AUSGABE 08

IT insider

TECHNIK. BUSINESS. TRENDS.

EINLEITUNG

KI erobert im Sturm die Welt

IT-INFRASTRUKTUR

Wie KI-Tools die Mitarbeiter beflügeln
In ganz unterschiedlichen Arbeitsbereichen können KI-Tools die Arbeit erleichtern. Ein Überblick.

IT-SICHERHEIT

KI macht Attacken gefährlicher
Cyberkriminelle greifen für ihre Attacken gern auf KI zurück. Was sind die besonderen Gefahren?

IT-SUPPORT

KI und Datenschutz – Hand in Hand?
Wer KI nutzen will, muss den Datenschutz beachten. Das Problem: Vieles ist noch ungeklärt.

IT-SERVICE .NETWORK

Sehr geehrte Damen und Herren, liebe Geschäftspartner,

vielleicht haben Sie es auch bemerkt: Seit dem Beginn des Jahres 2023 befinden wir uns in einer Zeit des Umbruchs. Manche Experten sprechen sogar davon, dass eine neue Phase der Menschheitsgeschichte beginnt. Warum? Weil nach der Automatisierung der körperlichen Arbeit nun auch das Kapitel der Automatisierung von intellektueller, geistiger und kreativer Arbeit beginnt. Konkret geht es darum, dass Anwendungen, die auf (generativer) Künstlicher Intelligenz (KI) basieren, ihren Durchbruch erleben – der entscheidende Schlag dafür ist dem KI-Chatbot ChatGPT gelungen.

Seitdem ist KI-Technologie zu einer echten Spielwiese geworden. Sogar mehr als das. KI-Tools werden längst nicht mehr nur spielerisch ausprobiert. Schon jetzt ist KI für viele Tätigkeiten einfach und effizient anwendbar und erste Unternehmen sind bereits dabei, sie in viele Prozesse einzubinden – und kommen damit zu überraschend guten Ergebnissen. Aus diesem Grund sind sich die Experten auch darin einig, dass KI kein aufflackernder Trend ist, der wieder verlöschen wird; vielmehr schätzen sie KI als einen Trend ein, der die (Arbeits-)Welt gerade in allen Bereichen verändert.

Und das wiederum bedeutet, dass Unternehmen genau jetzt auf den KI-Zug aufspringen sollten – bevor er bereits abgefahren ist. Es gilt zu erlernen, wie sich KI effizient einsetzen und in Workflows integrieren lässt und wie Mitarbeiter mit Hilfe von KI mehr Output erzielen können, indem sie bestimmte Tätigkeiten nicht mehr selbst machen, sondern einer KI präzise mitteilen, was sie zu tun hat. Unternehmen, die diesbezüglich nicht aktiv sind, werden – so die Prognosen – sehr schnell einen Wettbewerbsnachteil haben.

Diese Ausgabe unseres Kundenmagazins ITinsider soll daher ein erster Impuls sein. Wir werfen einen Blick auf die aktuellen Entwicklungen, stellen einige nützliche KI-Tools vor, gehen auf die Problematik des Datenschutzes und des Urheberrechts ein, nennen potenzielle Gefahren durch die neuen KI-Tools und geben Tipps, wie Unternehmen dieser neuartigen Bedrohung begegnen können.

Wir wünschen Ihnen viel Spaß beim Lesen!

Ihr Systemhaus

INHALT

EINLEITUNG

KI erobert im Sturm die Welt
Tools, die mit Künstlicher Intelligenz arbeiten, sind so gefragt, wie nie zuvor. Ist das ihr Durchbruch?

04 | 05

IT-INFRASTRUKTUR

»Hallo? Wer schreibt denn da?«
Ob ChatGPT, Google oder Bing – immer häufiger helfen KI-Textroboter im Berufsalltag.

08 | 09

IT-SICHERHEIT

KI macht Attacken gefährlicher
Cyberkriminelle greifen für ihre Attacken gern auf KI zurück. Was sind die besonderen Gefahren?

12 | 13

IT-SICHERHEIT

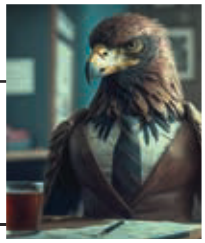
Härtetest für Security Awareness
Die neuen Möglichkeiten für Cyberkriminelle stellen die Security Awareness vor neue Aufgaben.

16 | 17

IT-INFRASTRUKTUR

Wie KI-Tools die Mitarbeiter beflügeln
In ganz unterschiedlichen Arbeitsbereichen können KI-Tools die Arbeit erleichtern. Ein Überblick.

06 | 07



IT-INFRASTRUKTUR

Ein Copilot für jeden Mitarbeiter
Künstliche Intelligenz, die wie eine persönliche Assistenz eingesetzt wird – das gibt es schon jetzt!

10 | 11

IT-SICHERHEIT

Wenn Maschinen sich bekämpfen
Auch in der IT-Sicherheit kommt Künstliche Intelligenz zum Einsatz – und wehrt KI-Angriffe ab!

14 | 15

IT-SUPPORT

KI und Datenschutz – Hand in Hand?
Wer KI nutzen will, muss den Datenschutz beachten. Das Problem: Vieles ist noch ungeklärt.

18 | 19

IMPRESSUM

Herausgeber
SYNAXON AG | Falkenstraße 31 | D-33758 Schloß Holte-Stukenbrock
Telefon 05207 9299 – 200 | Fax 05207 9299 – 296
E-Mail info@synaxon.de | www.synaxon.de
Redaktion
André Vogtschmidt (V.i.S.d.P.), Janina Kröger
Ansprechpartner
André Vogtschmidt | andre.vogtschmidt@synaxon.de

Konzept / Gestaltung
Mirco Becker
Druck
Wentker Druck GmbH | Gutenbergstraße 5 – 7 | 48268 Greven
www.wentker-druck.de

eco zoom natureOffice.com/DE-260-LY8G6DE | Rohstoffe Transporte Produktion | g CO2e 301 Pro Produkt | CO2-Emissionen ausgeglichen

FSC www.fsc.org 100% From well-managed forests FSC® C000000

Zur besseren Lesbarkeit verwenden wir in unseren Texten das generische Maskulinum, sprich die männliche Form. Gemeint sind jedoch immer alle Geschlechter und Geschlechtsidentitäten.

Stand 11/2023. Irrtümer und Druckfehler vorbehalten. Bildnachweise stock.adobe.com: # 616919278 © santima.studio (02); # 627978070 © CYB3RUSS; # 620032513 © KikkyCNX; # 613902473 © Andrey_Lobachev; # 612061420 © Michael; # 622377948 © Kill77ai; # 587821369 © MatinosPhoto; # 606172439 © Bo Dean; # 634411886 © Ai Inspire; # 607875679 © Mukul; # 544104104 © Tatiana Foxy

KI erobert im Sturm die Welt

Noch vor wenigen Jahren gehörte alles, was im Entferntesten mit Künstlicher Intelligenz in Zusammenhang stand, in den Bereich der Science Fiction. Inzwischen ist KI aber ein Thema, das in vielen Unternehmen auf der Agenda steht. Gefühlt kam diese Entwicklung ganz plötzlich: KI erobert im Sturm die Welt!

ChatGPT weckt Interesse an KI

Dieses Datum könnte als ein Meilenstein in die Geschichte eingehen: Am 30.11.2022 wurde der KI-Chatbot ChatGPT präsentiert. In nur zwei Monaten verzeichnete das Tool 100 Millionen Nutzer und stellte damit einen Rekord auf. Zum Vergleich: Instagram hat dafür zwei Jahre gebraucht. Hinz und Kunz wollten den Textroboter ausprobieren und sich ein Bild davon machen, ob er sich tatsächlich kaum von menschlichen Chatpartnern unterscheiden lässt. Über Monate hinweg war ChatGPT ein so präsentes Thema, dass im Mai 2023 bereits 83 Prozent der Bundesbürger wussten, was das eigentlich ist – das geht aus einer repräsentativen Forsa-Umfrage im Auftrag des TÜV-Verbands hervor.

