TCI
RECHTSANWÄLTE

Beglaubigte Abschrift

TCI Rechtsanwälte Berlin · Fasanenstr. 61 · D - 10719 Berlin

Vorab per Fax 9023-2223 (15 Seiten)
Landgericht Berlin
ZK 57

10174 Berlin

TCI Rechtsanwälte Berlin
Fasanenstr. 61
D - 10719 Berlin
Tel: +49 - (0)30 - 20 05 42-0
Fax: +49 - (0)30 - 20 05 42-11
www.tcilaw.de

Dr. Ralf Grote
Norman Müller
Markus Schmidt
Carsten Gerlach

In Kooperation mit

TCI Rechtsanwälte München

Ruth Dünisch
Dr. Truiken J. Heydn
Dr. Michael Karger [1,2]
Dr. Andreas Stadler
Harald Krüger [3]
Dr. Thomas Stögmüller [1]
LL.M. (Berkeley)

TCI Rechtsanwälte Mainz

Stephan Schmidt [1]
Sabine Brumme
Stephan Breckheimer
LL.M. (Medienrecht)
Dr. Olaf Griebenow

Fachanwalt für
[1] Informationstechnologierecht
[2] Verwaltungsrecht
[3] Arbeitsrecht

Berlin, den 26. Oktober 2011

Ansprechpartn [redacted]
E-Mail-Adresse: [redacted]
Aktenzeichen: 172/00123-08/ms

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

ist das Gutachten des Sachverständigen vom 29. Juli 2011 ungenügend. Die vom Sachverständigen auf Seite 3 des Gutachtens vorgenommene Zusammenfassung der Ergebnisse ist gerade nicht durch die späteren Ausführungen gedeckt. In wesentlichen Teilen widersprechen sich sogar die „Ergebnisse" und die späteren Ausführungen. Im Übrigen sind die Ausführungen des Sachverständigen teilweise offensichtlich unlogisch und inkonsequent.

Das Gutachten vermittelt vielmehr den Eindruck, dass die „Ergebnisse" feststanden und mit den Ausführungen der – letztendlich gescheiterte – Versuch unternommen wurde, die gewollten Ergebnisse in irgendeiner Form zu rechtfertigen. Im Einzelnen:

1. zur Beweisfrage 1

Zu dieser Frage ist bereits die Feststellung des Sachverständigen in der Zusammenfassung der „Ergebnisse" widersprüchlich. Einerseits behauptet er, die Speicherung von IP-Adressen entspräche nicht dem Stand der Technik, muss andererseits aber bereits im nachfolgenden Satz einräumen, dass die Speicherung von IP-Adressen jedenfalls einigen nationalen und internationalen Standards und Empfehlungen entspricht. In seinen Ausführungen schreibt der Sachverständige dazu weiter:

> *„Gleichwohl kann das Speichern von IP-Adressen der Erfüllung von nationalen und internationalen Empfehlungen, Standards und Regulierungen dienen. In der Tat existiert eine Vielzahl von relevanten und bedeutenden Standards, die das Speichern von IP-Adressen vorsehen."*

Wie der Sachverständige bei dieser Feststellung zu dem Ergebnis gelangen kann, die Speicherung der IP-Adresse entspräche nicht dem Stand der Technik, ist in keiner Weise nachvollziehbar, da der Stand der Technik gerade durch diese internationalen Empfehlungen, Standards und Regulierungen definiert wird.

Weiter führt der Sachverständige aus, es gäbe insoweit sich widersprechende Standards, da vermeintlich auch Standards existieren würden, die eine Speicherung von IP-Adressen verbieten. Nachfolgend listet der Sachverständige dann fünf Standards auf, von denen jedoch nach den Ausführungen des Sachverständigen keiner die Speicherung von IP-Adressen „verbietet". Im Gegenteil ist aus allen Beispielen die Notwendigkeit der Speicherung abzulesen.

1.1 DIN ISO/IEC 27001:2008-09

Nach den Ausführungen des Sachverständigen heißt es in dieser Norm ausdrücklich:

„Es müssen Auditprotokolle erstellt werden, in denen die Benutzeraktivitäten, Fehler und Informationsicherheitsvorfälle festgehalten werden. Sie müssen für einen vereinbarten Zeitraum verwahrt werden, um in zukünftigen Untersuchungen und Überwachungen der Zugriffskontrolle behilflich zu sein."

