Die eine Million-Dollar-Frage oder: Wird KI unsere Wahlen verändern?

2024 werden Menschen mit ihren Stimmen für Veränderungen sorgen. Aber spielen im diesjährigen Superwahljahr womöglich noch andere Kräfte mit? Wird künstliche Intelligenz zu einem politischen Player? Chester Wisniewski, Field CTO bei Sophos, hat sich dazu Gedanken gemacht.

Die USA beispielsweise steuern auf eine entscheidende Präsidentschaftswahl zu, genau zu einer Zeit, in der die generative KI-Technologie entwickelt genug zu sein scheint, potenzielle Wähler mit Bildern und Texten, die sie online sehen zu sehen bekommen, aktiv zu beeinflussen. Das hat dazu geführt, dass einige das Jahr 2024 als "die erste KI-Wahl" bezeichnen.

KI ist eine faszinierende Sache und die freie Zugänglichkeit für jeden, beispielsweise via die OpenAI-Webseite, eine Bereicherung. Aber wie man diese effektiv nutzten kann, das steht auf einem anderen Blatt. Ein Experte wird mit KI ganz andere Ideen angehen, als jemand der kriminelle Ziele verfolgt. Auch wir arbeiten bei Sophos mit KI und verwenden viel Zeit und finanzielle Ressourcen darauf, eigene Modelle zu entwickeln und sie für spezifische technologische Prozesse zu trainieren. Sie sollen unsere Forschenden bei der Beschleunigung von Arbeitsprozessen oder der Analyse riesiger Datenmengen unterstützen. Jemand mit weniger guten Absichten, stattdessen aber viel Geld, könnte sich KI-Modelle bauen, die weitaus effektiver sein könnten als das, worauf Normalnutzer zugreifen können, um Fake Content zu produzieren.

Eine Frage des Geldes

Geld ist eine entscheidende Ressource, um realistische Bedrohungsszenarien zu entwickeln. Gefälschte Bilder, Stimmen, Videos – dafür braucht man spezialisierte Datenexperten, keine Freizeit-Tüftler. Hinsichtlich des Einsatzes von KI besteht viel Desinformation. In den letzten Wahlzyklen der USA sahen wir Videos, die editiert wurden (vielleicht um jemanden kränker aussehen zu lassen, als er ist), oder mit erfundenen Worteinlassungen, die jemand im echten Leben so nie gesagt hätte. Und wir nähern uns dem Punkt, an dem das wirklich auf Abruf generiert werden kann. Sicherlich ist das Klonen von Stimmen oder das Klonen von Bildern für eine gut ausgestattete Organisation oder eine Nation jetzt möglich. Ich glaube allerdings nicht, dass Amateure das bereits effektiv tun können, weil die Anzeichen dafür, dass es gefälscht ist, ohne viel Aufwand und Ressourcen und Experten dahinter einfach zu offensichtlich sind.

Ich bezweifle auch, dass die Technologie bereits für jeden zugänglich ist, um überzeugende Deepfakes zu erstellen. Vielmehr besteht die größere Bedrohung wahrscheinlich von den koordinierten Bemühungen gut ausgestatteter staatlich unterstützter Gruppen.

Größtes Risiko: massenweise Fake Konten als Fangruppe

Das größte aktuelle Risiko ist meiner Meinung nach die massenweise Generierung von Fake-Konten, um eine bestimmte politische Agenda zu pushen. Zerstörerische Inhalte, die eine AI selbst schreibt , sind zunächst zu vernachlässigen. Es wird ein Mensch sein, der eine Idee haben und diese dank künstlicher Intelligenz in einem Maße umsetzen können wird, wie wir es bislang noch nicht gesehen haben.

Die großen Sprachmodelle ermöglichen es ausländischen Akteuren, sich in einem Ausmaß und mit einer Geschwindigkeit zu tarnen, die sie vorher nicht erreichen konnten.

Für ein Meme einer Internet-Forschungsagentur (in 2016 im Wahlkampf von Clinton und Trump) mussten zum Beispiel ein paar wirklich gute englische Redakteure die Grammatik überprüfen und die Texte verfassen, um dann jeweils noch kleine Änderungen vornehmen und all diese Tweets oder Instagram-Posts oder was auch immer manuell verschicken zu können. Das kann jetzt alles automatisiert werden. Ein Problem.

Eine Million Dollar in Rakete oder KI...
Es gibt nur sehr wenige tatsächliche politische Deepfakes. Warum? Weil wir es kaum nachweisen können. Die Betrügereien sind nicht raffinierter geworden durch KI, wohl aber effizienter. ChatGPT spricht fließend in fast jeder Sprache, es wäre leichtsinnig zu glauben, dass Phisher und Betrüger aller Art dies nicht für Übersetzungszwecke nutzen würden.

Wahrscheinlich werden wir keine Deepfakes von Amtsträgern oder oder ihren Herausforderern sehen, aber vielleicht etwas, das sich womöglich irgendwie seltsam oder verdächtig anfühlt.Wenn wir über Dinge in unserem persönlichen Maßstab nachdenken, vergessen wir schnell, wie billig KI-gesteuerte Betrugsaktivitäten im Vergleich zu traditionellen Waffen sind..

Eine Rakete kostet über eine Million Dollar. Die Menge an Grafikprozessoren, die man mit dieser einen Million Dollar kaufen kann, um KI-Fälschungen zu erstellen, ist enorm. Man kann also mit einer Million Dollar eine Einrichtung mit einer Rakete zerstören oder eine ganze Gesellschaft mit einer Desinformationskampagne aus dem Gleichgewicht bringen. Und das bedeutet, dass so ziemlich jedes Land auf der Welt, wenn es will, finanziell in der Lage ist, diese Dinge in großem Maßstab zu tun. Für einzelne Akteure jedoch, denke ich, ist diese Möglichkeit noch zu weit entfernt, als dass wir sie in 2024 sehen werden.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de