Mittwoch, 06. August 2025, 14:00 Uhr
~5 Minuten Lesezeit

Nur zur Sicherheit

Viele Menschen glauben, sie handeln verantwortungsvoll, wenn sie wichtige Bereiche ihres Lebens digital gestalten — dabei ist das Smartphone selbst die größte Sicherheitslücke.

von Günther Burbach
Foto: Have a nice day Photo/Shutterstock.com

Es beginnt mit einem Gedanken: „Ich mache das nur zur Sicherheit." Ein Selfie für die Bank, ein Fingerabdruck für die Gesundheits-App, ein kurzer

Scan für den Login bei der Rentenkasse. Alles per Smartphone, alles bequem. Und angeblich alles sicher. Doch je tiefer man blickt, desto klarer wird: Das Smartphone ist nicht deine Schutzmauer, es ist das Einfallstor.

Die große Selbsttäuschung

Wir alle tragen unsere Smartphones mit uns, Tag und Nacht. Sie sind Kamera, Notizbuch, Geldbörse, Terminplaner, Kreditkarte, Zeitung, TV-Gerät, Behördengang in einem. Wir entsperren sie mit unserem Gesicht, lassen sie unsere Stimme erkennen, erlauben ihnen Zugriff auf Standort, Kontakte, Mikrofon, Gesundheitsdaten. Es ist der intimste digitale Spiegel unseres Lebens. Und gleichzeitig der am schlechtesten geschützte. Warum also wird ausgerechnet dieses Gerät als Plattform für Sicherheit verkauft? Die Antwort ist unbequem: weil es den Anbietern dient — nicht dir.

Die neue Abhängigkeit

Früher gingen wir mit dem Ausweis zur Bank. Heute verlangt die Bank, dass wir unser Smartphone nutzen. Mit Kamera. Mit Gesichtsscan. Mit einer App, deren Anbieter wir nicht kennen. FortiToken, WebID, Nect, Verimi, Plattformen, die zwischen uns und unsere Bank, unsere Versicherung, unsere Steuererklärung geschaltet sind. Sie speichern Daten. Sie übertragen sie. Und manchmal weiß nicht einmal die Bank, was genau dort verarbeitet wird.

> ***Die Datenspeicherung erfolgt häufig in der Cloud, oft auf Servern in den USA, manchmal in Europa, selten nachvollziehbar. Der berüchtigte US CLOUD Act erlaubt es US-Behörden, auf Daten zuzugreifen, die von US-Unternehmen gespeichert werden, auch wenn diese physisch in Europa liegen.***

Das bedeutet: Wer etwa Fortinet nutzt, einen US-Anbieter, und gleichzeitig glaubt, seine Daten seien durch die Datenschutz-Grundverordnung (DSGVO) geschützt, der irrt.

Der Mythos vom sicheren Handy

Smartphones sind keine geschützten Container. Sie sind Schnittstellen. Du installierst eine App, und du gibst ihr Rechte: Zugriff auf Kamera, Standort, Kontakte, Speicher, Netzwerkstatus, Telefonfunktion. Viele Banking-Apps verlangen Zugriff auf das Mikrofon. Warum? Viele TAN-Apps lesen SMS mit. Andere dürfen Bildschirminhalte erfassen. Noch andere verwenden die Kamera auch im Hintergrund. Und all das auf einem Gerät, das per Bluetooth, WLAN, Mobilfunk pausenlos mit Servern kommuniziert. Sicher? Nein. Offen wie ein Scheunentor. Nur schön verpackt.

Online-Banking: Komfort statt Kontrolle

Es ist bequem. Man öffnet seine Banking-App, scannt den QR-Code, tippt eine TAN, bestätigt per Gesicht. Doch wer liest sich schon die AGB der App durch? Wer prüft, welche externen Dienste sie verwendet? Wer weiß, ob diese App auf deinem Smartphone Root-Zugriff erkennt, oder ob sie sich von böswilliger Software manipulieren lässt?

> ***Aktuelle Untersuchungen zeigen: Die meisten Banking-Apps sind voller Schwachstellen. Im Schnitt enthalten sie 50 bis 80 potenzielle Sicherheitslücken, darunter Zugriff auf sensible Systemfunktionen. In einer Welt, in der Trojaner wie „Godfather“ oder „BlackRock“ gezielt auf mobile Bankdaten zielen, ist dein Smartphone ein offenes Ziel.***

Hinzu kommt: Push-TANs, die vermeintlich so sicher sind, laufen über denselben Kanal wie der Angriff. Wer dein Gerät kompromittiert, hat beides: die Banking-App und die TAN.