Die Norm verlangt also ausdrücklich die Protokollierung und damit die Speicherung der Benutzeraktivitäten. Die Aktivitäten müssen sich bei der Protokollierung also mindestens verschiedenen Zugriffen zuordnen lassen. Hierzu kann nur die IP-Adresse als notwendiges (wenn auch nicht alleiniges) Mittel dienen, da diese alleine geeignet ist, überhaupt eine Unterscheidung zwischen unterschiedlichen Zugriffen herbeizuführen. Insoweit räumt der Sachverständige zur Beweisfrage 2 selbst ein, dass die IP-Adresse für eine Benutzeridentifizierung zwar nicht ausreichend, aber zumindest erforderlich ist.

Die Schlussfolgerung des Sachverständigen, aus der Norm lasse sich die Notwendigkeit zur Speicherung von IP-Adressen nicht ableiten, ist daher nicht nachvollziehbar.

1.2 DIN ISO/IEC 27002:2008-09

Diese Norm nennt „Netzadressen" und damit die IP-Adresse ausdrücklich als Bestandteil eines ordnungsgemäßen Auditprotokolls. Dementsprechend muss der Sachverständige hier selbst einräumen, dass die Speicherung der IP-Adresse der Erfüllung dieser Norm dient.

1.3 DIN ISO/IEC 15408-1…3

Hier kommt der Sachverständige zu dem Ergebnis, die Norm enthalte keine Notwendigkeit zur Speicherung von IP-Adressen. Dies steht allerdings in klarem Widerspruch zu dem von ihm selbst zitierten Auszug aus der Norm. Dort heißt es:

„The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of the event, subject identity, and the outcome (success or failure) of the event; …"

Die Verwendung des Wortes "shall" bezeichnet dabei im Englischen im Kontext eine bindende Verpflichtung, d.h. nicht „soll", sondern „muss". Dies wird auch noch einmal durch die Verwendung von „at least" (d.h. „wenigstens") unterstrichen. Gegenstand dieser Mindestanforderung ist eindeutig auch die „subject identity". Im Rahmen der hier streitgegenständlichen Internetzugriffe auf Webserver kann dies, da eine ausdrückliche Registrierung und Anmeldung nicht erforderlich ist, nur die IP-Adresse sein, da nur diese das Subjekt des Zugriffs (d.h. das zugreifende System) kennzeichnet.

1.4 BSI-Grundschutz

In Bezug auf diesen allgemein anerkannten Sicherheitsstandard muss der Sachverständige selbst einräumen, dass die Speicherung der IP-Adresse mehrfach ausdrücklich für notwendig erachtet wird. An wie vielen Stellen des gesamten Grundschutz-Katalogs dies erfolgt, ist dabei unerheblich. Notwendigkeit ist nicht steigerungsfähig. Notwendigkeit besteht daher dann, wenn die entsprechende Maßnahme auch nur an einer Stelle verbindlich gefordert wird.

1.5 ETSI TR 102 661 V1.2.1 (2009-11)

Nach eigenen Ausführungen des Sachverständigen beschäftigt sich diese Norm lediglich mit der Frage des „wie", nicht aber mit dem „ob" einer Datenspeicherung. Für die Beweisfrage ist daher keinerlei Relevanz der Norm erkennbar.

Der Sachverständige vermischt in seinem Gutachten unzulässigerweise die Frage der grundsätzlichen Notwendigkeit der Speicherung der IP-Adresse nach dem Stand der Technik und die Frage, ob diese Speicherung nach dem Stand der Technik unverschlüsselt erfolgen darf. Letzteres ist weder Gegenstand der Beweisfrage noch des Rechtsstreits, da der Kläger der Beklagten jegliche Form

der Speicherung, d.h. also auch eine verschlüsselte Speicherung untersagen lassen will.

