Sicherheitspanne mit Ansage

Instagrams eigener KI-Bot hilft Hackern dabei, Konten zu knacken

VON MATTHIAS SCHWARZER

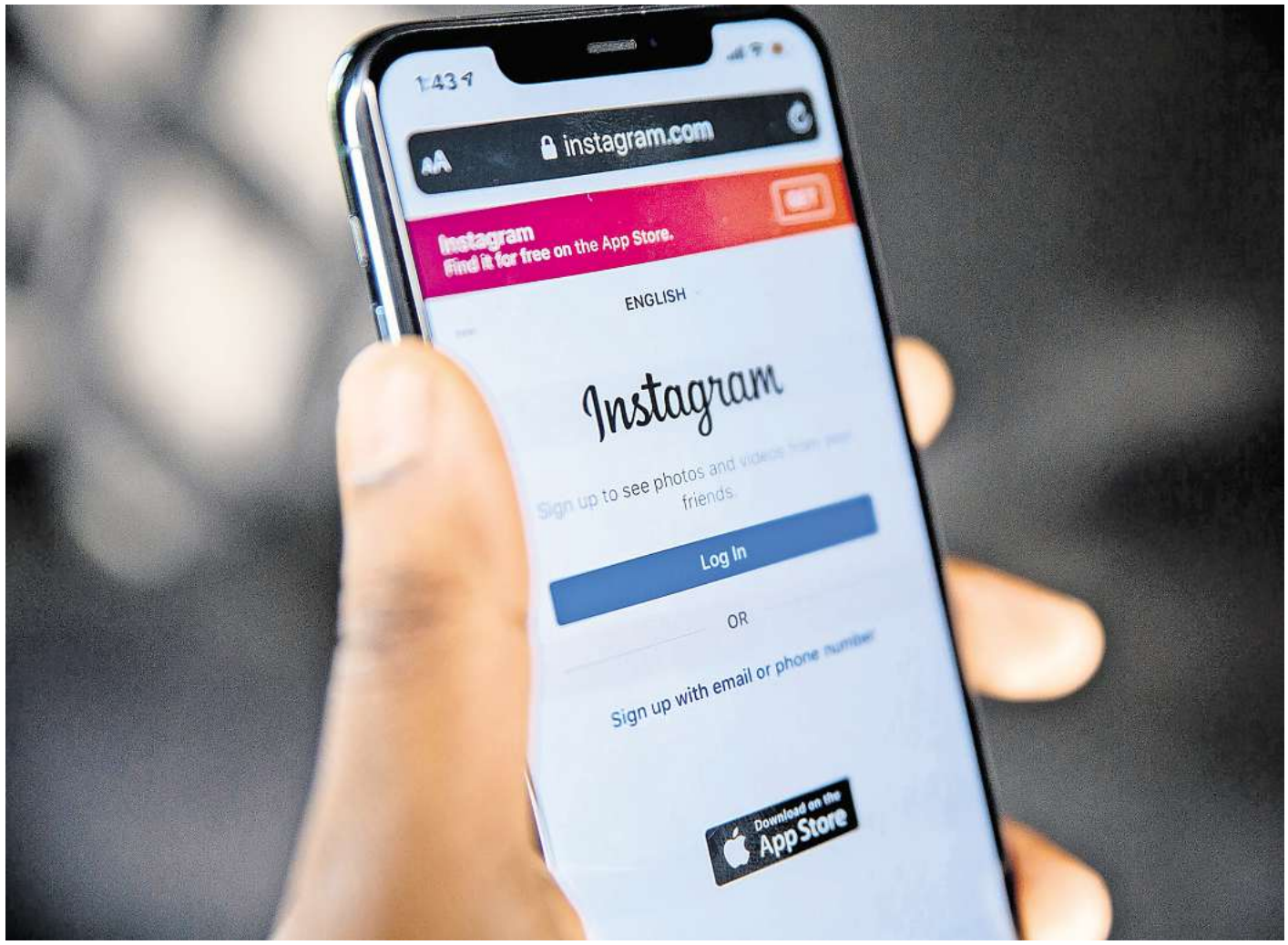

FOTO: SOLEN FEYISSA / UNSPLASH

Wie viele andere US-Techkonzerne setzt der Meta-Konzern von Mark Zuckerberg verstärkt auf Künstliche Intelligenz. In Apps wie Instagram und Whatsapp hat ein KI-Chatbot Einzug gehalten, mit einer KI-Brille plant der Konzern auch in Europa die Marktführerschaft – und Beschäftigte des Konzerns werden regelrecht ermutigt, bei der Arbeit KI-Tools zu nutzen. Zuletzt hatte Meta auch 8000 Beschäftigte zugunsten von KI-Investitionen entlassen.

Nun zeigt sich, was passieren kann, wenn man den eigenen KI-Systemen zu viel Vertrauen schenkt: Medienberichten zufolge soll es Hackern gelungen sein, mehrere prominente Instagram-Konten zu übernehmen. Und das ausgerechnet mithilfe des Meta-eigenen KI-Support-Chatbots.

Hacker bitten um Zurücksetzung des Passworts

Das Portal „404 Media“ berichtet über ein auf Telegram geteiltes Hacker-Video. Darin zeigt jemand, wie er den Support-Bot von Meta auffordert, die mit seinem Profil verknüpfte E-Mail-Adresse zu ändern und anschließend das Passwort zurückzusetzen.

Die KI soll daraufhin einen achtstelligen Code an die E-Mail-Adresse des Angreifers gesendet haben. Nach der Eingabe des Codes erhielt der Angreifer eine E-Mail zur Passwortzurücksetzung. Dadurch bekam er schließlich Zugriff auf das Konto.

Um den Support-Bot auszutricksen, mussten die Angreifer offenbar noch ein paar weitere Maßnahmen anwenden. So wurde wohl auch mit einer VPN-Verbindung der Standort des Kontoinhabers vorgegaukelt.

