Überwachungs-Experte: „Es ist heute unglaublich leicht, den Ruf eines Menschen zu zerstören“

Ronald Deibert hat mit seinem Citizen Lab weltweit Überwachungsskandale aufgedeckt. Im Interview erklärt der Kanadier, welche Bedrohung ihn zurzeit mehr beunruhigt als alle anderen zuvor – und warum er in Wien lieber inkognito bleibt.

„Es gibt eine neue Form der Überwachung, die kein Hacking braucht“, sagt Roland Deibert. Barbara Aichinger

06.06.2026 um 19:55
von Jürgen Streihammer

Artikel verschenken

Ronald Deibert sitzt zwischen meterhohen Bücherwänden in einer Bibliothek unweit des Donaukanals. Er trägt ein schwarzes T-Shirt und einen Dreitagebart. Seit ein paar Wochen schon ist er Gastwissenschaftler des Instituts für die Wissenschaft vom Menschen (IWM) in Wien. Aber groß publik gemacht hat er das zunächst nicht. „Ich wollte kein unnötiges Risiko eingehen.“ Denn erstens sei Wien ein „Zentrum der Spionage“: „Es ist hier absolut legal, dass Ausländer einander bespitzeln.“ Und zweitens hat sich Deibert mit mächtigen Gegnern angelegt. Sein „Citizen Lab“, angedockt an der Uni von Toronto, legte im Laufe der Jahre große Überwachungsskandale offen, darunter jenen um die Pegasus-Software, mit der Journalisten und Politiker bespitzelt wurden. Dabei ist Deiberts Team klein: rund zwei dutzend dauerhafte Mitarbeiter, die jedoch teils von Tech-Riesen übergelaufen sind und auf viel Geld verzichtet haben, um sich in den Dienst der Zivilgesellschaft zu stellen. Das Ergebnis erstaunt: Mehrfach schon führte die Arbeit des Teams dazu, dass eine Milliarde Apple-Nutzer Notfall-Sicherheitsupdates auf ihren Smartphones erhielten.

Ich nehme das Interview mit meinem Smartphone auf, falls Sie das nicht stört.

Ronald Deibert: Klar. Welches Betriebssystem? Android oder iOS?

Warum fragen Sie?

In unserer Arbeit macht das einen großen Unterschied. Android löscht bei jedem Neustart die Protokolldateien - aus forensischer Sicht ist das so, als würde man Beweise vernichten, sobald jemand sein Gerät neu startet. Das iPhone (iOS) speichert sie umgekehrt akribisch. Mit Zustimmung der Person können wir dann einen „Crash-Log“ - im Grunde einen Fehlerbericht - erzeugen und auf bekannte Spyware-„Fingerabdrücke“ analysieren. So arbeiten wir.

Wie kommt Überwachungssoftware (Spyware) überhaupt auf das Smartphone?

Zunächst braucht man einen Exploit - also eine Sicherheitslücke im Betriebssystem, die dem Hersteller nicht bekannt ist. Eine Apple nicht bekannte Schwachstelle kostet bei Händlern auf dem Schwarzmarkt zurzeit wohl um die zehn Millionen US-Dollar. Normalerweise muss das Opfer dann auf einen Link in einer SMS klicken oder Ähnliches. Bei der Pegasus-Version, die wir 2021 entdeckt haben, war das aber anders: Sie erforderte keinerlei Interaktion des Opfers. Man musste nichts anklicken oder öffnen. Ein Zero-Click-Exploit.

Wie schützen Sie eigentlich Ihr Handy?

Mit dem Lockdown-Modus von Apple. Er wurde bisher nicht kompromittiert. Ich empfehle ihn für besonders gefährdete Personen. Für Android-Nutzer gibt es das „Erweiterte Sicherheitsprogramm“.

Und wozu raten Sie Durchschnittsbürgern?

Die Software regelmäßig zu aktualisieren.

Und das hilft?

Kommt darauf an. Gegen Überwachungssoftware großer israelischer oder europäischer Firmen ist es fast unmöglich, sich ohne extreme Maßnahmen zu schützen.

Diese privaten Sicherheitsfirmen spielen heute offenbar eine wichtige Rolle.

Ja. Spionage wurde in den vergangenen Jahren zur Dienstleistung. Kleine Staaten ohne technische Kapazitäten können sich heute NSA-ähnliche Überwachungsfähigkeiten einfach kaufen. Das ist eine historische Wende. Sie bedeutet zu Ende gedacht die Privatisierung von Geheimdiensten - und zwar ohne Regulierung und ohne öffentliche Kontrolle. Denn Firmen, die geheim bleiben wollen, verkaufen an Staaten, die das alles auch geheim halten wollen. Was mich zurzeit aber am meisten beunruhigt, ist eine Methode, die ganz ohne das Hacken von Handys und ohne Spyware auskommt.

Wie funktioniert sie?

Sie nutzt Daten aus dem Werbe- und App-Ökosystem. Jedes Mal, wenn Sie eine App öffnen oder eine Website besuchen, werden Daten über Sie, Ihr Gerät, Ihren Browser, Ihren Standort und Ihr demografisches Profil an Werbetreibende versteigert, die wirklich binnen Millisekunden darum bieten, Ihnen eine gezielte Werbung anzeigen zu dürfen. Private Sicherheitsfirmen können diese Daten aber auch erwerben, bündeln und als Sicherheitsprodukt verkaufen.

Und dann?

Stellen Sie sich vor, ich arbeite für einen Geheimdienst und weiß, dass ein Treffen in diesem Gebäude stattfindet - genau wo Sie und ich jetzt sitzen. Ich ziehe also einen digitalen Zaun um das Gebäude und frage ab: „Wer ist gerade hier?“ Das System liefert mir nicht nur unsere Namen - es sagt mir, wo wir wohnen, für wen wir arbeiten und so weiter. Ich kann auch rückwirkend abfragen, wo wir vor sechs Monaten waren. Und das ohne dass ein einziges Gerät gehackt wurde. In Europa verstößt die Methode so gut wie sicher gegen die Datenschutz-Grundverordnung.

Welche Staaten setzen sie ein?

Ungarn war der erste bestätigte europäische Kunde einer Firma, die so etwas anbietet. Ich wette aber, es gibt viele weitere in Europa. Von Österreich weiß ich es nicht.

Apropos Österreich: Ist es Ihnen in Ihrer Arbeit untergekommen?

Wir haben eine Hack-for-Hire-Firma in Neu-Delhi untersucht, die von Wirecard beauftragt wurde, einen Leerverkäufer zu verfolgen. Dieser teilte seine Erfahrungen mit uns, und wir konnten nicht nur bestätigen, dass sein Gmail-Konto von indischen Hackern kompromittiert worden war, sondern auch ein ganzes globales Netzwerk weiterer Ziele aufdecken. Ich vermute, der Auftrag kam direkt von Jan Marsalek.

Auch das Citizen Lab wurde zum Ziel: „Das beunruhigt einen.“ Barbara Aichinger

Ihr Citizen Lab wurde selbst mehrfach zum Ziel von Überwachungsaktionen. Was war die schlimmste Situation?

Einmal wurde ein Mitarbeiter unter dem Vorwand kontaktiert, es gehe um syrische Flüchtlingshilfe. Das erste Treffen kam dem Mitarbeiter dann seltsam vor. Wir ließen die Operation aber weiterlaufen und arrangierten mit Associated Press eine Falle in einem New Yorker Restaurant - mit versteckter Kamera. Der Mann, der kam, war ein Ex-Mossad-Agent.

Was macht diese Bedrohung mit Ihnen?

Das ist nervenzehrend. Es beunruhigt einen.

