Bericht zum Vorgehen von Strafverfolgungsbehörden gegen das Projekt „AN.ON — Anonymität.Online“

Helmut Bäumler, Hannes Federrath, Claudia Golembiewski

September 2003

1 Kontaktaufnahme seitens der Strafverfolgungsbehörden

Am 23. Juni 2003 richtete das Hessische Landeskriminalamt per Telefax zwei Anfragen an die Technische Universität Dresden, mit denen in einem Ermittlungsverfahren im Zusammenhang mit dem Besitz kinderpornographischer Schriften um Herausgabe der einem bestimmten Nutzer, der den Anonymisierungsdienst offenbar *in der Vergangenheit* genutzt hatte, zu einer bestimmten Zeit zugeordneten IP-Adresse gebeten wurde. Dem Hessischen LKA wurde – wie in allen bisherigen Fällen üblich – vom Unabhängigen Landeszentrum für Datenschutz (ULD) schriftlich mitgeteilt, dass keine Daten über Nutzer erhoben und gespeichert werden und daher eine Auskunftserteilung nicht möglich ist.

Ein Beamter des Hessischen LKA wandte sich am 27. Juni 2003, noch bevor ihm das Schreiben des ULD zugegangen war, telefonisch an einen Projektmitarbeiter der TU Dresden und erkundigte sich, ob eine Überwachung und damit Identifizierung eines Nutzers *für die Zukunft* möglich wäre und ob dieses auch kurzfristig ermöglicht werden könne.

Ziel der Überwachung sollte die Rückverfolgung des Aufrufs einer bestimmten URL sein, mit der feststellbar ist, von welcher IP-Adresse der Aufruf stammt. Der Projektmitarbeiter bestätigte, dass eine derartige Überwachung technisch möglich gemacht werden könnte, es allerdings eines entsprechenden richterlichen Beschlusses bedürfte. Der Polizeibeamte schien kein Problem darin zu sehen, zeitnah einen derartigen Beschluss erwirken zu können und kündigte an, dass ein Beschluss alsbald erlassen würde. Der Polizeibeamte wurde hinsichtlich weiterer Kontaktaufnahmen an das ULD verwiesen.

Im Zuge dieser Anfrage wurde von den Projektpartnern intern diskutiert, wie und auf welcher gesetzlichen Grundlage eine solche Rückverfolgung im Einzelfall realisiert werden soll. Das Ergebnis dieser Überlegungen war, dass in Einzelfällen bei Vorliegen aller rechtlichen Voraussetzungen, d. h. eines rechtmäßigen richterlichen Beschlusses gemäß §§ 100a, b Strafprozessordnung (StPO), mit den Strafverfolgungsbehörden im Rahmen der technischen Möglichkeiten und gesetzlichen Notwendigkeiten kooperiert wird. Daraufhin wurde in die aktuelle Version der auf den Mix-Servern eingesetzten Software eine Funktion zur Rückverfolgung programmiert. Zum Hintergrund der technischen Realisierung siehe unten Abschnitt 3.

Am 30. Juni 2003 wandte sich ein Beamter des Bundeskriminalamtes in dieser Sache telefonisch an das ULD. Offensichtlich hatte das BKA die Ermittlungen übernommen. Der Beamte schilderte, dass die Zugriffe auf ein bestimmtes im Internet zur Verfügung stehendes Forum überwacht werden sollten und erkundigte sich, auf welcher Rechtsgrundlage ein derartiger Beschluss zu erlassen sei und an wen dieser gerichtet werden solle. Die Mitarbeiter des ULD gaben ihm die Auskunft, dass es sich nur um einen Beschluss nach den §§ 100 a, b StPO, d.h. nach den Vorschriften über die Telekommunikationsüberwachung, handeln könne, durch den das Mitspeichern der Zugriffe auf eine bestimmte URL angeordnet würde. Der Beamte erweckte den Eindruck, dass der Erlass eines derartigen Beschlusses innerhalb kürzester Zeit möglich wäre. Es vergingen vier Tage, bis das BKA dem ULD einen Beschluss des Ermittlungsrichters des Amtsgerichts Frankfurt am Main per Telefax zugehen liess.

