Niels Lepperhoff, Mareike Papendorf

# Bedeutung der jüngsten Änderungen des § 13 Abs. 7 TMG

Im Rahmen des „Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)", das am 25.07.2015 in Kraft trat, wurde neben anderen Gesetzen auch das TMG geändert. Die Berichterstattung rund um das Gesetz konzentrierte sich auf die neuen Regelungen für Betreiber kritischer Infrastrukturen, wie z. B. Energieversorgung. Dabei blieb weitgehend unbeachtet, dass vom neuen Absatz 7 des § 13 TMG (fast) alle Betreiber von Telemediendiensten betroffen sind. Damit bestehen jetzt Anforderungen an die Sicherheitsvorkehrungen von Webshops, Unternehmenshomepages, E-Mailservern u. v. m. aller Branchen und Unternehmensgrößen. Der Beitrag beleuchtet die neue Regelung, insbesondere aus dem technischen Blickwinkel, und schätzt die Konsequenzen für die Praxis ab.

## 1 Neu im TMG

Das am 25.07.2015 in Kraft getretene IT-Sicherheitsgesetz ergänzte § 13 Telemediengesetz (TMG) um einen neuen Absatz 7, der wie folgt lautet:

***„(7) Diensteanbieter haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass***

***1. kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und***

***2. diese***

***a) gegen Verletzungen des Schutzes personenbezogener Daten und***

***b) gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind,***

***gesichert sind. Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Eine Maßnahme nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens."***

Zusätzlich wurden die Bußgeldregelungen des § 16 Abs. 2 Nr. 3 TMG um Verstöße gegen § 13 Abs. 7 S. 1 Nr. 1 und Nr. 2a TMG ergänzt. Hervorzuheben ist, dass ein Verstoß gegen Nr. 2b nicht bußgeldbewehrt ist.

**Mareike Papendorf, LL.M.**

hat Wirtschaftsrecht an den Hochschulen Köln und Trier studiert. Sie ist bei der Xamit Bewertungsgesellschaft mbH als Beraterin beschäftigt. Ihr Tätigkeitsschwerpunkt liegt auf dem Datenschutzrecht.
E-Mail: info@xamit.de

**Dr. Niels Lepperhoff**

Geschäftsführer der Xamit Bewertungsgesellschaft mbH
Schwerpunkte: Datenschutz und IT-Sicherheit

E-Mail: info@xamit.de

## 2 Was wird geschützt?

§ 13 Abs. 7 TMG nennt drei Schutzanforderungen:

- Schutz vor unerlaubtem Zugriff auf die für Telemedienangebote genutzten technischen Einrichtungen (Nr. 1),
- Sicherung gegen Verletzungen des Schutzes personenbezogener Daten (Nr. 2a) und
- Sicherung gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind (Nr. 2b).

Diese Schutzanforderungen werden in den folgenden Kapiteln beleuchtet.

### 2.1 Für Telemedienangebote genutzte technische Einrichtungen

Die erste Anforderung beschränkt sich technisch auf den Zugriffsschutz. Ihr Anwendungsbereich umfasst neben dem eigentlichen Telemediendienst (Webseite, Shop, E-Mail usw.) auch alle „für ihre Telemedienangebote genutzten technischen Einrichtungen". Im Unterschied zu § 9 BDSG ist der sachliche Bezug der Telemediendienst und nicht der Personenbezug der Daten. Zu diesen technischen Einrichtungen zählt auf jeden Fall der Server.

Zugriffsmöglichkeiten bestehen

- auf Hardwareebene für alle Personen, die physikalischen Zugang zum Server besitzen,
- auf Betriebssystemebene, da moderne Betriebssysteme eine eigene Nutzerverwaltung besitzen,
- auf die lokal installierte Datenbank, die ihrerseits eine eigene Nutzerverwaltung mitbringt und
- auf die Software, die den Telemediendienst letztlich realisiert.

Server nutzen regelmäßig lokale Netzwerke, z. B. innerhalb eines Rechenzentrums, für den Anschluss an das Internet, an Festplatten („SAN"), Datenbanken oder Backupgeräte. Diese Geräte verfügen ebenfalls über Nutzerverwaltungen. Gleiches gilt für Netzwerkgeräte wie managed Switche, Router und Firewalls.

Sachlich ist diese Anforderung zutreffend, da prinzipiell alle unterschiedlichen Geräte im Netzwerk für ein unbefugtes Eindringen verwendet werden können. Neu ist hingegen die Bußgeldbewehrung.

