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

RA Starostik, Schillstraße 9, 10785 Berlin

An das
Landgericht Berlin
Littenstr. 12-17
10179 Berlin

Kanzlei vereidigter Buchprüfer:
Schwarzenberger Str. 7 • 08280 Aue
Tel.: 03771-290999

Berlin, den 9. Juni 2010

AZ: 45/08
(bitte stets angeben)

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

nehme ich zum Beschluss des Hohen Gerichts vom 20.05.2010 wie folgt Stellung:

1. Erforderlichkeit einer Beweiserhebung

Der Kläger begrüßt den Beschluss vom 20.05.2010 insoweit, als in der beabsichtigten Beweiserhebung zum Ausdruck kommt, dass das Gericht die Klage für zulässig hält und die IP-Adresse des Klägers als personenbezogenes Datum im Rechtssinne ansieht.

Der Kläger teilt dagegen die dem Beweisbeschluss zugrunde liegende vorläufige Rechtsauffassung des Gerichts insoweit nicht, wie die Protokollierung des klägerischen Internet-Nutzungsverhaltens offenbar zulässig sein soll, wenn sie „zur Gewährleistung und Aufrechterhaltung der IT-Sicherheit und der Funktionsfähigkeit“ der „Telemedien und Telekommunikationsnetze“ der Beklagten erforderlich sei, dem „Stand der Technik“ entspreche oder wenn alternative Schutzmaßnahmen zu teuer seien. Nach Überzeugung des Klägers kommt es auf all diese Fragen von Rechts wegen nicht an, weil der Gesetzgeber der Vertraulichkeit der Telemediennutzung aus gutem Grund den Vorrang vor Speicherinteressen der Anbieter eingeräumt hat.

Nach § 15 TMG darf der Diensteanbieter „personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen“. Die Behauptungen der Beklagten, über die Beweis erhoben werden soll, rechtfertigten dementsprechend die beanstandete Protokollierungspraxis nach dem Gesetz selbst dann nicht, wenn sie wahr wären. Mit der angekündigten Beweiserhebung würde sich das Gericht auf eine unzutreffende Rechtsauffassung festlegen. Es würde einen Erlaubnistatbestand anwenden,

dessen Einführung der Deutsche Bundestag im vergangenen Jahr ausdrücklich abgelehnt hat. [1]

Die nach § 15 TMG alleine maßgebliche Frage, ob die personenbezogene Internet-Nutzungsprotokollierung zur Ermöglichung der Telemedien der Beklagten erforderlich ist, ist unstreitig zu verneinen. Die Beklagte behauptet selbst nicht, dass die beanstandete Nutzerprotokollierung zur Bereitstellung ihrer Telemedien erforderlich sei. Dementsprechend stellt sie viele Telemedien, welche dieselbe Reichweite aufweisen und Schadsoftware ebenso ausgesetzt sind wie ihre sonstigen Telemedien, ohne Protokollierung der Nutzer-IP-Adressen bereit. Außerdem räumt die Beklagte ausdrücklich ein, dass sie „alternative Maßnahmen zur Schadprogrammabwehr“ einsetzen kann, „um einen sicheren Betrieb der entsprechenden Systeme der Beklagten zu gewährleisten“, dass also ein sicherer Betrieb der Systeme der Beklagten auch ohne die rechtswidrige Protokollierung des Surfverhaltens samt IP-Adressen möglich ist. Über Unstreitiges braucht Beweis nicht erhoben zu werden.

2. Beweisfragen

Sollte das Hohe Gericht gleichwohl eine Beweiserhebung für erforderlich halten, so wird beantragt, die Beweisfragen an dem gesetzlichen Erlaubnistatbestand und an dem Klageantrag auszurichten, indem Ziff. 1 des Beweisbeschlusses vom 20.05.2010 wie folgt neu gefasst wird:

> **1. Es soll durch Einholung eines schriftlichen Sachverständigengutachtens Beweis erhoben werden über die Behauptungen der Beklagten,**
>
> **a) um die Inanspruchnahme der Telemedien der Beklagten zu ermöglichen, sei es erforderlich, die Internetprotokolladresse (IP-Adresse) des zugreifenden Hostsystems des Klägers, die im Zusammenhang mit der Nutzung öffentlich zugänglicher Telemedien der Beklagten im Internet übertragen wird, über das Ende des jeweiligen Nutzungsvorgangs hinaus zu speichern oder durch Dritte speichern zu lassen, und zwar nicht nur dann, wenn die Speicherung im Störungsfall zur Wiederherstellung der Verfügbarkeit des Telemediums erforderlich ist,**
>
> **b) nach dem gegenwärtigen Stand der Technik sei es nicht durchführbar, die Inanspruchnahme der Telemedien der Beklagten zu ermöglichen, ohne die Internetprotokolladresse (IP-Adresse) des zugreifenden Hostsystems des Klägers über das Ende des jeweiligen Nutzungsvorgangs hinaus zu speichern oder durch Dritte speichern zu lassen,**
>
> **c) dass die Beklagte einige Telemedien wie www.bmj.bund.de, www.bundeskriminalamt.de und www.bundesfinanzministerium.de**

[1] Innenausschuss des Deutschen Bundestags, BT-Drs. 16/13259, 5 und 8. Dem Gesetzentwurf der Bundesregierung zufolge hätte der folgende § 15 Abs. 9 S. 1 TMG eingeführt werden sollen (BT.Drs. 16/11967, 9): „Soweit erforderlich, darf der Diensteanbieter Nutzungsdaten zum Erkennen, Eingrenzen oder Beseitigen von Störungen seiner für Zwecke seines Dienstes genutzten technischen Einrichtungen erheben und verwenden.“

bereit stellt, ohne die Internetprotokolladresse (IP-Adresse) des zugreifenden Hostsystems des Klägers über das Ende des jeweiligen Nutzungsvorgangs hinaus zu speichern oder durch Dritte speichern zu lassen, ändere nichts an der Erforderlichkeit einer solchen Speicherung zur Bereitstellung anderer Telemedien der Beklagten,

d) um die Inanspruchnahme der Telemedien der Beklagten zu ermöglichen, ohne die Internetprotokolladresse (IP-Adresse) des zugreifenden Hostsystems des Klägers über das Ende des jeweiligen Nutzungsvorgangs hinaus zu speichern oder durch Dritte speichern zu lassen, müssten die technischen Anlagen der Beklagten mit hohem Kostenaufwand umgestellt werden.