2 Erlass eines richterlichen Beschlusses gegenüber dem ULD

Obwohl dem Beamten des BKA, dem es um die Aufzeichnung der Zugriffe auf ein bestimmtes im Internet betriebenes Forum ging, ausdrücklich mitgeteilt worden war, dass rechtlich nur ein Beschluss gemäß §§ 100a, b StPO in Betracht komme, beruhte der erlassene Beschluss überraschender Weise auf den Regelungen der §§ 100g, h StPO.

Während auf der Rechtsgrundlage der §§ 100a, b StPO die künftige *Überwachung* der Telekommunikation angeordnet werden kann, ermöglicht eine Anordnung gemäß

§§ 100g, h StPO grundsätzlich nur die nachträgliche *Auskunft* über Telekommunikationsverbindungsdaten, zu denen auch die IP-Adresse gehört.

Eine solche Anordnung darf sich lediglich auf Daten beziehen, die seitens der Diensteanbieter nach bestehenden Regelungen zulässigerweise erhoben und gespeichert werden und insoweit bereits vorliegen. Bei dem Betrieb des Anonymisierungsdienstes werden allerdings entsprechend den Vorgaben des Teledienstedatenschutzgesetzes (TDDSG) keine Daten erhoben und gespeichert, die Rückschlüsse auf Nutzer zulassen könnten, z. B. IP-Adressen. Deshalb hätte der Beschluss nach §§ 100g, h StPO zu keinerlei verwertbaren Ergebnissen geführt.

Wie sich der Begründung zum Gesetzentwurf der §§ 100g, h StPO entnehmen lässt, ist mit der Regelung eine Verpflichtung zur Speicherung von Verbindungsdaten nur für Zwecke der Strafverfolgung, wie sie § 100a ermöglicht, nicht verbunden (siehe BT-Drucksache 14/7008, S. 7). Deshalb kann die Anordnung einer Aufzeichnung von Zugriffen über den Anonymisierungsdienst nicht auf der Grundlage der §§ 100g, h StPO erfolgen. Die materiellen und formellen Hürden für eine Überwachung nach § 100 a StPO (Straftat nach einem präzisen Straftatenkatalog) liegen erheblich höher als bei einer Auskunft gem. §§ 100 g, h StPO („Straftat von erheblicher Bedeutung“). Obwohl § 100g Abs. 1 Satz 3 StPO regelt, dass die Auskunft auch über zukünftige Telekommunikationsverbindungen angeordnet werden kann, stellt diese Vorschrift keine Rechtsgrundlage für eine Aufzeichnung dar.

Aus den Gesprächen mit den Polizeibeamten war zu entnehmen, dass im vorliegenden Fall eine Aufzeichnung der bei dem Betrieb des Anonymisierungsdienstes normalerweise nicht erhobenen Daten erfolgen sollte, so dass ausschließlich ein Beschluss nach §§ 100a, b StPO geeignet gewesen wäre, dieses Ziel zu erreichen.

Die Anordnung einer Aufzeichnung von Daten kann nur in den Fällen und bei Vorliegen aller Voraussetzungen des § 100a StPO erfolgen. Hierfür muss der Verdacht einer der in dem Katalog dieser Vorschrift genannten Straftaten vorliegen. Ein Beschluss auf der Grundlage von § 100 a StPO war aber offensichtlich von der Polizei bzw. Staatsan-

waltschaft nicht beantragt worden, möglicherweise weil die Voraussetzungen für einen derartigen Beschluss nicht vorlagen. Die Frage der Rechtsgrundlagen für das Vorgehen der Polizei ist keine abstrakte juristische Formdiskussion. Vielmehr sind die Voraussetzungen für einen Beschluss nach § 100 g, h StPO („Straftat von erheblicher Bedeutung“) deutlich weiter als bei § 100 a, b StPO (Straftat nach einem präzisen Straftatenkatalog).

