Die Zeitung am Sonntag

Tiratura: 37.000 | **Diffusione:** 115.713
Data: 02/07/2023
Categoria: Raiffeisen-Geldorganisation Print & Web

„Die Gefahr wird unterschätzt“

Er kann Businesspläne und Liebesbriefe schreiben. Und mittlerweile auch gefährliche Betrugs-E-Mails verfassen: Die Rede ist von ChatGPT. Wie der Chatbot für kriminelle Aktivitäten missbraucht werden kann – und warum er für Betrüger so interessant ist.

SÜDTIROL *(rm)* Seit November 2022 mischt ChatGPT die Onlinewelt kräftig auf. Denn die Texte, die der Chatbot *(Anm.: eine Software, die Nachrichten senden, auf Fragen antworten und Texte schreiben kann)* ausspuckt, sind oft so gut geschrieben, dass sie in Lexika stehen oder im Unterricht vorgetragen werden könnten *(die „Zett“ berichtete)*.
Bei aller Euphorie lassen viele allerdings außer Acht, welche Sicherheitsrisiken die Verwendung dieser künstlichen Intelligenz birgt. Denn: Mittlerweile hat sich ChatGPT in kriminellen Kreisen als leistungsstarkes Betrugswerkzeug etabliert, für das Betrüger nicht einmal besondere Programmierkenntnisse benötigen.

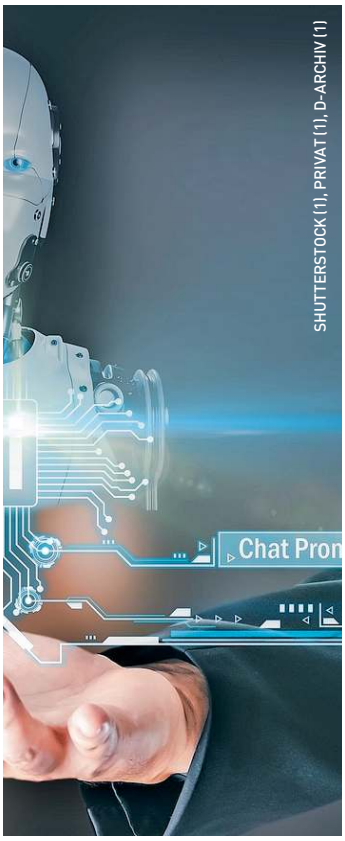
> Die Betrüger optimieren mit der Hilfe von ChatGPT sogenannte ‚Phishing-Angriffe.‘
>
> **Stefan Laimer, Sicherheitsexperte**

Mit Hilfe von ChatGPT zum „perfekten“ Betrug

So kann das KI-System mittlerweile bereits Sprach-Stile imitieren und Texte in allen möglichen Sprachen verfassen. Stefan Laimer (i.B.u.), Sicherheitsexperte beim IT-Unternehmen „KONVERTO“, sieht genau in diesen generierten Texten die Gefahr: „Die Betrüger optimieren mithilfe von ChatGPT sogenannte ‚Pishing-Angriffe‘ *(Anm. d. Red.: Daten von Internetnutzern werden über gefälschte Internetadressen, E-Mails oder SMS abgefangen)*. Die Gefahr, die davon ausgeht, wird unterschätzt.“

Die Zeitung am Sonntag

Tiratura: 37.000 | **Diffusione:** 115.713
Data: 02/07/2023
Categoria: Raiffeisen-Geldorganisation Print & Web



Fehler in Orthografie und Grammatik waren bisher oft ein Kriterium, mit dem ein „Phishing-Versuch“ leicht enttarnt werden konnte. Aber, so der Experte: „ChatGPT macht diese Fehler nicht mehr.“ Der Chatbot arbeite also verdeckt, genauso wie die Betrüger selbst. Deshalb sei es wichtig, über den Einsatz von ChatGPT in diesem Bereich aufzuklären: „ChatGPT kann aber nicht nur Texte bis zur Perfektion generieren, sondern hilft Kriminellen, sogenannte ‚Malewares‘ zu schreiben. ‚Malewares‘ bezeichnet jede Art von Software, die erstellt wird, um eine andere Software oder Hardware zu beschädigen oder zu missbrauchen.“ Da es jedoch auch für Experten noch schwierig sei, von ChatGPT generierte Texte für „Phishing-E-Mails“ oder „Phishing-SMS“ zu entschlüsseln bzw. vom Chatbot geschriebene „Malewares“ zu erkennen, stecke Laimer zufolge die Entwicklung wirkungsvoller Sicherheitsvorkehrungen derzeit noch in den Startlöchern.

> Es gibt keine ‚gute‘ oder ‚böse‘ künstliche Intelligenz.
>
> **Oswald Lanz, Professor an der Uni Bozen**

Keine Angst vor künstlicher Intelligenz!

Dass es einzelne Sicherheitstools gibt, die bereits erkennen, ob ein Text von einer künstlichen Intelligenz geschrieben wurde oder nicht, das bestätigt neben dem Security-Experten Stefan Laimer

auch Oswald Lanz (i.B.). Der Professor an der Fakultät für Ingenieurswissenschaften an der Uni Bozen sieht die größte Gefahr in diesem Bereich aber immer noch bei dem, der hinter dem Bildschirm sitzt: „Es gibt keine ‚gute‘ oder ‚böse‘ künstliche Intelligenz. Es kommt immer auf den Anwendungszweck an. Und der kann vom Nutzer eben gut- oder böswillig sein.“ Zudem setzen solche Betrugsmaschen ein breites Hintergrundwissen voraus. „Die KI ist für Betrüger schlussendlich nur ein Baustein in dem komplexen Missbrauchsgebilde“, so Lanz.