Bei Beantwortung der Beweisfrage d) soll der Sachverständige dazu Stellung nehmen, welche Kosten gegebenenfalls für die erforderlichen Maßnahmen aufzuwenden wären.

Zur Begründung:

Die vorgeschlagene Beweisfrage zu a) orientiert sich am gesetzlichen Erlaubnistatbestand des § 15 Abs. 1 TMG und stellt auf die Erforderlichkeit der Datenspeicherung zur Ermöglichung der Inanspruchnahme der Telemedien ab. Anders die vorläufigen Beweisfragen laut Beschluss vom 20.05.2010 begrenzt die hier vorgeschlagene Formulierung die Beweiserhebung auf den rechtlich maßgeblichen Tatbestand.

Die vorgeschlagene Beweisfrage hat nicht die Erforderlichkeit der Datenspeicherung „zur Gewährleistung und Aufrechterhaltung der IT-Sicherheit und der Funktionsfähigkeit der von [der Beklagten] betriebenen und verwendeten Telemedien und Telekommunikationsnetze“ zum Gegenstand, denn das Gesetz bietet für eine Datenspeicherung zu diesen Zwecken keine Grundlage. Es besteht keine Norm, aus der sich eine Zulässigkeit der Vorratsspeicherung personenbezogener IP-Adressen zu den genannten Zwecken ergeben würde. Umgekehrt untersagt § 15 TMG eindeutig die Speicherung von Nutzungsdaten über die Dauer des Nutzungsvorgangs hinaus. Auch ist der Begriff der „IT-Sicherheit“ zu unbestimmt, als dass er Grundlage einer Beweiserhebung sein könnte. Ferner ist nicht erkennbar, weshalb das Surfverhalten des Klägers erfasst werden soll, um die Funktionsfähigkeit der von der Beklagten nicht betriebenen, sondern nur „verwendeten Telemedien und Telekommunikationsnetze“ zu gewährleisten. Sind hiermit Internetportale Dritter oder das Telefonnetz Dritter gemeint, welche Bedienstete der Beklagten einsetzen? Es ist nicht ersichtlich, welchen Zusammenhang das Surfverhalten des Klägers damit aufweisen soll.

Die vorgeschlagene Beweisfrage zu a) orientiert sich am Klageantrag, indem sie gerade auf die vom Kläger genutzten IP-Adressen abstellt. Im vorliegenden Rechtsstreit ist nicht entscheidungserheblich, ob die Beklagte irgendwelche IP-Adressen speichern darf, sondern ob sie gerade die vom Kläger verwendeten IP-Adressen protokollieren darf, obwohl von der Internetnutzung durch den Kläger unstreitig keinerlei Gefahren für die Beklagte oder ihre Informationstechnik ausgehen. Der Sachverständige wird gegebenenfalls dazu Stellung zu nehmen haben, ob sich etwa erforderliche Speicherungen so

begrenzen lassen, dass die IP-Adressen rechtstreuer Nutzer wie des Klägers von ihnen ausgenommen bleiben.

Die vorgeschlagene Beweisfrage zu a) beschränkt sich ferner auf die Speicherung der IP-Adresse über die Dauer des Nutzungsvorgangs hinaus. Dass die IP-Adresse für die Dauer der Übertragung abgerufener Internetseiten gespeichert werden muss, ist zwischen den Parteien unstreitig.

Schließlich nimmt die vorgeschlagene Beweisfrage zu a) den Fall aus, dass die Speicherung im Störungsfall zur Wiederherstellung der Verfügbarkeit des Telemediums erforderlich sei. Diese Frage ist dadurch dem Streit entzogen, dass sie vom Klageantrag ausgenommen ist. Einer sachverständigen Stellungnahme dazu bedarf es infolgedessen nicht.

Die vorgeschlagene Beweisfrage zu b) knüpft an den Rechtsgedanken des § 14 BImSchG an. Nach dieser Vorschrift kann auf Grund privatrechtlicher Abwehransprüche nicht die Einstellung des Betriebs einer genehmigten Anlage verlangt werden, wenn die Vermeidung benachteiligender Einwirkungen der Anlage „nach dem Stand der Technik nicht durchführbar oder wirtschaftlich nicht vertretbar“ ist. Wäre das Angebot von Telemedien ohne Speicherung von IP-Adressen über die Nutzungsdauer hinaus „nach dem Stand der Technik nicht durchführbar oder wirtschaftlich nicht vertretbar“, so könnte diese Maßnahme als erforderlich zur Bereitstellung von Telemedien im Sinne des § 15 Abs. 1 TMG angesehen werden.