Wegen der offensichtlich bestehenden Rechtswidrigkeit des Beschlusses hat das ULD sofort nach dessen Erhalt das förmliche Rechtsmittel der Beschwerde beim Amtsgericht Frankfurt am Main eingelegt. In der Begründung zu dieser Beschwerde und in einem weiteren ergänzenden Schriftsatz wurde die von der herrschenden Kommentarliteratur sowie der Amtlichen Begründung des Gesetzgebers zum Gesetzentwurf der §§ 100g, h StPO gestützte Rechtsauffassung des ULD ausführlich dargelegt. Zugleich wurde beantragt, die Vollziehung des Beschlusses aufzuheben. Da der Beschwerde keine aufschiebende Wirkung zukommt, war es erforderlich, den Beschluss trotz des dagegen eingelegten Rechtsmittels umzusetzen und parallel seine Vollziehung anzufechten.

Die nach den Angaben des Beamten des BKA eigentlich zu überwachende IP-Adresse liess sich im Übrigen nicht dem Beschluss, sondern lediglich einem dem richterlichen Beschluss beigefügten informellen Begleitschreiben des BKA entnehmen.

3 Umsetzung des richterlichen Beschlusses

Nach dem Beschluss „wird auf Antrag gemäß §§ 100g, h StPO, § 3 Nr. 16 TKG das Unabhängige Landeszentrum für Datenschutz in Schleswig-Holstein verpflichtet, Auskunft über die Telekommunikation für die unter der Bezeichnung „JAP“ registrierten Remote-IP 141.76.1.122 für den Zeitraum bis 02.10.2003 zu erteilen.“

Bei der IP-Adresse 141.76.1.122 handelt es sich um eine der IP-Adressen, unter der die anonymen Benutzer im Internet surfen.

Bei wörtlicher Auslegung des Beschlusses wäre es erforderlich gewesen, Auskunft über alle IP-Adressen aller Nutzer des Anonymisierungsdienstes zu erteilen. Abgesehen davon, dass dieses bereits technisch angesichts der Menge anfallender Daten kaum realisierbar gewesen wäre, hätte dies zu einer Komplettüberwachung aller Nutzer geführt, was nach den angegangenen Telefonaten von Seiten der Strafverfolger gar nicht beabsichtigt war. Im Übrigen hätte eine solche Totalüberwachung wegen der bestehenden gesetzlichen Regelungen im TDDSG auch als rechtswidrig und unverhältnismäßig angesehen werden müssen.

Die Projektpartner kamen zu dem Ergebnis, dass der Beschluss nur im Lichte des Begleitschreibens des BKA auszulegen und in dieser Weise umzusetzen sei. Die in dem Begleitschreiben des BKA genannte IP-Adresse wurde an dem letzten Mix-Server eingetragen, so dass nunmehr für den Fall des Zugriffs auf diese IP-Adresse, die Teil einer URL ist, das Mitloggen der IP-Adresse des Anfragenden, sowie des Datums und der Uhrzeit ermöglicht werden konnte. Alle anderen Webseiten und alle anderen Nutzer des AN.ON-Dienstes blieben von der Protokollierungsfunktion unberührt.

Das System befindet sich noch im Aufbau. Gegenwärtig werden auch Kaskaden betrieben, die sich ausschließlich im Einflussbereich der Projektpartner befinden. Insbesondere die bisher als Standard konfigurierte und am meisten von den Nutzern frequentierte Test-Kaskade Dresden-Dresden wird allein von der TU Dresden betrieben.

Da es sich bei der entwickelten Software um eine Open-Source-Software handelt und der Quellcode der aktuellen Mix-Software somit öffentlich und für jedermann einsehbar war und ist, wurde auch die Funktion zur Rückverfolgung öffentlich bekannt. Durch die hohe Popularität und Verbreitung der Software begannen nach kurzer Zeit in den einschlägigen News- und Diskussionsforen Spekulationen darüber, ob die Betreiber von AN.ON ihre Nutzer überwachen würden. Die in der Mix-Software implementierte Funktion mit dem Namen „Crime Detection“ war von der Open-Source-Gemeinde entdeckt worden. Etwa zeitgleich wurde ein Zwangsupdate der Client-Software JAP veröffentlicht. Dieses führte bei einigen Nutzern zu Irritationen, da sie einen Zusammenhang

zwischen der implementierten Funktion und dem Zwangsupdate vermuteten. Das Zwangsupdate hatte mit der Protokollierungsfunktion jedoch nichts zu tun.

