Meinhard Starostik

Rechtsanwalt

Rechtsanwaltskanzlei:
Schillstr. 9 ◆ 10785 Berlin
Tel.: 030 - 88 000 345
Fax: 030 - 88 000 346
email: Kanzlei@Starostik.de
USt-ID-Nr. DE165877648

Kanzlei vereidigter Buchprüfer:
Schwarzenberger Str. 7 ◆ 08280 Aue
Tel.: 03771-290 999

RA Starostik, Schillstraße 9, 10785 Berlin

An das
Landgericht Berlin
Littenstr. 12-17
10179 Berlin

Berlin, den 23. September 2011

AZ: 45/08
(bitte stets angeben)

In dem Rechtsstreit
Breyer ./. Bundesrepublik Deutschland
57 S 87/08

begrüßt der Kläger die Ergebnisse des Sachverständigengutachtens vom 29.07.2011. Die wesentlichen Ergebnisse lassen sich wie folgt zusammenfassen:

> „Aus meiner Sicht dient die Speicherung von IP-Adressen nicht dem nationalen oder internationalen Stand der Technik. (S. 3) [...] Eine Speicherung von IP-Adressen ist weder zur Angriffserkennung noch zur Angriffsabwehr zwingend erforderlich. (S. 3) [...] Es treten jedoch im Wesentlichen keine zusätzlichen Kosten durch den Verzicht auf die IP-Adressen-Speicherung auf, da wie unter 2. erwähnt diese anderen Sicherheitsmaßnahmen in jedem Fall zwingend erforderlich für den sicheren Betrieb des IT-Systems sind. (S. 3) [...] Insbesondere ist in beiden Fällen die Absenderangabe frei festlegbar. (S. 5) [...] eine Speicherung von IP-Adressen kann bestenfalls einen marginalen Sicherheitsgewinn bringen (S. 9) [...] Zum anderen existiert für die Absicherung von IT-Systemen eine Vielzahl von anderen, wesentlich effektiveren Mitteln und Methoden. (S. 10)“.

Ich gehe davon aus, dass auf der Grundlage des Gutachtens auch die Kammer der Meinung ist, dass der Beklagten nicht der Beweis ihrer Behauptung gelungen ist, zur Gewährleistung und Aufrechterhaltung der IT-Sicherheit und der Funktionsfähigkeit der von ihr betriebenen und verwendeten Telemedien und Telekommunikationsnetze sei die systematische Speicherung und spätere Verwendung der IP-Adressen der zugreifenden Hostsysteme sämtlicher Nutzer ihrer Telemedien erforderlich und – insoweit nicht Gegenstand des Beweisbeschlusses – verhältnismäßig. In diesem Fall erübrigt sich nähere Aufklärung und ist der Kläger mit einer Entscheidung im schriftlichen Verfahren einverstanden.

Nur falls die Kammer die Klage nicht für begründet erachten sollte oder falls die Beklagte Erläuterung des Gutachtens durch den Sachverständigen beantragen sollte, wird von Klägerseite beantragt,

> den Sachverständigen zwecks mündlicher Erläuterung seines Gutachtens zu laden.

Der Sachverständige soll in diesem Fall klarstellend noch einmal zu der Hauptbeweisfrage befragt werden, denn sein Gutachten geht ausdrücklich nur auf die Einzelfragen ein, die der Beweisbeschluss „insbesondere“ zum Gegenstand hat. Auch soll der Sachverständige in diesem Fall zu denjenigen technischen Gesichtspunkten befragt werden, die Gegenstand der Schriftsätze des Klägers vom Juni 2010 (unter 4.) und vom Oktober 2010 (unter 3. und 4.) sowie der folgenden Ausführungen sind.

Es wird eine *mündliche* Anhörung beantragt, weil eine ergänzende schriftliche Stellungnahme des Sachverständigen den ohnehin schon lange dauernden Rechtsstreit weiter verzögern würde. Um mündliche Anhörung wird auch für den Fall gebeten, dass die Beklagte noch Fragen haben sollte.