In diesem Zusammenhang erlauben wir uns den Hinweis, dass ein gravierender Unterschied zwischen verschlüsselter, pseudonymisierter oder anonymisierter Speicherung besteht. „Verschlüsselte" Speicherung besagt, dass die gespeicherten Daten nicht im lesbaren Klartext gespeichert werden, d.h. bei einem Zugriff auf die Daten ohne entsprechendes Entschlüsselungsprogramm die Daten nicht lesbar sind. „Pseudonymisiert" bedeutet dagegen, dass die Daten zwar im Klartext gespeichert werden, personenidentifizierende Daten aber durch Pseudonyme ersetzt werden, die letztendlich nur im Zusammenhang mit einer getrennt gespeicherten Liste von Pseudonymen und zugehörigen personenidentifizierenden Daten wieder auf die Person zurückgeführt werden können. Insoweit stellen die hier streitgegenständlichen IP-Adressen bereits Pseudonyme dar, da ohne die Zuordnungsdaten des jeweiligen Telekommunikationsanbieters des Nutzers keine Personenidentifikation möglich ist. Lediglich mit einer „Anonymisierung" ist dagegen endgültig keine Rückbeziehung auf eine konkrete Person mehr möglich, da personenidentifizierende Daten so gelöscht oder verändert werden, dass ein Personenbezug der Daten auf keine Weise mehr hergestellt werden kann.

Insgesamt belegen daher die Ausführungen des Sachverständigen entgegen seiner Zusammenfassung, dass die Speicherung von IP-Adressen in vielen aktuellen Empfehlungen, Standards und Regulierungen als erforderliche Maßnahme zum Schutz von IT-Systemen genannt ist. Der Sachverständige bleibt jegliche plausible Erklärung dafür schuldig, weshalb trotz dieses Umstandes die Speicherung von IP-Adressen nicht mehr dem Stand der Technik entsprechen soll. Dies käme allenfalls dann in Betracht, wenn die einschlägigen Normen veraltet wären und nicht mehr dem Stand der Technik entsprächen. Dies wird vom Sachverständigen zwar behauptet, allerdings bleibt der Sachverständige hierfür jeglichen Beleg schuldig. Insbesondere sind die angeführten Normen und Standards auch nicht durch neuere oder andere Normen oder Standards ersetzt oder von der allgemeinen Praxis überholt worden.

2. zur Beweisfrage 2

2.1 Unzutreffend bzw. ungenau und damit tendenziös im Sinne des Streitgegenstandes sind bereits die einleitenden Erläuterungen des Sachverständigen. Während er für die Ziel-IP-Adresse ausführlich darauf hinweist, dass diese das Zielgerät und nicht die Person des Empfängers bestimmt, unterlässt der Sachverständige diesen Hinweis für die Quell-IP-Adresse. Auch hier kennzeichnet die IP-Adresse jedoch nur das Absendergerät und nicht den Absender. Insofern ist der Vergleich mit Absender- und Empfängeradresse im Postverkehr falsch, jedenfalls wenn man zur Absender- und Empfängeradresse im Postverkehr auch den Namen des Absenders bzw. Adressaten zählt. Die IP-Adresse kennzeichnet, wenn man schon bei dem Vergleich bleiben will, allenfalls das Absender- bzw. Empfängergebäude.

2.2 Unzutreffend ist weiter, dass der Absender die Absender-IP-Adresse in der Regel frei festlegen kann. Wäre dies tatsächlich der Fall, wüsste nur der Absender selbst, welche natürliche Person sich hinter der von ihm genutzten IP-Adresse verbirgt. Damit allerdings würde es sich zweifelsfrei nicht mehr um ein dem Datenschutz unterliegendes personenbezogenes Datum handeln, da dann außer dem Betroffenen selbst, niemand die IP-Adresse einem konkreten Gerät zuordnen könnte. Vielmehr erfolgt die Zuteilung der hier in Rede stehenden dynamischen IP-Adressen in aller Regel durch den Telekommunikationsanbieter des Absenders, über den der Absender seine Verbindung zum Internet herstellt.

