Meinhard Starostik

Rechtsanwalt

RA Starostik · Schillstraße 9 · 10785 Berlin

Landgericht Berlin
Littenstr. 12-12
10179 Berlin

Rechtsanwaltskanzlei:
Schillstraße 9 · 10785 Berlin
Tel.: 00 49 - 30 - 88 000 3 - 0
Fax: 00 49 - 30 - 88 000 346
Email: Kanzlei@Starostik.de
http://www.starostik.de
USt-ID-Nr. DE165877648

Zweigstelle und
Kanzlei vereidigter Buchprüfer:
Schwarzenberger Straße 7 · 08280 Aue
Tel.: 00 49 - 3771 - 564 700

Berlin, den 08.01.2013
Mein Zeichen: 45/08

Breyer ./. BRD
Aktenzeichen: 57 S 87/08

In vorbezeichneter Angelegenheit wird auf den Schriftsatz der Gegenseite vom 30.11.2012 und die Verfügung vom 11.12.2012 wie folgt Stellung genommen:

1. Zum Schriftsatz des Beklagtenvertreters vom 30.11.2012

1.1. Zum Personenbezug von IP-Adressen

In der neuen, 7. Auflage des von Prof. Dr. Dr. h.c. mult. Spiros Simitis herausgegebenen Standardkommentars zum Bundesdatenschutzgesetz heißt es unter § 3 Rn. 63: „Für die in den Logfiles der Anbieter von Telemediendiensten, so von Webseitenbetreibern oder Suchmaschinen, enthaltenen mit IP-Nummern verknüpften Daten über die Internet-Nutzung ist der Personenbezug ebenfalls zu bejahen [...] Eine Zusammenführung der Web-Nutzungsdaten mit solchen Daten, die eine Personenbestimmung ermöglichen, ist jedenfalls nicht mit so hoher Wahrscheinlichkeit ausgeschlossen, dass der Aufwand unverhältnismäßig erscheint und vernünftigerweise nicht in Betracht kommt."

Der von der Beklagten zitierte Entwurf einer EU-Datenschutzgrundverordnung ist für den vorliegenden Rechtsstreit unerheblich, weil er kein geltendes Recht darstellt. Im Übrigen stellt auch dieser Entwurf den Personenbezug der streitbefangenen Daten nicht in Frage. Der Begriff der „personenbezogenen Daten" soll danach alle Informationen umfassen, „die sich auf eine betroffene Person beziehen". „Betroffene Person" soll eine bestimmte natürliche Person oder eine natürliche Person sein, „die direkt oder indirekt mit Mitteln bestimmt werden kann, die der für die Verarbeitung Verantwortliche oder jede sonstige natürliche oder juristische Person nach allgemeinem Ermessen aller Voraussicht nach einsetzen würde, etwa mittels Zuordnung zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen". Eine Identifizierungsmöglichkeit durch „jede sonstige natürliche oder juristische Person", etwa durch den Internet-Zugangsanbieter oder durch eine Eingriffsbehörde, soll also auch weiterhin den Personenbezug des von der Beklagten aufgezeichneten Internet-Nutzungsverhaltens begründen.

Mit Urteil vom 24.11.2011 (Az. C-70/10) hat der EuGH dementsprechend ausgeführt: „Zum einen steht nämlich fest, dass die Anordnung, das streitige Filtersystem einzurichten, eine systematische Prüfung aller Inhalte sowie die Sammlung und Identifizierung der IP-Adressen der Nutzer bedeuten würde, die die Sendung unzulässiger Inhalte in diesem Netz veranlasst haben, wobei es sich bei diesen Adressen um personenbezogene Daten handelt, da sie die genaue Identifizierung der Nutzer ermöglichen." Auch der EuGH sieht IP-Adressen also als personenbezogene Daten an, wenn sie „die genaue Identifizierung der Nutzer ermöglichen", ohne dass eine Identifizierungsmöglichkeit speziell durch die speichernde Stelle gefordert wird.

Ferner soll noch einmal darauf hingewiesen werden, dass IP-Adressen der Klägers auch anders als über dessen Internet-Zugangsanbieter identifiziert werden können, nämlich wenn beispielsweise bei Bestellungen durch den Kläger oder bei der Nutzung anderer Dienste (z.B. E-Mail) dessen Identitätsdaten erhoben werden und gleichzeitig seine IP-Adresse gespeichert wird. Dies ist bei einer Vielzahl von Diensten der Fall.

