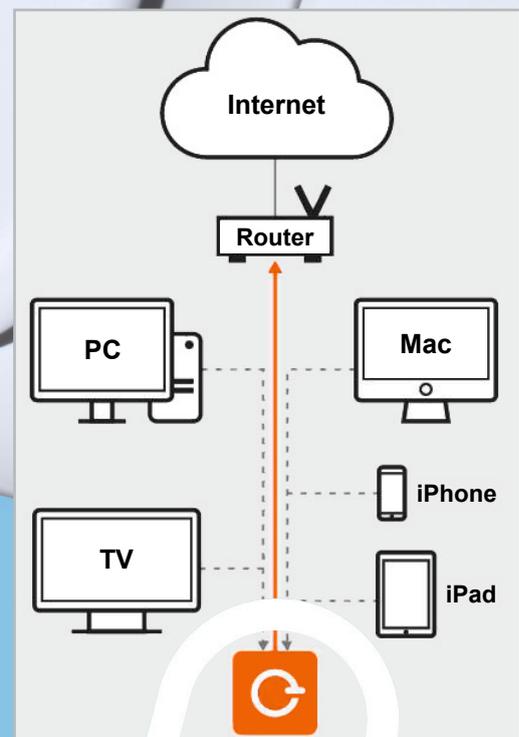




eBlocker Pro

Surfen ohne Werbung und anonym



Privat-
sphäre

Unter dem Namen eBlocker wird von dem Hamburger Unternehmen eBlocker GmbH ein Würfel mit knapp zehn Zentimeter Kantenlänge angeboten, der Hardware und Software enthält, mit deren Hilfe Surfen ohne Werbung und anonymes Surfen für alle Geräte innerhalb eines Netzwerkes ohne Installation von Software auf den Geräten möglich ist.



Das Problem: Informationspreisgabe und unerwünschte Werbung

Beim Besuch nahezu jeder kommerziell betriebenen Webseite wird man – legal – von Datensammelprogrammen erfasst. Die Unternehmen haben ein sehr großes Interesse daran, zu ermitteln, wo sich ein potenzieller Kunde geografisch befindet, was für ein Gerät er gerade benutzt, welche Seite er vorher besucht hat usw. Auf Basis der von den Unternehmen gesammelten Informationen wird dem Internetnutzer dann beispielsweise gezielt Werbung – auch auf Internetseiten ganz anderer Unternehmen – angeboten. Es ist auch möglich, Kunden Produkte oder Dienstleistungen je nach benutztem Endgerät zu anderen Preisen oder gar nicht anzubieten (dynamische Preisgestaltung, dynamic pricing). Nutzern von Apple-Geräten werden so teilweise höhere Preise angezeigt, weil sie als zahlungskräftigere Kunden gelten als Windows-, Linux- oder Android-Benutzer. Auf einem Smartphone werden manchmal höhere Preise angezeigt als auf einem Desktop-PC. Preise schwanken teilweise je nachdem, von welcher Internetseite ein Kunde gekommen ist. Es soll Internethändler geben, die bei Bestellungen aus bestimmten Stadtteilen nur Vorauszahlungen akzeptieren.

Sich diesem Datenkreislauf zu entziehen ist für Internetnutzer nahezu unmöglich. Das Datensammeln und das Auswerten der Daten ist für den Nutzer nicht nachvollziehbar. Meist erzeugen erst größere Skandale in der Presse das Bewusstsein über die vielfältigen Möglichkeiten der Unternehmen. Die Spitze des Eisbergs ist jedoch täglich für jeden zu sehen. Als eines von unzähligen möglichen Beispielen zeigt [Bild 1](#) den Aufruf einer harmlosen Internetseite (duden.de), bei der nicht nur Werbung eines Technikversenders eingeblendet wird, dessen Seiten der Autor tags zuvor besucht hatte, sondern auch Werbung eines Reiseportals, auf der der Autor sich kürzlich über ein Hotel in Garmisch und seine Frau sich unabhängig davon über ein komplett anderes Gerät im Heimnetzwerk (!) über Hotels in Lehrte informiert hatte. So wird einem Internetnutzer also neben der ei-

genen Werbung und der Werbung fester Kooperationspartner auch sehr gezielt Werbung aufgrund des Nutzerverhaltens (letzte besuchten Seiten, Cookies), des Standortes (IP-Adresse) oder des benutzten Gerätes angeboten. Das Sammeln dieser „öffentlich zur Verfügung stehenden“ Informationen ist übrigens weder