Unerheblich für die Beweisfrage ist dabei zunächst, ob und, wenn ja, wie leicht diese zugeteilte IP-Adresse vom Absender selbst oder durch Inanspruchnahme entsprechender Anonymisierungsdienste im Internet der Absender seine tatsächliche IP-Adresse verschleiern kann. Der Sachverständige führt in diesem Zusammenhang aus, dass deshalb nur „dumme“ Angreifer über die IP-Adresse identifizierbar seien und daher eine Speicherung der IP-Adressen nicht erforderlich sei. Dieser Rückschluss entbehrt aber jeglicher Logik. Selbst wenn man der Ausgangsthese vom „Dummenfang“ folgen sollte, kann daraus nicht gefolgert werden, dass die Möglichkeit zum „Dummenfang“ nicht erfolgen muss

oder gar darf. So käme auch niemand ernsthaft auf die Idee zu behaupten, dass man seinen Autoschlüssel im abgestellten Auto liegen lassen kann, weil viele Autodiebe auch ohne Autoschlüssel in der Lage sind, das Auto zu stehlen. Völlig außer Betracht lässt der Sachverständige über dies, dass eine Aufgabe der Möglichkeit zum „Dummenfang" letztendlich jeden „Dummen" zu einem Angriff auf die IT-Systeme der Beklagten einladen würde. Nicht von ungefähr gilt das Sprichwort „Gelegenheit macht Diebe".

2.3 Hinzukommt, dass die Speicherung der IP-Adressen (selbst gefälschter oder manipulierter IP-Adressen) die Möglichkeit eröffnet verschiedene Zugriffe dem gleichen Sendegerät zuzuordnen und damit auf verschiedenen Zugriffe verteilte Angriffe bzw. Angriffsmuster aufdecken zu können (vgl. hierzu die Ausführungen aus dem Schriftsatz vom 22. März 2010 zur Anomalieerkennung). Der Sachverständige räumt die Notwendigkeit einer derartigen Anomalieerkennung im Rahmen der Angriffserkennung sowie die dabei erforderliche eindeutige Zuordnung verschiedener Zugriffe zu einer Quelle selbst ein (vgl. Seite 7 unten des Gutachtens).

In diesem Zusammenhang behauptet der Sachverständige, sei keine Speicherung der IP-Adresse erforderlich, weil die Angriffserkennung und –abwehr sich im beschriebenen Szenario durch eine Speicherung einer verschlüsselten IP-Adresse erreichen lasse. Dies ist nicht nachvollziehbar. Wie bereits oben unter Ziffer 1.5 ausgeführt, ändert eine Verschlüsselung nichts daran, dass die IP-Adresse gespeichert bleibt. Sie ist lediglich nicht mehr im Klartext gespeichert, kann aber jederzeit wieder entschlüsselt werden. Auch eine Pseudonymisierung ändert nicht wirklich etwas, da diese, wie ebenfalls oben beschrieben, rückgängig gemacht werden kann. Diese Möglichkeit der „Rückübersetzung" ist auch in Abbildung 2 auf S. 7 des Gutachtens dargestellt.

Lediglich eine vollständige Anonymisierung würde dies verhindern, verhindert notwendigerweise aber auch, dass unterschiedliche Zugriffe einer Quelle einander zugeordnet werden können. Wesensgehalt der Anonymisierung ist nämlich, dass das entsprechende Datum, hier die IP-Adresse, völlig willkürlich und nicht nachvollziehbar geändert wird. Das bedeutet allerdings im Ergebnis, dass

bei jedem Zugriff notwendigerweise die zugreifende IP-Adresse anders abgeändert wird. Sofern für eine IP-Adresse immer die gleiche Abänderung erfolgen soll, muss es dafür notgedrungen eine definierte Regel geben, die dann konsequenterweise auch wieder „rückübersetzt" werden kann. Eine Erklärung, wie sich der Sachverständige eine Zuordnung willkürlich und in jedem Zugriffsfall unterschiedlich abgeänderte IP-Adressen zueinander vorstellt, bleibt er wenig überraschend schuldig.