Entgegen der Darstellung des Beklagtenvertreters hat das OLG Hamburg mit Beschluss vom 03.11.2010 (Az. 5 W 126/10) keineswegs festgestellt, dass dynamische IP-Adressen nur für Internet-Zugangsanbieter personenbezogene Daten darstellten. Das Gericht hat lediglich festgestellt, ein Personenbezug von IP-Adressen könne „ohne weitere Zusatzinformationen nicht hergestellt werden". Dies trifft in den meisten Fällen zu, steht der Einordnung als personenbezogenes Datum indes nach dem gesetzlichen Begriff der Bestimmbarkeit nicht entgegen.

Vollkommen verfehlt ist auch die Behauptung des Beklagtenvertreters, der Bundesgerichtshof habe mit Urteil vom 12.05.2010 (Az. I ZR 121/08) festgestellt, dass eine IP-Adresse kein personenbezogenes Datum darstelle. Der Bundesgerichtshof hat in dieser Entscheidung aufgeführt, der IP-Adresse komme „keine mit einem eBay-Konto vergleichbare Identifikationsfunktion zu". Anders als letzteres sei sie keinem konkreten Nutzer zugeordnet, sondern nur einem Anschlussinhaber. Die IP-Adresse gebe deshalb bestimmungsgemäß keine zuverlässige Auskunft über die Person, die zu einem konkreten Zeitpunkt einen bestimmten Internetanschluss nutzt. Diese Feststellung ist zutreffend, ändert aber nichts daran, dass die IP-Adresse ein auf die Person des Anschlussinhabers bezogenes Datum darstellt. Dies genügt zur Begründung des Personenbezugs. Im Übrigen ist bereits ausgeführt worden, dass der Kläger die Telemedien der Beklagten über einen Internetzugang nutzt, der auf seinen Namen registriert ist. Der Kläger ist also Anschlussinhaber.

Was schließlich das Urteil des BGH vom 13.01.2011 (Az. III ZR 146/10) angeht, ist bereits ausgeführt worden, dass der dort angewandte § 100 TKG für die von der Beklagten bereit gestellten Telemedien nicht einschlägig ist. Im Übrigen hat der Bundesgerichtshof die Erforderlichkeit einer IP-Protokollierung durch Internet-Zugangsanbieter in dieser Entscheidung offen gelassen und den Rechtsstreit an die Vorinstanz zurückverwiesen. Der Entscheidung des Bundesgerichtshofs kann auch in der Sache nicht gefolgt werden, wie an anderer Stelle ausgeführt worden ist.[1]

1.2. Zum Schriftsatz vom 30.11.2012 im Übrigen

Entgegen der Darstellung des Beklagtenvertreters sind die „Guidelines on Securing Public Web Servers" des US-amerikanischen „National Institute of Standards and Technology" keineswegs „international anerkannt". Es handelt sich um eine nationale US-amerikanische

1 Im Einzelnen Breyer, MMR 2011, 573.

Richtlinie, die vor dem Hintergrund zu sehen ist, dass die USA kein Datenschutzrecht im europäischen Sinne kennen. Immerhin findet sich selbst in dieser Richtlinie der Hinweis, dass die Aufbewahrung von Nutzungsprotokollen von den gesetzlichen Vorgaben („legal requirements") abhänge.[2] Im Übrigen datiert die Richtlinie aus dem Jahr 2007 und ist mithin nicht aktuell. Die tatsächlichen nationalen und internationalen Standards aktuellen Datums sind bereits in früheren Schriftsätzen dargestellt worden.

Soweit die Beklagte erneut behauptet, Sicherungsmaßnahmen ohne Protokollierung der Internetnutzung seien „nicht ausreichend", fällt sie erstens hinter ihr eigenes gegenteiliges Zugeständnis in früheren Schriftsätzen zurück, setzt sie sich zweitens aber auch in Widerspruch zu der Vielzahl von Internetportalen, welche sie selbst dauerhaft ohne IP-Totalprotokollierung anbietet.