Da es grundsätzlich nicht zulässig ist, Informationen über laufende Ermittlungsmaßnahmen zu veröffentlichen, sind die Projektpartner nach Erhalt des Beschlusses zunächst nicht an die Öffentlichkeit gegangen. Dies war ein Fehler, weil auf der einen Seite auf der Website von JAP keine Hinweise auf die nunmehr mögliche Strafverfolgungsfunktion gegeben wurden, während auf der anderen Seite aus der Änderung des Quellcodes eben dies abgeleitet werden konnte. Dies führte bei den informierten Nutzern zunächst zu Verwirrung und Verunsicherung. Die Projektpartner hatten zwischen den Geheimhaltungspflichten in einem laufenden Ermittlungsverfahren und ihrem eigenen Anspruch auf Transparenz gegenüber den Nutzern abzuwägen. Sie waren auf eine Situation wie diese nicht gut genug vorbereitet. Da die Projektpartner keinesfalls das Vertrauen ihrer Nutzer in den Anonymisierungsdienst verlieren wollten, informierten sie nach Bekanntwerden der Vorgänge in den Internetforen die Öffentlichkeit fortan sofort über alle weiteren Entwicklungen durch Pressemitteilungen, ohne dass sie allerdings Einzelheiten bekanntgaben, die die Ermittlungen hätten gefährden können (siehe Pressemitteilungen des ULD vom 19. August 2003, 27. August 2003 und 2. September 2003).

4 Fortgang der Auseinandersetzung

Auf die Beschwerde der Projektpartner setzte das Landgericht Frankfurt am Main am 11. Juli 2003 die Vollziehung des Beschlusses des Amtsgerichts aus. Dieser Beschluss ging dem ULD jedoch erst am 26. August 2003 zu. Einer Begleitnotiz war zu entnehmen, dass die frühere Zusendung durch ein „technisches Versehen“ unterblieben war.

Unmittelbar nach Kenntnis des Beschlusses deaktivierten die Projektpartner die Protokollierung. Bis zu diesem Zeitpunkt war ein einziger Zugriff mitgeloggt worden. Da der Zugriff im Zeitraum zwischen dem 11. Juli 2003 und dem 26. August 2003 erfolgt war, und deswegen aus Sicht der Projektpartner höchst fraglich ist, ob dieser überhaupt verwertet werden darf, gaben sie den Datensatz zunächst nicht an die Strafverfolgungsbe-

hörden heraus. Vielmehr vertraten sie die Auffassung, dass über die Verwendung dieses in der Obhut der Projektpartner befindlichen Datensatzes erst nach einer endgültigen Entscheidung des Landgerichts zu befinden sein sollte. Hierüber wurde in einer Pressemitteilung vom 27. August 2003 berichtet.

Trotz der Aussetzungsentscheidung des Landgerichts erwirkte das BKA daraufhin einen Durchsuchungs- und Beschlagnahmebeschluss beim Amtsgericht Frankfurt am Main. Am Samstag, den 30. August 2003, wurde von Beamten des BKA und LKA Sachsen die Herausgabe des Datensatzes erzwungen, indem die Beamten die Privatwohnung des Direktors des Instituts für Systemarchitektur an der Fakultät Informatik aufsuchten. Um weiteren Schaden (Durchsuchung der Institutsräume, Beschlagnahme von Rechnern) von der TU Dresden und den Projektpartnern abzuwenden, wurde der Datensatz unter Protest an die Beamten herausgegeben. Gegen den Beschluss wurde ebenfalls Beschwerde eingelegt. Der neue Beschluss des Amtsgerichts wurde nach Auffassung der Projektpartner unter rechtsmissbräuchlicher Umgehung der Entscheidung des Landgerichts erwirkt. Nach der vorläufig zugunsten von AN.ON ergangenen Entscheidung des Landgerichts durfte das BKA nicht auf allgemeine Herausgabe- und Beschlagnahmebestimmungen (§§ 103, 105 StPO) ausweichen. Eine gerichtliche Überprüfung auch dieses Vorgehens der Beamten ist zwingend erforderlich.

