Warum wir uns Sorgen machen sollten, dass Twitter Produkte des israelischen Überwachungsstaates übernimmt

Richard Silverstein, newarab.com, 06.09.23

Die Berichte, dass *X*, früher bekannt als *Twitter*, möglicherweise das digitale ID-Produkt eines israelischen Cybersicherheitsunternehmens nutzt, sollten Alarm auslösen, schreibt Richard Silverstein. Viele dieser Technologien werden eingesetzt, um Palästinenser:innen zu überwachen und als Ziel zu wählen.

Für ein Unternehmen wie *Twitter* und einen Geizhals wie Elon Musk könnte die Aussicht, die Erkennung von Betrügern zu automatisieren, ein Geschenk des Himmels sein. Aber für die legitimen Nutzer.innen selbst könnte es ein Albtraum sein.

Israel ist weltweit führend im Bereich Überwachungstechnologie und Cybersicherheitsprodukte. Es gibt dort zwar Unternehmen, die sich an Cyber-Verteidigungstechnologie beteiligen, jedoch ist es vor allem für seine offensive Technologie und Spyware bekannt und berüchtigt, die von Unternehmen wie *NSO Group, Candiru, Circles, Paragon, Intellexa, Citrox* und *Cellebrite* angeboten werden.

Ihre Produkte nutzen Schwachstellen in Sicherheitsprotokollen elektronischer Geräte aus, um Sprache, Video, Texte und E-Mails abzufangen. Geheimdienste und Strafverfolgungsbehörden sowohl in repressiven Regimen als auch in Demokratien nutzen sie, um politische Dissident:innen, Menschenrechtsaktivist:innen, Journalist:innen, Anwält:innen und Lehrer:innen zu verfolgen.

In mehreren Fällen wurden Geräte politischer Dissident:innen gehackt. Andere wurden aufgrund der auf diese Weise gesicherten Beweise festgenommen und inhaftiert. Die Spyware ermöglichte es einem saudischen Killerkommando, den Aufenthaltsort des saudischen Journalisten Jamal Khashoggi zu ermitteln, das ihn dann ermordete, als er im saudischen Konsulat in Istanbul ankam.

Israelische „Anti-Terror"-Technologie

Eine andere Nische in diesem Markt ist die digitale Identitätstechnologie. Es ermöglicht Unternehmen wie Finanzdienstleistern (einschließlich Banken) und Flughäfen, die einem hohen Betrugsaufkommen ausgesetzt sind, die Authentifizierung von Kundenidentitäten. Zu diesen Unternehmen gehört *AU10TIX* mit einem jährlichen Nettogewinn von 40 Millionen US-Dollar.

Das Unternehmen beschreibt sich selbst als „der langjährige Branchenführer für automatisierte Identitätsprüfungs- und Verwaltungslösungen für die digital abhängigen globalen Unternehmen von heute". Sein Hauptziel ist die Aufdeckung und Verhinderung von Betrug. Zu seinen weiteren Kunden zählen *PayPal, Google, Airbnb, LinkedIn, Payoneer, Uber* und *Santander*.

„Israelische Unternehmen wie *AU10TIX* behaupten, dass sie die höchsten ethischen Standards einhalten und die Datenschutzrechte derjenigen schützen, auf deren Daten sie zugreifen.“ Aber wenn Kunden diese Tools nutzen, selbst für einen ihrer Meinung nach legitimen Zweck, kaufen sie die Technologie und Ideologie ein, die sie geschaffen hat.“

Dazu muss *AU10TIX* eine riesige Datenbank mit den persönlichen Daten von Millionen oder sogar Dutzenden Millionen Menschen zusammenstellen. Seine Algorithmen wären so programmiert, dass sie für Betrug charakteristische Muster erkennen. Möglicherweise markieren sie sogar diejenigen, die kein solches Verhalten an den Tag gelegt haben, dies aber in Zukunft tun könnten.

Der Punkt ist, dass niemand außer *AU10TIX* und seinen Kunden weiß, was der Algorithmus ist und wie er solche Entscheidungen trifft. Sie werden wahrscheinlich nicht herausfinden, ob Sie ins Visier genommen werden. Selbst wenn Sie es wüssten, hätten Sie kaum Rückgriffsmöglichkeiten, es sei denn, Sie könnten nachweisen, dass Ihnen ein persönlicher Schaden entstanden ist.

