Gesunde Datenkekse backen – Firefox mit Erweiterungen absichern

von Bodo Schmitz

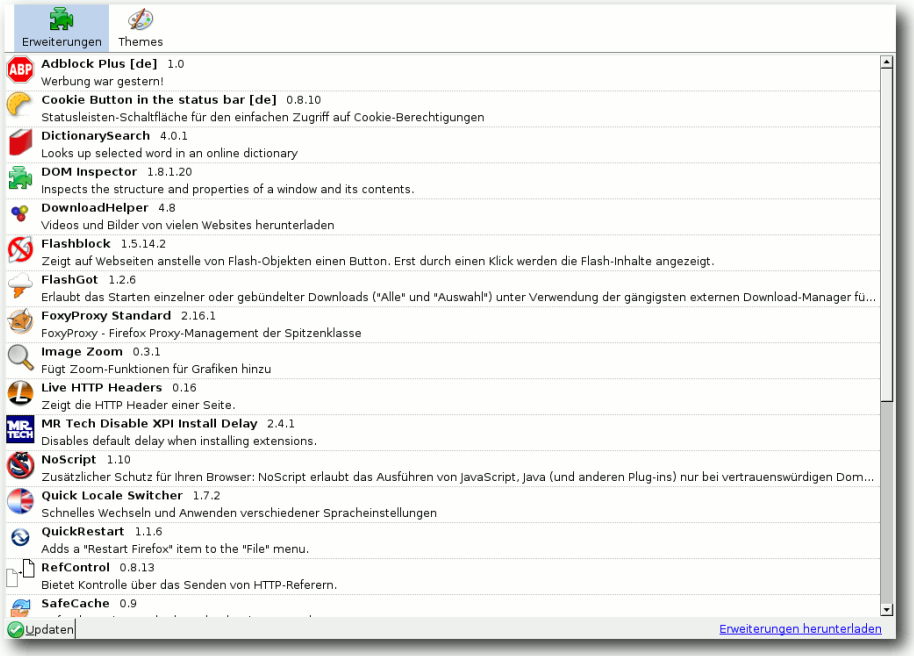
Der Browser Firefox sowie andere Produkte aus dem Hause Mozilla verfügen über eine Erweiterungsschnittstelle, die man einsetzen kann, um die benutzten Programme mit geeigneten Erweiterungen gegen Einbruch und Datenschnüffelei abzudichten. Der Artikel soll einige Erweiterungen vorstellen, die bei der Absicherung des Browsers dienen können.

Einleitung

Die Electronic Frontier Foundation (EFF) warnt vor Benutzeridentifikation durch Browser-Fingerprinting [1], doch sollte man sich nicht von Meldungen wie dieser dazu verleiten lassen, aus Gründen der „Unauffälligkeit“ seinen Browser nur noch in der Standardeinstellung zu betreiben, um sich damit dann ein Riesenloch in seine Sicherheitsinfrastruktur zu reißen.

Aus Gründen der Datensicherheit und des Schutzes vor allerlei Datenkraken ist es sehr wohl sinnvoll, seinen „Netzausbreiter“ so gut wie möglich abzudichten. Dabei ist es weitaus zielführender, statt dem unendlichen Versions- und Updatewahn hinterher zu hecheln, lieber grundlegende Risiken auszuschalten, indem man seinen Browser vernünftig konfiguriertund auf in der Mozilla-Welt verfügbare Erweiterungen zu setzen.

Neben Firefox (auf debian-basierten Distributionen heißt er aus lizenzrechtlichen Gründen „Iceweasel“; bei Ubuntu und Derivaten werden für Mozilla-Produkte allerdings wieder die Originalbezeichnungen verwendet) beinhaltet übrigens Seamonkey (Debian: „Iceape“, das Community-Projekt der inzwischen eingestellten Mozilla-Suite) seit Version 2 ebenfalls eine Erweiterungsschnittstelle, genauso wie der E-Mail-Client Thunderbird (Debian: „Icedove“).



So weit muss man es mit der Absicherung nicht unbedingt treiben.

Die hier vorgestellte Übersicht soll als Einblick in diese Thematik dienen, sie kann keineswegs vollständig sein, dafür sollte sie aber zu weiterer Recherche anregen. Auch überschneidet sich der Einsatzzweck einiger Erweiterungen, was aufgrund der Inkompatibilität mit einigen Browserversionen zu mehr Flexibilität führen dürfte, da nicht jede Browserversion mit jeder der aufgeführten Erweiterungen funktioniert.

