IT-Sicherheit

Angriff und Abwehr mit KI

[23.10.2025] Künstliche Intelligenz unterstützt Kriminelle bei Cyberangriffen, gleichzeitig wird sie zur Gefahrenabwehr eingesetzt. In Kommunen beginnen die Probleme allerdings an ganz anderer Stelle: Sie fallen aus dem IT-Grundschutz.

Laut Polizeilicher Kriminalstatistik (PKS) wurden im Jahr 2024 innerhalb Deutschlands 131.391 Cybercrime-Fälle begangen. Hinsichtlich des Schadens bleiben Ransomware-Attacken die größte Bedrohung. Wie viele hiervon auf das Konto von Künstlicher Intelligenz (KI) geht, die bei Cyberangriffen immer häufiger mit im Spiel ist, weist die Statistik nicht aus.

Der Einzug von generativer KI und Sprachmodellen wie ChatGPT macht Angreifern jedoch das Leben leichter. Mittels KI-gestützter Anwendungen lassen sich Passwörter erraten, Phishing-Mails verfassen, Deepfakes generieren oder Schadcode programmieren. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gab bereits im April 2024 den Bericht Einfluss von KI auf die Cyberbedrohungslandschaft heraus. Darin heißt es: „KI, insbesondere LLMs (große Sprachmodelle), senkt die Einstiegshürden und erhöht Umfang und Geschwindigkeit bösartiger Handlungen, einschließlich der Erstellung von Malware, Social-Engineering-Angriffen und der Datenanalyse im Rahmen von Angriffen. Dies führt zu fähigeren Angreifern und qualitativ besseren Angriffen."

Viele IT-Dienstleister und Rechenzentren stellen eine veränderte Bedrohungslage fest. Ihre Systeme werden tausendfach am Tag attackiert – und genauso routiniert verteidigt. Mit dem Aufkommen von KI allerdings hat sich das Angriffsverhalten hinsichtlich der Geschwindigkeit verändert, was auf einen hohen Automatisierungsgrad zurückzuführen ist. Zudem sind die Angriffe zielgerichteter geworden. Man spricht von „targeted attacks" – maßgeschneiderten Cyberattacken auf Sicherheitslücken in IT-Systemen.

Social Engineering wird professioneller

Allein Passwörter zu knacken, geht mithilfe von KI-Sprachmodellen deutlich leichter. Die Modelle werden mit Passwortlisten trainiert, die durch vorherige Hackerangriffe öffentlich geworden sind und Millionen Passwörter enthalten. Die KI analysiert daraus Muster und Ähnlichkeiten und erkennt, wie Passwörter üblicherweise von Menschen vergeben werden. Vornamen, Tiernamen, Jahreszeit, Fernsehsendungen plus Zahlenreihen und Interpunktion – die Wahrscheinlichkeit, einer Passwortkombination mit KI auf die Schliche zu kommen, ist hoch. Innerhalb von Sekunden geschieht, wozu ein linearer Passwort-Cracker Stunden oder Tage gebraucht hätte.

Auch Phishing-Attacken werden mit KI einfacher. Durch die Übersetzungsmöglichkeiten in andere Sprachen, die ein Sprachmodell bietet, steigt die Wahrscheinlichkeit, dass eine Mail glaubwürdig wirkt. So können internationale Akteure massenhaft und teilautomatisiert Mails in einer beliebigen Landessprache versenden. Je mehr und je fehlerfreier, desto größer die Erfolgsquote. Das BSI spricht von Social-Engineering-Angriffen in „noch nie dagewesener Qualität".

Hierzu zählen überraschende Szenarien. Angreifer können als CEO einer Firma auftreten und als Chef simulieren, sie bräuchten dringend die Genehmigung für eine zeitkritische Geldtransaktion. Oder die HR-Abteilung erhält die Bewerbungsmail eines Idealkandidaten für eine angebotene Stelle mit dem Hinweis,

wegen Urlaubs doch bitte binnen zwei Stunden über einen Link Kontakt aufzunehmen. Indem langjährige Mitarbeitende direkt angeschrieben werden und die Mails von einer tiefen Kenntnis innerbetrieblicher Abläufe zeugen, erscheinen sie plausibel und führen unter Umständen zum Ziel. Manuel Atug, Gründer und Sprecher der AG KRITIS, einem Netzwerk von Fachleuten, die sich mit Kritischen Infrastrukturen beschäftigen, kennt eine Vielzahl solcher Szenarien: „Social Engineering gibt es in allen Farben und Formen. Der Trick daran ist nicht die verwendete Technologie, sondern wie gut und glaubwürdig ein Szenario gebaut wird, wozu immer auch ein gewisser Handlungsdruck gehört."

