Beschlagnahme des AN.ON-Servers des ULD durch die Staatsanwaltschaft Konstanz

Beschwerde vom 15.09.2006 nach den §§ 304, 306 StPO gegen den Beschluss des Amtsgerichts Konstanz vom 23. August 2006, Az.: 10 Gs 669/06

Gegen den o.g. Beschluss des Amtsgerichts Konstanz lege ich als Leiter des Unabhängigen Landeszentrums für Datenschutz in Schleswig-Holstein nach §§ 304, 306 StPO Beschwerde ein und beantrage, die Rechtswidrigkeit des Beschlusses festzustellen.

Das ULD ist Kunde einer Firma in Karlsruhe und hat dort einen dezidierten Server angemietet. Auf diesem Server betreibt das ULD einen Anonymisierungsdienst, einen sog. Mix-Rechner. Der von uns angemietete Server wird unter einer bestimmten IP-Adresse betrieben.

Am 23. August 2006 hat das Amtsgericht Konstanz aufgrund eines strafrechtlichen Ermittlungsverfahrens gegen Unbekannt die Durchsuchung der Geschäftsräume des Dienstleisters und die Beschlagnahme des von uns betriebenen Servers angeordnet. Die Beschlagnahme wird damit begründet, dass der Beschuldigte zur Verschleierung der Identität Ladevorgänge „über einen sog. Bouncer“ vorgenommen habe, welcher die entsprechende IP-Adresse habe und bei dem entsprechenden Provider stehe.

Der Beschluss zur Beschlagnahme des Servers ist dem ULD erst auf Nachfrage und Anforderung am 13. September 2006 per Fax übermittelt worden. Der Ausfall des Servers wurde zuerst am 6. September 2006 abends von einem Mitarbeiter festgestellt und als Systemausfall bewertet. Der Provider selbst hat erst am 11. September 2006 auf die Staatsanwaltschaft Konstanz verwiesen, von der fernmündlich die Beschlagnahme eines Servers mit der entsprechenden IP-Adresse bestätigt wurde. Auf die dem zuständigen OStA per Fax am 11. September 2006 übermittelte Bitte hat das Landeskriminalamt Baden-Württemberg am 12. September zunächst einen Beschluss übermittelt, der sich auf einen anderen Server bezog. Erst am 13. September 2006 hat das ULD den seinen Server betreffenden Beschlagnahmebeschluss erhalten.

Der Server ist Teil eines gemeinsamen Forschungsprojektes der TU Dresden, Fakultät für Informatik, der Universität Regensburg sowie des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD). Ziel des vom Bundesministerium für Wirtschaft und Arbeit geförderten Projektes ist es, anonyme und unbeobachtbare Webzugriffe zu realisieren (http://anon-online.de/). Mit Hilfe des Projektes sollen die Umsetzung der Vorschriften des deutschen Teledienstedatenschutzgesetzes (TDDSG) gefördert werden. Diese verlangen, dass Diensteanbieter den Nutzern die anonyme oder pseudonyme Nutzung ermöglichen, soweit dies technisch möglich und zumutbar ist (§ 4 Abs. 6 TDDSG).

Die Beschlagnahme des o.g. Servers hat das Angebot des über den Server laufenden Anonymisierungsdienstes unterbunden. Als Betreiber des Servers ist das ULD somit auch belastet und beschwerdebefugt. An der Feststellung der Rechtswidrigkeit hat das ULD als Betreiber ein rechtlich geschütztes Interesse, um zu verhindern, dass durch weitere Maßnahmen die Funktionsfähigkeit des Dienstes und damit die Erfüllung des gesetzlich geforderten Angebotes an Anonymisierungsdiensten beeinträchtigt wird.

Die Beschlagnahme ist rechtswidrig, weil sie uns als dem Betreiber des Servers nicht bekannt gemacht worden ist. Der Provider ist zwar Eigentümer der Hard- und Software des Servers und als solcher auch Adressat, aber das ULD ist als Mieter des Servers Betreiber und durch die Beschlagnahme unmittelbar betroffen, weil uns die Beteiligung an dem Anonymisierungsdienst insoweit nicht mehr möglich ist.

Die Beschlagnahme hätte uns nach § 35 Abs. 2 StPO unverzüglich mit oder nach der Beschlagnahme mitgeteilt werden müssen. Die Adresse des ULD ist bei dem Provider hinterlegt. Eine Behinderung der Ermittlungen wäre mit der Information des ULD nicht zu erwarten gewesen, weil wir als Betreiber des Anonymisierungsdienstes selbst über keine Daten über Nutzer verfügen.

Der Beschlagnahme des Servers ist rechtswidrig, weil sie eine unzulässige Umgehung der Regelungen der §§ 100g, 100h StPO darstellt. Die Beschlagnahme wird damit begründet, dass ein unbekannter Beschuldigter seine Identität mit Hilfe des Servers verschleiert haben soll. Soll die Beschlagnahme dazu dienen, die Identität des Beschuldigten aufzudecken, dann ist dies nur über eine Auswertung von Logdateien möglich – soweit sie zur Verfügung stehen. Logdateien sind telekommunikationsrechtlich Verkehrsdaten, für deren Beauskunftung der Gesetzgeber mit den §§ 100g, 100h StPO eine spezielle Rechtsgrundlage geschaffen hat, die dem Schutzbedürfnis des in Art. 10 Abs. 1 GG geschützten Fernmeldegeheimnisses Rechnung tragen. Diese Regelungen verdrängen die Möglichkeit, im Wege der Beschlagnahme Verkehrsdaten zu Informationszwecken zu erlangen, wie bereits das Landgericht Frankfurt in einer ebenfalls unseren Anonymisierungsserver betreffenden Entscheidung rechtskräftig festgestellt hat.