Eine systematische Konzeption der technischen und organisatorischen Maßnahmen, die alle beteiligten Geräte einbezieht, erscheint geboten, um „vergessene" Geräte zu vermeiden und die Schutzmaßnahmen aufeinander abzustimmen. Administrationspasswörter bspw., die der Werkseinstellung entsprechen, dürften zukünftig eine Ordnungswidrigkeit darstellen, da sie wegen der regelmäßig gegebenen allgemeinen Bekanntheit keinen Zugriffsschutz bieten.

### 2.2 Schutz personenbezogener Daten

Die zweite Anforderung bezieht sich explizit auf den Schutz von personenbezogenen Daten, so dass sich für die inhaltliche Ausgestaltung ein Rückgriff auf § 9 BDSG und seine Anlage anbietet. An dieser Stelle wird deshalb auf die Literatur zu § 9 BDSG und seiner Anlage verwiesen.[1] [2]

### 2.3 Störungen

Die dritte Anforderung betrifft „Störungen, auch soweit sie durch äußere Angriffe bedingt sind". Der Begriff „Störung" ist im TMG nicht definiert und auch in anderen Gesetzen lässt sich eine Legaldefinition nicht finden. Daher ist der Begriff der „Störung" nach dem allgemeinen Sprachgebrauch auszulegen. Es bietet sich an, unter „Störung" ein Verhalten des Telemediendienstes zu verstehen, das nicht der vom Diensteanbieter festgelegten Spezifikation folgt. Auf das subjektive Erwarten eines Nutzers käme es nicht an. Abschaltungen für Wartungen wären demnach keine Störung. Aber auch intendierte Eigenschaften, wie z. B. ein langsamer Seitenaufbau bei Webseiten oder Shops, wären eine gewünschte Diensteigenschaft und keine Störung.

Eine Störung kann demnach auch eine beeinträchtigte Verfügbarkeit des Telemediendienstes sein. Mögliche Ursachen sind z. B. Hardwaredefekte, Softwarefehler oder Fehlbedienung. Allerdings können unerwartet viele Zugriffe ebenfalls zu einer Überlastung des Telemediendienstes führen, der in der Folge „gestört" ist. Mit Blick auf die oben vorgeschlagene Definition, wäre eine solche Überlastung keine „Störung" i. S. d. Gesetzes, da lediglich die für den Telemediendienst vorgesehene Nutzeranzahl überschritten wurde. Aus Sicht der Nutzer liegt indes eine Nichtverfügbarkeit vor. Die genauere Bestimmung des Begriffs „Störung" bleibt Aufgabe von Gerichten und Aufsichtsbehörden.

Äußere Angriffe auf den Telemediendienst werden durch den Zusatz von „auch" als *eine* mögliche Ursache einbezogen. Zu den Angriffen zählen sicherlich DDoS-Angriffe, bei denen eine Vielzahl leistungsfähiger Sever den PC des Telemediendienstes mit präparierten Anfragen überschütten, so dass er fast ausschließlich mit deren Verarbeitung anstelle der normalen Diensterbringung beschäftigt ist.

Der Begriff „Störung" lässt sich auch im Kontext der Störung Dritter begreifen. Denkbar wäre hier z. B., dass Unbefugte den Telemediendienst zur Mailware-Verteilung oder im Rahmen von DDoS-Angriffen nutzen.

Im Unterschied zu den beiden anderen Anforderungen ist diese nicht direkt bußgeldbewehrt (§ 16 Abs. 2 Nr. 3 TMG). Für Opfer eines DDoS-Angriffs ist es tröstlich, dass der wirtschaftliche Schaden nicht durch ein Bußgeld erhöht wird. Wenn ein Telemediendienst seinerseits für Angriffe unbefugt verwendet wird, liegt regelmäßig mindestens ein Verstoß gegen die Sicherungspflicht vor unbefugtem Zugriff (§ 13 Abs. 7 Nr. 1 TMG) vor, da andernfalls die Unbefugten keinen Zugriff hätten. Insofern kann auch im Schadensfall ein Bußgeld drohen. In beiden Fällen können zusätzlich Schadensersatzansprüche gegen den Diensteanbieter entstehen.

