Neue Sicherungspflicht für Telemediendiensteanbieter Webseitensicherheit jetzt Pflicht nach dem IT-Sicherheitsgesetz

Christian Djeffal

Das IT-Sicherheitsgesetz schafft eine Pflicht zur Sicherung von Telemediendiensten im neuen § 13 Abs. 7 TMG. Der vorliegende Beitrag untersucht diese Sicherungspflicht und illustriert ihre rechtlichen und praktischen Auswirkungen. Die Sicherungspflicht bezweckt, dem Trend entgegenzuwirken, durch Kompromittieren von Telemediendiensten auf Daten zuzugreifen und Schadcode zu verbreiten.

Der Beitrag erläutert eingehend die Tatbestandsmerkmale des § 13 Abs. 7 TMG und beleuchtet die rechtlichen Auswirkungen insbesondere im öffentlichen Recht und im Zivilrecht. In zwei fiktiven Fallstudien werden die praktischen Konsequenzen für einen Handwerksbetrieb mit einer einfachen Webseite und ein mittelständisches Unternehmen mit einem Webshop skizziert. § 13 Abs. 7 TMG statuiert eine abstrakte Regel, die sich dem raschen technischen Wandel anpasst, aber auch fortlaufend konkretisiert werden muss. In der Praxis lassen sich die Maßnahmen zumutbar an Dritte auslagern.

I. Einleitung

Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), das am 24.7.2015 in Kraft getreten ist,[1] fördert die IT-Sicherheit in der Spitze wie in der Breite. Im Vergleich zu den Informationspflichten der Betreiber kritischer Infrastrukturen wurden die Sicherungspflichten des § 13 Abs. 7 TMG trotz ihrer großen Praxisrelevanz bisher nur selten erörtert.[2] Deshalb untersucht dieser Beitrag die Norm eingehend, indem er Hintergrund und Gesetzeszweck (II.), Schutzgüter und Rechtsnatur (III.), dogmatische Struktur und Begriffsauslegung (IV.) sowie rechtliche und praktische Auswirkungen (V.) von § 13 Abs. 7 TMG erläutert.

II. Hintergrund und Gesetzeszweck

Der Zweck der neuen Norm wird erst vor dem Hintergrund der Umstände ihrer Einführung greifbar. Zusammengefasst steht einer wachsenden Bedrohung durch Cyberkriminalität aller Art eine verbreitete „digitale Sorglosigkeit" gegenüber.[3] Daten, die in gedruckter Form nicht zugänglich sind, werden digital mangelhaft gesichert und damit leicht zugänglich gemacht.

Die Zahl der Angriffe auf Computer und andere informationstechnische Systeme steigt immer weiter. Das *BKA* verzeichnet einen konstanten Anstieg von Cybercrime, der sich besonders im Bereich von Datenveränderung und Computersabotage auswirkt.[4] Täglich werden mittlerweile ca. 200.000 neue Schadcode-Samples entdeckt.[5] Konjunktur haben dabei insbesondere Methoden, die Schadcode über das Internet durch Webseiten und Dienste unbeteiligter Dritter verbreiten.[6] Bei sog. „drive-by"-Attacken wird der Computer des Nutzers infiziert, während er Webseiten oder Dienste eines unbescholtenen Drittanbieters nutzt.[7] Gefahren lauern sowohl auf großen Webseiten mit hohen Nutzerzahlen, wie Internetportalen oder Nachrichtenseiten,[8] aber auch auf weniger aufwendigen und weniger frequentierten Webseiten wie Blogs. Schadcode wird dabei auch auf

Flächen, die für Werbung („malvertising") oder „user-generated content" bereitgehalten werden, platziert.

Die führenden IT-Sicherheitsanbieter zählen diese Verbreitungsformen jetzt schon zu den größten Bedrohungen,[9] erwarten sogar eine Steigerung von Gefährlichkeit und Häufigkeit der Attacken.[10] Auch nach dem Lagebericht des *Bundesamts für die Sicherheit in der Informationstechnik* (*BSI*) resultiert aus solchen Attacken eine erhebliche Gefahr.[11] Das verwundert nicht, wenn man bedenkt, dass ein Sicherheitsanbieter 75% der im Internet erreichbaren Webseiten als verwundbar eingestuft hat, wobei 20% aller Webseiten kritisch verwundbar seien.[12] Beim (ungewollten) Hosten von Malware auf Webseiten wird Deutschland derzeit an zweiter Stelle gesehen.[13] Die u.a. dadurch geschaffenen Gefahren wirken sich deutlich aus: Schätzungen gehen weltweit von einem hohen wirtschaftlichen Schaden durch Cybercrime aus.[14] Nirgends sei dieser Schaden im Verhältnis zum Bruttoinlandsprodukt so hoch wie in Deutschland.[15]

Trotzdem werden oft einfache und teilweise sogar kostenlose Maßnahmen zur Sicherung der Integrität informationstechnischer Systeme schlichtweg unterlassen, sodass etwa personenbezogene Daten oder Geschäftsgeheimnisse leicht zugänglich sind. Vor dem Hintergrund dieser sich immer wieder realisierenden Gefahren und des daraus resultierenden Schadens ist die Regelung des § 13 Abs. 7 TMG zu lesen. Das Gesetz bezweckt die Sicherung von Telemediendiensten im Hinblick auf bestimmte Schutzgüter.

