Tiefgreifende Veränderung

Von Holger Köster

Holger Köster

Geschäftsführer der HERSA-Unternehmensgruppe und Vorsitzender des BDSW-Arbeitskreises Wirtschaftsschutz

Die Erfindung der Dampfmaschine oder der Elektrizität wird nicht ohne Grund als revolutionär bezeichnet. Sie haben das Leben der Menschen grundlegend verändert. Ähnlich wird es sich mit der Künstlichen Intelligenz (KI) verhalten. Ihr Einsatz im Bereich Sicherheit und Verteidigung bringt selbstverständlich tiefgreifende Veränderungen mit sich.

Während Chancen für innovative Sicherheitsanwendungen entstehen, wächst natürlich auch die Gefahr KI-gesteuerter Angriffe. KI ist dabei aber kein bloßer Teilaspekt technischer Entwicklung, sondern wird alle anderen Bereiche grundlegend transformieren. Nicht auf die leichte Schulter zu nehmen sind auch ethische Vorbehalte.

Andererseits birgt KI enormes Potenzial – sowohl zivil als auch militärisch. KI hat ja auch bereits unsere Sicherheitsbranche erreicht, denn, um nur ein Beispiel zu nennen, die ersten Roboter agieren bereits als Helfer im Wachschutz und in der Gebäudeinspektion. Sie sind nicht abgelenkt, können sehr viele Informationen gleichzeitig verarbeiten und werden im Einsatz niemals müde. Außer – der Akku ist leer.

Obwohl der Roboter seine Aufgaben zu 100 Prozent sicher und zuverlässig erfüllt, behält der Mensch derzeit noch die Kontrolle über ihn. Während der Roboter wacht, prüft und meldet, trifft der Mensch die ultimative Entscheidung und wird aktiv, wenn es sinnvoll und notwendig ist. Auf diese Weise wird moderne, KI-unterstützte Sicherheitsarbeit zu einer integrierten Teamlösung bestehend aus Mensch (Sicherheitsmitarbeiter) und Maschine.

So wäre KI sozialverträglich, ethisch vertretbar und somit auch in der Zukunft denkbar.

In diesem Sinne: Bleiben Sie auf der sicheren Seite!

Ihr
Holger Köster

Bild: Dieter Poschmann / pixelio.de

Automation und KI haben sich schon längst in der Industrie einen festen Platz erobert. Unser Bild zeigt einen Absetzroboter.

Künstliche Intelligenz: keine Zukunftsmusik, sondern schon längst Teil unseres Alltags

Von Klaus Henning Glitza

Niemand muss Terminator oder „Aufstand der Maschinen" gesehen haben, um Künstliche Intelligenz (KI) nicht zumindest ein bisschen unheimlich zu finden. Die Vorstellung, dass Maschinen intellektuelle Fähigkeiten des Menschen nachahmen oder gar übertreffen, ist vielen Zeitgenossen in nachvollziehbarer Weise ein Graus. Dabei ist KI keine Science-Fiction, sondern in bestimmten Varianten schon längst Teil unseres Alltags geworden. Auch im Wach- und Sicherheitsdienst haben KI-Anwendungen bereits ihren Platz gefunden.

Klaus Henning Glitza

Ehemaliger Redakteur der Hannoverschen Allgemeinen Zeitung, Träger des Deutschen Förderpreises Kriminalprävention (Stiftung Kriminalprävention, Münster) und seit 2003 als Fachjournalist für Sicherheitsfragen tätig