Die bloße Frage, ob die Speicherung von IP-Adressen dem „Stand der Technik dient“ (Beweisbeschluss vom 20.05.2010), ist dagegen zu unbestimmt, um den Gegenstand einer sachverständigen Begutachtung bilden zu können. Den Begriff „Stand der Technik“ verwendet der Gesetzgeber etwa in § 3 Abs. 12 KrW-/AbfG, § 3 Abs. 6 BImSchG, § 3 Nr. 11 WHG, § 3 Abs. 10 GefStoffV und § 2 Abs. 7 LärmVibrationsASchV, um Anlagebetreibern bestmögliche „Vorsorge gegen schädliche Umwelteinwirkungen“ ihrer Anlagen vorzuschreiben. In Rede steht hier indes nicht eine Vorsorge gegen Gefahren, die von den Anlagen der Beklagten ausgehen, sondern eine Vorsorge gegen Gefahren für die Anlagen selbst. Eine Ermächtigung, die zum Schutz eigener Anlagen die Ausschöpfung der technischen Möglichkeiten ohne Rücksicht auf die Rechte Dritter erlaubte, kennt die Rechtsordnung nicht. Anbieter von Telemedien werden vom Gesetzgeber an keiner Stelle verpflichtet oder ermächtigt, alle nach dem Stand der Technik möglichen Vorsorgemaßnahmen zu ergreifen. „Stand der Technik“ bezeichnet das „Stadium der technischen Möglichkeiten zu einem bestimmten Zeitpunkt“. [2] Rechtlich nicht haltbar wäre es, Anbietern von Telemedien auf Kosten der Privatsphäre und Datensicherheit ihrer Nutzer zu gestatten, rein vorsorglich sämtliche technisch verfügbaren Möglichkeiten zur Überwachung der Nutzer auszuschöpfen, nur weil dies in seltenen Fällen einmal zur Gefahrenabwehr nützlich sein könnte. Für eine solche Ermächtigung zu einer präventiven Erfassung des Telemedien-Nutzungsverhaltens bietet § 15 TMG keinerlei Anhalt.

Selbst eine Videoüberwachung, deren Zulässigkeit keine abschließende gesetzliche Regelung wie durch § 15 TMG erfahren hat, hat der

[2] Europäische Norm EN 45020, Ziff. 1.4.

Bundesgerichtshof bei öffentlich zugänglichen Räumen nur zugelassen, wenn gerade auf dem überwachten Grundstück [3] in der Vergangenheit schwerwiegende Rechtsverletzungen, etwa Angriffe gegen eine Person oder ihre unmittelbare Wohnsphäre, begangen worden sind und ihnen ohne Videoüberwachung nicht zumutbar begegnet werden könnte; [4] auch in diesem Fall darf eine Videoüberwachung nur zielgerichtet und zeitlich befristet zur Identifizierung des Täters dieser Handlungen und zur Durchsetzung der gegen ihn bestehenden Ansprüche eingesetzt werden und nicht dauerhaft. Im Vergleich zur Videoüberwachung ist eine Surfprotokollierung der weit schwerere Eingriff, weil die Beklagte den Inhaber des jeweils genutzten Anschlusses identifizieren lassen kann (§ 113 TKG) und weil sich Surfprotokolle – anders als Videoaufnahmen – unschwer maschinell auswerten und weiter verarbeiten lassen.

Die vorgeschlagene Beweisfrage zu c) hat die in der mündlichen Verhandlung erörterte Behauptung der Beklagten zum Gegenstand, die Nichterfassung von Besucher-IP-Adressen bei der Bereitstellung einiger ihrer Telemedien lasse nicht darauf schließen, dass die Erfassung von Besucher-IP-Adressen auch bei der Bereitstellung der übrigen Telemedien der Beklagten verzichtbar sei.

Die vorgeschlagene Beweisfrage zu d) knüpft an die Behauptung der Beklagten an, der Verzicht auf eine personenbezogene Surfprotokollierung sei nur durch eine äußerst kostenaufwändige Umstellung ihrer Anlagen möglich.

Die Vorschläge zur Neufassung der Beweisfragen lassen die Ausführungen zu Ziff. 1 unberührt, wonach die Beweisfragen nach Auffassung des Klägers von Rechts wegen nicht entscheidungserheblich sind oder bereits auf der Grundlage des unstreitigen Vortrags der Parteien beantwortet werden können.

3. Person des/der Sachverständigen

Als geeignete Sachverständige für eine etwa für erforderlich gehaltene Beweisaufnahme werden vorgeschlagen:

1. Dipl.-Inf. Constanze Kurz, [*...anonymisiert...*].
   Frau Kurz ist Diplom-Informatikerin und wissenschaftliche Mitarbeiterin in der Arbeitsgruppe Informatik in Bildung und Gesellschaft am Institut für Informatik der Humboldt-Universität zu Berlin sowie Sprecherin des Chaos Computer Club e.V. Frau Kurz war unter anderem schon für das Bundesverfassungsgericht als Sachverständige tätig.

2. Prof. Dr. rer. nat. Andreas Pfitzmann, [*...anonymisiert...*]
   [...]. Prof. Pfitzmann ist Informatiker und Inhaber der Professur für Datenschutz und Datensicherheit der Technischen Universität Dresden. Er war 10 Jahre lang Vorsitzender der Fachgruppe „Verlässliche IT-Systeme“ der Gesellschaft für Informatik e.V. Prof. Pfitzmann war unter anderem schon für das Bundesverfassungsgericht und für den Deutschen Bundestag als Sachverständiger tätig.

---

[3] KG, NZM 2009, 736.

[4] BGH, NJW 1995, 1955 m.w.N.

3. Dr. jur. Thilo Weichert, [*...anonymisiert...*]. Dr. Weichert ist Jurist und Datenschutzbeauftragter des Landes Schleswig-Holstein. Da das von ihm geleitete Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein als eigenständige Anstalt öffentlichen Rechts organisiert ist, weist er die erforderliche Unabhängigkeit für die Tätigkeit als Sachverständiger auf. Wegen seiner Zuständigkeit für den Bereich Datensicherheit und auch, weil das Landesdatenschutzzentrum ein eigenes Internetportal anbietet, kann Dr. Weichert die Beweisfragen beantworten. Dr. Weichert war unter anderem schon für den Deutschen Bundestag als Sachverständiger tätig.

