RUBIKON

Donnerstag, 28. September 2017, 12:50 Uhr
~5 Minuten Lesezeit

Anonym surfen im Internet

Schutz gegen Massenüberwachung ist machbar und Teil notwendiger digitaler Selbstverteidigung.

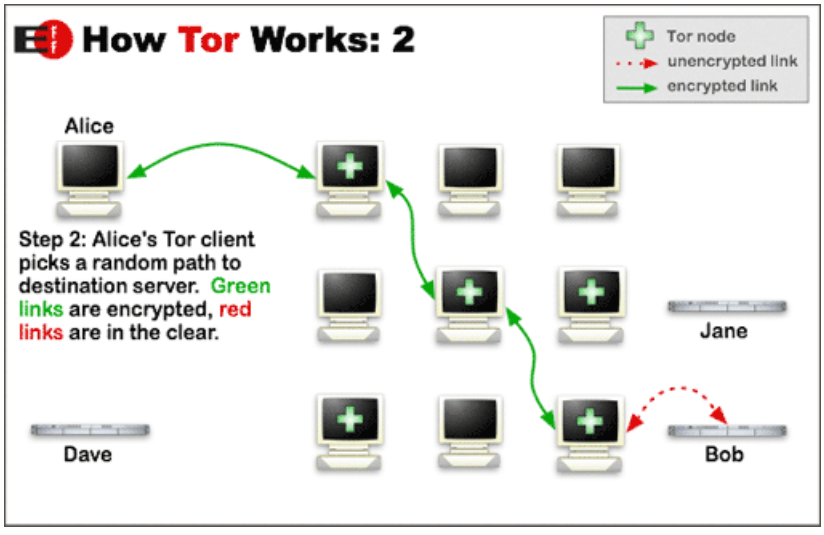
von Wolfgang Romey
Foto: gualtiero boffi/Shutterstock.com

Jede Seite, die Sie im Internet besuchen, wird vermerkt. Auch wie lange Sie dort geblieben sind und welche Seiten sie danach aufgesucht haben. Wenn Sie Werbung angeklickt haben, wird das gespeichert und für personenbezogene Werbung ausgewertet. Die Liste der möglichen Beispiele kann noch umfangreich ergänzt werden. Wollen Sie diese Ausforschung?

Neben der auf rubikon beschriebenen Absicherung des Internet-Browsers Firefox durch Verwendung von Add-Ons gibt es einen weiteren wirksamen Weg, sich gegen das Abgreifen von Daten beim Surfen im Internet zu schützen: Man verschleiert seine Internet-Adresse und surft anonym.

Möglich ist das, wenn man über das Tor-Netzwerk mit dem Tor-Browser surft, der eine Weiterentwicklung von Firefox ist. Selbstverständlich sind der Tor-Browser und die Software, mit der das Tor-Netzwerk betrieben wird Freie Software. Für sicherheitsrelevante Anwendungen ist das zwingend, da nur dann der Quellcode verfügbar ist und auf Sicherheitslücken und Hintertüren untersucht werden kann.

Das Tor-Netzwerk ist ein von Freiwilligen betriebenes Netzwerk von Rechnern, das es ermöglicht, sich weitgehend anonym im Internet zu bewegen. Dies wird erreicht durch das Zwiebel(Onion)-Verfahren. Dabei wird die Verbindung vom Ausgangsrechner zum Zielrechner, der besucht werden soll, über drei zufällig jeweils neu gewählte Zwischenstationen des Tor-Netzwerks hergestellt. Die Kommunikation vom Ausgangsrechner über die drei Zwischenstationen ist jeweils verschlüsselt. Erst die Verbindung von der letzten Station zum Zielrechner ist unverschlüsselt. In einer Grafik von den **Seiten des Torprojekts** (https://www.torproject.org/) wird das so dargestellt:



Das Besondere ist nun, dass nur der erste Rechner auf dem Weg vom Ausgangspunkt zum Ziel den Ausgangsrechner kennt. Rechner zwei kennt nur den Rechner eins und Rechner drei den Rechner zwei. Nur Rechner drei kennt den Rechner, der das Ziel der Verbindung ist.

Also:

- Rechner 1 kennt den Ausgangspunkt der Verbindung;
- Rechner 2 kennt nur Rechner 1;
- Rechner 3 kennt nur Rechner 2;
- Ziel-Rechner kennt nur Rechner 3.

Zum Zeitpunkt, als dieser Artikel geschrieben wurde, wurde die Verbindung meines Rechners zum Zielrechner über Frankreich, Spanien und Rumänien hergestellt.