Unglaublich ist die Unterstellung des Beklagtenvertreters, der gerichtliche Sachverständige habe eine detaillierte Ermittlung der Kosten alternativer Schutzmaßnahmen unterlassen, um das Prozessrisiko des Klägers gering zu halten. Der Kläger kennt den Sachverständigen nicht einmal und weist solche Unterstellungen schärfstens zurück. Der Sachverständige hat vielmehr überzeugend ausgeführt, dass sich die zusätzlichen Kosten für angemessene Schutzmaßnahmen seitens der Beklagten auf 0 belaufen. Es entstehen keine zusätzlichen Kosten, weil die Beklagte unstreitig und in jedem Fall angemessene Schutzmaßnahmen einzusetzen hat, welche eine totale IP-Protokollierung nicht voraus setzen. Durch Unterlassen der gesetzlich verbotenen IP-Protokollierung werden also keine zusätzlichen anderen Maßnahmen erforderlich. Damit ist die Beweisfrage beantwortet.

2. Zum „Gutachten" des Prof. Martini

2.1. Zur Einordnung des „Gutachtens"

Die Beklagte hält dem gerichtlichen Sachverständigengutachten ein eigenes Auftragsgutachten entgegen. Solche Parteigutachten sind nach der Rechtsprechung als bloßer Parteivortrag einzuordnen. Gerade im vorliegenden Fall ist das Auftragsgutachten keineswegs mit der unvoreingenommenen Prüfung durch den gerichtlich bestellten Gutachter vergleichbar:

Erstens dürfte Prof. Martini von Anfang an der Auftrag erteilt worden sein, ein „Privat(gegen)gutachten" zu dem gerichtlichen Gutachten zu erstellen (siehe Titelblatt des Auftragsgutachtens). Dem Gutachter war also das Ergebnis seiner Begutachtung bereits vorgegeben.

Zweitens dürfte Prof. Martini für das Auftragsgutachten großzügig entlohnt worden sein, was die Beklagte wiederum nicht offen legt.

Drittens gewährleistet Prof. Martini von seiner beruflichen Tätigkeit her eine unvoreingenommene, neutrale Prüfung nicht. Prof. Martini leitet das Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE. Dieses Institut ist nach eigenen Angaben „langjähriger technologischer Forschungspartner der Bundeswehr".[3] Es schreibt auf seiner Internetpräsenz: „Wollte man das Engagement des Fraunhofer FKIE für die Bundeswehr auf eine Formel bringen, könnte man es auch als das Institut für Vernetzte Operationsführung (NetOpFü) bezeichnen. Darunter versteht man Assistenzsysteme, die allen an einem Einsatz beteiligten Akteure ein schnell verfügbares, einheitliches Lagebild verschaffen

2 Abschnitt „9.1.4 Reviewing and Retaining Log Files".
3 http://www.fkie.fraunhofer.de/de/ueber-uns/zielgruppen.html.

und ihnen damit die Grundlage für eine profunde und erfolgreiche Entscheidungsfindung sichern. [...] Als kompetenter Partner des Verteidigungsministeriums sowie der nachgeordneten Bereiche vertritt das FKIE die Bundesrepublik Deutschland in zahlreichen internationalen Gremien und nimmt damit in ausgewählten Bereichen auch hoheitliche Aufgaben wahr." Das FKIE ist ferner Mitglied im „Fraunhofer-Verbund Verteidigungs- und Sicherheitsforschung". Es schreibt dazu: „Dem Bundesministerium für Bildung und Forschung (BMBF) und dem Bundesministerium der Verteidigung (BMVg) verpflichtet, hat sich der Verbund inzwischen als treibende Kraft im ganzen Verteidigungs- und Sicherheitsbereich durchgesetzt."[4]

Prof. Martini leitet ein Institut, dessen „Kernkompetenz" nach eigenen Angaben „Wehrtechnische Systeme zur vernetzen Operationsführung" sind.[5] Das Institut – und damit auch dessen Leiter – wurde bis 2009 vollständig vom Bundesverteidigungsministerium finanziert und wird auch heute noch weitgehend aus Bundesmitteln finanziert (die Grundfinanzierung erfolgt inzwischen durch das Bundesforschungsministerium). Es denkt von militärischen Aufklärungsbedürfnissen her, die mit dem Betrieb öffentlicher Telemedien nichts zu tun haben. Es sieht sich als Teil des bundesdeutschen Verteidigungs- und Sicherheitskomplexes, vertritt die Bundesrepublik gar in Gremien und nimmt hoheitliche Aufgaben wahr.

