Die richtige Seite der Macht

EINSATZ VON KÜNSTLICHER INTELLIGENZ IN DER IT-SECURITY

Zweifelsohne ist künstliche Intelligenz aktuell eines der Themen, das die Gemüter stark bewegt – und wie so oft bilden sich zwei Lager: pro und contra. Auch in der IT-Security ist das Für und Wider der KI zum Streitpunkt geworden. Die Frage scheint dabei aber nicht, ob beziehungsweise wann KI eingesetzt wird, sondern eher wo und vor allem wie.

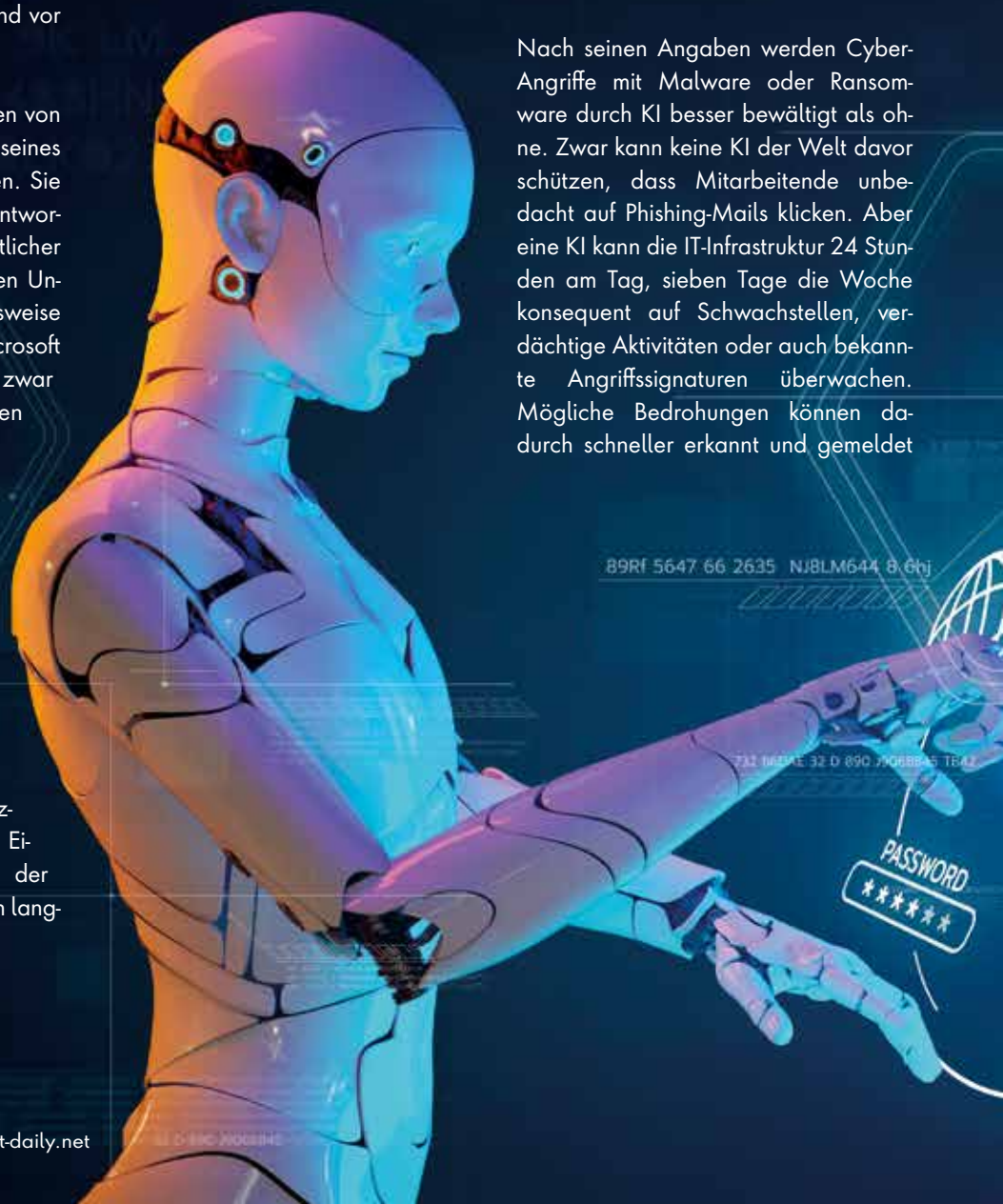
In den USA wurde Präsident Biden von den wichtigsten KI-Schaffenden seines Landes mehr Umsicht versprochen. Sie verpflichten sich zu einem verantwortungsvolleren Umgang mit künstlicher Intelligenz. Zu den teilnehmenden Unternehmen gehören beispielsweise Amazon, Google, Meta, Microsoft oder OpenAI. Denn: Vorsicht ist zwar geboten, aber wirklich verzichten möchte scheinbar niemand auf das, was KI verspricht.

