BSI

KI verändert Cyber-Bedrohungen

[03.05.2024] Künstliche Intelligenz ist keine weit entfernte Zukunftsvision mehr. Mit ihren verschiedenen Ansätzen und Lösungen ist die Technologie inzwischen im (IT-)Alltag angekommen – auch bei Kriminellen. Das BSI will herausfinden, wie sich Cyber-Angriffe dadurch verändern.

In einem aktuellen Forschungsbeitrag hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) untersucht, wie sich Künstliche Intelligenz (KI) auf die Cyber-Bedrohungslage auswirkt. Dazu werden zunächst KI-gestützte Anwendungen identifiziert, die schon heute für den offensiven Einsatz zugänglich sind. Anschließend bewertet der Bericht, wie sich diese Bedrohungen in naher Zukunft entwickeln könnten. So senkt generative KI nach Einschätzung des BSI die Einstiegshürden für Cyber-Angriffe und erhöht Umfang, Geschwindigkeit und Schlagkraft schadhafter Handlungen im digitalen Raum. Dies gelte vor allem für die großen Sprachmodelle (Large Language Models – das bekannteste ist ChatGPT). Neben allgemeinen Produktivitätsgewinnen für böswillige Akteure stellt das BSI derzeit eine maligne Nutzung vor allem im Bereich des Social Engineering und bei der Generierung von Schadcode fest.

Automatisierte Cyber-Angriffe sind möglich

KI ermöglicht es Angreifenden mit geringsten Fremdsprachenkenntnissen, qualitativ hochwertige Phishing-Nachrichten zu erstellen: Herkömmliche Methoden zur Erkennung betrügerischer Nachrichten wie die Prüfung auf Rechtschreibfehler und unkonventionellen Sprachgebrauch reichen zur Erkennung von Phishing-Angriffen damit nicht mehr aus. Einen Schritt weiter als die Unterstützung von Cyber-Angriffen, die durch Menschen ausgeführt werden, geht die Erstellung von Malware durch KI: Große Sprachmodelle sind bereits heute in der Lage, einfachen Schadcode zu schreiben. Darüber hinaus existieren erste Proofs of Concept, nach denen KI für die automatische Generierung und Mutation von Malware eingesetzt werden kann. Allerdings sind bösartige KI-Agenten, die vollkommen eigenständig IT-Infrastrukturen kompromittieren können – also Künstliche Intelligenz, die zur vollständigen Angriffsautomatisierung führt –, aktuell nicht verfügbar und werden mit hoher Wahrscheinlichkeit auch in naher Zukunft nicht verfügbar sein. Allerdings ist KI bereits heute in der Lage, Teile eines Cyber-Angriffs zu automatisieren.

Auch der Cyber-Abwehr hilft KI

Allerdings profitieren nicht nur Angreifer, sondern auch Cyber-Verteidiger von allgemeinen Produktivitätssteigerungen durch den Einsatz von KI. Darauf hatte die BSI-Präsidentin bereits im April bei der ersten Digitalministerkonferenz in Potsdam hingewiesen. Mögliche Einsatzbereiche von KI seien etwa die Codegenerierung, die Analyse von Quellcode auf Schwachstellen, die Detektion von Malware oder das Erstellen von Lagebildern. Es komme darauf an, mit den Angreifenden Schritt zu halten, sagt die BSI-Präsidentin Claudia Plattner. Das bedeute schneller zu patchen, IT-Systeme zu härten und nahende Angriffe noch früher als bisher zu erkennen. „Dabei hilft KI uns heute schon. Insbesondere für Open-Source-Projekte wird es von entscheidender Bedeutung sein, KI-Tools proaktiv zu nutzen, bevor böswillige Akteure dies tun. Des Weiteren ist es mit Blick auf den Fachkräftemangel maßgeblich, dass Wirtschaft, Wissenschaft und Politik ihre Kompetenzen bündeln – über Landes- und Ländergrenzen hinweg“, so Plattner.

Wie Künstliche Intelligenz im Detail die Cyber-Abwehr unterstützen kann, will die jetzt publizierte BSI-Untersuchung im Rahmen einer Fortschreibung thematisieren. In einer weiteren Untersuchung, die bereits vorliegt, informiert das BSI über Chancen und Risiken generativer KI-Sprachmodelle für Industrie und Behörden.

(sib)

- BSI: Einfluss von KI auf die Cyber-Bedrohungslandschaft
- BSI: Generative KI-Modelle – Chancen und Risiken für Industrie und Behörden

Stichwörter: IT-Sicherheit, BSI, Cyber-Sicherheit, KI