Parallel ist auch die Künstliche Intelligenz (KI) im Allgemeinen zum Thema geworden. Ihre (Weiter-)Entwicklung hat seit dem ChatGPT-Erfolg so richtig an Fahrt aufgenommen – scheinbar ungebremst. Die großen Tech-Konzerne mischen dabei ordentlich mit, aber auch zahlreiche kleinere Unternehmen und Startups bringen ihre KI-Tools auf den Markt. Branchenkenner beobachten im Bereich KI eine qualitative Entwicklung, die mit der Summe des technischen Fortschritts der vergangenen zehn Jahre in diesem Bereich vergleichbar ist. Das Tempo lässt Fachleute wie Laien gleichermaßen schwindlig werden.

Künstliche Intelligenz ruft Euphorie hervor

So mancher hat sich regelrecht in die neue KI-Technologie verliebt. Sie wird als »Wachstumsmotor« gefeiert (Digital-Gipfel), als »Schlüssel-

technologie des Jahrhunderts« bezeichnet (Bundesministerium für Wirtschaft und Klimaschutz) und als »Katalysator für den Fortschritt in Wirtschaft und Gesellschaft« gepriesen (McKinsey). Angesichts der Möglichkeiten, die sie in Aussicht stellt, ist das auch nicht verwunderlich: Die potenziellen Einsatzgebiete scheinen grenzenlos.

Die Verfechter von KI versprechen sich vor allem eine enorme Produktivitätssteigerung. Sie sind der Meinung, dass Unternehmen durch die Implementierung von KI-Technologien effizienter und agiler handeln und sich dadurch einen Wettbewerbsvorteil verschaffen können. Tatsächlich setzen schon heute Unternehmen aus unterschiedlichen Branchen auf Künstliche Intelligenz. Mit KI-Unterstützung werden Texte, Bilder, Audio- und Videoinhalte, Programmcode und 3D-Modelle erstellt; in der Kundenbetreuung übernehmen Chatbots zumindest einen Teil der Kommunikation; KI unterstützt beim Aufstellen von Geschäftsprognosen; und in der Industrie hilft sie, Wartungsarbeiten zu terminieren und Maschinenausfälle zu verhindern.

Skeptiker befürchten unkontrollierbare KI

Demgegenüber stehen aber auch negative Stimmen und Unsicherheiten bezüglich Künstlicher Intelligenz. Zum Beispiel aufgrund der Cybersicherheit. Was passiert mit Unternehmensdaten, die für die Nutzung von KI-Tools benötigt werden? Sind diese wirklich sicher? Entstehen durch KI-Technologien vielleicht auch neue Bedrohungen für die IT-Sicherheit? Dann wären da Bedenken bezüglich Urheberrechten: Wer gilt als Urheber eines Textes, der zunächst von ChatGPT generiert, dann aber durch einen Mitarbeiter weiter angepasst wurde? Auch ethische Fragen kommen auf. Muss beispielsweise kommuniziert werden, wenn KI im Unternehmen genutzt wird?

Damit finden die Bedenken noch längst kein Ende. In vielen Unternehmen kommt die Frage auf, welche Kosten entstehen, wenn sie KI einsetzen und mit den Entwicklungen in diesem Bereich – und mit dem Wettbewerb – mithalten möchten. Andere Unternehmen sehen kritisch auf die Auswirkungen von KI auf die Umwelt, da die Trainingsmodelle exponentiell mehr Rechenressourcen benötigen und diese wiederum bereitgestellt und betrieben werden müssen. Und dann gibt es noch diejenigen, die eine unkontrollierbare Künstliche Intelligenz befürchten, die auch nicht davor zurückscheuen würde, die Menschheit zu vernichten – der »Terminator« lässt grüßen.

Entwicklung lässt sich nicht mehr bremsen

Ausgenommen von Sorgen über eine Weltherrschaftsübernahme durch Roboter sollten Unternehmen ihre Bedenken bezüglich KI trotz aller Euphorie nicht so einfach beiseite schieben. Insbesondere rechtliche Fragen sollten geklärt werden, bevor KI in die Geschäftsabläufe integriert wird. Andernfalls haben sich Mitarbeiter womöglich schnell an die KI-Helferlein gewöhnt und wollen diese auch nicht mehr missen.

Daran, dass sich Unternehmen besser früher als später mit der KI-Thematik beschäftigen sollten, ist jedenfalls nicht zu rütteln. Denn: Allem Anschein nach lässt sich die rasante Entwicklung im Bereich der Künstlichen Intelligenz nicht mehr bremsen. Experten sind überzeugt davon, dass es sich längst nicht mehr um einen Trend handelt, sondern um eine grundlegende Veränderung des (Berufs-)Alltags. Die nächste Stufe der Digitalisierung scheint eingeläutet – und Unternehmen sind gut beraten, diese Entwicklung frühzeitig mitzugehen, denn ansonsten droht (wieder einmal) die Gefahr, im Wettbewerb unwiderruflich abgehängt zu werden. Wie das gelingen kann? Dazu finden Sie verschiedene Anregungen in dieser ITinsider-Ausgabe!

Wie KI-Tools die Mitarbeiter beflügeln

Innerhalb kürzester Zeit sind Tools, die mit Künstlicher Intelligenz arbeiten, wie Pilze aus dem Boden geschossen. Die Bandbreite ist dabei genauso groß wie die potenziellen Einsatzgebiete. Gemeinsam haben die zahlreichen Tools vor allem eins: Sie sollen die Produktivität ankurbeln.

Nützliche kleine Helferchen
Es gibt natürlich auch einen Grund dafür, weshalb sich KI-Tools derzeit so rasant verbreiten: Nachdem die anfängliche Zurückhaltung dank ChatGPT einmal abgelegt ist, wächst die Bereitwilligkeit, auch andere KI-Anwendungen zu testen. Und in der Praxis zeigt sich: Viele der Tools sind tatsächlich ziemlich nützlich! Aber inwiefern genau? Das hängt natürlich vom jeweiligen Tool ab; es gibt aber drei wesentliche Aspekte: KI-Tools können die Arbeit vereinfachen, die Produktivität erhöhen und teilweise sogar ganz neue Möglichkeiten eröffnen. Dabei sollten Unternehmen einen Grundsatz im Hinterkopf haben: Sie sollten KI-Tools als Werkzeug und nicht als Ersatz ansehen. Sprich: Die Tools werden – so schätzen es Experten ein – Arbeitskräfte nicht ersetzen, sie aber potenziell auf ein neues Leistungslevel katapultieren. Natürlich unter der Voraussetzung, dass sie gewillt sind, die Tools zu nutzen und im Umgang damit geschult werden. Unternehmen sind in der Pflicht, das Interesse der Mitarbeiter an KI zu fördern und Schulungen zu ermöglichen.

700+ KI-Tools stehen zur Wahl
Tatsächlich ist die Liste der verfügbaren KI-Tools inzwischen sehr lang. Wie lang? Die Webseite BUZZMATIC führt eine »ultimative Liste mit 700+ AI Tools«, die täglich wächst – und ein Ende dieses Trends ist nicht in Sicht. Entsprechend ist es auch nicht möglich, all diese Tools vorzustellen. Wir wollen aber zumindest einige Anwendungen exemplarisch nennen, die besonders beliebt sind. Achtung: Beachten Sie bei einer Nutzung unbedingt Datenschutz und Urheberrecht! Und zur Info: ChatGPT und Co. sind auf den Folgeseiten ein eigenes Thema.

Midjourney
Das KI-Tool Midjourney ist ein Bildgenerator, der auf der Grundlage von Textaufforderungen Bilder erzeugt. Nutzer können mit der Beschreibung ihrer Ideen eigene Bilder und Kunstwerke erstellen lassen. Probleme gab es anfänglich mit realistischen Darstellungen, beispielsweise bei Händen.

