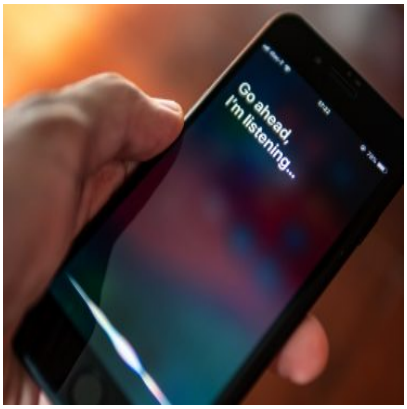

Apps und Spionage â?? der moderne Mensch Ã¼berwacht sich selbst

Morgens klingelt der Wecker auf meinem Handy, begleitet von einer Erinnerungsnotiz: â??Heute zÃ¤hlt es!â?? WÃ¤hrend des ZÃ¤hneputzens hÃ¶re ich einen Nachrichten-Podcast und Ã¼berprÃ¼fe auf meiner Smartwatch, wie viele Schritte mir diese Woche noch fÃ¼r meinen optimalen Bewegungsablauf fehlen. â??Verdammt, wieder 2.000 zu wenig.â?? Der Monatsbeitrag fÃ¼r meine Fitness-App, 15,99 Euro, wurde gestern abgebucht â?? auch diese Apps werden immer teurer. Heute steht ein wichtiger Kundentermin an. Ich gebe die Adresse in meine Navigations-App ein, um pÃ¼nktlich zu sein. Im Auto verbindet sich mein Handy automatisch, sodass ich gleichzeitig dem Vorzimmer Bescheid geben und dem Navi folgen kann. Ein Nachrichtensymbol leuchtet auf: Meine Frau schreibt, â??Viel Erfolg fÃ¼r heute!â??. Doch jetzt wieder auf den Verkehr konzentrieren â?? ein Unfall wÃ¤re katastrophal. Im RÃ¼ckspiegel ziehen andere Autos vorbei. Komisch, das schwarze Auto hinter mir war gestern auch schon da, als ich von Hannover heimfuhr.

Technologie: Segen und Risiko zugleich
Die Technologie von Smartphones und Apps hat unser Leben in den letzten 15 Jahren grundlegend verÃ¤ndert. Die Supercomputer in unseren Taschen bieten Wissen und Funktionen, die unseren Alltag bestimmen â?? aber sie laden auch ungebetene GÃ¤ste ein.

Die franzÃ¶sische Zeitung Le Monde deckte beispielsweise eine gravierende SicherheitslÃ¼cke auf: Ã?ber die Fitness-App Strava wurden unbeabsichtigt sensible Informationen aus dem Schutzteam des franzÃ¶sischen PrÃ¤sidenten Emmanuel Macron Ã¶ffentlich. Strava, mit knapp 100 Millionen Nutzern, zeichnet sportliche Leistungen auf und hat einen Social-Media-Charakter. Nutzer kÃ¶nnen anderen folgen, Erfolge kommentieren und Updates teilen.

Le Monde fand heraus, dass Macrons LeibwÃ¤chter regelmÃ¤Ã?ig ihre Joggingrouten teilten. Diese fÃ¼hrten oft zu Hotels, in denen Macron untergebracht war. So wurde beispielsweise das Londoner Hotel Savoy, in dem Macron 2022 zur Trauerfeier fÃ¼r Queen Elizabeth wohnte, durch die Strava-Daten seiner SicherheitskrÃ¤fte enttarnt. Ã?hnliche Leaks entdeckten die Journalisten beim US Secret Service, dessen Bodyguards Ã¶ffentlich ihre AktivitÃ¤ten und teils sogar Fotos teilten. Selbst im Umfeld von Wladimir Putin kamen Ã¼ber Strava sensible Informationen ans Licht, etwa der geheime Treffpunkt mit Kim Jong-un oder Routen um ein luxuriÃ¶ses Anwesen am Schwarzen Meer, dessen Eigentum Putin bestreitet.