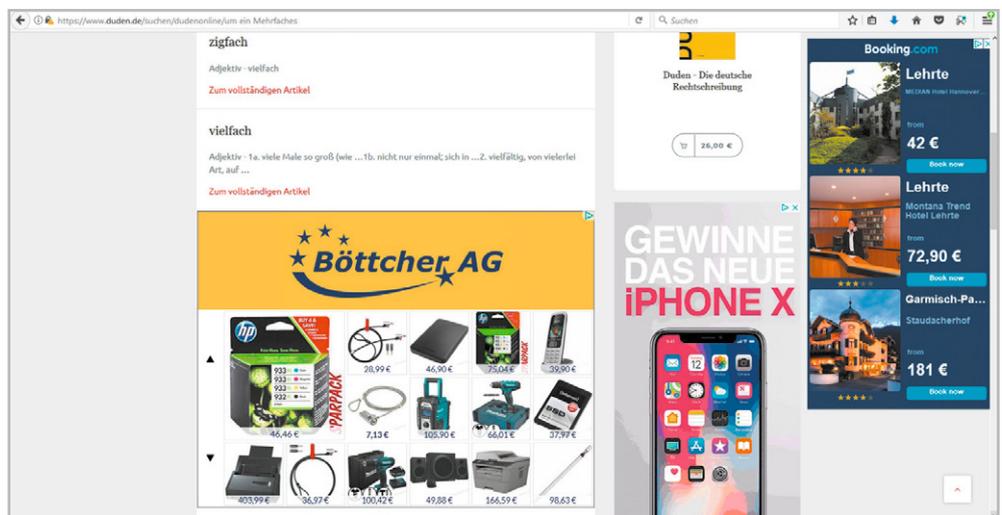


Bild 1: Werbung bei Duden.de

illegal noch verwerflich. Ob es allerdings vom Benutzer immer gewollt ist, steht auf einem anderen Blatt.

Auf vielen Seiten im Internet [1] kann man sich einige der sammelfähigen Informationen anzeigen lassen. [Bild 2](#) zeigt beispielsweise die Internetseite, die benutzte Betriebssystem und den ungefähren Standort eines Benutzers an. Diese und weitere Daten sendet der Benutzer automatisch ins Internet.