Landgericht Frankfurt am Main, Beschluss vom 21. Oktober 2003, Az.: 5/8
Qs. 26/03, DuD 2003, 778 = http://www.jurpc.de/rechtspr/20030326.pdf

Die Beschlagnahme ist ungeeignet und damit unverhältnismäßig, weil sich auf dem Server keine Logdateien befinden, die Rückschlüsse auf die Nutzer des Anonymisierungsdienstes zulassen. Der Anonymisierungsdienst ist so aufgebaut, dass über eine Kette von Rechnern (sog. Mixe) die Internetzugriffe verschlüsselt und technisch verborgen werden. Eine solche Kette von Rechnern wird auch als Kaskade bezeichnet. Der Weg über eine solche Kaskade ist fest eingestellt. Der erste Mix-Rechner in der Kaskade wird vom Nutzer über das auf seinem Rechner installierte Programm „JAP“ angesprochen. Die Software „JAP“ wird zwischen den Browser des Nutzers und das Internet geschaltet. Der erste Mix-Rechner leitet die Anfragen dann durch die Kaskade. Auch der Endpunkt der Kaskade ist festgelegt. An diesem letzten Mix-Rechner wird die Anfrage an den mittels eines Proxy-Servers aufgerufenen Webservers weitergeleitet. Die Antworten der angefragten Server im WWW gehen den umgekehrten Weg, d.h. zuerst zum Proxy, dann zum letzten Mix-Rechner, von dem aus sie über die anderen Mixe der Kaskade zum Nutzer gesendet werden. Da viele Nutzer gleichzeitig die Zwischenstationen des Anonymisierungsdienstes nutzen, werden die Internetverbindungen jedes Nutzers unter denen aller anderen Nutzer versteckt: Der Dienst ist so konfiguriert, dass kein Außenstehender, kein anderer Nutzer und auch nicht die Betreiber des Anonymisierungsdienstes herausbekommen können, welche Verbindungen zu einem bestimmten Nutzer gehören. Für die Einzelheiten verweisen wir auf die öffentlich und damit auch den Ermittlungsbehörden verfügbaren technischen Informationen über den Dienst unter

http://anon.inf.tu-dresden.de/desc/desc_anon.html.

Die Beschlagnahme ist auch mit Rücksicht auf die öffentlich verfügbaren Informationen über die Funktionsweise des Dienstes unverhältnismäßig. Als milderes Mittel hätte sich die Information und ggf. eine Nachfrage über die technischen Funktionen des Dienstes angeboten. Im Übrigen wird darauf verwiesen, dass die für den Betrieb einschlägigen Dokumente und Programme als Open Source öffentlich zugänglich sind, so dass auch aus diesem Grund eine Beschlagnahme nicht erforderlich ist.

Angesichts des Umstandes, dass auf dem Server keine Logdateien gespeichert sind, über die Nutzer identifiziert werden könnten, ist die formelhafte Begründung des Beschlagnahmebeschlusses, die angeordneten Maßnahmen seien „zur weiteren Aufklärung des Sachverhaltes notwendig und

angemessen“ tatsächlich nicht zutreffend. Die Begründung lässt eine eigenverantwortliche und verfassungsrechtlich geforderte Prüfung der Ermittlungen seitens des Amtsgerichts vermissen. Es drängt sich der Verdacht auf, dass in der Begründung lediglich die Antragsbegründung der Staatsanwaltschaft wiederholt wird.

Vgl. BVerfGE 96, 44, 51 – ständige Rechtsprechung.

Die Beschlagnahme des gesamten Servers ist auch deswegen unverhältnismäßig, weil die Beschlagnahme des Servers alle an der Nutzung des Dienstes Interessierten in ihren Kommunikationsmöglichkeiten beschränkt, statt nur den unbekannten Beschuldigten. Die Beschlagnahme hat damit in ihrer Wirkung eine erhebliche Streubreite. Das Bundesverfassungsgericht hat zuletzt in einem Beschluss

vom 12. April 2005, Az.: 2 BvR 1027/02

darauf verwiesen, dass die Beschlagnahme eines kompletten Datenträgers eingriffsintensiv ist und daher im Einzelfall in besonderer Weise einer regulierenden Beschränkung bedarf. So muss die Beschlagnahme zur Ermittlung und Verfolgung der Straftat insbesondere erforderlich sein. Dies ist nicht der Fall, wenn andere, weniger einschneidende Mittel zur Verfügung stehen.

Ein milderes Mittel wäre nicht nur die Beteiligung des Betreibers selbst gewesen, sondern auch die Nachfrage, welche Möglichkeiten zur Identitätsfeststellung bei dem Anonymisierungsdienst AN.ON bestehen. Staatsanwaltschaft und Gericht hätten auf diese Weise in Erfahrung bringen können, dass in AN.ON im Unterschied zu anderen Anonymisierungsdiensten eine Überwachungsschnittstelle aktiviert werden kann, um über eine Überwachungsanordnung nach §§ 100a, 100b StPO eine Aufzeichnung der Verkehrsdaten durchzuführen. Eine solche Überwachungsanordnung ist zur Identifizierung des unbekannten Beschuldigten nicht nur ein milderes Mittel als eine Beschlagnahme, sondern gegenüber der im Ergebnis nutzlosen Beschlagnahme auch Erfolg versprechender.

Mit Einlegung der Beschwerde wird gleichzeitig die Aussetzung der Vollziehung des genannten Beschlusses und die Rückgabe der beschlagnahmten Gegenstände gemäß § 307 Abs. 2 StPO beantragt.

Dr. Thilo Weichert
(Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein)