WENDLER TREMML
RECHTSANWÄLTE

Beglaubigte Abschrift

WENDLER TREMML · Fasanenstraße 61 · D - 10719 Berlin

Vorab via Fax: 9023-2223

Landgericht Berlin
ZK 57

10174 Berlin

BERLIN
Dr. Ralf Grote
Norman Müller
Markus Schmidt
Carsten Gerlach
Raimund E. Walch[3]

DÜSSELDORF
Michael Wendler
Kai F. Sturmfels, LL.M.[3]
Dr. Jutta Walther
Beata Kosny

MÜNCHEN
Dr. Bernd Tremml, M.C.J.[1]
Dr. Dr. Georg Scholz †
Dr. Michael Bihler
Wolf D. Schenk[2]
Dr. Michael Karger[1,4]
Dr. Andreas Stadler
Stefan Sandrock
Dr. Matthias von Oppen

BRÜSSEL
Sophie Melchinger
Dr. Michael Bihler
Kai F. Sturmfels, LL.M.[3]

1 Fachanwalt für Verwaltungsrecht
2 Fachanwalt für Arbeitsrecht
3 Fachanwalt für Bau- u. Architektenrecht
4 Fachanwalt für IT Recht

www.law-wt.de

Berlin, den 28. Juni 2010
Unser Zeichen:172/00123-08/ms

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

I. Beweisbeschluss

1. Die Beklagte schlägt in Erfüllung der Auflage gemäß Ziffer 2 des Beweisbeschlusses vom 20. Mai 2010 folgende Sachverständige vor:

a. Herrn Prof. Dr. Bernhard Hämmerli, Acris GmbH, [redacted]
CH-6005 Luzern, Schweiz

Prof. Hämmerli ist Mitglied in mehreren nationalen und internationalen Beratungsausschüssen in Wissenschaft und Industrie zum Thema IT-Sicherheit und arbeitet in Komitees von wissenschaftlichen Symposien und Kongressen. Er ist Vorsitzender der FGSec Fachgruppe Security der Schweizer Informatikgesellschaft, Mitglied der Schweizer Informatiker Gesellschaft (SI) und der IEEE Computer Society. Er ist Herausgeber der deutschen Fachzeitschrift „digma

BERLIN
Fasanenstraße 61
D - 10719 Berlin
Tel. 030/200 542-0
Fax 030/200 542-11
berlin@law-wt.de

DÜSSELDORF
Mörsenbroicher Weg 200
D - 40470 Düsseldorf
Tel. 0211/66 96 67-0
Fax 0211/66 96 67 66
dus@law-wt.de

MÜNCHEN
Martiusstraße 5/II
D - 80802 München
Tel. 089/38 89 9-0
Fax 089/38 89 9-155
munich@law-wt.de

BRÜSSEL
Avenue de la Renaissance 1
B - 1000 Bruxelles
Tel. 0032 2/739 63 54
Fax 0032 2/736 05 71
bruxelles@law-wt.de

HypoVereinsbank Berlin (BLZ 100 208 90) Konto-Nr. 354 971 577
IBAN: DE96 1002 0890 0354 9715 77 – SWIFT: HYVEDEMM488
USt-IdNr. DE814047461 - Steuernummer: 24/319/63777

Zeitschrift für Datenrecht und Informationssicherheit" (www.digma.info) und des European Critical Information Infrastructure Protection (CIIP) Newsletter (www.ci2rco.org).
Er ist seit dem Jahr 1992 Professor der Hochschule Technik und Architektur (HTA) in Luzern. Er war dabei zuständig für den Aufbau der Studiengänge Curriculum „Informatik", Nachdiplom Datenschutz, Executive Master Programm für IT Sicherheit, den Aufbau des ersten IT-Security Labs sowie der regionalen Cisco-Akademie Central Switzerland für Cisco Certified Network Associate (CCNA) und Cisco Certified Network Professional (CCNP)

b. Herrn Christoph Fischer
Geschäftsführer der bfk EDV-Consulting GmbH, [redacted]
Karlsruhe