Eine sehr gut sortierte Zusammenstellung zahlreicher Erweiterungen für die verschiedenen Mozilla-Produkte bietet die inzwischen eingefrorene, aber nach wie vor verfügbare Webseite erweiterungen.de [2], die rund die Hälfte der hier vorgestellten Erweiterungen listet. Von dort kann man die zahlreichen auf deutsch verfügbaren Erweiterungen installieren und über den Erweiterungsmanager des Browsers aktualisieren lassen, da es manchmal mühsam ist, auf den meist englischsprachigen Webseiten die deutsche bzw. internationale Version zu finden.

Einige Erweiterungen überprüfen beim Start des Browsers selbstständig, ob neue Versionen verfügbar sind, es empfiehlt sich aber dennoch, regelmäßig über den Erweiterungsmanager nach Aktualisierungen suchen zu lassen. Die Kompatibilität zu den unterschiedlichen Browserver-

sionen verändert sich im Laufe der Zeit. Somit empfiehlt es sich, auf der jeweiligen Homepage der Erweiterung in die Änderungsdatei (Changelog) zu schauen und im Falle der Inkompatibilität nach alternativen Erweiterungen zu suchen bzw. die letztmögliche Version zu verwenden (die normalerweise auf der Mozilla-AddOns-Seite ganz unten zu finden ist), denn es ist meist besser, eine Erweiterung mit älterer Versionsnummer zu benutzen, als sie auszulassen. Sollte es zu Problemen kommen, kann man im Firefox-Erweiterungsmanager per Rechtsklick die Aktualisierung für jede Erweiterung einzeln vornehmen.

Generell empfiehlt es sich, statt auf potentiell unsichere Plug-ins zu setzen (vor allem, wenn diese proprietärer Herkunft sind), die jeweiligen Medien (Audio, Video, PDFs etc.) manuell herunterzuladen und anschließend mit möglichst quelloffener Software einzusehen. Das erhöht zwar im Vergleich zu gestreamten und somit häufig nur teilweise konsumierten Medien in einzelnen Fällen die Serverlast, aber ebenso die Sicherheit des Anwenders. Eventuell lässt man vorher noch einen Virenscanner über die Medien schauen.

Die Erweiterungen

NoScript

Der wohl größte Anteil an Sicherheitsschwankungen wird hervorgerufen durch JavaScript in Kombination mit anderen Techniken. Da man JavaScript beim normalen Surfen in der Regel nicht braucht, sollte es standardmäßig deaktiviert werden, um Folgeschäden zu vermeiden. Dazu bietet sich in idealer Form die Erweiterung „NoScript“ an. Die standardmäßig blockierten Skripte lassen sich temporär (bis zum Ende der Sitzung) oder dauerhaft (bei regelmäßig besuchten Seiten) über das in der Statusleiste des Browsers erscheinende Icon aktivieren.

Das Ganze hat dann noch einige begrüßenswerte „Randerscheinungen“: Während JavaScript auf der Hauptseite aktiviert ist, bleiben die Skripte in den potentiell Schadcode-belasteten Werbeeinblendungen weiterhin deaktiviert. Viele dieser Einblendungen kann man ergänzend mit der unten beschriebenen Erweiterung „Adblock Plus“ komplett entfernen. Man kann somit die Webseite mit JavaScript bedienen, ohne gleichzeitig schmutziges Beiwerk mitgeliefert zu bekommen. Darüber hinaus kann „NoScript“ noch viel mehr: Neben JavaScript kann diese Erweiterung diverse potentiell gefährliche oder instabile Plugins blockieren (z. B. Flash, Silverlight etc.) sowie manche Datensammelei verhindern und Randgefahren, wie z. B. Umleitungen auf andere potentiell Schadcode-belastete Webseiten, verhindern.

Achtung: JavaScript muss in den Browser-Optionen aktiviert bleiben, da es durch die Erweiterung selbst blockiert wird. Bei der weiter unten beschriebenen Erweiterung „Cookie Button . . . “ verhält es sich dagegen genau umgekehrt.

