Bild: Andreas Martini

Einfach nur surfen

Surfen ohne Cookies, Tracking und Reklame

Man nehme Firefox, eine Handvoll Einstellungen und eine Prise Erweiterungen: Heraus kommt ein datenschutzfreundlicher Browser, der Ihre Nerven schont. Mit unserem Browser-Rezept surfen Sie deutlich entspannter – ganz ohne Cookie-Banner, Tracking und aufdringliche Reklame.

Von Ronald Eikenberg

Unerwünschte Dreingaben wie Tracking-Cookies und Werbung sind tägliche Begleiter, wenn man nur mal die News lesen oder online shoppen möchte. Doch das müssen Sie nicht hinnehmen: Mit unseren Empfehlungen konfigurieren Sie den Firefox-Browser so, dass er alle lästigen Elemente entfernt. Das schont Ihre Nerven und schützt Ihre Daten, denn hinter den Kulissen arbeitet ein effektiver Trackingschutz. Und die Zeiten, in denen Sie ein Cookie-Banner weggeklickt haben, sind auch vorbei.

Wir haben den von Haus aus datenschutzfreundlichen Firefox-Browser so eingerichtet, dass die Inhalte im Vordergrund stehen und unser Setup über mehrere Monate im Alltag getestet. Das Experiment verlief erfolgreich und der Unterschied ist deutlich sichtbar: Wo beim Aufrufen einer Website bislang nur ein schmaler Schlitz vom eigentlichen Inhalt zu sehen war – den Rest hatten Cookie-Banner und Werbung unter sich aufgeteilt – wurde nach den Änderungen die gesamte Bildschirmfläche für die eigentlichen Inhalte genutzt. Außerdem hinterließen wir beim Surfen deutlich weniger Datenspuren.

Unsere Beispielkonfiguration für PCs und Macs ist bestmöglich auf Komfort und Datenschutz ausgerichtet, was durchaus einen Kompromiss bedeutet: Denn viel Komfort bedeutet oft wenig Datenschutz und umgekehrt. Uns war wichtig, dass der

Browser komfortabel bedienbar bleibt und Websites weitgehend wie gewohnt funktionieren, ohne dass ein Nachjustieren der Privacy-Schutzfunktionen nötig ist. Dennoch sollte ein effektiver Schutz vor dem Website-übergreifenden Tracking greifen.

Starten Sie am besten mit einer frischen Installation der aktuellen Firefox-Version. Wenn Sie den Mozilla-Browser bereits eingerichtet haben und unsere Empfehlungen erstmal risikolos testen möchten, können Sie hierfür einfach ein neues Profil anlegen: Öffnen Sie mit Firefox die interne Adresse `about:profiles` und klicken Sie auf „Neues Profil anlegen“. Geben Sie dem Profil einen beliebigen Namen, etwa „Ungestört surfen“ und klicken Sie danach, zurück in der Profilverwaltung, auf „Profil zusätzlich ausführen“, um eine neue Browserinstanz mit dem leeren Profil zu öffnen. Das neue Profil wird automatisch zum Standard und fortan mit Firefox gestartet. Um das rückgängig zu machen, klicken Sie in der Profilverwaltung beim alten Profil (etwa „default-release“) auf „Als Standardprofil festlegen“.

Strenger Tracking-Schutz

Zunächst gilt es, die Bordmittel von Firefox optimal einzurichten. Öffnen Sie die Einstellungen über den Menüknopf oben rechts (drei Linien) und wechseln Sie auf „Datenschutz & Sicherheit“. Stellen Sie den Trackingschutz unter „Verbesserter Schutz vor Aktivitätsverfolgung” auf „Streng“ für die bestmögliche Privatsphäre. Seit Firefox 86 schalten Sie damit die „Total Cookie Protection“ ein, die quasi dafür sorgt, dass jede Website Ihre eigene Keksdose bekommt.