Zu dem schriftlichen Gutachten des Sachverständigen ist anzumerken:

1. Soweit der Sachverständige die Möglichkeit anspricht, IP-Adressen verschlüsselt oder durch eindeutige Ersetzung pseudonymisiert zu speichern, stellt eine solche Ersetzung eine Maßnahme zur Erhöhung der Sicherheit der Daten vor unbefugten Zugriffen Dritter dar. Sie schützt die Daten allerdings nicht vor Zugriffen der Beklagten selbst, welche über den zur Entschlüsselung bzw. Depseudonymisierung erforderlichen Schlüssel verfügt. Ziel der vorliegenden Klage ist es insbesondere, zu verhindern, dass Mitarbeiter der Beklagten oder mit ihrem Willen andere Behörden die Internetnutzung des Klägers und damit sein Privatleben und seine Persönlichkeit ausspionieren und dem Kläger dadurch gegebenenfalls weitere Nachteile entstehen (z.B. Ermittlungsverfahren aufgrund falschen Verdachts). Vor diesen Gefahren schützt eine verschlüsselte oder pseudonymisierte IP-Speicherung von vornherein nicht. Wenn der Klageantrag auf Unterlassung der Speicherung der IP-Adressen des Klägers gerichtet ist, so ist deshalb jede Art der personenbezogenen Speicherung gemeint, egal ob sie verschlüsselt, pseudonymisiert oder unverschlüsselt erfolgt.

2. Soweit der Sachverständige den Schutz vor Angriffen und Sicherheitsverletzungen diskutiert, ist dazu bereits mit Schriftsätzen vom Juni 2010 (unter 4.) und vom Oktober 2010 (unter 3. und 4.) Stellung genommen worden. Diese Ausführungen gelten weiterhin.

3. Der Sachverständige führt aus, die DIN ISO/IEC 27002:2008-09 empfehle eine Speicherung von IP-Adressen. Zur Einordnung dieses Dokuments ist zu beachten, dass die zugrunde liegende DIN ISO/IEC 27000 nur das Dokument 27001 als IT-Sicherheitsstandard definiert, der einzuhalten ist, während das Dokument 27002 lediglich als Vorschlag zur Umsetzung des Standards 27001 definiert wird („to be used as implementation guidance“), der nicht verbindlich und nicht Teil des IT-Sicherheitsstandards ist.

Was nun den vom Sachverständigen zitierten Abschnitt 10.10.1 der DIN ISO/IEC 27002:2008-09 angeht, so heißt es in dem übergeordneten Abschnitt 10.10 wörtlich (englische Originalfassung):

> „Step 10.10 – Monitoring (CobiT AI2, DS5, ME1, ME2, ME4)
> Systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure information system problems are identified. **An organization should comply with all relevant legal requirements applicable to its monitoring and logging activities.**“

Der letzte Satz lautet übersetzt: „Eine Organisation sollte alle einschlägigen rechtlichen Vorgaben, die für ihre Überwachungs- und Protokollierungsaktivitäten gelten, einhalten.“ Der gesamte Abschnitt 10.10 gilt also ausdrücklich nur im Rahmen der

einschlägigen gesetzlichen Vorgaben. Eine gegen das Telemediengesetz verstoßende Protokollierung wird von der DIN 27002 nicht nur nicht gefordert. Es ist sogar umgekehrt Bestandteil der DIN 27002, dass die gesetzlichen Vorgaben wie das Protokollierungsverbot des Telemediengesetzes eingehalten werden.

Dies bestätigt den schon mit Schriftsatz vom Oktober 2010 hervorgehobenen Umstand, dass Industrienormen kein Recht setzen und selbst anerkannten Regeln der Technik, die von Industrienormen zu unterscheiden sind, allenfalls im Vertragsrecht mittelbare rechtliche Bedeutung zukommen kann.

4. Im Grundschutz-Baustein „M 5.9 Protokollierung am Server“ des BSI-Grundschutzes heißt es, es sollten (nur) „sicherheitsrelevante Ereignisse“ protokolliert werden, insbesondere falsche Passworteingaben, Versuche unberechtigter Zugriffe, Stromausfälle und Daten zur Netzauslastung und -überlastung. Die Nutzung von Telemedien der Beklagten durch den Kläger stellt kein solches Ereignis dar. Insbesondere können Telemedien der Beklagten, die der Information der Öffentlichkeit dienen und damit jedermann zur Verfügung stehen, nicht „unberechtigt“ genutzt werden.

