



2020/44 Inland

<https://jungle.world/artikel/2020/44/der-staat-hackt-mit>

Die Bundesregierung plant, Geheimdiensten den Einsatz sogenannter Staatstrojaner zu erlauben

Der Staat hackt mit

Von **Enno Park**

Die Bundesregierung will Geheimdiensten den Einsatz sogenannter Staatstrojaner erlauben, mit denen Computer und Telefone überwacht werden können. Die Telekommunikationsanbieter sollen dabei helfen, die Schadsoftware auf die Handys ihrer Kunden zu spielen.

Dem Bundesnachrichtendienst, dem Militärischen Abschirmdienst sowie den Verfassungsschutzbehörden von Bund und Ländern soll es künftig gestattet sein, die Computer und Telefone der Bevölkerung zu hacken. Das geht aus einem Gesetzentwurf hervor, den die Bundesregierung vergangene Woche beschlossen hat und in den Bundestag einbringen will. Der sogenannte Staatstrojaner soll gegen Personen eingesetzt werden, die unter Verdacht stehen, Aktivitäten nachzugehen, die eine Gefahr für die Bundesrepublik Deutschland darstellen.

Eigentlich ist die Bezeichnung »Trojaner« etwas unglücklich für Schadsoftware, mit der Angreifer Computer aus der Ferne übernehmen können. Ursprung für diese Bezeichnung ist der Mythos vom Trojanischen Pferd: Wie einst die Bewohner Trojas angeblich ihre Neugierde nicht beherrschen konnten und das große Holzpferd mit den verborgenen Kriegeren darin in die Stadt holten, so verleiten moderne Trojaner dazu, auf E-Mail-Anhänge zu klicken, sofern sie nicht gleich unerkant als sogenannter Drive-by-Download auf die Geräte gelangen. Die Schadsoftware läuft dann unbemerkt im Hintergrund, beispielsweise um Kreditkartendaten auszuspionieren oder um Daten auf dem Gerät zu verschlüsseln, die erst gegen Zahlung eines Lösegelds wieder entschlüsselt werden.

Manchmal stammen ähnliche Programme von staatlichen Stellen. Beispielsweise können diese in einigen Ländern während der Sicherheitskontrolle am Flughafen unbeobachtet aufs Gerät gespielt werden, um den Nutzer zu überwachen. Hier passt das Bild vom Trojanischen Pferd zwar nicht mehr, trotzdem hat sich der Name Staatstrojaner für derartige Software durchgesetzt.

Die Polizei darf solche Online-Durchsuchungen bereits seit 2017 durchführen. Offiziell bezeichnet wird das als »Quellen-TKÜ«, also als Telekommunikationsüberwachung direkt an der Quelle. Gegen diese Praxis sind mehrere Verfassungsbeschwerden anhängig. Beim Einsatz durch die Polizei gilt allerdings zumindest *pro forma* ein Richtervorbehalt, die Überwachung wird im Ermittlungsverfahren dokumentiert und sollte in einem Gerichtsverfahren offengelegt

werden. Beim Einsatz durch Geheimdienste ist all dies nicht der Fall: Es gibt kein offizielles Verfahren, keine Anklage, keine Offenlegung und im juristischen Sinne keinen begründeten Verdacht, der plausibel gemacht werden müsste. Lediglich das Interesse des Geheimdienstes an der zu überwachenden Person entscheidet über den Einsatz.

Bundesinnenminister Horst Seehofer (CSU) hatte sich die Quellen-TKÜ für Geheimdienste schon lange gewünscht, war aber bisher am Widerstand des Koalitionspartners SPD, vor allem durch die frühere Justizministerin Katarina Barley, gescheitert. Unter Christine Lambrecht (ebenfalls SPD) ist das Justizministerium kooperativer geworden. Ausgerechnet die SPD-Vorsitzende Saskia Esken trägt den Gesetzentwurf mit. Sie hatte sich bisher als entschiedene Gegnerin von Staatstrojanern und ähnlichen IT-Überwachungsmaßnahmen zu profilieren versucht. Ihre Meinungsänderung begründete sie damit, dass die Geheimdienste mit den Staatstrojanern auch rechtsextreme Netzwerke überwachen sollen.

Die neue Überwachungsbefugnis geht also ausgerechnet an die Behörden, die selbst regelmäßig durch Verbindungen ihrer Mitarbeiter in rechtsextreme Netzwerke auf sich aufmerksam machen. Das Ansehen, das die Informatikerin Esken bis dahin parteiübergreifend in der IT-Branche, bei Bürgerrechtsbewegungen und netzpolitischen Aktivisten genossen hatte, dürfte sie damit schlagartig verspielt haben.

Der Entwurf, dem die SPD schließlich zustimmte, war zumindest ein Kompromiss. Statt eine komplette Durchsuchung des Telefons gestattet zu bekommen, wie bei der Online-Durchsuchung durch die Polizei sollen die Geheimdienstler lediglich Chats mitlesen dürfen – beispielsweise die Kommunikation über Messenger-Dienste wie Whatsapp. An deren verschlüsselte Kommunikationsinhalte kommt man allerdings nicht heran, ohne das Endgerät zu hacken, wodurch auch der Zugriff auf andere gespeicherte Daten ermöglicht wird. Unklar bleibt, wie überprüft werden soll, ob die Geheimdienste sich an diese Spielregeln halten.

Auch für den Richtervorbehalt, der für polizeiliche Überwachung gilt, wurde eine Entsprechung in den Gesetzentwurf eingebaut. Künftig soll das parlamentarische Kontrollgremium über den Einsatz der Quellen-TKÜ entscheiden. Das Kontrollgremium besteht bisher aus neun Parlamentariern, die mehr als 12 000 Geheimdienstmitarbeiter beaufsichtigen sollen und die sich einmal monatlich treffen, ohne Auskunft über die Inhalte ihrer Sitzungen geben zu dürfen. Teil des Kompromisses mit der SPD ist die Aufstockung des Gremiums auf zehn Mitglieder. Diese müssen künftig dem Einsatz der Quellen-TKÜ zustimmen – allerdings nur dann, wenn das Innenministerium dies bei Fällen, die es selbst als eilig erachtet, nicht eigenmächtig tut.

Der Einsatz sogenannter Staatstrojaner ist aber noch in einer anderen Hinsicht problematisch: Damit die Schadsoftware auf das Telefon oder den Computer gelangt, werden Sicherheitslücken in Computern und Telefonen benötigt, die die jeweiligen Hersteller noch nicht entdeckt und geschlossen haben. Solche Sicherheitslücken, auch »Exploits« genannt, werden schwarz im Internet gehandelt und können von jedem Angreifer genutzt werden. Durch den Einsatz der Quellen-TKÜ hat der Staat ein Interesse daran, diese Sicherheitslücken vor den Herstellern geheimzuhalten, damit sie so lange wie möglich funktionieren. Der Staat vergrößert bewusst das Risiko, dass seine Bürger Opfer eines kriminellen Angriffs zu werden.

Da das Unterjubeln von Trojanern sehr aufwendig sein kann – schließlich klicken nicht alle Menschen auf E-Mail-Anhänge, laden von präparierten Webseiten herunter oder nehmen ihr Hauptgerät mit auf die Flugreise –, sieht der Gesetzentwurf vor, die

Telekommunikationsanbieter in die Pflicht zu nehmen. Sie sollen dabei helfen, ihren Kunden Schadsoftware aufzuspielen, die zum Beispiel als Sicherheitsupdate getarnt daherkommen könnte. Programmieren müssen die Ermittlungsbehörden dazu nichts mehr. Die Trojaner und die entsprechende Software können sie bei der deutschen Firma Gamma/Finfisher einkaufen. Ausgerechnet dort ließ die Münchner Staatsanwaltschaft kürzlich 15 Büros und Wohnungen durchsuchen. Der Vorwurf: Die Überwachungssoftware soll illegal an die Türkei verkauft worden sein, wo sie benutzt worden sein soll, um Journalisten und Dissidenten zu überwachen.

Mit der finnischen Firma F-Secure hat bereits der erste Anbieter von Antivirensoftware angekündigt, nach dem deutschen Staatstrojaner zu suchen und diesen gegebenenfalls zu deaktivieren.