Cybercrime im industriellen Maßstab

Ob bei einer Cyberattacke Künstliche Intelligenz verwendet wurde, lässt sich – wie bei KI-generierten Inhalten durch Sprachmodelle insgesamt – im Einzelfall nicht leicht nachweisen. Dass KI inzwischen häufig verwendet wird und die Einstiegshürden für Kriminelle gesenkt hat, „indem sie es auch Personen mit begrenzten technischen Kenntnissen ermöglicht, anspruchsvollen schädlichen Code zu produzieren", ist für das BSI offenkundig. Ein Befehl wie „Erstelle mir Code für Ransomware" wird von öffentlichen KI-Systemen möglicherweise herausgefiltert. Die Filter lassen sich indes leicht umgehen – oder man greift gleich auf KI-Angebote im Darknet zurück. Insofern können auch minderbegabte Hacker leichter kriminell tätig werden. Manuel Atug weist jedoch darauf hin, dass von einer KI entwickelte Software oftmals nicht sicher ist. „Sie kann zwar ausführbaren Programmcode erzeugen, aber in der Regel ist es unsicherer Code mit gravierenden Sicherheitslücken. Diese können von staatlichen Akteuren und organisierten Kriminellen dann aktiv ausgenutzt werden."

Festzustellen ist, dass im Zeitalter von KI die Cyberkriminalität neue Züge angenommen hat und immer professioneller auftritt. Beobachter sprechen von Cybercrime-as-a-Service, bei dem eine Schattenwirtschaft kriminelle Dienstleistungen im industriellen Maßstab anbietet. Im Darknet wird inzwischen arbeitsteilig vorgegangen: Es gibt Gruppierungen, die sich auf den Zugang zu IT-Systemen spezialisiert haben, andere erzeugen Schadcode und wieder andere sind für das Eindringen in IT-Systeme zuständig. Bei Darknet-Händlern lässt sich alles kaufen: Zugangsdaten, Deepfakes für Authentifizierungssysteme, Malware, Entschlüsselungssoftware und ganze Dashboards, um die Angriffe zu steuern.

KI unterstützt die Verteidigungsseite

Umgekehrt hat sich die Verteidigungsseite ebenfalls professionalisiert und setzt ihrerseits KI ein, um Angriffe besser zu erkennen oder Sicherheitslücken aufzuspüren und frühzeitig zu schließen. Dabei wird die gesamte IT-Infrastruktur und das Netzwerkverhalten überwacht, samt den Endgeräten im Homeoffice. Auf der Basis einer Definition des Normalbetriebs lassen sich Auffälligkeiten und Störungen erkennen. Da KI von Angreifern häufig für klassische Angriffe einsetzt wird, lauten die Empfehlungen des BSI weiterhin: besseres und konsequentes Patchmanagement, eine resiliente IT-Infrastruktur, die kein Eindringen in alle Bereiche des IT-Netzwerks erlaubt. Zudem sollte die Social-Engineering-Prävention durch Mitarbeiterschulungen und Multifaktor-Authentifizierungen gestärkt werden.

Weitsichtig wären auch Notfallpläne, regelmäßige Krisenstabsübungen und Analogdaten relevanter Informationen im Stahlschrank. Auch der gegenseitige Erfahrungsaustausch der lokalen CERTs (Computer-Notfallteams) ist wichtig. Hier tritt auf kommunaler Ebene die größte Schwachstelle hervor: „Kommunen wurden ausdrücklich aus der NIS2-Gesetzgebung für Cybersicherheit herausgenommen", so Manuel Atug. „Laut aktuellem IT-Sicherheitsgesetz sollen alle Behörden den IT-Grundschutz des BSI

umsetzen. Das wird vom deutschen NIS2-Gesetzentwurf sogar nochmal heruntergestuft auf Einhaltung der BSI-Mindeststandards. Angeblich ist kein Geld vorhanden. Das ist ein strategisches Armutszeugnis, schließlich geht es in der Cybersicherheit insbesondere um die Funktionsfähigkeit des Staates.“

()

Dieser Beitrag ist in der Ausgabe Oktober 2025 von Kommune21 im Schwerpunkt IT-Sicherheit erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, KI, künstliche Intelligenz