DALL-E
DALL-E, der Bildgenerator von Open AI, erstellt aus einfachen Textaufforderungen Bilder und Kunstwerke. Auch die Bearbeitung von (generierten) Bildern ist möglich. Es lassen sich Komponenten entfernen, Stimmungen verändern oder Variationen erstellen.

Elai.io
Mit dieser KI-unterstützten Videogenerierungsplattform lassen sich personalisierte Videos mit digitalen Avataren erstellen. Zu den Funktionen gehören die Text-zu-Video-Konvertierung, anpassbare Videoerstellung, kamerafreie Produktion und Avatare in Studioqualität.

Elevenlabs
Diese KI-unterstützte Text-to-Speech-Software erzeugt auf der Basis von Texten realistische Audiodateien mit Emotionen und Intonation – nach eigenen Angaben in »jeder« Sprache. Die Audios können zum Beispiel als Voiceover in Videos oder Präsentationen genutzt werden.

Soundraw
Mit diesem KI-Musikgenerator lässt sich lizenzfreie Hintergrundmusik erzeugen. Nutzer können dabei das Tempo, die Stimmung, das Genre und das Thema des Liedes wählen.

Fireflies.ai
Mit Hilfe von KI transkribiert dieses Tool Meetings, Interviews und Anrufe in Echtzeit. Fireflies ist als Webdienst im Browser, als Chrome-Erweiterung, über die API oder als virtueller Teilnehmer in Meetings (u.a. in Zoom, MS Teams, Google Meet und Slack) nutzbar.

Beautiful.ai
Über diese Online-Plattform können Nutzer professionelle Präsentationen erstellen, ohne dass sie selbst über Design-Kenntnisse verfügen. KI hilft dabei, Vorlagen, Folienlayouts und sogar animierte Elemente zu generieren.

genei.ai
Das KI-basierte Tool unterstützt Nutzer dabei, Texte und Informationen effizienter zu lesen, zu recherchieren und zu verstehen. Dazu bietet das Tool Funktionen wie Zusammenfassungen, Keyword-Extraktion oder Volltextsuche.

Grammarly
Grammatik, Rechtschreibung und Stil verbessern – das gelingt mit diesem KI-unterstützten Tool. Grammarly analysiert Texte und liefert Korrektur- und Verbesserungsvorschläge.

tripplanner.ai
Dieses KI-Tool hilft dabei, Geschäftsreisen zu planen. Indem Nutzer Reiseziel(e), Budget, Anforderungen und Co. nennen, schlägt das Tool passende Unterkünfte und Reiserouten vor.

Interior AI
Die Büro- und Geschäftsräume benötigen eine Modernisierung? Einfach Bilder hochladen und durch dieses KI-Tool neu gestalten lassen!

INTEGRIERTE KI
FÜR NAHTLOSE
KOLLABORATION
Präsentieren Sie die beste Version
Ihrer Selbst mit KI-verbesserten
Windows-11-Funktionen und der
KI-Technologie von AMD Ryzen™.
AMD
RYZEN AI
Windows 11
Die AMD-Ryzen™-KI-Technologie ist mit allen Prozessoren der AMD-Ryzen™-7040-Serie kompatibel, mit Ausnahme des AMD-Ryzen™ 5 7540U und AMD-Ryzen™ 3 7440U. Eine OEM-Aktivierung ist erforderlich. Bitte überprüfen Sie vor dem Kauf die Verfügbarkeit der Funktionen bei Ihrem Systemhersteller. GD-220.

»Hallo? Wer schreibt denn da?«

Die Thematik der Künstlichen Intelligenz ist durch den KI-Textroboter ChatGPT richtig ins Rollen gekommen. Das Tool hat einen echten Hype ausgelöst und sogar einen Nutzerrekord gefeiert. Klar, dass sich andere Technologiekonzerne nicht abhängen lassen möchten und eigene KI-Chatbots an den Start bringen.

Textroboter führen KI-Hitliste an

Zu den KI-Tools, die derzeit sowohl privat als auch geschäftlich am häufigsten genutzt werden, gehören zweifellos KI-Chatbots. Das liegt sicherlich daran, dass ChatGPT den ganzen KI-Hype erst so richtig ausgelöst und die Neugier in der breiten Gesellschaft geweckt hat. Ein weiterer Grund ist, dass die Hemmschwelle hier besonders niedrig ist: Chats sind Internetnutzern schon bekannt, seit AOL, Skype, ICQ und Co. in den 2000er Jahren Gesprächspartner virtuell zusammenbrachten; auch WhatsApp, der Facebook-Messenger und Konsorten begleiten uns schon seit vielen Jahren im Alltag; und in Pandemie-Zeiten waren es dann Business-Kommunikationstools wie Microsoft Teams und Slack, die neue Impulse setzen konnten.

Die Chat-Funktion ist also längst vertraut. Nur die Tatsache, dass am anderen Ende kein Mensch, sondern eine Künstliche Intelligenz sitzt, ist noch relativ neu. Und irgendwie ist die Neugier doch recht groß, mit wem man es da eigentlich zu tun hat. Wir haben daher ein Gespräch mit ChatGPT, dem Bing-Chat und Google Bard als den drei derzeit wohl präsentesten KI-Textrobotern angefangen und ihnen erstmal eine simple Frage gestellt: »Hallo? Wer schreibt denn da?«

Im Chat mit künstlicher Intelligenz

Die Antworten fallen sehr unterschiedlich aus. »Hallo! Ich bin ChatGPT, ein KI-Modell von OpenAI. Wie kann ich Ihnen heute helfen?«, antwortet ChatGPT. Auch im Bing-Chat ist die Antwort kurz: »Hallo, das ist Bing. Ich bin ein Chat-Modus der Microsoft-Bing-Suchmaschine. Wie kann ich Ihnen helfen?« Nur Google Bard holt deutlich weiter aus als seine Konkurrenten: »Hallo! Ich bin Bard, ein großes Sprachmodell von Google AI. Ich bin ein Computerprogramm, das entwickelt wurde, um Texte zu generieren, Sprachen zu übersetzen, verschiedene Arten von kreativen Inhalten zu schreiben und deine Fragen auf informative Weise zu beantworten. Ich bin noch in der Entwicklung, aber ich habe gelernt, viele Arten von Aufgaben auszuführen.«

Google Bard – benannt nach dem mittelalterlichen Barden – nennt ein wichtiges Stichwort: großes Sprachmodell (Large Language Modell/LMM). Es handelt sich dabei um maschinelle Lernmodelle, die mit riesigen Mengen von Text und Code trainiert werden, um sprachbezogene Aufgaben zu übernehmen, wie sie Bard bereits beschreibt. Die Grundlage dafür bilden neuronale Netze, die dem menschlichen Gehirn nachempfunden sind und die aus den eingespielten Datensätzen Muster ableiten, um selbst Texte generieren zu können.

Gutes Prompting ist eine Kunst!

Unter einem »Prompt« versteht man die Anfrage an einen KI-Chatbot in Form einer Frage oder einer Anweisung. Es gilt der Grundsatz: Je besser die Anfrage, desto besser das Ergebniss. Wir haben Tipps für Sie!

- **1. Formulieren Sie Anfragen so präzise wie möglich!**
  Schreiben Sie genau, was Sie sich für ein Ergebnis wünschen. Mit »Erstelle ein Anschreiben« kommen Sie nicht weit. Nennen Sie möglichst viele Details!

- **2. Nutzen Sie kurze Sätze ohne Umgangssprache!**
  Mehrere kurze Sätze sind besser verständlich, vor allem wenn viele Details mitgegeben werden. Auch Umgangssprache und Trendbegriffe sind zu vermeiden.

