Inkognito

a --
[LINK]

Zusammenfassung: Etzel Gysling

Wenn wir uns den Umgang mit dem Internet nicht sehr gut überlegen, wird es bald so weit sein, dass die grossen «Provider» viel mehr über uns wissen als wir selbst. Man braucht deshalb gar nicht paranoid zu sein, wenn man sich mit einer vernünftigen «Schutzhülle» umgeben will. Mit anderen Worten: das Internet soll nicht alles wissen über uns. Dabei lässt es sich nicht vermeiden, dass man möglicherweise auf gewisse Annehmlichkeiten, an die man sich gewöhnt hat, verzichten muss. Auch darf man nicht vergessen, dass ein Schutz bei der Verwendung eines Smartphones oder Tablets mindestens so wichtig ist wie bei der Nutzung eines «richtigen» Computers.

Hier eine Auswahl von Möglichkeiten, wie man sich abschirmen kann:

– Browser nicht personalisieren, besser anonym surfen, d.h. ein «Virtual Private Network» (VPN) verwenden. VPN sind für alle Betriebssysteme erhältlich. Meistens bezahlt man für ein VPN, auch wenn es primär als «gratis» bezeichnet ist (siehe: http://pkweb.ch/2qZq8C7). Es gibt allerdings einige Anbieter, die tatsächlich auch langfristig Gratis-VPN anbieten; dies gilt auch für den Browser Opera (http://www.opera.com/de).

– Google-Dienstleistungen genau überprüfen und allenfalls heikle Funktionen abschalten. Wer ein Google-Konto hat, verschafft Google viele verschiedene Zugänge auf persönliche Daten (Mails, Fotos, Dateien, geographische Ortung und noch mehr). Dies lässt sich im sogen. Dashboard überprüfen und nach Bedarf ändern (http://pkweb.ch/2qVP9xF). Hier kann man zum Beispiel auch die «gezielte» (d.h. personalisierte) Werbung unterbinden (http://pkweb.ch/2msaBG4).

– Microsoft-Dienstleistungen sind ähnlich wie diejenigen von Google, lassen sich jedoch nicht an einem zentralen Ort verwalten (ausser von Administratoren bei Firmen).

– Statt der Online-Maildienste (GMail, Windows Mail, GMX usw.) ein Mailprogramm auf dem eigenen Computer verwenden (z.B. Thunderbird, eMClient, Opera Mail). Fachleute aus dem Gesundheitsbereich verwenden mit Vorteil das Health Information Network (HIN), das eine verschlüsselte Übermittlung sicherstellt. Ein ähnliches Angebot ist auch allgemein von anderen Anbietern (z.B. StartMail: https://www.startmail.com/de/) erhältlich.

– Auf Cloudspeicher wie OneDrive, Google Drive, Dropbox usw. verzichten und stattdessen einen «hauseigenen» NAS («network attached server») verwenden, der auch von auswärts (via Internet) erreichbar ist. Zu den NAS kann ich auf einen früheren Internet Corner verweisen (http://pkweb.ch/2murFLu). Alternativ steht beim HIN auch eine «Filebox» zur Verfügung.

– Internationale Online-Händler (wie Amazon) nach Möglichkeit vermeiden. Bei diesen ist es fast nicht möglich, personalisierten Informationen auszuweichen.

– Auf «Social Media» wie Facebook und Twitter verzichten. Andere Netzwerke wie z.B. LinkedIn sind wahrscheinlich weniger invasiv, aber teilweise auch aufdringlich.

Zuletzt möchte ich noch daran erinnern, dass der Schutz vor Eindringlingen – d.h. ein regelmässig aktualisiertes Virenschutzprogramm – auf alle Fälle unerlässlich ist.

Etzel Gysling