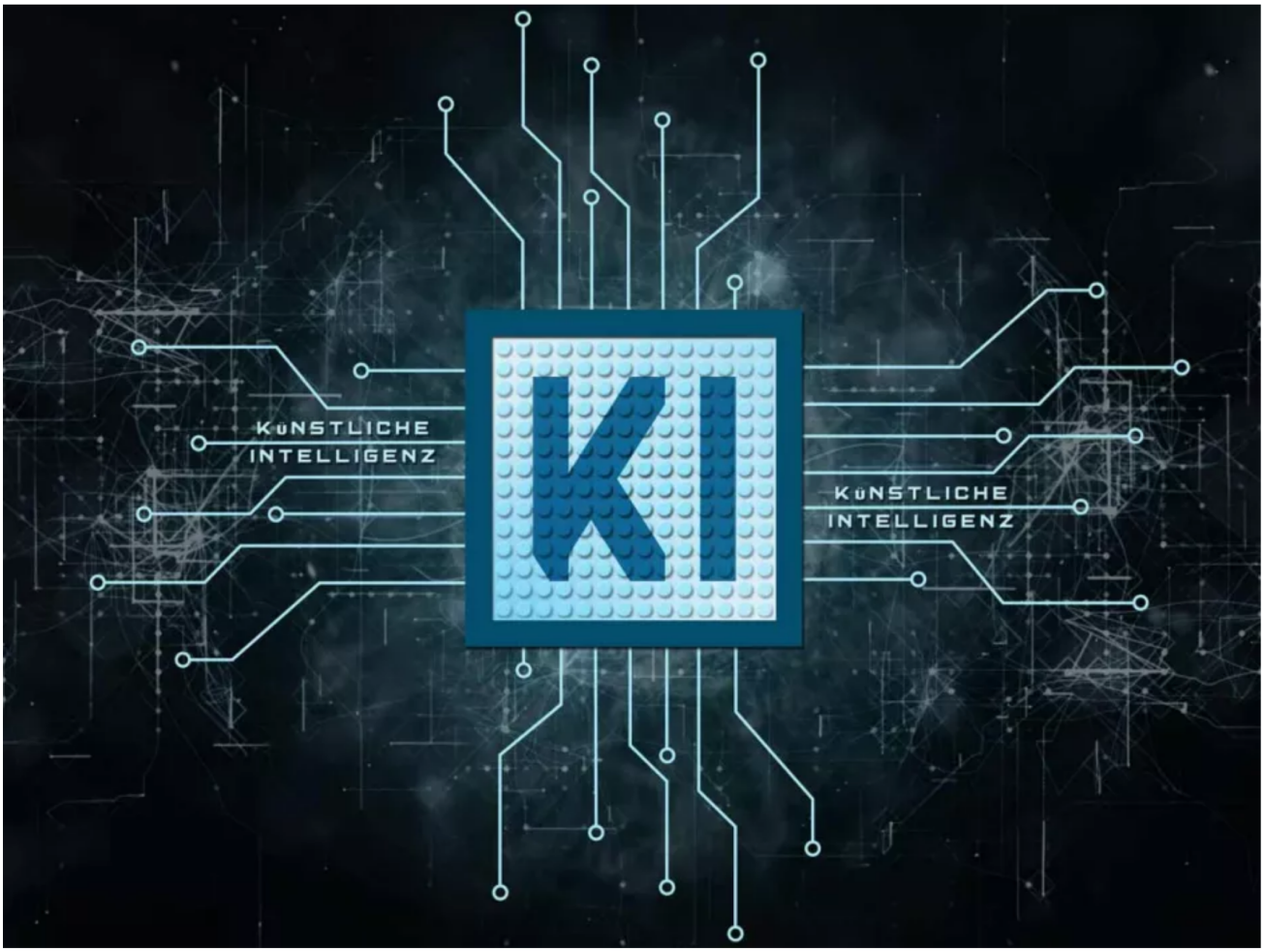
Wirtschaft

18. Apr. 2023 | 07:52 Uhr | von Siegfried Müller

Kolumne

KI und IT-Sicherheit: Passt das zusammen?

Künstliche Intelligenz birgt beim Thema IT-Sicherheit Chancen, aber auch Risiken, erklärt unser Kolumnist Siegfried Müller. Welche das sind, lesen Sie hier.



Es ist notwendig, sich mit den Chancen und Risiken bezüglich des Einsatzes von KI auseinandersetzen. (Bild: sabida - stock.adobe.com)

ChatGTP zu ignorieren war, jedenfalls für mein Empfinden, in den vergangenen Wochen so gut wie unmöglich. Ging es Ihnen auch so? Sowohl in den einschlägigen Social-Media-Kanälen als auch in nahezu jedem Medium – egal ob Fach- oder Publikumspresse – wurde ChatGPT nicht nur rauf und runter seziert, sondern ebenso aufs intensivste diskutiert.