III. Schutzgüter und Rechtsnatur

Die von der Vorschrift geschützten Rechtsgüter können insbesondere aus § 13 Abs. 7 Nr. 1 und Nr. 2 TMG abgelesen werden. Aus § 13 Abs. 7 Nr. 1 TMG ergibt sich, dass es um die Integrität und Vertraulichkeit informationstechnischer Systeme geht. Unmittelbar betrifft Nr. 1 zwar nur die Systeme des Telemediendiensteanbieters, mittelbar bezweckt die Vorschrift aber gerade den Schutz der Systeme der Nutzer. § 13 Abs. 7 Nr. 2a TMG adressiert den Schutz personenbezogener Daten und damit auch den Schutz des Rechts auf informationelle Selbstbestimmung, während § 13 Abs. 7 Nr. 2b TMG den Schutz der Funktionsfähigkeit des Telemediendienstes selbst regelt. Neben dem allgemeinen staatlichen Schutzauftrag dient die Vorschrift mithin auch der Erfüllung grundrechtlicher Schutzpflichten des allgemeinen Persönlichkeitsrechts. Sie dient vor allem dem Recht auf informationelle Selbstbestimmung[16] und dem Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme.[17]

Die Rechtsnatur des § 13 Abs. 7 TMG ergibt sich aus Wortlaut und Regelungstechnik: Es handelt sich um eine Sicherungspflicht. Der Regelungstechnik nach ist diese Sicherungspflicht eine generische Abwägungsregel, die Abwägungsschritte beschreibt, ohne alle Maßnahmen im Einzelnen zu regulieren. Diese Form der Regulierung erlaubt es, flexibel auf neue Bedrohungen zu reagieren, und belässt dabei genügend Spielraum für Einzelfallgerechtigkeit. Sie stellt aber auch hohe Anforderungen an die Abwägenden, also insbesondere an Rechtsberatung und Judikatur.

IV. Dogmatische Struktur und Begriffsauslegung

Gliedert man die Voraussetzungen der Sicherungspflicht aus § 13 Abs. 7 TMG nach ihrer dogmatischen Struktur, ergibt sich eine Prüfung in vier Schritten. Diese betreffen die Anwendbarkeit, den Inhalt, das Ziel – nämlich die Erfolgsverhinderung – und die Grenzen der Sicherungspflicht. Im Rahmen dieser Struktur werden die einzelnen Merkmale der Sicherungspflicht ausgelegt.

1. Anwendbarkeit

Die Pflicht aus § 13 Abs. 7 TMG ist anwendbar auf Diensteanbieter, die Telemediendienste geschäftsmäßig anbieten. Telemedien werden in § 1 Satz 1 TMG als elektronische Informations- und Kommunikationsdienste definiert, sofern es sich nicht um reine TK-Dienste, tk-gestützte Dienste oder Rundfunk handelt.[18] Webseiten im Internet können also in der Regel als Telemediendienste qualifiziert werden.

Nach der Gesetzesbegründung des § 13 Abs. 7 TMG liegt die Geschäftsmäßigkeit beim Erbringen von Telemediendiensten dann vor, wenn sie „auf einer nachhaltigen Tätigkeit beruht, es sich also um eine planmäßige und dauerhafte Tätigkeit handelt. Bei einem entgeltlichen Dienst liegt dies regelmäßig vor, so z.B. bei werbefinanzierten Webseiten. Das nicht-kommerzielle Angebot von Telemedien durch Private und Idealvereine wird demgegenüber nicht erfasst."[19] Anders als bei der enger gefassten Erwerbsmäßigkeit ist die Entgeltlichkeit nicht das entscheidende Kriterium zur Bestimmung der Geschäftsmäßigkeit.[20]

In persönlicher Hinsicht werden Diensteanbieter erfasst, also gem. § 2 Nr. 1 TMG „jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt".[21] Nicht nur das Bereithalten eigener, sondern auch fremder Inhalte fällt darunter. Auch Portalbetreiber, die Inhalte Dritter anbieten, Internetauktionshäuser oder Diskussionsforen sind Diensteanbieter.[22] Entscheidendes Kriterium ist die Ausübung der Funktionsherrschaft über den Telemediendienst aus Nutzerperspektive in rechtlicher und tatsächlicher Hinsicht.[23] Während die Diensteanbietereigenschaft im TMG sehr weit gefasst ist und sich nicht nur auf eigene Inhalte bezieht, sind Diensteanbieter nach den §§ 7 ff. TMG grundsätzlich nur für eigene (oder sich zu eigen gemachte) Informationen verantwortlich; für fremde Informationen bestehen keine allgemeinen Überwachungs- und Nachforschungspflichten. Der Diensteanbieter macht sich Informationen „zu eigen", wenn er sich dergestalt mit der Information identifiziert, dass sie als seine eigene erscheint.[24] Dass die Grenzen der Verantwortlichkeit auch für § 13 Abs. 7 TMG gelten, wird mit dem Zusatz „im Rahmen ihrer jeweiligen Verantwortlichkeit" klargestellt.

Obwohl die Abgrenzung von der generellen Sicherungspflicht zur Verantwortlichkeit für fremde Informationen trennscharf ist, kann es in der Praxis zu Abgrenzungsschwierigkeiten kommen. Grundsätzlich wird man davon ausgehen, dass fremder Schadcode, der etwa auf einer sichtbar abgetrennten Fläche verbreitet wird, nicht in den Verantwortungsbereich des Diensteanbieters fällt. Manipuliert ein Dritter den Code auf der Webseite des Diensteanbieters, so bleibt der Diensteanbieter für den Code verantwortlich, weil es sich um eigene Informationen handelt.[25] Schleust ein Dritter Code auf eine Webseite des Diensteanbieters, so ist der Diensteanbieter jedenfalls dann auch für fremde Schadprogramme verantwortlich, wenn sie aus der Sicht eines

verständigen Nutzers zum Angebot des Diensteanbieters gehören.[26] In diesem Fall hat er sich die Information aus Nutzerperspektive zu eigen gemacht.

2. Inhalt

Das Gesetz verpflichtet dazu, technische und organisatorische Sicherheitsmaßnahmen unter Berücksichtigung des Stands der Technik zu ergreifen.

a) Technische und organisatorische Maßnahmen

Der Begriff „technische und organisatorische Maßnahmen" ist dabei wie im Kontext des § 9 BDSG weit zu verstehen.

