Meinhard Starostik ◆ Rechtsanwalt

RECHTSANWALTSKANZLEI
Wittestr. 30E ◆ D- 13509 Berlin
+49 30 8800030 ◆ Fax: +49 30 88000310
kanzlei@starostik.de
USt-ID-Nr.: DE165877648

KANZLEI VEREIDIGTER BUCHPRÜFER
Schwarzenberger Str. 7 ◆ D-08280 Aue
+49 3771 564700 ◆ Fax: +49 3771 5647025

Commerzbank AG
Konto: 3 855 855 00 ◆ BLZ: 430 400 36
IBAN: DE57 4304 0036 0385 5855 00
BIC: COBADEFFXXX

RA Starostik ◆ Wittestr. 30 E ◆ D-13509 Berlin

Landgericht
Littenstr. 12-17
10179 Berlin
Nur per EGVP

Mein Zeichen: 45/08

Berlin, den … Juni 2018

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

Das Inkrafttreten der Datenschutz-Grundschutzverordnung am 28. Mai 2018 lässt das Telemediengesetz unberührt und ist für die Entscheidung des Rechtsstreits ohne Bedeutung. Dies wird in dem beigefügten Aufsatzmanuskript des Klägers näher erläutert.

Nur vorsorglich für den Fall, dass die Kammer nicht schon den Vortrag der Beklagten für unerheblich hält (vgl. dazu Schriftsatz vom 08.11.2017) oder die verdachtslose Surfprotokollierung unabhängig von ihrem behaupteten Nutzen als unverhältnismäßigen Grundrechtseingriff einstuft (vgl. Schriftsatz vom 21.08.2017), wird erneut beantragt,

> **den gerichtlich bestellten Sachverständigen zur mündlichen Erläuterung seiner schriftlichen Gutachten zu laden.**

Folgende Nachfragen sollen mündlich an den Sachverständigen gerichtet werden:

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.

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?

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 Sicherheitsmaßnahmen 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 vollständigen, unverkürzten 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") anlassbezogen 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 über das Ende des Nutzungsvorgangs hinaus protokollieren, um deren Funktionsfähigkeit zu gewährleisten?

(Meinhard Starostik – Rechtsanwalt)