Safer Internet

Tor-Browser als sicherer Zweitbrowser

Mal eben auf den Link in einer E-Mail klicken? Besser nicht, Angreifer nutzen Social Engineering, um ihre Opfer auf präparierte Websites zu locken und sie dort gezielt mit Browser-Exploits anzugreifen. Mit dem Tor-Browser schlagen Sie Hackern ein Schnippchen, denn der lädt problematische Inhalte gar nicht erst.

Von Mirko Dölle

Haufenweise JavaScript, nachzuladende Fonts und Videos – moderne Websites sind gespickt mit potenziell problematischen Inhalten. Schon eine Sicherheitslücke in einem Videocodec reicht aus, damit Angreifer Schadcode einschleusen können. E-Mails mit plausiblem Inhalt sind in Zeiten von Social Engineering eine beliebte Methode, die Opfer auf entsprechend präparierte Websites zu locken – der Browser lädt dann willig alle eingebetteten Inhalte herunter, Schadcode inklusive.

Mit dem Tor-Browser passiert das nicht: Hat man beim ersten Start einmalig die höchste Sicherheitsstufe eingestellt, lädt er nur noch HTML-Dateien, CSS und Bilder – JavaScript, Schriftarten, Videos und dynamische HTML5-Inhalte hingegen lässt er links liegen. Damit bietet er Angreifern eine deutlich kleinere Angriffsfläche als herkömmliche Browser und eignet sich gut, um unbekannte oder suspekte Websites in Augenschein zu nehmen.

Tor zur Welt

Den Tor-Browser gibt es auf https://torproject.org für Windows, macOS und Linux kostenlos zum Download. Anwender sollten ihn stets selbst installieren, damit die automatischen Updates des Browsers auch zuverlässig funktionieren und nicht etwa an mangelnden Rechten

scheitern. So erhält man Sicherheitsaktualisierungen unmittelbar nach ihrer Veröffentlichung und muss nicht etwa warten, bis der Linux-Distributor die Änderungen in sein Paket-Repository übernommen hat.

Der Tor-Browser ist eine modifizierte und erweiterte Variante von Firefox ESR, der wiederum für den Unternehmenseinsatz gedacht ist. Die wichtigste Erweiterung ist der Tor-Daemon, der zusammen mit dem Browser installiert wird. Er arbeitet als Proxy für den Browser und sorgt dafür, dass der Datenverkehr mehrfach verschlüsselt über mindestens drei Knoten des Tor-Netzwerks durch alle Welt geleitet wird, bevor er am Ziel ankommt. So lässt sich praktisch nicht feststellen, woher eine Anfrage kam, man surft anonym. Außerdem eröffnet der Tor-Daemon den Weg ins Darknet, sodass man sogenannte Hidden Services mit der Domain .onion ansurfen kann.

Die wichtigste Sicherheitskomponente des Tor-Browsers ist das Plug-in NoScript, das bereits vorinstalliert und scharf geschaltet ist. Mit den Sicherheitsstufen haben die Tor-Entwickler eine komfortable Möglichkeit implementiert, die doch zahlreichen NoScript-Optionen auch für Laien handhabbar zu machen.

In der höchsten Sicherheitsstufe sorgt NoScript dafür, dass weder JavaScript noch andere dynamische Inhalte automatisch geladen oder gar ausgeführt werden – nicht einmal Fonts. Das führt auf mit Weitblick gebauten Webseiten nur zu geringen Verfremdungen, etwa bei der Deutschen Bahn. Etliche Seitenbetreiber, insbesondere solche, die mit vielen Frameworks arbeiten, sind derart auf JavaScript angewiesen, dass ihre Seite mit scharfgeschaltetem NoScript unbedienbar sind.

Ohne JavaScript geht es dann nicht weiter. Sie sollten dann NoScript aber nicht einfach deaktivieren, sondern die Möglichkeit des Plug-ins nutzen, Skripte nur für einzelne Domains zu erlauben. So können Sie den Schutzschild nach und nach senken, bis Sie die gewünschte Funktionalität erreicht haben. Auf diese Weise bekommt man auch ein gutes Gefühl dafür, wie viele externe Inhalte manche Websites einbinden.

Andere Seiten kann der Tor-Browser bei höchster Sicherheitsstufe selbst dann nicht darstellen, wenn man JavaScript aktiviert. Ein solches Negativbeispiel ist die Homepage von Volkswagen: Bei den Wolfsburgern erhält man nur ein leeres Fenster mit einem kleinen VW-Symbol – auch dann, wenn NoScript gar nicht mehr im Spiel ist. Erst wenn man die Sicherheitsstufe im Tor-Browser auf das Minimum reduziert, sieht man den regulären Inhalt und kann auf der Seite navigieren.

