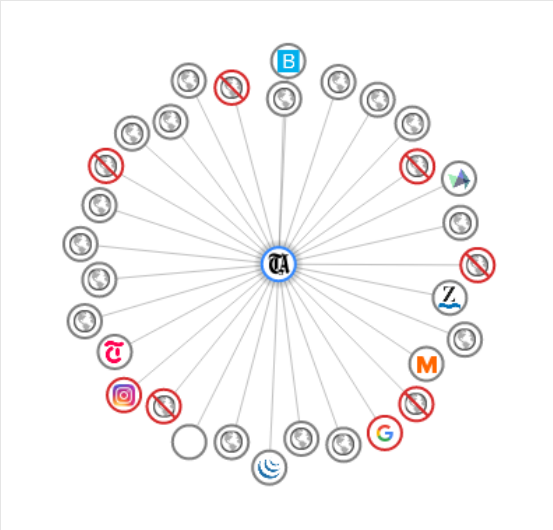
Online-Werbung ist doch nicht schlimm!

Das Lamento der Online-Verlage, dass sie sich nur über Werbung finanzieren können, wurde inzwischen so oft gebetsmühlenartig wiederholt, dass der unbedarfte Internetnutzer dieser Branche schon fast Mitleid entgegenbringt. Was soll denn schon schlimm sein an den blinkenden, flächendeckenden, animierten und ablenkenden Werbeeinblendungen auf Webseiten, wenn diese den Verlagen ermöglichen, qualitative Inhalte kostenlos anzubieten? Eine genauere Betrachtung der Problematik von Online-Werbung offenbart jedoch schnell, dass die sichtbaren Werbebanner nur die Spitze des Eisberges sind.

Hinter diesem sichtbaren Störfaktor «Werbung» lassen Online-Verlage eine Armada von Tracking- und Profiling-Skripten auf die Leser und Konsumenten los. Das heisst, dass ungefragt Daten über Internetnutzerinnen erhoben und auf Servern von Tracking- und Profiling-Firmen zusammengeführt werden. Bei den erhobenen Daten handelt es sich noch nicht um Namen und Anschriften, sondern um eindeutige einer Internetnutzerin zuzuordnende Informationen. Ein digitaler Fingerabdruck wird erstellt, der Surf- und -Kosumgewohnheiten einer Person nahezu flächendeckend erfasst, da fast alle grossen Content-Anbieter dieselben Werbe- und Tracking-Netzwerke einbinden. Die Zusammenführung solcher hochsensibler Daten mit Klarnamen ist die brutal-logische Konsequenz einer Branche, deren Geschäftmodell auf der Missachtung des Datenschutzes und des Schutzes der Privatsphäre aufbaut.



Beim Aufruf von tagesanzeiger.ch werden diese Tracking- und Werbe-Netzwerke über Ihre Anwesenheit informiert.

Angesichts solcher Verfolgungs-Praktiken ist es ein Hohn, dass die EU die Betreiber von Webseiten vor der Verwendung von Cookies warnen lässt. Auch das eingangs erwähnte Klagelied der Online-Verlage kann nur noch als heuchlerisch und verlogen bezeichnet werden. Sie verkaufen und verraten ihre Leser schamlos, ohne ihnen auch nur den geringsten Hinweis darauf zu geben. Allem Anschein nach haben Content-Anbieter, welche solche Werbe- und Tracking-Netwerke einbinden überhaupt keine Kontrolle darüber, welche Daten zu welchem Zweck erhoben werden und wie diese verarbeitet werden. Sie haben darüber hinaus auch keine Kontrolle über die Inhalte, welche von Werbe-Netzwerken auf ihren Seiten ausgespielt werden.

Darin besteht neben der Preisgabe von hochsensiblen Informationen die zweite Gefährdung von Internetnutzerinnen. Werbenetzwerke liefern mitunter auch Skripte aus, welche die Sicherheit von Internetnutzerinnen kompromittieren, da diese Skripte Sicherheitslücken in Browsern ausnützen und Geräte infizieren können. Über mit Werbe-Einblendungen ausgelieferte Skripte wurde in der Tat bereits Schadsoftware verbreitet. Die Konsequenz dieser Angriffe auf die Sicherheit und Privatsphäre von Internetnutzerinnen kann nur digitale Selbstverteidigung heissen.