- **3. Geben Sie dem Chatbot eine Rolle!**
  Oft hilft es, dem Chatbot eine bestimmte Rolle zuzuweisen – zum Beispiel: »Du bist Geschäftsführer eines Unternehmens in der Branche XY und möchtest... «

- **4. Stellen Sie Regeln auf!**
  Sie möchten einen kurzen Text und keinen Roman? Er sollte eine bestimmte Zahl an Absätzen und einen spezifischen Sprachstil haben? Legen Sie das alles fest!

- **5. Experimentieren Sie mit Ihren Anfragen!**
  Es gilt, kreativ zu sein und auszuprobieren – so lässt sich nach und nach ein Gespür dafür entwickeln, wie Chatbots besonders gute Antworten produzieren.

- **6. Kontrollieren Sie die Ergebnisse!**
  Beachten Sie, dass KI-Tools falsche Ergebnisse liefern können. Hier muss unbedingt eine Prüfung erfolgen!

ChatGPT, Google Bard und Bing-Chat noch in Lernphase

Wichtig: Die KI-Textroboter sind nicht ausgereift. Google Bard und Bing-Chat geben das auf Nachfrage selbst zu. Sie weisen darauf hin, dass sie zwar schon viel bieten, aber vorerst noch ein Experiment sind. Um ihre Fähigkeiten zu verbessern, würden sie stetig mit neuen Daten aktualisiert. ChatGPT ist weniger selbstkritisch und betont, im September 2021 eine »ziemlich ausgereifte Version« gewesen zu sein, aber ebenfalls noch weiterentwickelt zu werden. Dass die Ergebnisse teils zu wünschen übrig lassen, zeigt sich zum Beispiel in KI-Halluzinationen: Die Bots denken sich etwas aus, wenn sie keine Antwort haben.

Die Weiterentwicklung ist daher natürlich sehr wichtig. Das Training erfolgt weiterhin mit Daten aus Büchern, Artikeln und Webseiten; zudem werden die geführten Chats und Dialoge mit den Nutzern zu Lernzwecken verarbeitet – sofern dies in den Einstellungen nicht explizit untersagt wird. Auch Feedback, das Nutzer direkt in die KI-Tools zurückspielen können, wird für Verbesserungen genutzt.

Welcher KI-Textroboter ist der beste?

Während sich einige Unternehmen bereits für einen – oder auch mehrere – KI-Textroboter entschieden haben, stellt sich in anderen Unternehmen noch die Frage, welcher denn nun der beste ist: ChatGPT, Bing-Chat oder Google Bard? Eine eindeutige Antwort darauf gibt es nicht, denn jedes Tool hat Stärken und Schwächen.

ChatGPT ist gut darin, verschiedene Textarten zu generieren, darunter Gedichte, Geschichten, Analysen usw. Inzwischen kann ChatGPT auch auf das Internet zugreifen und ist mit seiner Datenbasis nicht mehr auf dem Stand von September 2021, wie es bis September 2023 der Fall war. Google Bard ist sogar direkt mit der Google-Suche verknüpft und punktet daher ebenfalls in Sachen Aktualität; zudem gibt Bard kurze und natürliche Antworten, die weniger textlastig sind. Bing-Chat, der in die Microsoft-Bing-Suche integriert ist, kann zusätzlich Bilder erzeugen und bietet personalisierte Hilfe, zum Beispiel bei der Websuche, beim Reisen oder Shopping. Unser Tipp: Testen Sie sich am besten durch!

Ein Copilot für jeden Mitarbeiter

So ein Copilot ist etwas Feines: Er ist stets an der Seite des Piloten und nimmt ihm viele Aufgaben ab. Etwas Ähnliches soll ab sofort auch der gemeine Büroarbeiter erleben dürfen – mit den beiden KI-Tools Microsoft 365 Copilot und Windows 11 Copilot.

Microsoft führt Copiloten ein

Dass Software für so viel Aufsehen sorgt wie jüngst die KI-Tools, kommt selten vor. Vergleichbar ist wohl nur die Anfangszeit der Pandemie, als unter anderem Microsoft Teams in vielen Unternehmen den Geschäftsbetrieb gerettet hat und daher in aller Munde war. Dass Software-Gigant Microsoft auch bei der KI-Thematik ganz vorne mitmischen und die Technologie bestmöglich für Anwender nutzbar machen möchte, ist natürlich keine Überraschung.

Schon früh hat sich Microsoft die Dienste von ChatGPT gesichert und die KI in die eigene Suchmaschine Bing integriert. Das war aber nur ein erster Schritt. Denn: Mit Microsoft 365 Copilot und Windows 11 Copilot haben inzwischen weitere Produkte eine KI-Unterstützung. Stellt sich die Frage, was genau dieser Copilot sein soll. Kurz vorab: Als rechte Hand des Nutzers soll er bei der täglichen Arbeit unterstützen und die Produktivität erhöhen.

Rechte Hand für Büroaufgaben

Microsoft 365 Copilot lässt sich bei der Abo-Lösung Microsoft 365 unter anderem in die klassischen Büroanwendungen Word, Teams, Outlook, PowerPoint und Excel integrieren. Er hilft dem Nutzer anschließend bei der Erledigung seiner Aufgaben. So, wie der Copilot im Flugzeug den Kapitän unterstützt, arbeitet der Microsoft Copilot dem Nutzer zu und nimmt ihm (Teil-)Aufgaben ab. Der Nutzer soll dadurch noch kreativer und produktiver arbeiten und seine persönlichen Fähigkeiten verbessern können.

Die Bandbreite der unterstützenden Tätigkeiten ist vielfältig: Copilot ist etwa in der Lage, Texte und Präsentationen zu erstellen, Daten zu analysieren, E-Mail-Kommunikation zu übernehmen oder Gesprächsprotokolle zur Verfügung zu stellen. Ganz neu ist ein Feature namens Business Chat, das wie ein persönlicher Assistent arbeitet. In einem Teams-Chat lässt es sich dabei mit dem Copiloten wie mit einem realen Geschäftspartner kommunizieren, zum Bespiel um ihm Aufgaben zu übertragen oder einen Projektstatus abzufragen.

Persönlicher Assistent im Arbeitsalltag

Auch der ebenfalls auf Künstlicher Intelligenz basierende Windows 11 Copilot soll wie ein persönlicher Assistent agieren und bei den täglichen Aufgaben unterstützen. Ist der Copilot einmal installiert, ist er fortan als Symbol in der Taskleiste zu finden. Hier lässt er sich per Mausklick oder alternativ über das Tastenkürzel »Windows-Taste + C« starten. Auf beiden Wegen erscheint der Windows-Copilot anschließend als Seitenleiste am rechten Bildschirmrand.

In dieser Seitenleiste bieten sich verschiedene Optionen. Unten ist der aus dem Bing-Chat bekannte Suchschlitz zu finden, über den sich Konversationen mit Copilot beginnen und Aufgaben an ihn stellen lassen. Falls gewünscht, bleibt die Seitenleiste bei allen weiteren Tätigkeiten in allen Apps und Programmen verfügbar und begleitet den Nutzer somit durch den Tag. Sie bietet die Möglichkeit, Fragen zu stellen, Einstellungen zu ändern, Programme zu starten, Texte zu schreiben und Bilder zu erzeugen.

Large Language Models sind die Basis

Die beiden kostenpflichtigen Copiloten greifen auf große Sprachmodelle (Large Language Models / LLM) zurück, um die genannten Funktionen bieten zu können, und kombinieren deren Fähigkeiten unter anderem mit Microsoft-Graph-Daten und den Microsoft-365-Apps. Die Copiloten sind dadurch in der Lage, Informationen und Daten aus verschiedenen Apps und Speicherorten zusammenzutragen und zu sinnvollen Ergebnissen zusammenzuführen.