Soweit der Baustein „M 4.47 Protokollierung der Sicherheitsgateway-Aktivitäten“ des BSI-Grundschutzes IP-Adressen anspricht, heißt es in dem einleitenden Absatz dieses Bausteins wörtlich: „Die Protokollierung muss den jeweils geltenden rechtlichen Bestimmungen entsprechen.“ Königshofen/Ulmer schreiben dazu im Datenschutz-Handbuch Telekommunikation (§ 100 TKG, Rn. 20):

> „Einer Gesamtprotokollierung des durch die Firewall fließenden Kommunikationsstroms ist nicht nur aus technischen Gründen der Systemperformance, sondern auch aus Rechtsgründen eine dokumentierte Protokollierung der Ereignisse vorzuziehen, die den Anfangsverdacht eines Missbrauchs rechtfertigen. Diese Form der intelligenten Protokollierung (nicht alles, sondern nur das wesentliche wird protokolliert) wird heutzutage insbesondere von modernen Intrusion-Detection-Systemen unterstützt, die auch unter dem Gesichtspunkt der Datenvermeidung und Datensparsamkeit so eingestellt werden können, dass sie damit verbundene Datenverarbeitung den Anforderungen des TKG gerecht werden.“

Im Fall einer solchen „intelligenten Protokollierung“ würde die IP-Adresse des zugreifenden Hostsystems des Klägers bei der Nutzung der Telemedien der Beklagten nicht protokolliert, denn die bloße Nutzung von Telemedien begründet keinen „ Anfangsverdacht eines Missbrauchs“. Im Übrigen gilt § 100 TKG für die Bereitstellung von Telemedien nicht, wie bereits umfassend ausgeführt worden ist.

Was die Maßnahme „M 4.182 Überwachen des IIS-Systems“ des BSI-Grundschutzes angeht, führt bereits der Sachverständige zutreffend aus, dass als milderes Mittel der Einsatz eines Apache-Systems anstelle eines IIS-Systems in Betracht kommt, weil bei Apache-Webservern keine IP-Vorratsdatenspeicherung vorgesehen ist. Im Übrigen heißt es auch unter M 4.182 nur allgemein, dass bei dem Betrieb von IIS-Systemen IP-Adressen protokolliert werden „sollten“, was keine ausnahmslose Regel aufstellt. IIS ist eine Software, mit deren Hilfe Dokumente und Dateien in Netzwerken zugänglich gemacht werden können. Erfolgt dies beispielsweise über ein Intranet oder über das Internet nur für interne dienstliche Zwecke, so brauchen die Vorgaben des Telemediengesetzes nicht eingehalten zu werden (§ 11 Abs. 1 TMG). Das Dokument M 4.182 hat die Besonderheiten gerade öffentlich zugänglicher Telemedien erkennbar nicht im Blick. Diese Fragen behandelt vielmehr der Grundschutz-Baustein „M 2.110 Datenschutzaspekte bei der Protokollierung“, in welchem es heißt: „Art und Umfang

von Protokollierungen hängen vom allgemeinen Datenschutzrecht und auch von bereichsspezifischen Regelungen ab."

In der Zusammenschau lässt sich aus dem BSI-Grundschutz keine Empfehlung ableiten, die IP-Adressen aller Nutzer öffentlicher Telemedien zu protokollieren.

5. Was den vom Sachverständigen angeführten ETSI-Bericht angeht, so heißt es unter Ziff. 1 dieses Berichts einleitend:

> „The scope of the present document is to recommend a framework for the secure provision of Lawful Interception (LI) and Data Retention (DR) services of a Communication Service Provider (CSP) towards the Law Enforcement Agencies."

