TCI
RECHTSANWÄLTE

TCI Partnerschaft von Rechtsanwälten Müller Schmidt mbB
Fasanenstr. 61 - D - 10719 Berlin

Vorab per Fax 9023-2223
Landgericht Berlin
ZK 57

10174 Berlin

TCI Partnerschaft von Rechtsanwälten Müller Schmidt mbB
Fasanenstr. 61
D - 10719 Berlin
Tel: +49 - (0)30 - 20 05 42-0
Fax: +49 - (0)30 - 20 05 42-11
www.tcilaw.de

Norman Müller
Markus Schmidt
Carsten Gerlach [1]

In Kooperation mit

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

TCI Rechtsanwälte Mainz
Stephan Breckheimer [5] LL.M. (Medienrecht)
Sabine Brumme
Dr. Olaf Griebenow
Stephan Schmidt [1]
Christian Welkenbach [3,4]

Fachanwalt für
1 Informationstechnologierecht
2 Verwaltungsrecht
3 Arbeitsrecht
4 Gewerblichen Rechtsschutz
5 Urheber- und Medienrecht

Berlin, den 28. September 2017

[redacted]
Aktenzeichen: 172/00123-08/ms

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

bedanken wir uns zunächst für die gewährte Fristverlängerung.

Zur Revisionsentscheidung des Bundesgerichtshofes nehmen wir wie folgt Stellung:

1. In Übereinstimmung mit der Entscheidung des Europäischen Gerichtshofes zur Auslegung von Art. 7 lit. f der Richtlinie 95/46 EG hat der Bundesgerichtshof festgestellt, dass § 15 Abs. 1 TMG über seinen reinen Wortlaut hinaus dahingehend auszulegen ist, dass eine Speicherung und Verarbeitung personenbezogener Daten, zu denen der Bundesgerichtshof auch die hier streitgegenständliche dynamische IP-Adresse eines Telemediennutzers zählt, über den konkreten Nutzungsvorgang hinaus auch dann erlaubt sein kann, wenn dies

zur Aufrechterhaltung der Funktionsfähigkeit des Telemediums erforderlich ist (BGH, U. v. 16.05/2017, VI ZR 135/13, Rz. 47).

Zur Entscheidung über die Zulässigkeit einer solchen Speicherung und Verarbeitung hat eine Interessenabwägung stattzufinden zwischen den Interessen des betroffenen Nutzers, dessen Daten gespeichert werden, und dem Interesse des Telemedienbetreibers die Funktionsfähigkeit des Telemediums aufrechtzuerhalten (BGH, a.a.O., Rz. 42).

Der Bundesgerichtshof hat dabei klar zum Ausdruck gebracht, dass im Hinblick auf die geringe Intensität des Eingriffs in das Recht auf informationelle Selbstbestimmung bei Speicherung der IP-Adresse durch die Beklagte dieser Eingriff bei der Abwägung eher gering wiegen dürfte (BGH, a.a.O., Rz. 43).

Außerdem abwägungsrelevant ist nach Ansicht des Bundesgerichtshofes auch der Gesichtspunkt der Generalprävention (BGH, a.a.O., Rz. 42).

Dabei dürfte unstreitig sein, dass die IP-Adresse des auf ein Telemedium zugreifenden Systems der einzige Anhaltspunkt für eine Ermittlung der Identität des Angreifers ist. Ist die IP-Adresse, mit der ein Angriff erfolgt ist, für den Telemedienbetreiber nicht (mehr) verfügbar, ist folglich eine Ermittlung des Angreifers ausgeschlossen. Wird dem Telemedienbetreiber die Speicherung der IP-Adresse generell untersagt, wie es das Klageziel des Klägers ist, bräuchte in der Konsequenz kein Angreifer mehr mit einer Identifizierung rechnen. Eine generalpräventive Wirkung entsprechender Vorschriften, die derartige Angriffe straf- oder zivilrechtlich sanktionieren, würde vollständig entfallen, da eine Sanktionsdrohung nur dann wirksam sein kann, wenn ein Täter mit seiner Entdeckung rechnen muss.

2. Entgegen der Ausführungen des Klägers in seinem Schriftsatz vom 21. August 2017 kann bei der Abwägung der Begriff der Funktionsfähigkeit nicht aus-

schließlich auf den Begriff der Erreichbarkeit und damit auf die Beachtlichkeit lediglich von „Denial-of-Service"-Angriffen (DoS-Angriffe) reduziert werden. Bei sachgerechter Auslegung muss der Begriff der Funktionsfähigkeit vielmehr auch alle Anforderungen umfassen, die für einen sicheren Betrieb des Telemediums erforderlich sind.

Moderne Angriffsszenarien, die letztendlich auch zu einem Ausfall bzw. Nichterreichbarkeit von Telemediensystemen führen können, werden häufig durch auf den ersten Blick unscheinbare Zugriffshandlungen vorbereitet bzw. eingeleitet (siehe dazu auch unten Ziffern 3.2 und 3.6).

