

26. Januar 2018, 18:00 Überwachung

Polizei spioniert Handynutzer mit Trojaner aus

- Das Bundeskriminalamt (BKA) setzt in laufenden Verfahren Trojaner-Software ein, mit der auch verschlüsselte Botschaften auf Smartphones und Tablets abgefangen werden können.
- Die Verschlüsselung selbst wird nicht gebrochen, sie wird umgangen.
- Ermittler setzen große Hoffnungen in diesen Trojaner. Sie sagen, dass sie ohne dieses Werkzeug zunehmend im Dunkeln tappen.
- Gegner der Software kritisieren, dass durch den Einsatz des Trojaners die digitale Sicherheit von Bürgern gefährdet werde.

Von Reiko Pinkert und Hakan Tanriverdi

Das Bundeskriminalamt (**BKA**) hat damit begonnen, eines der umstrittensten Ermittlungswerkzeuge der vergangenen Jahre einzusetzen: den Staatstrojaner für Smartphones. Nach Informationen von *Süddeutscher Zeitung*, WDR und NDR wird dieser bereits in aktuell laufenden Ermittlungsverfahren verwendet, um auf Daten und Dokumente von verdächtigen Personen zuzugreifen. Das BKA wollte aus "einsatztaktischen Gründen" keine Auskünfte erteilen, wie oft die Software bereits eingesetzt wurde.

Als Staatstrojaner wird in der Öffentlichkeit eine Software bezeichnet, die von staatlicher Seite eingesetzt wird und die Sicherheitslücken in Computern ausnutzt. Das gilt für Desktop-Rechner und Laptops als auch für die in der Regel besser geschützten Smartphones und Tablets. Ermittler lehnen den Begriff Staatstrojaner ab. Sie sprechen von Quellen-Telekommunikationsüberwachung (Quellen-TKÜ).

Strafverfolger beklagen sich seit Jahren darüber, dass sie nicht mehr in der Lage sind, effektiv im Internet zu ermitteln. Die Gesellschaft verlagert ihre Kommunikation zunehmend in Chat-Apps. Kriminelle tun das auch. Die Anbieter von Chat-Apps, zum Beispiel Whatsapp oder Signal, verschlüsseln die Kommunikation mitunter komplett. Dieser Code ist einbruchsicher, auch Ermittler bleiben draußen.

Es komme deshalb insgesamt "zu teils erheblichen Überwachungslücken", wie es BKA-Vizepräsident Peter Henzler in einer Anhörung im Bundestag formulierte. In die Quellen-

TKÜ setzen die Ermittler also große Hoffnungen, denn über diesen Weg gelingt es ihnen, an die Daten zu kommen, bevor sie verschlüsselt werden. Sie zapfen die Quelle an, daher die Bezeichnung Quellen-TKÜ.

In Haushaltsunterlagen für das Jahr 2017 beantragte das BKA Sachmittel im Umfang von 50 Millionen Euro, um die "operativen IT-Systeme" zu verbessern. Der Smartphone-Trojaner wurde damals als "3. Produktlinie" bezeichnet. Die erste und zweite Produktlinie galt Laptops und Desktop-Rechnern.

Im Sommer 2017 hatte die Bundesregierung in einem Gesetz die rechtlichen Rahmenbedingungen für den Einsatz von Trojanern klarer geregelt. Seither können Ermittler sowohl laufende Kommunikation - Telefongespräche, Chatprotokolle, E-Mails - überwachen, als auch Daten auslesen, die auf dem Gerät abgespeichert wurden, bevor Strafverfolger gegen die verdächtige Person ermittelt haben. Die Hürden im letzteren Fall, der Online-Durchsuchung, liegen höher. Befürchtet wird deshalb, dass diese Maßnahme in den polizeilichen Alltag einziehen könnte.

Rechner sind wie zusätzliche Gehirne

Das Bundesverfassungsgericht erlaubte in einem Urteil 2008 das Mittel der Online-Durchsuchung, setzte aber enge Grenzen. Auch ein neues Grundrecht entwickelte man in Karlsruhe aus der Überzeugung heraus, dass Rechner mittlerweile verwendet werden wie zusätzliche Gehirne und dort deshalb intime und schützenswerte Details zu finden sein können: das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Der Einsatz von Staatstrojanern wird von IT-Sicherheitsexperten kritisiert. Denn für die Quellen-TKÜ und Online-Durchsuchung wird es in vielen Fällen nötig sein, Schwachstellen auszunutzen, die der Öffentlichkeit unbekannt sind. Das Problem ist: Eine Sicherheitslücke in einem iPhone betrifft alle iPhones und nicht ausschließlich die der Kriminellen.

Behördenmitarbeiter, die nicht namentlich zitiert werden wollen, betonten bisher stets, dass der Einsatz des Staatstrojaners kein Standardwerkzeug werde. Schließlich seien die Entwicklungskosten sehr hoch und jeder Einsatz berge die grundsätzliche Gefahr aufzufliegen. IT-Sicherheitsexperten fordern dagegen, die entdeckten Lücken zu schließen. Schließlich könnten auch kriminelle Hacker diese Lücken nützen, um Bürger auszuspionieren. Werden die Firmen auf einen Fehler aufmerksam, dann wird eine neue Version des Betriebssystems veröffentlicht, in der diese Lücke gestopft ist.

Kritik an "digitaler Spitzelei"

Dass Strafverfolger auch ganz ohne Staatstrojaner erfolgreich ermitteln können, zeigt sich daran, dass es ihnen im zweiten Halbjahr 2017 in zwei Dutzend Fällen gelungen ist, Messenger zu überwachen. Teilweise haben die Ermittler einfach ein weiteres mobiles Endgerät auf dem Account der verdächtigten Person angemeldet. Das ist zum Beispiel

dann möglich, wenn eine App die Chats nicht komplett verschlüsselt. Mit dem Verfahren war es dem BKA auch 2015 gelungen, monatelang Chat-Nachrichten der rechtsextremen Gruppe "Oldschool Society" mitzulesen. Deren Mitglieder wurden im März 2017 vom Oberlandesgericht München zu mehrjährigen Haftstrafen verurteilt.

Das Vertrauen der Bürger in digitale Privatsphäre werde durch die "digitale Spitzelei" ausgehöhlt, sagte Andrej Hunko (Linke), als Anfang dieser Woche Zahlen zu weiteren Ermittlungsmaßnahmen von Polizei und Verfassungsschutz öffentlich wurden. "Handys sind zum Telefonieren da, nicht um deren Besitzer heimlich zu verfolgen", betonte Hunko.

Die Bürgerrechtsorganisation "Gesellschaft für Freiheitsrechte" plant, gegen das Gesetz, das den Staatstrojaner erlaubt, Verfassungsbeschwerde zu erheben. Derzeit werde an einer Beschwerdeschrift gearbeitet.

[Der Staatstrojaner frisst die Grundrechte auf](#)
[Der größte, umfassendste, weitreichendste, heimlichste und gefährlichste Grundrechtseingriff hat](#)
[begonnen. Kommentar von Heribert Prantl mehr...](#)

URL: <http://www.sueddeutsche.de/digital/ueberwachung-polizei-spioniert-handynutzer-mit-trojaner-aus-1.3842439>

Copyright: Süddeutsche Zeitung Digitale Medien GmbH / Süddeutsche Zeitung GmbH

Quelle: SZ vom 27.01.2018/hatr/jab

Jegliche Veröffentlichung und nicht-private Nutzung exklusiv über Süddeutsche Zeitung Content. Bitte senden Sie Ihre Nutzungsanfrage an syndication@sueddeutsche.de.