Wer sich die Funktionen von Microsoft 365 Copilot und Windows 11 Copilot genau ansieht, wird schnell merken, dass sie so manche Vorteile für Unternehmen mitzubringen scheinen. In erster Linie wäre die potenzielle Arbeitserleichterung zu nennen: Wenn Mitarbeiter mit wenigen Tastenanschlägen und Klicks Programme aufrufen, Einstellungen ändern oder Texte erstellen lassen können, bedeutet das eine deutliche Zeitersparnis. Und mit der Zeitersparnis geht eine höhere Produktivität einher, denn die gewonnene Zeit lässt sich für andere Aufgaben nutzen, sodass sich unterm Strich mehr Tätigkeiten erledigen lassen.

So sichern Sie sich Ihre Copiloten!

Sowohl Microsoft 365 Copilot als auch Windows 11 Copilot werden vermutlich noch im Herbst 2023 veröffentlicht – nachdem sie ausgiebig getestet worden sind. Für Unternehmenskunden werden die Tools dann als Addons zur Verfügung stehen, die kostenpflichtig hinzugebucht beziehungsweise erworben werden können. Denn: Während es sich bei Microsoft 365 um ein Abonnement-Produkt handelt, ist die Lizenz für Windows 11 per Einmalkauf erhältlich. Sie benötigen Unterstützung bei der Beschaffung und Implementierung der KI-Tools? Wir helfen gern!

Setzen Sie auf Original-Software!

In den Jahren 2021 und 2022 waren mehr als zwei Drittel der Unternehmen Opfer eines Firmware-Angriffs – und in einigen Fällen war die Nutzung von gefälschter Software der Grund für den Erfolg der Angreifer. Denn: Anders als es bei korrekt lizenzierter und geprüfter Original-Software der Fall ist, erhalten gefälschte Kopien keine regelmäßigen Updates, mit denen neu entdeckte Sicherheitslücken geschlossen werden. Die Verwendung von Nicht-Original-Software ist daher eines der größten Cybersecurity-Risiken. Unternehmen sollten dieses Risiko unbedingt vermeiden, da mit erfolgreichen Cyberangriffen unter anderem Datenverluste, die Unterbrechung des Geschäftsbetriebs sowie Reputations- und Sachschäden einhergehen. Aber nicht nur das: Es drohen weiterhin Strafzahlungen bei Verstößen gegen die europäische Datenschutzgrundverordnung. Auch falsch lizenzierte Software kann zu Strafzahlungen in ungeahnter Höhe führen. Daher lautet unser Rat: Setzen Sie auf Original-Software von Microsoft und schützen Sie Ihre Unternehmensdaten dadurch vor Bedrohungen verschiedener Art – für weitere Informationen sprechen Sie uns gern an!

KI macht Attacken gefährlicher

Dass KI-Tools nützlich sind, haben auch Cyberkriminelle entdeckt: Sie nutzen die praktischen Helferlein gezielt für ihre Betrugstechniken. Für Unternehmen bedeutet das, noch mehr Wachsamkeit an den Tag zu legen, um nicht zum Opfer von KI-Angriffen zu werden.

Auch Hacker nutzen KI-Tools

Anwendungen, die mit Künstlicher Intelligenz arbeiten, haben sich als sehr nützlich erwiesen. Die schier unendlichen Einsatzmöglichkeiten sind aber nicht nur für Unternehmen vielversprechend. Denn: Cyberkriminelle haben das Potenzial genauso erkannt wie der Rest der Welt. Längst nutzen sie KI-Tools, um ihre Attacken auf ein neues Level zu bringen. Bereits jetzt zeigt sich, dass Cyberangriffe eine zunehmende Häufigkeit und eine höhere Erfolgsquote aufweisen.

Künstliche Intelligenz ist somit der beste Komplize: Sie lernt schnell, ist genauso erfinderisch wie die Cybergangster selbst, hat keine moralischen oder ethischen Bedenken und leistet mühelos das, was als Beihilfe zu einer Straftat oder als Herstellung von Tatwaffen bekannt ist. Das Schadenspotenzial von KI-Angriffen ist dabei riesig – so wie die Bandbreite potenzieller Angriffe. Einige Methoden stellen wir hier vor.

Methode 1: ChatGPT als Phishing-Thema

Beim Phishing versuchen Kriminelle, über betrügerische Webseiten, E-Mails, Textnachrichten oder Anrufe an vertrauliche Daten zu gelangen – darunter Bank- und Anmeldedaten oder Sozialversicherungsnummern. Diese werden dann für Identitätsdiebstahl, Kreditkartenbetrug oder Ransomware-Angriffe genutzt. Phishing-Attacken sind oft mit finanziellen Verlusten und Datenschutzverstößen verbunden.

Für ihre Attacken wählen die Angreifer meist Aufhänger, die potenziell eine große Nähe zum Opfer haben oder ein aktuelles, brisantes Thema aufgreifen. Neuerdings wird daher auch gern ChatGPT als Köder genutzt. So wird beispielsweise in E-Mail-Betreffzeilen ein Bezug zum derzeit bekanntesten KI-Chatbot hergestellt – in der Hoffnung, dass potenzielle Opfer auf die Masche hereinfallen.

Methode 2: Chatbots als Phishing-Helfer

Cyberkriminelle lassen sich von KI-Tools die Texte für ihre Phishing-E-Mails und Webseiten schreiben und können dadurch den Erfolg ihrer Kampagnen maßgeblich verbessern. Bisher galten sprachliche Ungenauigkeiten nämlich als ein wichtiges Indiz dafür, dass es sich bei E-Mails, Nachrichten oder Webseiten um Betrug handeln könnte. Dieses Indiz wird nun hinfällig, da die Textroboter innerhalb kürzester Zeit korrekte und sogar personalisierte Texte erstellen.

Noch perfekter wird ein Phishing-Versuch, wenn die Kriminellen zusätzlich KI-Tools nutzen, die täuschend echte Kopien von Webseiten erstellen. Über einen Link in den Phishing-E-Mails gelangen die Opfer auf perfekt gefälschte Webseiten, auf denen Anmeldedaten abgefragt oder per Drive-by-Download Malware-Arten ausgeliefert werden.

7 Maßnahmen zu Ihrem Schutz!

- **Moderne Sicherheitslösungen nutzen:** Die Hersteller von Sicherheitslösungen haben die Gefahr von KI-Attacken auf dem Schirm und passen ihre Software an.
- **KI mit KI bekämpfen:** Manche Angriffe lassen sich nur mit den eigenen Mitteln bekämpfen – auch im Fall von KI-Angriffen. Spezielle KI-Systemen decken Anomalien auf (dazu mehr auf den Seiten 14/15).
- **Mitarbeiter schulen:** Die Angestellten sollten über die Risiken von KI-Angriffen informiert sein, damit sie verdächtige Aktivitäten und Phishing-Versuche erkennen. Security-Awareness-Schulungen sind ideal.
- **Mehrstufige Authentifizierung nutzen:** Ob KI oder nicht – vor vielen Cyberangriffen schützt eine mehrstufige Authentifizierung. Sie stellt sicher, dass nur autorisierte Personen auf sensible Daten zugreifen können.
- **Regelmäßig Updates durchführen:** Neu entdeckte Sicherheitslücken durch Updates zu schließen, ist extrem wichtig. KI könnte nämlich auch genutzt werden, um Schwachstellen in Software aufzuspüren.
- **Drittanbieter-Software überprüfen:** Betriebe sollten die Software von Lieferanten/Partnern auf Schwachstellen prüfen. Stichwort: Supply-Chain-Angriff.
- **VPN-Dienste verwenden:** Ein Virtual Private Network (VPN) ist für Unternehmen wichtig. Es erhöht die Netzwerksicherheit, indem es verschlüsselte Verbindungen zwischen Unternehmenssitz und Endgeräten herstellt.

Methode 3: Chatbots als Malware-Erzeuger
KI-Chatbots können sogar selbst Malware erstellen – praktisch für jene Kriminellen, die selbst keine Programmierkenntnisse haben. Häufig kommen dabei zwar keine raffinierten Schadprogramme heraus; das könnte sich aber bald ändern, schließlich KI ist lernfähig.