Prof. Martini verantwortet, dass das FKIE selbst jegliche rechtmäßige Nutzung seiner Internetpräsenz mit IP-Adresse des Nutzers protokolliert. Er hat das Gutachten also quasi in eigener Sache erstellt. Dies gilt auch, soweit Gegenstand seiner Forschung gerade die streitbefangenen Überwachungstechniken der Beklagten sind (z.B. „Intrusion Detection"). Nachvollziehbarerweise hat der Auftragsgutachter kein Interesse daran, dass der Einsatz der von ihm erforschten, entwickelten und angewandten Technologien für unzulässig erklärt wird.

All dies macht deutlich, dass das Auftragsgutachten ebenso gut als Schriftsatz der Beklagten selbst hätte vorgelegt werden können.

2.2. Zum Inhalt des „Gutachtens"

Dementsprechend wenig unterscheidet sich die Argumentation des Auftragsgutachters von der Argumentation der Beklagten selbst in früheren Schriftsätzen. Zur Entlastung des Gerichts soll deshalb nur auf diejenigen Teile des Auftragsgutachtens eingegangen werden, die über den bisherigen Vortrag der Beklagten hinaus gehen. Im Übrigen genügt die Bezugnahme auf den früheren Vortrag des Klägers, der auf die Behauptungen der Beklagten bereits eingegangen ist (z.B. zu Verfügbarkeitsangriffen, zur Identifizierung von Angreifern, zur automatischen Angriffserkennung bzw. automatischen Analysesystemen), etwa mit Schriftsatz vom 9. Juni 2010.

Das Auftragsgutachten nimmt Bezug auf einen „2011 Top Cyber Security Risks Report" der US-amerikanischen Firma Hewlett Packard. Dieser Bericht bezieht sich nur auf Internetpräsenzen von Unternehmen, nicht von staatlichen Einrichtungen. Ferner ist es falsch, dass die Zahl der bekannten Sicherheitslücken auf ca. 2.000 im Jahr 2011 gesunken sei. Richtig ist, dass einer Datenbank im Jahr 2011 ca. 2.000 Sicherheitslücken gemeldet worden sind. Diese Zahl sagt nichts über das Fortbestehen der Sicherheitslücken aus. Normalerweise werden bekannt gewordene Sicherheitslücken vom Hersteller behoben und erst dann veröffentlicht. Es ist also davon auszugehen, dass alle in der Datenbank registrierten Sicherheitslücken namhafter Hersteller geschlossen sind. Grob irreführend ist es daher, von einer ho-

4 http://www.fkie.fraunhofer.de/de/ueber-uns/verbuende-und-allianzen.html.
5 http://www.fkie.fraunhofer.de/de/ueber-uns.html.

hen Zahl an bekannten Sicherheitslücken zu sprechen, ohne offenzulegen, dass sich diese Zahl vor allem auf alte, nicht aktualisierte Softwareversionen bezieht. Auch soweit der HP-Bericht und der Auftragsgutachter von fortbestehenden Sicherheitslücken bei „sehr vielen der heutigen attraktiven Web-Präsenzen" spricht, wird verkannt, dass die untersuchten kommerziellen US-amerikanischen Internetpräsenzen eben nicht unter den der Beklagten zumutbaren Sicherheitsgesichtspunkten betrieben und in Stand gehalten werden, sondern dort oftmals längst bekannte und geschlossene Sicherheitslücken fortbestehen.

Soweit der Auftragsgutachter eine Sicherheitslücke des Betriebssystems „Windows" anführt, handelt es sich dabei nicht um eine Software zur Bereitstellung von Telemedien. Die meisten aktiven Webserver setzen die Software „Apache" ein, die nicht unter Windows läuft.

Soweit der Auftragsgutachten von Angriffen auf Client-Systeme spricht, stellt ein Webserver zur Bereitstellung von Telemedien kein Client-System dar. Client-Systeme sind von Webservern strikt abzuschotten, wie auch das BSI empfiehlt.