Angenommen, Facebook liefert Ihnen beim Besuch von Website A ein Cookie, weil dort ein Like-Button oder ein Facebook-Post eingebettet wurde. Anschließend surfen Sie auf Website B, die ebenfalls mit eingebetteten Facebook-Inhalten arbeitet. Normalerweise würde Ihre Browser jetzt das Cookie von Website A an Facebook senden, weil es zur gleichen externen Domain passt und Facebook könnte nachvollziehen, dass Sie zunächst auf Website A und dann auf Website B waren. Die neue Schutzfunktion verhindert dies effektiv, weil sich Firefox merkt, dass das Cookie beim Besuch von Website A ausgeliefert wurde. Beim Besuch von Website B steht es nicht zur Verfügung.

So wird verhindert, dass Sie beim Surfen auf Schritt und Tritt durch Third-Party-Cookies verfolgt werden können. Firefox warnt davor, dass „einige Websites nicht korrekt Inhalte anzeigen oder funktionieren“, wenn Sie den Trackingschutz voll aufdrehen. Im Alltag konnten wir jedoch nur geringe Komforteinbußen feststellen. So wurden von extern eingebettete Social-Media-Inhalte auf Websites nicht mehr automatisch geladen. Stattdessen fand wir jedoch stets einen Link vor, über den wir den jeweiligen Beitrag direkt aufrufen konnten.

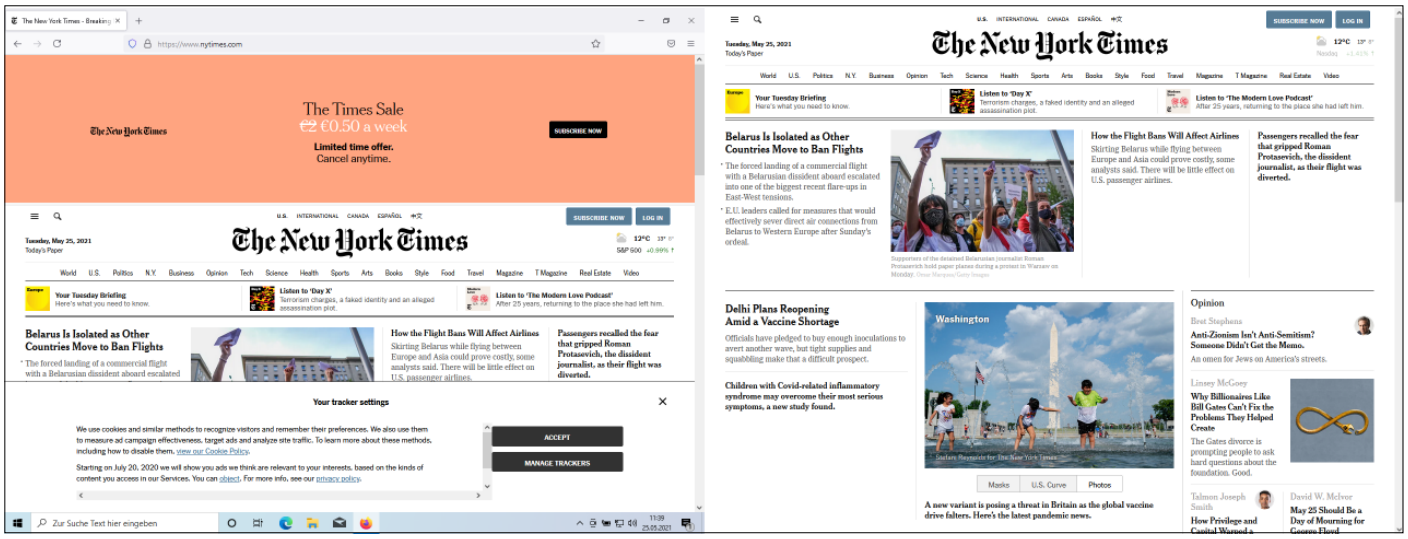
Mozilla nennt diesen Schutz auch „Dynamic Partitioning“ (siehe ct.de/y5et), er betrifft neben den Cookies etwa auch das localStorage-API. Hinter den Kulissen speichert Firefox den Ursprung der Cookies in seiner Cookie-Datenbank (cookies.sqlite) durch einen sogenannten Partition-Key, zum Beispiel `partitionKey=(https,heise.de)`.