Herr Fischer ist als Geschäftsführer der bfk seit vielen Jahren mit der Abwehr von Angriffen auf IT-Systeme beschäftigt. Herr Fischer berät dabei eine Reihe großer deutscher Unternehmen im Zusammenhang mit Sicherheitsmaßnahmen im IT-Bereich. Darüber hinaus ist Herr Fischer selbst unmittelbar verantwortlich für den Betrieb von Webservern. Herr Fischer war bereits mehrfach im Zusammenhang mit Angriffen auf IT-Systeme als gerichtlicher Gutachter tätig. Herr Fischer ist Mitbegründer des ersten deutschen Computer Notfall Teams (CERT) und sowohl auf nationaler (CERT-Verbund) als auch internationaler Ebene (USA: FIRST; Europa: EICAR) in Institutionen für Computersicherheit engagiert.

c. Herr Udo Schweigert

Herr Udo Schweigert leitet den Konzerndienst CERT der Siemens AG, welcher für die Verhinderung und Aufklärung aller IT-Sicherheitsvorfälle der Siemens AG weltweit zuständig ist und von einem 14-köpfigen Team von Sicher-

heitsspezialisten erbracht wird. Hierbei werden alle Aspekte der IT-Sicherheit berücksichtigt bis hin zur IT-Forensik.

Udo Schweigert ist ein anerkanntes Mitglied der nationalen und weltweiten Sicherheits-Community. Er ist Vorsitzender des Membership Committee von FIRST, dem internationalen Dachverband der Computer-Notfall-Teams. Vier Jahre lang gehörte er auch dem Vorstand von FIRST an, darunter zwei Jahre als stellvertretender Vorsitzender. Darüber hinaus ist er Mitglied im Lenkungskreis des Deutschen CERT Verbundes und sitzt regelmäßig im Programm-Komitee einschlägiger Sicherheits-Konferenzen.

Herr Schweigert ist durch seine Tätigkeit mit den Möglichkeiten professioneller Täter bestens vertraut. Er analysiert derartige Angriffe und trägt zur ständigen Verbesserung der bei Siemens betriebenen Abwehrmechanismen bei. Daher ist er auch besonders geeignet, realistische wirtschaftliche Betrachtungen zu den in Frage kommenden Technologien anzustellen.

2. Generell erlauben wir uns zur Geeignetheit eines Sachverständigen folgende Anmerkung zu machen:

2.1 Das Gericht hat als Beweisthema eine komplexe technische Frage aufgeworfen, die nicht nur theoretische Möglichkeiten, sondern auch die praktische Umsetzbarkeit technischer Lösungen einschließt. Zur Beantwortung des Gutachtensauftrages sind daher nach hiesiger Einschätzung nicht nur besondere theoretische Fachkenntnisse erforderlich, sondern auch praktische Erfahrung beim Betrieb und der Absicherung von Webservern gegen Angriffe durch professionelle Angreifer. .

Soweit der Kläger mit seinem Schriftsatz vom 9. Juni 2010 bereits vorsorglich versucht, von der Beklagten vorgeschlagene Sachverständige generell zu diskreditieren, so ist dies nachgerade absurd. Würde man die vom Kläger geforderte Bedingung ernst nehmen, hätte der Kläger auch sämtliche von ihm benannten Sachverständigen ausgeschlossen, da diese nach eigenem Vortrag des

Klägers allesamt bereits für die Beklagte entgeltlich tätig waren. Dem Kläger dürfte ohne weiteres bekannt sein, dass Sachverständige im Rahmen einer gerichtlichen Gutachtertätigkeit gemäß JVEG vergütet werden. Da auch das Bundesverfassungsgericht ein Organ der Beklagten ist, sind die vom Kläger benannten Sachverständigen Kurz und Pfitzmann also bereits entgeltlich für die Beklagte tätig gewesen. Herr Schaar bezieht als Bundesbeauftragter für den Datenschutz (ebenso wie die BSI-Mitarbeiter) sogar sein Gehalt permanent von der Beklagten.

Da die Beklagte gerade in Form des Bundesministeriums des Innern und dem ihm nachgelagerten Bundesamt für Sicherheit in der Informationstechnik gesetzlich für die Sicherheit von Informationssystemen nicht nur innerhalb der Beklagten, sondern auch für die Öffentlichkeit gerade für die Sicherheit von Informationssystemen zuständig ist, dürfte es äußerst schwierig werden, einen Gutachter zu finden, der zu dem beweisgegenständlichen Thema über ausreichenden Sachverstand verfügt und gleichzeitig noch nicht in irgendeiner Weise für die Beklagte tätig war.