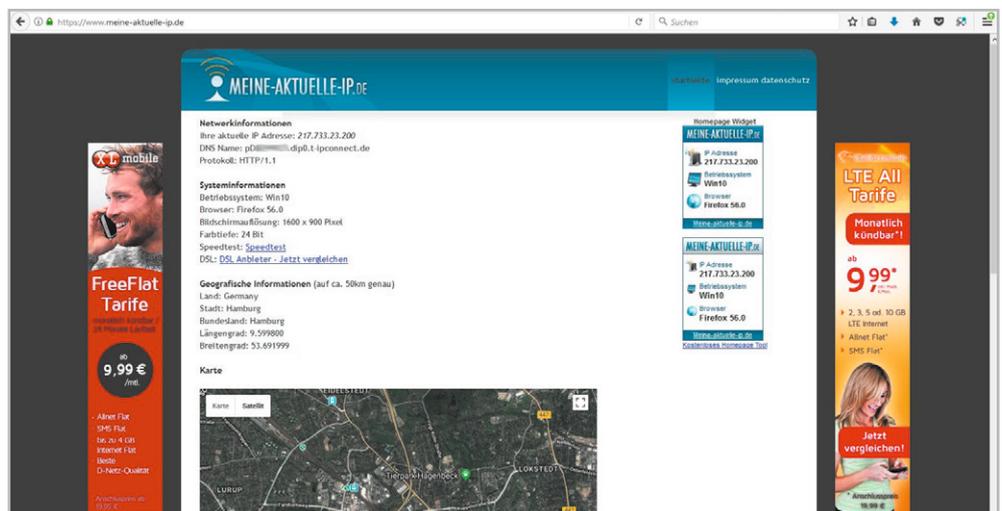


Bild 2: IP-Adresse, Betriebssystem, Browser, Ort

Lösungsansätze

Für technisch versierte Internetnutzer gibt es eine Vielzahl an Möglichkeiten, die Privatsphäre beim Surfen besser zu schützen und unerwünschte Werbung zu minimieren. Manche Browser (IE, Chrome, Firefox ...) bieten Einstellungen, mit denen die unerwünschte Informationsübermittlung vermieden werden kann, es gibt Browser-Plug-ins (AdBlocker etc.), lokale Proxys (AdGuard+, Tor-Client) oder Internet-Proxys (hidemyass.com, disconnect.me ...) und DIY-Gateways (Pi-hole, AdTrap, Danubebox). Der Nachteil ist, dass man für derartige Maßnahmen einigermaßen tief in die Materie einsteigen muss, dass man auf jedem zu schützenden Gerät entsprechende Softwareinstallationen vornehmen muss und diese auch regelmäßig updaten muss. Das Unternehmen eBlocker GmbH hat alle benötigten Maßnahmen auf geschickte Weise in einem kleinen Würfel zusammengefasst, der sich (automatisch!) in das Heimnetzwerk einklinkt und alle angeschlossenen Geräte schützt, ohne dass der Benutzer Software installieren muss.

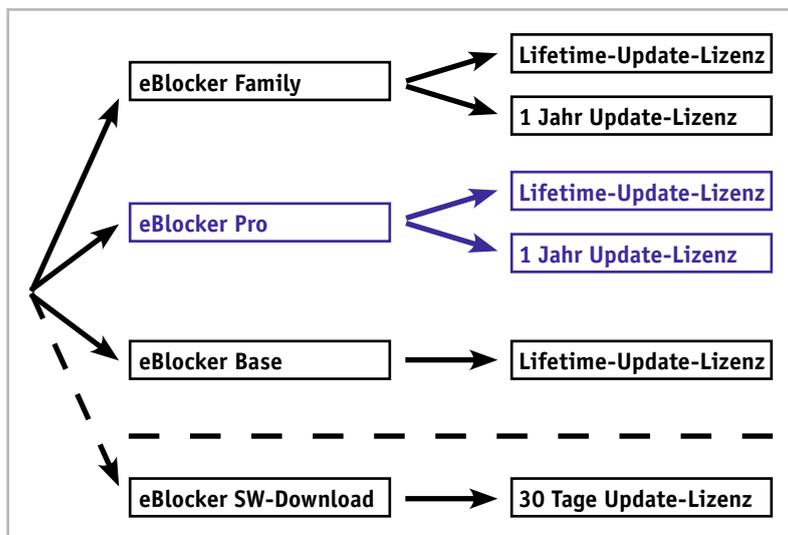


Bild 3: eBlocker-Modelle

eBlocker

Es gibt von der eBlocker GmbH verschiedene Produkte, die sich durch ihren Funktionsumfang und die Update-Lizenz unterscheiden (Bild 3). Allen Produkten – eBlocker Base, eBlocker Pro, eBlocker Family – ist gemeinsam, dass es sich um einen Würfel zum Anschluss an den Router handelt, auf dem die benötigte Software fertig installiert ist. Es ist weder auf dem Gerät selbst noch auf einem vom Benutzer verwendeten Gerät irgendeine Software vom Benutzer zu installieren. Jedes eBlocker-Modell kann alle im Netzwerk angeschlossenen Geräte – egal mit welchem Betriebssystem oder welchem Browser – schützen und ermöglicht eine IP-Anonymisierung (Tabelle 1).

Unterschiede der eBlocker-Modelle				
	eBlocker Base	eBlocker Pro (eBlocker SW-Download)	eBlocker Family	
Tabelle 1	Keine Softwareinstallation	✓	✓	✓
	Schützt für alle Betriebssysteme, Endgeräte und Browser	✓	✓	✓
	IP-Anonymisierung	✓	✓	✓
	Stoppt Werbung und Tracker	-	✓	✓
	Gerätetarnung	-	✓	✓
	Individuelle Nutzerkonten	-	-	✓
	Jugendschutz	-	-	✓