Falls Ihnen der erweiterte Trackingschutz einmal in die Quere kommt, klicken Sie einfach auf das Schutzschild-Symbol links in der Adressleiste und deaktivieren Sie den Schalter „Verbesserter Schutz vor Aktivitätsverfolgung ist für diese Website AKTIVIERT“, um die problematische Website auf die Ausnahmeliste zu setzen. Dort erfahren Sie auch, was Firefox auf der aktuellen Website blockiert hat.

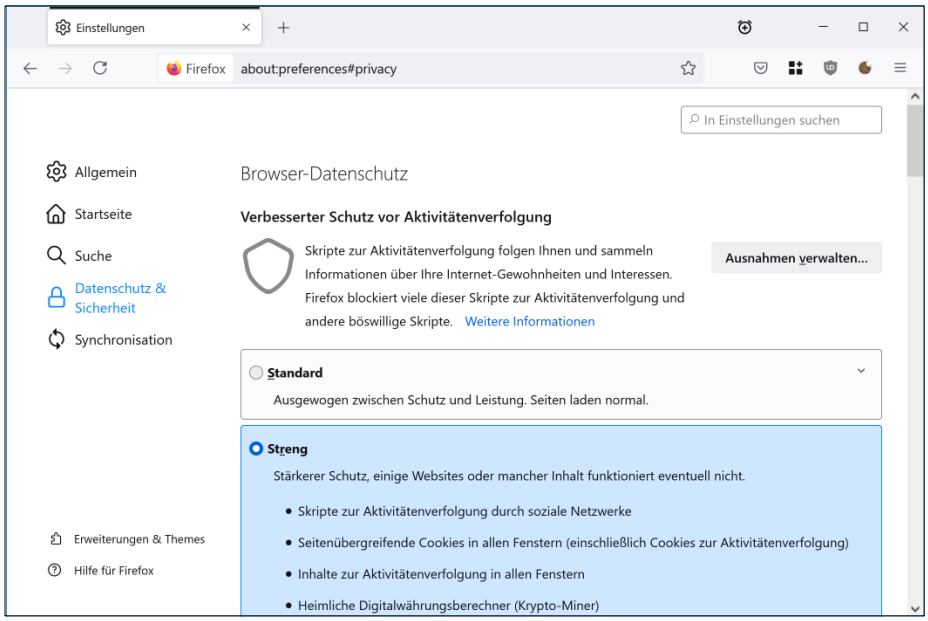
Alternativ können Sie den Tracking-Blocker auch im Standardmodus betreiben – das ist immer noch deutlich besser als nichts, denn Firefox blockiert auch in diesem Modus bekannte Tracking-Cookies und -Skripte. Zudem ist in beiden Betriebsmodi das sogenannte „Network Partitioning“ aktiv, welches Supercookies eliminieren soll, die Browserfunktionen als Tracking-Helfer zweckentfremden. Aktivieren Sie unterhalb der Tracking-Blocker-Einstellung noch die „Do No Track“-Header, um Websites mitzuteilen, dass Sie nicht getrackt werden möchten.

Diagnose und Sicherheit

Wenn Sie mögen, können Sie unter „Datenerhebung durch Firefox und deren Verwendung“ alle Häkchen entfernen, damit Firefox keine Diagnosedaten über Ihre Installation an Mozilla sendet. Sie sollten auch in Erwägung ziehen, unter „Suche“ die Suchvorschläge in der Adressleiste zu deaktivieren. Diese Funktion sorgt dafür, dass Firefox beim Tippen in der Adresszeile jedes Zeichen an Google sendet, um passende Suchvorschläge abzurufen.



Vorher und nachher: Wenn Sie alle Empfehlungen befolgen, zeigt Ihnen Firefox schon beim ersten Besuch einer Website deutlich mehr vom eigentlichen Inhalt.



Viel hilft viel: Auf der Stufe „Streng“ fängt der Trackingschutz von Firefox jede Menge weg.

Wenn Ihnen Google ohnehin suspekt ist, sollten Sie hier auch gleich eine andere Standardsuchmaschine einstellen, zum Beispiel die Privacy-freundliche Alternative DuckDuckGo.