4. Peter Schaar, [*...anonymisiert...*]. Herr Schaar ist Bundesbeauftragter für den Datenschutz und die Informationsfreiheit. Da er in seiner Tätigkeit nicht weisungsgebunden ist, weist er die erforderliche Unabhängigkeit für die Tätigkeit als Sachverständiger auf. Wegen seiner Zuständigkeit für den Bereich Datensicherheit und auch, weil seine Behörde ein eigenes Internetportal anbietet, kann Herr Schaar die Beweisfragen beantworten. Er hat bereits vielfältige Stellungnahmen gegenüber dem Bundesverfassungsgericht und anderen Gerichten abgegeben.

Das von dem Beklagtenvertreter in der mündlichen Verhandlung vorgeschlagene Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie dessen Mitarbeiter sind nicht als Sachverständige geeignet, weil das BSI eine nachgeordnete Behörde des Bundesinnenministeriums ist und seine Mitarbeiter an Weisungen des Bundesinnenministers, der die Beklagte im vorliegenden Prozess vertritt, gebunden sind. Auch sonst sollte kein von der Beklagten benannter Sachverständiger bestellt werden, der bereits gegen Entgelt für die Beklagte tätig gewesen ist.

Für den Fall der Beweiserhebung wird im Hinblick auf die bisherige Verfahrensdauer gebeten, dem oder der Sachverständigen eine kurze Frist von höchstens zwei Monaten für die Vorlage des Gutachtens zu setzen (§ 411 Abs. 1 ZPO).

4. Vermeintliche Notwendigkeit der Speicherung von IP-Adressen

Während der Beklagtenvertreter gegen Ende des Schriftsatzes vom 22.03.2010 behauptet, die Speicherung von IP-Adressen über die Dauer des Nutzungsvorgangs hinaus sei notwendig, räumt er auf Seite 8 desselben Schriftsatzes – wie schon zuvor mit Schriftsatz vom 27.01.2009 – ausdrücklich ein, dass die Beklagte „alternative Maßnahmen zur Schadprogrammabwehr“ einsetzen kann, „um einen sicheren Betrieb der entsprechenden Systeme der Beklagten zu gewährleisten“, dass also ein sicherer Betrieb der Systeme der Beklagten auch ohne die rechtswidrige Protokollierung des Surfverhaltens samt IP-Adressen möglich ist. Der Vortrag der Beklagten zur vermeintlichen Notwendigkeit der Speicherung von IP-Adressen ist mithin in sich widersprüchlich und deshalb unbeachtlich.

Die Beklagte widerlegt die Behauptungen ihres Prozessbevollmächtigten im Übrigen dadurch, dass sie selbst eine Vielzahl von Internet-Portalen ohne Aufzeichnung von IP-Adressen anbietet, ohne dass diese Angebote häufiger gestört oder sonst beeinträchtigt wären als ihre sonstigen Portale. Ohne

Speicherung von IP-Adressen bieten etwa die folgenden Ministerien und Behörden der Beklagten Internetportale an:

- Bundesjustizministerium
- Bundesdatenschutzbeauftragter
- Bundesrechnungshof
- Bundesforschungsministerium
- Bundeskriminalamt
- Bundesversicherungsamt
- Bundesanstalt für Arbeitsschutz
- Bundesanstalt für Wasserbau
- Kraftfahr-Bundesamt
- Bundeseisenbahnvermögen
- Bundesstelle für Seeschiffahrt und Hydrographie
- Bundesanstalt für Gewässerkunde
- Bundesfinanzministerium

Der hypothetische Fall, dass die Speicherung von IP-Adressen einmal zur Wiederherstellung der Verfügbarkeit eines Telemediums erforderlich sein könnte, ist von vornherein dem Streit entzogen, indem er vom Klageantrag ausgenommen worden ist.

In rechtlicher Hinsicht nennt der Beklagtenvertreter keine einzige Norm, aus der sich eine Zulässigkeit der verschiedenen insbesondere vom Bundesverwaltungsamt praktizierten Auswertungen ergeben soll. Vielmehr untersagt § 15 TMG eindeutig die Speicherung personenbezogener Nutzungsdaten über die Dauer des Nutzungsvorgangs hinaus.

Im Hinblick auf das Eingeständnis der Beklagten zu Alternativmöglichkeiten, die sachliche Selbstwiderlegung des Beklagtenvortrags durch ihre eigene Praxis und die rechtliche Unerheblichkeit ist bislang darauf verzicht worden, auf die einzelnen Datennutzungen des Bundesverwaltungsamts einzugehen und im Einzelnen zu widerlegen, dass anlasslos protokollierte IP-Adressen zur Aufrechterhaltung des Betriebs oder der Systemsicherheit erforderlich seien. Nachdem das Hohe Gericht die von der Beklagten beschriebenen „Angriffsszenarien und Sicherheitsmaßnahmen“ nunmehr für erheblich zu halten scheint, soll dazu näher Stellung genommen werden.

Vorab ist darauf hinzuweisen, dass hier alleine die Sicherheit sogenannter Webserver der Beklagten in Rede steht, also von Systemen zur Bereitstellung von Telemedien. Gegenstand der Klage ist nämlich allein die Benutzung öffentlicher Telemedien der Beklagten durch den Kläger. Webserver sind andere Computer als diejenigen, welche die Mitarbeiter der Beklagten am Arbeitsplatz oder für eigene Zwecke (z.B. E-Mail-Server) einsetzen. Die Sicherheit dieser anderen Systeme und die dazu erforderlichen Maßnahmen sind für das vorliegende Verfahren irrelevant. Auf Webservern dürfen laut BSI andere Anwendungen nicht vorhanden sein. [5] Der Webserver muss dementsprechend von anderen Rechnern der Beklagten getrennt und abgeschottet sein, so dass die zuständigen Mitarbeiter der Beklagten zwar auf den Webserver zugreifen können, dass umgekehrt von dem Webserver aus aber kein Zugriff auf andere

[5] BSI, IT-Grundschutzkatalog „M4 Hardware und Software“, M 4.97: „Ein Dienst pro Server“, https://www.bsi.bund.de/cln_174/ContentBSI/grundschutz/kataloge/m/m04/m04097.html.