Soweit der Auftragsgutachter „reaktive Maßnahmen" auch bei gut gesicherten Systemen für unverzichtbar hält, folgt daraus nicht die Erforderlichkeit einer Aufzeichnung des rechtmäßigen Nutzungsverhaltens des Klägers. In früheren Schriftsätzen ist bereits ausgeführt worden, dass eine Angriffserkennung ohne personenbezogene Aufzeichnung sämtlicher rechtmäßiger Zugriffe möglich ist (z.B. durch Beobachtung der Auslastung und regelmäßige Integritätsprüfung).

Der Auftragsgutachter nennt Alarmanlagen und Wachdienste als Sicherheitsmaßnahmen aus der „realen Welt". Diese Sicherheitsmaßnahmen beinhalten aber gerade nicht, dass sämtliche rechtmäßige Besucher eines öffentlichen Gebäudes registriert und Schritt für Schritt aufgezeichnet werden. Im Übrigen ist die Nutzung von Telemedien nicht mit dem Betreten eines fremden Gebäudes vergleichbar. Die Nutzung von Telemedien der Beklagten beschränkt sich auf den Abruf und die Übermittlung von Informationen. Sie ist der Nutzung anderer Medien vergleichbar (z.B. Printmedien, Rundfunk). Deswegen müssen Telemedien auch ebenso unbeobachtet und anonym genutzt werden können wie andere Medien.

Soweit der Auftragsgutachter die von Mitarbeiter-Computern ausgehenden Risiken anspricht, betrifft die vorliegende Klage nicht die Frage, ob und inwieweit die Nutzung von Mitarbeiter-Computern protokolliert werden darf. Der Kläger ist nicht Mitarbeiter der Beklagten.

Soweit der Auftragsgutachter behauptet, das Entdeckungsrisiko für Internetdelikte sei geringer als das Entdeckungsrisiko bei anderen Straftaten, ist das Gegenteil zutreffend. Dies zeigt der Vergleich der Aufklärungsraten für Internetbetrug einerseits und sonstigem Betrug andererseits, aber auch für Datenveränderung einerseits und Sachbeschädigung andererseits.

Dementsprechend falsch ist die Schlussfolgerung des Auftragsgutachters, bei Telemedien sei eine weiter reichende Nutzerüberwachung erforderlich als bei der Bereitstellung anderer Medien.

Soweit der Auftragsgutachter – wie zuvor schon die Beklagte – „reaktive Maßnahmen" beim Betrieb von Internetportalen beschreibt, ist dazu bereits umfassend Stellung genommen worden. Das Telemediengesetz erlaubt die Totalprotokollierung jeglicher Telemediennutzung aus guten Gründen nicht. Sie ist bereits nicht geeignet, die Sicherheit (Verfügbarkeit, Integrität und Vertraulichkeit) von Telemedienangeboten messbar zu erhöhen. Dies gilt ins-

besondere dann, wenn die verfügbaren alternativen Sicherheitsmaßnahmen ausgeschöpft werden. In jedem Fall steht der nicht nachzuweisende, nach Einschätzung des Gerichtsgutachters bestenfalls marginale Sicherheitsnutzen vollkommen außer Verhältnis zu den damit für Millionen rechtschaffener Nutzer verbundenen Datensicherheitsrisiken und Freiheits- und Unbefangenheitsverlusten bei der Nutzung öffentlicher Informationskanäle.

Soweit der Auftragsgutachter der Beklagten Fälle einer Erpressung der Betreiber von Internetportalen anführt, ist bereits angeführt worden, dass die vorliegende Klage die gesetzlichen Befugnisse der Strafverfolgungsbehörden unberührt lässt. Selbstverständlich können diese bei Verdacht einer Straftat gezielte Überwachungsmaßnahmen einleiten. Eine eigenmächtige Strafverfolgungsvorsorge durch Telemedienanbieter erlaubt § 15 TMG dagegen aus guten Gründen nicht, erst Recht keine anlasslose Vorratsdatenspeicherung der Internetnutzung. Soweit Verfügbarkeitsangriffe eingesetzt werden mögen, um Erpressungsversuchen zum Erfolg zu verhelfen, ist der richtige Umgang mit Verfügbarkeitsangriffen bereits dargestellt worden (Schriftsatz vom 09.06.2010, Punkt „Anomalieerkennungssystem").