Noch kurz ein Wort zum Thema Sicherheit: Der wichtigste Schutz heißt Aktualität! Halten Sie Ihren Browser stets auf dem aktuellen Versionsstand, da mit fast jedem Update auch Sicherheitslücken geschlossen werden. Stellen Sie sicher, dass in den Einstellungen unter „Allgemein / Firefox-Updates“ die Option „Firefox erlauben ... Updates automatisch zu installieren (empfohlen)“ ausgewählt ist. Unter „Datenschutz & Sicherheit / Sicherheit“ sollte zudem der „Schutz vor betrügerischen Inhalten und gefährlicher Software“ aktiv sein sowie darunter die automatische Überprüfung von Zertifikaten mittels OCSP.

Um zu verhindern, dass Firefox Daten im Klartext in die weite Welt schickt, können Sie darunter den „Nur-HTTPS-Modus in allen Fenstern aktivieren“. Dann zeigt Firefox eine Warnung an, bevor eine unverschlüsselt übertragene HTTP-Website geöffnet wird. Davon gibt es noch ein paar, Sie werden den Warnhinweis also dann und wann zu Gesicht bekommen. In diesem Fall wissen Sie Bescheid, dass Sie auf der folgenden Website keine sensiblen Daten eintippen sollten. Sinnvoll ist auch, unter „Allgemein / Verbindungs-Einstellungen“ ein Häkchen bei „DNS über HTTPS aktivieren“ zu setzen, damit Firefox Ihre DNS-Anfragen verschlüsselt durchführt. Sie haben die Wahl zwischen Cloudflare und NextDNS, die beide an Mozillas Trusted-Recursive-Resolver-Programm teilnehmen. Damit verpflichten sie sich unter anderem, anfallende Daten über die Nutzung nach spätestens 24 Stunden zu löschen. Alternativ können Sie einen beliebigen anderen Anbieter einstellen, dem Sie vertrauen.

Bitte keine Werbung einwerfen

Damit haben Sie die wichtigsten Browsereinstellungen erledigt. Nach so viel Fleißarbeit hinter den Kulissen soll es jetzt um den Komfort gehen. Mit geringem Aufwand können Sie Ihren Surfalltag sicht- und spürbar verbessern, indem Sie all die nervigen Dinge auf Websites eliminieren.

Zunächst einmal sollten Sie Ihren Browser mit einem unabhängigen Content-Blocker ausstatten, der Websites auch – aber nicht nur – von Werbung befreit. Bewährt hat sich uBlock Origin von Raymond Hill, das Sie über das Add-on-Verzeichnis (siehe ct.de/y5et) mit zwei Klicks an den Start bringen. Den Content-Blocker gibt es übrigens nicht nur für Firefox, sondern für alle wichtigen Desktop-Browser. Er ist stimmig vorkonfiguriert, sodass Sie normalerweise nichts weiter einstellen müssen. Da sich auf den voreingestellten Filterlisten auch etliche bösartige URLs befinden, sorgt uBlock nicht nur für Komfort, sondern auch für Sicherheit.

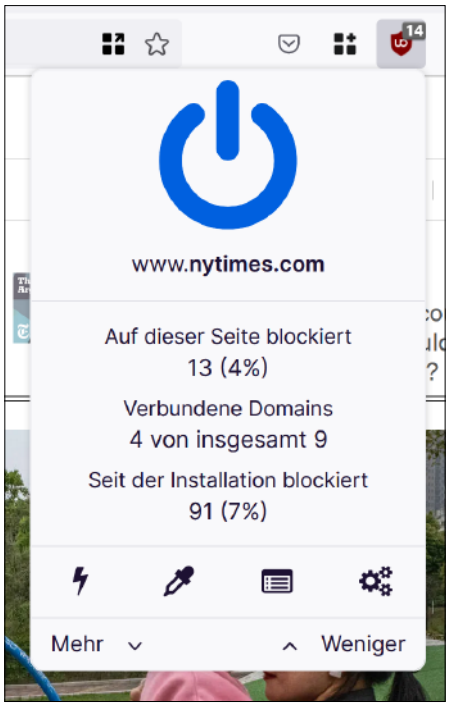
Über den roten Schutzschild in der Symbolleiste erfahren Sie, wie viele Elemente uBlock auf der aktuellen Website blockiert hat. Klicken Sie ihn an und zweimal auf „Mehr“, erfahren Sie auch, um welche Elemente es geht. Von den rot markierten Domains hat die Erweiterung sämtliche Elemente blockiert, von den orange markierten nur manche. Wenn eine Website nicht wie gewohnt funktioniert, klicken Sie einfach auf den großen blauen Ausschalter im uBlock-Menü und auf den Aktualisieren-Knopf, der rechts daneben erscheint. Der Content-Blocker ist dann für diese Website deaktiviert. Dies ist insbesondere dann nötig, wenn eine Website den Blocker erkennt und die Auslieferung der Inhalte verweigert.