Systeme der Beklagten möglich ist. Dies im Blick, werden im folgenden die von der Beklagten angeführten „Angriffsszenarien“ bewertet.

a) Anomalieerkennungssystem

Die Beklagte trägt vor, das Bundesverwaltungsamt setze zur Erkennung von Verfügbarkeitsangriffen („DoS-Angriffe“) ein „Anomalieerkennungssystem“ ein, das protokollierte IP-Adressen verarbeite.

Zur Bereitstellung der Telemedien der Beklagten (§ 15 Abs. 1 TMG) ist dieses System unstreitig nicht erforderlich, aber auch nicht zur Erkennung von Verfügbarkeitsstörungen:

- Um Verfügbarkeitsstörungen zu erkennen, genügt die Erhebung **anonymer Daten**. Schon aus der bloßen Anzahl der in einem bestimmten Zeitraum erfolgten Zugriffe, welche die Behörde ohne Verstoß gegen § 15 TMG erheben darf, lassen sich technische Störungen erkennen, ohne dass dazu personenbezogen – gar flächendeckend und permanent – aufzeichnet werden müsste, wer welche Internetseiten aufgerufen, Suchworte eingegeben und Forenbeiträge geschrieben hat.
- Verfügbarkeitsstörungen können auch dadurch erkannt werden, dass die Beklagte regelmäßig **Testverbindungen** zu ihren Angeboten herstellt oder herstellen lässt. Auch diese Möglichkeit erfordert die Erhebung personenbezogener Daten des Klägers nicht.
- Erfolglos versuchte Verfügbarkeitsstörungen („**Angriffe**“), die ohne Auswirkung auf die Verfügbarkeit des Telemediums bleiben, brauchen nicht erkannt zu werden.
- Verfügbarkeitsangriffe können nicht verhindert werden, indem man Daten sammelt. Vielmehr muss die von der Beklagten genutzte **Hardware und Software** so eingerichtet werden, dass solche Angriffe erfolglos bleiben. Der Einsatz dieser Verfahren und Technologien bei den Bundesbehörden erfolgt bereits heute und ist mit keinem Grundrechtseingriff verbunden. In einer Entschließung vom 06./07.11.2008 führt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder zutreffend aus: „Es ist daher nicht erforderlich, zur Gewährleistung der Netz- und Informationssicherheit einzelfallunabhängig personenbezogene Verkehrsdaten zu speichern. Die Anbieter von Telekommunikationsdiensten sind aufgefordert, ihre Systeme so sicher zu gestalten, dass Angriffe von vornherein erfolglos bleiben.“ [6]
- Da diese Verfahren zur „Härtung“ von Informationstechnik ohnehin eingesetzt werden müssen und die Ausnutzung bekannter Sicherheitslücken verhindern, verbleiben für weitere Maßnahmen nur noch unbekannte Angriffswege. Die automatisierte Auswertung von Kommunikations- und Informationsprotokollen ist denkbar schlecht geeignet, unbekannte Angriffswege aufzudecken. Der Diplominformatiker Dirk Fox, Geschäftsführer eines Beratungsunternehmens für IT-Sicherheit, führt dazu aus: [7] Das beobachtbare Kommunikationsverhalten unterliege starken „Schwankungen“, die sich von Anomalien praktisch nicht unterscheiden ließen und daher in erheblichem Ausmaß **Fehlalarme** auslösten. Fehlalarme

[6] http://www.datenschutz.hessen.de/k76.htm#entry2919.

[7] Fox, DuD 2005, 422.

binden laut Fox so viele Ressourcen, dass eine gezielte Sicherheitsarbeit insgesamt eher behindert wird. Wegen der Fehlalarme seien viele Erkennungssysteme schon deaktiviert worden oder ihre Meldungen würden nicht mehr beachtet. Viele Angriffe (z.B. Trojaner) entfalteten zudem ein Kommunikationsverhalten, das die Alarmierungsschwelle nicht überschreite, da es von „normalem“ Nutzungsverhalten nicht unterschieden werden könne. Auffällige Angriffe hingegen, wie z.B. die eine massive Auslastung und Verlangsamung von Servern verursachende DoS-Attacken, bemerke man auch ohne personenbezogene Protokollierung. Insgesamt bleibe der Einsatz von „Einbruchserkennungsvorrichtungen“ „ohne einen erkennbaren Sicherheitsgewinn“. [8]

- **Das BSI selbst** bewertet „Einbruchserkennungssysteme“ öffentlich mit den folgenden Worten: „Die Wahl der Parametereinstellung ist äußerst kritisch und kann leicht zu Fehlalarmen bzw. zum Übersehen von Angriffen führen. Es werden keine klaren Aussagen getroffen; es kann lediglich von einer Wahrscheinlichkeit für einen Angriff gesprochen werden. Anomalieerkennung ist derzeit noch Gegenstand der aktuellen Forschung und weit von der praktischen Einsetzbarkeit entfernt.“ [9]
- Im **Leitfaden des BSI** für die Einführung von Intrusion-Detection-Systemen heißt es zu Telemedien-Angeboten im Internet: „Allgemeine Informationsbereitstellung über statische Webseiten [...] In diesem Szenario werden auf einem Webserver Informationen zum Abruf über das Internet bereitgestellt. [...] Die Betrachtung der Einflussgrößen zeigt, dass in diesem Szenario der sicherheitstechnische Zusatznutzen bei Einsatz eines IDS eher gering ist. [...] Typische Angriffe auf Webserver nutzen entweder Schwächen der Serverprogramme oder Schwachstellen bei der Realisierung dynamischer Inhalte aus. Bei einer rein statischen Bereitstellung von Daten kann ein angemessener Schutz des Webangebots in der Regel mit bestehenden Mitteln realisiert werden. Bestehende Restrisiken sind auch ohne Einsatz eines IDS tolerierbar.“ [10]
- Gegenmaßnahmen unter Anknüpfung an die Quelle einer Überflutung sind schon deshalb untauglich, weil Verfügbarkeitsangriffe heutzutage über eine Vielzahl – mitunter Hunderttausende („**Farming**“) – von Quellen (Servern) erfolgen.

