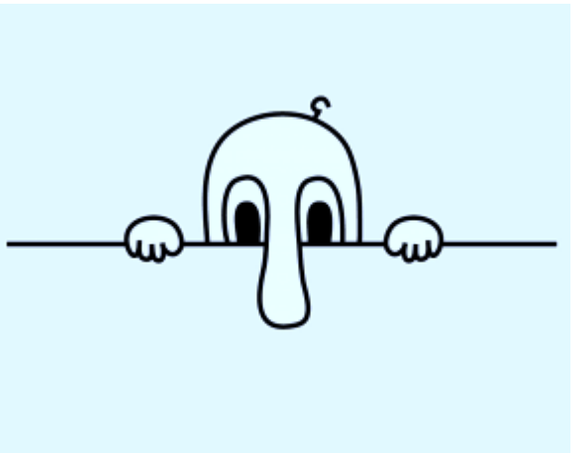
Empfehlungen für sicheres Browsen im Internet

Allgemeines

Wer im WWW (World Wide Web - das ist der mit Browsern erschlossene Teil des Internets) unterwegs ist, muss sich dabei bewusst sein, dass jene Browser schon aus technischen Gründen Plaudertaschen sind. Die Ersteller von Internetseiten müssen wissen, mit wem sie es tun haben, um ihre Inhalte möglichst so zu übermitteln, wie sie es sich gedacht haben.
Diese Informationen können natürlich auch zur Identifikation und Beobachtung des eigenen Verhaltens genutzt werden, denn in Summe sind sie wie ein Fingerabdruck des Browsers im Verbund mit dem Gerät (PC, Smartphone, Rechner), auf dem sie installiert sind. Da weltweit weitaus mehr Menschen Englisch nutzen als Deutsch, sind Browser mit Englisch (etwas) schwerer identifizierbar. Wer Englisch kann, sollte also ernsthaft überlegen, einen englischsprachigen Browser zu nutzen.
Eine weitere Möglichkeit, die Besucher einer Internetseite zu identifizieren und bei deren nächsten Besuch auch wieder zu erkennen, sind **Cookies** (zu Deutsch „Kekse“). Das sind kleine Textdateien, die sowohl Inhalte speichern können (z.B. was hat die Besucher interessiert?) als auch eindeutige Identifikationscodes. In faktisch allen gebräuchlichen Browsern lassen sich Cookies abschalten und bei Bedarf als Ausnahme für einzelne, gut beleumdete Seiten zulassen (manche Seiten arbeiten sonst nicht mehr richtig). Mindestens sollten aber sogenannte **Drittanbieter-Cookies** blockiert werden, denn die dienen ausschließlich zur Verfolgung über mehrere Seiten hinweg. Eine gute Idee ist es auch, alle Cookies automatisch löschen zu lassen, wenn der Browser geschlossen wird.



Kann denn Werbung schädlich sein?

Werbung ist oft aggressiv, blinkt, wechselt die Farben, zeigt Laufschriften oder Animationen und lenkt von den eigentlich gewünschten oder zu suchenden Inhalten einer Seite ab. Im mobilen Betrieb oder auch dort, wo das Internet nicht sonderlich schnell ist, macht sie den Aufbau der besuchten Seiten signifikant langsamer – und sie kann auch Schadcodes transportieren und installieren. Mitglieder des CCC (Chaos-Computer-Club) haben live auf der re:publica TEN vorgeführt, wie ein von ihnen produziertes und von einer Werbefirma als sicher zertifiziertes (!) Werbebanner den Taschenrechner eines Windows-Rechners geöffnet hat. Wer das erreicht, kann noch viel mehr...

Aktive Inhalte

Internetseiten im WWW möchten oft dynamisch Inhalte nachladen oder aber interaktive Inhalte darstellen. Dazu bieten sie den Browsern Elemente an, die zusätzliche Programme erfordern oder auch Textzeilen, die als Programmbefehle interpretiert werden können. Einiges davon wird nachfolgend behandelt.

Zuweilen standardmäßig eingebettete Zusätze (*Plug-ins*) sind der **Adobe Flash-Player** oder **Microsoft Silverlight**. Beide werden eigentlich nicht mehr benötigt, sind unsicher und traditionell schlecht gepflegt. Es ist daher eine gute Idee, die betreffenden Zusätze zu **deaktivieren**, besser sogar, zu **deinstallieren** – wenn möglich. Moderne Browser können nahezu alle Inhalte ohne weitere Zusätze darstellen.

Java ist oft die Programmiersprache der Wahl, sollte aber nicht im Browser gestartet werden können. Es dürfte offenkundig sein, dass aktive Programme aus dem Internet potentiell schädlich sein können. Seiten, die Java fordern, sollten mit großer Vorsicht betrachtet werden.