2.2 Was die konkret vom Kläger benannten Sachverständigen Schaar und Weichert anbelangt, so bestehen hier erhebliche Bedenken hinsichtlich der Kompetenz beider zu den aufgeworfenen rein technischen Fragestellungen. Herr Dr. Weichert ist nach eigenen Angaben des Klägers Jurist. Eine technische Ausbildung bzw. Tätigkeit auf technischem Gebiet ist nicht ersichtlich. Herr Schaar ist Volkswirt und verfügt nach hiesiger Kenntnis ebenfalls über keine technische Ausbildung oder Tätigkeit.

Bezüglich Herrn Prof. Pfitzmann ist weder aus seinen Veröffentlichungen, noch aus seinen aktuellen Forschungsgebieten ersichtlich, dass er sich mit den hier in Rede stehenden Technologien zur Angriffserkennung und –abwehr und damit den aktuellen Anforderungen an einen sicheren Betrieb von Telemedien näher beschäftigt oder beschäftigt hat.

Für Frau Kurz ist ebenfalls weder eine intensivere theoretische noch eine praktische Beschäftigung mit den beweisgegenständlichen technischen Themen ersichtlich.

II. Stellungnahme zum Schriftsatz des Klägers vom 9. Juni 2010

1. Keine Personenbezogenheit von IP-Adressen

Die Beklagte hält nach wie vor IP-Adressen für kein personenbezogenes Datum. Dynamische IP-Adressen werden vom Internetzugangsanbieter jeweils nur für kurze Zeit an seine das Internet nutzenden Kunden vergeben. Wie lange eine IP-Adresse einem Kunden zugeordnet bleibt, liegt im Betriebsermessen des jeweiligen Internetzugangsanbieters und ist daher von Anbieter zu Anbieter unterschiedlich. Der Internetnutzer erhält mindestens bei jeder neuen Anwahl des Internets, möglicherweise aber auch während einer laufenden Sitzung unterschiedliche IP-Adressen. Die Beklagte kann daher nicht einmal aus der gleichen mehrfach protokollierten IP-Adresse darauf schließen, dass es sich jeweils um den gleichen Nutzer handelte. Für die Beklagte als Anbieterin von Telemedienangeboten sind IP-Adressen somit lediglich Kennnummern aus einem einem Internetzugangsanbieter zur Verfügung stehenden Kontingent von IP-Adressen, den bei jedem Zugriff auf ihre Angebote ein anderer, für die Beklagte nicht zu identifizierender Kunde des Internetzugangsanbieters verwenden kann. Die für die Herstellung des Personenbezugs erforderliche Information, nämlich welchem Kunden des Internetzugangsproviders zu einem bestimmten Zeitpunkt eine bestimmte IP-Adresse zugeteilt war, steht der Beklagten nicht zur Verfügung. Die IP-Adresse ist daher für die Beklagte weder personenbezogen, noch personenbeziehbar.

2. Inhalt des Beweisbeschlusses

Selbst wenn man dies anders sieht und IP-Adressen für personenbezogene Daten hält, verkennt der Kläger offensichtlich die Funktion des § 15 TMG. Bei § 15 TMG handelt es sich um eine reine Verbotsnorm, die selbst keine Anspruchsgrundlage für den klagegegenständlichen zivilrechtlichen Unterlassungsanspruch darstellt. Auch im Übrigen enthält das TMG keine Anspruchsnorm für einen Unterlassungsanspruch. Dieser ergibt sich vielmehr ausschließlich aus §§ 823, 1004 BGB. Anspruchsvoraussetzung im Rahmen des Deliktsrechts und damit von § 823 BGB ist aber unzweifelhaft nicht nur die objektive Rechtsverletzung, sondern auch deren Rechtswidrigkeit. Das Gericht hat daher völlig zu Recht die Frage aufgeworfen, ob ein objektiver Verstoß der Beklagten gegen § 15 TMG und damit die nach § 823 BGB geschützten Persönlichkeitsrechte des Klägers analog § 904 BGB gerechtfertigt sein könnte, da der Verstoß technisch erforderlich ist, um drohende erhebliche Gefahren für die IT-Systeme der Beklagten abzuwehren. Ein solcher objektiver Verstoß gegen die geschützten Persönlichkeitsrechte des Klägers wird im Übrigen beklagtenseitig in Ermangelung ausreichender Personenbezogenheit der IP-Adresse nach wie vor ausdrücklich bestritten.

