In welchen Situationen könnte meine Privatsphäre gefährdet sein?

Social Networks

Bei der Benutzung von sozialen Netzwerken wie Facebook oder SchülerVZ kann Deine Privatsphäre auf verschiedene Art gefährdet sein.

1. Du könntest **versehentlich Informationen über Dich dem »falschen« Personenkreis preisgeben**, weil die Privatsphäre-Einstellungen nicht so sind, wie Du das möchtest oder wie Du glaubst.
2. Du **gibst grundsätzlich alle Informationen dem Anbieter des Netzwerks preis**, der dann wiederum weitreichende Möglichkeiten für die Verwendung (Werbung, Verkauf Deiner Daten etc.) oder des Missbrauchs hat.
3. Deine Daten könnten **durch Hacker gestohlen** und dann zu Geld gemacht werden, wenn diese durch Sicherheitslücken große Mengen von Datensätzen aus den Datenbanken eines Netzwerks stehlen, was immer wieder vorkommt.

Geodaten

Viele Handys und auch Kameras können feststellen, an welchem Ort sie sich gerade befinden. Sie tun das mit Hilfe des so genannten Global Positioning System (GPS) und in der Regel speichern sie diese so genannten »Geodaten« (also Deine geographische Position beim Fotografieren) »in« das Foto.

Die Geodaten können später wieder ausgelesen werden, wenn Du z.B. ein Foto zu Facebook hochlädtst. Facebook erkennt, an welchem Ort das Foto aufgenommen wurde. Da auch Aufnahmedatum und -uhrzeit mit dem Foto gespeichert wurden, kann man nun also genau sagen, an welchem Tag, zu welcher Uhrzeit sich das Handy oder die Kamera an welchem Ort befunden hat.

Aber nicht nur das: Man kann nun z.B. auf einer Karte anzeigen, an welchen Orten Du häufig Fotos machst und wann. Insgesamt kann man mit Hilfe von Geodaten ein sehr genaues »Bewegungsprofil« über Dich erstellen und damit sichtbar machen, wo Du Dich wie häufig aufhältst, zu welchen Zeiten Du typischerweise an welchen Orten bist etc. Somit könnte z.B. jemand sehen, dass Du häufig Samstag Abends Fotos in einer bestimmten Disco machst und nun wissen, dass er Dich zu dieser Zeit

also dort abpassen könnte.

Weitere Informationen

- Facebook spinnt das Hier-bin-ich-Netz
- Das ignorierte Risiko Geodaten
- Facebook bringt Places jetzt auch nach Deutschland
- Dank "Places" mit dem Finger auf andere zeigen
- Die stille Angst des Weltkonzerns

Wie kannst Du Dich schützen?

- Du kannst prüfen, ob die **Geodaten-Funktion** man bei Deinem Handy oder Deiner Kamera **abschalten** kann.
- Wenn Du Fotos zu einem Online-Dienst hochlädtst, kannst Du prüfen, ob es eine Funktion gibt, die **»Geodaten nicht speichern«** oder **»Geodaten nicht mitzuschicken«** oder ähnlich heißt und diese aktivieren.
- Du kannst genau darauf achten, wer **Zugang zu Deinen Fotos** hat und entsprechend möglicherweise Geodaten daraus entnehmen kann.

Letzlich muss Dir bewusst sein, dass **jedes mit einem Handy aufgenommene Foto möglicherweise Geodaten enthält**. Sobald Du ein solches Foto bei einem Online-Dienst hochlädtst, besteht die Gefahr, dass das Foto einem bestimmten Ort (und durch das Aufnahmedatum auch einem Zeitpunkt) zugeordnet werden kann.

Biometrie

Einkauf

Suchmaschinen

privatsphaere, reflexion, medien, datenschutz