Staatstrojaner: *Wie sie funktionieren und was sie tun*

Veröffentlicht am 06.03.2018 von web.de/magazine

Von *Cornelia Meyer*

Der Weg für Staatstrojaner ist frei: Seit Anfang des Jahres sollen die Sicherheitsbehörden laut Medienberichten die Überwachungssoftware *Finspy/FinFisher* bei Verdächtigen einsetzen dürfen.

? Doch wie funktionieren die Staatstrojaner? Welchen Nutzen haben sie, und welche Risiken? Die wichtigsten Fragen und Antworten.

Die gerade diskutierten Staatstrojaner haben vor allem eine Aufgabe: Sie sollen Nachrichteninhalte von verschlüsselten Nachrichtendiensten wie WhatsApp, Signal oder Telegram abgreifen und an die Geheimdienste übermitteln. Das Späh-Programm knackt dabei nicht den Verschlüsselungscode, sondern liest die Nachrichten einfach mit.

Daneben können noch zahlreiche weitere Daten auf dem Smartphone ausgelesen werden, wie Kontakte, Fotos oder Videos. Ob die deutschen Sicherheitsbehörden die Überwachungssoftware bereits in Ermittlungsverfahren einsetzen, ist unklar.

Öffentliche Stellungnahmen des Bundeskriminalamts gibt es zu der Quellen-Telekommunikationsüberwachung (*Quellen-TKÜ*) genannten Methode nicht.

Warum wollen die Behörden Staatstrojaner einsetzen?

Das Problem für Ermittler: Kriminelle nutzen gerne Messenger-Dienste, da die hier verschickten Nachrichten meist verschlüsselt und daher für die Sicherheitsbehörden nicht zugänglich sind.

Generalbundesanwalt Peter Frank warnte vor einem Jahr, dass bereits 85 Prozent der Kommunikation von Verdächtigen nicht mehr überwacht werden könne. Staatstrojaner sollen dem abhelfen.

Wie funktionieren Staatstrojaner?

Eine der größten Herausforderungen ist, dass die Überwachungssoftware unbemerkt auf das Endgerät der Verdächtigen aufgespielt werden muss.

Auch für den IT-Sicherheitsexperten Andreas N. *(Name auf Wunsch geändert)* bleibt unklar, wie genau der Staatstrojaner auf das Handy kommt. In einem Fall in Bayern wurde das Programm vermutlich bei der Sicherheitskontrolle am Münchner Flughafen auf den Laptop des Verdächtigen eingeschleust.

- Laut N. seien aber auch die Kooperation mit Mobilfunkanbietern oder offene Drahtlosnetzwerke denkbar. Dass sich die Software durch hohen Energieverbrauch bemerkbar mache, glaubt der IT-Sicherheitsexperte nicht: *"Das*

Programm ist nur selektiv aktiv, das zehrt nicht so viel Energie. Ich glaube, ein normaler Nutzer merkt davon nichts."

→ Das *Überwachungsprogramm FinFisher* beispielsweise sei da "*gut gemacht*". Eventuell falle der Trojaner auf dem Handy aber auf, weil es sich um eine App handelt, gibt N. zu bedenken.

Haben die Staatstrojaner tatsächlich einen Nutzen?

Das Einschleusen der Software und die Auswertung der Daten bedeuten einen sehr hohen Aufwand. Daher ist der Einsatz von Staatstrojanern auf den Verdacht auf bestimmte schwere Straftaten beschränkt, wie Terrorismus, Drogenhandel oder schwere Steuerhinterziehung. Hinzu kommen die juristischen Hürden, wie das Einholen einer richterlichen Genehmigung.

