Südtiroler
Wirtschaftszeitung
Wochenblatt für Wirtschaft und Politik

Tiratura: 4.500 | **Diffusione:** 18.000
Data: 07/07/2023
Categoria: Raiffeisen-Geldorganisation Print & Web

Kriminelle Intelligenz

IT-SICHERHEIT (2) – ChatGPT eröffnet faszinierende Möglichkeiten. Doch die KI-Anwendung droht auch zum **Helferlein für Cyberkriminelle** zu werden.

Bozen – Die Fortschritte im Bereich der künstlichen Intelligenz und speziell im Bereich der LLM (Large Language Models) haben zu einer Vielzahl aufregender Entwicklungen geführt, darunter auch Chatbots wie ChatGPT (Generativ Pre-trained Transformer). ChatGPT hat Ende des vergangenen Jahres die Welt in eine Mischung aus Faszination und Schreck versetzt (SWZ 2/23, nachzulesen auf SWZonline und in der SWZapp). Das leistungsstarke KI-Modell von OpenAI wurde darauf trainiert, auf eine Vielzahl von Fragen und Anfragen in natürlicher Sprache zu antworten. So kann ChatGPT in kürzester Zeit Texte generieren, Lieder komponieren, E-Mails schreiben, Informationen bereitstellen (manchmal veraltet oder falsch dargestellt) und bei Problemlösungen helfen. Im Frühjahr wurde das Tool in Italien kurzzeitig gesperrt, ist mittlerweile aber wieder verfügbar.

Phishing und Social Engineering

Die Fähigkeit von ChatGPT, menschenähnliche Texte zu generieren, eröffnet Cyberkriminellen neue Möglichkeiten zur Täuschung. Durch die Nachahmung echter Personen oder Institutionen können sie Phishing-Angriffe durchführen. Ein Beispiel hierfür ist das Erstellen von gefälschten Websites oder authentischen E-Mails: Dabei werden Opfer dazu verleiten, ihre Zugangsdaten oder finanziellen Informationen preiszugeben. Hierfür wird ein Social-Engineering-Ansatz verwendet, welcher durch die Ausnutzung menschlicher Eigenschaften deren Vertrauen erweckt und diese so zum Handeln verleitet. Zwar wurden bei ChatGPT Sicherheitsvorkehrungen getroffen, um potenziell bedrohliche Absichten zu erkennen, jedoch können diese durch eine richtig gestellte Frage (Prompt-Engineering) umgangen werden.

> **Die Fähigkeit von ChatGPT, menschenähnliche Texte zu generieren, eröffnet neue Möglichkeiten der Täuschung.**

Automatisierung von Angriffen

ChatGPT kann auch dazu verwendet werden, Angriffe auf Computersysteme zu automatisieren. Durch die Verwendung der KI können Cyberkriminelle maßgeschneiderte Malware erstellen, Schwachstellen identifizieren oder Angriffe auf Netzwerke durchführen, schreibt der IT-Dienstleister in einer Aussendung.

Erstellung von Malware, Exploits und Ransomware

Cyberkriminelle könnten ChatGPT laut Konverto darüber hinaus dazu nutzen, maßgeschneiderte Malware (Schadsoftware) und Exploits (Malware/Befehlsfolge zur Ausnutzung von Sicherheitslücken und Fehlfunktionen) zu entwickeln. Durch die Programmierung des Sprachmodells mit Kenntnissen über Schwachstellen und Angriffsmethoden können die Kriminellen automatisch schädlichen Code generieren, der auf bestimmte Ziele angepasst ist. Dies könnte die Effektivität und Verbreitung von Malware erhöhen und die Entdeckung durch Sicherheitslösungen erschweren.

Bei einer Ransomware-Attacke werden Daten des Opfers zunächst verschlüsselt, um anschließend Lösegeld für deren Freigabe zu erhalten. Für die Zahlung des Erpressergeldes nutzen Hacker die KI auch, um Zahlungssysteme für Kryptowährungen zu erstellen. Doch nicht nur für diese Finanzbewegungen wird die KI verwendet, sondern auch für Geldwäsche. Durch die authentischen Gespräche über Geschäftsaktivitäten werden die Transaktionen von Überwachungssystemen übersehen oder als unauffällig eingestuft.

Ernst zu nehmende Risiken

Die potenzielle Verwendung von ChatGPT als Helfer für Cyberkriminelle birgt ernsthafte Risiken. Es ist entscheidend, dass Entwickler- und Herstellerfirmen sowie Benutzer:innen dieser Technologie ihre Verantwortung erkennen und Maßnahmen ergreifen, um Missbrauch zu verhindern. Konverto macht in seiner Aussendung auch Hoffnung: Durch die Implementierung einer umfangreichen Sicherheitslösung sowie durch kontinuierliche Überwachung können die Risiken minimiert werden.