Grundsätzlich fallen alle Maßnahmen darunter, die den Regelungszweck der Norm verwirklichen können.[27] Technische Maßnahmen können sowohl die Sicherung der Hardware als auch die Sicherung der Software betreffen. Das Gesetz hebt hierbei besonders Verschlüsselungsverfahren hervor. Daneben sind aber zahlreiche weitere Maßnahmen – wie etwa das Scannen der gehosteten Daten oder die Installation einer Firewall – denkbar. Organisatorische Maßnahmen betreffen die Organisation des eigenen Betriebs. Relevant ist etwa der Kreis derer, die mit Administratorenrechten ausgestattet sind oder Zugriff auf bestimmte personenbezogene Daten haben. Diese Maßnahmen umfassen die Schulung und Überwachung der Berechtigten, vertragliche Abreden mit Geschäftspartnern und die vertragliche Auslagerung von Sicherheitsmaßnahmen an spezialisierte Dienstleister.

b) Stand der Technik

Diese Maßnahmen müssen den „Stand der Technik" berücksichtigen. Dies ist rechtlich, mithin auch gerichtlich voll überprüfbar.[28] Der Stand der Technik wird in anderen Kontexten etwa in § 3 Abs. 6 BImSchG und § 3 Nr. 11 WHG legal definiert. Wesentlich ist dabei, dass es sich um den „Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen handelt", welcher praktisch zur Erreichung eines „allgemein hohen Schutzniveaus geeignet ist". Im Kontext des § 13 Abs. 7 TMG tritt an die Stelle von „Verfahren, Einrichtungen und Betriebsweisen" der Begriff „technische und organisatorische Maßnahmen". Der Bedeutungsgehalt des „Entwicklungsstandes fortschrittlicher Maßnahmen" lässt sich durch die Abgrenzung von verwandten Begriffen konturieren: Ein geringeres Schutzniveau haben die „allgemein anerkannten Regeln der Technik".[29] Letztere bezeichnen das Verständnis, das aktuell als fachlich richtig gilt und erprobt und bewährt ist.[30] Ein höheres Schutzniveau wird vom „Stand von Wissenschaft und Technik" vorausgesetzt, der dazu zwingt, auch Maßnahmen in Erwägung zu ziehen, die neuesten wissenschaftlichen Erkenntnissen entsprechen, auch wenn diese technisch noch nicht erprobt sind.[31]

Zusammenfassend stellt der Stand der Technik damit auf Maßnahmen ab, die evident praxistauglich sind und den Schutzzweck am besten verwirklichen.

3. Ziel: Erfolgsverhinderung

Verhindert werden soll nach § 13 Abs. 7 Nr. 1 TMG der unerlaubte Zugriff auf die für die Telemedienangebote genutzten technischen Einrichtungen. Zugegriffen werden kann entweder unmittelbar oder aus der Ferne. Zur Beurteilung, wann eine Verletzung des Schutzes personenbezogener Daten nach Nr. 2a vorliegt, ist auf die Maßstäbe des BDSG zu verweisen. Eine Verletzung liegt jedenfalls vor, wenn es zu einer Verarbeitung und Nutzung von personenbezogenen Daten kommt, die nicht gem. § 4 BDSG gerechtfertigt sind.

Zu verhindern sind gem. § 13 Abs. 7 Nr. 2b TMG auch Störungen. Gemeint sind damit ausweislich des Wortlauts Störungen der Telemediendienste unabhängig davon, ob eine Störung einer technischen Einrichtung vorliegt. Selbst der Störungsbegriff in § 100 Abs. 1 TKG, der sich auf TK-Anlagen bezieht, wird vom *BGH* so ausgelegt, dass auch die Sperrung von einzelnen IP-Nummernbereichen darunter fällt.[32] Eine Störung kann entsprechend § 8a Abs. 1 BSIG-E angenommen werden, wenn Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit des Telemediendienstes beeinträchtigt sind.[33] Der Hinweis in § 13 Abs. 7 Nr. 2b TMG, dass auch Störungen von außen erfasst sind, ist klarstellender Natur.

4. Grenzen

Schon aus Erwägungen der Verhältnismäßigkeit ergibt sich, dass Diensteanbieter durch die Sicherungspflichten nicht übermäßig belastet werden dürfen. Um solche Begrenzungen zu ermöglichen, führt § 13 Abs. 7 TMG grundsätzlich einen relativen Standard ein, weil der Stand der Technik nach dem Wortlaut „berücksichtigt" und nicht „eingehalten" werden muss wie i.R.d. § 8a Abs. 1 Satz 2 BSIG. Anders als bei kritischen Infrastrukturen kann es nämlich unverhältnismäßig sein, alle Diensteanbieter zur Befolgung des Stands der Technik zu verpflichten. Die Sicherungspflicht wird auf Maßnahmen beschränkt, die technisch möglich und wirtschaftlich zumutbar sind. Die Kriterien der technischen Möglichkeit und der wirtschaftlichen Zumutbarkeit sind im Regulierungsrecht gängige[34] Konkretisierungen des Verhältnismäßigkeitsgrundsatzes[35].

Bei der technischen Möglichkeit kommt es auf die Kapazität im Einzelfall an, also die subjektive Möglichkeit. Erforderlich sind grundsätzlich nur Maßnahmen, die vom Telemediendiensteanbieter selbst oder durch Beauftragung umgesetzt werden können. Der Begriff ist folglich nicht mit dem Stand der Technik gleichzusetzen,[36] da sonst eines der beiden Tatbestandsmerkmale redundant wäre. Technisch möglich ist auch, was organisatorisch an Dritte ausgelagert werden kann. In einem solchen Fall kann allenfalls noch fraglich sein, ob die Beauftragung eines Dritten wirtschaftlich zumutbar ist.

Bei der Bestimmung der wirtschaftlichen Zumutbarkeit sind die Kosten und die sonstigen wirtschaftlichen Nachteile einer Maßnahme mit den Gefahren ex ante abzuwägen. Dabei ist auf die Umstände des Einzelfalls abzustellen.[37] Folgende Kriterien können dabei eine Rolle spielen:

die Maßnahmenkosten,

- •die Effektivität der Maßnahme,

Auswirkungen auf die Webseite, insbesondere auf Layout und Funktionsumfang,

- •die zu erwartenden Reaktionen der Nutzer,

die Wettbewerbssituation insbesondere im Hinblick auf Mitbewerber, die dieser Pflicht nicht unterliegen,

- •die Folgen für die Umsatz- und Gewinnspanne sowie die sonstigen verkehrswerten Vorteile, die aus dem Betrieb der Webseite resultieren,

die Gefahren einer Unterlassung der Maßnahme,

- •die Möglichkeit der Nutzer, sich selbst zu schützen,

alternative Maßnahmen zur Verhinderung der Gefahren.