Info/Download:

- http://www.noscript.net/
- https://addons.mozilla.org/de/firefox/addon/noscript/

Cookie Button in the status bar („CBitsb“)

Die Erweiterung „CBitsb“ verhält sich in gewisser Weise ähnlich wie „NoScript“. Mit ihr können Cookies generell gesperrt und bei Bedarf für einzelne Webseiten temporär oder dauerhaft aktiviert werden. Die Steuerung funktioniert ebenfalls über ein Symbol in der Statusleiste des Browsers.

Im Gegensatz zur JavaScript-Steuerung mittels „NoScript“ müssen die Cookies bei „CBitsb“ in den Browser-Optionen gesperrt werden. Die Erweiterung entsperrt sie dann entsprechend der Konfiguration.

Info/Download:

- https://addons.mozilla.org/de/firefox/addon/cookie-button-in-the-status-ba/

View Cookies

Den Inhalt der ungeliebten „Datenkekse“ kann man mit „View Cookies“ in einem separaten Browser-Tab anschauen.

Info/Download:

- https://addons.mozilla.org/de/firefox/addon/view-cookies/

Flashblock

Wer „NoScript“ nicht verwenden kann oder möchte, kann alternativ mit der Erweiterung „Flashblock“ Flash und Silverlight blockieren.

Info/Download:

- http://flashblock.mozdev.org/
- https://addons.mozilla.org/de/firefox/addon/flashblock/

Adblock Plus
Mit „Adblock Plus“ können Filterlisten, die Quelltextmuster beinhalten, abonniert werden, um Werbung und andere lästige Einblendungen von diversen „Dienstleistern“ auszublenden. Zusätzlich können diese Listen durch eigene Filterregeln erweitert werden. Zur einfacheren Verwaltung empfiehlt sich zusätzlich die Installation der Erweiterung „Adblock Plus: Element Hiding Helper“.

Info/Download:

- http://www.adblockplus.org/de/
- https://addons.mozilla.org/de/firefox/addon/adblock-plus/
- http://www.erweiterungen.de/detail/Adblock_Plus_Element_Hiding_Helper/
- https://addons.mozilla.org/de/firefox/addon/elemhidehelper/

Remove It Permanently
Ergänzend zu „Adblock Plus“ ermöglicht „RIP“ das permanente Blocken von unerwünschten Webseiteninhalten.

Info/Download:

- http://rip.mozdev.org/

RefControl
Der sogenannte Referer teilt einer Webseite mit, von wo aus man herkommt, sodass z. B. in Kombination mit Cookies ein Besucherprofil erstellt werden kann. Das hat in der Regel wenig Mehrwert für den Seitenbesucher, birgt aber hohes Missbrauchspotential und sollte somit blockiert werden. Einzelne Domains können bei Bedarf in einer Liste von der Sperrung ausgenommen werden. Der Browser Opera kann diese Information übrigens von Haus aus nach entsprechender Konfiguration blockieren.

Nach Installation von „RefControl“ muss die standardmäßige Blockierung noch aktiviert und die Standardregel auf „*Blockieren*“ gesetzt werden. Zur bequemen Umschaltung erscheint ein Button in der Statuszeile des Browsers, falls die Zusammenarbeit mit einigen Webseiten (wie beispielsweise bei Download-Portalen) aufgrund der Referer-Blockierung einmal scheitern sollte.

Info/Download:

- http://www.stardrifter.org/refcontrol/
- https://addons.mozilla.org/de/firefox/addon/refcontrol/

No-Referer
Die Erweiterung „No-Referer“ stellt eine Alternative zu „RefControl“ dar. Beim Öffnen von Links in einen neuen Tab per Rechtsklick erscheint im Kontextmenü ein weiterer Eintrag, der den Klick ohne Übermittlung des Referers ermöglicht.

Info/Download:

- https://addons.mozilla.org/de/firefox/addon/no-referer/

BetterPrivacy
Mit „BetterPrivacy“ wird man die penetranten „Flash-Cookies“ [3] los, die von Webseiten wie YouTube und eBay zur Erstellung von Besucherprofilen gesetzt werden. Diese Objekte lassen sich nämlich nicht über den normalen Cookie-Manager des Browsers entfernen.

Info/Download:

- https://addons.mozilla.org/de/firefox/addon/betterprivacy/

IDN Info
Beim sogenannten Domain Spoofing wird der Besucher durch Austausch ähnlich aussehender Zeichen (z. B. aus dem kyrillischen Zeichensatz) im Domain-Namen unbemerkt auf eine zwar visuell gleich aussehende, aber logisch andere Domain gelockt, um von dort seinen Rechner anzugreifen. „IDN Info“ warnt den Besucher durch ein entsprechendes Icon.