Der eBlocker Pro (CV-12 73 65 bzw. CV-12 73 66) kann zusätzlich unerwünschte Werbung und Tracker blockieren und ermöglicht es, sich als ein anderes Gerät auszugeben – zum Beispiel als Linux-Gerät statt als Apple-Gerät. In der Family-Version ist es zusätzlich möglich, für verschiedene Nutzer unterschiedliche Profile anzulegen und einen Jugendschutz einzustellen. Die Hardware der drei Modelle ist identisch. Die Unterschiede liegen nur in der Software und werden bei der Aktivierung durch Eingabe des Lizenzschlüssels aktiviert. Ein Upgrade von Base zu Pro und von Pro zu Family ist auch im Nachgang noch möglich. Bei den Modellen Pro und Family kann man entweder eine einjährige Software-Update-Lizenz oder eine zeitlich unbegrenzte Update-Lizenz erwerben (Bild 3). Zusätzlich zu diesen Paketen ist es dem versierten Benutzer möglich, kostenfrei (!) die reine eBlocker-Pro-Software für Raspberry Pi 2 oder 3 oder Banana Pi M2 oder M2+ von [2] herunterzuladen. Dadurch kann man kostenfrei die Funktionalität testen.

Zum Lieferumfang des eBlockers gehört die Hardware mit der eBlocker-Software, ein Netzteil, ein LAN-Kabel, eine Kurzanleitung, der Lizenzschlüssel und Aufkleber für Webcams (Bild 4).



Bild 4: Lieferumfang eBlocker

Inbetriebnahme

Im Normalfall sind alle Geräte über WLAN oder per LAN-Kabel an einen Router angeschlossen, der wiederum die Verbindung zum Internet darstellt (Bild 5). Der Anschluss des eBlockers ist sehr einfach: Der eBlocker wird mit dem beiliegenden LAN-Kabel direkt an den Router angeschlossen und mit dem Netzteil verbunden. Nach der vollständigen Aktivierung verbinden sich dann alle Geräte im Netzwerk mit dem eBlocker statt mit dem Router. Der eBlocker stellt die gefilterte Verbindung zum Internet her (Bild 6).

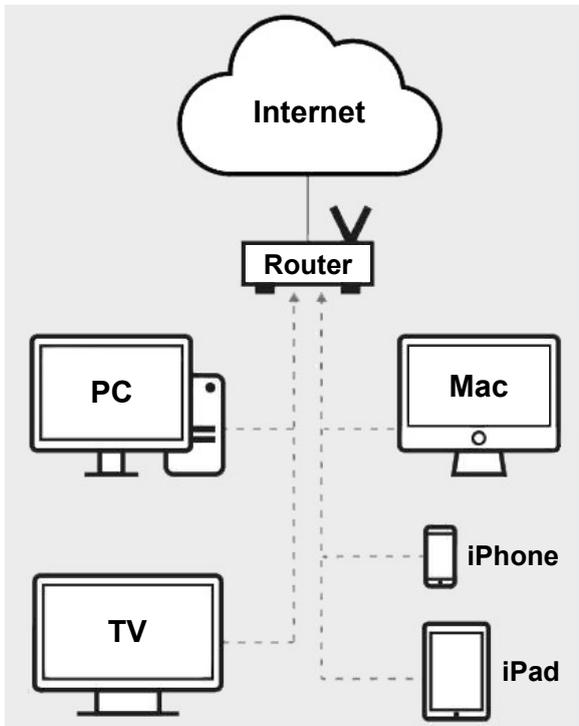


Bild 5: Netzwerk ohne eBlocker

Nach dem Anschluss der Hardware wird in einem Internet-Browser die URL <http://setup.eblocker.com> aufgerufen. Es erscheint ein Willkommensschirm (Bild 7). Im Browser erscheint hier nun zum ersten Mal in der rechten oberen Ecke ein durchsichtiges eBlocker-Icon (Bild 7 oben rechts).

Durch Klicken auf dieses Icon erscheint die sogenannte eBlocker Controlbar (Bild 8) und der Aktivierungsassistent wird gestartet.

