Humanistische Union

Der Staatstrojaner außer Kontrolle - Überwachungstechnik am Abgrund. Und darüber hinaus.

Grundrechte-Report 2012, Seite 32

Da hatte sich das Bundesverfassungsgericht so viel Mühe gegeben: In dem furiosen Urteil vom 27. Februar 2008 zur so genannten Online-Durchsuchung beschrieb das höchste deutsche Gericht ausführlich die Grenzen, welche die Grundrechte dem heimlichen Ausspähen von privaten Computern setzen. Diese Grenzen müssen anspruchsvoll sein, denn in seinem Computer speichert der Mensch von heute, ob er es will oder nicht, fast alles Wissenswerte über sein Leben. Weil kaum ein Datenbestand so aussagefähig über den Einzelnen und seine Überwachung zugleich so gefährlich für seine Freiheit und Privatsphäre ist, entwickelte das Bundesverfassungsgericht sogar eine neue Art von Grundrecht, das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (vgl. Erhard Denninger, Grundrechte-Report 2009, S. 20 ff.). Dagegen stand das nicht enden wollende Drängen der Sicherheitsbehörden, dass man auf den Zugriff auf private Computer zwecks Überwachung verschlüsselter E-Mails, Internet-Telefonie und sonstiger Internet-Kommunikation (so genannte Quellen-Telekommunikationsüberwachung) unter keinen Umständen verzichten könnte. Wenn man in Zukunft noch schwerste Straftaten bekämpfen wolle, müssten die Behörden mit der technischen Entwicklung mithalten können. Die Behörden versprachen, dass die Vertraulichkeit und Integrität privater Computer bei solchen Zugriffen geschützt werden könnten und nur das Fernmeldegeheimnis nach Artikel 10 Absatz 1 des Grundgesetzes von dieser Art der Telekommunikationsüberwachung betroffen sein würde. Dem kam das Gericht entgegen: Quellen-Telekommunikationsüberwachungen seien zulässig, wenn technisch sichergestellt werden könnte, dass nichts anderes als die zu überwachende Kommunikation den Behörden bekannt werden kann und der Computer des Betroffenen nicht auch sonst ausgespäht oder manipuliert wird. Die ausführlichen Worte des Bundesverfassungsgerichts zu den technischen und verfahrensrechtlichen Absicherungen, welche die Privatsphäre vor dem hoch brisanten Zugriff auf private Computer schützen müssen, gehören zu den tiefgründigsten Stellungnahmen, die wohl je ein deutsches Gericht zu technischen Detailfragen abgegeben hat. Wer sie liest, fühlt sich unweigerlich an die juristischen Formeln erinnert, mit denen die Risiken der Atomkraft beherrscht werden sollen.

Recht ist Theorie, Technik ist Praxis

Mit solchen verfassungsgerichtlichen Ratschlägen bestens präpariert, machten sich die Gesetzgeber in Bund und Ländern an die Arbeit, Online-Durchsuchung und Quellen-Telekommunikationsüberwachung mittels Schnüffelsoftware (so genannte Trojaner) zu regeln. Dabei kamen umfangreiche und bis heute umstrittene Regelungen zustande, beispielsweise im Bundeskriminalamt-Gesetz. Für strafrechtliche Ermittlungen aber meinte man, es bei den bestehenden §§ 100a, 100b der Strafprozessordnung belassen zu können. Nach den klaren Worten des Bundesverfassungsgerichts aber erwarteten die Bürgerinnen und Bürger trotzdem, dass die Sicherheitsbehörden in Bund und Ländern nur mit höchster Sensibilität vorgehen und nur zu einer bestmöglich ausgereiften Trojaner-Technik greifen würden. Weit gefehlt: Im Oktober 2011 veröffentlichten Aktivistinnen und Aktivisten des Chaos Computer Club (CCC) die Ergebnisse ihrer Untersuchung mehrerer, auf infizierten privaten Festplatten gefundener Trojaner der Sicherheitsbehörden. Die technische Analyse der Computerexperten ergab, dass die überwachte Kommunikation unverschlüsselt über Server in den Vereinigten Staaten von Amerika an deutsche Behörden weitergeleitet werden sollte, die Steuerung der

Trojaner bereits mit verhältnismäßig simplen Softwarewerkzeugen möglich und nicht durch wirksamen Passwort-Schutz abgesichert war und die eingesetzten Schnüffelprogramme um Funktionen erweitert werden konnten, welche die Totalüberwachung und Manipulation der infizierten Computer erlaubt hätten. Nicht nötig zu erwähnen, dass es bei keinem der betroffenen Ermittlungsverfahren um Terrorismus oder schwerste Straftaten ging, sondern um Steuer- und sonstige Vermögensdelikte.

