Wir über uns

Das Bundesamt für Sicherheit in der Informationstechnik als die nationale Cyber-Sicherheitsbehörde gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.

Wir sind der zentrale IT-Sicherheitsdienstleister des Bundes. Wir sind für IT-Sicherheit in Deutschland verantwortlich. Grundlagen unserer Arbeit sind Fachkompetenz und Neutralität.

Bundesamt
für Sicherheit in der
Informationstechnik

Kontaktieren Sie uns

Bundesamt für Sicherheit in der Informationstechnik

Postfach 200363
53133 Bonn
Telefon: 0228 99 9582-0

bsi@bsi.bund.de

Tracking auf Smartphones mit Gegenmaßnahmen

Gegenmaßnahmen zu Canvas Fingerprinting

Canvas Fingerprinting lässt sich insgesamt nur schwer verhindern, wenn man nicht auf viele gestalterische Möglichkeiten im Webbrowser verzichten möchte.

Dennoch kann man das Tracking etwas erschweren, indem man einige kleine Tipps beachtet:

Eine Möglichkeit ist das komplette Abschalten von JavaScript oder extern nachgeladenen Skripten, jedoch schränkt das auch die Praxistauglichkeit für den Anwender ein.

Eine andere, unabhängige Aufklärung über das Tracking liefert die Chrome-Erweiterung Chameleon: Das Tool meldet, sobald Canvas Fingerprinting auf der aktuell besuchten Webseite eingesetzt wird.

Die Firefox-Erweiterung NoScript erlaubt das Ausführen von JavaScript und anderen Plugins ausschließlich für vertrauenswürdige Seiten.

Einen gewissen Schutz bietet der TOR-Browser, er weist auf die Canvas-Bilddaten von Websites hin.

Komplett verhindern lässt sich Canvas Fingerprinting mit Adblock Plus. Die Übermittlung der Canvas-Grafik wird blockiert, sobald die Filterliste "EasyPrivacy" abonniert ist. Adblock Plus verhindert durch die Erweiterung zwar nicht das Anfertigen des Fingerprints, blockiert aber die Übertragung an die Webseiten-Betreiber.

Was ist Canvas Fingerprinting?

Canvas Fingerprinting ist ein Tracking-Modell, das verschiedene Parameter verwendet, um einen Nutzer beim Surfen zu identifizieren. Beim Canvas Fingerprinting werden die relativ einzigartigen Merkmale des Smartphones des Nutzers verwendet, um ein sogenanntes Canvas-Bild zu erzeugen, welches einen kurzen Text enthält. Das Bild wird im Hintergrund geladen und nutzt dazu die Systemkonfigurationen des Anwenders. Daraufhin werden Nutzern eindeutige, personenunabhängige Identifikationsnummern zugewiesen. Mithilfe dieser können Anwender beim Besuch einer Website, die ebenfalls die Canvas-Tracking-Methode verwendet, identifiziert werden.

Was ist Ultraschall-Tracking?

Es wurden 234 Android-Apps entdeckt, die im Hintergrund und ohne Zustimmung von Usern deren Nutzungsverhalten per Ultraschall verfolgen. Die als Ultrasound Cross-Device Tracking (uXDT) bezeichnete Technik, ist in der Lage, Informationen über benutzte Apps, besuchte Orte und sogar aufgerufene Websites zu sammeln.

Die Apps machen sich den Umstand zunutze, dass Lautsprecher – auch die eines Smartphones – Töne im Ultraschallbereich ausgeben können, die für das menschliche Ohr unhörbar sind. Zudem können die Mikrofone mobiler Geräte Ultraschall-Töne aufzeichnen. Die Technik lässt sich aber auch auf Einzelhandelsgeschäfte oder Werbeplakate ausweiten.

Eine entsprechende Empfangs-App auf dem Handy vorausgesetzt, könnte eine Online-Werbung damit beispielsweise einen Cookie auf dem Gerät setzen. Dann wüssten Werbetreibende, dass Desktop und Smartphone von derselben Person genutzt werden.

Generell ist das Ultraschall-Tracking eine Bedrohung für die Privatsphäre, da es unbemerktes Tracking von Standorten, Verhalten und Geräten erlaubt. Zudem können Nutzer nicht erkennen, welche Apps auf Ultraschallsignale aus ihrer Umgebung warten.

Konkret wird die Technik beispielsweise benutzt, um standortbezogene Werbung wie Rabattcoupons oder Gutscheine anzuzeigen. Werbung lässt sich demnach über die Ermittlung des Standorts eines Nutzers, seines Verhaltens und sogar seiner Kaufgewohnheiten optimieren, die sich ebenfalls per Ultraschall ausspähen lassen.

Einen gewissen Schutz bietet der TOR-Browser, er weist auf die Canvas-Bilddaten von Websites hin.

Gegenmaßnahmen zu Ultraschall-Tracking

Der einzige mögliche Hinweis auf das Tracking ist die Berechtigung für den Zugriff auf das Mikrofon. Nutzer, die sich vor derartigen Bedrohungen schützen wollen, sollten in den Einstellungen ihres Smartphones die App-Berechtigungen überprüfen. Beispielsweise Nachrichten-Apps oder Spiele sollten keinen Zugriff auf das Mikrofon benötigen.