Im Hinblick auf die rechtshängige Unterlassungsklage führen die Ausführungen des Klägers zum Inhalt des Beweisbeschlusses daher an der Sache vorbei.

Der Kläger muss sich in Anbetracht seiner Ausführungen allerdings fragen lassen, ob er möglicherweise nicht mehr einen zivilrechtlichen Unterlassungsanspruch geltend machen will, sondern nur noch festgestellt haben will, dass die Beklagte mit der Speicherung von IP-Adressen gegen § 15 TMG verstößt. Zivilrechtlich dürfte hierfür ein ausreichendes Feststellungsinteresse fehlen. Verwaltungsrechtlich mag ein Feststellungsinteresse insoweit gegeben sein, hierfür ist das Landgericht aber unzuständig.

Im Übrigen sieht auch bereits § 15 TMG eine entsprechende Einschränkung ausdrücklich vor. Gemäß § 15 TMG ist nämlich die Speicherung personenbe-

zogener Daten des Nutzers ausdrücklich zulässig, soweit dies „erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen". Da es sich insoweit um eine Rechtsnorm handelt, ist der Begriff „erforderlich" zunächst rechtlich auszulegen. Unter rechtlicher Betrachtung kann die „Erforderlichkeit" nicht nur das umfassen, was technisch mindestens notwendig ist, um das Telemedienangebot zu unterhalten und den Zugriff darauf zu ermöglichen. „Erforderlich" ist vielmehr auch Alles, was notwendig ist, um einen nach dem Stand der Technik für Dienstanbieter, Nutzer und Dritte sicheren Betrieb zu gewährleisten.

Der Beweisbeschluss des Gerichtes ist daher inhaltlich richtig, da er dem Sachverständigen gerade nicht die Frage stellt, wie der Begriff der „Erforderlichkeit" auszulegen ist, sondern die rechtliche Auslegung dieses Begriffes durch das Gericht zutreffend vorwegnimmt und damit ausschließlich technischen und nicht rechtliche Fragen zum Gegenstand des Sachverständigenauftrages macht.

Die vom Kläger vorgetragenen Beweisfragen zielen dagegen ausschließlich darauf ab, den Begriff der „Erforderlichkeit" der rechtlichen Auslegung durch den Sachverständigen zu überlassen, was nicht dessen Aufgabe ist. Auch der denkbare Ansatz des Klägers, die „Erforderlichkeit" im Sinne des § 15 TMG unzutreffenderweise auf die technischen Mindestanforderungen für das Bereithalten und Abrufen der Telemedien im Internet zu reduzieren, geht fehl. Denn hierbei muss zwingend berücksichtigt werden, dass ein solcher „Mindestbetrieb" den üblichen Sicherheitsstandards nicht entspricht und gegebenenfalls aufgrund des bloßen Mindestbetriebs die Sicherheitsinteressen und damit Rechtsgüter der Beklagten und Dritter gefährdet werden.

Insgesamt vermögen die Einwände des Klägers gegen den Beweisbeschluss daher nicht zu überzeugen.

3. Speicherung der IP-Adressen durch die Beklagte

Die Beklagte verwahrt sich zunächst gegen die fortwährenden unzutreffenden Behauptungen über den Vortrag der Beklagten. Die Beklagte hat zu keinem Zeitpunkt vorgetragen, ihr stünden gleichwertige alternative Methoden zur Gefahrenabwehr, die eine Speicherung der IP-Adressen unnötig machen würden zur Verfügung. Die Ausführungen der Beklagten auf Seite 8 ihres Schriftsatzes vom 22. März 2010 tangieren diese Frage nicht im Entferntesten. Soweit der Kläger vermeintlich Ausführungen der Beklagten zitiert, erfolgt dies gezielt auszugsweise und dadurch offensichtlich bewusst entstellend. Die Beklagte hat insoweit vorgetragen:

„Bei diesen Kosten noch völlig unberücksichtigt sind Kosten für die Entwicklung alternativer Maßnahmen zur Schadprogrammabwehr, die jedoch erforderlich wären, um einen sicheren Betrieb der entsprechenden Systeme der Beklagten zu gewährleisten."

