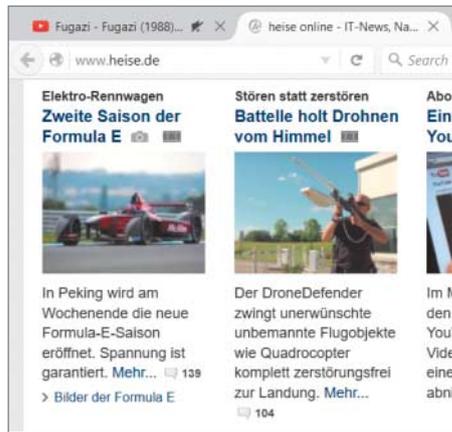


Firefox blockt Tracker

Mit der Firefox-Version 42, die am 3. November für Windows, Linux, Mac OS und Android erscheinen soll, will Mozilla nicht nur die Frage nach dem Leben, dem Universum und dem ganzen Rest beantworten, sondern auch ein paar besondere neue Features einführen. Das meistdiskutierte ist der eingebaute Tracking-Schutz: Sobald der Nutzer im privaten Modus surft, lädt Firefox keine Inhalte mehr herunter, die Datensuren sammeln.

Die Nutzer würden vom privaten Modus erwarten, dass er ihre Privatsphäre auch nach außen schützt, so Mark Mayo, der Leiter der Firefox-Entwicklung. Dabei sollte das Feature schonender mit den Inhalten umgehen als beim kompletten Blocken von Drittinhalten, das auch weiterhin möglich ist. Die Filterliste übernimmt Mozilla von dem Open-Source-Unternehmen disconnect.me.

Diese Neuerung kommt zu einem Zeitpunkt, an dem Online-Werbung im Kreuzfeuer steht und Werbeblocker eine kritische Masse erreicht haben. Der Tracking-Schutz ist nicht explizit als Werbeblocker konzipiert, filtert



aber im Praxistest einen Großteil der Werbeeinblendungen aus. Bei Stichproben von Nachrichten-Websites reduzierte der Blocker die HTTP-Anfragen und das Datenvolumen durchschnittlich auf gut die Hälfte.

Mayo schätzt die direkten Auswirkungen auf die Werbe- und Medienbranche dennoch gering ein. Nur eine Minderheit – vermutlich im einstelligen Prozentbereich – nutze den privaten Modus. Außerdem lässt Firefox Tracker durch, die sich verpflichtet haben, dem „Do Not Track“-Wunsch Folge zu leisten, den Firefox im privaten Modus standardmäßig sendet. Dass der Tracking-Blocker irgendwann auch

im Standard-Modus aktiviert sein könnte, wollte Mayo zumindest nicht ganz ausschließen.

Nicht nur den Inhalteanbietern, sondern auch den Add-on-Entwicklern gibt Mozilla eine bittere Pille mit. Kürzlich kündigte man an, die bisherigen Erweiterungs-Schnittstellen langfristig zu schließen und stattdessen auf das ursprünglich für Chrome entwickelte WebExtensions zu setzen. Vor allem die etwa 30 Prozent Add-ons, die XUL-Overlays einsetzen, müssen komplett neu entwickelt werden.

Firefox 42 unterstützt nun erstmals WebExtensions. Damit zeichnet sich ein einheitliches API für Browser-Erweiterungen

Geräuschvolle Tabs lassen sich in Firefox 42 auch identifizieren, wenn sie im Hintergrund liegen, und mit einem Klick zum Verstummen bringen.

ab; Microsoft Edge soll 2016 nachziehen. Wer eine Erweiterung für Chrome, Safari oder Opera geschrieben hat, muss diese für Firefox neu verpacken und signieren. Der Browser kann auch Sound abspielende Tabs identifizieren, man kann sie direkt von der Tableiste aus stumm schalten. Android-Nutzer können Links in einer „Tab Queue“ speichern, um sie zu gegebener Zeit rasch zu öffnen.

Etwa gleichzeitig mit Firefox 42 soll eine weitere Neuheit erscheinen: Firefox für iOS. Mozilla hatte sich lange gegen eine iOS-Version gewehrt, weil diese unter der Oberfläche mit der eingebauten WebKit-Engine arbeiten muss. Mozilla testet den iOS-Browser bisher in vier Ländern, darunter Österreich. Als Zugabe gibt es eine zweite iOS-App namens „Signal“. Da Firefox auf dem iPhone/iPad keine Inhalte filtern kann, tut Mozilla dies mit einer separaten App, von der auch andere Browser profitieren können. Die Standardeinstellung entspricht etwa dem Tracking-Blocker von Firefox 42, aber auch strengere Vorgaben sind möglich. (Herbert Braun/ad@ct.de)

Bild-Zeitung lässt Anleitungen für Werbeblocker abmahnen

Der Axel-Springer-Verlag reagiert ungehalten auf Versuche, die Adblocker-Sperre seines Online-Angebots Bild.de zu umgehen. Durch technische Maßnahmen wurden Nutzer mit Werbeblockern von der Nutzung ausgeschlossen. Ein Nutzer, der auf YouTube ein Anleitungsvideo eingestellt hatte, das die Über-

windung der Adblocker-Sperre beschrieb, erhielt dafür eine Abmahnung des Medienkonzerns. Das Unternehmen will gegen alle vorgehen, die die Anti-Adblocker-Initiative „unlauter umgehen“ würden.

