Wer heute schon Trojaner einsetzt, verspottet unseren Rechtsstaat

12. Juli 2015

Martin Steiger, NZZ

Der polizeiliche Einsatz von Spionage-Software ist im geltenden Recht klar illegal. Daran würde auch ein neues Gesetz nichts ändern: Trojaner gehören nicht in die Hände des Staats.

Das italienische Hacking Team verkauft Überwachungssoftware in alle Welt. Kunden sind vor allem autoritäre Staaten, die damit unter Verletzung der Menschenrechte gegen Aktivisten, Journalisten und Nichtregierungsorganisationen vorgehen. Für Reporter ohne Grenzen zählt die Mailänder Firma zu den «Feinden des Internets», Menschenrechtsorganisationen kritisieren seit Jahren solche digitalen Waffen, und die Uno eröffnete sogar eine Untersuchung.

Nun wurde das Hacking Team selbst gehackt. Zahlreiche Geschäftsunterlagen gelangten an die Öffentlichkeit und entlarvten auch die Kantonspolizei Zürich als Kundin. Gekauft wurde eine umfassende Trojaner-Infrastruktur, also ein Spionageprogramm, das gegen die gängigen Computer und Smartphones eingesetzt werden kann. Dazu gehört auch der Kauf geheimer Sicherheitslücken in Software wie Microsoft Word oder dem Android-Betriebssystem.

Trojaner werden meist über solche geheimen Sicherheitslücken bei den Opfern der Überwachung eingeschleust. Möglichkeiten dafür bieten manipulierte Word-Dokumente in E-Mails, aber auch lokale Funknetze und Websites können missbraucht werden - in der Korrespondenz mit der Zürcher Polizei wird etwa Blick.ch erwähnt. Eingeschleuste Trojaner können vollständig auf das gehackte System und dessen Funktionen zugreifen. Sie können sämtliche Chats und E-Mails mitlesen, Mikrofone und Webcams unbemerkt verwenden sowie jegliche Nutzung überwachen. Dafür müssen Trojaner ein infiziertes System zwingend manipulieren, unter anderem für den Fernzugriff mittels Internet. Dateien und alle anderen Daten können spurlos gelöscht, hinzugefügt und verändert werden. Antivirus-Software wird deaktiviert, da sie den Trojaner entdecken könnte. In der Folge sind überwachte Personen und Firmen nicht mehr vor den Gefahren im digitalen Raum geschützt und riskieren, sich weitere Viren und andere schädliche Software einzufangen oder Angriffen aus dem Internet ausgesetzt zu sein.

Der Einsatz von Staatstrojanern ist rechtswidrig. Grundlage und Schranke für jedes staatliche Handeln ist das Recht, doch für Trojaner gibt es in der Schweiz keine Rechtsgrundlage. Solche Rechtsgrundlagen werden im Parlament erst noch beraten, wobei das Referendum gegen das so erweiterte Überwachungsgesetz des Bundes (Büpf) bereits beschlossen ist. Wer heute schon Trojaner einsetzt und genehmigt, verspottet unseren demokratischen Rechtsstaat.

Bestehende Gesetze zur herkömmlichen geheimen Überwachung genügen nicht als Rechtsgrundlage. Bei solchen Überwachungen werden nicht die Geräte der Überwachten manipuliert, sondern Telefongespräche und andere Daten unverändert erhoben. Ein Trojaner dringt dagegen tief in die digitale Intimsphäre ein, und Grundrechte wie der Schutz der Privatsphäre oder die Meinungsfreiheit werden stark eingeschränkt. Die Bundesverfassung

verlangt dafür eine direkte gesetzliche Grundlage. Staatsanwaltschaften und Zwangsmassnahmengerichte scheinen sich im Dunkel der Geheimhaltung um dieses Legalitätsprinzip zu foutieren.

Trojaner sollten in einem Rechtsstaat aber auch mit einer angepassten Rechtsgrundlage nicht eingesetzt werden dürfen. Beweise, die so erhoben werden, sind nicht gerichtsfest und stammen faktisch aus dem rechtsfreien Raum. Manipulationen und Missbrauch jeder Art sind mit Trojanern immer möglich, auch durch die Überwachten selbst oder durch unbefugte Dritte. Trojaner sind nicht zuverlässig kontrollierbar, und die Sicherheitsbehörden sind von fragwürdigen Anbietern abhängig. Das Hacking Team ergänzte seinen Trojaner - durchaus branchenüblich - mit einer nur dürftig verschlossenen Hintertüre für den eigenen Zugriff und erwähnt sogar das mögliche Hochladen (!) von Kinderpornografie zum Überwachten. Eine gerichtliche Beschränkung auf die blosse Überwachung der Kommunikation ist technisch gesehen nicht möglich. In der Praxis gibt es auch keine Trennung zwischen dem alleinigen Überwachen der Telekommunikation und dem Überwachen der zu schützenden digitalen Intimsphäre als Kerngehalt der Privatsphäre.

Die grundlegenden Mängel beim staatlichen Einsatz von Trojanern können weder mit der Schaffung einer Rechtsgrundlage noch mit technischen Mitteln behoben werden. Gleichzeitig gefährden Sicherheitsbehörden die Sicherheit aller, indem sie geheime Sicherheitslücken für die eigene Verwendung kaufen, anstatt sie so bald wie möglich beheben zu lassen. Staatstrojaner taugen nicht zur rechtsstaatlichen und verhältnismässigen Überwachung. Will die Polizei Gespräche bei Skype überwachen, kann sie dies schon heute rechtshilfeweise über dessen Sitz in Luxemburg tun. Staatstrojaner müssen verboten werden, um die Grundrechte im digitalen Raum zu schützen - in der Schweiz und im Ausland im Einklang mit Europas Menschenrechtskonvention.