Damit war Schluss mit der Legende von der verfassungsverträglichen Quellen–Telekommunikationsüberwachung. Der Chaos Computer Club forderte jetzt die Offenlegung aller Trojaner und den Verzicht auf ihren Einsatz. Als ersten Schritt dahin, dass es nicht bei einer bloßen Forderung bleibt, veröffentlichte der Club gleich auch den Code der gefundenen Trojaner. Die können jetzt leichter entdeckt und unschädlich gemacht werden. Das ist schlecht für die polizeilichen Ermittlungen, aber es verschwinden zumindest einige Versionen der gefährlichen Software einstweilen vom Markt. Die Suche nach weiteren Trojanern ist noch nicht zu Ende.

Für die Öffentlichkeit, die sich nach behördlichen Beteuerungen über sichere Überwachungstechnik und ihren sensiblen Einsatz in Sicherheit wog, war die Entdeckung dieser schwer mangelhaften Trojaner ein harter Aufschlag in der Realität. Für manche Polizeibehörden und Innenminister allerdings auch. Während Bundes- und Landesregierungen noch sich und den Bürgerinnen und Bürgern versicherten, dass man die entdeckte gefährliche Software entweder gar nicht einsetzen würde oder man auf keinen Fall die verfassungsgerichtlich verbotenen Funktionen hätte nutzen wollen und inzwischen ja auch über viel bessere Technik verfügte, legte der Club mit neuesten Trojaner-Versionen nach, welche immer noch erhebliche Sicherheitslücken aufwiesen.

Ist das Recht noch zu retten?

Angesichts der erdrückenden Beweislage fragt sich die beunruhigte Öffentlichkeit: bewusste Fahrlässigkeit oder frecher Rechtsnihilismus? Was nützen jahrelange Verfassungsgerichtsverfahren, ausführliche Urteile, Berge von Sachverständigengutachten und lange Parlamentsdebatten, wenn die Polizei trotzdem mit unausgereifter Technik genau die Gefahren produziert, die sie in den Griff hätte bekommen sollen, bevor sie überhaupt über den Einsatz der umstrittenen Methode nachdenkt? Dachte da überhaupt jemand kritisch nach? Konnte man die Beteuerungen der Trojaner-Hersteller nicht überprüfen? Oder war der Erfolgsdruck so stark, dass jedes Mittel recht sein sollte?

Diese Realität zeigt einmal mehr: heimliche Ermittlungen und der staatliche Einsatz von Überwachungstechnik bleiben für die Bürgerinnen und Bürger ebenso wie für das Bundesverfassungsgericht reine Vertrauenssache. Wenn Behörden eine heimliche Überwachungsmaßnahme nicht nach den rechtlichen Vorgaben umsetzen und die Politik diese Entwicklung nicht beherrschen kann, kommt das Recht immer zu spät. Der zufällig entdeckte Staatstrojaner droht so zu einem trojanischen Pferd im Grundrechtsschutz zu werden, und dieser Gaul trampelte auch schon munter auf dem Telekommunikationsgeheimnis und auf der Integrität und Vertraulichkeit privater Computer herum. Seit der grundlegenden Entscheidung des Bundesverfassungsgerichts waren da erst dreieinhalb Jahre vergangen. Zeit, dieser Technik den Stecker zu ziehen.

---

https://www.humanistische-union.de/publikationen/grundrechte-report/2012/publikation/der-staatstrojaner-ausser-kontrolle-ueberwachungstechnik-am-abgrund-und-darueber-hinaus/
Abgerufen am: 06.11.2026