Falls Ihnen die vordefinierten Filter mal nicht weit genug gehen, klicken Sie im uBlock-Menü auf das Blitzsymbol, um den Element-Entfernungsmodus zu starten. Klicken Sie anschließend auf das störende Element der Website, um es sofort zu entfernen. Mit der Pipette neben dem Blitz können Sie den neuen Filter nach der Auswahl des Elements zunächst ausprobieren und feinjustieren, ehe Sie ihn dauerhaft übernehmen. Ihre neuen Filter, die genutzten Filterlisten und viele weitere Einstellungen finden Sie in den uBlock-Optionen, die Sie über das Zahnrad-Symbol erreichen.

Keksdiät

Sie surfen jetzt zumeist werbefrei, ein weiterer Störfaktor ist jedoch noch übrig: Auf fast allen Websites werden Sie von Cookie-Consent-Bannern begrüßt, um die sich uBlock Origin erstmal nicht kümmert. Es gibt zwar kompatible Filterlisten dagegen, jedoch haben diese in unserem Praxistest nur mäßig funktioniert, da es häufig nicht ausreicht, das Banner zu blockieren – es muss bestätigt werden. Greifen Sie daher am besten gleich zu der Browser-Erweiterung „I don't care about cookies“, die es für alle relevanten Desktop-Browser gibt (siehe ct.de/y5et).

Die Erweiterung tut, was nötig ist, um das Cookie-Banner loszuwerden. In Härtefällen klickt sie auf den „Akzeptieren“-Knopf, was Sie daran erkennen, dass das Banner zunächst angezeigt wird und im nächsten Augenblick wieder verschwindet, ohne dass Sie aktiv werden müssen. Behalten Sie bei der Konfiguration Ihres Browsers im Hinterkopf, dass Sie „I don't care about cookies“ zwar vor den lästigen Cookie-Dialogen bewahrt, nicht aber vor den Cookies selbst. Sie sollten also zusätzlich den Trackingschutz wie oben beschrieben scharf schalten.



Wer ungestört surfen will, sollte einen unabhängigen Content-Blocker wie uBlock Origin nachrüsten.

Es ist sinnvoll, uBlock Origin und „I don't care about cookies“ auch für den privaten Browsermodus zu freizugeben, denn standardmäßig sind Add-ons dort nicht aktiv. Öffnen Sie hierzu die Add-ons-Verwaltung über das Firefox-Menü oder `about:addons`. Klicken Sie bei der jeweiligen Erweiterung rechts auf den Knopf mit den drei Punkten und „Verwalten“. Unter „Details / In privaten Fenstern ausführen“ wählen Sie anschließend „Erlauben“ aus. Bei den nun im Artikel folgenden Erweiterungen ist dies hingegen nicht nötig.

Datenschutz-Container

Mit Cookies ist es kompliziert: Es geht nicht mit, aber auch nicht ohne. Die oben vorgestellte Total Cookie Protection von Firefox versucht bereits, das Problem für Sie zu lösen, indem sie praktisch für jede Website einen eigenen Cookie-Speicher anlegt. Das funktioniert gut, allerdings haben Sie keine Kontrolle darüber. Mit Containern könnten Sie das Konzept weiter ausbauen.

Das Prinzip ist schnell erklärt: Sie öffnen Websites in Containern, die von voneinander abgeschottet sind. Die Websites in Container A können nicht auf die Ressourcen von Container B zugreifen. Das ist fast so, als würden Sie mehrere Browser parallel nutzen – nur viel komfortabler, da die Container als farblich markierte Tabs im gleichen Browserfenster laufen. So verhindern Sie nicht nur Website-übergreifendes Tracking, Sie können zum Beispiel auch Berufliches und Privates sauber voneinander trennen oder sich auf einer Website mit zwei Accounts gleichzeitig einloggen, indem Sie die Site in zwei Containern öffnen.