Die Beklagte bringt damit genau das Gegenteil dessen zum Ausdruck, was der Kläger mit seinem Vortrag suggerieren will. Der Beklagten stehen derzeit solche alternativen Möglichkeiten gerade nicht zur Verfügung. Diese müssten zukünftig erst entwickelt werden. Dabei kann naturgemäß niemand zum jetzigen Zeitpunkt voraussagen, ob und wann solche Technologien zur Verfügung stehen werden.

Ebenso unzutreffend ist die Behauptung, bei Zugriffen auf die vom Kläger in seinem Schriftsatz vom 9. Juni 2010 genannten Internetprotale würde keine Speicherung der IP-Adressen erfolgen. Der Kläger übersieht hier, dass in Fällen der Nichtspeicherung durch den jeweiligen Inhalteanbieter, sehr wohl durch den Betreiber des Webservers eine Speicherung in Logfiles vorgenommen werden kann.

So speichert etwa das Bundeskriminalamt als Inhalteanbieter keine IP-Adressen von Besuchern seiner Webseiten. Die Webseiten des Bundeskriminalamtes werden jedoch nicht vom Bundeskriminalamt selbst, sondern vom Zentrum für Informationsverarbeitung und Informationstechnik (ZIVIT) (IT-Dienstleister aus dem Geschäftsbereich des Bundesfinanzministeriums) gehostet. Als Provider ist das ZIVIT vertraglich verpflichtet, zum ordnungsgemäßen Betrieb der Webseiten die notwendigen Protokollierungen im Rahmen der gesetzlichen Vorschriften durchzuführen. Gemäß dieser Vorgaben werden dort somit im Rahmen der Sicherung der Log-Files auch IP Adressen gespeichert. Die Protokollierung dient hierbei

- der Sicherstellung des ordnungsgemäßen Betriebes,
- der Problemanalyse im Fehlerfall und der Fehlerbehebung,
- der Feststellung der Performance bzw. der Netzlast,
- der Erkennung von Angriffsversuchen sowie
- der Auswertung nach erfolgreichen Angriffen.

Auch bei der Auslagerung des Betriebs von Webservern von einigen Behörden der Bundesverwaltung an private Dienstleister ist davon auszugehen, dass diese zum Schutz der bei ihnen betriebenen Webdienste eine Speicherung von IP-Adressen vornehmen. Dies entspräche zumindest dem Stand der Technik.

4. Notwendigkeit der Speicherung

Die Beklagte nimmt zunächst davon Abstand, die Ausführungen des Klägers, der offensichtlich nicht nur die Rolle des Gerichtes (Formulierung des Beweisbeschlusses), sondern auch die Rolle des Sachverständigen in persona übernehmen möchte, umfassend zu kommentieren. Die Beklagte hat zur Notwendigkeit der Speicherung der IP-Adressen umfangreich vorgetragen. Wir beschränken uns daher auf einige entscheidende Anmerkungen:

4.1 Wenn der Kläger behauptet, bei sachgerecht betriebenen Webservern handele es sich um Systeme, auf denen keine andere Anwendung laufe, ist dies falsch. Für viele Telemedien erforderlich und damit sehr häufig ist mindestens die Verbindung zu einer Datenbankapplikation. Im Übrigen zielen Angriffe häufig darauf, die Abschottung der Webserver zu durchbrechen. Völlig ausgeblendet wird seitens des Klägers außerdem, dass ständig neue Angriffsszenarien und –methoden entstehen, gegen die vorsorgliche Maßnahmen nicht immer ausreichend sind. Umso wichtiger ist es in diesen Fällen, auch anhand von gespeicherten IP-Adressen solche Angriffe analysieren und zurückverfolgen zu können.

4.2 Der Kläger übersieht, dass moderne Anomalieerkennungsysteme nicht nur Verfügbarkeitsangriffe erkennen, sondern auch Angriffe zur Veränderung von Daten oder zur Löschung von sonstigen Logdaten. Die vom Kläger ersatzweise „empfohlenen" Maßnahmen können die Speicherung der IP-Adressen nicht ersetzen, da mit ihnen jedenfalls keine Vorsorge gegen weitere zukünftige Angriffe möglich ist.