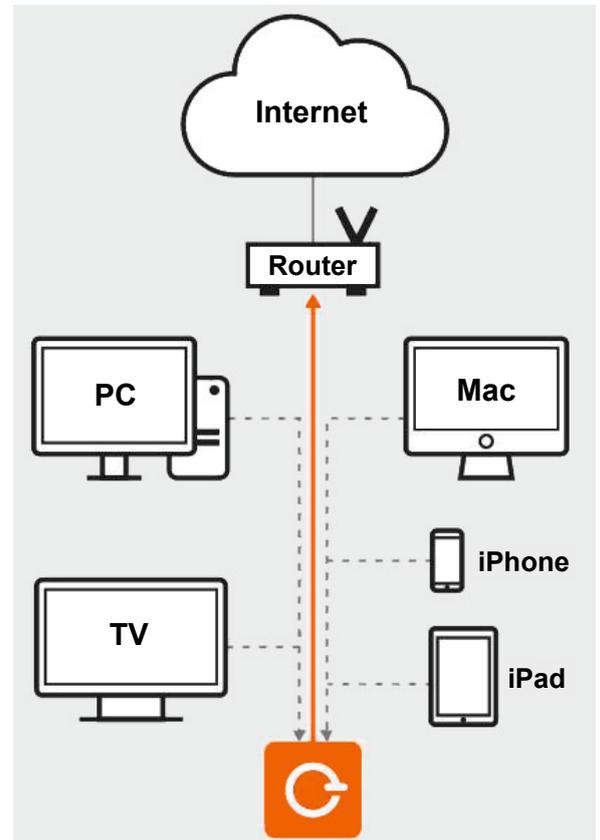


Bild 6: Netzwerk mit eBlocker

Nach Eingabe der Sprache (Deutsch), der Zeitzone, der Seriennummer (von der Unterseite des Würfels) und des Lizenzschlüssels (im Lieferumfang) ist die