In Darknet-Foren werden die Möglichkeiten der Malware-Generierung übrigens ausgiebig diskutiert. Die Forscher von Checkpoint Research haben dort verschiedene von ChatGPT generierte Schadcodes entdeckt, die Daten stehlen oder verschlüsseln können – also Infostealer und Ransomware. Mit Hilfe weiterer KI-Tools können Cyberkriminelle sogar ganze Angriffsketten kreieren. Das Schadenspotenzial ist riesig!

Methode 4: Deepfakes als Köder
KI-Technologien werden auch eingesetzt, um gefälschte Bilder, Videos und Sprachdateien zu erstellen – sogenannte Deepfakes. Auch hier ist das Schadenspotenzial schier grenzenlos. Angreifer können beispielsweise frei erfundene Geschichten durch Fotofälschungen glaubwürdig erscheinen lassen oder anhand von Fotos die Gesichter von Personen in Videos eingefügen, die gar nicht anwesend waren.

Derartige Deepfakes gibt es auch bei Sprachnachrichten. Alles, was man dafür braucht, ist ein entsprechendes KI-Tool sowie echte Sprachaufnahmen einer Person. Mit etwas Training ist das Tool bald in der Lage, die Stimme nachzubilden und gefälschte Sprachnachrichten zu erstellen – beste Voraussetzungen für einen CEO-Fraud!

KI-Tools erschaffen böse neue (Cyber-)Welt
Die Liste an Methoden, mit denen Künstliche Intelligenz schon jetzt für kriminelle Zwecke eingesetzt wird, ließe sich noch viel weiter ausführen. Mit FraudGPT und WormGPT beispielsweise gibt es inzwischen sogar KI-Tools speziell für Cyberkriminelle. Die Szenarien, die von Sicherheitsfachleuten gezeichnet werden, sehen dementsprechend düster aus. Sogar von einer Terminator-Malware ist die Rede! Ob etwas Wahres dran ist oder nicht: Unternehmen haben keine andere Wahl, als sich vor den neuen KI-Angriffen zu wappnen.

Wenn Maschinen sich bekämpfen

Die dunkle Seite der Macht nutzt KI bereits für ihre Attacken. KI wird aber auch zunehmend eingesetzt, um Unternehmen vor Angriffen zu schützen: Sie kann nämlich dabei helfen, Bedrohungen schneller und präziser zu erkennen und sie dadurch abzuwehren.

Neue Angriffsarten, neue Abwehrtechnik
Es ist ein ständiger Wettlauf: Cyberkriminelle entwickeln neue Angriffstechniken, woraufhin die Anbieter von Sicherheitslösungen ihre Anwendungen nachrüsten, um auch vor den neuen Angriffsarten zu schützen. Das allein wäre für IT-Sicherheitsteams eigentlich schon Herausforderung genug. Jetzt aber haben Cyberkriminelle auch noch Künstliche Intelligenz für sich entdeckt, wodurch ihre Attacken an Quantität und Qualität massiv zugenommen haben.

Die Folge dessen ist, dass traditionelle Sicherheitslösungen damit kaum mehr Schritt halten können. Dementsprechend macht der Einsatz von KI als Cyberwaffe den Einsatz von KI in der Abwehr von KI-unterstützten Cyberattacken unabdingbar. Oder anders gesagt: In diesem neuen Zeitalter kämpft KI gegen KI, Maschine gegen Maschine. Der Schlüssel des Ganzen ist selbstlernende KI-Technologie, die die Hersteller nun in ihren Sicherheitslösungen einsetzen.

So arbeiten KI-Sicherheitstools
Die selbstlernenden, KI-basierten Sicherheitstechnologien machen sich in erster Linie die fortlaufende Analyse enormer Mengen an Risikodaten zunutze. Sie analysieren Netzwerke im Hintergrund auf typische Verhaltensmuster von berechtigten Nutzern, Geräten und Systemen, lernen dabei ‚normales' Verhalten kennen und können dadurch schon kleinste Anomalien, die auf Cyberattacken (auch bisher unbekannten Typs) hindeuten könnten, in Echtzeit identifizieren. Ein solches Machine Learning kann auch (Angriffs-)Muster und Verhaltensweisen erkennen, die herkömmlichen Programmen womöglich entgehen.

Das maschinelle Lernen steht aber häufig nicht allein im Kampf gehen (KI-)Attacken. Vielmehr hilft in einigen Lösungen auch die Verarbeitung natürlicher Sprache, die Bedrohungsdaten aus Millionen von Forschungsberichten, Blogs und Nachrichten filtert. Dadurch lassen sich die Flut täglicher Warnmeldungen bewältigen, Erkenntnisse zu aktuellen Angriffsarten gewinnen und Reaktionszeiten verkürzen.

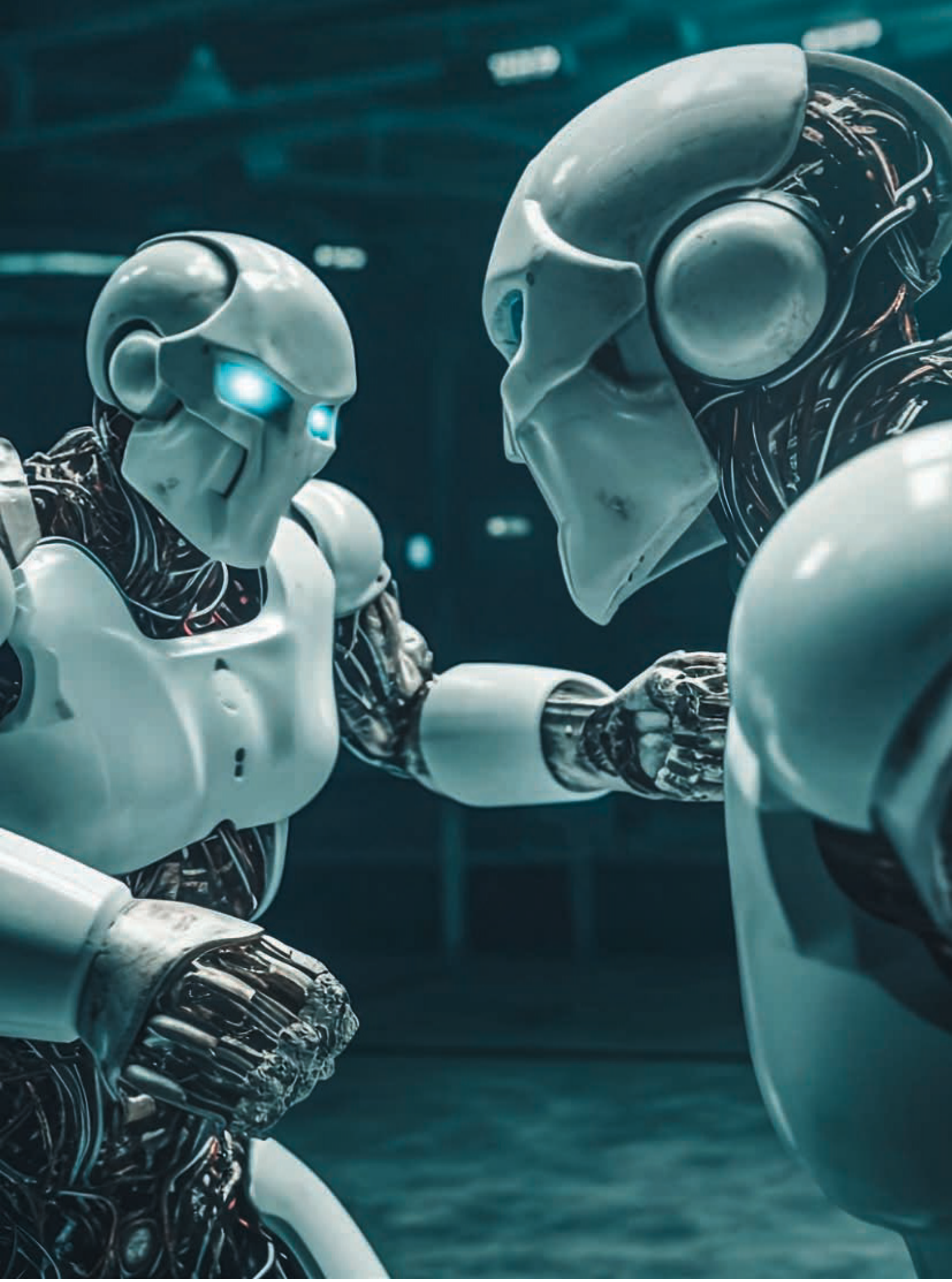
KI-basierte Sicherheitstools einsetzen
KI-gestützte Antivirensoftware kann (un-)bekannte Malware schneller und genauer erkennen; KI-gestützte Intrusion Detection Systeme (IDS) können ungewöhnliche Aktivitäten im Netzwerk identifizieren und melden; KI-gestützte Log-Analysen können Sicherheitsvorfälle schneller und präziser identifizieren; KI-gestützte Spam-Filter können Phishing-Mails effektiver erkennen und blockieren; und KI-gestützte Sicherheitsanalysen können Schwachstellen besser identizifieren und beheben.