Der IT-Fachanwalt Thomas Stadler setzte sich mit der Abmahnung auseinander und wi-

dersprach der juristischen Argumentation von Springer, dass die Werbeblocker eine „Umgehung einer wirksamen technischen Maßnahme zum Schutz urheberrechtlicher Werke“ darstellten. Die Werbeblocker-Maßnahme fällt nach seinem Dafürhalten nicht unter den Schutz des Urheberrechts, weil solche Blocker

nur dem Zweck dienen, unerwünschte Werbung auszublenken, wie er in einem Blog-Eintrag (siehe c't-Link) erläutert. Das Ziel hat Springer dennoch erreicht: Das Video verschwand. (uma@ct.de)

ct Blog-Eintrag von Thomas Stadler: ct.de/y5bj

Jetzt im Handel: c't wissen Bloggen

Ein Blog ist mit WordPress, Tumblr & Co. schon in wenigen Minuten startklar. Richtig Spaß macht das Bloggen aber erst, wenn auch Leser vorbeischaun und Kommentare hinterlassen. Das neue Heft c't wissen Bloggen erklärt, wie gezielte Marketing-Maßnahmen mehr Besucher ins Blog locken.

Das von c't zusammengestellte Heft zeigt außerdem, was WordPress alles kann: Mit den

richtigen Plug-ins erstellen Sie ein schickes Foto-Blog und schützen es vor Spammern und Trollen. Fortgeschrittene Nutzer basteln ein eigenes WordPress-Theme und setzen ein einmaliges Design um – ein ausführlicher Praxisartikel hilft bei den ersten Schritten.

Damit kein Anwalt Ihnen den Spaß am Bloggen verdirbt, beantworten wir die wichtigsten Rechtsfragen: Welche Angaben

müssen in ein Impressum? Wie sieht eine vollständige Datenschutzerklärung aus? Und wie muss man Werbung im Blog korrekt kennzeichnen?

Das Heft gibt es ab sofort als E-Magazin im PDF-Format im heise Shop, es kostet 7,99 Euro. Die gedruckte Version kostet 8,90 Euro und liegt ab dem 2. November am Kiosk. (dbe@ct.de)

ct Bestellung: ct.de/y5bj



Angriff aufs mTAN-Verfahren

Kriminelle haben eine neue Methode gefunden, das mTAN-Verfahren zu überlisten und vollen Zugriff auf Online-Konten zu erlangen. Beim mTAN-Verfahren wird für jede Transaktion eine TAN an ein Mobiltelefon geschickt, meist per SMS. Erst mit der Eingabe dieser TAN wird die Transaktion ausgeführt. Das Mobiltelefon mit der SIM-Karte dient also als Identitätsnachweis des Nutzers.

Die mobile TAN löst die herkömmlichen TAN-Verfahren ab, bei denen der Nutzer ausgedruckte TAN-Listen hatte, die er auf Anforderung eingab. Der Komfortgewinn wird aber mit möglichen Sicherheitsrisiken erkauft.

Die Opfer waren diesmal Mobilfunkkunden der Telekom. Die Täter gaben sich gegenüber dem Unternehmen als Mitarbeiter von Mobilfunk-Shops aus und ergaunerten auf diesem Wege Zweit- oder Ersatz-SIM-Karten, mit denen sie per SMS

versandte TANs abfingen und damit zuvor ausgespähte Bankkonten abräumten. Dabei gingen sie offenbar gezielt vor und wählten Konten mit großem Verfügungsrahmen aus. Obwohl die Zahl der Fälle laut einem Sprecher der Telekom nur im mittleren zweistelligen Bereich lag, betrug der Gesamtschaden über eine Million Euro.

Die Telekom ergriff umgehend Maßnahmen, um die Händleridentifikation sicherer zu gestalten. In einer Stellungnahme wies sie den Kunden die Schuld zu. Das Grundproblem, schrieb das Unternehmen, sei die Sicherung des Rechners.

Kunden, die ihre Sicherheit beim Online-Banking erhöhen wollen, sollten den Verfügungsrahmen auf das erforderliche Minimum reduzieren und auf das sicherste Authentifizierungsverfahren umsteigen, das ihre Bank anbietet, etwa TAN-Generatoren oder den Zugriff per HBCI, möglichst mit Chipkarte. (uma@ct.de)

Kommentar: Das Elend mit der mTAN

Der Kunde ist schuld, verkündete die Telekom nach dem jüngsten Angriff auf das mTAN-Verfahren. Der Kunde habe seinen Rechner nicht ordentlich gesichert, da liege das Grundproblem für den jüngsten erfolgreichen Angriff. Der Weltkonzern Telekom hat Kriminellen ohne jede Prüfung geglaubt, dass sie für einen Mobilfunk-Shop arbeiten, und SIM-Karten herausgerückt, die auf den Namen von Kunden lauteten. Das hält er für kein ernsthaftes Problem.

Die Telekommunikations-Riesen wollten schon immer das Telefon zum Zahlungsmittel machen – 0900-Rufnummern, WAP-Billing, mobile Payment. Die Liste der Möglichkeiten ist lang, die der Ideen noch länger. Die Sicherheit nehmen die Anbieter dabei aber immer noch auf die leichte Schulter.

Wenn die Telekommunikationsfirmen beim mTAN-Verfahren wiederholt das schwächste Glied in der Sicherheitskette sind, wie sollen ihre Systeme da für alle möglichen Online-Bezahlverfahren taugen?

Immer wieder klagen Kunden über zu hohe Telefonrechnungen. Ihre Beschwerden scheitern häufig daran, dass sie nicht nachvollziehen können, was da passiert ist, und dass sie nicht nachweisen können, dass die Rechnung falsch ist. Das Ende vom Lied ist meistens, dass die Kunden zahlen müssen. Zahlungssysteme und Telefon miteinander zu verheiraten scheint mir vor diesem Hintergrund derzeit keine gute Idee; erst einmal müssen die Telefonfirmen ihre Hausaufgaben machen.

Urs Mansmann

Anzeige