Info/Download:

- http://www.erweiterungen.de/detail/IDN_Info/

SpoofStick
„SpoofStick“ gibt durch eine Texteinblendung in der Menüleiste zu erkennen, ob man auf eine gefälschte Seite umgeleitet worden ist. Die in der Regel kryptischen, gefälschten Internet-Adressen werden in eine für Menschen leichter lesbare Form gebracht und sind laut Hersteller ein brauchbarer Start, nicht auf die Fälschungen hereinzufallen.

Info/Download:

- http://www.spoofstick.com/

LayerBlock
Über so genannte Layer (Ebenen) lassen sich Seitenelemente exakt positionieren. Aber auch

Werbung einblenden, die nicht durch Popup-Filter oder Deaktivierung von JavaScript ausgeblendet werden kann. „LayerBlock“ sperrt diese Form der Werbeeinblendungen. Zahlreiche bekannte Standard-Werbe-Layer können alternativ von der oben beschriebenene Erweiterung „AdBlock Plus“ blockiert werden.

Info/Download:

- http://home.arcor.de/jonha/lb/

FoxyProxy
Mit der Erweiterung „FoxyProxy“ lassen sich sehr komfortabel Proxydienste, wie z. B. Jondos/JAP [4], verwalten und nach Bedarf per Button ein- und ausschalten. Das erspart das lästige und fehleranfällige manuelle Umstellen der Netzwerkeinstellungen des Browsers.

Info/Download:

- http://foxyproxy.mozdev.org/
- https://addons.mozilla.org/de/firefox/addon/foxyproxy-standard/

SwitchProxy Tool („SPT“)
„SPT“ geht in die gleiche Richtung wie die oben angesprochene Erweiterung „FoxyProxy“, bietet allerdings weniger Optionen (so fehlt z. B. der „Tor Wizard“), tut aber grundlegend seinen Dienst.

Info/Download:

- http://www.erweiterungen.de/detail/SwitchProxy_Tool/

Torbutton
„Torbutton“ ist eine sehr leistungsfähige Erweiterung mit zahlreichen sicherheitsrelevanten Optionen zur Teilnahme am Tor-Proxynetzwerk [5]. Ähnlich wie die beiden oben genannten Proxy-Erweiterungen lässt sich das Proxy-Netzwerk per Klick auf einen Statusleisteneintrag bequem ein- und ausschalten.

KDE-Nutzern empfiehlt sich darüber hinaus die Installation des Konfigurationswerkzeugs TorK [6].

Info/Download:

- http://www.torproject.org/torbutton/
- https://addons.mozilla.org/de/firefox/addon/torbutton/

Tor-Proxy.NET-Toolbar
Über diese Erweiterung wird eine Toolbar installiert, in die man die zu besuchende Webadresse eingeben kann, die man dann verschlüsselt über den Anonymisierungsdienst von Tor-Proxy.NET aufrufen kann, der die Anfragen zur weiteren Verschleierung an einen Proxy-Dienst wie Tor oder JonDos/JAP weiterleitet.

Info/Download:

- http://tor-proxy.net/index.php?q=de/node/5
- https://addons.mozilla.org/de/firefox/addon/tor-proxynet-toolbar/

HTTPS Everywhere
„HTTPS Everywhere“ greift, soweit eine entsprechende Unterstützung durch die Webseite angeboten wird, über HTTPS auf die jeweiligen Seiteninhalte zu und versucht, HTTP-Verlinkungen in die sichere HTTPS-Version umzuwandeln. Das klappt allerdings nicht immer zur vollen Zufriedenheit, wie Oliver Herold detailliert erläutert [7]. Eine permanente Kontrolle ist also nötig.

Info/Download:

- http://www.eff.org/https-everywhere

Quick Locale Switcher
Mittels des „Quick Locale Switcher“ kann man einer Browserweiche vortäuschen, aus einem anderen Land zu kommen, um somit anders lokalisierte Webseiten betrachten zu können. Außerdem kann man damit wunderbar „Datenkraken“ irritieren.

Aus einer sehr umfangreichen Liste verfügbarer „Herkunftsländer“ kann man sich eine Auswahl zusammenstellen. Nach Wechsel der Lokalisierung wird man allerdings zum Neustart des Browsers aufgefordert.