Wird anschließend eine andere Seite im Internet aufgesucht, wird ein anderer Weg vom Ausgangs- zum Zielrechner gewählt. Auf diese Weise wird eine sehr weitgehende Anonymität beim Surfen sichergestellt.

Auch für Leute, die nicht wie z.B. Whistleblower auf Anonymität angewiesen sind, ist die Nutzung von Tor sinnvoll, da damit z.B. Profilbildung oder Ausforschung des Surfverhaltens durch die Werbewirtschaft deutlich erschwert werden, da der Rechner, mit dem man sich im Internet bewegt, nicht erkannt wird und z.B. Cookies nicht sinnvoll platziert werden können.

Damit man das Tor-Netzwerk zum Surfen nutzen kann, muss der Tor-Browser installiert werden. Er kann von **https://www.torproject.org/projects/torbrowser.html.en#downloads** (https://www.torproject.org/projects/torbrowser.html.en#downl

oads)
für das jeweilige Betriebssystem in der Landessprache heruntergeladen werden.

Auf der Seite
https://www.torproject.org/docs/documentation.html.en (https://www.torproject.org/docs/documentation.html.en) findet sich eine über den Punkt „Install Tor-Browser“ erreichbare Installationsanleitung für den Tor-Browser für die gängigen Betriebssysteme und Android-Smartphones.

Damit die Anonymität weitestgehend gesichert ist, muss man ggf. seine Surfgewohnheiten ändern. Wenn z.B. in einem Webformular Namen und Anschrift oder Kreditkarteninformationen eingegeben werden müssen, hebelt dies den Schutz durch Tor u.U. dauerhaft aus. Wenn die Eingabe von persönlichen Daten notwendig ist, sollte man einen anderen Webbrowser verwenden.

Tor bringt zur Erhöhung der Sicherheit einige Add-Ons in der Grundausstattung mit, u.A. die Add-Ons NoScript und HTTPS-Everywhere, deren Funktion in
https://www.rubikon.news/artikel/nichts-bleibt-verborgen (https://www.rubikon.news/artikel/nichts-bleibt-verborgen) beschrieben wurde. Das hat zur Folge, das einige Internet-Seiten nicht wie vorgesehen angezeigt werden. Zudem wird der Zugang zu einigen Seiten geblockt, wenn sie über Tor angesurft werden, weil die Herkunftsadresse eben verschleiert ist. Man muss dann u.U. auf einen anderen Webbrowser ausweichen. Wie in vielen anderen Bereichen bringt größere Sicherheit und ein höheres Maß an Selbstbestimmung eben Unbequemlichkeiten mit sich.

Es ist leider selbstverständlich, dass das Tor-Netzwerk und der Tor-Browser Ziel von Angriffen ist. Es wird fortlaufend versucht, durch Unterwanderung des Tor-Netzwerkes die Nutzer zu entschleiern. In den letzten Tagen bekannt geworden ist, dass auch der BND

intensiv versucht, die Anonymisierung auszuhebeln. Bis heute kann man aber davon ausgehen, dass dies nicht umfassend gelungen ist, auch weil das Tor-Projekt versucht, durch Weiterentwicklung der verwendeten Software die Angriffe abzuwehren. Wie immer bei der Nutzung von IT-Technik sind dabei die Nutzer die größte Schwachstelle.