2.4 Den einfachsten Anforderungen der Logik entbehren die Ausführungen des Sachverständigen zur Angriffsabwehr mittels eines Firewallsystems. Zutreffend ist hieran lediglich, dass ein leistungsfähiges Firewallsystem zum Stand der Technik für die Angriffsabwehr zählt. Nach den insoweit zutreffenden Ausführungen des Sachverständigen können mittels Firewall Zugriffe einer bestimmten IP-Adresse von vorne herein unterbunden werden. Im Gutachten heißt es dazu auf S. 7:

> *„Hier ist eine Speicherung der IP-Adresse nicht notwendig. Vielmehr kann ein derartiger Angriffsversuch unmittelbar durch die Firewalls des zu schützenden IT-Systems abgewehrt werden, indem dort vermerkt wird, daß alle IP-Pakete von der Absender-IP-Adresse 1.2.3.4 verworfen und nicht in das eigentliche Kernnetz des IT-Systems weitergeleitet werden."*

Dies erfordert aber notwendigerweise, dass bestimmte IP-Adressen in der Firewall „vermerkt", d.h. gespeichert werden – andernfalls kann die Firewall Zugriffe dieser IP-Adressen nicht verwerfen. Diese Speicherung („Regel: Blockiere IP_C") geht auch aus dem Schaubild auf S. 7 hervor. Die einleitende Feststellung, dass zur Nutzung der Firewall „eine Speicherung der IP-Adresse nicht notwendig" sei, ist somit schlicht unrichtig und wird schon im nächsten Satz in ihr Gegenteil verkehrt.

Die Abwehr eines Zugriffs von einer bestimmten IP-Adresse mittels Firewall ist also ohne Speicherung genau dieser IP-Adresse technisch gar nicht möglich.

Völlig unklar ist darüber hinaus, wie die Beklagte nach Ansicht des Sachverständigen zu der IP-Adresse, welche in der Firewall als potentieller Angreifer gespeichert werden soll, kommen soll. Die Identifikation der IP-Adresse als potentielle Angreiferadresse setzt notgedrungen die Speicherung der IP-Adresse mindestens in der Firewall voraus, da anderenfalls die Beklagte gar nicht wissen kann, unter welcher IP-Adresse der Angriff erfolgt ist.

Die Schlussfolgerung auf S. 8 des Gutachtens, dass „*eine Abwehr durch eine Firewall leicht möglich ist, wofür eine Speicherung der IP-Adresse jedenfalls nicht erforderlich ist*", ist somit schlicht falsch. Mindestens die Firewall muss nach den eigenen Ausführungen und dem eigenen Schaubild des Gutachtens die zu sperrende IP-Adresse zwangsläufig speichern.

2.5 Sogar wenn man das vom Sachverständigen herangezogene Beispiel eines Angriffes von Botnetzen heranzieht (die Beklagte hatte diese Angriffsform bislang gar nicht als Beispiel für die Notwendigkeit der Speicherung von IP-Adressen angeführt), erschließt sich die Notwendigkeit der Speicherung der IP-Adressen.

Bei sogenannten „Botnetzen" handelt es sich um Angriffe, bei denen sich der Angreifer zahlreicher virenverseuchter Rechner (dem „Botnetz") ohne Wissen der jeweiligen Anwender bedient.

Auch wenn unstreitig auf diesem Wege der eigentliche Angreifer nicht in jedem Fall ermittelt werden kann, so können jedenfalls die für das Botnetz missbrauchten Rechner über die IP-Adresse identifiziert werden – die in diesen Fällen auch kaum anonymisiert oder verfälscht ist, da die Eigentümer dieser Rechner regelmäßig gar keine Kenntnis von dem Missbrauch haben – und auf diesem Wege die Eigentümer über den Missbrauch unterrichtet werden. Auf diese Art und Weise kann u. U. der weitere Einsatz des konkreten Rechners für weitere Angriffe verhindert werden.

2.6 Soweit schließlich der Sachverständige auf andere Möglichkeiten der Angriffserkennung und –abwehr hinweist, bleibt er vage und die Nennung konkreter technischer Lösungen schuldig.

Zum einen nennt er den von der TU Dresden betriebenen Anonymisierungsdienst AN.ON7. Welche Verfahren konkret hier eine zur Speicherung der IP-Adressen vergleichbare Alternative zur Angriffserkennung und –abwehr darstellen sollen, beschreibt der Sachverständige bezeichnenderweise nicht.