Außerdem sollte außer Frage stehen, dass ein Anbieter von Telemedien selbstverständlich dafür Sorge zu tragen hat, dass von seinen Telemediensystemen keine vermeidbaren Gefahren für eine Kompromittierung mit Schadsoftware für andere eigene IT-Systeme, insbesondere aber auch für die IT-Systeme Dritter und hier vor allem der Telemediennutzer selbst ausgehen. Dies gilt umso mehr als die Beklagte im Zuge der voranschreitenden und unvermeidbaren Digitalisierung auch des Verwaltungshandelns zahlreiche wichtige Verwaltungsvorgänge (nur noch) über Telemediendienste anbietet.

Kommt es dennoch zu einer Infektion mit Schadsoftware durch den Zugriff auf Telemediensysteme, so ermöglicht es die Speicherung der IP-Adresse der zugreifenden Systeme dem Betreiber der Telemedien durch Weitergabe entsprechender Warnungen an die Zugangsprovider die jeweiligen Nutzer durch die Zugangsprovider warnen zu lassen und dadurch Schäden für den Nutzer oder auch nur eine weitere Ausbreitung der Schadsoftware möglicherweise zu verhindern. Gleiches gilt im Übrigen auch für Mitteilungen an Nutzer, dass deren Systeme für Botnetze missbraucht werden (s. hierzu auch die Ausführungen unter Ziffer 2.5 des Schriftsatzes vom 26. Oktober 2011 sowie unten unter Ziffer 3.5).

3. Die aktuelle Cyber-Bedrohungslage für die Telemediensysteme der Beklagten ist unverändert hoch.

3.1 So wurden alleine im 2. Quartal 2017 weltweit ca. 500 DoS-Angriffe täglich beobachtet, speziell auch mit dem Ziel der Erpressung, der politischen Einflussnahme oder einer sonstigen Schädigung des Betreibers.

Telemedien und insbesondere Webserver stehen als Angriffsziel im besonderen Fokus, da sie nach einer Übernahme durch einen Angreifer zur Verbreitung von Schadsoftware an eine Vielzahl von Opfern genutzt werden können.

Eine aktuelle Übersicht der aktuellen Angriffsmethoden bietet die OWASP Top 10 Liste (https://github.com/OWASP/Top10/raw/master/2017/OWASP%20Top%2010%20-%202017%20RC1-English.pdf).

3.2 Auf Webangebote der Beklagten erfolgen pro Woche mehrere 10.000 Angriffsversuche, hierzu gehören u.a.

- Schwachstellenscans oder potentiell gefährliche Paketanomalien,
- TCP- oder andere Protokoll-Anomalien,
- unzulässige Zugriffsversuche,
- Anomalien im Netzwerkverkehr,
- Verstöße gegen die Zugangsbeschränkung zu einzelnen Portalen und
- Verstöße gegen eine sichere Schlüsselaushandlung (wird oft zur Schwachstellenprüfung genutzt),
- DoS-Angriffe

Beweis: Zeugnis des Herrn Dr. Kai Fuhrberg, zu laden über das Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 185, 53175 Bonn

3.3 Auf Webangebote der Beklagten erfolgen pro Monat im Schnitt zwei DoS-Angriffe. Ein aktueller Vorfall erfolgte in der KW 34 auf das Webangebot der Bundesministerien für Familie, Senioren, Frauen und Jugend sowie für Wirtschaft und führte zu Ausfällen der Telemedien.

Beweis: wie vor

3.4 Betroffen sind von den Angriffen nicht nur reine Informationsangebote der Beklagten, sondern auch Fachverfahren wie das Meldeportal nach § 8b BSIG, das Warnungsportal des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe, die Plattform des Bildungsministeriums für elektronische BAföG-Anträge „eBAföG", die E-Vergabe-Plattform des Bundes für die Vergabe von öffentlichen Aufträgen des Bundes, die Plattform des Bundesverwaltungsamtes für die Online-Beantragung von Bildungskrediten sowie zahlreiche weitere Verfahren im Zuwendungsbereich.

Beweis: wie vor

Diese Verfahren haben nicht nur eine hohe Bedeutung für ein ordnungsgemäßes und fristgerechtes Verwaltungshandeln, sondern teilweise sogar für die Sicherheit der Bürger und kritischen Infrastrukturen in Deutschland.

3.5 Es ist nur mit Hilfe von IP-Adressen möglich, Besitzer von Botnetz-Clients über die Infektion ihrer Systeme zu informieren und damit u.a. Botnetze zu bekämpfen, die für Angriffe auf die Webseiten der Bundesverwaltung verwendet werden. Hierbei erfolgt die Weitergabe der IP-Adresse an die jeweils betroffenen Provider, die dann im Rahmen ihrer Möglichkeiten versuchen, das speziell betroffene IT-System zu identifizieren und dessen Betreiber zu informieren.