## 3 Wer ist betroffen?

§ 13 TMG befindet sich im Abschnitt 4 des Gesetzes. Dieser Abschnitt enthält hinsichtlich der Erhebung und Verwendung personenbezogener Daten Ausnahmen für Dienst- und Arbeitsverhältnisse sowie für die Steuerung von Arbeits- und Geschäftsprozessen (§ 11 Abs. 1 TMG). Die neuen Vorgaben zur Sicherheit beziehen sich nicht auf die Erhebung oder Verwendung personenbezogener Daten, d. h. die genannten Ausnahmen sind nicht einschlägig.

Dem Wortlaut nach richtet sich der Abs. 7 an „geschäftsmäßig angebotene Telemedien". Die Bezeichnung findet sich bspw. auch bei der Impressumspflicht in § 5 Abs. 1 TMG, so dass sich eine analoge Auslegung anbietet. Nach der Gesetzesbegründung zu § 5 TMG versteht der Gesetzgeber unter „geschäftsmäßig" in der Regel gegen Entgelt erbrachte Telemediendienste.[3] Das OLG Hamburg[4] präzisiert in seiner Auslegung den Begriff dahingehend, dass er kommerzielle, d. h. den Vertrieb von Waren oder Dienstleistungen fördernde oder Werbung schaltende Telemediendienste umfasse. Auf die Erhebung eines Entgelts komme es nicht an. Geschäftsmäßige Dienste grenzen sich lediglich von privaten Webseiten wie auch Webseiten von Idealvereinen ab, die nach dem Willen des Gesetzgebers nicht der Impressumspflicht unterliegen sollen.

Damit unterfallen alle Telemediendienste von Unternehmen, Behörden, Vereinen und Parteien der neuen Regelung. Beispiele:

- Webshops
- Webseiten
- Apps
- E-Mailserver
- Instant Messaging Server (z. B. Teamspeak)
- FTP Server

1 GOLA, Peter ; KLUG, Christoph ; KÖRFFER, Barbara ; SCHOMERUS, Rudolf: Bundesdatenschutzgesetz. 10., überarb. und erg. Aufl. Beck, München 2010–, § 9.

2 DÄUBLER, Wolfgang ; KLEBE, Thomas ; WEDDE, Peter ; WEICHERT, Thilo: Bundesdatenschutzgesetz. Vollst. neu bearb. Aufl. Bund-Verl., Frankfurt 2010. § 9.

3 Deutscher Bundestag, 16. Wahlperiode, Drucksache 16/3078 vom 23.10.2006, § 5.

4 OLG Hamburg (2007): Urteil v. 03.04.2007 – Az. 3 W 64/07

§ 13 Abs. 7 S. 1 TMG beinhaltet drei Schranken. Vorkehrungen müssen nur getroffen werden, sofern sie

- technisch möglich sind,
- wirtschaftlich zumutbar sind und
- in die jeweilige Verantwortlichkeit des Diensteanbieters fallen.

### 3.1 Verantwortlichkeit

Die Begrenzung auf die jeweilige Verantwortlichkeit wirft Fragen auf. Zivilrechtlich beschränkt sich „Verantwortlichkeit" grundsätzlich auf die eigene Handlungssphäre. Datenschutzrechtlich sind Auftraggeber im Rahmen einer Auftragsdatenverarbeitung zusätzlich für die Handlungen ihrer (Unter-)Auftragnehmer verantwortlich (§ 11 Abs. 1 BDSG). Die Verantwortlichkeit erstreckt sich auch auf die IT-Sicherheitsmaßnahmen (§ 11 Abs. 2 BDSG). Mit der Neuregelung im TMG wird, mit Blick auf die Bußgeldbewehrung, diese Abgrenzungsfrage bedeutsam, wie am Beispiel des Hostings einfach nachvollziehbar ist (Tabelle 1).

**Tabelle 1 | Verantwortlichkeit eines Hosting-Dienstleisters**

| | Auslegung zivilrechtlich | Auslegung datenschutzrechtlich |
|---|---|---|
| Hoster im shared Hosting eines Webshops | Hardware<br>Netz-Firewall<br>Betriebssystem<br>Datenbank<br>Middleware (z.B. PHP)<br>Virtualisierung | weisungsabhängig |
| Betreiber eines Webshops | Shopsystem | Hardware<br>Netz-Firewall<br>Betriebssystem<br>Datenbank<br>Middleware (z.B. PHP)<br>Virtualisierung<br>Shopsystem |

Die zivilrechtliche Auslegung entspricht der tatsächlichen Verfügungsgewalt über die technischen Komponenten. Die datenschutzrechtliche Auslegung bürdet dagegen dem Betreiber die Verantwortung auch für die Einrichtungen beim Hoster auf, d. h. der Betreiber müsste die Sicherheitsmaßnahmen in Gänze konzipieren und die Umsetzung überwachen. Beim Shared Hosting teilen sich zahlreiche Betreiber eine Hardware, sodass Weisungen eines Betreibers bspw. auf Betriebssystemebene alle anderen Betreiber tangieren.