Wir haben das Konzept über Monate im Alltag ausprobiert und zu schätzen gelernt. Wenn Sie Ihre wichtigsten Websites einmalig mit passenden Containern verknüpfen, etwa Arbeit, Freizeit, Banking und Shopping, haben Sie damit anschließend keine Arbeit mehr: Die Websites werden fortan automatisch in den gewünschten Containern geöffnet. Wenn Sie den

erweiterten Trackingschutz aktiviert haben, arbeitet dieser parallel dazu weiter. Gehen Sie am besten noch einen Schritt weiter und lassen Sie alle anderen Websites in temporären Tabs öffnen, um zu verhindern, dass selten oder einmalig angesteuerte Sites Cookies auf Ihrem Rechner hinterlassen – auch das ganz automatisch.

Die wichtigste Container-Erweiterung heißt „Firefox Multi-Account Containers“ und stammt direkt von Mozilla (siehe ct.de/y5et). Nach der Installation finden Sie einen neuen Knopf mit drei Kästchen und einem Pluszeichen oben rechts in der Symbolleiste des Browsers. Nach der Begrüßung können Sie darüber (oder Strg+Punkt) die Container-Einstellungen öffnen. Es sind bereits vier Container für Freizeit, Arbeit, Banking und Einkaufen eingerichtet, die Sie direkt benutzen können. Beliebige weitere legen Sie über „Manage Containers“ an.

Klicken Sie im Menü der Erweiterung auf einen Container, öffnet sie einen neuen Browser-Tab. Sie erkennen den aktuell genutzten Container an der farbigen Linie am oberen Rand des Tab-Titels und dem Containernamen in der Adresszeile. Richtig komfortabel wird das Leben mit den Containern erst, wenn Sie die Erweiterung anweisen, bestimmte Websites automatisch im passenden Container zu öffnen. Steuern Sie hierzu eine Website an und klicken Sie anschließend auf den Knopf der Erweiterung und „Always Open This Site in...“. Danach wählen Sie den Container aus, in dem die Site künftig geöffnet werden soll. Beim nächsten Aufruf der Website werden Sie noch gefragt, ob sie wirklich im zugeordneten Container geöffnet werden soll. Damit diese Rückfrage in Zukunft ausbleibt, klicken Sie auf „Remember my decision for this site“ und “Open in [Name] Container”. Fahren Sie so mit allen Websites fort, die Sie regelmäßig ansteuern.

Wenn Sie in einem Container-Tab einen Link anklicken oder eine beliebige Adresse eintippen, wird auch die folgende Website in dem Container geöffnet. Das ist nicht immer erwünscht: Wenn Sie etwa den Container „Arbeit“ ausschließlich mit Intranet-Websites verknüpft haben, möchten Sie wahrscheinlich nicht, dass auch Links auf externe Websites darin laufen. Das verhindern Sie, indem Sie unter „Manage Containers“ auf einen Container klicken und dort die Option „Limit to Designated Sites“ aktivieren. Wenn es keinen passenden Container gibt, werden externe Sites dann wie gewohnt containerlos geöffnet. Ein Blick in die Vorabversion von Firefox 90 zeigt, dass Mozilla offenbar daran arbeitet, die Containerfunktion auch ohne Erweiterung nutzbar zu machen. Allerdings ist es hier bislang nicht möglich, Websites fest mit Containern zu verknüpfen.

Cookies im Wegwerf-Container

Grundsätzlich sollten Sie sich die Frage stellen, ob Websites, denen Sie keine Container zugeordnet haben, überhaupt dauerhaft Cookies speichern sollen – denn dort profitiert man nur selten davon. Während unseres Experiments haben wir Gefallen an einer weiteren Container-Erweiterung gefunden, nämlich „Temporary Containers“ von stoically (siehe ct.de/y5et).

