Bürgerrechtsorganisation warnt: Online-Werbung als „ernstes Sicherheitsrisiko“

Originalartikel

Backup

<html> <header class=„entry-header“> Das Online-Werbesystem ist eine Goldgrube für Geheimdienste und andere bösartige Akteure. Zu diesem Schluss kommt die irische Nichtregierungsorganisation ICCL in einer neuen Untersuchung. Vermeintlich harmlose Werbedaten könnten nicht nur nach Russland und China abfließen, sondern auch zur Erpressung genutzt werden. <time class=„published dt-published posted-on“ datetime=„2023-11-19T16:08:30+00:00“>19.11.2023 um 16:08 Uhr</time> - , - in Datenschutz - keine Ergänzungen </header><figure class=„wp-caption entry-thumbnail“><figcaption class=„wp-caption-text“>Alles andere als harmlos: Die unkontrollierten Datenflüsse der Werbewelt – Gemeinfrei-ähnlich freigegeben durch unsplash.com Glenn Carstens Peters</figcaption></figure> Wenn es um die Risiken von Online-Werbung geht, dann ist oft die Rede von Manipulation und Diskriminierung, manchmal auch von Spam und Desinformation. Die Irish Council for Civil Liberties (ICCL) fügt der Liste an Gefahren nun drei weitere hinzu, die bislang weniger im Fokus der Öffentlichkeit stehen: Erpressung, Rufschädigung und Hackerangriffe. Der unkontrollierte Datenhandel auf Werbemarktplätzen im Internet sei insgesamt eine Gefahr für die nationale Sicherheit. Zu diesem Schluss kommt die irische Bürgerrechtsorganisation in einer neuen Untersuchung. Das derzeitige Werbesystem sorge für eine bislang versteckte Sicherheitskrise, denn bösartige Akteur:innen könnten über Werbeplattformen nicht nur GPS-Daten und Verhaltensmuster, sondern auch die sexuelle Orientierung, Gesundheitsinformation, den ökonomischen Status und sogar mögliches Suchtverhalten von Zielpersonen ermitteln. Der Werbemarkt sei „eine Goldgrube an Erkenntnissen“ für Geheimdienste und nichtstaatliche Akteure, so der Bericht. „Die Federal Trade Commission der USA, die europäischen Datenschutzbehörden