Die Position der Vorschrift im Abschnitt 4 „Datenschutz" des TMG spricht für die datenschutzrechtliche Auslegung. Allerdings geht die Formulierung „gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind" in § 13 Abs. 7 S. 1 Nr. 2 b) TMG über einen reinen Datenschutzbezug hinaus. Vor dem Hintergrund der für den Betreiber faktisch nicht bestehenden Verfügungsgewalt spricht vieles für die zivilrechtliche Auslegung. Sie ist insofern sachgerechter, als sie jeden Beteiligten in seiner Einflusssphäre in Verantwortung nimmt.

Manche Telemediendienste (z. B. Microsoft Exchange mit Outlook, Teamspeak, Whatsapp) bestehen aus einer Server- und Clientkomponente. Im Unterschied zu den Servern werden die Clients beim Nutzer installiert und von diesem genutzt. Der Client befindet sich in der Einflusssphäre des Nutzers. Allerdings kann der Betreiber – je nach Dienst – über Servereinstellungen die Sicherheitseinstellungen beim Client ohne Mitwirkung des Benutzers beeinflussen. Beispiel: Passwortvorgabe bei Outlook. Einstellungen die nur der Betreiber vornehmen kann, lassen sich eindeutig seiner Einflusssphäre zuordnen, d. h. er ist für eine gesetzeskonforme Konfiguration verantwortlich.

### 3.2 Wirtschaftlich zumutbar

Während § 9 BDSG, der die technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten allgemein regelt, von „einem angemessenen Verhältnis zu dem angestrebten Schutzzweck" spricht, begrenzt § 13 Abs. 7 S. 1 TMG die Maßnahmen u. a. auf solche, die „wirtschaftlich zumutbar" sind. Eine Abwägung gegen den Schutzzweck ist nicht vorgesehen.

Die Orientierung am Schutzzweck sorgt für eine Balance zwischen Kosten für Sicherheitsmaßnahmen und dem erreichten Schutzniveau. Bspw. bedürfen IP-Nummern sicherlich weniger starker Schutzmaßnahmen als Röntgenbilder.

Die wirtschaftliche Zumutbarkeit orientiert sich am Diensteanbieter. Für die Bestimmung der Zumutbarkeit könnte bspw. der Umsatz herangezogen werden, womit umsatzschwächere Unternehmen weniger Sicherheitsmaßnahmen treffen müssten als umsatzstärkere. Wie hoch muss der Anteil der Sicherheitsausgaben am Umsatz oder an den Gesamtausgaben sein, damit es wirtschaftlich zumutbar ist? Ist die Bezugsgröße eine Einzelmaßnahme oder die Summe aller Maßnahmen? Die Aufsichtsbehörden und Gerichte dürften sich bald mit diesen Fragen beschäftigen müssen.

### 3.3 Technisch möglich

Auf dem ersten Blick erscheint die Einschränkung auf das technisch Mögliche redundant, da keiner zu einer unmöglichen Handlung verpflichtet werden kann. Deshalb lässt die Formulierung „[…] Diensteanbieter haben, soweit dies technisch möglich […] sicherzustellen, dass […]" in § 13 Abs. 7 S. 1 TMG auch die Auslegung zu, dass *genau* das technisch Mögliche umzusetzen sei.

Sicherheit hängt neben der eingesetzten Technik auch von der Nutzerakzeptanz ab, wie sich leicht am Beispiel der Passwortlänge nachvollziehen lässt. Passwörter sichern zahlreiche Telemedien vor unbefugtem Zugriff. Die Längen von Passwörtern sind ein Faktor, der über den Erfolg von Brute-Force-Angriffen entscheidet.[5] Bisher orientieren sich die empfohlenen Passwortlängen auch an der zum Erraten nötigen Zeit.[6] Nutzer bevorzugen kurze und leicht zu merkende Passwörter. Eine Orientierung an der technisch maximal möglichen Länge lässt deshalb die Akzeptanz beim Nutzer außer Acht und stellt auf großzügig gewählte Längen ab: Passwörter mit 1.000 und mehr Zeichen sind technisch möglich, sofern ausreichend Speicherplatz zur Verfügung steht.