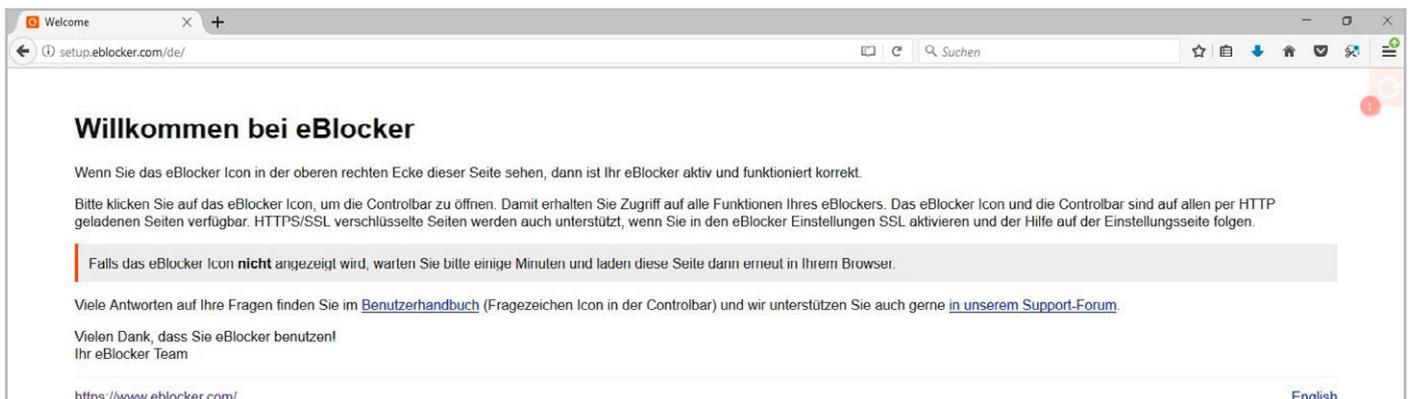


Bild 7: Willkommensschirm

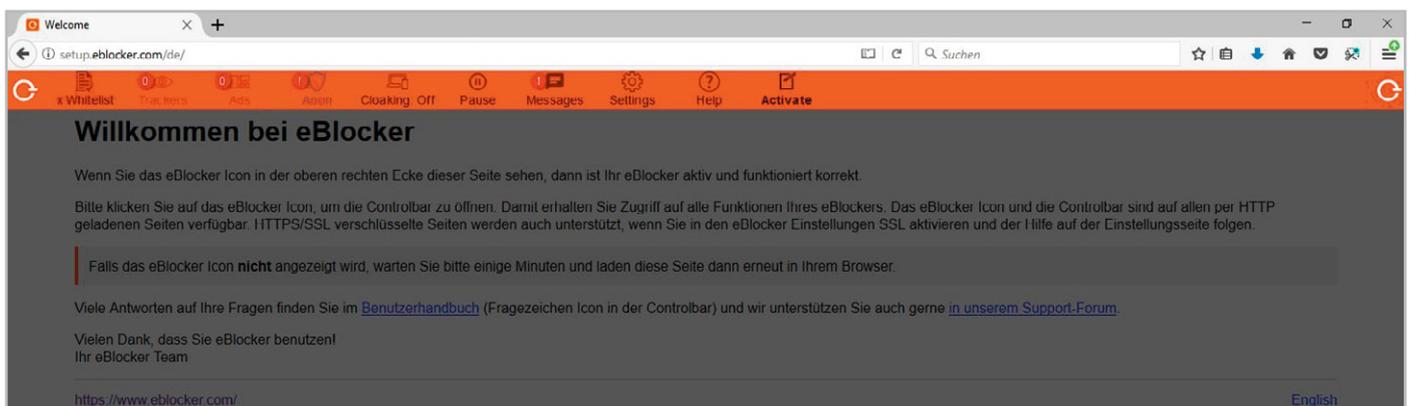


Bild 8: Die sogenannte Controlbar



Aktivierung erfolgreich beendet und man kann weitere Einstellungen vornehmen (Bild 9). Wichtig ist, die Unterstützung für HTTPS/SSL-Verbindungen zu aktivieren.

Ausführliche Informationen findet man in deutscher Sprache im Internet unter [3] und [4].

Die Inbetriebnahme für alle Geräte im Netzwerk ist damit beendet!