JavaScript, bereits 1995 entwickelt, dient dazu, Aktionen von Seitenbesuchern auszuwerten, dynamisch Inhalte zu verändern oder zu generieren oder auch Informationen zu sammeln, zu speichern oder an Dritte weiterzuleiten. Auch ohne Verfolgungsdrang oder böse Absichten funktionieren viele Internetseiten nicht mehr ohne diese Skripte. Die zu interpretierenden Befehle liegen in Textform (also lesbar) vor. Werden Besucher erkannt, kann personalisierte Werbung eingespielt werden, dubiose Seiten können aber auch Schadcodes auf dem Gerät der Besuchenden (ja, auch Smartphones und Tablets gehören dazu) installieren.

Web Beacons (Funkbake, Funkfeuer, Leuchtfeuer) tun nicht genau das, was der Name verspricht. Nicht uns wird mitgeteilt, wo wir uns gerade befinden, sondern es sind überwiegend unsichtbare Bildpunkte (ein Punkt in der Farbe des Hintergrunds), die einer entfernten Internetseite mitteilen, was wir uns gerade wo angesehen haben. Deshalb werden sie auch als **Zählpixel** bezeichnet. Auch die oben beschriebene Geschwätzigkeit wird dadurch unterstützt. *Web Beacons* bringen den Seitenbetreibern Geld ein und haben keinerlei Funktion. Natürlich können dafür auch „richtige“ Bilder herhalten. Aber, es sind nicht die Bilder oder Bildpunkte selbst, die uns verfolgen, sondern die damit verknüpften Skripte (siehe oben).

Maßnahmen gegen (zu) aktive Inhalte und Tracking (Verfolgung)

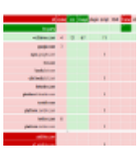
Im Browser einzustellen: Eher der Rubrik „es möge nützen“ zuzuordnen ist die mittlerweile in allen Browsern verfügbare Einstellung **do not track** (verfolge mich nicht). Es gibt keine Verbindlichkeit bei der Berücksichtigung, aber oft „gute Gründe“ den Wunsch zu ignorieren. Es sollte aber dennoch eingestellt werden.

Nachfolgend werden neben den oben beschriebenen Empfehlungen einige Hilfsmittel genannt, die sich als Ergänzung (sogenannte **Add-ons**) in gängigen Browsern installieren lassen (manche sogar in Apples Safari). Wo nicht anders aufgeführt, wird auch Deutsch unterstützt. Nach dem Prinzip „viel hilft viel“ beißen sich auch die genannten Browserzusätze nicht und ergänzen sich eher. Das gilt insbesondere für die ersten drei der folgenden Auflistung. Allen gemeinsam ist die Möglichkeit, sie temporär oder dauerhaft für bestimmte Internetseiten zu deaktivieren.

Disconnect wurde von Google 2015 wegen Verletzung der Bedingung, andere Apps nicht zu stören, aus dem Google-Store geworfen. Nach massiven Protesten und einer eingereichten Klage ist es auch dort wieder zu haben. Andere (z.B. die *New York Times*) hatten es fast zeitgleich zur besten Software zur Wahrung der Privatsphäre des Jahres gekürt. Wer sehen will, was los ist, sollte es vor allen anderen Hilfsmitteln installieren. Es läuft fast in allen Browsern (auch auf Smartphones).
Für Anfänger geeignet.

Privacy Badger kommt auf die sanfte Tour. Es ist von der Stiftung *Electronic Frontier Foundation* entwickelt worden, die besonders die Privatsphäre und digitale Freiheitsrechte im Auge hat. Werden „Do not track"-Wünsche von Trackern ignoriert, werden sie fortan geblockt. Aktive Skripte, angetroffen auf drei verschiedenen Websites, werden zukünftig blockiert. Es beschränkt sich auf die Unterdrückung potentiell unerwünschter Inhalte, „saubere Werbung" kann also durchkommen. Wer kostenlose gute Inhalte durch die Werbung auf deren Seiten unterstützen möchte, hat mit dem *Privacy Badger* das richtige Instrument für dennoch sicheres Surfen.
Für Anfänger geeignet.

uBlock Origin ist auch für unerfahrene Nutzer anwendbar. Es muss faktisch nicht konfiguriert werden und bietet sehr guten Schutz vor aggressiven (Werbe-) Inhalten und blockt auch als gefährlich erkannte Webseiten (z.B. aus angeklickten Links). Es unterstützt ebenfalls die Filterlisten von *Adblock Plus,* kennt aber keine Ausnahmen für (bezahlte) Werbeinhalte. Darüber hinaus hat es den Schutz der Privatsphäre besonders im Fokus. Das Add-on basiert selbst auf *JavaScript* und läuft daher unter vielen Browsern.
Für Anfänger geeignet.



uMatrix ist der „Radikalinski" unter den Blockern, auch wenn der Entwickler von *uBlock Origin* dahinter steht. *uMatrix* ist funktional eine *Firewall.* Was nicht ausdrücklich erlaubt ist, wird an der Ausführung gehindert. Das bedeutet, dass die Wahrscheinlichkeit, dass Internetseiten nicht mehr dargestellt werden oder nicht funktionieren, recht groß ist. Es ist Open Source, aber bisher hat sich offensichtlich kein Übersetzer gefunden, und so ist nur die englische Sprachversion erhältlich.
Nur sehr erfahrene Benutzer, die die Mechanismen einschätzen können, sollten es anwenden.