Apps als Sicherheitsrisiko
Trotz solcher VorfÃ¤lle sehen BehÃ¶rden das Risiko unterschiedlich. WÃ¤hrend das WeiÃ?e Haus neue Vorschriften prÃ¼ft, erklÃ¤rte die franzÃ¶sische PrÃ¤sidentschaft gelassen, es gebe â??kein Sicherheitsrisikoâ??. Der Kreml schwieg.

Doch Strava ist kein Einzelfall. Oft erlauben wir Apps leichtfertig den Zugriff auf Standort, Mikrofon und Kamera â?? ideale AngriffsflÃ¤chen fÃ¼r Hacker oder andere Akteure. Auch groÃ?e App-Anbieter geraten in Kritik. So wird Meta, dem Facebook, Instagram und WhatsApp gehÃ¶ren, vorgeworfen, GesprÃ¤che Ã¼ber das Handymikrofon abzuhÃ¶ren. Viele Nutzer berichten, dass sie nach privaten Unterhaltungen gezielte Werbung zu den angesprochenen Themen erhalten hÃ¤tten.

Facebook: Kein AbhÃ¶ren, aber umfangreiche Daten
Offiziell dementiert Facebook solche Praktiken. Das Unternehmen verweist darauf, dass das AbhÃ¶ren technisch aufwendig und leicht nachweisbar wÃ¤re. Zudem wÃ¼rde es die Akkulaufzeit der GerÃ¤te stark beeintrÃ¤chtigen. Experten und

Apple, ein selbsternannter Gegner von Datensammlungen, bestÃ¤tigen, dass eine solche Funktion in Facebook-Apps bisher nicht gefunden wurde. Ironischerweise sieht sich Apple selbst VorwÃ¼rfen gegenÃ¼ber, dass die EinfÃ¼hrung von App Tracking Transparency (ATT) nur dabei helfe, das Tracking durch Drittanbieter zu reduzieren. Allerdings habe Apple gleichzeitig sein eigenes Werbenetzwerk, SkadNetwork, ausgebaut.

Doch Facebook benÃ¶tigt solche Daten auch gar nicht. Es sammelt bereits umfassende Informationen aus der Plattformnutzung: Gruppenmitgliedschaften, Aufenthaltsorte, Interessen und demografische Daten. Hinzu kommen Webtracking-Methoden, etwa Ã¼ber Cookies oder Links mit speziellen Codes wie â??fbclidâ??, die externe Webseiten mit Facebook-Daten verknÃ¼pfen.

Das Fazit
Die personalisierte Werbung, die uns so oft Ã¼berrascht, basiert auf umfangreichen Datensammlungen, nicht auf abgehÃ¶rten GesprÃ¤chen. Doch ob detailliertes Nutzerprofiling durch Tracking besser ist als das direkte AbhÃ¶ren, bleibt fraglich. Klar ist: Wir Ã¼berwachen uns oft selbst â?? und laden damit die Risiken bewusst ein.

Quellenangaben
Titelbild von Robert Kneschke â?? stock.adobe.com (redaktionelle Nutzung)

https://www.sueddeutsche.de/politik/sicherheitsluecke-strava-biden-putin-macron-leibwaechter-lux.DgVAXqhL7FU1swsw8FfLPt
https://www.spiegel.de/sport/strava-ist-die-fitness-app-ein-sicherheitsrisiko-a-505b6ea8-0498-4aa7-b007-efb04fdb9d7d
https://www.businessinsider.com/guides/tech/does-facebook-listen-to-you
https://www.chip.de/news/Massive-Sicherheitsprobleme-Perso-App-am-Handy-laesst-sich-uebertoelpeln_184378889.html
https://www.lemonde.fr/en/pixels/article/2024/10/27/strava-the-exercise-app-filled-with-security-holes_6730709_13.html
https://www.dr-datenschutz.de/apple-das-datenschutz-unternehmen-oder-doch-nicht/