

EBLOCKER PRO

Tarnkappe fürs Netz

Smarter Werbeblocker und engagierter Hüter der Privatsphäre: Der eBlocker verwischt Spuren im Netz und schlägt Trackern ein Schnippchen. Und erfordert dabei so gut wie keine Aufmerksamkeit.

Hand aufs Herz: Niemand mag gern Werbung auf Webseiten. Weshalb knapp 20 Prozent der deutschen Internetnutzer laut einem Quartalsbericht des „Bundesverband Digitale Wirtschaft“ (BVDW) einen sogenannten Adblocker nutzen, der lästige Werbeeinblendungen eliminiert. Der offensichtlichste Nachteil einer softwarebasierten Plug-in-Lösung: Smartphones und Tablets, aber auch Smart-TVs, Set-Top-Boxen und Spielkonsolen bleiben häufig außen vor.

Der Internetnutzer als offenes Buch

Die auf einer Webseite sichtbare Werbung stellt indes nur die Spitze des Daten-Eisbergs dar: Unter der Oberfläche greifen ausgeklügelte Tracking-Systeme ungeniert nach der Privatsphäre des Besuchers. Im Durchschnitt werkeln zwischen zehn und zwanzig Tracker im Hintergrund, um Informationen über das Konsumverhalten zu gewinnen und daraus ein möglichst feinmaschiges Persönlichkeitsprofil zu weben. Dabei gilt: Wer eine Webseite besucht, den erfassen ihre verborgenen Algorithmen auch. Denn immerhin muss jeder Nutzer deren Deaktivierung nachträglich selbst vornehmen – wenn er sich dieser Möglichkeit überhaupt bewusst ist. Hinzu kommen Geräte, die in der öffentlichen Wahrnehmung als eifrige „Datenbienen“ bisher kaum vorkommen: Laut einer Studie greifen die aktuellen Smart-TVs von Samsung ständig personenbezogene Daten wie die IP-Adresse, zur App-Nutzung und den Senderverlauf ab.

Smarter Würfel mit Liebhaf-Faktor

Der eBlocker des gleichnamigen Hamburger Start-ups nimmt sich somit der beiden brennendsten Probleme der Internetnutzer an: Die kleine weiße Box in der Größe eines Rubik-Zauberwürfels fungiert als zuverlässiger Werbeblocker, anonymisiert das Anwenderverhalten und schiebt Trackern sowie anderen Datenschnüfflern einen Riegel vor. Kurzum: Der eBlocker will seinem Besitzer das gute Gefühl der gewährten Privatsphäre zurück in dessen Hände legen. Und das geräteübergreifend: Einmal installiert, schützt das smarte Device mit Liebhaf-Faktor

nicht nur per Kabel am Router angeschlossene Macs vor Werbung und allzu neugierigen digitalen Blicken, sondern auch per WLAN am Netzwerk partizipierenden iPhones, iPads und natürlich Tablets, Spielkonsolen, Set-Top-Boxen, Smart-TVs und alle erdenklichen Geräte anderer Hersteller und Betriebssystemanbieter.

Apropos Installation: Die ist denkbar einfach und belegt nicht mal eine der so wertvollen Schnittstellen am Mac. Den eBlocker schließen Sie mit einem beiliegenden Netzwerkkabel direkt an einem freien LAN-Port des Routers an, der autarke weiße Würfel richtet sich innerhalb von Minuten selbst ein und hält sich zudem mit der neuesten Firmware stets aktuell. Ein weiteres Kabel entfällt auf den Stromanschluss. Zusätzliche Software auf den Endgeräten? Fehlanzeige und komplett überflüssig. Eine Anpassung an die eigene Daten-Freigebigkeit erfolgt – ähnlich wie bei einem Router – im Webbrowser.

