20.11.2017 – 14:54 Uhr

Im Netz der Datensammler: Zehn schockierende Mythen rund ums Surfen im Internet

---

Weitere Informationen
http://ots.de/ls7xa

Hamburg (ots) -

Die stille Gefahr des Sammelns von Profildaten im Internet
Wie Persönlichkeitsprofile gar nicht erst entstehen

Wie würden Sie reagieren, wenn die Dame an der Supermarktkasse über Ihre Probleme beim Wasserlassen bescheid weiß? Oder der Metzger von nebenan über Ihre finanziellen Engpässe? Wahrscheinlich empört. In Zeiten des Internets ist es inzwischen jedoch ganz normal, dass Unternehmen und andere Organisationen bestens über private Dinge informiert sind. Denn bei jedem Ausflug ins Web hinterlassen Nutzer unbemerkt Spuren, die sich zu detaillierten Persönlichkeitsprofilen verdichten lassen. Diese Nutzerprofile können Informationen über Gesundheitszustand, politische Gesinnung oder sogar sexuellen Vorlieben enthalten. "Meine Daten sind sicher!" - Ein weit verbreiteter Irrtum. Genau wie andere Mythen, die sich in den Köpfen vieler Internet-Nutzer verankert haben. eBlocker erläutert die zehn wichtigsten Mythen.

Mythos 1: Die Daten sind in guten Händen
Die Erfahrung lehrt uns, dass gesammelte Daten fast immer früher oder später missbraucht werden. Selbst in den Händen von großen "seriösen" Unternehmen sind sie alles andere als sicher. Egal ob Postbank, Telekom, Sony oder sogar der deutsche Bundestag: Missbrauchsfälle von Verbraucherdaten gibt es immer wieder. Ursächlich ist meist der schlechte Schutz. So geraten Namen, Adressen, Geburtsdaten, Anmeldedaten und sogar Kontonummern millionenfach auf den lukrativen Schwarzmarkt für persönliche Daten. Hinzu kommt: Jedes US-Unternehmen muss die Dateien seiner Kunden herausrücken, wenn Geheimdienste wie die NSA anklopfen.

Mythos 2: Es werden sowieso nur "anonyme" Metadaten gesammelt
Datensammler sind besonders gierig auf sogenannte Meta- oder Verkehrsdaten. Dabei handelt es sich nicht um konkrete Inhalte, sondern vielmehr um Informationen, die Rückschlüsse auf ein bestimmtes Verhalten zulassen. Beispielsweise wann eine Person eine bestimmte Internetseite besucht hat. Mithilfe von Analysen lassen sich dann erstaunlich detaillierte Informationen erlangen. Eine Studie der Universität Stanford zeigte: Allein durch die Auswertung von Metadaten waren die Forscher über bestimmte Krankheiten und den Drogenkonsum freiwilliger Probanden im Bilde. Dazu kommt: Ein genaues Persönlichkeitsprofil lässt sich mit ausgeklügelten Algorithmen anhand von Metadaten jedes Internet-Nutzers bilden und eindeutig einer Person zuordnen.

Mythos 3: Tracking ist böse
Nicht immer. Techniken, die das Verhalten von Surfern auswerten, dienen oft zur Verbesserung von Internetseiten. So kann etwa ein Shop-Betreiber Probleme erkennen und so seine Website optimieren. Jedoch ist es eher die Regel als die Ausnahme, dass der Nutzer vermeintlich kostenlose Webseiten-Betreiber mit seinen Daten bezahlt. Einer dieser schwarzen Schafe unter den Trackern ist Google Analytics, wo es allein ums Abgreifen persönlicher Daten geht. Tracker wie Google Analytics verfolgen Surfer über sämtliche Websites und Geräte hinweg und erstellen so detaillierte Persönlichkeitsprofile. Beispiel: Wenn sich ein Nutzer etwa morgens über "Migräne" informiert, nachmittags nach örtlichen Ärzten sucht und abends "Spezialklinken für Hirntumore" recherchiert, weiß das Unternehmen genau Bescheid. Dieses Wissen verkauft es gewinnbringend an Werbekunden und andere Dritte.

Mythos 4: Persönlichkeitsprofile entstehen nur am Windows-PC

Der PC steht in der IT-Welt für das Sicherheitsrisiko schlechthin: Viren, Ransomware und Banking-Trojaner? Immer trifft es gefühlt Windows-Computer. Für Datensammler spielt es aber keine Rolle, mit welchem Gerät Nutzer ins Web geheb. Egal ob PC, Mac, Smart-TV, Spielekonsole, Tablet oder Handy, alle gesammelten Daten werden Geräte-übergreifend miteinander verknüpft und zu detaillierten Persönlichkeitsprofilen verdichtet.