und die EU-Kommission müssen dringend handeln“, appelliert Johnny Ryan von der ICCL. Man dürfe es der Werbeindustrie nicht erlauben, Politik und Militärpersonal zu gefährden. <h3>Zielgruppe: Angestellte von Militär und Rüstungskonzernen</h3> Für die Studie hat die ICCL gemeinsam mit dem Wiener Tracking-Forscher unter anderem die Angebotslisten von Werbemarkplätzen untersucht. Im Ökosystem des Targeted Advertising können Werbetreibende ihre Zielgruppe aus hunderttausenden verschiedenen Kategorien auswählen. Erst in diesem Jahr hatte netzpolitik.org gemeinsam mit dem US-Medium The Markup aufgedeckt, dass der zu Microsoft gehörende Datenmarktplatz mehr als 650.000 Zielgruppensegmente im Angebot hatte. Zu den auswählbaren Kategorien zählen der Studie zufolge „Menschen, die beim Militär arbeiten“, „Menschen, die bei Rüstungskonzernen arbeiten“, Richter:innen, Politiker:innen und andere sicherheitsrelevante Personen in der EU. Wenn jemand Zugriff auf diese Daten hat, kann sie nutzen, um Personen unter Druck zu setzen. Wie genau das aussehen kann, verdeutlichen die Autor:innen an einem Beispiel aus den Vereinigten Staaten. 2021 wurde ein Priester mithilfe von Daten unfreiwillig geoutet, die über ihn bei Datenhändler:innen erstanden wurden. Der Mann verlor seinen Job. Ein Artikel der Washington Post stellte in diesem Jahr fest, dass eine Gruppe konservativer Katholiken aus Colorado Millionen von Dollar ausgab, um homosexuelle Priester bloßzustellen. <h3>Ein Datenleck unbekannten Ausmaßes</h3> Damit Werbeanzeigen auf Zielgruppen zugeschnitten werden können, sammeln die beteiligten Firmen riesige Mengen Daten über die Online- und Offline-Aktivität von Menschen. Wann immer eine Person eine Website oder App nutzt, die Targeted Advertising ermöglicht, findet eine automatisierte Auktion statt. Innerhalb weniger Millisekunden werden in einem Zusammenspiel mehrerer Plattformen die Nutzer:innen von Websites und Apps erkannt und anhand ihrer Eigenschaften als Zielgruppe ausgewiesen. Noch bevor die Website oder App geladen hat, wird der Werbeplatz unter allen Firmen versteigert, die diesen Personen eine Anzeige ausspielen wollen. Weil es so schnell ist, wird das Verfahren Real-Time-Bidding (RTB) genannt. Bei jeder Auktion werden RTB-Daten der Nutzer:innen an hunderte Firmen übertragen. Dazu zählen etwa Identifier, Aufenthaltsorte und Uhrzeiten, die es laut ICCL ermöglichen, Personen zu identifizieren. Möglich ist das Ausnutzen von Online-Werbung demnach, weil es in diesem Ökosystem kaum Kontrollen gebe, wohin die Daten fließen und wer an den Auktionen teilnimmt. Eine der wichtigsten Schnittstellen im Werbesystem ist Google. Der Studie zufolge lässt Google auch Unternehmen aus Russland und China am Werbesystem teilnehmen, sodass die Daten auch dorthin fließen könnten. Dem Bericht zufolge ist das ein Anlass zur Sorge, denn die dortigen Gesetze ermächtigen die Sicherheitsbehörden auf die Daten zuzugreifen, sobald sie im Besitz von heimischen Unternehmen sind. Auf Nachfrage des Spiegels widerspricht Google den Vorwürfen. Die Zusammenarbeit mit Geschäftspartner:innen aus Russland sei seit 2022 eingestellt. Zudem würden bei den Auktionen keine Informationen übertragen, die es direkt ermöglichen, konkrete Personen zu identifizieren. Man habe die Geschäftsbeziehungen zu Datenhändler:innen gekündigt, die sich nicht an diese Bedingungen in der Vergangenheit gehalten haben. <h3>Advertising Intelligence</h3> Dass die im Report skizzierten Risikoszenarien nicht bloße Theorie sind, das belegen die Autor:innen unter anderem mit dem Beispiel <a href=„https://web.archive.org/web/20231003181009/https:/sovsys.co/wp-content/uploads/2020/04/PA

TTERNZ-NATIONAL-SECURITY-PATTERN-DETECTION.pdf“>eines Überwachungswerkzeugs namens Patternz. Laut eigenen Angaben der israelischen Firma ISA Security mit Hauptsitzt in Kokhav Ya’ir konnte sie in den letzten fünf Jahren mithilfe von RTB-Daten 5 Milliarden Nutzer:innenprofile erstellen. Die Datensätze würden unter anderem die GPS-Daten der Zielpersonen und sogar Informationen über ihre Kinder enthalten. Dass das unkontrollierte Werbesystem ein Sicherheitsrisiko darstellt, darauf wiesen in diesem Jahr bereits mehrere Organisationen hin. Erst kürzlich veröffentlichen Forscher:innen in den USA eine Studie, die darauf aufmerksam macht, wie einfach bei US-Datenhändler:innen Informationen über Soldat:innen erworben werden können. Zuvor hatte die israelische Zeitung Haaretz in einem umfassenden Insider-Bericht aus der Branche der Überwachungsfirmen aufgedeckt, dass einige Akteure das Ökosystem der Online-Werbung bereits lange infiltriert haben. Der Zeitung zufolge nutzen sie es nicht nur für das Ausspionieren von Zielpersonen, sogenannte Advertising Intelligence, sondern auch für das Ausspielen von Schadsoftware. Die ICCL betont in ihrem Bericht, dass nicht immer klar ist, wie sehr die Überwachungsfirmen in ihrer Selbstvermarktung übertreiben. Dennoch sei das Sicherheitsrisiko, das vom unkontrollierten Online-Werbe-System ausgehe, gravierend. Die Autor:innen sind sich sicher, RTB-Daten ermöglichen ausländischen Staaten und nichtstaatlichen Akteuren die Bewegungen und Online-Aktivitäten von hochrangigen Zielpersonen zu verfolgen. Die Bürgerrechtler:innen fordern deshalb ein entschiedenes Handeln von den USA und Europäischer Union. Unter anderem müssten sich der Europäische Datenschutzausschuss und die EU-Agentur für Cybersicherheit des Themas annehmen und Untersuchungen starten. </html>