Was halten Sie für das größte Missverständnis über digitale Überwachung?

Die Haltung: „Ich habe nichts Falsches gemacht und daher nichts zu verbergen.“ In unserem Bericht „Catalangate“ haben wir dokumentiert, wie Spanien systematisch die katalanische Zivilgesellschaft ausspioniert hat. Dabei wurden Telefone von Familienmitgliedern gehackt, die keine politische Rolle spielten, darunter eine Onkologin, die Daten ihrer Krebspatienten auf dem Handy hatte. Außerdem möchte ich nicht in einer Gesellschaft leben, in der eine Regierung auf Knopfdruck herausfinden kann, wo man war und wem man begegnet ist. Die liberale Demokratie ist wirklich in Gefahr.

Was bereitet Ihnen eigentlich größere Kopfschmerzen: Überwachungssoftware oder Desinformation?

Desinformation. Es gibt inzwischen viele Firmen, die so etwas wie „dunkle PR“ verkaufen – auf den Philippinen, in Afrika, in Mexiko und anderswo. Wer den Ruf einer Person zerstören will, kann solche Anbieter beauftragen. Sie können mit KI gefälschte Videos oder Kampagnen erstellen, die das Opfer zum Beispiel im Zusammenhang mit Minderjährigen zeigen. Anschließend werden solche Inhalte gezielt in sozialen Netzwerken verbreitet. Die Plattformen sind ein idealer Verstärker: Ihre Algorithmen belohnen genau jene Inhalte, die extrem oder empörend sind. Es ist heute jedenfalls unglaublich leicht, den Ruf eines Menschen zu zerstören.

Vielleicht sind wir in einer Übergangsphase und lernen bald, Inhalten im Netz grundsätzlich zu misstrauen?

Aber wem nützt das? Wenn alle denken, alles sei erfunden und es gebe keine Wahrheit, begünstigt das doch nur Autoritarismus und Faschismus.

Da Sie KI erwähnt haben: Welche Rolle spielt sie in all dem?

KI verändert gerade alles. Die meisten erfolgreichen KI-Konzerne sind US-amerikanisch, und ihre Eigentümer sagen oft offen, dass ihr Geschäft im Dienst US-amerikanischer Machtinteressen steht. Für alle Nicht-US-Amerikaner ist das beunruhigend - besonders weil Menschen KI heute für intimste Themen nutzen: Beziehungsprobleme, Steuern, persönliche Krisen. Diese Daten verschwinden nicht. Sie landen bei Unternehmen, die damit detaillierte Profile erstellen können. Werden diese Informationen an Behörden weitergegeben, ist das ein massiver Eingriff in die Bürgerrechte. Das ist ein Game-Changer.

Eine Pointe ist: Um KI-Missbrauch aufzudecken, könnte es KI brauchen.

Mozilla, die Entwickler des Firefox-Browsers, haben zwar gezeigt, wie die Zahl entdeckter Sicherheitslücken steil nach oben schoss, sobald sie dafür KI einsetzten. Man könnte also meinen, das gleicht sich aus. Aber der Zugang zu KI verteilt sich nicht gleichmäßig. Es gibt mächtige Akteure, die KI-Systeme offensiv einsetzen. Bis die Verteidigung aufholt, wird es lange dauern. Das wird sich nicht einfach einpendeln.

Zur Person

Ronald Deibert (62) ist Professor für Politikwissenschaft an der Universität Toronto. 2001 gründete er dort das Citizen Lab, das seither zahlreiche illegale Überwachungstätigkeiten aufgedeckt hat. 2013 wurde Deibert dafür mit der Diamantenen Jubiläumsmedaille von Königin Elizabeth II. ausgezeichnet.

Der Politologe – Schwerpunkt internationale Beziehungen und Sicherheitspolitik –
ist Visiting Fellow am Institut für die Wissenschaft vom Menschen IWM) in Wien.