- Ein Beispiel für eine zumutbare Maßnahme ist grundsätzlich das Scannen der auf dem Server gehosteten Daten auf Malware. Das Gesetz selbst erwähnt die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens. Dagegen wäre die Verpflichtung zu einer Zwei-Wege Authentifizierung für den

Nutzerlogin für einen E-Mail-Provider zumindest nach den bisherigen Geschäftsmodellen wohl wirtschaftlich unzumutbar. Die Gesetzesbegründung stellt klar, dass die Barrierefreiheit der Verfahren besonders zu beachten ist.[38]

V. Rechtliche und praktische Auswirkungen

1. Rechtsfolgen

Wie andere Sicherungspflichten entfaltet § 13 Abs. 7 TMG Wirkungen in verschiedenen Regelungszusammenhängen und kann dabei besonders in folgenden Konstellationen relevant werden.

a) Öffentliches Recht

Eine offensichtliche Rechtsfolge des § 13 Abs. 7 TMG ist in § 16 Abs. 2 Nr. 3 TMG statuiert, der beim Eintritt von Verletzungserfolgen des § 13 Abs. 7 Nr. 1 und Nr. 2a TMG mit einem Bußgeld droht. Im Hinblick auf das Vorsatzerfordernis des § 10 OWiG kann sich ein Diensteanbieter jedenfalls immer dann entlasten, wenn er eine seinem Dienst entsprechende „Best Practice-Leitlinie" umgesetzt hat. Qualifiziert man § 13 Abs. 7 TMG als datenschutzrechtliche Bestimmung, weil die Vorschrift im entsprechenden 4. Abschnitt des TMG steht,[39] sind gem. § 59 Abs. 1 RStV die nach den allgemeinen Datenschutzgesetzen des Bundes und der Länder zuständigen Kontrollbehörden für dessen Durchsetzung zuständig. Sieht man jedoch in § 13 Abs. 7 Nr. 1 und Nr. 2b TMG als über den Datenschutz hinausgehende allgemeine Sicherungspflichten an, sind nach § 59 Abs. 2 RStV die durch Landesrecht bestimmten Behörden der Länder zuständig.[40] Ihre Befugnisse, die erforderlichen Maßnahmen zu treffen, ergeben sich entweder aus § 59 Abs. 3 RStV selbst oder aus den darauf aufbauenden Gesetzen der Länder wie etwa § 32 Landesmediengesetz Baden-Württemberg oder § 55 Mediengesetz Sachsen-Anhalt. Diese Maßnahmen umfassen die Untersagung und Sperrung von Telemedienangeboten.[41]

Eine drohende Verletzung des § 13 Abs. 7 TMG kann daneben als Gefahr für die öffentliche Sicherheit qualifiziert werden.[42] Bei Vorliegen der entsprechenden polizei- und sicherheitsrechtlichen Voraussetzungen können die jeweils (eil-)zuständigen Behörden präventiv tätig werden.[43]

b) Zivilrecht

Daneben kann § 13 Abs. 7 TMG mittelbare Wirkung im Zivilrecht entfalten. In vertraglichen Schuldverhältnissen konkretisiert § 13 Abs. 7 TMG Nebenpflichten, also Schutz- und Leistungspflichten.[44] Eine Schadensersatzpflicht kann sich zudem aus dem allgemeinen Deliktsrecht ergeben. § 13 Abs. 7 TMG ist ein Schutzgesetz i.S.d. § 823 Abs. 2 BGB. Denn der Schutzzweck[45] des § 13 Abs. 7 TMG zielt nicht nur auf die Allgemeinheit, sondern auch auf den einzelnen Nutzer ab, wie sich schon aus der Gesetzesbegründung und § 13 Abs. 7 Nr. 2a TMG ergibt.

Neben § 823 Abs. 2 BGB kann ein Anspruch aus § 823 Abs. 1 BGB relevant werden, wenn eines der dort genannten Rechtsgüter betroffen ist. In diesem Fall konkretisiert § 13 Abs. 7 TMG die Mindestanforderungen für eine entsprechende Verkehrssicherungspflicht. Zivilrechtliche Schadensersatzansprüche sind allerdings in der Praxis schwer zu beweisen, insbesondere was die haftungsausfüllende Kausalität angeht. Dass andererseits solche Ansprüche nicht undenkbar sind, zeigt ein Sammelklageverfahren in den USA gegen ein großes soziales Netzwerk, das die Passwörter seiner Nutzer nicht ausreichend verschlüsselt hatte.[46] Das Verfahren wurde durch einen Vergleich und Zahlung von US-$ 1,25 Mio. beigelegt.[47]

c) Sonstige Rechtsfolgen

Die Auswirkungen in anderen Rechtsbereichen können hier nur angerissen werden. Wie bei § 823 Abs. 1 BGB konkretisiert § 13 Abs. 7 TMG auch in anderen Zusammenhängen Verkehrssicherungspflichten. Eine Verletzung einer solchen Verkehrssicherungspflicht kann die Verantwortlichkeit für fremde Handlungen begründen. Im Wettbewerbsrecht führt eine solche Pflichtverletzung zu einer Haftung als Täter.[48] Im Urheberrecht können aus Verletzung einer Verkehrssicherungspflicht Unterlassungsansprüche erwachsen.[49] Im Wettbewerbsrecht, aber auch im Urheber- und Markenrecht hat der *BGH* in der „Halzband"-Entscheidung eine Haftung als Täter bejaht, wenn ein Webseitenbetreiber seine Webseite nicht ausreichend sichert und ein Dritter in seinem Namen auftritt.[50] Was dabei als „ausreichende" Absicherung anzusehen ist, bestimmt sich nunmehr nach § 13 Abs. 7 TMG. Daneben können strafrechtliche Garantenpflichten auch Host- und Content-Provider treffen,[51] diese Garantenpflichten werden wiederum von § 13 Abs. 7 TMG konkretisiert.[52]

