Safety First

Jeder kennt das Fenster auf den Webseiten, das sich am schnellsten mit einem Klick auf „Alle Cookies akzeptieren“ wieder schliessen lässt: Sogenannte Tracking-Cookies „spionieren“ Internetnutzer aus.

Cookies sind kleine Textinformationen, die der Browser automatisch speichert. Ein Browser ist dabei das Programm, um ins Internet zu gelangen. Firefox ist der weltweit führende Browser, andere sind beispielsweise Chrome oder Safari. Die Cookies dienen unter anderem dazu, persönliche Daten zu speichern und auszunutzen.

Zum Beispiel merken sich Cookies die Suchanfrage nach einer Unterkunft in London. Später wird verstärkt Werbung für Hotels in London angezeigt. Diese Infos, die ein Cookie sammelt, sind daher für die Werbeindustrie sehr interessant. Tracker arbeiten still und leise im Hintergrund. Facebook trackt beispielsweise sogar ausserhalb von Facebook. Das bedeutet, wenn jemand in einem Online-Shop Schuhe kauft, weiss Facebook sogar davon.

Plug-Ins können schützen

Viele Experten empfehlen die Installation eines Tracking-Blockers. Um sich besser zu schützen, gibt es eine Vielzahl an Plug-Ins (kleine Zusatzprogramme), die die Internetaktivität verschlüsseln. Zu den bekanntesten zählen HTTPS Everywhere und Block Origin, beide erzwingen – wo möglich – automatisch eine verschlüsselte Verbindung. Die Installation dieser Plug-Ins ist auch für Laien recht einfach, außerdem finden sich zahlreiche Anleitungen im Internet. Bei manchen Browsern sind die Standardeinstellungen schon auf Datenschutz getrimmt, Brave beispielsweise erhielt dazu erst kürzlich Bestnoten.

Digitalisierung? Ja, bitte! Aber…

Jeder, der die Chancen der Digitalisierung optimal nutzen möchte, sollte sich immer auch der Risiken bewusst sein. Beim Mountainbiken wird der Helm aufgesetzt und das altbackene Tagebuch wird mit einem Schloss versehen – sicher ist sicher. Wer mit Tracking-Blockern das Abgreifen persönlicher Daten verhindert, schützt sich vor dem Verlust seiner Privatsphäre im Netz.