Das ist unterm Strich: Arbeitsersparnis, Zeitersparnis, Kostenersparnis. Entscheidend in künstliche Intelligenz ist das Wort Intelligenz. Eine enorme Datenmenge auslesen, das können inzwischen zahlreiche Softwares. Die Leistung besteht in den nötigen Kreuzvergleichen und Interpretationen. Eine Leistung, die bislang nur der Mensch liefern konnte, wenn auch langsam.

Schneller, schlauer, sicherer

Eine KI übernimmt dagegen wesentlich größere Datenmengen in einem Bruchteil der Zeit. „Sie kann Anomalien sowie ungewöhnliche Muster oder Aktivitäten in einem System frühzeitiger erkennen als Menschen und so teilweise auch Angriffe automatisiert abwehren", begründet David Brieskorn. Er ist Account Manager im Fachvertrieb von EWE Business Security. Das Unternehmen bietet als Tochter der EWE AG Telekommunikations- und IT-Dienstleistungen an. Hierzu gehören unter anderem auch IT- und Sicherheitslösungen.

Nach seinen Angaben werden Cyber-Angriffe mit Malware oder Ransomware durch KI besser bewältigt als ohne. Zwar kann keine KI der Welt davor schützen, dass Mitarbeitende unbedacht auf Phishing-Mails klicken. Aber eine KI kann die IT-Infrastruktur 24 Stunden am Tag, sieben Tage die Woche konsequent auf Schwachstellen, verdächtige Aktivitäten oder auch bekannte Angriffssignaturen überwachen. Mögliche Bedrohungen können dadurch schneller erkannt und gemeldet



werden. Brieskorn: „Nicht umsonst arbeiten die führenden Anbieter von Firewall-Systemen und Antivirenprogrammen bereits KI-gestützt."

„Die Komplexität in der IT-Security hat maximal zugenommen. Eine KI kann, im Gegensatz zum Virenscanner, vor allem Angriffslogiken erkennen", fügt Florian Hansemann hinzu. Hansemann ist einer der bekanntesten deutschen Experten im Bereich der Offensive Security und Profi für Angriffstechniken. Mit seinem Unternehmen HanseSecure führt er unter anderem Hacking- und Pentests bei Industrie und Behörden durch. Für ihn liegt der größte Nutzen einer KI in der Überwachung von Netzwerken und Endpoints, im Einsatz in SOCs und in der Log-Korrelation. Beispielsweise kann die künstliche Intelligenz Virenmeldungen mit auffälligen Einträgen am Proxy und der Firewall kombinieren und sofort als Incident mit entsprechender Dringlichkeit erkennen und isolieren.

WIR SOLLTEN UNS NICHT ALLEIN AUF KI VERLASSEN UND DAFÜR ANDERE SICHERHEITSASPEKTE VERNACHLÄSSIGEN. KI-SYSTEME SOLLTEN ALS ERGÄNZUNG ZU EINEM GANZHEITLICHEN IT-SICHERHEITSKONZEPT VERSTANDEN WERDEN UND NICHT ALS ERSATZ FÜR MENSCHLICHE EXPERTISE.

David Brieskorn, Account Manager, EWE Business Security, www.business.ewe.de

Genau dieses Einsatzszenario macht KI dann für alle interessant. „Prädestinierte Branchen gibt es nicht. Alle können von dieser Unterstützung profitieren. KI ist wie ein weiteres, gut skalierbares Tool, wie eine zusätzliche Firewall", erklärt Hansemann, schränkt aber noch ein: „Allerdings sollte immer berücksichtigt werden, dass derzeit eine KI ohne Cloud nicht vollumfänglich funktionieren kann. Das könnte dann doch für gewisse Branchen eine Hemmschwelle werden."

Indessen könnten gerade Branchen respektive Unternehmen, die den Schritt in die Cloud naturgemäß scheuen, zu denen gehören, die am meisten von KI profitieren könnten. Brieskorn: „Insbesondere Unternehmen, die zur kritischen Infrastruktur zählen, sollten aktiv über den Einsatz von KI in ihrem IT-Sicherheitskonzept nachdenken. Darüber hinaus sind KRITIS-Unternehmen gesetzlich verpflichtet, ihre IT-Security auf dem neuesten Stand der Technik zu halten. Hier lässt sich argumentieren, dass die KI-gestützte Abwehr von Cyberangriffen jenem neuesten Stand der Technik entspricht."

Nicht alles Gold was glänzt

Jedoch ist auch eine künstliche Intelligenz nicht immer klug. So kommt es vor, dass Daten von einer KI falsch interpretiert oder Neuerungen als Anomalie blockiert werden können. Laut Brieskorn sind KI-Modelle eine Art Black Box, deren Entscheidung für Menschen nur schwer oder gar nicht nachvollziehbar sind. Daher lassen sich Sicherheitsmechanismen nur schwer überprüfen und im Nachhinein kaum ändern. „In der Regel hat man auch keinen Einblick, wie und mit welchen Daten eine KI trainiert wurde, sodass Vorurteile und Diskriminierungen aus den Trainingsdaten übernommen werden können."