Gegenstand dieses Berichts ist also ausschließlich die Bereitstellung gesetzlich vorgesehener Überwachungs- und Vorratsspeicherungsleistungen durch einen Anbieter elektronischer Kommunikationsdienste für Eingriffsbehörden, in Deutschland umgesetzt durch die Technische Richtlinie zur Telekommunikations-Überwachungsverordnung. Der Betrieb von Webservern durch die Beklagte hat evidentermaßen nichts mit gesetzlich vorgesehener Telekommunikationsüberwachung oder Vorratsdatenspeicherung zu tun. Selbst als die verfassungswidrige Regelung zur Vorratsdatenspeicherung noch in Kraft war, erfasste diese Anbieter von Telemedien nicht, sondern nahm den Abruf von Internetseiten ausdrücklich aus (§ 113a Abs. 8 TKG a.F.).

6. Aus den einschlägigen technischen Dokumenten ist danach allenfalls die Empfehlung abzuleiten, „sicherheitsrelevante Ereignisse" in dem rechtlich zulässigen Umfang zu protokollieren. In welchem Umfang dies rechtlich zulässig ist, ist eine normative und keine technische Frage. Aus technischen Empfehlungen, die ausdrücklich auf die gesetzlichen Vorgaben verweisen, lässt sich ohne Zirkelschluss nichts für die Auslegung der gesetzlichen Vorgaben entnehmen.

7. Das Bundesamt für Sicherheit in der Informationstechnik definiert den Begriff der „IT-Sicherheit" wie folgt:[1]

> **„IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind."**

Selbst bei Zugrundelegung des Begriffs der IT-Sicherheit, den das Telemediengesetz aus guten Gründen nicht als Rechtfertigung einer Nutzerprotokollierung anerkennt, ist also nicht eine maximale Sicherheit ohne Rücksicht auf die Grundrechte unbescholtener Bürger das Ziel, sondern nur ein angemessenes Sicherheitsniveau, bei dem Risiken „auf ein tragbares Maß reduziert sind".

Der Gesetzgeber hat mit den §§ 13, 15 TMG bewusst und in Kenntnis der Risiken der Informationstechnologie entschieden, dass ein angemessenes Sicherheitsniveau ohne personenbezogene Protokollierung jedes Klicks im Internet zu erreichen ist, dass eine personenbezogene Aufzeichnung des Internetnutzungsverhaltens sogar gerade wegen der bekannten IT-Sicherheitsrisiken unterbleiben muss, um die 51 Mio. Internetnutzer in Deutschland vor Missbrauch ihrer Informationsspuren zu schützen. Diese Entscheidung des Gesetzgebers ist verbindlich, im Übrigen aber auch inhaltlich richtig.

[1] https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html.

Ihre Richtigkeit bestätigt die Praxis vieler Telemedienanbieter einschließlich Behörden und Ministerien der Beklagten selbst, die ihre Telemedien seit Jahren erfolgreich ohne IP-Vorratsdatenspeicherung bereitstellen. Der Sachverständige hat die Verfügbarkeit einer „Vielzahl von anderen, wesentlich effektiveren Mitteln und Methoden“ zur Erreichung eines angemessenen Sicherheitsniveaus bestätigt. Sogar die Beklagte selbst hat im vorliegenden Prozess die Verfügbarkeit solcher alternativen Mittel zur Gewährleistung der IT-Sicherheit zugestanden, wobei der Sachverständige ihre Behauptung hoher Zusatzkosten nicht bestätigt hat.

Die Beklagte wird sich dementsprechend mit der Entscheidung des Gesetzgebers abfinden müssen. Ihr hilft dabei vielleicht die Erkenntnis, dass das höchstmögliche Maß an Sicherheit in Deutschland sicherlich dadurch erreicht werden könnte, dass jeder Bürger in ein Gefängnis eingesperrt würde. Ein solches Maß an Sicherheit will gleichwohl niemand und wäre auch mit den Grundwerten unserer freiheitlichen Gesellschaft unvereinbar. Deswegen darf die Beklagte auch im Internet ihre Bürger nicht von vornherein als „potenzielles Sicherheitsrisiko“ behandeln, sondern muss deren Recht respektieren, sich über das Internet ebenso frei, unbefangen und anonym zu informieren wie aus Zeitungen oder über das Fernsehen.

Meinhard Starostik
Rechtsanwalt