Mythos 5: Apps sind harmloser als Internetseiten
Das Gegenteil ist der Fall - Apps sind noch viel schlimmer. Denn im Vergleich zum Browser können sie proprietäre Protokolle zum Datenaustausch nutzen, um Schutzfunktionen wie Firewalls auszutricksen. So genießen sie oft zusätzlich Zugriff auf Positionsdaten, Kamera, Kalender und Kontakte. Das geschieht oft ohne Einwilligung des Nutzers. Obendrein lassen sich Daten über Kennziffern eindeutig einer bestimmten Person zuordnen. Zwielichtige App-Entwickler freut's; Sie sammeln fleißig vertrauliche Daten, übermitteln die ungefragt an Dritte und machen kräftig Kasse.

Mythos 6: Gütesiegel schützen vor Datensammlern
Gütesiegel wie "Trusted Shops" oder "TÜV-Süd" suggerieren: Hier sind Kunden sicher. Das gilt aber nicht unbedingt für den Datenschutz. Wer auf einer Shop-Seite etwa Name, Anschrift und Email-Adresse eintippt, muss dem Betreiber vertrauen, dass dieser sich an die geltenden Datenschutzbestimmungen hält. Tests haben gezeigt, dass sich nicht alle daran halten. Hinzu kommt, dass Gütesiegel nichts darüber aussagen, welche Anbieter Nutzerdaten gewinn¬bringend weiterverkaufen.

Mythos 7: Cookies sind gefährlich
Cookies haben einen schlechten Ruf, doch tatsächlich nutzen professionelle Datensammler inzwischen ganz andere Werkzeuge. Der oft gut gemeinte Rat, Cookies generell abzuschalten, ist nicht nur ineffektiv in Puncto Datenschutz, sondern geht auch noch zu Lasten des Komforts: Internet-Seiten speichern dadurch keine Anmeldedaten, Warenkörbe oder Einstellungen mehr.

Mythos 8: Ich habe nichts zu verbergen
Wer soll schon etwas mit meinen Daten anfangen? Die interessieren doch keinen. Außerdem habe ich sowieso nichts zu verbergen. Zu sicher sollte man sich nicht sein. Ist für Krankenkassen etwa nicht der Gesundheitszustand von potentiellen Neukunden interessant? Oder für die Bank die Spielsucht? Oder für den Scheidungsanwalt die Anmeldung bei einem Seitensprungportal? Oder einem potenziellen Arbeitgeber die Mitgliedschaft in der Gewerkschaft?

Mythos 9: Daten sammeln dient der Sicherheit
Nicht nur Unternehmen, auch Geheimdienste setzen auf Profildaten. Das verbessere die Sicherheit, etwa vor Terroranschlägen, so der Irrglaube. Die Argumentation lautet oft: Wenn nichts passiert, dann haben wir das der guten Überwachung zu verdanken. Nach einem Anschlag werden dann die Forderungen nach noch mehr Überwachung lauter. Doch wie verhältnismäßig ist diese Forderung, wenn man bedenkt, dass das Risiko, an einer Pilzvergiftung oder im Straßenverkehr zu sterben, weitaus höher liegt als bei einem Terroranschlag?

Mythos 10: Ich kann nichts gegen die Datensammelwut tun
Das Internet generell zu verteufeln, ist keine Lösung. Die gute Nachricht: Schützen ist ganz einfach. Möglich macht's der eBlocker. An den Router angedockt, ist die kleine Box in wenigen Minuten einsatzbereit und kontrolliert den gesamten Internet-Datenverkehr. So kann sie bei allen angeforderten Seiten sämtliche Datenerfassungsdienste, Tracker und Werbung effektiv herausfiltern. Und das Beste: Der Schutz wirkt auf allen internettauglichen Geräten, egal ob Computer, Smartphone, Tablet oder Spielekonsole. Infos gibt's unter www.eblocker.com.

Über die eBlocker GmbH
Nach zweijähriger Vorbereitung im Stealth Mode ging 2015 die eBlocker GmbH mit Sitz in Hamburg an den Start. Das gleichnamige Produkt

eBlocker ist die nutzerfreundliche Lösung für die Kontrolle über die eigenen Daten auf allen Endgeräten. Das multi-user-fähige Gerät stellt die verloren gegangene Privatsphäre im Internet wieder her, lässt den Nutzer vollkommen anonym surfen und blockiert Daten sammelnde Online-Werbung. Dank einfachem Anschluss an das Heimnetzwerk, automatischer Konfigurierung und Software-Updates ist der eBlocker auch für technisch unerfahrene Nutzer unkompliziert einsetzbar. So schützt er im Handumdrehen private Daten und Surfprofile über alle Endgeräte hinweg: Computer, Tablet, Smart-TV sowie jegliche im Heimnetzwerk angeschlossene Geräte sind effektiv vor Datenspionage geschützt. www.eblocker.com

Kontakt:

Griffel & Co. Kommunikation GmbH
Ulrike Voß
Forsmannstraße 8b
22303 Hamburg, Germany
Email: de-press@eblocker.com
Telefon: +49 40 6094586 00