- Als Normalbürger sei es unwahrscheinlich, von einem solchen Programm ausspioniert zu werden, meint IT-Sicherheitsexperte N.*: "Vor den Staatstrojanern muss man keine Angst haben."* Auch er weiß nicht, ob der Nutzen der Staatstrojaner den enormen Aufwand rechtfertigt. Die Sicherheitsbehörden geben dazu keine Informationen preis.
- N. vermutet allerdings, dass die Nachrichten von Verdächtigen ohnehin kaum gelesen würden. Oft reichten schon die Metadaten, also wann die betreffende Person mit wem kommuniziert habe. "Da sieht die Kommunikation eines Drogenhändlers schon anders aus als bei Otto Normalbürger", so N.
- Für den Normalbürger sei eher die Massenüberwachung bzw. massenhafte Speicherung von Daten als kritisch einzustufen: "Da wissen Unternehmen wie Facebook, WhatsApp oder Google oft mindestens so viel wie die Geheimdienste."

Wer entwickelt die Staatstrojaner?

Neben dem selbstentwickelten Programm RCIS verfügt das BKA auch über die kommerzielle Überwachungssoftware FinSpy, das von dem *deutsch-britischen Unternehmen FinFisher* bzw. *Gamma Group* gekauft wurde. Die Sicherheitsbehörden wollen aber künftig die Kontrolle über solche Späh-Programme im eigenen Haus behalten*. "Das BKA stellt IT-Leute ein, um solche Tools selbst entwickeln zu können. Man will sich das Wissen selbst aneignen",* sagt N.

In München wurde eigens eine komplett neue Behörde gegründet, ZITIS, die im Auftrag des Staates Verschlüsselungen knacken soll. Allerdings sei es laut N. schwierig, hochqualifiziertes Personal zu finden, da private Unternehmen in dem Bereich deutlich besser zahlen würden.

Was sind die Risiken von Staatstrojanern?

Die Voraussetzung für das Einschleusen von Staatstrojaner bleiben jedoch Sicherheitslücken - beispielsweise im Betriebssystem von Android. Doch solche Sicherheitslücken gelten nicht nur für die Smartphones von verdächtigen Kriminellen, sondern für alle entsprechenden Smartphones.

Für viele IT-Experten besteht deswegen eine Pflicht der Behörden, die Sicherheitslücken den entsprechenden Firmen zu melden, damit sie für alle geschlossen

werden können. Auch Andreas N. sieht den "Zwiespalt": *"Die Behörden brauchen die Sicherheitslücken und die Informationen, aber aus Sicht der Bürger sind sie ein sehr großes Risiko."*

Datenschützer wollen deswegen eine Verfassungsbeschwerde gegen die Staatstrojaner einlegen, dazu gehören unter anderem der Verein Digitalcourage oder der Bundesverband für IT-Sicherheit Teletrust. Letzterer befürchtet zudem Schaden für den IT-Standort Deutschland, der in der Branche großes Vertrauen genieße. IT-Sicherheitsexperte N. sieht dabei auch einen Widerspruch im Koalitionsvertrag: *"Deutschland soll einerseits der Verschlüsselungsstandort Nummer eins werden, andererseits findet sich darin auch Zustimmung zum Mitlesen von verschlüsselter Kommunikation durch Sicherheitsbehörden."*

Das Interesse an Sicherheitslücken ist bei Software-Firmen und Geheimdiensten, und auch bei Cyberkriminellen und Terroristen groß.

Es gibt sogar einen Handel mit ihnen, sowohl im Darknet als auch von normalen Firmen, die sie als Geschäftsmodell nutzen. Manche Sicherheitslücken, beispielsweise bei Apple iOS, können dabei bis zu einer Million Dollar wert sein, weiß IT-Experte N.

Die Gefahr hat auch der Fall des *Erpressungstrojaners "WannaCry"* gezeigt, der unter anderem das IT-System in britischen Krankenhäusern lahmlegte.

Der NSA war die Sicherheitslücke bei Windows bekannt, der US-Geheimdienst behielt dieses Wissen aber lange Zeit für sich.

Der Grund liegt auf der Hand: *"Sicherheitslücken sind eine potenzielle Waffe, eine Cyberwaffe",* sagt N.