In den **Empfehlungen des BSI** zum Schutz vor verteilten Denial of Service-Angriffen im Internet werden unter anderem die folgenden Maßnahmen vorgeschlagen: [11]

- Einsatz von **Paketfiltern** bei Serverbetreibern
- Etablierung eines **Notfallplans**
- Sichere **Konfiguration** der Server
- Restriktive **Rechtevergabe** und Protokollierung
- Einsatz von **Open-Source-Produkten**
- Auswahl geeigneter und IT-sicherheitsbewußter **Serverbetreiber**
- Vermeidung **aktiver Inhalte**
- Tägliche **Überprüfung** von Dateien auf Viren und Angriffsprogrammen

[8] Fox, DuD 2005, 422.

[9] https://www.bsi.bund.de/cln_136/ContentBSI/Themen/sinet/Uebersicht/angriff.html.

[10] https://www.bsi.bund.de/cae/servlet/contentblob/486992/publicationFile/30698/Leitfadenv10_pdf.pdf.

[11] https://www.bsi.bund.de/cln_136/ContentBSI/Themen/sinet/Gefaehrdungen/DDoSAngriffe/ddos.html.

- Zuverlässiger und aktueller **Virenschutz** und das Abschalten aktiver Inhalte im Browser, ggf. auch der Einsatz von Hilfsprogrammen zum Online-Schutz des Clients (beispielsweise PC-Firewalls)
- **IT-Grundschutz** für Rechner mit Internet-Anschluss
- Zeitnahes Einspielen von **Sicherheits-Updates**
- Tool-Einsatz und **Schulung** der Mitarbeiter

Keine dieser Schutzmaßnahmen erfordert die Aufzeichnung der IP-Adressen der Nutzer öffentlicher Telemedien der Beklagten. Auch soweit eine „automatische Angriffserkennung“ durch ständige Überwachung typischer Kennwerte (Speicherauslastung, Stacks, Netzauslastung, …) empfohlen wird, sind dazu ausschließlich anonyme Daten erforderlich und nicht etwa personenbeziehbare Daten.

b) Sperrlisten

Die Beklagte trägt vor, das Bundesverwaltungsamt speichere IP-Adressen, von denen möglicherweise Angriffe ausgehen, um sie gegebenenfalls auf eine Sperrliste zu setzen.

Zur Bereitstellung der Telemedien der Beklagten (§ 15 Abs. 1 TMG) ist die Sperrung von IP-Adressen unstreitig nicht erforderlich, aber auch nicht zur Abwehr von Einbrüchen in Webserver:

- Zum wirksamen Schutz vor Angriffen muss die von der Beklagten genutzte **Hardware und Software** so eingerichtet werden, dass solche Angriffe erfolglos bleiben. Der Einsatz dieser Verfahren und Technologien bei den Bundesbehörden erfolgt bereits heute und ist mit keinem Grundrechtseingriff verbunden. In einer Entschließung vom 06./07.11.2008 führt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder zutreffend aus: „Es ist daher nicht erforderlich, zur Gewährleistung der Netz- und Informationssicherheit einzelfallunabhängig personenbezogene Verkehrsdaten zu speichern. Die Anbieter von Telekommunikationsdiensten sind aufgefordert, ihre Systeme so sicher zu gestalten, dass Angriffe von vornherein erfolglos bleiben.“ [12]
- In den meisten Fällen ist die Erhebung der **IP-Adressen von Telemediennutzern** schon deshalb nicht zur Verhinderung unberechtigter Zugriffe erforderlich, weil unberechtigte Zugriffe nicht unter Nutzung eines Telemediums erfolgen. Ein Telemedium wird regelmäßig nur über bestimmte Zugänge bereit gestellt. Wer über andere Zugänge (Ports) versucht, in ein System einzudringen, ist nicht Nutzer des bereit gestellten Telemediums und genießt nicht den gesetzlichen Protokollierungsschutz. Im Bereich von Zugängen, über die kein Telemedium bereit gestellt wird, kann die Beklagte daher auch ohne Protokollierung der IP-Adressen unschuldiger Surfer nach Maßgabe des Bundesdatenschutzgesetzes angemessene Vorkehrungen zum Schutz ihrer Systeme treffen.
- Die nachträgliche Sperrung einer IP-Adresse ist **sinnlos**: War der Angriff erfolgreich, kommt eine Sperrung zu spät. War er erfolglos, ist die Sperrung überflüssig.

[12] http://www.datenschutz.hessen.de/k76.htm#entry2919.

- Einbrüche in Webserver können nicht verhindert werden, indem man nachträglich IP-Adressen sperrt, von denen frühere Angriffe ausgegangen sind. Eine Sperrung der für einen Angriff eingesetzten Quelle (IP-Adresse) ist untauglich, weil eine beliebige Vielzahl anderer Rechner zur Fortsetzung der Zugriffsversuche eingesetzt werden können. Es gibt über **40 Mrd. nutzbare IP-Adressen** im Internet. Ernsthafte Angreifer, die überhaupt nur Schaden anrichten können, werden durch Sperrung einer IP-Adresse nicht abgehalten. Man stelle sich die Webserver der Beklagten als ein Gebäude mit 40 Mrd. Eingängen vor: Einen dieser Eingänge zu sperren, stoppt Eindringlinge offensichtlich nicht.