Info/Download:

- https://addons.mozilla.org/de/firefox/addon/quick-locale-switcher/

User Agent Switcher
Vergleichbar mit der oben genannten Erweiterung „Quick Locale Switcher“ kann man über den „User Agent Switcher“ eine falsche Browserkennung senden, da es leider immer noch Webdesigner gibt, die offensichtlich der Meinung sind, dass es nur einen Browser (und ein Betriebssystem) auf der Welt gibt. Möglicherweise lassen

sich so sonst nicht zugreifbare Webseiten benutzen. Darüber hinaus kann man damit YouTube überreden, wieder Flash mit Firefox 2 abzuspielen, da man dort inzwischen ohne erkennbaren Grund „leicht penetrant“ gedrängt wird, seinen Browser zu aktualisieren.

Auch ist es möglich, sich als Suchmaschinen-Spider auszugeben. Es lassen sich beliebige Kennungen erzeugen sowie die Liste der Kennungen im- und exportieren.

Info/Download:

- http://chrispederick.com/work/user-agent-switcher/
- https://addons.mozilla.org/de/firefox/addon/user-agent-switcher/

SafeCache/SafeHistory
Es gibt Angriffsmethoden, bei denen durch das Auslesen der Link-Einfärbung besuchter Webseiten ein Profiling des Seitenbesuchers möglich ist bzw. der Besuch einer (unliebsamen) Webseite nachgewiesen werden kann. Die beiden Erweiterungen „SafeCache“ und „SafeHistory“ unterbinden dieses Loch in der Privatsphäre.

Info/Download:

- http://www.safecache.com/
- https://addons.mozilla.org/de/firefox/addon/safecache/
- http://www.safehistory.com/
- https://addons.mozilla.org/de/firefox/addon/safehistory/

ShowIP
Die Erweiterung „ShowIP“ zeigt die IP-Adresse der gerade besuchten Webseite in der Statuszeile an. Das erhöht die Chancen, nicht auf verdeckte Umleitungen hereinzufallen.

Info/Download:

- https://addons.mozilla.org/de/firefox/addon/showip/

My IP Tool („IPT“)
„IPT“ zeigt über ein Symbol in der Statusleiste die lokale bzw. öffentliche IP-Adresse des Computers an. Dies kann z. B. zur Funktionskontrolle eines Proxy-Dienstes eingesetzt werden.

Info/Download:

- http://fux.zuhage.de/my_ip_tool/
- http://www.erweiterungen.de/detail/My_IP_Tool/

Fazit

Zusammengefasst erhöhen die oben genannten Erweiterungen Komfort und Sicherheit der gängigen Mozilla-Produkte. Da es auch in Zukunft keine wirklich „sichere“ Applikationen geben wird, ist es sinnvoller, mit einer entsprechenden Zusatzausstattung seine Anwendungen größtmöglich abzudichten. Dann kann man sich auch fast ohne schlechtes Gewissen mit der Lieblingsversion seines Lieblingsbrowsers im Netz bewegen. Der Google-Browser Chrome enthält inzwischen auch eine ähnliche Erweiterungsschnittstelle. Mit Firefox 4 soll allerdings eine neue Erweiterungsschnittstelle eingeführt werden, um z. B. den Neustart der Anwendung nach Installation und Aktualisierung der Erweiterungen unnötig zu machen.

Darüber hinaus lohnt sich ebenfalls die Auseinandersetzung mit sicherheitsrelevanten Erweiterungen für den E-Mail-Client Thunderbird wie auch dem gerade erschienenen Opera 11, der nun ebenfalls eine Erweiterungsschnittstelle beinhaltet.

LINKS

[1] http://www.pro-linux.de/news/1/15331/1,eff-gegen-browser-fingerprinting.html
[2] http://www.erweiterungen.de/
[3] https://secure.wikimedia.org/wikipedia/de/wiki/Flash-Cookie
[4] http://anonymous-proxy-servers.net/de/
[5] http://www.torproject.org/
[6] http://www.anonymityanywhere.com/tork/
[7] http://www.fixmbr.de/fragwuerdige-sicherheit-mittels-effs-https-everywhere/

Autoreninformation

Bodo Schmitz (Webseite) wollte seinen Browser sehr weit absichern. Mit den im Artikel beschriebenen Erweiterungen erreichte er dabei ein höheres Sicherheitsniveau, als es die Standard-Einstellmöglichkeiten des Browsers je bieten können.

Diesen Artikel kommentieren