Alter Obama-Account gehackt

Der Vorfall hatte offenbar Folgen: Etwa zur selben Zeit wie das Bekanntwerden des Hacks wurden mehrere prominente Instagram-Konten erfolgreich angegriffen – darunter der Archiv-Account des Weißen Hauses unter Barack Obama. Dort seien am Sonntag Bilder mit iranischer Propaganda gepostet worden. Auch die Konten des Chief Master Sergeant der US Space Force und des Kosmetikhändlers Sephora sollen gekapert worden sein.

Die IT-Sicherheitsforscherin Jane Manchun Wong berichtet ebenfalls von einem erfolgreichen Angriff auf ihr Konto: „Das Passwort wurde ohne mein Wissen geändert, und ich habe gestern den ganzen Tag über verschiedene Versuche zur Passwortzurücksetzung erhalten“, so Wong. „Außerdem wurde ich wiederholt aus der IG-iOS-App abgemeldet.“

Meta selbst beantwortete Fragen des RedaktionsNetzwerks Deutschland (RND) nicht, verwies aber auf einen knappen Post des Kommunikationschefs Andy Stone. Dieser hatte das Problem indirekt auf der Plattform X bestätigt. Unter einem Post antwortete Stone: „Dieses Problem wurde behoben und wir sichern die betroffenen Konten“. Mehrere Hacking-Kanäle bestätigten laut „404 Media” auf Telegram, die Schwachstelle funktioniere inzwischen nicht mehr.

KI-Bot sollte den Support verbessern

Der KI-gestützte Support-Chatbot war erst im März von Meta eingeführt worden. In einem Blogpost hatte das Unternehmen damals erklärt, der Bot solle „rund um die Uhr Hilfe für Konto-Probleme wie die Aktualisierung deines Passworts und Einstellungen für dein Profil“ liefern.