Praxis

Im Praxistest arbeitete der eBlocker als zuverlässiger Werbeblocker, was besonders auf einem iPad für ein entspanntes Surferlebnis sorgt. Wo vorher noch Pop-ups und Banner das Lesen auf Webseiten allzu oft verdarben, herrscht nun endlich Ruhe. Hinzu kommt das gute Gefühl, Tracker noch vor dessen Datenabgriff ausgetrickt zu haben. Zudem verwischt das smarte Device die IP-Adresse, sodass Sie keine digitalen Fingerabdrücke mehr im Netz hinterlassen. Browserbasierte Erweiterungen wie AdBlock

**Wussten Sie schon,**

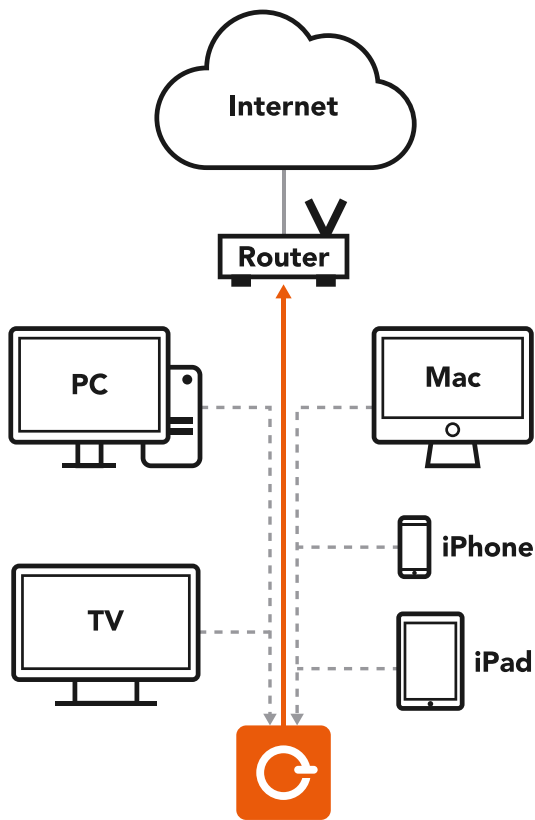
... dass Online-Anbieter Ihr Surfverhalten auf jeder besuchten Webseite und über alle Endgeräte hinweg verfolgen? So entstehen genaue Persönlichkeitsprofile, die sogar intimste Details über Sie verraten.

... dass Online-Shops Ihre Kaufkraft auf Basis des verwendeten Endgeräts prognostizieren, um so Angebot und Preise entsprechend anzupassen? Das Ergebnis: Benutzen Sie etwa ein teures iPad Pro, bezahlen Sie für ein Produkt eventuell mehr als ein Android-Nutzer.

... dass Kreditanbieter Ihr Onlineverhalten für Bonitätsbewertungen heranziehen? Frequentieren Sie etwa Seiten von Wettanbietern, kann sich dies negativ auf Ihre Kreditaussichten auswirken.

... dass softwarebasierte Werbeblocker wie etwa AdBlock Plus zwar Werbung ausschließen, nicht aber das Sammeln Ihrer persönlichen Daten?

... dass knapp 20 Prozent aller Internetnutzer Adblocker und Privacy-Erweiterungen mit Virenschutzprogrammen verwechseln und sich so fälschlich sicher fühlen?



Der eBlocker findet an einem freien LAN-Port des Routers Anschluss und schützt alle am Netzwerk partizipierenden Geräte vor neugierigen Blicken und unerwünschter Werbung.

Plus, Facebook Disconnect und Ghostery sind somit überflüssig – was sich nicht zuletzt auch auf die Surfgeschwindigkeit positiv auswirkt. Interessant ist auch die „Gerätetarnung“: Damit gibt sich etwa Ihr Mac als Windows- oder Linux-Rechner aus, um Datensammler rotzfrech in die Irre zu führen und eine Beurteilung der eigenen Kaufkraft anhand der verwendeten, zumeist wertigeren Apple-Hardware, zu verhindern (siehe Kasten).