Das Telemediengesetz bietet auch keine Grundlage dafür, IP-Adressen ohne Einwilligung von Nutzern aufzuzeichnen, um diese über angebliche Schadsoftware zu informieren oder informieren zu lassen. Das Gesetz überlässt dem Nutzer die Entscheidung, ob er in ein Aufspüren angeblicher Schadsoftware auf seinem Privatcomputern einwilligt oder nicht. Der Kläger willigt nicht ein und trifft eigene Maßnahmen zum Schutz vor Schadsoftware, die eine Aufzeichnung und Auswertung seiner Internetnutzung nicht erforderlich machen (siehe Schriftsatz vom 09.06.2010 unter „Schadprogramme"). Ohnehin genügt zur Erkennung infizierter Rechner der Einsatz von Fallen („Honeypots", „Spamtraps") durch Internet-Zugangsanbieter,[6] wie es etwa im Rahmen der sogenannten Anti-Botnetz-Initiative des Verbands der deutschen Internetwirtschaft eco e.V. (www.botfrei.de) geschieht. Der Einsatz solcher Fallen erfordert keine Protokollierung der Nutzung der Telemedien der Beklagten. (Übrigens protokolliert auch das Portal botfrei.de selbst keine personenbezogenen IP-Adressen der Nutzer.) Im Übrigen bleiben die Befugnisse der Strafverfolgungsbehörden bei Verdacht einer Datenveränderung, Computersabotage oder anderer Straftaten, wie sie mithilfe von Schadsoftware begangen werden können, unberührt.

Soweit der Auftragsgutachter eine pseudonymisierte Totalprotokollierung diskutiert, ist es für die vorliegende Klage unerheblich, ob die beklagtenseits praktizierte Surfprotokollierung verschlüsselt, pseudonymisiert oder anders erfolgt, da der Personenbezug in jedem Fall hergestellt werden kann. Der Klageantrag richtet sich gegen jede personenbezogene Nutzungsprotokollierung über die Nutzungsdauer hinaus.

3. Anhörung des Sachverständigen

Folgende Nachfragen sollen mündlich an den Sachverständigen gerichtet werden:

3.1. Mangelnde Eignung einer Totalprotokollierung zur Erhöhung der Sicherheit

Vorbemerkung zu allen Fragen: Soweit im Folgenden von einer Aufzeichnung von IP-Adressen oder des Internet-Nutzungsverhaltens die Rede ist, ist jede Art der personenbezogenen Speicherung über die Dauer des Übertragungsvorgangs hinaus gemeint, egal ob die Speicherung der IP-Adresse verschlüsselt, pseudonymisiert („gehasht") oder unverschlüsselt erfolgt.

6 Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2011, 10.

Vorbemerkung zur ersten Frage: Schutzziele der IT-Sicherheit sind die Gewährleistung der Verfügbarkeit, Unversehrtheit und Vertraulichkeit von Informationen.

1. Frage: Ist jemals von unabhängiger Seite die IT-Sicherheit eines fachgerecht eingerichteten und gewarteten Webservers mit der IT-Sicherheit eines vergleichbaren Webservers, der zusätzlich sämtliche Zugriffe samt IP-Adresse protokolliert und darauf aufbauende Maßnahmen (z.B. „Intrusion Detection Systems") einsetzt, über einen längeren Zeitraum empirisch miteinander verglichen worden?

2. Frage: Gibt es eine unabhängige empirische Studie, derzufolge eine unterschiedslose und anlasslose Protokollierung sämtlicher Zugriffe auf einen Webserver samt IP-Adresse sowie darauf aufbauende Maßnahmen zu einer signifikant (messbar) höheren Verfügbarkeit des Webservers oder zu signifikant (messbar) weniger Verletzungen der Unversehrtheit oder Vertraulichkeit des Systems führen?

3. Frage: Gibt es eine unabhängige empirische Studie, derzufolge durch den zusätzlichen Einsatz eines „Intrusion Detection"-Systems eine signifikant (messbar) höhere Verfügbarkeit eines Webservers oder eine signifikante (messbare) Verringerung der Zahl von Verletzungen der Unversehrtheit oder Vertraulichkeit des Systems erzielt werden konnte?

Vorbemerkung zur nächsten Frage: Sie führen in Ihrem Gutachten aus, die DIN ISO/IEC 27002:2008-09 empfehle eine Speicherung von IP-Adressen.

