Verfolger abschütteln

Werbeblocker, Teil 2. Hier erfahren Sie, welche Browser-Einstellungen empfehlenswert sind und wie Sie mit der Erweiterung Ghostery Tracking und Werbung reduzieren.

In KONSUMENT 9/2019 haben wir den Basisschutz der Browser unter „besser als gar nichts" abgehakt, was bedeutet, dass man die vorhandenen Möglichkeiten trotzdem ausschöpfen sollte. Bevor wir ins Detail gehen, Allgemeingültiges vorab:

- Soll der Datenschutz über dem Komfort stehen, sollten Sie auf das Synchronisieren von Verlauf/Chronik, Lesezeichen, Einstellungen, Passwörtern etc. über mehrere Geräte hinweg verzichten (z.B. PC und Smartphone). Das heißt, Sie sollten sich bei keinem Browser mit einem persönlichen Konto anmelden bzw. laut unseren Anleitungen verhindern, dass dies automatisch geschieht, denn sonst landen Ihre Daten in einem Cloud-Speicher im Internet.
- Das Senden sogenannter Do-Not-Track-Anforderungen oder -Informationen benachrichtigt den Betreiber einer Website davon, dass Sie den Wunsch haben, beim Internetsurfen nicht verfolgt zu werden. Ob er diesem Wunsch nachkommt, entscheidet der Betreiber; das Aktivieren dieser Option bringt daher wenig.
- Ob „Privates Fenster", „InPrivate Browsen", „Inkognito-Fenster" oder „Anonymes Browsen": Diese Funktion bewirkt, dass der Browser keine lokalen Aufzeichnungen über Ihren Suchverlauf am Computer selbst macht. Sie ist z.B. dann praktisch, wenn Sie einen fremden Computer benutzen und sich nicht darum kümmern wollen, den Verlauf am Ende manuell zu löschen, hat aber nichts mit Anonymität im Internet zu tun.

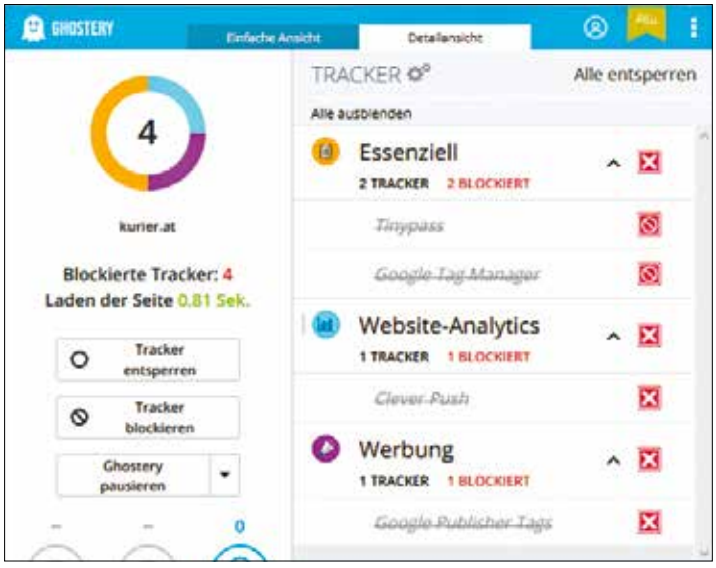
Chrome

Gegen den Chrome-Browser (www.google.com/intl/de/chrome) ist nur eines einzuwenden – nämlich, dass er vom Datensammler Google kommt (siehe „Was Google über uns weiß" in KONSUMENT 10/2018 bzw. www.konsument.at/datenschutz-google-konto-verwalten102018). Nutzen Sie auf demselben Gerät andere Google-Dienste mit Ihrem persönlichen Konto (was im Fall von Gmail unvermeidlich ist), können Sie in Chrome automatisch angemeldet werden. Um das zu verhindern, klicken Sie im Browser auf das Menüsymbol (drei Punkte), dann im Menüfenster auf „Einstellungen", gehen im folgenden Browserfenster ganz nach unten und klicken auf „Erweitert". Unter „Datenschutz und Sicherheit" deaktivieren Sie „Anmeldung in Chrome zulassen". Schalten Sie außerdem „Seiten vorab laden …" ab. Unter „Synchronisierung und Google-Dienste" können Sie im Prinzip alles deaktivieren, wobei aber das Belassen von „Safe Browsing" durchaus sinnvoll ist. Unter „Website-Einstellungen" und „Cookies" aktivieren Sie „Drittanbieter-Cookies blockieren"; unter „Werbung" sollte der Schalter wie vom Anbieter empfohlen auf „Aus" stehen.