2. Praktische Konsequenzen

Wie sich der neue § 13 Abs. 7 TMG in der Praxis auswirkt, wird im Folgenden anhand von zwei fiktiven Fallstudien erläutert. Die eine betrifft einen Handwerksbetrieb mit einer Online-Präsentation seines Dienstleistungsangebots, die andere ein mittelständisches Unternehmen mit einem Webshop.[53]

a) Einfache Webseite eines Handwerksbetriebs

Im ersten Szenario möchte ein kleiner Handwerksbetrieb eine einfache Webseite platzieren, auf der das Angebot des Betriebs beschrieben wird, wobei von einem geringen Verbreitungsgrad auszugehen ist. Weil der Handwerksbetrieb eine Internetseite betreibt, ist er

Telemediendiensteanbieter i.S.v. § 2 Nr. 1 TMG. Für eigene Inhalte ist er nach § 7 TMG auch verantwortlich. Unabhängig davon, dass die Nutzung der Webseite nicht entgeltlich ist und über das Internet auch keine Verträge zu Stande kommen, liegt allein in der Werbung für seine Dienstleistung ein geschäftsmäßiges Handeln. § 13 Abs. 7 TMG ist mithin

Djeffal: Neue Sicherungspflicht für Telemediendiensteanbieter - Webseitensicherheit jetzt Pflicht nach dem IT-Sicherheitsgesetz(MMR 2015, 716) 720

anwendbar. Die Grenzen des technisch Möglichen bzw. wirtschaftlich Zumutbaren i.S.d. § 13 Abs. 7 TMG greifen nicht, da Webhoster alle genannten Maßnahmen als Zusatzdienstleistungen in sog. Baukastensystemen[54] (nach kostenpflichtiger Einrichtung) schon für ca. € 5,– bis € 20,– pro Monat anbieten.

Entscheidet sich der Betrieb jedoch dazu, sich bei einem Hoster Webspace ohne zusätzliche Dienstleistungen zu bestellen,[55] sind nach § 13 Abs. 7 TMG insbesondere folgende Maßnahmen zu ergreifen:

Regelmäßige Software-Updates aller i.R.d. Erstellung und Aktualisierung der Homepage verwendeten Programme

- Updatemaßnahmen betreffen in erster Linie Content-Management-Systeme (CMS), aber auch andere Programme, insbesondere auch die Betriebssysteme der betreffenden technischen Einrichtungen. Immer wieder werden in CMS Sicherheitslücken gefunden, die durch Updates behoben werden. So wurde z.B. erst kürzlich eine kritische Sicherheitslücke in Wordpress gefunden.[56] Trotz der kostenlosen Verfügbarkeit eines Updates waren über zweieinhalb Monate nach dessen Veröffentlichung nach Schätzungen immer noch 86% der auf Wordpress basierenden Seiten verwundbar, und das, obwohl das Update in der Regel ohne Probleme und weitere Anpassungen eingespielt werden konnte.

Überprüfung der Programmeinstellung unter Sicherheitsgesichtspunkten

- Der bloße Erwerb sicherer und aktueller Software ist bei weitem nicht ausreichend. Hinzu kommen muss die fachgerechte Einstellung und Bedienung. Einfache Konfigurationsfehler können verheerende Konsequenzen haben, wie das Beispiel der verbreiteten Datenbank „Mongo DB" zeigt. Diese wurde vielfach falsch eingestellt, sodass über 40.000 Datenbanken im Internet frei abrufbar waren, darunter auch Kundendatenbanken von Webshops in Deutschland.[57] Dieser Fehler war nach Angaben der Entwickler vermeidbar, wenn man die Bedienungsanleitung und Checklisten zu Rate gezogen hätte.[58]

Sichere Authentifizierung der Administratoren

- Administratorenzugänge nach dem Stand der Technik zu schützen, heißt zuerst, dass eine doppelte Zugangsabfrage stattfinden muss: Auch der Zugang zur Login-Seite selbst sollte durch ein Passwort geschützt sein.[59] Als Administratorenname ist kein gebräuchlicher Name wie „Admin" oder „Administrator" zu verwenden, das Passwort ist sicher zu gestalten.[60] Passwörter sind in regelmäßigen Abständen durch gänzlich verschiedene Passwörter zu ersetzen und sicher zu verwahren.

Einsatz von Sicherheitssoftware

- Ferner muss eine spezialisierte Firewall[61] fachgemäß installiert, eingestellt und regelmäßig gewartet werden. Meldungen der Firewall sind zu untersuchen. Zudem ist der gehostete Inhalt regelmäßig mit einem Virenscanner zu überprüfen.[62] Die Webseite sollte auch in regelmäßigen Abständen auf Verwundbarkeiten gescannt werden.[63]

Bezug regelmäßiger Informationen allgemeiner Art

- Daneben sind regelmäßig allgemeine Informationen etwa über wichtige Sicherheitsupdates oder breit angelegte Attacken zu beziehen[64] und ggf. zu berücksichtigen.

Bei Hinweisen auf Angriffe: Einsatz von spezieller Software und ggf. auch spezialisierten Dienstleistern

- Gibt es Hinweise auf die Kompromittierung der Webseite, ist dies mit Hilfe von spezialisierter Software und u.U. auch externen Dienstleistern zu untersuchen und zu bereinigen.[65] Am besten ist es, sich schon in der Konzeptionsphase über entsprechende Angebote zu informieren und Vorabsprachen zu treffen.

b) Online-Auftritt eines mittelständischen Unternehmens mit Webshop

Die zweite fiktive Fallstudie nimmt ein mittelständisches Unternehmen in den Blick. Es stellt Produkte für Konsumenten her, konzipiert einen neuen Webauftritt, der auch einen Webshop beinhalten soll. Über diesen sollen die Produkte direkt vertrieben werden, die Kunden haben die Möglichkeit, Profile anzulegen und ihre Daten zu hinterlegen, um zukünftige Bestellungen schneller zu tätigen. Dieser Webauftritt fällt in den Anwendungsbereich des § 13 Abs. 7 TMG. Im Hinblick auf die unten aufgeführten Maßnahmen greifen die Begrenzungstatbestände der technischen Möglichkeit und der wirtschaftlichen Zumutbarkeit nicht ein, weil das Unternehmen diese Dienstleistungen bei Hostern oder Drittanbietern für monatlich € 20,– bis € 100,– buchen kann. Will es die Anforderungen jedoch selbst erfüllen, sind neben den oben erwähnten insbesondere folgende Sicherheitsmaßnahmen zu ergreifen:

Maßnahmen nach § 9 BDSG

- Nachdem im Webshop auch personenbezogene Daten erhoben werden, müssen die Anforderungen des § 9 BDSG und des § 13 Abs. 4 TMG erfüllt werden, die sich teilweise mit § 13 Abs. 7 TMG überschneiden. Es muss also ein Konzept ausgearbeitet werden, das Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrolle gewährleistet und das Trennungsgebot berücksichtigt,[66] wobei die Maßnahmen nicht nur nach außen, sondern auch auf das innerbetriebliche Datenmanagement abzielen müssen.

