

SICHER IN SOZIALEN NETZWERKEN



Vom Cybermobbing bis
zur staatlichen Überwachung

Tipps & Anleitungen
zum Schutz persönlicher Daten

4 Spionage und Zensur durch staatliche Behörden

4.1 Motivationen

4.1.1 Terrorprävention

4.1.2 Politische Verfolgungen

4.1.3 Verbrechensaufklärung

4.2 Wege zu Benutzerinformationen

4.2.1 Manuelle Analyse von (öffentlichen)

Benutzerprofilen

4.2.2 Automatisiertes Crawling von Benutzerinformationen

4.2.3 Zugriffe auf die Datenbestände der Betreiber

4.2.4 Überwachung des Netzwerkverkehrs

4.3 Bekannte Überwachungsprogramme

4.3.1 Die Bedeutung von Edward Snowdens Enthüllungen

4.3.2 Das PRISM-Programm der NSA

4.3.3 Überwachung der Internet-Kommunikation

4.3.4 SQUEAKY DOLPHIN

4.3.5 XKEYSCORE

4.4 Staatliche Zensur

4.4.1 QUANTUMTHEORY Hacking durch NSA und GCHQ

4.4.2 Projekt Goldener Schild in China

4.4.3 Zensur durch Gerichtsbeschlüsse, Gesetze und internationale Verträge

5 Datenmissbrauch durch

Netzbetreiber

5.1 Der finanzielle Wert von Benutzerdaten

5.2 Missbrauch freiwillig veröffentlichter Daten

5.2.1 Gefällt-mir-Angaben

5.2.2 Soziale Netzwerke

5.2.3 Beiträge und andere Textinhalte

5.2.4 Datenspeicherung verhindern

5.3 Ermittlung zusätzlicher Daten

5.3.1 Tracking-Technologien

5.3.2 Standort-Analysen

5.3.3 Freundefinder und Adressbuch-Uploads

5.4 Die grenzenlosen Überwachungsmöglichkeiten durch „Smart“-Technologie

5.5 Die Macht der Technologiekonzerne

6 Identitäts- und Datendiebstahl