Ursprünglich stellte das Unternehmen Cybersicherheitsdienste für Flughäfen auf der ganzen Welt bereit. Seine Technologie war Teil des Mysteriums der angeblich konkurrenzlosen Anti-Terror-Expertise Israels, die durch seine Wachsamkeit gegenüber palästinensischen Angriffen verfeinert wurde. Das Verkaufsargument bestand darin, dass das Modell bei der Identifizierung und Verhinderung von Terrorismus auf israelischen Flughäfen auf Flughäfen weltweit übertragen werden könnte. Anti-Terror-Technologie wurde zum „nächsten großen Ding“ und israelische Unternehmen ernteten die finanziellen Früchte.

Damit die digitalID effektiv ist, wirft sie ein Netz aus, in dem riesige Datenmengen erfasst werden. Es könnte aus einer Vielzahl von Quellen zusammengestellt werden, von denen einige öffentlich und andere über nicht öffentliche Mittel zugänglich sind. Zusätzlich zur eigenen Datenbank von *AU10TIX* könnte es private Informationen kaufen oder sich Zugriff darauf verschaffen, die von anderen Unternehmen, Regierungen, Strafverfolgungsbehörden, Gerichten, Geheimdiensten usw. zusammengestellt wurden. Der Mangel an Transparenz bei der Zusammenstellung dieser Datenbanken ist besorgniserregend, ganz zu schweigen von der damit verbundenen Verletzung der Privatsphäre.

Von gezielten Angriffen auf Palästinenser:innen bis hin zu *Twitter*

AU10TX nutzt die Gesichtserkennungstechnologie, die von der *SIGNT Unit 8200* der israelischen Armee entwickelt wurde. Letztere entwickelt einige der fortschrittlichsten Überwachungstechnologien der Welt. Es wird verwendet, um die palästinensische Bevölkerung auszuspionieren und diejenigen zu identifizieren, die möglicherweise erpresst werden können, als Informanten für den israelischen *Shin Bet* zu dienen. Solche Personen wurden unter anderem damit beauftragt, äußerst wichtige Geheimdienstinformationen zu liefern, die palästinensische Widerstandsführer verraten, die ermordet werden sollen. Eine solche Technologie löst bei den Palästinenser:innen Angst und Misstrauen aus, bringt sie gegeneinander auf und zerstört den Zusammenhalt ihrer Gesellschaft.

Aktuellen Berichten in Technologiemedien zufolge erwägt *X* – früher bekannt als *Twitter* – die Registrierung einer digitalen ID für seine Premium-Benutzer. Um sich anzumelden, müsste man einen amtlichen Ausweis und ein Selfie vorlegen. Für *AU10TIX* wäre es ein weiterer hinzugefügter Datenpunkt, um seine Datenbanken zu füllen. Für das Unternehmen, das früher als *Twitter* bekannt war, würde es diese Daten nutzen, um diese

High-End-Nutzer anzusprechen. Die einzigen, die davon profitieren könnten, wären diejenigen, die Wert darauf legen, ihre Online-Identität vor Betrügern zu schützen.

> #X ist möglicherweise kurz davor, die ID-Verifizierung freizugeben!! Es scheint notwendig zu sein, die Blue-Funktionen zu aktivieren!
>
> Sie haben auch die Möglichkeit, Ihren Ausweis zur Identitätsprüfung auszublenden. pic.twitter.com/hMIrcQhojZ
>
> – Nima Owji (@nima_owji) 3. August 2023

AUTO10TIX und die oben aufgeführten Spyware-Unternehmen sind Produkte des israelischen Überwachungsstaates. Viele von ihnen nehmen nicht nur Palästinenser:innen ins Visier und greifen sie an, ihre Produkte werden auch in repressive und völkermörderische Staaten exportiert. Israelische Unternehmen wie *AU10TIX* behaupten, dass sie die höchsten ethischen Standards einhalten und die Datenschutzrechte derjenigen schützen, auf deren Daten sie zugreifen. Aber wenn Kunden diese Tools verwenden, selbst für einen ihrer Meinung nach legitimen Zweck, akzeptieren sie die Technologie und Ideologie, die sie geschaffen haben.

Die Gesichtserkennungstechnologie, die *AU10TIX* zur Authentifizierung von Benutzern verwendet, ist vom selben Typus, wie sie von der israelischen Armee und vom *Shin Bet* verwendet wird, um Bilder von jedem/r Palästinenser:in zu erstellen, der/die aus dem Westjordanland nach Israel einreist. Darüber hinaus ist das Westjordanland einer der am stärksten überwachten Orte der Welt, und in fast jedem Häuserblock jedes palästinensischen Dorfes sind Überwachungskameras angebracht. Dieses Videomaterial zeichnet praktisch jeden/r Palästinenser:in in der Gegend auf und ist Teil einer riesigen Datenbank, die ausgewertet wird, um jede:n zu identifizieren, der/die als Spion:in rekrutiert werden könnte; jede:r, die/der bei einem Angriff auf Israelis verdächtigt werden könnte; oder jemand, der noch nie einen gewalttätigen Angriff begangen hat oder darüber nachgedacht hat, dies aber in Zukunft tun könnte.