Tor kicken

Es gibt auch Websites, die Tor gezielt blockieren, etwa die deutsche Homepage von Ferrari: Erkennt die über Cloudfront ausgelieferte Seite einen Zugriff aus dem Tor-Netz, liefert sie lediglich den Fehler-Code 403. Außerdem kostet die mehrfache Umleitung der Verbindung über drei Tor-Knoten Zeit, und die Bandbreite ist je nach Datenaufkommen bei den einzelnen Nodes ziemlich beschränkt. Längere Ladezeiten sind deshalb keine Seltenheit, was gerade interaktive Websites stark ausbremsen kann.

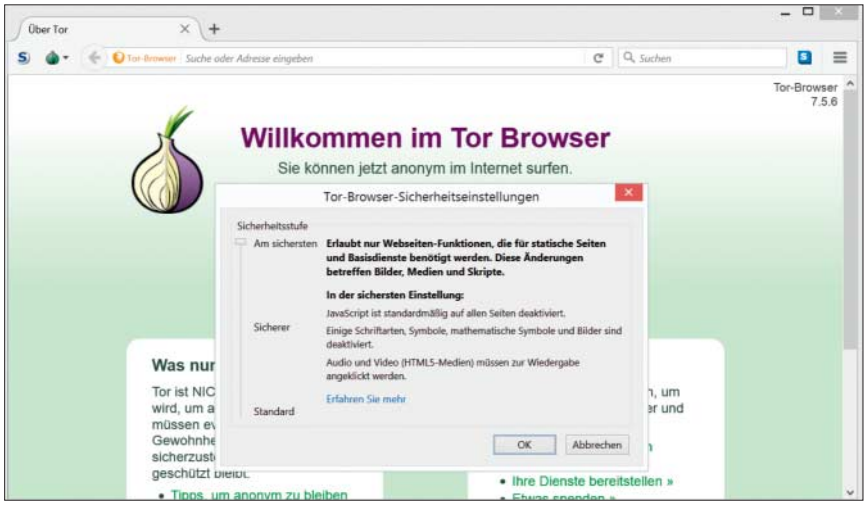
Welchen Weg Ihre Daten durch das Tor-Netz nehmen, bekommen Sie durch einen Klick auf das Zwiebelsymbol in der Adressleiste heraus: Dort zeigt der Tor-Browser die IP-Adressen und das Land der einzelnen Tor-Knoten an. Indem Sie auf den Menüeintrag „Neuen Kanal für diese Seite“ klicken, können Sie den Tor-Browser eine neue, möglicherweise schnellere Route zum Ziel suchen lassen.

Blockiert die Zielseite den Tor-Browser oder finden Sie keine schnelle Route, können Sie den Datenverkehr des Tor-Browsers an Tor vorbeilaufen lassen und so auf direktem Weg und mit der vollen Internetbandbreite Ihres Anschlusses surfen. Anonym sind Sie dann allerdings nicht mehr – jeder Server, den Sie ansurfen, wird Ihre tatsächliche IP-Adresse zu sehen bekommen.

Dazu gehen Sie in die Einstellungen des Tor-Browsers und klicken unter „Erweitert“ auf das Register „Netzwerk“ und dort unter „Verbindung“ wieder auf „Einstellungen“ – womit Sie in der Proxy-Konfiguration des Tor-Browsers landen. Hier ist standardmäßig der im Hintergrund laufende Tor-Daemon als Proxy mit der Adresse 127.0.0.1, dem Port 9150 und dem Proxy-Protokoll SOCKS5 eingetragen. Außerdem löst der Browser DNS-Anfragen über den Proxy auf.

Indem Sie zuerst die DNS-Auflösung über den Proxy deaktivieren und erst dann den Internet-Zugriff auf „Kein Proxy“ setzen, kappen Sie die Datenverbindung zwischen dem Tor-Browser und dem Tor-Daemon. Nicht betroffen ist davon die Kontrollverbindung auf Port 9151 – der Tor-Browser versucht weiterhin, im Hintergrund einen Tor Circuit bestehend aus drei Tor-Knoten bis zum Ziel aufzubauen, auch wenn er sie anschließend nicht nutzt.

Die Kontrollverbindung dürfen Sie nicht kappen, andernfalls startet der Tor-Browser nicht mehr, weil er keine Verbindung zum Tor-Netz findet. Außerdem werden die Proxy-Einstellungen nach jedem Neustart wieder auf die Standardwerte zurückgesetzt – um wieder torlos zu surfen, müssen Sie die Proxy-Einstellungen also erneut deaktivieren. Das ist auch gut so, verhindert diese Automatik doch, dass sich jemand dauerhaft deanonymisiert, der den Proxy nur versehentlich abgeschaltet hatte. *(mid@ct.de)* c't



Schotten dicht: In der höchsten Sicherheitsstufe lädt der Tor-Browser weder JavaScript noch Schriften oder dynamische Inhalte wie Videos und Audiodateien. So bietet der Browser Hackern kaum eine Angriffsfläche.