2021/25 Inland

https://shop.jungle.world/artikel/2021/25/trojaner-fuer-alle

Künftig dürfen auch die Geheimdienste Staatstrojaner extensiv verwenden

Trojaner für alle

Von **Enno Park**

Eine Gesetzesänderung verschafft der Bundespolizei und allen 19 Geheimdiensten erweiterte Möglichkeiten, Smartphones und Computer zu hacken, teilweise sogar ohne dass Tatverdacht bestünde. Außerdem sollen Provider den Behörden Zugang zu den Geräten der Nutzer verschaffen.

Der Überlieferung nach bauten die Achäer ein riesiges Pferd aus Holz, um Troja zu erobern. Sie täuschten vor, die Belagerung zu beenden, und hinterließen das Pferd als vermeintliches Geschenk an die sich siegreich wähnenden Trojaner. Diese holten das Pferd in die Stadtmauern und im Pferd versteckte Krieger konnten die Stadttore von innen öffnen. Wer heute von »Trojanern« spricht, meint indes Schadsoftware: Wie die Krieger im Trojanischen Pferd verstecken sich Computerviren zum Beispiel in E-Mail-Anhängen und nach einem unbedachten Doppelklick übernehmen sie heimlich die Kontrolle über den Computer oder das Smartphone.

> Ein Staat, der darauf angewiesen ist, dass Sicherheitslücken möglichst lange bestehen, und der ständig neue braucht, arbeitet daran mit, die Software der Bevölkerung insgesamt unsicher zu halten.

Mittlerweile nutzen nicht nur kriminelle Hacker, sondern auch die Landespolizeien diese Techniken, um in die Smartphones und PCs einzudringen. Das erlaubt die Strafprozessordnung seit einigen Jahren. Allerdings gibt es unterschiedliche Regeln, was die Ermittler mit den Daten anstellen dürfen, die sie auf den Geräten finden. Bei der herkömmlichen Online-Durchsuchung sichtet die Polizei alle Daten auf strafrechtlich relevantes Material. Eine solche Durchsuchung kann von einem Landgericht angeordnet werden, wenn Verdacht besteht, dass der Beschuldigte eine besonders schwere Straftat begangen hat und eine Aufklärung auf andere Weise schwer bis unmöglich ist.

Davon abzugrenzen ist die Telekommunikationsüberwachung (TKÜ). Während es relativ einfach ist, Telefongespräche abzuhören oder Briefe zu öffnen, stellen moderne Messenger wie Whatsapp oder Signal die Ermittler vor ein Problem. Sie verschlüsseln die Nachrichten, weshalb sie nicht mehr von außen mitgelesen werden können. Deshalb kam man auf die Idee, in die Kommunikationsgeräte einzubrechen, um die Chats direkt an der Quelle mitlesen zu können, weshalb diese Art der Überwachung auch »Quellen-TKÜ« genannt wird. Eine Variante davon, bei der die Ermittler neben der gerade erfolgenden Kommunikation auch Daten älteren Datums

ansehen dürfen, wird euphemistisch »Quellen-TKÜ plus« genannt. Die Unterschiede zwischen diesen Varianten sorgen in politischen Debatten immer wieder für Verwirrung und Fehlinformationen.

Vorvergangene Woche nun hat der Bundestag mit den Stimmen der Großen Koalition das Gesetz zur Anpassung des Verfassungsschutzrechts angenommen, das die bestehenden Möglichkeiten zum Einsatz der »Quellen-TKÜ plus« nochmals ausweitet. Auch die Bundespolizei und alle 19 Geheimdienste dürfen sich ihrer bedienen, wenn sie in die Geräte ihrer Zielpersonen einzudringen. Aus rechtsstaatlicher Sicht ist das höchst problematisch, weil es anders als im Strafprozess nicht möglich ist, sich juristisch gegen eine Überwachung durch Geheimdienste zu wehren. Ähnlich schwer wiegt, dass die Bundespolizei nicht einmal einen Tatverdacht benötigt, um eine Person zu überwachen. Sie muss nur noch der Ansicht sein, es gehe um die Abwehr »einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse liegt«.

Überdies hat der Bundestag die Internet-Provider verpflichtet, der Polizei und den Geheimdiensten künftig dabei behilflich zu sein, ihren Kunden Staatstrojaner unterzujubeln. Schließlich müssen die Geräte zunächst einmal gehackt werden, um sie ausspähen zu können. Weil umsichtige Benutzer längst nicht mehr auf seltsame E-Mail-Anhänge klicken, war es bisher oft nötig, dass die Beamten sich physischen Zugriff auf zu überwachende Geräte verschaffen. Da ist es bequemer, die Provider einspannen zu können, die manchmal Zugriff auf die DSL-Router ihrer Kunden haben oder ihre als vertrauenswürdig angesehenen Websites für das Aufspielen von Schadsoftware auf die Geräte nutzen können. Das beeinträchtigt das Vertrauensverhältnis zwischen Anbieter und Kunde.

Gesellschaftlichen Schaden richten Staatstrojaner auch an, weil sie auf Sicherheitslücken in der Software der Geräte angewiesen sind. Die gibt es praktisch in jeder Anwendung, und sie auszunutzen oder zu per Update zu schließen, läuft auf ein ständiges Wettrüsten zwischen Angreifern und Herstellern hinaus. Hacker ohne kriminelle Absichten melden Sicherheitslücken üblicherweise an die Hersteller und veröffentlichen sie erst nach einer bestimmten Frist, beispielsweise drei Monaten, was den Herstellern Zeit gibt, die Lücken zu schließen. Ein Staat, der darauf angewiesen ist, dass Sicherheitslücken möglichst lange bestehen, und der ständig neue Sicherheitslücken braucht, muss die entsprechenden Kenntnisse realistischerweise auf dem Schwarzmarkt einkaufen und arbeitet so unmittelbar daran mit, die Software der Bevölkerung insgesamt unsicher zu halten. Das wiederum erleichtert kriminellen Hackern das Geschäft, die mit Hilfe dieser Sicherheitslücken beispielsweise Computer verschlüsseln und hinterher Lösegeld für die Entschlüsselung verlangen.

Die Ausweitung des Einsatzes von Staatstrojanern sorgt bei Anbietern wie Netzaktivisten für seltene Einigkeit: Unternehmerverbände wie Eco, Konzerne wie Google, *social media*-Plattformen wie Facebook, E-Mail-Provider wie Mailbox.org und Aktivistengruppen wie der Chaos Computer Club veröffentlichten vor der Abstimmung einen offenen Brief, der die Gesetzesänderungen ablehnte, allerdings ohne Auswirkungen blieb.