Meta versprach einen „zuverlässigen Support“ für „nahezu jedes Support-Problem“ und „Lösungen, nicht nur Vorschläge“. Hilfe sei damit nur noch einen „Fingertipp entfernt“ – man müsse sich nicht mehr durch das Hilfedokument der Website klicken.

Wer auf Plattformen wie Instagram, Facebook und Whatsapp menschliche Hilfe suchte, war auch schon zuvor weitestgehend aufgeschmissen. Nur wer ein bezahltes „Meta Verified“-Abo besitzt, kommt in den Genuss eines echten Kundenservices. Dennoch klagen immer wieder Nutzerinnen und Nutzer über Probleme – etwa über wahllos gesperrte Accounts, bei denen Meta dann kaum weiterhilft.

Bei Meta ist alles KI

Dass diese Probleme nun mit Künstlicher Intelligenz gelöst werden sollen, passt ins Bild. Wie kaum ein anderer Konzern hatte Meta seine Unternehmensstruktur zuletzt verändert, um sich ganz auf den KI-Hype zu konzentrieren. In einem Interview mit dem RND hatte der deutsche Public-Policy-Director des Konzerns, Semjon Rens, kürzlich erklärt, man strebe die Technologieführerschaft im KI-Bereich und glaube daran, diese auch zu gewinnen. Helfen soll dabei nicht zuletzt die smarte KI-Brille des Unternehmens.

Diese Haltung spiegelt sich auch in der Mitarbeiterführung wider. Vor einigen Wochen berichtete die „New York Times“, Meta zeichne neuerdings Eingaben und Mausbewegungen seiner Beschäftigten am Computer auf, um mit den Daten KI-Modelle trainieren zu können. Im Konzern sorgte das dem Bericht zufolge für massiven Unmut.

Als bekannt wurde, dass der Konzern rund zehn Prozent seiner Belegschaft zugunsten von KI-Investitionen entlassen wird, blieben die betroffenen Angestellten Medienberichten zufolge zunächst lange im Ungewissen. Mehr noch: In der Übergangszeit soll das Unternehmen laut „Futurism“ die täglichen Arbeitsabläufe der Entwickler gezielt genutzt haben, um die eigenen KI-Modelle zu trainieren. Das Magazin beruft sich auf einen an die Öffentlichkeit geratenen Audio-Mitschnitt von CEO Mark Zuckerberg.

Immer wieder Sicherheitsprobleme

Gleichzeitig hat der Konzern jedoch immer wieder mit Sicherheitsproblemen zu kämpfen. Erst im Herbst vergangenen Jahres war es Forschern der Uni Wien gelungen, Daten von Milliarden Whatsapp-Nutzern abzugreifen. Jahre zuvor waren Millionen Handynummern durch ein Facebook-Datenleck in die Hände von Kriminellen gelangt.

Der IT-Sicherheitsexperte Florian Dalwigk analysierte damals gegenüber RND: „Meiner Einschätzung nach könnte das darauf hindeuten, dass Meta in der Vergangenheit funktionale und wachstumsorientierte Aspekte teilweise höher gewichtet hat als eine strikte Umsetzung von Privacy-by-Design-Prinzipien.“ Der IT-Grundsatz „Privacy-by-Design“ meint, dass der Datenschutz von Anfang an bei der Entwicklung mitgedacht wird, und nicht erst nachträglich.

Gergely Orosz, der Herausgeber des Newsletters „The Pragmatic Engineer“, schreibt zum aktuellen Fall auf Bluesky, sein Team habe angesichts der Entlassungen das Vertrauen in die Sicherheitsmaßnahmen von Meta verloren. „Die Ingenieure bei Instagram übertreiben es damit, KI für alles einzusetzen, und haben keinerlei Anreize für Dinge wie … Sicherheit.“ Das sei eine Warnung an alle Unternehmen, die denselben Weg wie Meta einschlagen wollten.