Gleiches gilt für den Anonymisierungsdienst auf der Website isharegossip.com. Ausweislich der Beschreibung setzte die Website ein spezielles Verfahren, das lediglich zur Prävention eines bestimmten Mißbrauchsszenarios („Spam" einer Diskussionsplattform) diente („*Das System dient lediglich dem unterbinden [sic] von Spam […]*"). Zudem handelte es sich bei dieser Website um einen Anbieter, dessen Geschäftsmodell im „Online-Mobbing" bestand und der daher zwangsläufig als „unique selling point" der Anonymität des Dienstes Priorität vor der EDV-technischen Sicherheit einräumen musste. Da die Website nicht zuletzt aufgrund von Hacker-Angriffen inzwischen nicht mehr verfügbar ist, muss im Übrigen die praktische Wirksamkeit ernsthaft bezweifelt werden (vgl. z.B. Focus-Online vom 15.6.2011: „*Umstrittene Mobbing-Website nach Hacker-Angriff weiter offline*", http://www.focus.de/digital/digital-news/isharegossip-umstrittene-mobbing-website-nach-hacker-angriff-weiter-offline_aid_637270.html).

Schließlich verweist der Sachverständige auf eine Dissertation von Dr. Ulrich Flegel aus dem Jahr 2007. Bei den dort vorgestellten Maßnahmen handelt es sich jedoch um wissenschaftlich-theoretische Darstellungen. Der Beweis der Praxistauglichkeit steht nach Kenntnis der Beklagten bis heute aus. Die von Dr. Flegel vorgestellten Maßnahmen sind bislang nicht über einen prototypischen Einsatz hinausgekommen. Keine der vom Sachverständigen genannten Maßnahmen/Anwendungen hat jedenfalls bislang seine Praxistauglichkeit in großen und sehr großen IT-Systemen und –netzen, wie die Beklagte sie betreibt unter Beweis gestellt. Folgerichtig nennt der Sachverständige auch keinen einzigen „Großanwender". Kein einziger Hersteller eines gängigen Produktes zum Schutz von IT-Systemen verzichtet auf die Speicherung von IP-Adressen. Es bleibt daher rätselhaft, aufgrund welcher nachvollziehbaren Sachverhalte der Sachverständige dies als „veraltet" und nicht mehr dem Stand der Technik entsprechend einstufen kann.

Der Sachverständige muss deshalb seine eigenen Aussagen relativieren, indem er selbst einräumt:

> *„In vielen Fällen sollte sich allerdings eine sinnvolle Ersetzung ohne relevanten Informationsverlust vornehmen lassen."* (Seite 8 oben des Gutachtens)

Mit anderen Worten: In bestimmten Fällen ist eine sinnvolle Ersetzung der Speicherung der IP-Adresse gerade nicht möglich.

2.7 Der Sachverständige muss weiterhin selbst einräumen, dass die Speicherung der IP-Adresse zur Angreiferidentifizierung „nützlich" sein kann. So führt er z.B. auf S. 8 des Gutachtens aus:

> *„Allerdings kommt es hier auf die konkrete Arbeitsweise insbesondere der vorhandenen Angriffserkennungssysteme an, da diese aus der Absender-IP-Adresse eventuell noch weitere Informationen ableiten […]"*

Zur Angreiferidentifizierung schreibt er auf S. 5:

> *„Natürlich lässt sich nicht ausschließen, dass ein Angreifer eine korrekte Absenderangabe vornimmt und insofern identifizierbar ist."*

Da er keinerlei Alternativen aufzeigen kann, wie ohne die Speicherung der IP-Adresse eine Angreiferidentifizierung überhaupt erfolgen soll, muss dieses „nützlich" wohl als ein „erforderlich" angesehen werden. Bezeichnend ist dabei das vom Sachverständigen auf Seite 9 des Gutachtens dazu selbst gewählte Beispiel von verschlossenen Türen und Überwachungskameras. Die Beklagte hat zu keinem Zeitpunkt die These aufgestellt, die Speicherung von IP-Adressen sei die einzige und alleine ausreichende Maßnahme zur Angriffserkennung und –abwehr. Insofern verschließt die Beklagte, um im Bild zu bleiben, selbstverständlich auch die Türen. Allerdings käme wohl auch niemand auf die Idee, dass bei hochgefährdeten Objekten (die IT-Systeme und -netze

der Beklagten sind derartige hochgefährdete Systeme) auf Überwachungskameras vollständig verzichtet werden kann und muss.