„Künstliche Intelligenz" ist nach einer Definition des Europäischen Parlaments „die Fähigkeit einer Maschine, menschliche Fähigkeiten wie logisches Denken, Lernen, Planen und Kreativität zu imitieren". Das ist von der klassischen Automation, bei der praktisch im Sinne einer Dressur alle Schritte vorprogrammiert und angelernt sein müssen, zu unterscheiden. Eine KI-Anwendung kann, so ist es das Ziel, ähnlich einem Menschen sehen, hören und „fühlen", sprich: spüren und messen. Auf dieser Grundlage ist eine Maschine imstande, Muster und Schemata zu erkennen und zu verallgemeinern. Das befähigt sie, eine neue Situation einzuschätzen, aus Erfahrungen zu lernen und auf dieser Grundlage autonom zu entscheiden und zu handeln. Ohne dass sie dafür speziell programmiert werden muss. Entscheidend ist dafür Maschinelles Lernen (ML). Dabei werden laut SAP „Algorithmen darauf trainiert, Muster und Korrelationen in großen Datensätzen zu finden und auf Basis dieser Analyse die besten Entscheidungen und Vorhersagen zu treffen". Kurzum: Die lernende Maschine entwickelt sich selbstständig weiter. Dank neuronaler Netze, die dem menschlichen Gehirn nachempfunden sind. Das ist zumindest die noch ferne Vision von Forschenden, die aber nach Eigenaussagen diesem Endziel jeden Tag ein Stückchen näherkommen.

Wir merken: KI ist aber nicht unbedingt KI. Wir haben es heute weitestgehend mit einer teilautonomen Künstlichen Intelligenz zu tun. In dieser hat der Mensch seinen festen Platz. Die etwas irritierende Bezeichnung dafür ist „schwache KI". Damit werden Anwendungen bezeichnet, die den Menschen in Einzelbereichen unterstützen, ihm praktisch dienen. Menschen werden dadurch genau so wenig überflüssig wie Mathematiker, nur weil es Rechenmaschinen und Supercomputer gibt.

„Starke KI" steht für Systeme, die selbstständig auch komplexe Aufgaben meistern können, ohne dass zwingend ein Mensch dabei sein muss. Sie sind somit in der Lage, den Menschen zu ersetzen und/oder die Manpower insgesamt erheblich, bis in die Nähe der Nulllinie, zu reduzieren.

Eine nicht zu verkennende Problematik liegt darin, dass eine KI-Anwendung zwar ähnlich wie ein Mensch nach den Gesetzen der Logik handelt, aber dies quasi auf mathematischen Wegen. Das

