Spurlos im Netz

Wer sich ins Internet begibt, wird überwacht - das dürfte sich rumgesprochen haben. Die Überwachung beschränkt sich nicht auf die kommerzielle Überwachung von Facebook, Google oder zahlreichen anderen Werbenetzwerken, deren Namen nur noch wenige Internetnutzer kennen. Auch staatliche Stellen wie der BND, GCHQ oder NSA überwachen unseren Internetverkehr. Die Überwachung beschränkt sich dabei nicht auf Inhaltsdaten. Metadaten verraten oft mehr über uns, als uns bewusst und lieb ist, Firmen interessieren sich für die Standortdaten unseres Smartphones und im öffentlichen Raum erkennen Kameras unsere Gesichter, Bewegungen und Emotionen in Echtzeit. Es könnte der Eindruck entstehen, dass wir zukünftig einen terroristischen Anschlag planen oder uns zumindest ein überflüssiges Produkt verkaufen lassen. Und wieder andere Firmen haben Interesse daran, unsere politische Meinung zu beeinflussen.

Doch sind das valide Gründe, um immer mehr von unserer Privatsphäre aufzugeben? Wollen wir es wirklich so hinnehmen, dass nahezu alle unsere Aktivitäten getrackt und analyisiert werden? Edward Snowden kommentierte es mit „Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.“

Doch sind das valide Gründe, um immer mehr von unserer Privatsphäre aufzugeben? Wollen wir es wirklich so hinnehmen, dass nahezu alle unsere Aktivitäten getrackt und analyisiert werden? Edward Snowden kommentierte es mit „Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.“

Der TOR-Browser ist eine der Möglichkeiten, sich der ausufernden Überwachung beim Surfen im Netz ein Stück weit zu entziehen. Dafür muss man wahrlich kein Experte sein - es reicht, den Browser auf torporject.org herunterzuladen und nach der Installation kann es losgehen. Die Bedienung unterscheidet sich kaum von anderen Browsern, schließlich basiert er auf dem bekannten Open Source Browser Firefox. Schon bewegt man sich viel anonymer im Netz.

TOR steht für „The Onion Routing“. Die Basis für das Anonymisierungsnetzwerk sind über 6.000 sogenannte TOR-Nodes, also Knoten im Netzwerk. Alle Aktivitäten, die wir im Netz vornehmen, werden über drei solcher Knoten geleitet. Daher weiß der Server, an den wir unsere Anfrage senden, nicht mehr, von wem die Anfrage eigentlich kommt - schließlich fragt ein Server aus dem TOR-Netzwerk an - und nicht mehr der eigentliche Nutzer. Außerdem werden die Daten in mehreren Schichten verschlüsselt (daher die Referenz auf die Zwiebel), dass die Stellen, die eigene Internetkommunikation mitlesen können, diese Kommunikationsdaten nicht mehr interpretieren können. Inhaltsdaten werden verschlüsselt. Metadaten sind Nutzern nicht mehr zuortbar.

Aber Achtung, um sich mit dem TOR-Browser sicher zu bewegen, gibt es ein paar Grundsätze zu beachten (LINK). Der Browser verschleiert lediglich den eigenen Standort, alle anderen Daten und Verhaltensweisen entstehen weiterhin. Eine 100%ig Sicherheit liefert der TOR-Browser nicht, auch wenn er ein sehr effektives Werkzeug ist.

Weitere Tools zur Erhöhung der eigenen Privatsphäre sind zum Beispiel VPN-Dienste, das dezentrale betriebene soziale Netzwerk Mastodon, der Smartphone-Messenger Signal oder PEP (Pretty Easy Privacy).

Chaos macht Schule, https://www.ccc.de/schule