4. Frage: Trifft es zu, 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?

Vorbemerkung zu den nächsten Fragen: Als „anerkannte Regeln der Technik" werden Regeln bezeichnet, die in der Wissenschaft keinem Meinungsstreit ausgesetzt und damit als theoretisch richtig anerkannt sind und feststehen sowie insbesondere in dem Kreise der für die Anwendung der betreffenden Regeln maßgeblichen, nach dem neuesten Erkenntnisstand vorgebildeten Techniker durchweg bekannt und auf Grund fortdauernder praktischer Erfahrung als technisch geeignet, angemessen und notwendig anerkannt sind.

5. Frage: Ist die von der Beklagten behauptete Eignung, Notwendigkeit und Angemessenheit einer unterschiedslosen personenbezogenen Aufzeichnung jeglicher Nutzung von Telemedienangeboten in der Wissenschaft allgemein anerkannt und keinem Meinungsstreit ausgesetzt?

6. Frage: Ist die von der Beklagten behauptete Eignung, Notwendigkeit und Angemessenheit einer unterschiedslosen personenbezogenen Aufzeichnung jeglicher Nutzung von Telemedienangeboten unter den Technikern, die für die Bereitstellung solcher Angebote verantwortlich sind, allgemein anerkannt und keinem Meinungsstreit ausgesetzt?

7. Frage: Ist es heute Bestandteil der Ausbildung von Technikern, dass bei der Bereitstellung eines Telemediums eine unterschiedslose Protokollierung jeglicher Nutzung von Telemedienangeboten samt IP-Adresse geeignet, erforderlich und angemessen sei?

3.2. Mangelnde Erforderlichkeit einer Totalprotokollierung zur Gewährleistung der IT-Sicherheit

Vorbemerkung zu den nächsten Fragen: Das Bundesamt für Sicherheit in der Informationstechnik definiert den Begriff der „IT-Sicherheit" wie folgt: „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."

8. Frage: Ist ein Web-Server, der auf eine unterschiedslose Totalprotokollierung sämtlicher Zugriffe samt IP-Adresse verzichtet, jedoch fachgerecht eingerichtet ist und gewartet wird, im Sinne dieser Definition sicher? Lassen sich Sicherheitsrisiken also durch andere angemessene Maßnahmen als eine unterschiedslose Totalprotokollierung sämtlicher Zugriffe auf ein tragbares Maß reduzieren?

9. Frage: Lassen sich die Sicherheit und Funktionsfähigkeit der Informationstechnik der Beklagten somit durch andere Maßnahmen als durch eine unterschiedslose Totalprotokollierung sämtlicher Zugriffe gewährleisten?

Vorbemerkung zur nächsten Frage: Sie führen in Ihrem Gutachten aus, eine Speicherung von IP-Adresse könne bestenfalls geringfügig zum Schutz eines IT-Systems beitragen.

10. Frage: Wenn auf diesen „bestenfalls geringfügigen" Beitrag verzichtet wird, lassen sich die Sicherheitsrisiken durch andere Maßnahmen auf ein tragbares Maß reduzieren?

Vorbemerkung zur nächsten Frage: Ohne Speicherung von IP-Adressen bieten nach eigenen Angaben etwa die folgenden Bundesministerien und -behörden Internetportale an:

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

11. Frage: Belegt das langjährige IP-protokollierungsfreie Angebot von Telemedien durch diverse Bundesbehörden und Einrichtungen der Beklagten, dass etwaige verbleibende Restrisiken für die Systemsicherheit tragbar sind?

Vorbemerkung zur nächsten Frage: In Ihren Gutachten heißt es unter anderem,

- „Aus meiner Sicht dient die Speicherung von IP-Adressen nicht dem nationalen oder internationalen Stand der Technik." (S. 3 des Ausgangsgutachtens)
- „Es treten jedoch im Wesentlichen keine zusätzlichen Kosten durch den Verzicht auf die IP-Adressen-Speicherung auf, da wie unter 2. erwähnt diese anderen Sicher-