Mit kleinen Erweiterungen des Browsers können Internetnutzerinnen sich vor einer Kompromittierung ihrer Person und Geräte schützen. Dabei ist es entscheidend, die richtigen Erweiterungen zu installieren, da hinter manchen dubiose Firmen mit kommerziellen Geschäftsmodellen stecken. Nachfolgend werden drei dieser Browser-Anwendungen vorgestellt, die im Zusammenspiel bereits einen starken Schutz vor Verfolgung und Infizierung bieten. Ein schlechtes Gewissen ist bei der Installation dieser Erweiterungen angesichts der dreisten Praktiken von Online-Verlagen und Werbe-Netzwerken beileibe nicht angebracht. Die vorgestellten Erweiterungen stehen für alle modernen Browser zur Verfügung.

1. Browser-Erweiterung «Disconnect»

Das Browser-Addon «Disconnect»

Die Erweiterung «Disconnect» unterbindet die Kontaktaufnahme mit Werbe- und Tracking-Netzwerken. Die Auslieferung von Tracking-Skripten und Werbe-Inhalten an den Browser wird blockiert. Ferner gibt diese Erweiterung Auskunft über die auf der jeweiligen Webseite blockierten Verfolgungs- und Werbe-Netzwerke und kann diese graphisch darstellen (sh. obige Illustration).

Diese Erweiterung steht für Chrome, Firefox, Opera und Vivaldi zum Download und zur unmittelbaren Installation bereit.

2. Browser-Erweiterung «uBlock Origin» (Hot)

Das Browser-Addon «uBlock Origin»

Die Erweiterung «uBlock Origin» verhindert die Anzeige von Werbung äusserst effizient und blockiert Tracking- und Werbe-Netzwerke. Diese Erweiterung ist Open Source und kann deshalb von allen Interessierten eingesehen und weiterentwickelt werden. Als für Online-Verlage fatale Zugabe umgeht «uBlock Origin» die Sperren von Adblockern auf allen Webseiten, die zur Deaktivierung von Adblockern auffordern.

Diese Erweiterung steht für Chrome, Firefox, Opera und Vivaldi zum Download und zur umittelbaren Installation bereit. Diese Erweiterung läuft auch auf der mobilen Version von Firefox (für Smartphones).
Video-Demo: Opera mit integriertem Adblocker vs. Firefox mit «uBlock Origin»

3. Browser-Erweiterung «HTTPS Everywhere»

Das Browser-Addon «HTTPS Everywhere»

Diese Erweiterung erzwingt sichere, verschlüsselte Verbindungen zu Webseiten, sofern diese zur Verfügung stehen. Eine HTTPS-Verbindung stellt sicher, dass zwischengeschaltete Server weder mitlesen noch übertragene Daten manipulieren können. Eine HTTPS-Verbindung ist zum Beispiel für Online-Banking zwingend notwendig.

Diese Erweiterung steht für Chrome, Firefox, Opera und Vivaldi zum Download und zur unmittelbaren Installation bereit.

4. Zugabe: Schutz gegen Canvas- und Audio-Fingerprinting

Fingerprinting-Technologien zur eindeutigen Erkennung von Internetnutzerinnen

Neue Tracking-Methoden versuchen, eindeutige System-Konfigurationen über den HTML-Standard «canvas» zu erfassen und diese einer Nutzerin zuzuordnen. Dagegen schützen zahlreiche Erweiterungen mit unterschiedlichen Herangehensweisen. Interessierte suchen auf den Addon-Seiten des jeweiligen

Browser-Hersteller nach dem Stichwort «Fingerprinting». Firefox-Nutzerinnnen wird an dieser Stelle das Addon "Canvas Fingerprint Defender" empfohlen.

Ferner werden auch eindeutige Audio-Signaturen von Internetgeräten ausgewertet und Nutzerinnen zugeordnet. Firefox-Nutzerinnen wird an dieser Stelle das Addon "AudioContext Fingerprint Defender" empfohlen.

FAZIT

Mit kleinen Erweiterungen können sich Internetnutzerinnen vor Verfolgung, lästiger Werbung und der Kompromittierung ihrer Geräte schützen. Es gibt dabei weder rechtliche noch moralische Bedenken angesichts des Grossangriffs auf den Datenschutz und die Privatsphäre. Im Endeffekt müssen Konsumenten sich aus Notwehr gegen solche Angriffe wehren können. Mit den obigen Browser-Erweiterungen kann mit wenigen Klicks eine starke Privatsphäre wiederhergestellt werden. Es ist zu hoffen, dass Online-Verlage im Bezug auf Werbung und Tracking irgendwann zur Vernunft kommen. Bis dahin ist digitale Selbstverteidigung Pflicht und Notwendigkeit.