Edge

Edge ist seit Windows 10 der vorinstallierte Microsoft-Browser. Standardmäßig schlägt Windows 10 beim erstmaligen Einrichten vor, dass Sie ein Microsoft-Konto erstellen bzw. sich mit einem vorhandenen anmelden. (Ein solches besitzen Sie z.B., wenn Sie über eine E-Mail-Adresse verfügen, die als Bestandteil @hotmail, @live oder @outlook enthält, oder wenn Sie die von Microsoft bereitgestellte Cloud, also den Onlinespeicher OneDrive, nutzen.) Melden Sie sich auf Ihrem Windows-10-Computer mit Ihrem Microsoft-Konto an, werden Sie automatisch auch im Edge-Browser, im OneDrive sowie im Windows-Store angemeldet. Nutzen Sie hingegen ein lokales Konto „(Windows-Symbol)/Einstellungen/Konten/Ihre Infos/Stattdessen mit einem lokalen Konto anmelden", entfällt die automatische Anmeldung bei den genannten Microsoft-Diensten und es erfolgt keine Synchronisation der Browserdaten und -einstellungen. Das bedeutet jedoch nicht, dass beim Internetsurfen gar keine Daten mehr an Microsoft und andere übermittelt werden.

Klicken Sie auf die drei Punkte rechts oben und danach im Menüfenster auf „Einstellungen". Unter „Allgemein" können Sie ganz unten das Synchronisieren ausschalten. Klicken Sie nun in der Leiste links das Schloss-Symbol („Datenschutz und Sicherheit") an. Im Feld unter der Überschrift „Cookies" wählen Sie „Nur Cookies von Drittanbietern blockieren". „Such- und Websitevorschläge" sowie „Suchverlauf" sind Komfortfunktionen, auf die man ungern verzichtet, aber Sie können es ausprobieren. Unbedingt abschalten sollten Sie die „Seitenvorhersage". In der Kritik von Datenschützern steht die Funktion „Windows Defender SmartScreen". Auch wenn es sich an sich um eine Sicherheitsfunktion handelt, raten wir, sie abzuschalten. Sowohl mit als auch ohne sollten Sie beim Surfen und Herunterladen aufmerksam und kritisch sein. Wenn Sie ein Microsoft-Konto verwenden, klicken Sie abschließend auf das Schieberegler-Symbol („Erweitert"). Dort können Sie Microsofts Sprachassistentin Cortana in Edge abschalten.



Glossar

App (Kurzform von englisch: Application). Applikation, Anwendung, Programm für Computer und/oder Smartphone.
Browser-Erweiterung (auch: Add-on). Softwaremodul, das in einen Internetbrowser integriert wird und dessen Funktionsumfang erweitert.
Cloud (englisch: Wolke). Ein von einem Anbieter betriebener Verbund von Computern und Festplatten, der von den Nutzern standortunabhängig via Internet als Datenspeicher verwendet werden kann.
Cookie (englisch: Keks). Kleine Textdatei. Speichert lokal auf der Computerfestplatte Daten über besuchte Webseiten, die beim erneuten Besuch automatisch wieder aufgerufen werden. Dadurch hat aber auch der Webseitenbetreiber Zugriff auf diese Informationen.
Tracker (englisch: Verfolger). Oberbegriff für Tools (Werkzeuge) zur Nachverfolgung (Tracking) und Auswertung des Nutzungsverhaltens im Internet.

Werbung und Tracking

In KONSUMENT 9/2019 haben wir festgehalten, dass ein effektiver Schutz vor Werbung und Tracking nur mithilfe einer Browser-Erweiterung möglich ist. Dort haben wir uBlock Origin empfohlen; nun wenden wir uns der – einfacher bedienbaren – Alternative Ghostery zu. Leider ist diese Erweiterung mit dem blauen Gespensterlogo in letzter Zeit selbst etwas aufdringlich geworden, was sich aber abstellen lässt.