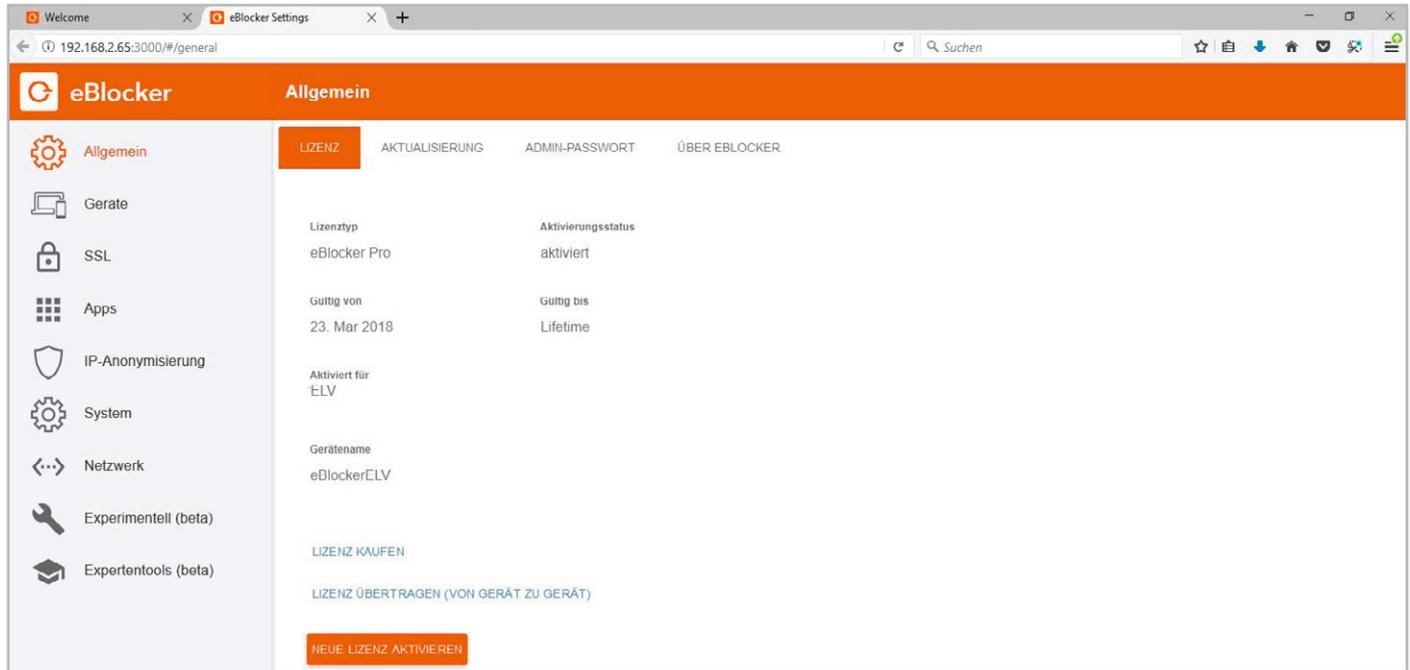


Bild 9: eBlocker-Menü



Bild 10: Ohne Werbung mit eBlocker-Icon oben rechts

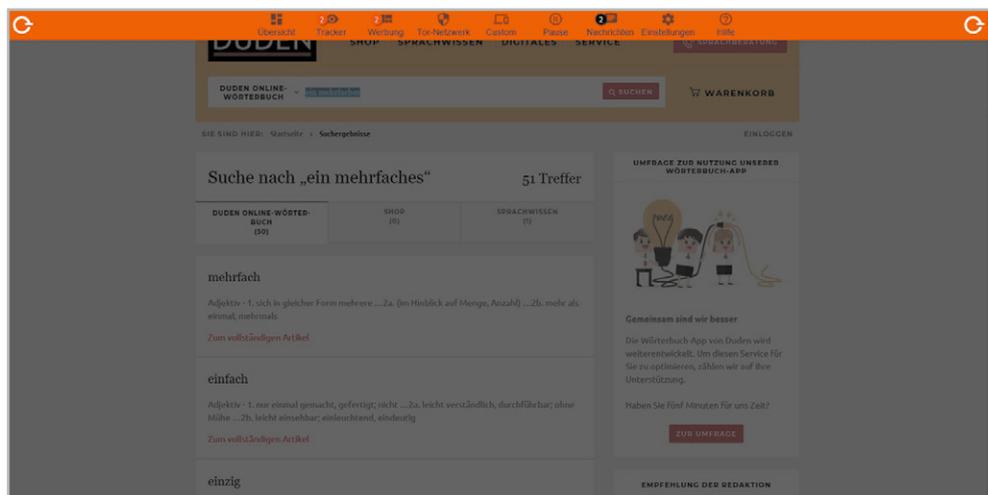
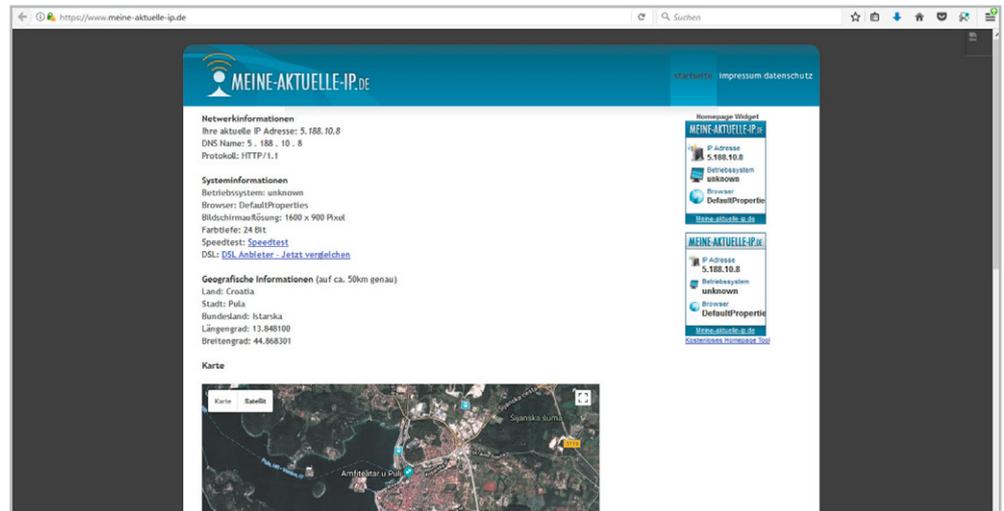