Besonders bemerkenswert war meines Erachtens dabei, dass keinesfalls nur in Deutschland die Meinung diesbezüglich nicht unisono positiv ist, sondern auch in den USA oder anderen nicht-europäischen Ländern darüber kontrovers debattiert wird. Unabhängig von dem Ausgang dieses Dissens im Speziellen sehe ich auf jeden Fall etwas positiv daran: durch ChatGPT ist KI in den Fokus einer breiteren Öffentlichkeit gerückt und so eine tiefergehende Diskussion über Chancen und Risiken initiiert wurde. Auch wenn daraus nicht ad hoc Ergebnisse resultieren können – denn es hat sich ja bereits verschiedentlich gezeigt, dass Technologie und deren (sinnvolle) Nutzung respektive Auswirkungen oder Einfluss auf die Gesellschaft immer unter den verschiedensten Perspektiven über einen längeren Zeitraum betrachtet werden muss.

Dafür gibt es einige Beispiele – bezüglich der KI auch manchmal banalere, etwa jenes, dass mittels Algorithmen zuverlässig Hits hervorgebracht werden könnten: vor einigen Monaten hieß es noch, mittels KI ließen sich neue Musiktitel exakt so erzeugen, dass sie präzise dem Geschmack der breiten Masse entsprächen - einfach, weil diese aus erfolgreichen Kompositionen neu zusammengesetzt würden.

Jetzt haben Forscher der University of York herausgefunden, dass Computer-generierte Stücke mit musikalischen Werken, die von Menschen komponiert worden sind, qualitativ nicht mithalten können. Denn – so die Analyseergebnisse der Wissenschaftler (verkürzt auf den Punkt gebracht) – Musikstücke, die von Menschen komponiert worden sind, werden signifikant höher bewertet und sind stilistisch betrachtet erfolgreicher.

Aus KI-Lösungen ergeben sich auch Angriffsmöglichkeiten

Ganz abgesehen davon, dass es hierbei sowieso noch die Problematik im Hinblick auf Verstöße gegen geltendes Urheberrecht umfassend zu klären gilt – und zwar unter den verschiedensten Aspekten. Denn eine unerlaubte Handlung in diesem Sinne lässt sich zum Beispiel schon allein aufgrund von Fehlern in den Algorithmen – was bereits bei der Auswahl der Trainingsdaten zum Tragen kommen kann – potenziell nicht ausschließen.

Wenn wir schon einmal auf die Schwächen der KI zu sprechen kommen, dann dürfen an dieser Stelle natürlich nicht die IT-/Cyber-Sicherheitsaspekte fehlen. Zum einen bezogen auf die Angreifbarkeit der KI-Modelle und zum anderen mit Sicht auf die Angriffsmöglichkeiten, die sich aus einer KI-Lösung ergeben. Aber – das sollte in diesem Kontext keinesfalls unerwähnt bleiben – der Einsatz von KI-Technologien dient ebenso zum Schutz gegen kriminelle Angreifer. Doch first things first.

Neue Sicherheitsprobleme durch KI

(IT-)Sicherheit spielt bereits bei der Entwicklung von KI-Lösungen eine Rolle. Wie die meisten IT-Systeme weisen auch KI-Modelle konzeptionelle Schwachstellen auf. Diese können von kriminellen Akteuren dahingehend genutzt werden KI-Modelle zu manipulieren, um die Ergebnisse gemäß ihren Vorstellungen zu beeinflussen.

Dafür bieten sich verschiedene Optionen an: So ist es beispielsweise möglich, durch Veränderung der Trainingsdaten Einfluss auf den Entscheidungsprozess eines KI-Modells zu nehmen – also auf diesem Wege intendierte Fehlentscheidungen zu evozieren. Zudem kann durch Veränderung einer Eingabe die Position im Eigenschaftsraum verschoben werden, sodass diese individuell falsch klassifiziert wird. Des Weiteren ist es möglich, bei der Interaktion mit einem KI-Modell Eingabe-Ausgabe-Paare zu sammeln, um dadurch sowohl Aufschluss über die Funktionsweise als auch die verwendeten Trainingsdaten zu erhalten.

Primär muss jedoch ganz klar das Augenmerk darauf gerichtet werden, dass die KI an sich dem Arsenal der Angreifer mehr als zuträglich ist. Denn mithilfe des Fachwissens der in diesem Bereich mittlerweile sehr versierten Experten lassen sich Standard-Attacken mit Ransomware durch Automatisierung noch weiter optimieren. Damit einher geht unter anderem, dass sich Erpressungssoftware zügig und gleichzeitig effizienter dahingehend modifizieren lässt, um die Abwehrmechanismen der Unternehmen auszuhebeln.

Mit anderen Worten – es dauert nicht mehr Tage oder Wochen, sondern nur noch Minuten bis angepasste Varianten von Schadcodes verfügbar sind und ein neuer Angriffsversuch gestartet werden kann.

Auch Phishing-Attacken lassen sich unter Einsatz von KI effektiver umsetzen – ChatGPT garantiert diesbezüglich extrem gut geschriebene E-Mails und die technologischen Möglichkeiten rund um Deep Fakes eignen sich ausgezeichnet für Spear Phishing-Attacken, die vorrangig zum Ziel haben hohe Geldbeträge oder Daten zu erbeuten.