heitsmaßnahmen in jedem Fall zwingend erforderlich für den sicheren Betrieb des IT-Systems sind." (S. 3 des Ausgangsgutachtens)
- „eine Speicherung von IP-Adressen kann bestenfalls einen marginalen Sicherheitsgewinn bringen" (S. 9 des Ausgangsgutachtens)
- „Zum anderen existiert für die Absicherung von IT-Systemen eine Vielzahl von anderen, wesentlich effektiveren Mitteln und Methoden." (S. 10 des Ausgangsgutachtens)
- „da die Speicherung keinen signifikanten Beitrag zur Sicherheit des IT-Systems leistet" (S. 5 des Ergänzungsgutachtens)
- „bedarf es für den sicheren Betrieb eines IT-Systems nicht der Speicherung von IP-Adressen" (S. 6 des Ergänzungsgutachtens)
- „dass für den sicheren Betrieb eines IT-Systems die Speicherung der IP-Adressen der zugreifenden Hostsysteme nicht zwingend erforderlich ist." (S. 37 des Ergänzungsgutachtens)

12. Frage: Schließen diese Schlussfolgerungen den Fall ein, dass jede Form der unterschiedslosen personenbezogene Protokollierung der IP-Adressen aller Nutzer unterbleibt, dass also – wie bei den oben genannten Angeboten der Beklagten – eine Protokollierung der IP-Adressen weder in verschlüsselter noch in pseudonymisierter oder unverschlüsselter Form erfolgt?

Vorbemerkung zur nächsten Frage: Im Ergänzungsgutachten führen Sie einerseits aus, auch eine pseudonymisierte, anonymisierte oder verschlüsselte Speicherung von IP-Adressen sei „in vielen Fällen nicht notwendig" (S. 6). Andererseits schreiben Sie zur Hauptfrage, eine Speicherung von IP-Adressen sei zur Gewährleistung der IT-Sicherheit nicht erforderlich und könne zur Gewährleistung der Funktionsfähigkeit nur dann erforderlich sein, wenn ein Telemediendienst gerade die Speicherung von IP-Adressen zum Gegenstand habe (S. 37 f.). Sie hätten jedoch kein Telemedium der Beklagten feststellen können, bei dem die Speicherung von IP-Adressen Funktionsvoraussetzung sei.

13. Frage: Soweit Sie in Ihrem Gutachten auf den Einzelfall abstellen, verstehe ich Ihr Gutachten richtig, dass Sie im Fall der Beklagten einen solchen Einzelfall, der eine IP-Speicherung oder darauf aufbauende Maßnahmen notwendig mache, nicht haben feststellen können?

Vorbemerkung zur nächsten Frage: Sie schreiben, zur Gewährleistung der Verfügbarkeit eines Webservers, welcher einem Überlastungsangriff ausgesetzt sei, könne die Vorhaltung von IP-Adressen im flüchtigen Speicher nützlich sein, um eine Drosselung vornehmen zu können. Die Erkennung einer Überlastsituation sei auch ohne IP-Speicherung möglich. Der Kläger hat von seinem Unterlassungsantrag den Fall ausgenommen, dass die Speicherung seiner IP-Adresse erforderlich sei, um die Verfügbarkeit von Telemedien der Beklagten wieder herzustellen.

14. Frage: Kann die Beklagten ihre Systeme so einrichten, dass eine Speicherung der IP-Adressen von Nutzern zur Abwehr eines Überlastungsangriffs („Drosselung") erst dann erfolgt, wenn die Verfügbarkeit eines Webservers aufgrund eines solchen Angriffs tatsächlich gestört ist?

Vorbemerkung zur nächsten Frage: Die Beklagte hat im Laufe des Rechtsstreits eingeräumt, dass sie „alternative Maßnahmen zur Schadprogrammabwehr" einsetzen könne, „um einen sicheren Betrieb der entsprechenden Systeme der Beklagten zu gewährleisten".

15. Frage: Können Sie bestätigen, dass ein sicherer Betrieb der Systeme der Beklagten auch ohne Aufzeichnung sämtlicher Zugriffe auf Telemedien samt IP-Adressen möglich ist?

16. Frage: Wäre damit ein „hoher Kostenaufwand" verbunden und, wenn ja, in welcher Höhe?

17. Frage: Zusammenfassend: Muss die Beklagte sämtliche Zugriffe des Klägers auf ihre Telemedien samt IP-Adresse protokollieren, um deren Inanspruchnahme zu ermöglichen?

Beglaubigte und einfache Anschrift anbei.

Mit freundlichen Grüßen

Meinhard Starostik
- Rechtsanwalt -