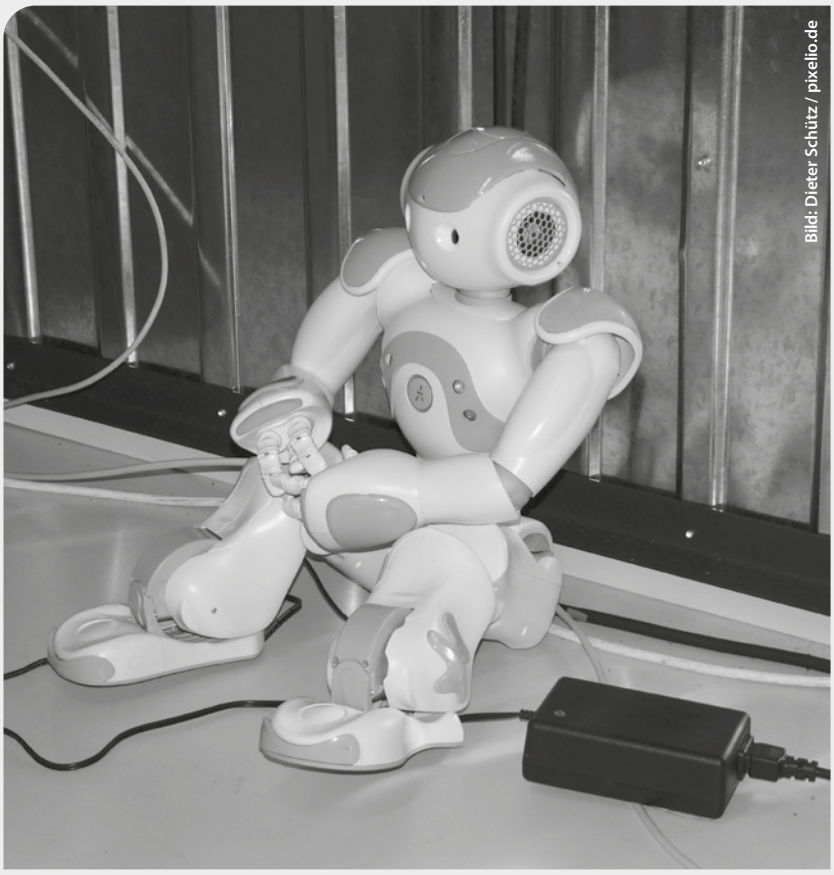

Bild: Dieter Schütz / pixelio.de

Ein müder Roboter? Das gibt es in der Hightech-Welt nicht. Es sei denn, der Akku ist leer.

„Hier ist ein Mensch und keine Maschine." Diese Botschaft hat ihren Hintergrund in ChatGPT, einem KI-gesteuerten Programm, das menschliche Sprache versteht und individuell darauf antworten kann. ChatGPT ist schon bei vielen Unternehmen im Einsatz.

Bild: Stefan Bayer / pixelio.de

heißt zum einen, dass dem Output eines Roboters nach gegenwärtigem Stand der Technik nichts von dem zugrunde liegt, was wir als Menschlichkeit betrachten. Wenn eine Maschine entscheidet, kann dies durchaus zu einer Diskriminierung führen. Und natürlich fehlerhaft sein, denn auch ein Roboter kann Daten fehlinterpretieren. Und die „kalten" Entscheidungen einer Maschine sind für Menschen nicht unbedingt nachvollziehbar. Was ihnen fehlt und wahrscheinlich auch nicht nachgerüstet werden kann, sind Gefühle, die immer in menschliche Entscheidungen einfließen – und das keineswegs nur zum Schlechten. Fatal für den menschlichen Teil eines Maschine-Mitarbeiter-Teams: Wie sich die Maschine entscheidet, ist nicht voraussehbar, da ihre Denkmuster sich von denen menschlicher Wesen diametral unterscheiden.

Menschen könnten in verzwickte Situationen kommen, wenn sie den Entscheidungen einer Maschine folgen. Die Frage stellt sich: Ist es letzten Endes beweisbar, wie sich der Roboter entschieden hat, zum Beispiel bei Zerstörung? Im Ergebnis haftet immer der Mensch, denn einen Gegenstand, auch wenn er smart ist und menschenähnlich denkt, kann niemand zur Rechenschaft ziehen. Folgt ein Mensch also der Maschine und haftet dafür eventuell höchstpersönlich oder trifft er eine eigene Entscheidung? KI kann Probleme lösen, aber auch Probleme generieren.

Ein weiterer negativer Aspekt ist das Faktum, dass Maschinen den Menschen verdrängen könnten. Und der Mensch letzten Endes als fühlendes, aber fehlbares Wesen in die zweite, wenn nicht dritte Reihe rückt. Das ist wohl das Hauptproblem, das diverse Skeptiker auf den Plan ruft.

Bild: www.helenesouza.com / pixelio.de

Ein Mensch am Lenkrad. Ein Bild mit Nostalgiecharakter, denn künftig sollen Kraftfahrzeuge dank KI autonom fahren. Der Mensch: nur noch ein Zuschauer. Dieser Ansatz wird am häufigsten mit der KI in Zusammenhang gebracht.

Doch nun zu der Frage, die noch spannender ist als die allgemeine Darstellung des KI-Prinzips. Nämlich: Welche Anwendungen gibt es in der Sicherheitsbranche bereits?

Hier sind in erster Linie smarte Roboter zu nennen, die sich als „unerschrockene Helfer im Wachschutz und in der Gebäudeinspektion" erweisen. Solche Systeme, in den USA konstruiert, aber in Deutschland auf Kundenbedürfnisse hin programmiert, bieten unter anderem hiesige Technologieunternehmen an. „Die neuen Mitarbeiter im Sicherheitsdienst sind dabei zuverlässig, belastbar, stets fokussiert und rundum vernetzt", wird nach Eigenangaben auf die Vorteile einer robotergestützten Lösung verwiesen. Nimmermüde und nie abgelenkt – die Wachkraft der Zukunft?