NoScript arbeitet ähnlich, wenn auch nicht ganz so radikal, denn es werden standardmäßig alle aktiven Inhalte geblockt. Dadurch funktionieren aber auch etliche seriöse Seiten nicht mehr, und wer gerne im Browser Videos betrachtet, muss an den Einstellungen „schrauben". Es ist quelloffen (Open Source) und für Browser auf der Basis von Mozilla Firefox und Google-Chrome verfügbar.
Nur für Fortgeschrittene geeignet.

Ghostery®, mittlerweile ebenfalls Open Source, beschränkt sich beim Blocken auf potentiell gefährliche Inhalte von Internetseiten und Werbung. Wer es erstmals installiert, sollte auf jeden Fall alle Einstellungen (es sind die drei Punkte links oben, wenn die Maus über dem Icon schwebt) überprüfen. Empfehlenswert ist das Blockieren aller aufgeführten Inhalte. Auch der Haken bei den „Allgemeinen Einstellungen" beim Punkt „Von Webseitenbetreibern erstellte Tracker" sollte weg, der Rest aber markiert bleiben. Unter der Rubrik „Benachrichtigen" könnte der oberste Punkt „Ankündigungen ..." nerven.
Empfehlung: kein Haken neben allen Positionen von „Opt-in/-out" und unter „Lila Box", die Zeit auf drei Sekunden beschränken.
Für leicht fortgeschrittene Anfänger geeignet.

HTTPS Everywhere ist ein Zusatzprogramm, dessen einziger Zweck es ist, eine sichere, weil verschlüsselte Verbindung zwischen dem Browser und der aufgerufenen Seite herzustellen. Das Lauschen oder gar Verfälschen sind damit ausgeschlossen. Unsichere Verbindungen können mit einem Klick unterbunden werden. Seiten mit Inhalten aus unsicheren Verbindungen (z.B. mit Symbolbildern von Drittanbietern) können allerdings fehlerhaft angezeigt werden.
Für leicht fortgeschrittene Anfänger geeignet.

Der sicherste Weg

Wer allerdings wirklich privat unterwegs sein möchte, muss einen eigens dafür entwickelten und fortwährend gepflegten eigenen Browser dafür nutzen. Das wird zwar zuweilen deutlich langsamer als gewohnt, tut aber nicht weh.

Der **TOR-Browser** ist Open Source und läuft auf praktisch allen gängigen Betriebssystemen. Er nutzt das **Tor-Netzwerk**, das ist eine große Zahl über die Welt verteilter Server, aus denen per Zufall drei für den Aufbau einer angefragten Verbindung ausgewählt werden. Zusätzlich wird alle zehn Minuten eine neue Auswahl getroffen. Jeder Server kennt nur den Vorgänger und den Nachfolger in der Kette, und selbst hochgerüstete Geheimdienste sind nicht notwendigerweise in der Lage, schnell genug den vollständigen Weg einer Verbindung aufzuklären. Despoten und Innenminister mögen diesen Browser nicht.
Er kann zwar ins Darknet, den nicht mit normalen Browsern erreichbaren Teil des Internets, was aber weit überwiegend für legale und friedliche Zwecke genutzt wird. Für unsereins ist er aber äußerst nützlich, um z.B. ortsneutrale Preisauskünfte einzuholen, denn der anfragende Rechner und dessen Standort bleiben unerkannt. Da *NoScript* vorinstalliert ist, werden ohne Nutzereingriff etliche Internetseiten nicht so funktionieren, wie deren Entwickler sich das vorgestellt haben. Auch *HTTPS Everywhere* ist standardmäßig dabei. Für den Betrieb ist es allerdings wichtig, dass die Fenstergröße und sonstige Einstellungen des Browsers nicht geändert werden. Das würde ihn wiedererkennbarer machen.
Auch für Anfänger geeignet.

Wer Fragen hat, kann sich gerne an mich wenden. *Axel Birsul*

Auszug aus "Der graue Computer-Freak", Ausgabe #231, Nov. 2019,
Mitteilungsblatt des DSCC-Berlin e.V. (dscc-berlin.de)