Wäre die Beklagte daher gezwungen, auf die Speicherung der IP-Adressen völlig zu verzichten, gäbe es keinerlei Generalprävention gegen Angriffe auf die IT-Systeme der Beklagten, da kein Angreifer (auch nicht die „Dummen") mit seiner Identifizierung rechnen müsste.

3. zur Beweisfrage 3

Die Frage wurde durch den Sachverständigen schlicht nicht beantwortet. Zur Begründung führt er aus, dass ihm die hierfür notwendigen Informationen nicht vorliegen. Allerdings hat sich der Sachverständige auch nicht ansatzweise die Mühe gemacht, diese Informationen zu erlangen. Auch dies zeigt, dass es dem Sachverständigen nicht um die vollständige und neutrale Beantwortung der Beweisfragen ging, sondern das Ergebnis aus welchen Gründen auch immer vorgegeben war.

Unzutreffend ist jedenfalls die Behauptung, alle zusätzlichen Kosten seien ohnehin aufzuwenden. Zu diesem „Ergebnis" kann der Sachverständige nur deshalb gelangen, weil er zur Beweisfrage 2 gleichfalls jegliche konkrete Alternative schuldig bleibt, wie die Speicherung von IP-Adressen im Rahmen der erforderlichen Angriffserkennung und –abwehr wirksam ersetzt werden kann. Unstreitig ist dabei, dass die Speicherung von IP-Adressen keinesfalls alleine ausreichend ist, um eine dem Stand der Technik entsprechende Vorsorge zu treffen. Insoweit hat die Beklagte auch nie behauptet, dass die Speicherung der IP-Adresse ihre einzige Maßnahme zur Angriffserkennung und –abwehr sei. Die Kosten für diese weiteren Maßnahmen sind in der Tat Kosten die ohnehin bei der Beklagten anfallen. Die Kosten dieser weiteren Maßnahmen sind jedoch nicht Gegenstand der Beweisfrage gewesen. Insoweit ist die Aussage des Sachverständigen ohne jeglichen Wert für die Beantwortung der Beweisfrage.

Beweiserheblich wäre dagegen z.B. gewesen, welche Aufwendungen erforderlich wären, um die vom Sachverständigen völlig vage erwähnten Alternativ-

maßnahmen (z.B. aus der genannten Dissertation von Dr. Flegel) vom theoretisch prototypischen Entwicklungsstand in ein für IT-Systeme mit Hochsicherheitsanforderungen praxistaugliches und praxiserprobtes Produkt zu überführen. Leider bleibt der Sachverständige diesbezügliche Ausführungen schuldig.

4. Zusammenfassung

4.1 Der Sachverständige räumt zur Beweisfrage 1 selbst ein, dass eine Reihe von nationalen und internationalen Normen und Standards die Speicherung von IP-Adressen für einen sicheren Betrieb von IT-Systemen vorsieht. Ob die Speicherung dabei verschlüsselt oder unverschlüsselt erfolgen soll, kann dahingestellt bleiben, da es in beiden Fällen eine Speicherung der IP-Adresse im Sinne des Klageantrags ist.

4.2 Die Ausführungen des Sachverständigen zur Beweisfrage 2 weisen schwere logische Fehler auf. Die Ausführungen zu angeblichen Alternativen sind schwammig und unpräzise und daher wertlos. Festzuhalten bleibt jedenfalls, dass der Sachverständige konkret nicht ein den Gesetzen der Logik genügendes Verfahren zur Angriffserkennung und –abwehr nennen kann, das die Speicherung der IP-Adressen ersetzten könnte. Im Gegenzug muss der Sachverständige aber selbst einräumen, dass die Speicherung der IP-Adresse zur Angreiferidentifizierung „*nützlich*“ sein kann.

4.3 Die Beweisfrage 3 hat der Sachverständige schlicht unbeantwortet gelassen.

4.4 Insgesamt drängt sich der Eindruck auf, dass der Sachverständige seine Ausführungen vorrangig unter dem Gesichtspunkt der Frage einer verschlüsselten/pseudonymisierten oder unverschlüsselten Speicherung der IP-Adressen gemacht hat. Diese Erwägung spielt jedoch für die Klärung der Beweisfragen im Hinblick auf den umfassenden generellen Unterlassungsantrag des Klägers keine Rolle, so dass der Sachverständige den Gutachtensauftrag völlig falsch verstanden hat.

