Bizarre Telefonüberwachung: Handy-Akku als Spionagewerkzeug

von Andreas von Rétyi

Quelle: KOPP Online vom 10.08.2016

Eine Studie der amerikanischen Princeton University warnt vor einer völlig neuen Form der Datenüberwachung.

- **Plötzlich wird sogar der Ladezustand eines Handys zur ungewollten Informationsquelle für Unbefugte.**

Dieser zusätzliche Eingriff in die Privatsphäre könnte manchen Dienstleistern sogar zusätzliche Profite bescheren – und etlichen Nutzern so manche Unannehmlichkeiten.

Trotz aller Abhörskandale und Warnungen leben die meisten Menschen immer noch in einem ziemlich ungetrübten Verhältnis zu ihrem Telefon. Und doch sind wir vielfach Sklaven von Handy & Co. geworden. Natürlich weiß heute jeder um die Überwachungsgefahren, die mit der Telekommunikation verbunden sind.

Spätestens seit Snowden sollte das nicht mehr als »Verschwörungstheorie« gelten. Umso erstaunlicher, dass wir nach wie vor unzählige private Informationen per Telefon austauschen, die kaum für Dritte gedacht sind. Die Gesellschaft zeigt sich hier eher gleichgültig, wo es doch ohnehin alle betrifft, sogar die Kanzlerin. Und außerdem, die ganze Sache scheint alternativlos.

Also, das Problem beruht nicht allein auf Bequemlichkeit oder dem alten Gewohnheitsprinzip. Dass die »andere Seite« diese Situation weidlich ausnutzt, ist ja hinlänglich bekannt. Geheimdienste und Hacker greifen Handy-Daten ab, überwachen die GPS-Nutzung und erstellen umfassende Profile unserer Aktivitäten. Doch jetzt warnen Forscher der Princeton University vor einer neuen Falle.

Ein 2015 veröffentlichtes Programmier-Interface ermöglicht Web-Entwicklern, den Akkustand von Geräten zu überwachen, mit denen Internetseiten und entsprechende Apps angesteuert werden. Die Idee dahinter wirkt zunächst völlig harmlos: Das Ziel soll automatisch erkennen, wenn der Akkustand des Besuchergeräts niedrig ist. Dann soll es den Nutzer mit einer abgespeckten Version der gewählten Seite versorgen, um Energie zu sparen.

So gelangt der dankbare Gast mit größerer Wahrscheinlichkeit noch an alle benötigten Informationen, bevor der Akku schlappmacht. Die Princeton-Forscher berichten nun allerdings, entdeckt zu haben, wie dieser neue Code missbraucht werden kann, um persönliche Nutzerinformationen abzugraben.

Jedes Handy sammelt verschiedene Messdaten zum Energiestatus. Drei getrennte Messungen betreffen den aktuellen Prozentsatz gegenüber voller Ladung, die verbleibende Sekundenzahl bis zur Entladung sowie die Zeit bis zur vollen Ladung nach Anschluss an ein Ladegerät. Wie die amerikanischen Handy-Forscher erläutern, sind hier mehr als 14 Millionen individuelle Kombinationen möglich, weshalb allein der Ladestatus eines jeden Handys als nahezu sichere Identifikationshilfe genutzt werden könne.

Die Princeton-Wissenschaftler starteten daraufhin ein Projekt zur Überwachung der Überwachung, indem sie Webseiten mit einem speziellen Browser besuchten. Der ermöglichte ihnen die Identifikation und Überwachung aller Seiten oder Apps, die ihre Daten abgriffen. Während dieses Experiments fanden sie immerhin zwei Seiten, die den Akku-Indikator tatsächlich zur Überwachung der individuellen Daten nutzten und dem jeweiligen Gerät eine Art »Fingerabdruck« zuordneten. So wurde der aktuelle Ladungszustand ermittelt und mit verschiedenen anderen Identifizierungsmerkmalen kombiniert, um anschließend den Datenverkehr zu verfolgen.

Dr. Łukasz Olejnik ist Berater für Informationssicherheit. Er sieht in der überwachten Akku-Anzeige sogar eine künftige Einnahmequelle für Seitenbetreiber. Schwarze Schafe der Branche könnten die zusätzliche Information skrupellos ausnutzen: Die Ebbe im Akku könne sich auf Kundenentscheidungen auswirken, so dass einige Leute bereit wären, schneller zu handeln und für bestimmte Dienstleistungen plötzlich auch mehr zu bezahlen.

Also das alte Prinzip, aus einer mehr oder minder ausgeprägten Notsituation zu profitieren. Und ganz selbstverständlich profitiert auch der Sicherheitsberater aus der wachsenden Unsicherheit.

Wenn immer mehr Methoden und Möglichkeiten gefunden werden, um Daten abzugreifen und die private Kommunikation auf verschiedenen Ebenen und zu den unterschiedlichsten Zwecken auszuloten, und wenn diese Attacken künftig immer häufiger werden, dann werden vielleicht auch Abwehrmaßnahmen wie die vom NSA-Renegaten Edward Snowden und dem US-Hacker Andrew Huang gemeinschaftlich entworfene Introspection Engine zum verbreiteten Zubehör avancieren.

Diese »Anti-Spionage-Hülle« fürs Handy soll Nutzer warnen, sobald eine heimliche Datenübertragung stattfindet. Vielleicht aber werden die Menschen auch noch gleichgültiger, weil sie nicht ständig an die Überwachung erinnert werden wollen, weil alles längst zur Gewohnheit geworden ist, weil Privatsphäre eben gestern war und weil sie ohnehin nichts zu verbergen haben.

Doch umsichtige Zeitgenossen warnen eindringlich. Sie erinnern daran, dass uns die Geschichte immer wieder vorgeführt hat, wie eine Verschiebung in der politischen Landschaft aus ehedem völlig normalen und harmlosen Menschen plötzlich Verbrecher macht. Dann könnten diese oder jene arglos ausgetauschten Informationen ebenso plötzlich zum Verhängnis werden.