Übrigens ist letzteres eine Möglichkeit von Cyberbetrug, der leider seitens vieler Unternehmen (noch) nicht ernst genug genommen wird – wie eine von YouGov durchgeführte Studie zeigt: Knapp die Hälfte der Befragten (45 Prozent) gab an zu wissen, was ein Deep Fake ist, aber nur sieben Prozent erkannten darin eine Gefahr für das eigene Unternehmen. Meines Erachtens zeigt sich daran, dass das Bewusstsein für die potenzielle Bedrohung resultierend aus KI insgesamt geschärft werden muss.

Neue Sicherheitslösungen mit KI

Doch selbstverständlich ist es keinesfalls statthaft bei der Betrachtung von KI im Kontext der Cyber-Sicherheit nur über die negativen Seiten zu sprechen. Ganz im Gegenteil. Denn die Technologie wird nicht nur dabei helfen, Cyber-Sicherheit auf ein neues Niveau zu heben, sondern im Weiteren dringend notwendig sein als Unterstützung beziehungsweise Entlastung der (viel zu wenigen) Cyber-Sicherheitsexperten.

Bereits heute sind die Einsatzmöglichkeiten subsidiär: Mithilfe von KI lässt sich zum Beispiel eine Erhöhung der Erkennungsrate von Angriffen erreichen – durch die Auswertung von Daten, die mit modernen Sensoren in den Netzwerken sowie in den Endgeräten erhoben werden, ist es möglich Bedrohungen und Angriffe besser zu identifizieren. Zukünftig kann KI zudem bei der Priorisierung von kritischen Ereignissen unterstützen. Die Idee hier ist, dass aus den vielen sicherheitsrelevanten Ereignissen, die von einem SIEM oder anderen Systemen generiert werden, jene zu priorisieren, die für das Unternehmen aktuell die höchste Priorität haben. Entsprechend entlastet dies die Cyber-Sicherheitsexperten, da es ihnen möglich ist sich auf bestimmte Vorfälle vorrangig zu konzentrieren, statt sich mit allen parallel beschäftigen zu müssen.

Doch nicht nur beim Erkennen und Auswerten von Angriffen ist die KI zunehmend dienlich – im Bereich der (Teil)Autonomie zur Abwehr von Angriffen wird die Technologie helfen, sehr schnell reagieren und damit eine Erhöhung der Resilienz erreichen zu können.

Natürlich ist meine Aufzählung hier nicht vollständig – es gibt bei weitem mehr Segmente, in denen KI sehr gute Dienste für mehr IT-Sicherheit leistet: zum Beispiel bei der Erkennung von Malware, Spam, Fake News und Deep Fake aber auch im Rahmen von sicherer Softwareentwicklung, IT-Forensik oder Threat Intelligence.

Fazit:

Meines Erachtens führt kein Weg daran vorbei – es ist notwendig, sich mit den Chancen und Risiken bezüglich des Einsatzes von KI auseinandersetzen. Vielleicht fragen Sie sich jetzt, ob dies auch bereits im Kontext des Produktionsbereichs relevant sein könnte? Diese Frage kann ich mit einem „Ja, zunehmend mehr“ beantworten und es gibt auch hier bereits interessante Lösungen, zum Beispiel die nachfolgende Anwendung zur Angriffserkennung:

Mittels Machine Learning wird der bestätigte Normalzustand der Produktionsanlagen erfasst. So ist es möglich Anomalien, die von Angriffen ausgelöst werden, gemäß allgemeingültiger Standards basierend auf Empfehlungen von etablierten Institutionen – wie etwa dem BSI – zu erkennen. Zusammengefasst beruht die Methode auf der Identifikation von Änderungen im Kommunikationsmuster der Anlage als Folge eines Angriffs. Da jede Kommunikation, die sich außerhalb des erlernten Datenverkehrsprofils bewegt, als Anomalie bewertet wird und folglich einen Alarm auslöst, ist es darüber möglich, auch neue und unbekannte Angriffe zu erkennen.

Ich halte diesen Ansatz nicht nur für sehr überzeugend, sondern auch dringend notwendig, da die Zahl der Angriffe weiter steigen wird. Nicht zuletzt aufgrund der Möglichkeiten der KI.

Das ist unser Kolumnist Siegfried Müller

(Bild: MB Connect Line)

Siegfried Müller ist Vice-President Advanced Technologies bei der MB Connect Line GmbH Fernwartungssysteme.
In seinen ersten Berufsjahren als Steuerungstechniker für den Maschinenbau hat er den Nutzen von Fernwartung erkannt. Im Alter von 25 Jahren gründete er MB Connect Line. Unter seiner Leitung entwickelte sich das Unternehmen zum Technologieführer in den Bereichen Fernwartung, Datenerfassung und Industrial Security. Heute ist die MB Connect Line der europäische Standort der Red Lion Inc. in der Industrial Division der Spectris PLC Gruppe.