Mit Beschluss vom 15. September 2003 hob das Landgericht Frankfurt am Main den Beschluss des Amtsgerichts Frankfurt am Main, mit dem die Auskunftserteilung angeordnet worden war, auf. Das Gericht führt in dem Beschluss aus: „Die Vorschriften der §§ 100g, h StPO regeln nur die Fälle, in denen Daten grundsätzlich aufgezeichnet und gespeichert werden, was vorliegend jedoch nicht der Fall ist.“ Das Gericht nimmt Bezug auf die „zutreffenden Ausführungen“ des Beschwerdeführers, also des ULD. Nach dem ersten Teilerfolg der Aussetzung der Vollziehung des Beschlusses hat das ULD nun auch abschließend Erfolg in der gerichtlichen Auseinandersetzung errungen. Offen ist jetzt noch die Beschwerde gegen den zweiten Beschluss des Amtsgerichts vom 30.08.2003, der auf die Durchsuchung der Räume in Dresden und auf die Beschlagnahme des Protokolldatensatzes gerichtet war. Über die Beschwerde des ULD hiergegen hat das LG Frankfurt noch nicht entschieden.

5. Lehren für die Zukunft

Den Projektpartnern war von Anfang an bewusst, dass zwischen starker Anonymität und den Notwendigkeiten der Strafverfolgung ein Spannungsverhältnis besteht. Sie hatten das Projekt AN.ON so geplant, dass in Phase eins zunächst der Dienst technisch sicher realisiert werden sollte und in Phase zwei die mit der Strafverfolgung zusammenhängenden technischen und rechtlichen Fragen geklärt werden sollten. Durch das Vorgehen des BKA waren sie gezwungen, bereits jetzt zu solchen Fragen Stellung zu beziehen. Im Wesentlichen haben sich die Projektpartner zu einer Policy entschieden, die auch in Zukunft starke Anonymität für die Nutzer von AN.ON gewährleistet, die sich in Übereinstimmung mit den gesetzlichen Vorschriften befindet. Eine vorsorgliche Massenprotokollierung wird abgelehnt und auch in Zukunft nicht durchgeführt. Sie wäre ein klarer Verstoß gegen das Teledienstedatenschutzgesetz. Strikte Bindung an Recht und Gesetz bedeutet aber auch die Befolgung richterlicher Anordnungen.

Wenn hingegen ein richterlicher Beschluss nach § 100 a StPO vorliegt, dann bindet er auch AN.ON. Nach dieser Vorschrift darf die Überwachung und Aufzeichnung der Telekommunikation unter den dort genannten Voraussetzungen angeordnet werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine der im Katalog dieser Vorschriften genannten Taten begangen hat oder zu begehen versucht. Voraussetzung ist außerdem, dass die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre. Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss benutzt. Die Anordnung ist auf drei Monate begrenzt, kann aber verlängert werden. Für die erlangten Daten bestehen Verwendungsregelungen, d. h. eine Nutzungsbeschränkungen.

Für die weitere Arbeit im Rahmen von AN.ON haben sich die Projektpartner vorgenommen, eine Massenüberwachung auch technisch definitiv auszuschließen. Die Überwachung im Einzelfall soll technisch so realisiert werden, dass alle anderen Teilnehmer davon nicht erfasst werden können. Zu lösen bleiben auch die Fragen von Transparenz und Vertrauen. Die Projektpartner wollen ausloten, ob sie über die öffentliche Bekanntgabe ihrer Policy in Strafverfolgungsfragen hinaus auch im Einzelfall Hinweise auf die aktivierte Strafverfolgungsfunktion geben können, ohne dass sie sich strafrechtlichen Vorwürfen (etwa der Strafvereitelung) aussetzen.

***