Erste Erfahrungswerte beim Einsatz solcher KI-Sicherheitstools geben durchaus Grund zur Hoffnung. Ein Lösungsanbieter, dessen Tool von 6.500 Nutzern eingesetzt wird, berichtet beispielsweise, dass durch den Einsatz von KI durchschnitllich 150.000 Bedrohungen pro Woche autonom unterbrochen werden konnten – dank einer Frühindikatoranalyse, die die Muster potenzieller Cyberangriffe in mehreren Phasen auf Anomalien untersucht.

Security-Teams entlasten
KI-gestützte Systeme können eine Reihe von Sicherheitsaufgaben automatisieren, die sonst von menschlichen Sicherheitsexperten durchgeführt werden müssten; die Experten haben dadurch mehr Zeit für die Reaktion auf komplexe Bedrohungen, wodurch sich die Effizienz und Effektivität der Cybersicherheit insgesamt verbessert. Wichtig: KI-basierte Sicherheitslösungen sind nicht perfekt und nur ein Teil einer umfassenden Cybersicherheitsstrategie.

Diese Software-Anbieter setzen auf KI

KI-basierte Sicherheitslösungen werden immer beliebter, da sie Unternehmen dabei helfen können, ihre Cybersicherheitslage zu verbessern und sich effektiv vor den sich ständig weiterentwickelnden Bedrohungen aus dem Cyberraum zu schützen – vor allem wenn hier ebenfalls KI zum Einsatz kommt. Anbieter wie CrowdStrike, Cisco, Fortinet, IBM Security, Kaspersky, Microsoft, Palo Alto Networks, PhishLabs und Symantec bieten daher bereits eine breite Palette von Sicherheitslösungen an, die unter anderem für die Anomalieerkennung, für die Threat Intelligence, für das Benutzer-Management oder den Endpoint-Schutz auf KI setzen. Neben diesen großen Anbietern gibt es auch eine Reihe von kleineren Lösungsanbietern, die sich mit ihren KI-Anwendungen auf bestimmte Bereiche der Cybersicherheit konzentrieren.



Härtetest für Security Awareness

KI-Technologien können die Arbeitswelt revolutionieren, sie bringen aber auch neue Herausforderungen mit sich: KI in den Händen von Cyberkriminellen macht Cyberangriffe noch gefährlicher. Unternehmen müssen daher die Security Awareness der Mitarbeiter ausbauen, um sich vor KI-Gefahren zu schützen.

Die Rolle von KI in der Bedrohungslage

Cyberkriminelle setzen immer häufiger auf Künstliche Intelligenz, um ihre Angriffe zu verfeinern. Die Folge: Phishing-E-Mails und gefälschte Webseiten erscheinen täuschend echt, Deepfakes sind immer schwerer von echten Videos, Bildern oder Sprachnachrichten zu unterscheiden, und es wird für Angreifer immer einfacher, personalisierte Angriffe zu starten. Für die potenziellen Opfer wird es im Gegenzug immer schwieriger, nicht auf die Täuschungsmanöver hereinzufallen – und das wiederum ist für Unternehmen ein ernsthaftes Problem, denn nach wie vor gilt die sogenannte »Schwachstelle Mensch« als die größte Gefahr für die Sicherheit von Unternehmensnetzwerken.

Laut einer Studie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist der Mensch in 90 Prozent aller Cyberangriffe das Einfallstor. Cyberkriminelle zielen gezielt auf menschliche Schwächen ab, um in Unternehmensnetze einzudringen. Wie? Indem sie ihre Opfer leider allzu häufig mit Hilfe von sogenannten Social-Engineering-Methoden manipulieren, dabei menschliche Emotionen wie Angst oder Neugier adressieren und die Opfer dazu bringen, sensible Daten preiszugeben oder bösartigen Code auszuspielen.

Security Awareness – was ist das?

Ausmerzen lässt sich diese Schwachstelle eigentlich nur, indem die Security Awareness der Mitarbeiter gestärkt wird. Aber was genau ist das? Security Awareness bezieht sich auf das Bewusstsein und die Wachsamkeit einer Person oder Organisation in Bezug auf die Sicherheitsrisiken und -gefahren in der digitalen Welt. Es geht darum, dass Menschen für die verschiedenen Bedrohungen sensibilisiert sind, die in der heutigen vernetzten Welt existieren, und dass sie in der Lage sind, diese Gefahren zu erkennen und zu verhindern.

Dazu gehört beispielsweise, sichere Passwörter zu erstellen und zu verwalten, auf Phishing-Versuche zu achten, sicher mit sensiblen Daten umzugehen und verdächtige Aktivitäten zu erkennen. Ebenfalls gehört dazu, dass Software-Updates regelmäßig durchgeführt und Sicherheitssoftware genutzt wird – wobei hier natürlich auch die IT-Abteilung des Unternehmens beziehungsweise der zuständige externe IT-Dienstleister in der Verantwortung ist. Unternehmen sollte bewusst sein, dass eine starke Security Awareness die erste Verteidigungslinie gegen Cyberangriffe darstellt und dabei hilft, Unternehmensdaten und persönliche Informationen zu schützen.

Security Awareness unter Druck

Wenn eine mangelnde Security Awareness schon vorher ein Problem war, ist sie es im Zeitalter der KI noch mehr. Denn: Die steigende Nutzung von KI durch Cyberkriminelle stellt die Security Awareness vor einen echten Härtetest. Es ist zum Beispiel nicht mehr ausreichend, verdächtige E-Mails oder Webseiten auf Rechtschreibfehler zu untersuchen, was zuvor als ein wichtiges Indiz für Phishing-Versuche galt – dank KI-Tools werden Texte nun grammatikalisch korrekt erstellt.

Das bedeutet: Security Awareness erfordert ab sofort ein noch tieferes Verständnis der neuen Angriffsmethoden und ein kritisches Bewusstsein für Online-Aktivitäten. Um die Gefahren von KI-basierten Angriffen zu mindern, sind daher spezielle Security-Awareness-Schulungen entscheidend. Sie sensibilisieren Mitarbeiter für die Risiken von Phishing, Deepfakes und Co. und helfen ihnen dadurch, neue Bedrohungen zu erkennen und angemessen darauf zu reagieren.

Am Ball bleiben und sich anpassen

Die Bedrohungen durch KI entwickeln sich ständig weiter. Was heute als sicher gilt, kann morgen bereits veraltet sein. Daher ist es entscheidend, dass Unternehmen und ihre Mitarbeiter ständig auf dem neuesten Stand bleiben und sich an die sich ändernde Bedrohungslage anpassen. Allerdings ist das im normalen Geschäftsalltag so nebenbei kaum möglich – und genau deshalb ist es insbesondere für kleine und mittelständische Unternehmen ratsam, sich Hilfe zu suchen.