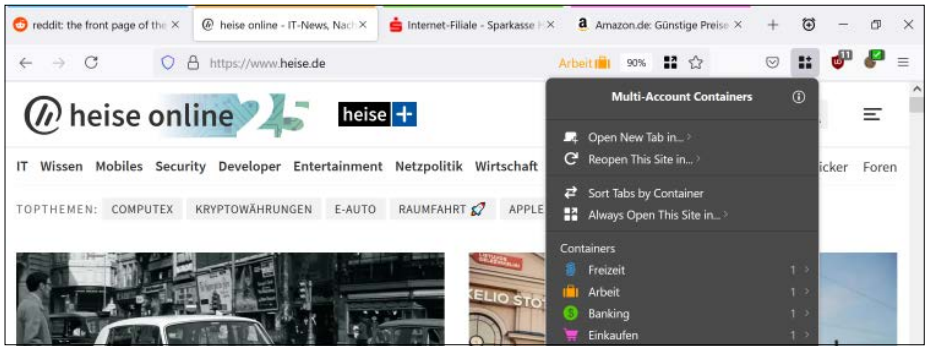
Sie öffnet auf Wunsch sämtliche Websites, die nicht mit einem Container verknüpft sind, in kurzlebigen Wegwerf-Tabs. Schließt man einen solchen Tab, killt die Erweiterung den dazugehörigen Container samt Cookies nach fünfzehn Minuten. Das ist fast so, als würden Sie die ganze Zeit im privaten Modus surfen, mit Ausnahme der Sites, die Sie mit Containern verknüpft haben. Nach der Installation öffnet Temporary Containers seine Einstellungen. Hier sollten Sie ganz oben den „Automatic Mode“ aktivieren, damit Sie sich um nichts kümmern müssen. Alternativ können Sie über das Wecker-Symbol jederzeit selbst Tabs in temporären Containern öffnen. Die kurzlebigen Container erkennen Sie am Namen, der stets mit „tmp“ beginnt.

Mehr Schutz

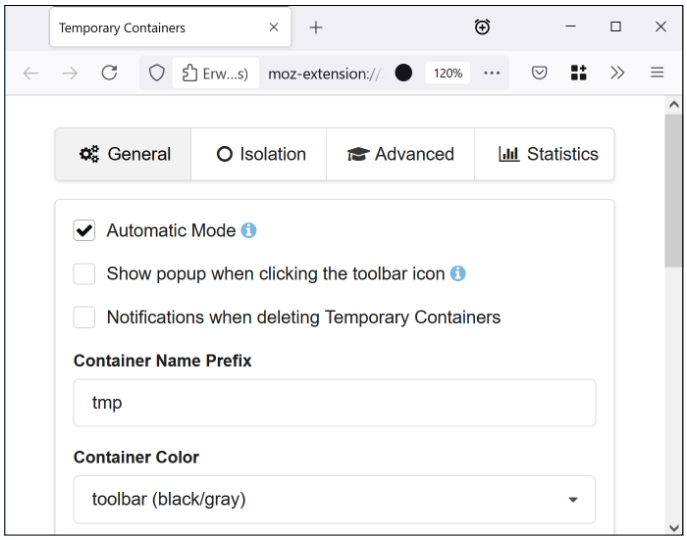
Die Liste möglicher Privacy-Gefährdungen ist fast beliebig lang. Wer sich gegen alle Eventualitäten absichern will, erreicht schnell einen Punkt, an dem das Surfen sehr mühsam ist, weil Websites nicht mehr wie gewohnt funktionieren und die Schutzfunktionen häufig nachjustiert werden müssen. Zu den sinnvolleren Maßnahmen gehört ein Schutz gegen das Canvas-Fingerprinting (siehe Seite 14). Bei dieser Trackingart werden Zeichenfunktionen des Browsers zur Identifizierung missbraucht.

Abhilfe verschafft die Firefox-Erweiterung CanvasBlocker, welche die Identifizierung durch zufällige Daten erschwert. Im Alltag stand Sie uns jedoch häufig im Weg, weil wichtige Elemente auf Websites fehlten und Browsertabs unvermittelt abstürzten. Recht beliebt sind Skript-Blocker wie NoScript oder uMatrix: Damit kann man unter anderem feingranuliert festlegen, welche Skripte auf welchen Websites ausgeführt werden dürfen. Das funktioniert gut, macht aber auch Arbeit: Die Filteregeln müssen nicht selten nachjustiert werden, ehe eine Website funktioniert. Diese und weitere zusätzliche Schutzmaßnahmen haben wir in unserem Firefox-Sicherheitskompendium zusammengestellt (siehe ct.de/y5et).

