

Background

Allein in Deutschland entsteht durch Wirtschaftsspionage ein jährlicher Schaden von 102,9 Milliarden Euro¹ und 88% der Unternehmen waren in den letzten zwei Jahren von Datendiebstahl betroffen², 28% davon durch Abhören. Dabei sind über 30 Prozent der Täter Konkurrenten, Lieferanten und Kunden aus Deutschland.

¹ https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf S.23

² https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf S.7

Aktuell verstoßen 55% aller Apps aus dem Google Playstore gegen die Datenschutz-Grundverordnung³.

³ <https://www.dr-datenschutz.de/55-aller-android-apps-verstossen-gegen-die-dsgvo-so-geht-es-richtig/>

Die Überwachungssoftware Pegasus ist seit mindestens 2016 aktiv und gilt laut The Guardian als das mächtigste je entwickelte Abhörtool. Sie ist kontaktlos installierbar und greift auf Daten, Mikrofone und Kameras von Smartphones zu. 2021 wurde eine Liste von 50.000 potentiellen Zielen davon gefunden. Darunter Journalist*innen, Aktivist*innen, Oppositionelle und Politiker, wie zB. der französische Präsident Macron. Die Software wird auch vom deutschen BKA und BND eingesetzt⁴.

⁴ <https://projekte.sueddeutsche.de/artikel/politik/pegasus-project-cyberangriff-auf-die-demokratie-e519915/>

Ein Schutz vor ungewollten Aufnahmen durch Smartphones ist fast unmöglich: Das Ausschalten oder das Blockieren des Netzes eines Telefons ist zumeist wirkungslos - viele Aufnahme-Prozesse laufen weiter und das Telefon versendet, sobald es wieder online ist. Sprache wird in Text umgewandelt und ist dadurch einfach zu speichern, nach Schlüsselwörtern zu filtern und als Big Data verwertbar⁵.

⁵ <https://eu.usatoday.com/story/tech/columnist/komando/2014/06/20/smartphones-nsa-spying/10548601/>

Die spanische Fußballliga Primera Division betreibt eine App für Smartphones mit etwa 10 Millionen Nutzern für Fußballrelevante Anwendungen. Durch Zufall wurde 2018 bekannt, dass die Liga während Ligaspielen die Mikrofone der Nutzer aktiviert und Audiomaterial aufnimmt, was im Umfeld der Telefone zu hören ist. Das Audiomaterial wird auf ihren Server geladen und analysiert. Ist im Hintergrund eine Fußballübertragung zu hören, so wird der Standpunkt des Nutzers getrackt. Befindet sich der Nutzer in einem öffentlichen Gebäude, wie einer Bar, so wird überprüft, ob diese Bar eine Konzession zur Übertragung von Fussball besitzt. Ist dem nicht der Fall, so wird die Lokalität abgemahnt⁶.

⁶ https://www.t-online.de/digital/sicherheit/id_83915210/250-000-euro-datenschutz-strafe-spanische-fussballliga-spionierte-fans-per-app-aus.html

www.pellta.com