06.12.2017 – 15:14 Uhr

"Bin ich schon im Darknet?" "Braucht das nicht nur Edward Snowden?" - Sechs Irrtümer rund um IP-Anonymisierung

---

www.eBlocker.com
http://ots.de/jcU1o

Hamburg (ots) -

Jeder Internetausflug hinterlässt Spuren, mit denen sich Nutzer eindeutig identifizieren lassen. Denn bei der Einwahl wird dem Router eine weltweit einmalige Zahlenkombination zugeteilt, die IP-Adresse. So lässt sich selbst Wochen später herausfinden, wann und mit welcher IP-Adresse eine Internetseite besucht wurde. Dabei kann nicht nur jeder Seitenbetreiber leicht herausfinden, in welcher Region der Nutzer lebt und über welchen Internetanbieter er ins Netz geht. Auch Google, Facebook, NSA und Cyberkriminelle wollen wissen, wer was im Internet unternimmt. Das Dumme ist: Fast alle machen es ihnen leicht. Viele besuchen sozusagen mit dem Personalausweis auf die Stirn getackert abenteuerliche Seiten, googlen nach schweren Krankheiten und erkundigen sich munter nach Krediten oder Seitensprüngen. Dabei ist es heute ganz einfach möglich, die IP-Adresse zu anonymisieren. Für Datensammler sieht es dann so aus, als käme ein deutscher Surfer zum Beispiel aus einer Kleinstadt in den USA. Und neben verbesserter Sicherheit hat das Surfen mit Tarnkappe weitere angenehme Nebeneffekte. So lassen sich etwa Internetdienste nutzen, die für Kunden aus anderen Ländern eigentlich gesperrt sind, etwa Videodienste oder Sportsender. Doch nur die Wenigsten nutzen die Vorteile der Anonymität, denn es kursieren viele Missverständnisse rund um dieses Thema.

Irrtum 1: Meine IP-Adresse wird doch sowieso regelmäßig geändert

Was stimmt: Dynamische IP-Adressen kommen bei fast allen privaten Internet-Anschlüssen zum Einsatz. Theoretisch können sie sich also immer wieder ändern. Das geschieht spätestens, wenn sich der Router neu mit dem Internet verbindet. Im Gegensatz zu früher geschieht das aber immer seltener. Die ehemals übliche "Zwangstrennung", bei der der Provider einmal pro Tag die Verbindung kurz kappte, ist im Prinzip Geschichte. Sie kommt nur noch bei Analog- und ISDN-Anschlüssen zum Einsatz. Bei modernen DSL- und Kabelanschlüssen verzichten die meisten Provider darauf, da in diesem Fall auch der Telefonanschluss von der Trennung betroffen wäre. Das bedeutet, dass es in vielen Fällen nur noch bei einem Router-Neustart eine andere IP-Adresse gibt. Oder, wie im Fall der Deutschen Telekom, spätestens nach 180 Tagen. Die meisten Nutzer sind also in der Regel wochen- oder sogar monatelang anhand ihrer IP-Adresse eindeutig identifizierbar. Dazu kommt: Selbst dynamische Adressen schützen nicht vor Rückverfolgung. In Deutschland existieren rechtliche Möglichkeiten, um Anschlussinformationen vom Provider zu erlangen und so problemlos die Identität eines Internet-Nutzers zu ermitteln.

Irrtum 2: Ich brauche das nicht

Natürlich - nicht jeder muss oder will im Internet anonym sein. Wer zum Beispiel auch auf offener Straße seine Krankheiten herausposaunt, der Kreditbank freimütig über seine Spielleidenschaft berichtet oder auf jeder Party frisch von der Leber jedem seine sexuellen Neigungen auf die Nase bindet, kann getrost auch im Web auf Privatsphäre verzichten. Wer nicht zu dieser Gruppe gehört, sollte dagegen auf der Hut sein. Inzwischen lauert eine riesige Industrie auf im Web unbemerkt preisgegebene Surfprofile jedes Einzelnen. Diese wertet die Daten aus und verdichtet sie zu detaillierten Persönlichkeitsprofilen. Und jeder Besuch im Internet hinterlässt eine Menge Spuren. Durch die IP-Adresse erfahren Seitenbetreiber etwa den ungefähren Wohnort und die Internetbandbreite. Nur durch eine wirksame Kombination aus IP-Anonymisierung plus weiterer Schutzmaßnahmen behalten Nutzer die volle Hoheit über ihre Daten.

Irrtum 3: Ich nutze Browser-AddOns wie Ghostery und Adblock. Das reicht als Schutz

Tatsächlich blocken derartige Browser-Erweiterungen Tracker, Cookies und Social Media-Schaltflächen, die das Surfverhalten ausspionieren. Sie verbessern somit nicht nur die Privatsphäre, sondern verringern auch das Werbeaufkommen. Die Sache hat aber mehrere Haken:

- Schützt nur den Browser: Browser-Erweiterungen schützen logischer Weise nur den Browser selbst, nicht aber den PC generell und noch weniger andere internetfähige Geräte im Netzwerk.
- Blocken nicht alles: Derartige AddOns schützen zwar passabel vor Trackern und Werbung, vollkommen anonymes Surfen ermöglichen sie aber nicht.
- Verbindungen zur Werbeindustrie: Egal ob Web of Trust oder Ghostery. Nicht nur einmal entpuppten sich die Dienste hinter den Erweiterungen selbst als Datenschleudern. Die Erweiterung blockt zwar viele Tracker, sammelt aber gleichzeitig fleißig Daten und verkauft diese an Werbefirmen.

