner Unternehmensprozesse auch ohne die kompletten IT-Systeme am Laufen halten?"

Ist das klassische Passwort eigentlich ein Auslaufmodell? Wohin geht die Entwicklung, Stichwort „Passkeys oder biometrische Authentifizierung"?

Das Passwort ist ein Auslaufmodell. Das zeigt die aktuelle Auswertung des Hasso-Plattner-Instituts.[1] Der durchschnittliche Anwender nutzt aus Bequemlichkeit oder Missverständnis heraus keine sicheren Passwörter und wird das wohl auch nie tun. Passkeys bieten da eine echte Chance, da unser Smartphone das Passwort ist. Wir haben es immer dabei und die darauf gespeicherten Passkeys sind verschlüsselt abgelegt. Hier ist aber wieder der Knackpunkt: Wie habe ich mein Smartphone abgesichert? Nutze ich einen 4-stelligen PIN-Code wie „1234", dann sind auch die Passkeys nicht sicher, denn mit diesem PIN-Code gebe ich den Zugriff auf meine Passkeys frei. Daher muss man das Smartphone mit einem langen Passwort schützen oder mit biometrischen Maßnahmen, was für viele Anwender das Einfachste ist und auch deutlich sicherer als jede schlechte PIN. Ich denke, dass es in Unternehmen auch einen Wandel zu Hardware-Tokens geben wird, die in den Rechner gesteckt und anschließend einen PIN eingeben werden muss. So habe ich automatisch eine Zwei-Faktor-Authentifizierung, die auch phishingresistent ist, da der Angreifer für das Login auch meinen Hardware-Token bräuchte.

Wie hat sich das Bild eines typischen Cyberangriffs in den letzten 5 Jahren verändert?

Heute kann man sich komplette Werkzeuge für einen Cyberangriff kaufen, sogenannte Ransomware-as-a-Service-Angebote. Das heißt, ich muss kein Programmierer oder IT-Nerd sein, um dem Geschäftsmodell „Erpressung“ nachzugehen. Daher gibt es viele neue Gruppen, die sich in diesem Markt tummeln und schnell „erfolgreich“ sind. Dieser für jeden bezahlbare Werkzeugkoffer, gepaart mit KI-Modellen, die darauf trainiert sind, Viren oder Phishing-Mails zu entwickeln, beschleunigt die Angriffe enorm. Die aktuelle Statistik des BKA[2] zeigt beispielsweise, dass eine Gruppe, die es 2024 noch gar nicht gab, 2025 die zweithäufigste Angriffsvariante ist. Was dazukommt, ist die Variabilität von Schadsoftware (Software, die den Rechner manipuliert). Es wurden schon erste Varianten gefunden, die sich anhand ihrer Zielumgebung, also dem System, auf dem sie sich befinden, umprogrammiert haben. Das heißt, ein schädliches Programm auf meinem Rechner spioniert meine Schutzmaßnahmen aus und erhält per KI-Modell Informationen darüber, wie es sich umprogrammieren muss, damit es nicht erkannt wird. Diese Funde von Google Threat Intelligence[3] befinden sich zwar noch in der Entwicklung, werden aber in kurzer Zeit zur neuen Realität werden. Mit solchen „Evil-KI“-Modellen kann man sehr viel Geld verdienen, wenn sie funktionieren. Wo ein Markt ist, werden sich die Anbieter etablieren.

Wo ein Markt ist, werden sich die Anbieter etablieren

Quellen:

[1] HPI (2026): HPI veröffentlicht meist geleakte Passwörter 2025. Verfügbar unter: https://hpi.de/artikel/hpi-veroeffentlcht-meist-geleakte-passwoerter-2025/ (Stand: 26.05.2026)

[2] Bundeskriminalamt (BKA) (2026): Cybercrime Bundeslagebild 2025. Verfügbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2025.html (Stand: 26.05.2026)

[3] Google Threat Intelligence Group (2025): GTIG AI Threat Tracker: Advances in Threat Actor Usage of AI Tools. In: Google Cloud Blog. Verfügbar unter: https://cloud.google.com/blog/topics/threat-intelligence/threat-actor-usage-of-ai-tools (Stand: 26.05.2026)

Checkbox - 5 Tipps für ein sicheres Passwort

- Passkeys sollten eingesetzt werden, wo es möglich ist.
- 15+ Länge schlägt Komplexität, d. h. 15+ Zeichen sind besser als 8 Zeichen mit allen möglichen Sonderzeichen.
- Multi-Faktor-Authentifizierung einsetzen.
- 1x Jedes Passwort nur einmal verwenden.
- Passwörter nur anlassbezogen ändern, beispielsweise nach einer Phishing-Attacke, keine monatlichen Rotationen.

KI-Agenten: Zwischen Hype und Umsetzung

KI-Agenten, KI-Assistenten oder agentische Workflows?

Mit der zunehmenden Verbreitung von Künstlicher Intelligenz tauchen immer häufiger Begriffe wie KI-Agent, KI-Assistent oder agentischer Workflow auf. Oft werden diese Konzepte synonym verwendet, obwohl sie unterschiedliche Aufgaben erfüllen und für verschiedene Einsatzszenarien geeignet sind. Für den erfolgreichen Einsatz von KI ist daher nicht entscheidend, dem neuesten Trend zu folgen, sondern das passende Modell für den jeweiligen Anwendungsfall zu finden.

Das passende Modell schlägt jeden Trend

KI-Assistenten unterstützen Nutzende bei klar formulierten Aufgaben. Ausgangspunkt ist immer eine Frage oder Anweisung, auf die das System reagiert. Typische Beispiele sind das Formulieren einer E-Mail, das Zusammenfassen von Dokumenten oder das Erstellen von Textentwürfen. KI-Assistenten arbeiten dialogorientiert, flexibel und kreativ. Die Kontrolle bleibt dabei weitgehend beim Menschen.