Ghostery

Nach der Installation von Ghostery erscheint im Browser ein Willkommensfenster mit zwei wesentlichen Optionen: „Absolvieren Sie ein Tutorial", was zugleich die Zustimmung zur Beibehaltung der Voreinstellungen ist, sowie „Benutzerdefiniertes Setup" (= Einrichtung). Letzteres ist datenschutzfreundlicher und wird von uns empfohlen. Klicken Sie also auf die Schaltfläche im Feld „Benutzerdefiniertes Setup".
Im nächsten Fenster klicken Sie auf „Alles blockieren". Das bewirkt zwar möglicherweise, dass Sie auf Internetseiten bestimmte Angebote (z.B. Bildergalerien, Videos, Nutzerkommentare) vorerst nicht nutzen können, es ist aber der einfachere Zugang, einzelne Elemente nachträglich wieder freizuschalten.

Nach Klick auf „Nächstes", stellen Sie die Schalter bei „Smart Blocking" und „Rewards" auf „Aus" und klicken erneut auf „Nächstes". Auf dieser Seite entfernen Sie den Haken im Kästchen, in dem es um das Teilen von „Human-Web-Daten" geht. Es handelt sich um einen vom Anbieter kreierten Begriff für eine Methode zur Sammlung anonymer Daten. Nach Klick auf „Nächstes" ist die Einrichtung abgeschlossen. Sie können das Tutorial absolvieren, um Ghostery kennenzulernen, oder klicken sofort auf „Erledigt". Um das Setup später zu wiederholen, müssen Sie in den Browser-Einstellungen zu den Add-ons/Erweiterungen gehen. Die restlichen Ghostery-Einstellungen erreichen Sie über das kleine Gespenst in der Symbolleiste des Browsers. Rufen Sie eine Ihnen bekannte Internetseite auf. Neben dem Gespenstersymbol wird in einem kleinen Feld eine Zahl angezeigt. Ein Klick darauf öffnet ein Fenster mit einer Statistik. Wählen Sie „Detailansicht", um die Liste der gefundenen und blockierten (= durchgestrichenen) Elemente zu sehen. Sie können hier durch Klick auf den Namen mehr zu den Trackern erfahren bzw. sie auf der aktuellen Website oder generell zulassen und sie auch wieder blockieren (Klick auf eines der drei rechts vom Namen angezeigten Symbole. Danach nicht vergessen: jedes Mal via Ghostery-Fenster die Seite neu laden!).
Wenn Sie auf die drei Punkte rechts oben klicken, gelangen Sie zu den Ghostery-Einstellungen. Gehen Sie in der linken Spalte zu „Allgemeine Einstellungen". Belassen Sie die gesetzten Häkchen bis auf zwei Ausnahmen: Deaktivieren Sie „Von Websitebetreibern erstellte Tracker zulassen" und aktivieren Sie im Gegenzug „Neue zu Ghostery hinzugefügte Tracker standardmäßig blockieren". Die „Benachrichtigungen" können Sie unverändert lassen. Sie erhalten so Zusatzinformationen. „Opt-in" meint die Möglichkeit, anonyme Daten mit Ghostery zu teilen. Ob und in welcher Ecke Sie die „Lila Box" (= eine Benachrichtigung über aktuell gefundene Tracker) anzeigen lassen möchten oder nicht, ist Geschmacksache und lässt sich jederzeit ändern. Die voreingestellte Zeit von 15 Sekunden ist jedenfalls zu lang; es genügen auch 5 Sekunden.

MEHR ZUM THEMA

- Details zu den alternativen Browsern Firefox und Opera finden Sie auf www.konsument.at/werbeblocker102019.
  Nach Veröffentlichung der neuen Edge-Version, werden wir die Änderungen dort nachtragen.
- Teil 1 dieses Beitrags können Sie in KONSUMENT 9/2019 und auf www.konsument.at/werbeblocker092019 nachlesen.

Rat und Hilfe für Verbraucher in Europa
ECC-Net
Finanziell unterstützt durch die Europäische Union

Dieser Artikel wurde aus den Mitteln des Verbraucherprogramms der Europäischen Union (2014 – 2020) gefördert.