Bild 11: Ohne Werbung mit Controlbar



Bild 12: Ohne Werbung, falsche IP, falsches Betriebssystem, falscher Ort



Benutzung

Die Benutzung des eBlockers ist sehr einfach: Man ruft einfach auf einem der angeschlossenen Geräte mit einem Web-Browser eine Seite auf. Dabei erscheint oben rechts im Browserfenster das transparente eBlocker-Icon (Bild 10). Im Vergleich zu Bild 1 ist in Bild 10 zu sehen, dass keine unerwünschte Werbung mehr angezeigt wird. Dadurch erfolgt der Seitenaufbau übrigens sogar schneller, weil die Werbilder nicht angezeigt werden. An kleinen Ziffern beim eBlocker-Icon sieht man, wie viel Werbung bzw. wie viele Tracker geblockt wurden. Durch Klicken auf das eBlocker-Icon öffnet sich die Controlbar (Bild 11). So hat man von jedem Browserfenster aus die Möglichkeit, Einstellungen vorzunehmen. In der Übersicht (Dashboard) kann man den eBlocker pausieren. Durch Klicken auf Tracker bzw. Werbung kann man sehen, was für die aktuelle Seite geblockt wurde und man kann individuelle Einstellungen vornehmen. Unter IP-Anon/Tor-Netzwerk kann man das anonyme Surfen über das Tor-Netzwerk aktivieren/deaktivieren. Dadurch wird nicht die wirkliche IP-Adresse in das Internet übertragen. Unter Tarnung/Custom kann man einstellen, ob man sich im Internet „als jemand anderes ausgeben“ möchte. So kann man beispielsweise als Apple-User beim Empfänger erscheinen, als wäre man ein Windows- oder Linux-User. Ein Klick auf das eBlocker-Symbol verkleinert die Controlbar wieder. In Bild 12 ist exemplarisch das Ergebnis der eBlocker-Filterung im Vergleich zu Bild 2 zu sehen. Zum einen ist auch hier die unerwünschte Werbung geblockt. Zum anderen ist zu sehen, dass die IP-Adresse, der Betriebssystem-/Browser-Typ und der Standort nicht wahrheitsgemäß übertragen werden. Dadurch können im Internet keine Rückschlüsse über den Benutzer erfolgen.

Fazit

Die Inbetriebnahme des eBlockers ist sehr einfach und erfolgt weitgehend automatisch. Der Nutzer muss keine Software installieren. Alle im Netzwerk angeschlossenen Geräte nutzen automatisch den Funktionsumfang des eBlockers – egal welches Betriebssystem und welcher Browser. Die Internetverbindung der angeschlossenen Geräte erfolgt über den

eBlocker, der abgehende Informationen filtert und eingehende unerwünschte Werbung blockt. Man kann sich anzeigen lassen, was geblockt wurde. Den Grad der Abblockung kann man für einzelne Geräte (und bei der Family-Version für einzelne User) individuell einstellen. Insgesamt ist es also mit dem eBlocker möglich, unerwünschte Werbung zu blocken und das unerwünschte Übermitteln von persönlichen Informationen ins Internet zu vermeiden. **ELV**



Weitere Infos:

- [1] Welche Infos gebe ich preis?
<https://www.eblocker.com/de/privacy-check/>
<https://www.meine-aktuelle-ip.de/>
<https://meineipadresse.de/>
<https://meine-ip-info.de/>
<https://www.meineip.de/>
<https://www.wieistmeineip.de/>
- [2] eBlocker Software-Download:
<https://www.eblocker.com/de/download/>
- [3] eBlocker Quickstart Guide:
https://www.eblocker.com/wp-content/uploads/2016/09/Quick_Start_Guide_For_eBlocker_global_v3_DE-2.pdf
- [4] eBlocker Handbuch:
https://www.eblocker.com/wp-content/uploads/2018/03/User_Manual_eBlocker_v55.pdf

Preisstellung April 2018 – aktuelle Preise im ELV Shop

Empfohlene Produkte	Best.-Nr.	Preis
eBlocker Pro privater Netzwerkschutz, inkl. 1 Jahr Update-Lizenz	CV-12 73 65	€ 189,-
eBlocker Pro privater Netzwerkschutz, inkl. unbegrenzter Update-Lizenz	CV-12 73 66	€ 269,-