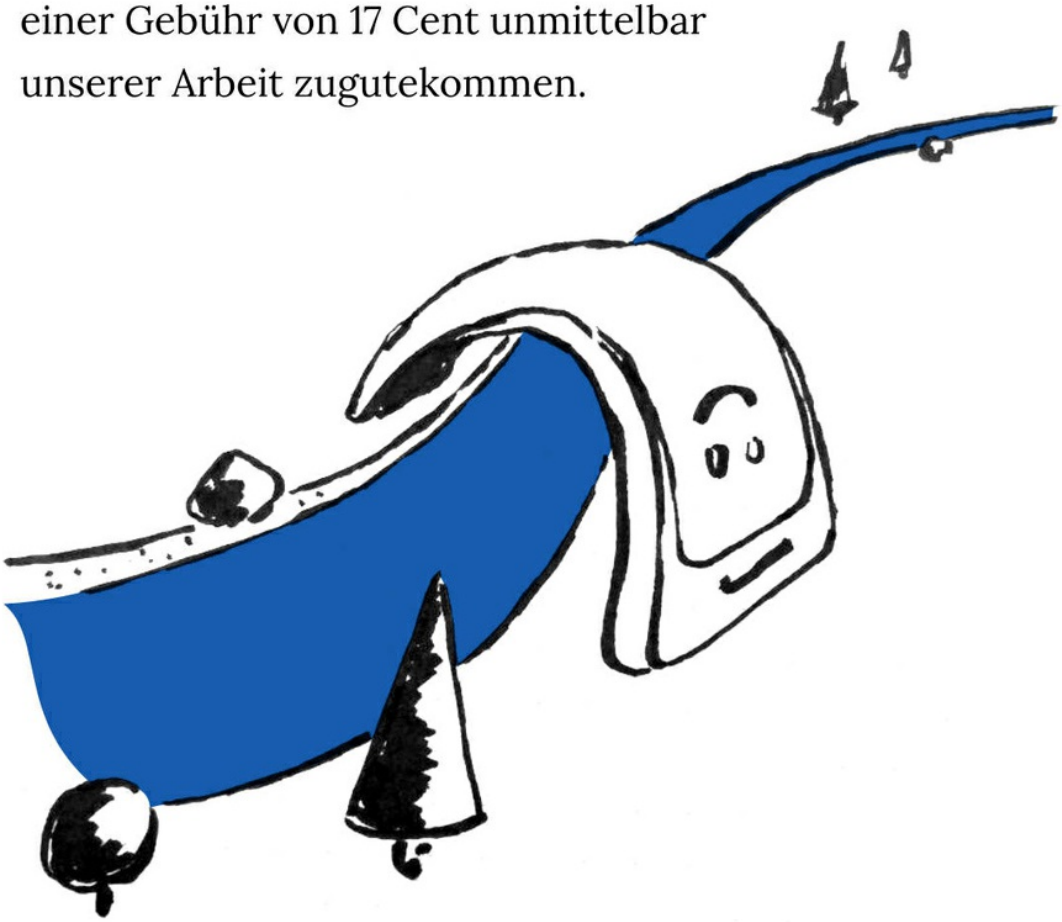
Reicht das durch die auf rubikon beschriebenen Maßnahmen erreichte Sicherheitsniveau nicht aus, gibt es weitere Möglichkeiten: So kann z.B. der eigene Rechner vollständig verschlüsselt werden. Eine weitere Möglichkeit ist die Verwendung des Betriebssystems „**Tails** (https://tails.boum.org/about/index.de.html)“.

Tails wird in der Regel nicht auf dem eigenen Rechner installiert, sondern von einer DVD oder einem USB-Stick betrieben und hinterlässt nach der Verwendung keinerlei Spuren auf dem Rechner. Tails wurde u.A. von Edward Snowden und Glen Greenwald genutzt, um ihre Kommunikation wirksam zu schützen. Will man ein Dokument erstellen, das besonders schutzwürdig ist, und sicher an ein Ziel bringen, erstellt man es auf einem Rechner, der mit keinem Netzwerk verbunden ist. Dann wird es mit einem Speichermedium, das nicht verändert werden kann, zu einem Rechner gebracht, auf dem Tails läuft, und von dort über das Internet zu seinem Ziel geschickt. Hohe Sicherheit muss mit einem hohen Aufwand erkauft werden.

Auch wenn man als Nutzer allen bisher auf rubikon beschriebenen Empfehlungen folgt, muss man sich allerdings über eines im Klaren sein: Da die Angriffsverfahren immer ausgefeilter werden, gibt es vollständigen Schutz nur, wenn man seinen Rechner auf den Dachboden oder in den Keller bringt und ihn dort verstauben lässt. Aber selbst das könnte in Zukunft nicht reichen.

Hat Ihnen dieser Artikel gefallen?

Dann unterstützen Sie unsere Arbeit auf die denkbar schnellste und einfachste Art: per SMS. Senden Sie einfach eine SMS mit dem Stichwort **Rubikon5** oder **Rubikon10** an die **81190** und mit Ihrer nächsten Handyrechnung werden Ihnen 5,- bzw. 10,- Euro in Rechnung gestellt, die abzüglich einer Gebühr von 17 Cent unmittelbar unserer Arbeit zugutekommen.



Wolfgang Romey arbeitete nach dem Studium der Theoretischen Elektrotechnik als Lehrer für Mathematik, Elektrotechnik und Digitaltechnik im Berufsbildenden Bereich, später als Lehrerausbilder im

Vorbereitungsdienst, dem Referendariat. Dann folgte ein Wechsel in die Bezirksregierung Düsseldorf als Dezernent für Lehrerausbildung und später auch -fortbildung. Er verfügt über etwa 20 Jahre Erfahrung darin, angehende Lehrerinnen und Lehrer auf die Bildungsarbeit mit Digitalen Medien vorzubereiten und deren Urteilskraft in diesem Feld zur Entfaltung zu verhelfen. Die kritische Auseinandersetzung mit den dramatischen Folgen der Digitaltechnik, die ihm extrem unterentwickelt scheint, ist bis heute sein Thema.