Auf Wunsch weist der eBlocker auf bereits lauernde Tracker hin – vertraut man also einem Webseitenanbieter oder Webshop so weit, dass eine Protokollierung des eigenen Kaufverhaltens bewusst gewünscht wird, um später maßgeschneiderte Produkthinweise zu erhalten, bleibt die Entscheidung pro oder contra Erfassung beim Nutzer selbst. Zudem können Sie eine „Weißliste“ mit erlaubten Webadressen anlegen und einzelne Geräte gezielt von der Anonymisierung ausnehmen. Dabei bleiben alle Daten auf der Box und somit in den eigenen vier Wänden – eine Übertragung etwa in einen Cloud-Speicher des Herstellers entfällt. Auch die Datenverarbeitung selbst erfolgt komplett in der lokalen Lösung.

Fazit

Einfache Installation und Handhabung, ein extrem verbessertes Nutzererlebnis durch den Wegfall von Werbung und ein nachhaltiger Schutz der Privatsphäre auf allen Geräten im Netzwerk – das eBlocker-Debüt ist rundum gelungen. ◀

eBlocker Pro

- kompatibel mit allen Betriebssystemen, Geräten und Browsern
- keine Softwareinstallation
- blockiert Tracker und datensammelnde Werbung
- IP-Anonymisierung
- Gerätetarnung
- Vorab-Schutz vor Ausspionierung
- schützt mobile Datenverbindungen (ab Ende 2016)
- Ein gemeinsames Nutzerkonto
- ab 219 Euro

eBlocker Family (ab 2017)

- kompatibel mit allen Betriebssystemen, Geräten und Browsern
- keine Softwareinstallation
- blockiert Tracker und Daten sammelnde Werbung
- IP-Anonymisierung
- Gerätetarnung
- Vorab-Schutz vor Ausspionierung
- schützt mobile Datenverbindungen
- Multinutzerfähig mit zehn individuellen Konten
- Jugendschutzfunktion
- ab 249 Euro

www.eblocker.com

3 FRAGEN AN ...

Christian Bennefeld, eBlocker-Erfinder

Christian, warum reicht für die Unterdrückung von Werbung nicht einfach die Installation eines Werbeblockers im Browser – und für den Schutz der Privatsphäre ein Plug-in wie „Disconnect“?

Alle auf Software basierenden Werkzeuge haben den großen Nachteil, dass sie nicht auf sämtlichen Geräten funktionieren. In der Regel kann man diese Plug-ins beispielsweise auf Smart-TVs, der Xbox oder einem iPad nicht installieren. Zudem leiten Cloud-Dienste wie Disconnect alle aufgerufenen URLs an zentrale Server in die USA, die anhand der URLs ein Persönlichkeitsprofil erstellen könnten. Als NSA oder Hacker würde ich genau bei diesen zentralen Diensten angreifen.

Lässt sich nicht letztlich auch der eBlocker hacken?

Sony wurde gehackt, der Bundestag, Walmart – und auch Apples App Store. Niemand kann eine hundertprozentige Sicherheit garantieren – auch wir nicht. Da der eBlocker aber eine vollständig lokale Lösung darstellt, auf die wir gar keinen Zugriff haben, muss der Angreifer einen hohen Aufwand treiben. Zunächst muss er die Zielperson genau auswählen, etwa deren dynamische IP-Adresse kennen, dann die Sicherheitsmechanismen der Firewall des Routers überwinden und sich schließlich dem eBlocker im lokalen Netz der Zielperson widmen.

Über 200 Euro für eine auf den ersten Blick recht simple Hardware ist ein satter Preis – besonders im Vergleich zu kostenlosen Softwarelösungen. Wie würdest du ihn trotzdem rechtfertigen?

Wer seine Privatsphäre auf mehreren Endgeräten wie Mac, iPhone, iPad, Spielekonsole und Smart-TV schützen will, kann selbst nachrechnen, dass die einzelnen Softwareprodukte sehr teuer werden können. Diese sind zudem nicht zentral administrierbar, der Nutzer muss sie manuell synchron halten. Für jeden, der diesen Aufwand nicht betreiben möchte und auch seine smarten Geräte vor dem „Nach-Hause-Telefonieren“ schützen will, bietet der eBlocker hingegen eine Plug-und-Play-Alternative, die sich schnell rechnet.