Irrtum 4: Anonymes Surfen ist lahm

Beim Einsatz des kostenlosen Tor-Netzwerks ist an dieser These zweifelsohne etwas dran. Schließlich müssen die Anfragen erst über mehrere Proxy-Server laufen, bis sie beim Empfänger landen. Das macht den Dienst zwar sicher, für's tägliche Surfen aber nahezu unbrauchbar. Denn die Geschwindigkeit beim Seitenaufbau sowie beim Herunterladen und Abspielen von Videos leidet deutlich unter dem Anonymi-sierungsprozess. Deutlich flotter läuft es dagegen mit kommerziellen VPN-Diensten. Denn in diesem Fall müssen die Daten nur den Umweg über die Server-Infrastruktur des VPN-Anbieters nehmen. Wenn die genügende Bandbreite zur Verfügung steht, liegt die Geschwindigkeit nahe am Maximaltempo der Internetleitung.

Irrtum 5: Wenn ich das Tor-Netzwerk nutze, lande ich gleich im Darknet

Genauso korrekt wäre die Aussage, dass jeder Surfer im Internet automatisch auf Pornoseiten landet. Richtig ist: Über das Tor-Netzwerk ist der Zugang zum Darknet möglich. Wer aber nicht ins Darknet will, wird auch nicht dort landen. Darüber hinaus gibt es Mittel und Wege, die Wege ins Darknet zu blockieren. Mit dem eBlocker beispielsweise ist die Privatsphäre des Internetnutzers geschützt, indem das Gerät zur Anonymisierung der IP-Adresse auf Tor zurückgreift. Allerdings erlaubt der eBlocker keinen Zugriff auf Darknet-Domains. Wer trotzdem hineinwill, muss diese Schranken aktiv umgehen.

Irrtum 6: Das ist doch alles viel zu kompliziert

Es kommt darauf an: Wer tatsächlich jedes einzelne internettaugliche Gerät im Haushalt einzeln anonymisieren will, steht vor einer nahezu unlösbaren Mammutaufgabe. Denn Plug-Ins oder VPN Software funktionieren beispielsweise nicht auf Smart-TVs, Spielekonsolen oder IoT-Geräten. Einfacher macht es der eBlocker. Angeschlossen ans Heimnetzwerk, anonymisiert der kleine Kasten das Online-Verhalten sämtlicher internetfähiger Geräte im Netzwerk. Er schützt neben dem Computer also auch Tablets, Smart-TVs, Spielekonsolen und IoT-Geräte, für die es bislang kaum Möglichkeiten zum Schutz der Privatsphäre gibt. Die IP-Anonymisierung wird wahlweise durch das Tor-Netzwerk oder per VPN-Anbieter gelöst. Darüber hinaus blockt der eBlocker zuverlässig alle Tracker und die datensammelnde Werbung. Dank dieser Kombination bietet der eBlocker erstmals einen umfangreichen Schutz der Privatsphäre auf Netzwerkebene - ganz ohne Softwareinstallation.

Über die eBlocker GmbH

Nach zweijähriger Vorbereitung im Verborgenen ging 2015 die eBlocker GmbH mit Sitz in Hamburg an den Start. Deren Produkte eBlocker Pro und eBlocker Family geben Privatpersonen die Kontrolle über ihre ungewollt während des Surfens im Internet preisgegebenen Informationen zurück. So erhalten die Nutzer wieder die Hoheit und volle Kontrolle über Ihre Daten. Der eBlocker Family verfügt zusätzlich über Jugendschutzfunktionen, über die sich unter anderem Web-Inhalte und Surfdauer beschränken lassen. Unmittelbar nach Anschluss des eBlockers blockiert er effektiv sämtliche Tracker und datensammelnde Werbung, anonymisiert die IP- Adresse und lässt alle Nutzer vollkommen anonym surfen. Der eBlocker schützt dabei sämtliche Geräte im Heimnetz per Plug&Play, ohne zusätzliche Softwareinstallation. Dank einfachem Anschluss, automatischer Konfigurierung und täglichen Software-Updates ist der eBlocker auch für technisch unerfahrene Nutzer schnell und unkompliziert einsetzbar.
www.eBlocker.com

Kontakt:

Griffel & Co. Kommunikation GmbH
Forsmannstraße 8b

22303 Hamburg, Germany
Email: de-press@eblocker.com Telefon: +49 40 6094586 00

Medieninhalte

Anonym surfen? So geht das! Weiterer Text über ots und www.presseportal.de/nr/128614 / Die Verwendung dieses Bildes ist für redaktionelle Zwecke honorarfrei. Veröffentlichung bitte unter Quellenangabe: "obs/eBlocker GmbH/Copyright: eblocker 2017"

Intimste Leidenschaften mit jedem teilen? Weiterer Text über ots und www.presseportal.de/nr/128614 / Die Verwendung dieses Bildes ist für redaktionelle Zwecke honorarfrei. Veröffentlichung bitte unter Quellenangabe: "obs/eBlocker GmbH/Copyright: eblocker 2017"