Einen Ausweg bietet Satz 2 an: „Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen." Zum Stand der Technik lässt sich nicht nur die technische Entwicklung der Sicherheitsmaßnahmen zählen, sondern – spiegelbildlich – auch die der Angriffstechniken. Unter Berücksichtigung von Angriffstechniken wären Sicherheitsmaßnahmen so auszuwählen, dass sie die angestrebten Schutzzwecke erreichen, d. h. die Angriffe vereiteln. Übertragen auf das Beispiel der Passwörter wäre eine

5 Fox, Dirk (2009): Mindestlängen von Passwörtern und kryptographischen Schlüsseln, DuD 10/2009. S. 620-623.

6 Fox, Dirk; Schaefer, Frank (2009): Passwörter – fünf Mythen und fünf Versäumnisse, DuD 7/2009, S. 425-429.

Länge, die einen Brute-Force-Angriff unattraktiv macht, ausreichend, auch wenn diese kleiner als die technisch möglich wäre.

## 4 Stand der Technik

§ 13 Abs. 7 S. 2 TMG verlangt, dass die Vorkehrungen, d. h. die technischen und organisatorischen Maßnahmen, den Stand der Technik berücksichtigen müssen. Das anschließend gegebene Beispiel „Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens" – auch wenn es sich in ähnlicher Formulierung in § 9 Anlage BDSG findet – hilft bei der Interpretation des Begriffs „Stand der Technik" nicht weiter, da eine Verschlüsselung gegen unbefugten Datenzugriff hilft aber bspw. nicht gegen Hardwaredefekte. Eine Verschlüsselung kann mittels unterschiedlicher Algorithmen erreicht werden, die ihrerseits dem technischen Fortschritt unterworfen sind.

„Stand der Technik" wird weder im TMG noch im BDSG definiert. Wegen der vergleichbaren Regelungsmaterie bietet sich ein Rückgriff auf § 3 Abs. 6 BImSchG an, so dass „Stand der Technik" im Bezug zu IT-Sicherheit verstanden werden kann als der „Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme […] gesichert erscheinen lässt". Verfahren, Einrichtungen oder Betriebsweisen entsprechen den im Datenschutz geläufigen technischen und organisatorischen Maßnahmen. Entscheidendes Kriterium ist die gesicherte Eignung in der Praxis zur Erfüllung der gesetzlichen Anforderungen.

Für die konkrete Ausgestaltung bietet sich der BSI-Grundschutz-Katalog[7] an, der für 570 Gefahren Maßnahmen zur Reduktion der Eintrittswahrscheinlichkeit oder Schadenshöhe vorschlägt. Welche Maßnahmen ergriffen werden sollten, muss im Einzelnen ausgehend von dem Schutzbedarf und der konkreten Gestaltung des Telemediendienstes entschieden werden. Ein Vorgehen zur Auswahl der Maßnahmen analog zu etablierten Standards wie BSI 100-2[8] oder DS-BvD-GDD-01[9] ist empfehlenswert, um nachweisen zu können, dass die Konzeption der IT-Sicherheitsmaßnahmen sorgfältig und dem Stand der Technik entsprechend erfolgte. Zusätzlich können für Teilaspekte weitere Normen, wie die ISO 27001 für das Informationssicherheitsmanagement, herangezogen werden.

PHP stellt für zahlreiche Content-Management-Systeme und auch Webshop-Systeme Basisfunktionen bereit, d. h. es wird von sehr vielen Websites eingesetzt. 2013 verwendeten 45% der untersuchten Webpräsenzen mit PHP die zum damaligen Zeitpunkt nicht mehr gepflegten Versionen 5.0 bis 5.2.[10] Diese Versionen können Sicherheitslücken enthalten, die unbefugte Zugriffe auf die mit diesen Versionen betriebenen Websites ermöglichen. Solche Lücken würden nicht mehr geschlossen werden.

