BSI

Diskussion zu KI und Cyber-Sicherheit

[26.02.2024] Auf der Münchner Sicherheitskonferenz hat sich BSI-Präsidentin Claudia Plattner mit Sicherheitsexpertinnen und -experten über Gefahren und Chancen von KI für die Cyber-Sicherheit ausgetauscht.

Die Präsidentin des Bundesamts für Sicherheit in der Informationstechnik (BSI), Claudia Plattner, hat auf der diesjährigen Münchner Sicherheitskonferenz (MSC) bei einer Diskussion unter dem Titel „HackGPT? Cybersecurity in the Age of Artificial Intelligence“ mit internationalen Sicherheitsexpertinnen und -experten sowie Entscheiderinnen und Entscheidern weltweit führender Technologieunternehmen gesprochen. Wie das BSI mitteilt, haben die Fachleute darüber diskutiert, wie es gelingen kann, die Chancen Künstlicher Intelligenz (KI) zu nutzen und gleichzeitig die Risiken von KI im internationalen Sicherheitskontext zu reduzieren.

Dem BSI zufolge nehmen hybride Gefahren aus dem Cyber-Raum zu und werden immer häufiger zu geopolitischen Risiken. Auch unter Zuhilfenahme von KI gelinge es Angreifenden, immer schneller und effizienter zu agieren. Die Diskutanten seien sich darüber einig gewesen, dass man sich auch mit Blick auf viele in diesem Jahr anstehende Wahlen auf multiple Angriffsszenarien gefasst machen müsse, deren Ziel es sei, Chaos zu stiften und Vertrauen in Regierungen zu zerstören. So müsse man mit Cyber-Attacken auf Kritische Infrastrukturen (KRITIS) in Kombination mit breit angelegten Desinformationskampagnen rechnen. Vor diesem Hintergrund sei eine enge und transparente Zusammenarbeit zwischen staatlichen Akteuren, Wirtschaft und Wissenschaft essenziell, um die Resilienz im Cyber-Raum signifikant zu erhöhen.

Schritt halten

BSI-Präsidentin Claudia Plattner erläuterte: „Hinsichtlich Cyber-Bedrohungen im Zusammenhang mit Künstlicher Intelligenz kommt es darauf an, dass wir als Verteidiger mit den Angreifenden Schritt halten. Dafür sind drei Punkte entscheidend: Erstens ist Geschwindigkeit von größter Bedeutung, zum Beispiel beim Umgang mit Sicherheitslücken. Eine neue Schwachstelle kann mit KI innerhalb weniger Tage oder sogar Stunden ausgenutzt werden. Wir müssen dafür sorgen, dass unsere Abwehrsysteme mindestens ebenso schnell und effizient funktionieren. Dabei kann KI uns helfen. Der zweite entscheidende Faktor ist der Zugang zu und Umgang mit Informationen: Große KI-Sprachmodelle können durch prompt injections ausgetrickst werden, sodass sie sensible Informationen preisgeben. Wir müssen also sicherstellen, dass nur notwendige Informationen in KI-Werkzeugen wie Large Language Models (LLM) gespeichert werden, und verhindern, dass Unbefugte durch KI sensible Informationen erlangen. Das erfordert gemeinsame Anstrengungen der Technologiekonzerne. Der dritte Punkt ist Technologiekompetenz: Wir müssen die Herausforderung annehmen und schnellstmöglich sicherstellen, dass wir genügend Fachleute auf unserer Seite haben, die KI verstehen, um unseren Technologievorsprung halten zu können. Hierbei sind Kooperationen zwischen öffentlicher Hand und privater Wirtschaft, so genannte Public Private Partnerships, unabdingbar.“

KI-Portfolio erweitert

Das BSI hat eigenen Angaben zufolge sein KI-Portfolio deutlich erweitert und ein Kompetenzzentrum eingerichtet, das sich mit Bewertungsverfahren, Regulierungsmaßnahmen und dem Schutz von Verbraucherinnen und Verbrauchern im KI-Kontext befasst. Das BSI betrachte KI-gestützte Erkennungssysteme zur Cyber-Abwehr und forsche zu KI in Bereichen wie beispielsweise dem Finanz- und Gesundheitssektor, dem autonomen Fahren und in Bezug auf Technologien zur Sicherung des Grenzverkehrs.

(th)

Stichwörter: IT-Sicherheit, BSI, Cyber-Sicherheit, künstliche Intelligenz (KI)