Zum Beispiel bei uns! Wir stehen Ihnen zur Seite, um Ihr Unternehmen vor den Gefahren der KI-basierten Bedrohungen zu schützen. Dafür bieten wir Ihnen entweder selbst umfassende Security-Awareness-Schulungen an oder können Ihnen diese vermitteln. Gern unterstützen wir Sie auch dabei, Ihre IT-Infrastruktur so sicher wie möglich aufzustellen. Wir sind Ihr Partner im Kampf gegen die wachsenden Bedrohungen der Cyberwelt. Melden Sie sich für weitere Infos!

KI und Datenschutz – Hand in Hand?

Bedenken hinsichtlich des Datenschutzes lassen viele Unternehmen vor einer KI-Nutzung zurückschrecken. Das ist durchaus berechtigt – immerhin werden jede Menge (personenbezogene) Daten verarbeitet. Lassen sich KI und Datenschutz irgendwie in Einklang bringen?

KI und Datenschutz – was ist das Problem?
Künstliche Intelligenz soll Intelligenz und Handeln des Menschen nachempfinden und muss dazu von ihm selbst lernen – beziehungsweise aus den Daten, die er produziert. Die Large Language Models (LLMs), die in Form von neuronalen Netzwerken (ähnlich dem menschlichen Gehirn) hinter (generativer) KI stecken, werden dazu mit riesigen Datensätzen trainiert, unter anderem aus Büchern, Artikeln, Bildern, Videos und Code. Für die Weiterentwicklung der KI-Tools werden zudem Daten aus der praktischen Anwendung herangezogen. ChatGPT und Google Bard beispielsweise lernen mit jeder geführten Unterhaltung dazu.

Problematisch ist das, weil jede Menge personenbezogene Daten involviert sind. Mit jeder Eingabe können Nutzer direkt oder indirekt teils sensible Informationen über sich und andere preisgeben – etwa zu politischen, religiösen, weltanschaulichen oder wissenschaftlichen Fragen oder auch zur persönlichen Lebenssituation. Und genau solche Informationen sind besonders schützenswert.

Personenbezogene Daten in Gefahr
Das zentrale Problem von KI und Datenschutz besteht also darin, dass personenbezogene Daten mit im Spiel sind. Das eröffnet einen regelrechten Fragenhagel. Welche Daten werden erhoben und wie werden sie verwendet? Wie sicher sind solche Daten bei den Betreibern der Tools? Ist ein Schutz vor Datenlecks gewährleistet? Besteht die Gefahr eines Datendiebstahls durch Hacker? Lassen sich Tools dazu bringen, sensible Informationen offenzulegen (Stichwort: Training Data Extraction Attack)? Besteht die Gefahr von Profiling, wenn personenbezogene Daten aus verschiedenen Quellen kombiniert werden? Welche Chance gibt es, eine Datensammlung zu verhindern? Was ist mit dem Recht auf Vergessenwerden? All das sind berechtigte Fragen, die zu KI und Datenschutz gestellt werden. Es gilt, angemessene Datenschutzbestimmungen und Ethikrichtlinien zu entwickeln und sicherzustellen, dass KI-Technologien mit den Rechten und Bedürfnissen von Individuen im Einklang stehen.

Datenschutzbehörden prüfen KI-Tools
Natürlich sind die zuständigen Datenschutzbehörden längst dabei, sich damit auseinanderzusetzen. Sie stellen den Technologie-Entwicklern umfangreiche Fragenkataloge, die auch die bereits genannten Fragen enthalten. Abgeklärt werden soll damit, zu welchen Zwecken eingegebene Daten verarbeitet werden und aus welchem Datenpool die KI ihr Wissen speist – und ob dabei die datenschutzrechtlichen Grundprinzipien eingehalten werden. Die Forderungen des Datenschutzes sollen aber nicht darauf abzielen, KI zu blockieren, sondern KI und Datenschutz in Einklang zu bringen. Oder anders gesagt: Aus den neuen KI-Technologien soll sich größtmöglicher Nutzen ziehen lassen, gleichzeitig sollen Grundrechte und Datenschutzprinzipien bei ihrer Verwendung geschützt und gefördert werden.

Risiken bewerten & abwägen
Einen wichtigen ersten Schritt zur Regulierung von KI und Datenschutz hat das Europäische Parlament bereits gemacht: mit dem AI Act – dem weltweit ersten Gesetz zur Arbeit mit Künstlicher Intelligenz. Dennoch ist vieles noch ungeklärt. Eine Entscheidung dazu, ob sich ChatGPT datenschutzkonform nutzen lässt, steht seitens der Datenschutzbehörden zum Beispiel noch aus (Stand: Okt. 2023). Sowohl OpenAI als auch Google haben aber bereits Enterprise-Lösungen angekündigt, bei denen ein noch höheres Maß an Datenschutz zu erwarten ist. Grundsätzlich muss jedes Unternehmen für sich selbst die (Datenschutz-)Risiken bewerten und abwägen. Wir helfen dabei gern!

Mensch oder KI: Wer ist der Urheber?

Mit dem Urheberrecht werden künstlerische oder wissenschaftlich-technische Leistungen geschützt, die eine gewisse Originalität und Kreativität repräsentieren. Allerdings muss es sich dabei um eine »persönliche geistige Schöpfung« handeln. KI aber ist keine Person, sodass sich die Frage stellt: Wer ist der Urheber eines KI-generierten Werkes – die KI oder der Mensch, der die KI beauftragt hat? Aktuell geht man davon aus, dass KI-generierte Werke nicht durch das Urheberrecht geschützt sind, da sie kein »Werk« sondern ein »Output« sind. Achten Sie bezüglich des Urheberrechts unbedingt auf die Angaben des jeweiligen Herstellers!

Tipps zur KI-Nutzung im Betrieb

- **Seien Sie bei der Nutzung von KI-Tools vorsichtig!**
  Sie sollten die Ergebnisse der Datenschutzaufsichtsbehörden unbedingt beachten. Bleiben Sie bezüglich aktueller Entscheidungen und Entwicklungen am Ball!

- **Stellen Sie klare Regeln zur KI-Nutzung auf!**
  Überlegen Sie, für welche Zwecke Sie KI nutzen möchten. Für Recherchen ist die Nutzung weniger problematisch, denn daraus lassen sich höchstens Rückschlüsse auf (Unternehmens-)Interessen ziehen.

- **Geben Sie keine personenbezogenen Daten ein!**
  Wenn ein KI-Chatbot ein Kundenanschreiben für Sie erstellen soll, können Sie Pseudonyme wie Max Mustermann nutzen und den Textentwurf später in ihrem Schreibprogramm mit den realen Namen anpassen.

- **Erlauben Sie die Nutzung nur betrieblich!**
  Eine private Nutzung sollte ausdrücklich verboten werden – nicht um Ihre Mitarbeiter zu ärgern, sondern um deren persönliche Daten zu schützen.

- **Nehmen Sie die sichersten Einstellungen vor!**
  Sie können bei manchen Tools verhindern, dass Unterhaltungen in die Trainingsdaten der KI übernommen werden. Möglich ist auch, dass Suchverläufe nicht oder nur eine bestimmte Zeit lang gespeichert werden.

- **Lassen Sie sich durch Experten schulen!**
  Schulungen für Sie und Ihre Mitarbeiter helfen nicht nur dabei, die internen Richtlinien zu verstehen und umzusetzen. Sie sorgen auch dafür, dass Sie über neue Entwicklungen auf dem Laufenden bleiben.

ÜBERREICHT DURCH

cosoft computer consulting gmbh

Borkener Str. 134a
48653 Coesfeld

Telefon +49 2541 94750
E-Mail order@cosoft.de

http://www.cosoft.de

cosoft
Ihr IT-Systempartner – seit 1985