Einsatz von Sicherheitssoftware

- Wie oben bereits erwähnt, ist Sicherheitssoftware z.B. in Form von Firewalls, Malware- und Vulnerability-Scannern zu verwenden. Auf Grund der höheren Nutzerzahlen sind die Scans in kürzeren Abständen auszuführen, der Malware-Scan nach Möglichkeit täglich.

Trennung von Datenbank- und Webserver

- Ist der Webshop mit Datenbanken verbunden, sollten diese nicht auf demselben Server gehostet werden, um Risiken zu minimieren.

Nutzerauthentifizierung

- Da Nutzer auch sensible Daten wie etwa die Kreditkartennummer hinterlassen, ist es gerechtfertigt, eine gute Nutzerauthentifizierung zu verlangen. Benutzername und Passwort sind auf dem Server nur verschlüsselt zu hinterlegen (durch „hashen" und „salten"). Auch für Nutzerpasswörter sollten Mindestsicherheitsstandards gelten.

Daten- und Transportverschlüsselung

- Bei der Übertragung der Account- oder Zahlungsdaten ist auf eine Transportverschlüsselung zu achten. Hierbei wird derzeit insbesondere das Verschlüsselungsprotokoll Transport Layer Security (TLS) verwandt. Vorzugsweise ist ein fortgeschrittener Standard zu implementieren, derzeit also SHA-2 oder SHA-3. Ferner sollte die Verschlüsselung so implementiert werden, dass sie immer eingeschaltet ist. Nutzerdaten, aber auch Cookies und Backups sind zu verschlüsseln. Sowohl die Schlüssel als auch Passwörter sind gegen innerbetrieblichen Zugriff und Zugriff von außen zu sichern.

Notfallszenario

- Ferner ist zu klären, wie Mitarbeiter auf Notfälle reagieren sollen. Das betrifft insbesondere innerbetriebliche Zuständigkeiten bzw. Ersatzzuständigkeiten. Hierbei sind die Verantwortlichkeiten zu klären, außerdem das Vorgehen einschließlich des Einschaltens von Sicherheitsexperten und der Benachrichtigung der Nutzer. Je nach Nutzerzahlen und Sensibilität der erhobenen Daten kann es angezeigt sein, einen Notfall testweise zu simulieren.

VI. Fazit

§ 13 Abs. 7 TMG ist eine Norm, die ein aktuelles Problem adressiert und die in vielen Konstellationen relevant werden könnte. Ein Schutz der persönlichen Daten und der Integrität informationstechnischer Systeme tut Not, wenn man die vielen und faszinierenden Möglichkeiten auskosten möchte, die die Digitalisierung bietet. Eine nachhaltige Digitalisierung setzt IT-Sicherheit als integralen Bestandteil voraus, der in jeder Phase von Projekten mit bedacht werden sollte. Sicherheit ist nicht Zweck, aber ein notwendiges Mittel. § 13 Abs. 7 TMG leistet einen Beitrag dazu, IT-Sicherheit auch in die Breite zu tragen. Anstelle einer ausdifferenzierten, aber starren Regulierung verpflichtet die Norm zum Selbstschutz unter Berücksichtigung des Stands der Technik, ist aber auch strikt an Verhältnismäßigkeitsgesichtspunkten orientiert.

Ob diese Norm in Zukunft zum „lebenden Recht" werden wird, hängt von Normanwendern auf verschiedenen Ebenen ab. Ein erster wichtiger Schritt wäre die fortlaufende Konkretisierung der Norm, um Normanwendern konkrete Anhaltspunkte für ihre Befolgung zu bieten. Hier ist insbesondere das *BSI* gefordert, für eine zuverlässige und fortlaufende Konkretisierung zu sorgen. Ebenso sollten aber auch Branchenverbände und Interessengruppen ihren Teil beitragen. Dann müssten diese Standards auch von Telemediendiensteanbietern umgesetzt werden, und das auf allen Ebenen. Das kann nur gelingen, wenn es auch zu einem Bewusstseinswandel kommt. Vom Entscheider in der Wirtschaft über den Programmierer bis zum Nutzer müsste sich das Bewusstsein verstärken, dass neben dem großen Potenzial der Informationstechnologien auch Missbrauchsgefahren bestehen und deshalb etwa Webanwendungen und Webservices in angemessenem Maße abzusichern sind. Bei Entscheidungen von Verantwortlichen und Nutzern

müssten Sicherheitsaspekte stärker neben anderen Gesichtspunkten wie Wirtschaftlichkeit, Design, Benutzerfreundlichkeit oder zeitlichen Ressourcen gewichtet werden. Ein erster Schritt in diese Richtung – nicht mehr und nicht weniger – ist § 13 Abs. 7 TMG.

Anmerkung der Redaktion

Dr. Christian Djeffal

ist derzeit Rechtsreferendar am OLG Frankfurt/M. Seine Stationen verbrachte er u.a. beim Bundesamt für die Sicherheit in der Informationstechnik.

[1] Vgl. hierzu *Roos*, MMR 2015, 636; *Gitter/Meißner/Spauschus*, ZD 2015, 612; zu einer ersten Einschätzung des Entwurfs s. *Roos*, MMR 2014, 723; *Eckhardt*, ZD 2014, 599 und *Roth*, ZD 2015, 17.

[2] Ausnahmen sind etwa *golem*, http://www.golem.de/news/innenminister-de-maizi-re-jeder-kleine-webshop-muss-sicher-sein-1412-111244.html; *Dörner*, http://www.wsj.de/nachrichten/SB10972589309364634370204580342880750558068.