Die *Blue Wolf-App* beauftragt Soldat:innen damit, Fotos von Palästinenser:innen zu machen, wo immer sie sie finden, um sie in eine Datenbank hochzuladen, auf die der *Shin Bet* und der Militärgeheimdienst zugreifen. Es gibt sogar Belohnungen für diejenigen, die die meisten Fotos machen.

Der Prozess, mit dem die Algorithmen bestimmen, wer als Verdächtige:r gilt, ist völlig undurchsichtig. Aus diesem und anderen Gründen ist das System fehleranfällig. Eine völlig unschuldige Person könnte aus Gründen, die der *Shin Bet* niemals öffentlich bekannt geben muss, nicht einmal in einem Gerichtsverfahren, zum Verdächtigten werden und verfolgt, verhaftet oder eingesperrt werden.

Dan Yerushalmi, CEO von *AU10TIX*, hat genau dieses Problem unabsichtlich hervorgehoben: „In einer Welt, in der die ‚Automatisierung' die meiste Zeit tatsächlich durch menschliche ‚Experten' verbessert wird, zeichnet sich *AU10TIX* durch seinen Grad an Prozessvollautomatisierung aus."

Mit anderen Worten: Das Produkt macht es überflüssig, dass ein Mensch entscheiden muss, wer legitim ist und wer nicht. Für ein Unternehmen wie *Twitter* und einen Geizhals wie Elon Musk könnte die Aussicht, die Erkennung von Betrügern zu automatisieren, ein Geschenk des Himmels sein. Aber für die legitimen Nutzer.innen selbst könnte es ein Albtraum sein.

AU10TIX rühmt sich, „zum bevorzugten Partner großer globaler Marken für … Automatisierung der Kundenüberprüfung geworden zu sein – und arbeitet weiterhin an den Rändern dessen, was als nächstes für die Rolle der Identität in der Gesellschaft ansteht."

Auch dies mag Musik in den Ohren von Unternehmen sein, in denen es häufig zu Diebstählen oder Betrügereien kommt, aber die Vorstellung, dass es sich dabei um eine „an den Rändern" der Authentifizierung persönlicher Identitäten handelt, ist abschreckend. Das Unternehmen gibt an, eine betrügerische Person oder Transaktion in nur drei Sekunden erkennen zu können.

Wie hoch ist die Fehlerquote? Wie viele Personen werden fälschlicherweise markiert? Wie werden solche Fehler eingedämmt? Welcher Schaden entsteht gegebenenfalls für den Ruf oder die Verbraucherbilanz einer Person, die fälschlicherweise gemeldet wurde?

Social-Media-Plattformen wie *X* betrachten ihre Kundendatenbanken als ihre Kronjuwelen. Obwohl sie sie etwa wie Fort Knox bewachen, nutzen sie sie maximal als Einnahmequelle aus. Es ermöglicht Werbetreibenden, gezielt auf die von ihnen gesuchte Kundengruppe abzuzielen. Sobald Sie Elon Musk Ihren amtlichen Ausweis und Ihr Foto geben, haben Sie keine Ahnung, was er damit machen wird. Sie verlieren Ihre Autonomie bei der Entscheidung, wie diese Bilder verwendet werden. Sie sind zu einem Datenpunkt statt zu einem Menschen geworden.

Jede/r, der das blaue Häkchen von *X* und seine digitale ID erwirbt, sollte sich darüber im Klaren sein, dass seine persönlichen Daten Elon Musk gehören.

Richard Silverstein schreibt den Blog Tikun Olam und ist ein freiberuflicher Journalist, der sich auf die Aufdeckung von Geheimnissen des israelischen nationalen Sicherheitsstaates spezialisiert hat. Er setzt sich gegen Intransparenz und die negativen Auswirkungen der israelischen Militärzensur ein.

Quelle: https://www.newarab.com/opinion/why-twitter-using-israels-surveillance-products-worrying

Übersetzung: R. Häberle, Palästinakomitee Stuttgart – palaestinakomitee-stuttgart.de