NACHRICHTEN AG

13. August 2024

Künstliche Intelligenz unter Beschuss: Cybersecurity im Fokus der Black Hat USA

Microsofts AI Copilot kann als automatisierte Phishing-Maschine missbraucht werden. Sicherheitsprobleme betreffen viele Unternehmen weltweit.

Die zunehmende Integration von KI-Technologie in den Unternehmensalltag bringt sowohl Chancen als auch erhebliche Risiken mit sich, insbesondere im Bereich der Cybersicherheit. Bei der letztwöchigen Black Hat USA Konferenz, die als wichtigste Veranstaltung zur Diskussion über aktuelle Cyberbedrohungen gilt, standen diese Themen im Mittelpunkt, während Experten aus aller Welt zusammenkamen, um sich über Strategien zur Abwehr dieser Bedrohungen auszutauschen.

Die Gefahren durch Microsofts Copilot verstehen

Ein besonderer Vortrag von Michael Bargury, Mitbegründer und CTO von Zenity, beleuchtete, wie Microsofts KI-Tool Copilot von Angreifern ausgenutzt werden kann. Dieses Tool, das in Anwendungen wie Word und Teams integriert ist, stellt ein wichtiges Produktivitätsinstrument dar, indem es Nutzern hilft, Informationen zusammenzufassen, E-Mails zu durchsuchen und Texte zu erstellen. Bargurys Demo zeigte, dass Angreifer durch den Zugriff auf die eigene E-Mail das Tool missbrauchen können, um Malware zu verbreiten oder verantwortungsvollen Mitarbeitern schädliche Links zu senden.

Manipulation durch KI: Das Zukunftsbild der Cybersicherheit

Die Techniken, die Bargury vorstellte, verdeutlichen, wie KI nicht nur zur Effizienzsteigerung, sondern auch als Werkzeuge für Cyberkriminalität eingesetzt werden kann. Selbst einfache Tricks wie das Versenden einer betrügerischen E-Mail können dazu führen, dass ein Mitarbeiter aus Versehen Geld auf ein Konto eines Hackers überweist, da das Tool die betrügerische Anfrage als legitime Informationen präsentiert. Diese Vorfälle machen die Verletzlichkeit von Unternehmen durch Manipulation von Technologien wie LLMs (Large Language Models) deutlich.

Die gemeinschaftliche Reaktion der Sicherheitsfachleute

Bargury hat mit seinem Vortrag auf eine dringend notwendige Diskussion hingewiesen. Philim Misner, Leiter für die Erkennung und Reaktion auf KI-Vorfälle bei Microsoft, betonte, dass das Unternehmen diese Schwachstellen ernst nimmt und an deren Behebung arbeitet. Diese Verantwortung bedeutet, dass nicht nur Microsoft, sondern auch andere Unternehmen in der Tech-Branche ähnlich gefährdete Systeme entwickeln, die ebenfalls anfällig für Missbrauch sein können.

Ein breiteres Problem: Die Sicherheitslandschaft im Wandel

Die Herausforderungen im Bereich der Cybersicherheit sind nicht auf Microsoft beschränkt. Mit der steigenden Verbreitung von KI-gestützten Tools in Unternehmen sehen sich Sicherheitsforscher und Führungskräfte mit einer neuen Welle von Bedrohungen konfrontiert, die durch generative KI-Technologien verstärkt wurden. Die Black Hat-Konferenz verdeutlichte, dass solche Technologien die Sicherheitslandschaft eher verschärfen als entschärfen.

Der Blick nach vorn: Sicherheit und Innovation an einem Scheideweg

Es ist entscheidend, dass Unternehmen, die auf KI setzen, auch Maßnahmen ergreifen, um sich gegen potenzielle Bedrohungen zu wappnen. Während Technik immer fortschrittlicher wird, müssen auch Verteidigungsmechanismen entsprechend angepasst werden. Die Cybersicherheit erfordert einen ständigen Dialog und innovative Lösungen, um die Technik sowohl zu schützen als auch zu ermöglichen, dass sie sicher verwendet werden kann.

Abschließend lässt sich sagen, dass mit den rasanten Fortschritten im Bereich der KI auch die Gefahren zunehmen. Unternehmen und ihre Mitarbeiter müssen sich dieser Realität bewusst sein und proaktiv handeln, um ihre sensiblen Daten und Systeme zu schützen.

Details

Besuchen Sie uns auf: n-ag.de