4.5 Sofern man den Detailausführungen des Sachverständigen überhaupt konkrete Aussagen entnehmen kann, stützen diese den Vortrag der Beklagten, dass die Speicherung von IP-Adressen internationalen Normen und Standards für den Betrieb von IT-Systemen entsprechen und diese Speicherung für die Angriffserkennung und –abwehr erforderlich (im Sprachgebrauch des Sachverständigen „nützlich") ist.

Demgegenüber weist der Sachverständige ausdrücklich darauf hin, dass es für jeden Nutzer, d.h. also auch den Kläger, ohne Probleme möglich wäre, mit im Internet angebotenen Anonymisierungsdiensten seine Identität (d.h. die Identität seines Endgerätes) einfach, wirkungsvoll und kostenfrei zu verschleiern.

Im Rahmen der erforderlichen Interessenabwägung zwischen den Interessen des Klägers und den Interessen der Beklagten kann daher die Abwägung nur zu Gunsten der Beklagten und damit der Speicherung von IP-Adressen ausfallen. Während die Beklagte bei einem Verbot der Speicherung auf eine international anerkannte, dem Stand der Technik entsprechende Sicherheitsmaßnahme, die selbst nach Ansicht des Sachverständigen für die Angriffserkennung und -abwehr zumindest „nützlich" ist, vollständig verzichten müsste, steht dem Kläger eine einfache und kostenlose Möglichkeit zur Verfügung, die von ihm behauptete Personenbezogenheit seiner IP-Adresse endgültig selbst zu beseitigen und damit seine „Identifizierung" abschließend unmöglich zu machen.

5. Soweit das Gericht das Sachverständigengutachten im Hinblick auf die jüngste obergerichtliche Rechtsprechung zur Personenbezogenheit von IP-Adressen (vgl. unseren Schriftsatz vom 24. November 2010) überhaupt noch für entscheidungserheblich halten sollte, ist aus hiesiger Sicht eine Erläuterung des Gutachtens durch den Sachverständigen gemäß § 411 Abs. 3 ZPO für eine angemessene Beantwortung der Beweisfragen kaum zielführend, da für eine bloße Erläuterung die aufgezeigten Mängel des Gutachtens zu tiefgreifend sind. Wir beantragen daher die Einholung eines neuen Gutachtens gemäß § 412 ZPO.

Gemäß § 411 Abs. 4 ZPO beantragen wir hilfsweise, den Sachverständigen mindestens aufzufordern, eindeutig klarzustellen, ob er an seinen „Ergebnissen" festhält oder diese im Hinblick auf seine dazu im eindeutigen Widerspruch stehenden „detaillierten Ausführungen" korrigiert. Eine Stellungnahme muss dabei insbesondere auf die oben genannten logischen Fehler eingehen und konkrete praxistaugliche, d.h. praxiserprobte Produkte, Techniken und Maßnahmen benennen, mit denen nach Ansicht des Sachverständigen nach dem Stand der Technik die Speicherung der IP-Adressen bei Aufrechterhaltung eines identischen Schutzniveaus vollständig ersetzt werden kann. Nur dann ist der Beklagten eine substantiierte inhaltliche Auseinandersetzung mit den Feststellungen des Sachverständigen möglich. Die schlichten Behauptungen des Sachverständigen, es gäbe IT-Systeme, die ohne Speicherung der IP-Adressen auskommen, sind insoweit nicht einlassungsfähig, da ohne detaillierte Kenntnis der dort zur Substitution ergriffenen Maßnahmen eine sicherheitstechnische Beurteilung und damit die Richtigkeit der Aussage des Sachverständigen nicht möglich ist. Die Beantwortung der Beweisfragen hat dabei im Hinblick darauf zu erfolgen, dass weder eine verschlüsselte noch eine pseudonymisierte Speicherung der IP-Adressen notwendig sein darf, d.h. eine spätere Ermittlung der eigentlichen IP-Adresse völlig ausgeschlossen ist.

Beglaubigte und einfache Abschrift anbei

[redacted]

Rechtsanwalt