Soweit die Beklagte vorträgt, die von ihr beschriebenen Angriffe erfolgten wöchentlich, so sind die ohne Besucherprotokollierung betriebenen Webserver der Beklagten ebenso häufig Ziel derartiger Angriffe, ohne dass die unterlassene Protokollierung negative Auswirkungen auf Integrität, Vertraulichkeit oder Verfügbarkeit dieser Webserver hätte.

c) Drittmeldungen

Erhält das Bundesverwaltungsamt die Information, von bestimmten IP-Adressen seien Angriffe ausgegangen, überprüft es angeblich anhand seiner Surfprotokolle, auf welche seiner eigenen Server in der Vergangenheit Zugriffe dieser IP-Adressen verzeichnet wurden, um diese Server zu „bereinigen“ und die IP-Adressen zu sperren.

Zur Bereitstellung der Telemedien der Beklagten (§ 15 Abs. 1 TMG) ist dieses Verfahren unstreitig nicht erforderlich, aber auch nicht zur Abwehr von Gefahren und Beseitigung von Störungen der Webserver:

- Ist der von dritter Seite gemeldete Angriff unter Ausnutzung einer **Sicherheitslücke** erfolgt, so muss diese auf allen Webservern der Beklagten geschlossen werden und nicht nur auf bereits betroffenen Servern; ein derart beschränktes Vorgehen wäre unverantwortlich. Vor diesem Hintergrund muss nicht nachvollziehbar sein, ob in der Vergangenheit von bestimmten IP-Adressen auf bestimmte Server zugegriffen wurde.
- Ist im Wege des gemeldeten Angriffs ein neues **Schadprogramm** eingebracht oder sind sonst Veränderungen vorgenommen worden, so müssen alle Systeme der Beklagten darauf überprüft und dagegen abgesichert werden und nicht nur einzelne Server; ein solch beschränktes Vorgehen wäre unverantwortlich.
- Die Sperrung von dritter Seite gemeldeter IP-Adressen ist aus den zu Punkt b) ausgeführten Gründen nicht geeignet und erforderlich und kann im Übrigen **auch ohne eigenen Protokollierung** von IP-Adressen durch die Beklagte erfolgen.

d) Automatisches Analysesystem

Die Beklagte trägt vor, das Bundesverwaltungsamt verwende ein automatisches Analysesystem, das anhand von Zugriffsprotokollen verdächtige Zugriffe erkenne, melde und blockiere. Auf diese Weise könne die Ausnutzung von Sicherheitslücken verhindert werden.

Weshalb solche „Einbruchserkennungssysteme“ zur Abwehr von Einbrüchen nicht geeignet, erforderlich und verhältnismäßig sind, ist bereits oben zu Punkt a) dargestellt worden. Auf die dortigen Ausführungen wird Bezug genommen.

Soweit die Beklagte vorträgt, die von ihr beschriebenen Angriffe erfolgten mindestens monatlich, so sind die ohne Besucherprotokollierung betriebenen Webserver der Beklagten ebenso häufig Ziel derartiger Angriffe, ohne dass die unterlassene Protokollierung negative Auswirkungen auf Integrität, Vertraulichkeit oder Verfügbarkeit dieser Webserver hätte.

e) Schadprogramme

Die Beklagte trägt vor, das Bundesverwaltungsamt erkenne Schadprogramme zur Weiterleitung von Angriffen (Bots) anhand ungewöhnlicher Einträge in Zugriffsprotokollen.

Zur Bereitstellung der Telemedien der Beklagten (§ 15 Abs. 1 TMG) ist dieses Verfahren unstreitig nicht erforderlich, aber auch nicht zur Abwehr von Gefahren und Beseitigung von Störungen der Webserver:

- Die Ausführung von Schadprogrammen auf Webservern kann nicht verhindert werden, indem man Daten sammelt. Vielmehr muss die von der Beklagten genutzte **Hardware und Software** so eingerichtet und in Stand gehalten werden, dass Versuche zur Einschleusung von Schadprogrammen erfolglos bleiben. Der Einsatz dieser Verfahren und Technologien bei den Bundesbehörden erfolgt bereits heute und ist mit keinem Grundrechtseingriff verbunden.
- Um gleichwohl eingeschleuste Schadprogramme auf Webservern zu erkennen, ist eine Protokollierung der Telemediennutzung kaum geeignet, jedenfalls nicht erforderlich. Es genügt nämlich, die vom BSI empfohlene „**regelmäßige Integritätsprüfung**“ durchzuführen.[13] Bei diesem Verfahren wird der Webserver regelmäßig, beispielsweise jede Nacht, auf Veränderungen überprüft (z.B. Dateiänderungen, Prozessänderungen, Konfigurationsänderungen). Modifikationen werden erkannt, indem die vorher erstellte kryptographische Prüfsumme mit der aktuell berechneten Prüfsumme verglichen wird. Auf diese Weise kann eingebrachte Schadsoftware früher und effektiver erkannt werden als zu versuchen, aus dem Heuhaufen des gesamten Datenverkehrs die Nadel der Außenkommunikation von Schadprogrammen herauszusuchen, zumal viele Schadprogramme nicht nach außen kommunizieren.
- Ferner ist als milderes und wirksameres Mittel **Software zum Auffinden** bekannter Schadprogramme verfügbar (z.B. Virenerkennung, Schadsoftwareerkennung).
- Vor dem Innenausschuss des Deutschen Bundestages hat der Sachverständige Prof. Dr. Hartmut Pohl, der Inhaber eines Lehrstuhls für **Informationssicherheit** der Hochschule Bonn-Rhein-Sieg ist, zu § 5 BSIG zutreffend ausgeführt: [14] „Das Gesetz erweckt den Eindruck, als würden diese

[13] BSI, IT-Grundschutzkatalog „M4 Hardware und Software“, M 4.93: „Regelmäßige Integritätsprüfung“, https://www.bsi.bund.de/cln_174/ContentBSI/grundschutz/kataloge/m/m04/m04093.html.