Stößt der „Robot-Dog" auf eine unbekannte Person auf dem Gelände oder eine andere Auffälligkeit (beispielsweise Tür/Fenster offen), sendet er Livebilder an die Leitstelle. Dabei folgt er keinem starren Programm, sondern nutzt dynamische Algorithmen, um aus jeder neuen Situation eigenständig zu lernen. Gibt die Leitstelle bei einem bestimmten Objekt Entwarnung, weil es sich beispielsweise um eine neue oder zusätzliche Maschine in der Produktionsstraße handelt, so erkennt der Roboter fortan dieses Objekt und schlägt nicht mehr Alarm, macht eines der Technologieunternehmen deutlich.

KI ist die „Seele" dieser vierbeinigen und laut Hersteller geländegängigen Laufroboter, die Hunden ähneln. Ganz wie die echten Vierbeiner können sie vor-, rück- und seitwärts gehen und Treppen steigen. Ausgestattet sind sie mit einer hochauflösenden 360-Grad-Rundumkamera, ultrahellem LED-Licht und einem Lichterkennungssystem (LiDAR), „das auf die Reflexion von elektromagnetischen Wellen setzt, um den Raum vor ihnen zu vermessen und abzubilden". So könne der Roboter „Menschen und Objekte erkennen und zuordnen, Veränderungen in der Umgebung wahrnehmen und auch Instrumente präzise ablesen", beschreibt einer der Anbieter die Leistungsmerkmale.

Ähnlich, nur ohne vierbeinige Robot-Wächter, funktionieren smarte Videoüberwachungssysteme. Sie können KI-basiert verdächtige Verhaltensmuster erkennen. Dadurch, dass beispielsweise Kleintiere von Eindringlingen und berechtigt abgestellte Gegenstände von fragwürdigen unterscheiden können, reduzieren sie Fehlalarme.

In der akuten Phase der COVID-19-Pandemie wurde verschiedentlich eine Screening-Plattform auf Basis einer industrietauglichen Infrarotkamera eingesetzt. Dieses System schaffte es, vollautomatisch und berührungslos die Körpertemperatur von Personen als Indikator einer COVID-Infektion

zu messen und zusammen mit weiteren Analysen mittels KI auszuwerten. Bei Mitarbeitenden, deren Daten bereits hinterlegt waren, dauerte das 20 Sekunden, bei Erstbesuchern eine Minute. Die Screening-Plattform hatte sich in Industriebetrieben, Krankenhäusern, Altenheimen und bei Veranstaltungen/Meetings bewährt. Nicht zuletzt wegen der kurzen Reaktionszeiten.

KI ist bereits heute integraler Bestandteil von Zutrittskontrollsystemen, die auf Fingerprints oder Personenerkennung basieren. Der bekannte Vorteil solcher Systeme: Fingerabdrücke und Gesichtszüge können weder verloren noch gefälscht werden. Auf diesem Gebiet kommt eine sich fortentwickelnde KI der wünschenswerten Perfektionierung eines Zutrittskontrollmanagements entgegen, das auf biometrischen Merkmalen basiert.

Die immer mehr zur Digitalisierung neigende Gebäudesicherheit kann relativ leicht um Wachschutzkomponenten erweitert werden. Das sind KI-basierte Systeme, die beispielsweise abweichende Temperaturen in Räumlichkeiten detektieren können. Die Messgenauigkeit ist so hoch, dass bereits ein Mensch, der sich außerhalb der Arbeitszeit in einem Büro bewegt, aufgrund seiner Wärmeabstrahlung erkannt wird.