[3] So etwa der Befund des Präsidenten des BSI, *Michael Hange*, bei der Vorstellung des letzten Jahresberichts, s. etwa unter: http://www.heute.de/bundesamt-beklagt-digitale-sorglosigkeit-cyberkriminelle-ruesten-auf-36708906.html.

[4] *BKA*, Cybercrime, Bundeslagebild 2013, S. 5, 6.

[5] *Pandalabs*, www.pandasecurity.com/mediacenter/src/uploads/2015/02/Pandalabs2014-DEF2-en.pdf, S. 5.

[6] Zur Entwicklung s. *Chen/Li*, www.trendmicro.com/ cloud-content/ us/ pdfs/ security-intelligence/ white-papers/ wp-evolution-of-exploit-kits.pdf., S. 2, 3.

[7] *Websense*, https://www.websense.com/assets/reports/websense-2013-threat-report.pdf 10-11.

[8] S. etwa zum Hack des MSN-Portals in Italien und der Nachrichtenseite des Senders NBC *pcadvisor*, http://www.pcadvisor.co.uk/news/security/3436915/major-websites-hacked-leaving-users-vulnerable.

[9] *European Network and Information Security Agency (ENISA)*, https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014; iv, S. 16 ff.; *G Data*, https://public.gdatasoftware.com/Presse/Publikationen/Whitepaper/EN/2014_GDATA_Exploit_Prot

ection_Whitepaper_EN.pdf, S. 2; s.a. *Websense*, http://www.websense.com/assets/reports/report-2014-threat-report-en.pdf, S. 13-17; *F-Secure*, Threat Report H2 2014, S. 10.

[10] S. dazu etwa *Chen/Li* (o. Fußn. 6), S. 8; *Kapersky*, https://securelist.com/files/2014/12/Kaspersky-Security-Bulletin-2014-EN.pdf, S. 7.

[11] *BSI*, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile, S. 17.

[12] *Symantec*, https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf, S. 38.

[13] S. z.B. *Kapersky* (o. Fußn. 10), S. 32, 33.

[14] Eine Schätzung beläuft sich etwa auf US-$ 400 Mrd. pro Jahr, wobei das Ergebnis naturgemäß stark von der Schadensberechnung abhängt; s. *Center for Strategic and International Studies*, http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf, S. 2.

[15] S. o. Fußn. 14, S. 9.

[16] S. dazu m.w.Nw. *di Fabio*, in: Maunz/Dürig, GG, 73. EL 2014, Art. 2 Rdnr. 189-191.

[17] S. zur Schutzdimension *BVerfG* MMR 2008, 315 m. Anm. *Bär*.

[18] Zu den Details s. *Ricke*, in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, TMG § 1 Rdnr. 10 unter Verweis auf die Gesetzesbegründung.

[19] BT-Drs. 18/4096, S. 34.

[20] Zur Abgrenzung im Rahmen etwa von § 29 BDSG s. *Klug/Körffer/Gola*, in: Gola/Schomerus, BDSG, 12. Aufl. 2015, § 29 Rdnr. 6, 7.

[21] Für eine nähere Erläuterung s. etwa *Martini,* in: BeckOK InfoMedienR, 8. Ed., 1.2.2015, TMG § 2 Rdnr. 4, 5.

[22] *Heckmann*, in: jurisPK-Internetrecht, 4. Aufl. 2014, Kap. 1 Rdnr. 94.

[23] *Ricke* (o. Fußn. 18), § 2 Rdnr. 3; zu der zweiten Alternative der Zugangsvermittlung s. ausf. *Heckmann* (o. Fußn. 22), Kap. 1 Rdnr. 96.

[24] *BGH* NJW-RR 2009, 1413, 1415; s.a. *Roggenkamp/Stadler*, in: jurisPK-Internetrecht (o. Fußn. 22), Kap. 10 Rdnr. 430.

[25] *Hoffmann*, in: Spindler/Schuster (o. Fußn. 18), TMG § 7 Rdnr. 13 unter Verweis auf *Pelz*, in: Bräutigam/Leupold, Online Handel, 2003, Kap. B1 Rdnr. 72.

[26] So sind auch zu lesen: *Hoffmann* (o. Fußn. 25), TMG § 7 Rdnr. 13 unter Verweis auf *Pelz* (o. Fußn. 25), Kap. B1 Rdnr. 72; der letztere Beitrag unterscheidet im Hinblick auf die Verantwortlichkeit grds. danach, von wem der jeweilige Schadcode stammt. Dies ist ein Kriterium für die Beurteilung der Frage, ob sich der Telemediendiensteanbieter den Code aus Nutzerperspektive zu eigen gemacht hat.

[27] *Schulze-Melling*, in: Taeger/Gabel, BDSG, 2. Aufl. 2013, § 9 Rdnr. 20; *Brink,* in: Karg/Wolff, Datenschutzrecht, § 9 Rdnr. 68 m.w.Nw.

[28] *Faßbender*, in: Landmann/Rohmer, Umweltrecht, 75. EL 2015, WHG § 3 Rdnr. 84; *Guckelsberger*, in: BeckOK Umweltrecht, 35. Ed., 1.4.2015, WHG § 3 Rdnr. 31; *Jarass*, BImSchG, 11. Aufl. 2015, § 3 Rdnr. 98.

[29] Jarass (o. Fußn. 28), § 3 Rdnr. 93; *Schulte/Michalk*, in: BeckOK Umweltrecht (o. Fußn. 28), BImSchG § 3 Rdnr. 95.

[30] *Seibel*, NJW 2013, 3000, 3001.

[31] BVerfGE 49, 89,136.

[32] *BGH* NJW 2014, 2500 = ZD 2014, 461 m. Anm. *Eckhardt*; der Gesetzgeber hat diese Auslegung durch die Neufassung des § 100 Abs. 1 TKG im IT-Sicherheitsgesetz bestätigt.

[33] BT-Drs. 18/4096, S. 10.

[34] Vgl. etwa §§ 7 Abs. 4, 9 Abs. 2, 3, 14 Abs. 1 KrWG; § 11 Abs. 1 Elektrogesetz; § 14 Batteriegesetz; Art. 48 der Bayerischen Bauordnung.

