Teil 2: Sicher surfen mit HTTPS - einfach erklärt!

Der Hinweis auf "https everywhere" ist fein, reicht aber m. E. für sicheres surfen nicht aus. Ja, es geht primär um die Verschlüsselung des Datenverkehrs zwischen dem Client (an dem ich sitze und surfe) und dem Server, der die Inhalte bereitstellt die ich sehen möchte. Das Internetprotokoll HTTPS ist genau dafür zuständig aber durch kostenlos erhältliche Zertifikate mittlerweile auch sehr weit verbreitet. Dritte können also nicht mitlesen, was ich mir gerade ansehe oder welche Informationen ich gerade anfordere.

Dem Film und seinem Ziel ist also nichts hinzuzufügen. Was bleibt, ist die nötige Aufmerksamkeit, insbesondere dann, wenn ich einem Link zu einer Seite gefolgt bin. Das Schloss und ein „https://…“ schützen mich nicht vor Schadcode oder einer gefälschten Bankseite mit echtem Zertifikat.

Bevor wir aber die höchste Stufe der Privatheit beim Surfen erklimmen sei deshalb der Hinweis auf weitere Absicherungsmaßnahmen des Browsers erlaubt:

Sicher surfen – was nicht im Film erscheint

Die Verschlüsselung das Datenverkehrs war vor vier Jahren noch nicht selbstverständlich. Sie schützt mich aber auch nicht vor Schadcode, der auf täuschend echt gestalteten Seiten mit Schloss und Zertifikat untergebracht werden kann.

Leider legal, aber auch in manchen Auswirkungen unschön, ist die Verfolgung durch die Werbeindustrie und deren Wunsch, mich ausrechnen zu können und mit personalisierter Werbung zu bombardieren (wo ich auch immer gerade bin). Das geschieht mit technischen Mitteln direkt auf der besuchten Internetseite.

Sobald ich als Besucher erkannt werde, sorgen eine Vielzahl im Hintergrund ablaufender Prozesse dafür, dass ich nach allen Regeln der Kunst entkleidet und möglichst auch identifiziert werde. Da im Internet ja alles kostenlos sein soll, erfolgt auf vielen Seiten die Refinanzierung über Werbeeinnahmen. Es würde viel zu weit führen, hier alle Prozesse zu erläutern. Die Branche ist erschreckend kreativ.

Wer als Mitglied des DSCC unsere Zeitung („Der graue Computer-Freak“) im November gelesen hat, kennt den hier verlinkten Artikel schon (https://dscc-berlin.de/pdf/pdf-tipps/freak-231-seite-08-11.pdf). Die Botschaft kurz: **Werbeblocker machen Sinn**, wie auch das Verhindern der Ausführung potentiell gefährlicher Scripte.

Der Chaos Computer Club (CCC) hat auf der re:publica TEN (2016) eindrucksvoll vorgeführt, wie selbst angeblich als sicher zertifizierte Werbung auch Schadsoftware transportieren kann (ab Minute 31:53 auf https://youtu.be/zJUmjtjCtY8?t=1913). Natürlich ist auch der Teil davor sehenswert. Dabei wurden für einen eigentlich veralteten Browser eine Schwachstelle (ein *Exploit*) genutzt, für eine aktuelle Version wurde eigens eine solche geschaffen.

Weder die Werbenden, noch die Betreiber der Seiten mögen Werbeblocker. Der „Krieg“ darum tobt daher immer noch – teilweise mit immer härteren Mitteln. Wer nicht will, dass ich mich schütze, den muss ich aber auch nicht besuchen.

Moderne Browser lassen sich mittlerweile so restriktiv konfigurieren, so dass die Verfolgung der Nutzenden oder auch das Unterschieben schädlicher Skripte nicht mehr ganz so einfach ist wie in der Vergangenheit. Es gibt aber eine Reihe nützlicher Zusätze (*plug-ins*), die (fast) jedem Browser gut tun. Im Jahr 2016, als der Film entstand, hätte mich der Hinweis auf einen Zusatz wie „uBlock Origin“ noch zufrieden gestellt. Heute kämen „Disconnect“ und eventuell auch der „Privacy Badger“ dazu – neben weiteren Ergänzungen für andere Sicherheitsaspekte.

Es gäbe dazu noch viel mehr zu schreiben aber hier sollen eigentlich die Filme im Mittelpunkt stehen und die haben die Privatsphäre und die Verschlüsselung im Fokus.