Gemäß des Bausteins M 2273 aus dem BSI-Grundschutz-Katalog ist ein zeitnahes Einspielen sicherheitsrelevanter Patches notwendig,[11] d. h. Stand der Technik. Wird auf das Einspielen verzichtet und bleiben in der Folge Sicherheitslücken bestehen, die Unbefugten Zugriff eröffnen (§ 13 Abs. 7 Nr. 1 TMG) oder den Schutz personenbezogener Daten (§ 13 Abs. 7 Nr. 2a TMG) verletzen können, droht ein Bußgeld (§ 16 Abs. 3 TMG) von bis zu 50.000 Euro. Was vor der Gesetzesänderung wie eine Nachlässigkeit behandelt wurde, stellt jetzt u. U. eine Ordnungswidrigkeit dar.

Der Umgang mit Patches ist nur ein Beispiel dafür, dass die Gesetzesänderung nicht den Status quo festschreibt, sondern neue Anforderungen definiert. Der Gesetzgeber beabsichtigt mit der Änderung des TMG „Defizite im Bereich der IT-Sicherheit […] abzubauen".[12] Die Schutzwirkung von IT-Sicherheitsmaßnahmen hängt auch von den Mitteln der Angreifer ab. Insofern lässt sich der Ausdruck „Stand der Technik" auch als „Stand der *Angriffs*technik" begreifen. Der Baustein M 2.35 des BSI-Grundschutz-Katalogs[13] sieht die Pflicht zur regelmäßigen Informationsbeschaffung über Sicherheitslücken vor. Auch wenn die Informationsbeschaffung keine direkte Auswirkung auf die Sicherheit eines Telemediendienstes hat, ist sie doch eine Vorbedingung, um neue Gefahren zu erkennen. Damit dürfte die Informationsbeschaffung zu den gesetzlich geforderten organisatorischen Vorkehrungen zu rechnen sein.

Die beiden vorgenannten Beispiele verdeutlichen, dass der Begriff „Stand der Technik" die Umsetzung des BSI-Grundschutz-Katalogs – oder vergleichbarer Maßnahmen – nahe legt. Für Diensteanbieter besteht deshalb Handlungsbedarf, die technischen und organisatorischen Maßnahmen ihrer Telemediendienste strukturiert zu konzeptionieren und umzusetzen. Dieses schließt eine sorgfältige Auswahl des Hosters mit ein.

## 5 Fazit

Der neu in § 13 TMG aufgenommene Absatz 7 lässt Raum für unterschiedliche Auslegungen. Diese betreffen zentrale Aspekte der Vorschrift, von der Verantwortlichkeit der an der Erbringung eines Telemediendienstes mitwirkenden Akteure über die Begriffe „Störung" und „technisch möglich" bis hin zur Schranke des „wirtschaftlich zumutbaren". Damit besteht Unsicherheit hinsichtlich der Frage, welche Maßnahmen konkret gesetzlich vorgeschrieben sind – und wie die Grenzen der Verpflichtung zu ziehen sind. Eine zügige Auslegung durch Gerichte und Aufsichtsbehörden ist wünschenswert, um den momentanen Zustand der Rechtsunsicherheit zu beenden.

Automatisierte Schwachstellenscanner testen Telemediendienste auf bekannte Lücken und damit auch auf das Vorhandensein von technischen Vorkehrungen. Damit werden Aufsichtsbehörden in die Lage versetzt, die Einhaltung der neuen Regeln zu überwachen. Weiterhin lässt sich mit Blick auf die Rechtsprechung zu §§ 5[14] und 13 Abs. 1[15] TMG nicht ausschließen, dass Verstöße gegen § 13 Abs. 7 TMG auch als Wettbewerbsverstöße gelten könnten. Daher sind wettbewerbsrechtliche Abmahnungen durch Konkurrenzunternehmen oder Verbraucherzentralen und ähnliche Organisationen nicht auszuschließen.

7 URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

8 URL: https://www.bsi.bund.de/DE/Publikationen/BSI_Standard/it_grundschutzstandards.html

9 URL: http://www.dsz-audit.de/datenschutzstandard/

10 Xamit (2014): Datenschutzbarometer 2013. URL: http://www.xamit-leistungen.de/downloads/XamitDatenschutzbarometer2013.pdf S. 14.

11 URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02273.html

12 Deutscher Bundestag (2015): Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme. Drucksache 18/4096. S. 2

13 URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02035.html

14 z.B. OLG Hamburg (2007): Urteil v. 03.04.2007 – Az. 3 W 64/07

15 z.B. OLG Hamburg, 27.06.2013 – 3 U 26/12