KIF – Konferenz der Informatik-Fachschaften

Resolution „Cyberpeace“

Die 44,0. Konferenz der deutschsprachigen Informatikfachschaften schließt sich den Forderungen des FIfF e. V.[1] an und fordert:

- dass Deutschland auf eine offensive Cyberstrategie verzichtet,
- dass sich Deutschland verpflichtet, keine Cyberwaffen zu entwickeln, zu beschaffen und zu verwenden,
- dass internationale Abkommen zu einem weltweiten Bann von Cyberwaffen angestrebt werden.

Wir verstehen unter einer digitalen Waffe (auch „Cyberwaffe“) eine Software, Hardware oder Methode, die dazu bestimmt ist, IT-Systeme zu stören, zu beschädigen, für fremde Absichten zu missbrauchen oder in ihrer Integrität zu beeinträchtigen. Die Herstellung einer digitalen Waffe, also eines Werkzeuges zum Ausnutzen einer Sicherheitslücke eines IT-Systems, zeichnet sich durch die Geheimhaltung und den Erhalt derselben aus.

Ein Bann schlösse die Entwicklung, Herstellung und Verwendung sowie den Besitz von Cyberwaffen ein.

1 *Cyberpeace-Kampagne des FIfF e. V., http://cyberpeace.fiff.de/Kampagne/Appell*

FIfF e. V., Chaos Computer Club e. V. – Pressemitteilung

Urteil zum BKA-Gesetz: Die Grenzen des Staatstrojaners

20. April 2016 – *Nach mehrjähriger Verzögerung nahm das Bundesverfassungsgericht (BVerfG) heute das BKA-Gesetz (BKAG) aus dem Jahr 2008 auseinander und erklärte es in Teilen für verfassungswidrig. Abermals wurde damit eines der vielen Überwachungsgesetze der vergangenen Legislaturperioden eingefangen. Gemeinsame Erklärung des Chaos Computer Clubs (CCC e. V.) und des Forum Informatiker.innen für Frieden und gesellschaftliche Verantwortung (FIfF e. V.).*

Dem Bundeskriminalamt sollten weitreichende Überwachungs- und Datenweitergabemöglichkeiten an die Hand gegeben werden. Konkret wurden die Wohnraumüberwachung, die *heimliche Online-Durchsuchung* (Staatstrojaner), die sogenannte *Quellen-Telekomunikationsüberwachung* (Quellen-TKÜ, auch Staatstrojaner) und die Datenübermittlung an andere Behörden im In- und Ausland geregelt.

Die künstliche *Trennung* zwischen Staatstrojanern, die einerseits auf die gesamte Festplatte zugreifen dürfen, und Staatstrojanern, die andererseits nur Kommunikation ausspionieren dürfen, bleibt mit dem Urteil bestehen. Das Gericht unterscheidet abermals zwischen Quellen-TKÜ und heimlicher Online-Durchsuchung; diesmal sogar noch schärfer als im Urteil von 2008. Nun sind Maßnahmen, die Telekommunikationsvorgänge abfangen sollen, nur noch nach Artikel 10 GG (Telekommunikationsgeheimnis) abzuwägen. Zwar forderte das Gericht begrüßenswerterweise weitreichende Protokoll-, Transparenz-, Benachrichtigungs- und Prüfpflichten, am grundlegenden technischen Missverständnis ändert das jedoch wenig: Ein Trojaner, der ausschließlich Kommunikation erfassen kann, *ist technisch illusorisch.*

Der Sprecher des Chaos Computer Clubs (CCC), Dirk Engling, kommentiert: *„Das Gericht geht offenbar davon aus, dass sich das heimliche Einbrechen des Staats in unsere digitalen Begleiter nachträglich beschränken lässt. Dass das Gericht dabei der Ansicht folgt, es gäbe eine Quellen-TKÜ, die fundamental verschieden von anderen Staatstrojanern sei, lässt den eigentlichen Eingriff durch die Infiltration außer acht.“*

Insgesamt betonten die Richterinnen und Richter jedoch die persönlichkeitsbezogene Brisanz der Daten, die regelmäßig durch heimliche Online-Durchsuchung, Wohnraumüberwachung oder Quellen-TKÜ gewonnen werden. Weil die so erlangten Daten oft dem *Kernbereich privater Lebensgestaltung* zuzurechnen sind, werden für den Einsatz nun neue Hürden gefordert: Abbruch bei kernbereichsrelevanten Inhalten, Richtervorbehalt, unabhängige Nachprüfung der Informationen und belastbare, konkrete Anhaltspunkte für bevorstehende Straftaten oder für die Verfolgung schwerer Kriminalität.

Es ist beachtenswert, dass diese Schranken nicht von Anfang an im BKAG zu finden waren. Dies wirft ein Schlaglicht auf die *politische Nachlässigkeit beim Schutz der Grundrechte* von denjenigen Mitgliedern des Bundestages, die das Gesetz bei der Abstimmung im Jahre 2008 mittrugen.

Im Urteil ist zwar vom „absolut geschützten Kernbereich privater Lebensgestaltung“ die Rede, aber das „absolut“ ist inhaltlich ausgehöhlt. Man könne diesen absoluten Schutz, der sich aus der Menschenwürde ableitet, beim Einsatz von Trojanern *technisch nicht garantieren*, die technische Methode an sich, mit der nicht sicher ausgeschlossen werden kann, dass Höchstpersönliches abgriffen wird, mochten die Richter aber nicht grundsätzlich überdenken.

Problematisch ist das Urteil auch in ganz anderer Hinsicht. Im Urteil herrscht eine Vorstellung von informationstechnischen Systemen, die sich auf konkrete technische Geräte, soziale Netzwerke, E-Mailprovider bis hin zur „Cloud“ bezieht. Doch anzugreifende Systeme mit IP-Adresse sind auch heute schon nicht mehr nur Laptops oder Mobiltelefone: *„Das können Autos, Kraftwerke, Notrufsäulen oder Herzschrittmacher sein. Somit könnte also nicht nur Höchstpersönliches abgegriffen werden, sondern tatsächlich Gefahr für Leib und Leben verursacht werden, wenn solche Systeme infiltriert werden. Die im Urteil attestierte ‚geringe Streubreite‘ der Staatstrojaner muss nicht immer gegeben sein“*, kommentiert

Rainer Rehak, Vorstandsmitglied des Forum Informatiker.innen für Frieden und gesellschaftliche Verantwortung (FIfF).

Im Urteil wurde mehrfach auf additive Effekte der Überwachung und die *„Gesamtüberwachungsrechnung"* abgestellt. Diese sieht vor, dass nicht nur die Einzelmaßnahme abgewogen werden darf, sondern dass immer auch der Gesamtkontext aller Überwachungsmaßnahmen betrachtet werden muß. In der Tat müssen wir dabei auch die neuen geplanten Überwachungsmaßnahmen der EU mit einbeziehen.

Referenzen

Das Urteil: http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html

CCC-Meldung von 2015: https://www.ccc.de/de/updates/2015/bkag

FIfF-Meldung: http://www.fiff.de/urteil-zum-bka-gesetz-die-grenzen-des-staatstrojaners

Patrick Breyer, MdL – Pressemitteilung

EU-Generalanwalt gegen deutsches Verbot der Protokollierung des Surfverhaltens im Internet

12. Mai 2016 – Der Bundestag darf Anbietern von Internetportalen nicht verbieten, flächendeckend auf Vorrat zu speichern, wer was im Internet liest, schreibt oder sucht. Die Entscheidung darüber obliege nach EU-Recht vielmehr den Gerichten, die eine Abwägung vorzunehmen hätten. Diese Meinung verkündete der Generalanwalt am Europäischen Gerichtshof (EuGH) heute bezüglich der Klage des Piratenpolitikers und Datenschützers Patrick Breyer gegen die Bundesregierung (Az. C-582/14).

Breyer: „Das ist ein Angriff auf das deutsche Datenschutzrecht und die digitalen Grundrechte. Die EU droht das klare deutsche Verbot einer Protokollierung unseres Surfverhaltens im Telemediengesetz auszuhebeln und die Verantwortung auf Einzelfallentscheidungen der Gerichte abzuschieben. Ich fordere die EU-Kommission auf, unverzüglich ein eindeutiges Verbot der anlasslosen Protokollierung unseres Surfverhaltens vorzulegen! Europa muss der NSA-Methode einer Totalerfassung des digitalen Lebens eine klare Absage erteilen und den Grundrechten auf Informations- und Meinungsfreiheit im Internet zur Geltung verhelfen."