[14] Pohl, Protokoll Nr. 16/94 der Anhörung am 11.05.2009, http://www.bundestag.de/ausschuesse/a04/anhoerungen/Anhoerung_21/Protokoll.pdf, 15 f.

Schadprogramme vom Himmel fallen und würden uns überfluten. Das ist ein völlig falscher Eindruck. Schadprogramme können nur Schaden anrichten, wenn sie tatsächlich eine Sicherheitslücke ausnutzen. Wenn die Sicherheitslücke geschlossen ist, dann nutzt auch ein Schadprogramm nichts. Ein aktuelles Beispiel ist der schon erwähnte Conficker-Wurm, der eine Sicherheitslücke, die längst gepatcht und korrigiert war, ausnutzte und deswegen Schaden anrichten konnte, weil viele Anwender die Fehlerkorrekturen nicht eingefahren haben. Eine Diskussion von Schadprogrammen, wie sie im Gesetzentwurf vorgesehen ist, die Untersuchungen und der Versuch, sie abzuwehren, ist aus meiner Sicht völlig nutzlos und kratzt an der Oberfläche der Informationssicherheit. Wir müssen uns an die Ursachen halten. Die Ursache ist jeweils eine Sicherheitslücke, zu der eine ganze Reihe von Schadprogrammen zugeordnet werden können und die Schadprogramme können dann diese Sicherheitslücke ausnutzen. Die Diskussion über Schadprogramme ist überflüssig. Wir müssen uns auf die Sicherheitslücken konzentrieren. Das ist auch der Stand der Technik in Unternehmen, die sich nicht dazu verleiten lassen zu protokollieren, wer greift auf unsere Systeme wann zu und sendet etwas, sondern, wenn ein Angriff stattgefunden hat, wird nicht eruiert, wer der Täter ist, es wird eruiert, wo liegt die Sicherheitslücke, und die wird geschlossen. Das ist der Stand der Technik. Wenn ich ein Beispiel aus dem Brandschutz bringen darf: Wenn Sie sich hier umsehen, es werden Sicherheitsmaßnahmen ergriffen, im Schrank ist ein Feuerlöscher, es gibt eine Sprinkleranlage, die Decke ist schwer entflammbar – selbst wenn es hier brennt, geht der Brand nicht aus dem Raum hinaus. Ganz wichtig, Sie sehen auch die Hinweise auf die Fluchtwege, wir kommen noch hinaus – auch wenn es hier brennt, der Brand geht nicht in die anderen Räume. Sie würden sehr lachen, wenn jemand fordert, wir wollen vor dem Raum eine Videokamera aufstellen und kontrollieren, protokollieren, auswerten und speichern, wer in den Raum hinein- und wer hinausgeht. Das ist kein Brandschutz, das ist Überwachung."

In den **Empfehlungen des BSI** zum Schutz vor Schadprogrammen werden unter anderem die folgenden Maßnahmen vorgeschlagen: [15]

- Einsatz regelmäßig aktualisierter **Viren-Schutzprogramme**
- Alle **von Dritten erhaltenen Dateien** und Programme sollten vor der Aktivierung auf möglicherweise enthaltene Schadprogramme überprüft werden.
- Schadprogramme verfolgen häufig den Zweck, **Passwörter** oder andere Zugangsdaten auszuspähen. Daher sollten Passwörter nie auf den IT-Systemen abgespeichert werden.
- Grundsätzlich sollten alle Programme vor Installation und Freigabe auf **Testsystemen** hinsichtlich der Funktionssicherheit und hinsichtlich eines Befalls durch Schadprogramme überprüft werden.
- Bei **CERTs** bzw. anderen sicherheitsbezogenen Informationsdiensten sollte regelmäßig recherchiert werden, ob eingesetzte Programme dahingehend aufgefallen sind, dass sie Daten vom IT-System des Benutzers ohne dessen Wissen an andere IT-Systeme übertragen.
- Einsatz von **Paketfiltern** (Firewalls).
- Einschränkung von **Benutzerrechten**.

[15] BSI, IT-Grundschutzkatalog „M2 Organisation", M 2.224: „Vorbeugung von Schadprogrammen", https://www.bsi.bund.de/cln_183/ContentBSI/grundschutz/kataloge/m/m02/m02224.html.

- Interne **Abschottung** von Netzwerken.

Keine dieser Schutzmaßnahmen erfordert die Aufzeichnung der IP-Adressen der Nutzer öffentlicher Telemedien der Beklagten. Auch soweit eine „Beobachtung des Netzes“ empfohlen wird, sind dazu ausschließlich anonyme Daten erforderlich und nicht etwa personenbeziehbare Daten. Das BSI führt aus, häufig zeige sich die Aktivität von Schadprogrammen durch unerwünschten Datenverkehr. In Frage kämen insbesondere ungewöhnlich große übertragene Datenmengen, wiederholte Übertragungen in bestimmten Zeitintervallen oder eine auffällig ansteigende Anzahl zu übertragender E-Mails. [16] All dies kann bereits anhand anonymer Protokolle des ausgehenden Datenverkehrs festgestellt werden. Die IP-Adressen der Nutzer von Telemediendiensten mitzuschneiden, ist dazu nicht erforderlich.

Meinhard Starostik
Rechtsanwalt

[16] BSI, IT-Grundschutzkatalog „M2 Organisation“, M 2.224: „Vorbeugung von Schadprogrammen“, https://www.bsi.bund.de/cln_183/ContentBSI/grundschutz/kataloge/m/m02/m02224.html.