[35] Vgl. *Hofmann,* in: BeckOK Umweltrecht (o. Fußn. 28), § 7 Rdnr. 13; *Beckmann*, in: Landmann/Rohmer (o. Fußn. 28), KrWG § 7 Rdnr. 60. Da der Verhältnismäßigkeitsgrundsatz hier ausdrücklich niedergelegt ist, ist es nicht erforderlich, diesen in andere Begriffe wie etwa „Stand der Technik" oder „berücksichtigen" hineinzulesen.

[36] Vgl. *Hofmann* (o. Fußn. 35), KrWG § 7 Rdnr. 14; *Beckmann* (o. Fußn. 35), KrWG § 7 Rdnr. 62.

[37] Vgl. *Beckmann* (o. Fußn. 35), KrWG § 7 Rdnr. 65 ff.

[38] BT-Drs. 18/4096, S. 34.

[39] *Fiedler*, in: BeckOK InfoMedienR, 8. Ed., 1.5.2015, RStV § 59 Rdnr. 1; *Volkmann* in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, RStV § 59 Rdnr. 3.

[40] Eine Übersicht über die nach jeweiligem Landesrecht zuständigen Organe bietet *Fiedler* (o. Fußn. 39), RStV § 59 Rdnr. 5-7.

[41] *Fiedler* (o. Fußn. 39), Rdnr. 9 ff.; *Schulz,* in: Hahn/Vesting, Rundfunkrecht, 3. Aufl. 2012, RStV § 59 Rdnr. 42 ff.

[42] Die öffentliche Sicherheit umfasst nach einhelliger Meinung die gesamte Rechtsordnung und damit auch § 13 Abs. 7 TMG.

[43] Auf Grund der individuellen Schutzrichtung des § 13 Abs. 7 TMG können Behörden im Rahmen ihres Ermessens ggü. Einzelnen zum Eingreifen verpflichtet sein.

[44] Zum Verhältnis von gesetzlichen Schutzpflichten und § 241 Abs. 2 BGB s. *Olzen,* in: Staudinger, BGB, 15. Aufl. 2015, § 241 Rdnr. 164 f.

[45] S. zum Erfordernis des Schutzzwecks nur BGHZ 125, 366, 374 m.w.Nw.

[46] Zu den technischen Details s. *Sophos,* https://nakedsecurity.sophos.com/2015/02/25/linkedin-settles-class-action-suit-over-2012-unsalted-password-leak/.

[47] Vgl. unter: http://www.nzz.ch/mehr/digital/linkedin-zahlt-125-millionen-dollar-schadensersatz-1.18489588.

[48] S. dazu *BGH* MMR 2007, 634 m. Anm. *Jürgens*/*Köster*.

[49] *V. Wolff*, in: Wandtke/Bullinger, UrhG, 4. Aufl. 2014, § 97 Rdnr. 19; eine eingehende Betrachtung der Übertragbarkeit der Verkehrssicherungspflichtendogmatik auf das Marken- und Urheberrecht findet sich bei *Leistner*, GRUR-Beil. 2010, 1, 18 ff.

[50] *BGH* MMR 2009, 391.

[51] Zu Garantenpflichten mit Internetbezug in diesem Rahmen s. etwa *Stree*/*Bosch,* in: Schönke/Schröder, StGB, 29. Aufl. 2014, § 13 Rdnr. 44; s. grds. auch *Freund*, in: MüKoStGB, 2. Aufl. 2011, § 13 Rdnr. 157 ff.

[52] Kausalität und bedingter Vorsatz werden nach strafprozessualen Grundsätzen nur sehr schwer nachzuweisen sein.

[53] Auf Grund der Vielzahl der möglichen Gestaltungen im Einzelnen und des schnellen Wandels der Technik kann hier nur ein exemplarischer und nicht zwangsläufig vollständiger Überblick über die zu treffenden Maßnahmen gegeben werden, der eine sorgfältige Prüfung im Einzelfall nicht ersetzen kann.

[54] Einen Überblick bieten z.B. *Bager*/*Bleich*, c't 14/14, 94.

[55] Nicht behandelt werden hier Maßnahmen zum Eigenbetrieb eines Root-Servers, s. diesbezüglich unter: http://www.princeton.edu/itsecurity/technical/best-practices.

[56] S. den ausf. Bericht von *Oy*, http://klikki.fi/adv/wordpress.html; zusammengefasst ist der Bericht in *golem*, http://www.golem.de/news/cross-site-scripting-kritische-wordpress-luecke-betrifft-86-prozent-der-seiten-1411-110750.html.

[57] *ZDNet,* http://www.zdnet.de/88218674/saarbruecker-studenten-entdecken-tausende-ungesicherte-datenbanken-im-netz.

[58] *CISPA*, http://cispa.saarland/mongodb.

[59] S. dazu etwa *Gleich*, c't 4/15, 114.

[60] Für eine Einführung hinsichtlich sicherer Passwörter für Bürger s. *BSI*, https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Passwoerter/passwoerter_node.html.

[61] Hierbei wird nicht auf Server-Firewalls, sondern auf sog. Web Application Firewalls Bezug genommen.

[62] Ein täglicher Scan wird empfohlen von *Symantec*, https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf, S. 104.

[63] Der Dienstleister Virustotal etwa bietet eine Metasuchmaschine für URL-Scanner an, https://www.virustotal.com; darüber kann man sich auch über einzelne Anbieter informieren.

[64] Solche Informationen werden neben den vielen wissenschaftlichen und kommerziellen Zeitschriften auf diesem Gebiet etwa zur Verfügung gestellt von http://www.heise.de/security/ und http://www.zdnet.com/topic/security.

[65] Eine instruktive Maßnahmenübersicht findet sich etwa unter: https://www.google.com/webmasters/hacked.

[66] Für ausf. Darstellungen mit weiteren Verweisen s. *Polenz*, in: Kilian/Heussen, Computerrecht, 32. EL 2013, Rdnr. 1-25; *Kramer*/*Meints*, in: Hoeren/Sieber/Holznagel, Hdb. Multimedia-Recht, 40. EL 2014, Rdnr. 28-49.