Nach so viel Datenschutz soll es noch mal um den Komfort gehen: Wenn Sie mit einem Notebook oder einem kleineren Monitor arbeiten, dann zählt jedes Pixel. Für unseren Versuch nutzten wir oft ein kompaktes Notebook mit gerade einmal 13,5-Zoll Bildschirmdiagonale. Um Komfort und Effizienz unserer Firefox-Installation abzurunden, haben wir hier noch die Erweiterung „Auto Fullscreen“ von tazeat (siehe ct.de/y5et) nachgerüstet. Der Name ist Programm: Nach der Installation läuft Firefox dauerhaft im Vollbildmodus, wodurch die Websites die gesamte Bildschirmfläche einnehmen. Die Bedienelemente des Browsers erscheinen sofort, wenn man mit dem Mauszeiger den oberen Bildschirmrand berührt und verschwinden wieder, wenn sie nicht länger gebraucht werden.



Container schotten Websites voneinander ab und schützen so effektiv vor Tracking.



Die Firefox-Erweiterung „Temporary Containers“ öffnet Websites auf Wunsch in Wegwerf-Containern. So können Sie sorglos alle Cookies akzeptieren, denn nach dem Schließen des Tabs werden sie ohnehin gelöscht.

Zweigleisig surfen

Mit unserer beispielhaften Firefox-Konfiguration surfen Sie nicht nur ungestört ohne Cookie-Banner und Werbung, sondern auch weitgehend ohne Tracking. Passen Sie unseren Vorschlag gern nach Ihren eigenen Vorstellungen an. Falls Sie ihn erstmal in Ruhe ausprobieren möchten, installieren Sie Firefox und die Erweiterungen einfach parallel zu Ihrem bisherigen Browser und schauen Sie, ob unsere Empfehlungen für Sie passen. Ein zweiter Browser ist auch für Fälle nützlich, in denen eine Webseite aufgrund der angezogenen Trackingbremsen nicht wie gewohnt funktioniert.

Falls Sie bereits hauptsächlich Firefox nutzen, dann werden Sie sich schnell zurecht finden. In diesem Fall probieren Sie unsere Vorschläge am besten mit einem zweiten Profil aus, das Sie wie eingangs beschrieben anlegen können. Möchten Sie das neue Profil nur dann und wann nutzen, legen Sie einfach eine weitere Verknüpfung zur firefox.exe an, die den Browser automatisch mit dem gewünschten Profil öffnet. Das Verknüpfungsziel kann unter Windows wie folgt lauten: `"C:\Program Files\Mozilla Firefox\firefox.exe" -p "Profilname"`. Starten Sie Firefox wie gewohnt, um das eingestellte Standardprofil zu nutzen. Wenn Sie die neue Verknüpfung doppelklicken, öffnet sich der Browser hingegen direkt mit dem neuen Profil. So können Sie von Fall zu Fall entscheiden, welche Konfiguration Sie nutzen möchten.

Abschließend noch ein Hinweis, auch in eigener Sache: Insbesondere der Einsatz eines Content-Blockers wie uBlock Origin ist ein zweischneidiges Schwert. Sie entfernen damit nicht nur invasive Werbung, die Ihnen häufig auf Grundlage Ihrer persönlichen Interessen ausgeliefert wird. Sie schneiden den Websites auch eine wichtige Einnahmequelle ab. Statten Sie Ihren Lieblingssites also ruhig mal ohne Content-Blocker einen Besuch ab und setzen Sie eine Site auf die Ausnahmeliste, wenn Sie die Werbung nicht stört. Viele Website-Betreiber können Sie zudem für eine Handvoll Euro im Jahr durch ein Abo oder Spenden unterstützen. Manche Websites bieten auch ein Pur-Abo an, mit dem Sie Tracking und Werbung für einen kleinen Betrag weitgehend loswerden. *(rei@ct.de)* c't

Firefox-Erweiterungen: ***ct.de/y5et***