3.6 Eine rein präventive Absicherung bietet u.a. aufgrund der Tatsache, dass Software nicht fehlerfrei ist, keinen ausreichenden Schutz. Die im Zuge der Snowden-Veröffentlichungen bekannt gewordenen Angriffsmethoden und -tools inkl. die Ausnutzung von Zero-Day-Exploits (z. B. EternalBlue-Sicherheitslücke im Vorfall „WannaCry" (https://technet.microsoft.com/en-us/library/security/ms17-010.aspx)) oder andere aktuelle kritische Schwachstellen (z. B. in Apache Struts (https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k17-0402_update_2.html)) zeigen, dass auch IT-Systeme, die dem Stand der Technik entsprechend abgesichert werden, nicht so gestaltet werden können, dass Angriffe von vornherein erfolglos bleiben. Eine permanente Überwachung der Systeme inklusive einer angemessenen Protokollierung von notwendigen Informationen ist daher unverzichtbar.

Speziell die Speicherung von IP-Adressen über das Ende eines Nutzungsvorgangs ist in diesen Fällen erforderlich, um im konkreten Fall die generelle Funktionsfähigkeit der jeweils in Anspruch genommenen Dienste zu gewährleisten, da die Angreifer in Form von Mehrschrittangriffen (u. a. APT), zunächst versuchen, Schwachstellen der angegriffenen Webserver festzustellen um diese dann im weiteren Vorgehen auszunutzen.

Hierzu exemplarisch folgender konkreter Vorfall:

Bei einem aus dem Internet erreichbaren Webserver einer Bundesbehörde, welcher nach Stand der Technik geschützt war, wurde aufgrund eines externen Hinweises eine Uroburos-Infektion4 festgestellt. Neben dem Hinweis auf eine Infektion enthielt die Information nur einen Zeitstempel. Mit Hilfe dieses Zeitstempels konnte in den Protokolldaten die IP-Adresse des Angreifers festgestellt werden. Mit dieser Information konnten die weiteren Zugriffe des Angreifers und der konkrete Infektionsweg festgestellt und die Ursache beseitigt werden.

Ohne die gespeicherte IP-Adresse wäre eine Zuordnung nicht möglich gewesen.

Beweis: wie vor

Wie dieses Beispiel zeigt, ist es zum Schutz der angegriffenen Webserver wesentlich, verschiedene Schritte des Angriffsversuchs als zusammengehörig zu erkennen. Bei vielen Angriffen steht hierzu nur die IP-Adresse des Angreifers zur Verfügung. Erst durch die Zusammenführung mehrerer, verschiedener Schritte des Angreifers werden der Angriff und seine Auswirkungen erkennbar.

Beweis: Sachverständigengutachten

Sollte das Gericht weitere Beispiele über Art, Umfang und Wirkung von Angriffen auf die Telemedien der Beklagten sowie die Bedeutung der Telemedien für erforderlich halten, dürfen wir um einen ergänzenden Hinweis des Gerichtes bitten.

4. Zur generellen Erforderlichkeit der Speicherung von IP-Adressen für einen nach dem Stand der Technik sicheren Betrieb von Telemedien verweisen wir auf das von der Beklagten bereits als Anlage BB 5 vorgelegte Gutachten von Prof. Martini. Zu dem vom Kläger erneut angeführten Gutachten des gerichtlich bestellten Sachverständigen verweisen wir zur Vermeidung von Wiederholungen auf die dazu ergangenen Stellungnahmen vom 26. Oktober 2011 und 30. November 2012 sowie den Antrag gemäß § 412 ZPO zum Gutachten des Sachverständigen Dr. Köpsell unter Ziffer 5 des Schriftsatzes vom 26. Oktober 2011.

5. Im Hinblick auf die Ziffer 47 der Entscheidung des Bundesgerichtshofes erlauben wir uns noch einmal darauf hinzuweisen, dass die Speicherung der Zu-

griffsdaten, d. h. Zeitpunkt des Zugriffs, aufgerufene Webseite, Herkunftsseite und IP-Adresse des zugreifenden Systems bei der Beklagten generell losgelöst von der Speicherung irgendwelcher im Rahmen des Zugriffs vom Nutzer z. B. in Formularen eingegebener Daten erfolgt. Da letztere ohne Zeitstempel gespeichert werden, ist auch eine spätere Zusammenführung der Daten und damit eine Zuordnung der IP-Adresse zu möglicherweise den Nutzer identifizierenden Angaben bei der Beklagten nicht möglich.

Die vom Bundesgerichtshof geforderte Interessenabwägung kann daher auch in den Fällen nicht anders ausfallen, in denen der Nutzer während des Nutzungsvorgangs seine Personalien oder ein anderes ihn unmittelbar identifizierendes Datum angibt.

Beglaubigte und einfache Abschrift anbei

[redacted]

Rechtsanwalt