KI-Agenten gehen einen Schritt weiter. Sie erhalten nicht nur eine Frage, sondern eine Aufgabenstellung oder ein Ziel. Anschließend planen sie eigenständig die notwendigen Arbeitsschritte, nutzen verschiedene Werkzeuge und bewerten Zwischenergebnisse. So können sie beispielsweise Daten analysieren und daraus selbstständig einen Bericht erstellen. KI-Agenten arbeiten proaktiv, mehrstufig und mit einem hohen Grad an Autonomie.

Zwischen diesen beiden Ansätzen liegen **agentische Workflows**. Hier sind die einzelnen Prozessschritte klar definiert und werden automatisiert ausgeführt. Ein Beispiel ist die Verarbeitung eingehender E-Mails: Anhänge werden automatisch ausgelesen, Informationen extrahiert und an die richtigen Systeme weitergeleitet. Solche Workflows sind besonders transparent und gut nachvollziehbar, bieten jedoch weniger Flexibilität.

Nicht der neueste Trend entscheidet, sondern das passende Modell für die jeweilige Aufgabe.

Diese 3 Modelle sollten nicht miteinander konkurrieren. Viel mehr entscheidend ist, wie die Anforderungen an eine Aufgabe sind. Für standardisierte Prozesse eignen sich agentische Workflows, für die Unterstützung einzelner Arbeitsschritte KI-Assistenten und für komplexe, mehrstufige Aufgaben KI-Agenten. Der aktuelle Fokus auf KI-Agenten ist daher nachvollziehbar, dennoch bleibt der wichtigste Erfolgsfaktor die Wahl des passenden Konzepts.

Wer die Berichterstattung der vergangenen Monate verfolgt hat, stößt immer wieder auf ähnliche Schlagzeilen: „2025 wird das Jahr der KI-Agenten“, „2026 wird das Jahr der KI-Agenten“ oder „Die neue KI-Revolution“. Kaum ein KI-Trend erhält derzeit so viel Aufmerksamkeit wie das Thema KI-Agenten. In der Realität sieht es aber schnell ernüchternd aus: in Unternehmen ist die Anwendung von KI-Agenten noch nicht weit verbreitet. Nur wenige Unternehmen haben bereits KI-Agenten im Einsatz. Vorwiegend große Unternehmen nutzen KI-Agenten und machen bei der Einführung die ersten Schritte. In Bezug auf ihrer Funktionsweise erfüllen viele KI-Agenten noch nicht die Erwartungen der Unternehmen. Von KI-Agenten erhofft man sich vor allem eine deutliche Produktivitätssteigerung und eine spürbare Entlastung der Mitarbeitenden durch die autonome Bearbeitung von Aufgaben. Doch bei den meisten KI-Agenten ist bereits nach wenigen Arbeitsschritten menschliches Eingreifen nötig.

Fazit: Das Thema KI-Agenten erlebt momentan zwar einen Hype, die Umsetzung ist allerdings erst am Anfang. Die meisten Unternehmen die schon KI-Agenten nutzen, setzen diese derzeit eher in Pilotprojekten um. Es ist aber davon auszugehen, dass der produktive Einsatz von KI-Agenten in den nächsten Jahren eine wichtige Rolle spielen wird.

KI-Agenten: Viel Potenzial, wenig Praxis

Good Practice

Chocoversum
Von der Prozessanalyse bis zur erfolgreichen Umsetzung von KI-Use-Cases.

Jetzt entdecken

Stop Apotheke
IT-Sicherheit stärken, Prozesse optimieren und Mitarbeitende aktiv mitnehmen.

Jetzt entdecken

RWS Vermögens-planung AG
Chatbot oder Website-Optimierung? Was bringt wirklich Mehrwert?

Jetzt entdecken

Diese Aufnahme wurde freundlicherweise von Chocoversum GmbH zur Verfügung gestellt.

Inspirierende Erfolgsgeschichten

Unsere Referenzprojekte repräsentieren erfolgreiche Digitalisierungsinitiativen, die wir umgesetzt haben. Von den ersten Schritten Richtung KI, der Optimierung von Prozessen oder den Einsatz von Generativer KI bis hin zu Beschäftigtenqualifizierung haben wir Unternehmen verschiedener Größen und Branchen unterstützt.

Jetzt entdecken

Sie haben Fragen?

beratung@zukunftszentrumnord.de

Auf unserer Website zukunftszentrumnord.de finden Sie weitere Informationen zu unseren Angeboten, Praxisbeispielen sowie aktuellen Workshops und Veranstaltungen!

Impressum

Herausgeber: Regionales Zukunftszentrum Nord, Bildungswerk der Niedersächsischen Wirtschaft gemeinnützige GmbH, Höfestraße 19-21, 30163 Hannover. Redaktion: Regionales Zukunftszentrum Nord, beratung@zukunftszentrumnord.de, www.zukunftszentrumnord.de. Bildnachweise: Details zu einzelnen Bildnachweisen auf Anfrage, Bildmaterial: Fotos der Veranstaltung Fotografin Annalena Pelz. Hinweis: Enthält KI-generierte Bildmaterialien. Gestaltung: Annalena Pelz.

Das Projekt „Regionales Zukunftszentrum Nord (RZ.Nord)“ wird im Rahmen des Programms „Zukunftszentren“ durch das Bundesministerium für Arbeit und Soziales und die Europäische Union über den Europäischen Sozialfonds Plus (ESF Plus) gefördert.

Gefördert durch:

Bundesministerium für Arbeit und Soziales

Kofinanziert von der Europäischen Union