Auch bei der Abwehr von IT-Bedrohungen kann KI überaus hilfreich sein. Konventionelle Virenscanner und Firewalls reagieren mehr oder minder zeitversetzt auf bereits aktive Schadprogramme. KI kann dagegen aufgrund bestimmter Muster, die den meisten Viren/Trojanern zu eigen sind, die Schädlinge identifizieren und abblocken. Diese vordergründig tolle Option hat jedoch einen gefährlichen Haken. KI kann auch, und vielleicht noch optimaler, für IT-Angriffe genutzt werden. So können zum Beispiel automatisiert Schwachstellen erkannt werden. Solche Programme sind nach zuverlässigen Angaben in kriminellen Kreisen bereits im Einsatz. Geld spielt dabei keine Rolle. Wir alle wissen, die Finanzkraft von Cybercrime-Strukturen lässt sich durchaus mit der von Konzernen vergleichen. Auf dem Gebiet der IT-Sicherheit ist KI somit Segen und Fluch zugleich.

Segen und Fluch – das zieht sich durch sämtliche denkbaren KI-Anwendungen im Sicherheitswesen. Ein Segen kann KI im Zeichen des Fachkräftemangels und der Personalnot sein. Ein Fluch ist sie dort, wo sie dazu dient, Menschen „wegzurationalisieren", respektive allzu viele Fragen offenlässt oder nicht nur der Sicherheit dient, weil sie auch Angreifern Mittel an die Hand gibt.

KI muss wohldosiert ein- und umgesetzt werden. Die Verlockungen der Technik hin und her. Der Mensch muss das Maß aller Dinge bleiben. An ihm muss sich alles orientieren. Das ist eine unabdingbare Voraussetzung für eine allseits kompatible und akzeptierbare KI.

Analysen und Hilfestellungen zum Wirtschaftsschutz

Von Rechtsanwalt Dr. Berthold Stoppelkamp

Verfassungsschutzbericht 2022

Im letzten Jahr gab es mehr politisch motivierte Straftaten. Die Anzahl linker Straftaten sank, rechts stieg sie an. Ebenso war ein Anstieg von Ermittlungsverfahren bei Spionagefällen zu verzeichnen. Diese richten sich gegen mutmaßliche Zuträger russischer, türkischer und marokkanischer Dienste. Die größte Bedrohung in Bezug auf Wirtschafts- und Wissenschaftsspionage bleibt aber China.

www.verfassungsschutz.de

eco-Umfrage zu fünf Jahren Datenschutz-Grundverordnung

78,4 Prozent der 2.500 Befragten nennen mindestens eine aktive Maßnahme zum Datenschutz. 49,7 Prozent schränken auf dem Smartphone die Berechtigungen von Apps ein. 40,2 Prozent konfigurieren ihren Internetbrowser, um ihre Daten zu schützen, und 35,2 Prozent nutzen soziale Medien bewusst mit Blick auf ihre persönlichen Daten.

www.eco.de

DsiN-Sicherheitsindex 2023

Der diesjährige DsiN-Sicherheitsindex zur Sicherheitslage von Verbrauchern im Netz fällt mit 57,2 Punkten auf den tiefsten Wert seit seiner ersten Erhebung vor zehn Jahren. Maßgeblich dafür ist der starke Anstieg von IT-Sicherheitsvorfällen um 11,2 Indexpunkte (+20 Prozent). Rund 56 Prozent der Menschen im Netz benötigen zusätzliche Hilfestellungen.

www.sicher-im-netz.de

TÜV Cybersecurity Studie 2023

Befragt wurden allein Verantwortliche für IT-Sicherheit bei 501 Unternehmen ab zehn Mitarbeitern in Deutschland. Elf Prozent der Unternehmen waren im vergangenen Jahr von einem IT- Sicherheitsvorfall betroffen. 57 Prozent fühlen sich von organisierten Hacker-Banden bedroht. Jeweils 27 Prozent sehen staatlich organisierte Wirtschaftsspionage oder politisch motivierte Akteure als große Gefahr.

www.tuev-verband.de

RA Dr. Berthold Stoppelkamp

zuständiges Geschäftsführungsmitglied für den BDSW-Arbeitskreis Wirtschaftsschutz