Ob eine Speicherung von IP-Adressen durch Webseitenbetreiber zulässig ist, lässt der Generalanwalt offen. Zwar sei das Ziel, die Funktionsfähigkeit des Telemediums zu gewährleisten, grundsätzlich legitim. Deswegen anlasslos IP-Adressen zu speichern, sei aber nur gerechtfertigt, wenn dem Interesse des Anbieters „Vorrang gegenüber dem Interesse oder den Grundrechten der betroffenen Person zuerkannt worden ist" (Abs. 106). Zu der Art und Weise, wie diese Interessenabwägung ausfällt, ist nach Ansicht des Generalanwalts „nichts weiter zu sagen", weil der Bundesgerichtshof hierzu keine Frage vorgelegt habe (Abs. 103).

Breyer: „Die Entscheidung über diese Abwägung werden damit die deutschen Gerichte zu treffen haben. Das Bundesverfassungsgericht hat in seinem Urteil zur Vorratsdatenspeicherung großen Wert darauf gelegt, dass nach dem Telemediengesetz die Internetnutzung nicht inhaltlich festgehalten und damit rekonstruierbar bleiben darf. Ein Gerichtsgutachten belegt, dass ein sicherer Betrieb von Internetportalen (Webservern) bei entsprechender Systemgestaltung auch ohne Vorratsspeicherung von IP-Adressen möglich ist.

Ich hoffe, der Gerichtshof wird anders entscheiden als der Generalanwalt und die unterschiedslose Erfassung des Inhalts unserer Internetnutzung als von vornherein völlig unverhältnismäßiges Mittel verwerfen. Sollte sich der Gerichtshof aber dem Generalanwalt anschließen und die Abwägung den deutschen Gerichten überlassen, werde ich gegen die Surfprotokollierung notfalls bis zum Bundesverfassungsgericht ziehen.

Nur wenn Regierung und Internetkonzernen die Aufzeichnung unseres Surfverhaltens verboten wird, sind wir vor Ausspähung unseres Privatlebens, fälschlichen Abmahnungen und falschem Verdacht der Strafverfolger sicher. IP-Adressen haben sich als extrem fehleranfälliges und unzuverlässiges Mittel zur Personenidentifizierung erwiesen. Und solange wir uns schon wegen des Lesens von Internetseiten verdächtig machen können, gibt es keine echte Informations- und Meinungsfreiheit im Internet. Niemand hat das Recht, alles, was wir im Netz sagen, und alles, was wir tun, aufzuzeichnen. Als Generation Internet haben wir das Recht, uns im Netz ebenso unbeobachtet und unbefangen informieren zu können, wie es unsere Eltern aus Zeitung, Radio oder Büchern konnten."

Laut Generalanwalt unterliegen die beim Surfen übermittelten Kennungen der Internetnutzer (IP-Adressen) dem Datenschutz, solange der Internetprovider sie zuordnen kann. Nach dem umstrittenen Gesetz zur Vorratsdatenspeicherung soll dies künftig zehn Wochen lang der Fall sein. Die Bundesregierung hatte den Personenbezug von IP-Adressen bestritten.

Mit dem Urteil kann im Sommer gerechnet werden.

Referenzen

Die Schlussanträge des Generalanwalts: http://www.daten-speicherung.de/wp-content/uploads/Surfprotokollierung_2016-05-12_Generalanwalt.pdf

Ausführliche Informationen und die Gerichtsdokumente im Wortlaut: http://www.daten-speicherung.de/index.php/prozessdokumentation-meine-klage-gegen-die-vorratsspeicherung-unserer-internetnutzung/

Gerichtsgutachten zur Notwendigkeit einer Speicherung von IP-Adressen: http://www.daten-speicherung.de/wp-content/uploads/Surfprotokollierung_2011-07-29_Sachverst_an_LG.pdf

Untersuchung: Ministerien erfassen illegal unser Surfverhalten: http://www.daten-speicherung.de/index.php/untersuchung-ministerien-erfassen-illegal-unser-surfverhalten/

Aufsatz über den „Personenbezug von IP-Adressen": http://www.daten-speicherung.de/wp-content/uploads/Breyer-Personenbezug-IP-Adressen.pdf

Web Tracking Report 2014 des Fraunhofer-Instituts für Sichere Informationstechnologie: https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Web_Tracking_Report_2014.pdf