4.3 Nicht nachvollziehbar ist die Aussage, erfolglose Angriffe müssten nicht erkannt werden. Diese Aussage ist aus Sicht einer sorgfältigen Angriffsabwehr naiv, da einem erfolgreichen Angriff häufig erfolglose Angriffe vorausgehen. Es ist sicherlich nicht im Sinne einer sorgfältigen Bedrohungsabwehr, eine Angreifen so lange unerkannt probieren zu lassen, bis er Erfolg hat. Gleiches gilt für die Feststellung der Datenschutzbeauftragten, „Systeme seien so sicher zu gestalten, dass Angriffe von vornherein erfolglos bleiben". Dies kommt in seiner Realitätsnähe der Aufforderung an die Pharmaindustrie gleich, endlich einen Grippeimpfstoff zu entwickeln, der gegen alle zukünftigen Mutationen der Grippeviren schützt.

4.4 Die vom Kläger zitierten Aussagen von Herrn Fox stammen aus dem Jahr 2005 und sind zwischenzeitlich überholt. Anomalieerkennung gehört heutzutage jedenfalls zum Standardrepertoire für eine sicheren IT-Betrieb. Auch die insoweit zitierten Aussagen des BSI stammen aus inzwischen veralteten Informationen des BSI. Sie beruhen auf der Annahme von statischen Webseiten, welche heute durch dynamische Webseiten weitgehend abgelöst sind.

Ebenso bezieht sich die Aussage des BSI zu der klägerseitig als „Alternative" genannten „regelmäßigen Integritätsprüfung" auf solche statischen Webseiten, die bei den heutigen dynamischen Webauftritten keinerlei Wirkung mehr haben.

4.5 Unzutreffend ist die Behauptung des Klägers, Sperrlisten seine aufgrund der Menge der IP-Adressen wirkungslos. Dabei ist bereits die angegebene Anzahl der nutzbaren IP-Adressen falsch. Diese beträgt lediglich 4,2 Milliarden Adressen. Heutige Sperrlisten enthalten teilweise bis zu 47 Millionen Einträge und stellen somit eine erheblich Einschränkung des Risikopotentials dar.

4.6 Ausschließlich ablenkender Natur ist das Argument, Sicherheitslücken müssten auf allen Webservern geschlossen werden. Dies ist eine Selbstverständlichkeit. Dies hat jedoch nichts mit dem Umstand zu tun, dass umfangreiche Hackingangriffe mit verschiedenen, zeitlich unabhängigen Aktivitäten häufig nur über die Zuordnung verschiedener Protokollinformationen mit Hilfe der IP-Adressen erkannt, analysiert und für die Zukunft abgewehrt werden können.

4.7 Insgesamt ist festzuhalten, dass die vom Kläger genannten „Alternativen" keinen ausreichenden Schutz vor Angriffen bieten können. Zu berücksichtigen ist dabei insbesondere auch, dass ohne Speicherung der IP-Adressen eine Rückverfolgbarkeit des Angriffs zum Internetzugangsanbieter und bei Straftatverdacht über diesen zum Angreifer nicht mehr möglich ist. Insoweit nützt es auch nichts, IP-Adressen „zur Wiederherstellung der Verfügbarkeit des Tele-

mediums“ speichern zu können, wie es der Kläger großzügigerweise der Beklagten gestatten will. Dies kommt dem Anschalten der Alarmanlage, nachdem der Einbrecher das Haus verlassen hat, gleich. Der Verzicht auf jegliche Rückverfolgbarkeit bedeutet aber auch den Verzicht auf jegliche Generalprävention. Es wäre somit jeder Internetnutzer eingeladen, sich als Hacker der Telemedien der Beklagten zu versuchen, da er keinerlei Konsequenzen zu fürchten hätte. Es muss an dieser Stelle nicht erläutert werden, wie sinnvoll Geschwindigkeitsbegrenzungen auf Straßen sind, die garantiert nicht überwacht werden.

Beglaubigte und einfache Abschrift anbei

[redacted]

Rechtsanwalt Rechtsanwalt