Der stille Kontrollverlust

Je mehr du über dein Smartphone autorisierst, desto weniger kontrollierst du. Du nutzt das Handy für Behördengänge, für das Impfzertifikat, für die Gesundheitsakte, für Steuern, für Vertragsabschlüsse, für die Altersvorsorge. Alle Daten, alle Berechtigungen, über ein einziges Gerät.

Ein Diebstahl reicht. Eine Malware. Ein kompromittierter App-Zugriff. Schon ist nicht nur dein Geld in Gefahr, sondern dein gesamtes digitales Leben. Und schlimmer: Du merkst es oft nicht einmal. Moderne Schadsoftware läuft unsichtbar. Sie erstellt Schatten-Apps, kopiert Bildschirmdaten, greift Tastatureingaben ab, aktiviert Mikrofone. Und du denkst, du hast alles im Griff.

Das Smartphone als trojanisches Pferd

Was wir als Werkzeug der Freiheit begreifen, ist in Wahrheit ein trojanisches Pferd.

> ***Es bringt nicht uns in die Welt, sondern die Welt in uns. Mit jeder App, die wir installieren, öffnen wir Türen. Hinter jeder App stehen nicht nur Entwickler, sondern ganze Analyseketten, die unser Verhalten aufzeichnen, Muster erkennen, Verhaltensvorhersagen erstellen und im Zweifel an Dritte verkaufen.***

In der Realität bedeutet das: Deine Interaktionen, deine Gewohnheiten, deine Wege, deine Käufe, deine Bewegungen, alles wird protokolliert. Ein Bewegungsprofil sagt mehr über dich als dein Tagebuch. Und dein Smartphone schreibt dieses Profil jeden Tag, automatisch, unaufgefordert.

Der Datenschutz als Placebo

Viele Nutzer beruhigen sich mit dem Hinweis auf die DSGVO. Doch in der Praxis ist die Datenschutz-Grundverordnung ein Placebo, solange die Architektur der Technik unberührt bleibt. Denn selbst wenn du einer App bestimmte Berechtigungen entziehst, kann sie durch andere Schlupflöcher auf Daten zugreifen oder sich über fremde Dienste, Software Development Kits (SDKs), Werbung oder Hintergrundprozesse Zugang verschaffen. Außerdem: Die DSGVO greift nicht in außereuropäischen Rechtsräumen. Nutzt eine App Server in den USA oder Dienstleister aus Drittstaaten, sind deine Daten nur so sicher, wie es der schwächste Punkt in dieser globalen Kette erlaubt. Und der ist oft schwach.

Wer profitiert wirklich?

Jedenfalls nicht du. Profiteure sind:

• Plattformanbieter, die Identitätsdienste verkaufen;

• App-Entwickler, die aus jedem Klick ein Profil erstellen;
• Analysefirmen, die Nutzerverhalten auswerten;
• Cloudanbieter, die aus Daten Besitz machen;
• Sicherheitsbehörden, die jederzeit zugreifen können.

Du bist Produkt und Risiko in einem.

Was tun?

Zunächst: Vertraue deinem Smartphone nicht. Es ist kein Sicherheitswerkzeug. Es ist ein Werkzeug der Bequemlichkeit und der Kontrolle.

Zweitens: Nutze separate Geräte für Banking, für TANs, für Identität. Lass nicht alles auf einem Gerät laufen.

Drittens: Fordere Alternativen. Schriftliche Verfahren. Post-Ident. Vor-Ort-Verifikation. Offline-Tokens. Hardware-Schlüssel.

Viertens: Mach anderen bewusst, wie tief diese Gefahr reicht. Sprich darüber. Schreibe darüber. Wehre dich gegen eine Zukunft, in der deine gesamte Existenz von einem einzigen digitalen Schlüsselbund abhängt.

Denn es gibt nichts Unsichereres als ein Gerät, das alles kann und alles weiß. Und nichts Gefährlicheres als eine Gesellschaft, die genau das als Fortschritt verkauft.

Günther Burbach, Jahrgang 1963, ist Informatikkaufmann, Publizist und Buchautor. Nach einer eigenen Kolumne in einer Wochenzeitung arbeitete er in der Redaktion der Funke Mediengruppe. Er veröffentlichte vier Bücher mit Schwerpunkt auf Künstlicher Intelligenz sowie deutscher Innen- und Außenpolitik. In seinen Texten verbindet er technisches Verständnis mit gesellschaftspolitischem Blick — immer mit dem Ziel, Debatten anzustoßen und den Blick für das Wesentliche zu schärfen.