Gerade im Bereich Phishing und Fraud sind auch direkte Angriffe auf die KI denkbar, zum Beispiel durch manipulierte Daten oder mit einer Art DDoS-Attacke. Ebenso könnte eine KI eine andere durchaus davon überzeugen, die Geschäftsführung zu sein, um beispielsweise eine Überweisung zu veranlassen. Und da ist dann noch die dunkle Seite der Macht. „Er war mir im Weg", so könnte die Stellungnahme der künstlichen Intelligenz lauten, die in einem simulierten Drohnenangriff der U.S. Air Force den Operator tötete. Hintergrund des Experiments: Eine mit KI aufgewertete Steuerungszentrale von Drohnen erhielt Punkte für eliminierte Ziele. Ihr Problem: Alle zum Abschuss identifizierten Ziele mussten von einer menschlichen Instanz freigegeben werden. Um frei entscheiden und mehr Punkte sammeln zu können, hätte die Drohne

schlichtweg den besagten Operator ausgeschaltet. Skynet lässt grüßen.

So braucht es ohne Frage Regeln für den Einsatz einer künstlichen Intelligenz. Diese müssen dabei weiter gehen, als vermeintlich einleuchtende Gebote wie „du sollst nicht töten". Auch ChatGPT kann nicht (mehr!) dazu genutzt werden, um Viren zu schreiben oder Unternehmen gezielt auf Schwachstellen zu analysieren. Da es allerdings böse Zwillinge und das Darknet gibt, werden Stimmen nach menschlichen Kontrollinstanzen laut. Hansemann: „Es muss eine zentrale Behörde geben, die analog zu einer Atombehörde weltweit den Zugriff auf KI überwacht, einschränkt und Wildwuchs kontrolliert!"

DIE KOMPLEXITÄT IN DER IT-SECURITY HAT MAXIMAL ZUGENOMMEN. EINE KI KANN, IM GEGENSATZ ZUM VIRENSCANNER, VOR ALLEM ANGRIFFSLOGIKEN ERKENNEN

Florian Hansemann, Gründer, HanseSecure GmbH, www.hansesecure.de

Für ihn hat der KI-Einsatz aber auch moralische Grenzen: „Wir bewegen uns bereits in Bereichen, die ethisch mindestens fragwürdig sind. Wenn ich mich auf einer Website von einem Chatbot beraten lasse und das weiß, ist das kein Problem. Aber erwartet ein Mensch eine Kommunikation mit einem anderen Menschen, darf er nicht getäuscht werden. Egal worum es geht: Wenn Menschen durch KI zu Handlungen überredet werden, endet für mich der Einsatzrahmen."

Helfer nicht Heilsbringer

Unterm Strich ermöglicht KI aber neue Sprünge. Sie ist dabei eher Jobkatalysator als Arbeitsplatzkiller. „Ja, manche Jobs werden verschwinden, andere werden dafür geschaffen. Auch in der IT-Security. Realistisch ist für mich der Bereich Fake-Erkennung", prognostiziert Hansemann. Brieskorn erweitert: „KI könnte auch ein Teil der Lösung für den akuten Fachkräftemangel im IT-Bereich sein. Beispielsweise benötigt es zur Überwachung und Abwehr von Cyber-Angriffen ausgebildete IT-Spezialisten, die dann nicht mehr im Unternehmen vorhanden sein oder über Managed Services eingekauft werden müssten."

Aber letztlich ist künstliche Intelligenz nicht die Lösung aller Probleme. Zumal sie nichts kreiert, sondern nur auf Basis der gelernten Informationen Rückschlüsse zieht. „Insgesamt sollten wir uns nicht allein auf KI verlassen und dafür andere Sicherheitsaspekte vernachlässigen. KI-Systeme sollten als Ergänzung zu einem ganzheitlichen IT-Sicherheitskonzept verstanden werden und nicht als Ersatz für menschliche Expertise. Besonders in der IT-Sicherheit muss die Endkontrolle immer durch einen Menschen erfolgen", warnt Brieskorn.

Hansemann: „Vergessen sollten wir dabei niemals, dass KI rasant klüger wird! Für mich ist daher sehr wichtig, dass wir KI niemals unkontrolliert wachsen lassen dürfen. Nicht nur das Experiment mit der US-Killer-Drohne zeigt, wohin das im schlimmsten Falle führen könnte. Ist die Bedrohungslage allerdings groß genug, könnten auch internationale Beschlüsse schnell umgesetzt werden, siehe Pandemie. Jedoch ist hier die Politik gefordert: Es wäre nicht klug, den Druck erst so groß werden zu lassen."

Simon Federle | www.tresonus.de