Abschrift

Hanseatisches Oberlandesgericht

Az.: 5 U 33/19
310 O 219/18
LG Hamburg

Verkündet am 18.06.2020

, JAng
Urkundsbeamtin der Geschäftsstelle

Urteil

IM NAMEN DES VOLKES

In der Sache

- Antragsteller und Berufungskläger -

Prozessbevollmächtigter:

gegen

1)

- Antragsgegnerin und Berufungsbeklagte -

2)

- Antragsgegnerin und Berufungsbeklagte -

Prozessbevollmächtigte zu 1 und 2:

erkennt das Hanseatische Oberlandesgericht - 5. Zivilsenat - durch den Vorsitzenden Richter am Oberlandesgericht , den Richter am Oberlandesgericht und die Richterin am Oberlandesgericht auf Grund der mündlichen Verhandlung vom 29.04.2020 für Recht:

1. Die Berufung des Antragstellers gegen das Urteil des Landgerichts Hamburg vom 22.01.2019, Az. 310 O 219/18, wird zurückgewiesen.
2. Der Antragsteller hat die Kosten des Berufungsverfahrens zu tragen.

Gründe:

I.

Die Parteien streiten im Rahmen eines einstweiligen Verfügungsverfahrens um die Verantwortlichkeit der Antragsgegnerinnen für ein durch einen Hackerangriff auf deren Internetseite hochgeladenes Lichtbild, an dem der Antragsteller Urheberrechte bzw. Lichtbildschutz geltend macht.

Der Antragsteller ist Berufsfotograf. Die Antragsgegnerinnen betreiben die Internetseite www. .de als Webseite des . Sie sind im Impressum als Verantwortliche genannt.

Die Internetseite der Antragsgegnerinnen soll die Implementierung von Diversity Management in Studium und Lehre vernetzen und dient Informationszwecken. In deren Datenbanken sind weder Drittwerbung noch wirtschaftliche Angebote aufgenommen. Auf der Seite finden sich lediglich Verweise auf wissenschaftliche Expertisen über Diversity Management mit Hochschulbezug. Die Internetseite der Antragsgegnerinnen wurde über das Content-Management-System verwaltet, wozu sich die Antragsgegnerinnen eines externen Dienstleisters, der Fa. p , bedienten. Ein Content-Management-System (CMS) ist eine Software zur Erstellung, Bearbeitung und Organisation von Inhalten auf Internetseiten. Ein solches System besteht aus einem „Frontend", einem Bereich, den der Besucher der Internetseite sieht, und einem „Backend", einem passwortgeschützten Bereich, der nur Redakteuren und Administratoren der Internetseite zugänglich und über den eine Bearbeitung der Internetseite möglich ist.

Eine seit April 2017 verfügbare neuere Version des CMS ließen die Antragsgegnerinnen bis Juni 2018 nicht aufspielen, weil diese nicht uneingeschränkt abwärtskompatibel war, so dass Erweiterungen der vorherigen Version dann nicht mehr „gelaufen" wären. Zu Beginn des Jahres 2018 waren zwei von den Antragsgegnerinnen verwendete Systemerweiterungen („ " und „ ") „unsicher", wie ihr IT-Dienstleister nach Erhalt der streitgegenständlichen Abmahnung feststellte.

In der Zeit zwischen dem 23.01.2018 und dem 19.06.2018 „hackten", wie im Berufungsverfahren unstreitig geworden ist, Dritte die Internetseite der Antragsgegnerinnen und luden das streitgegenständliche Foto „ " – neben weiteren Programmdateien – unter Ausnutzung vorhandener Sicherheitslücken auf dem Server der Webseite hoch und speicherten es dort.

Bei Eingabe der konkreten URL: http:// .php war das Foto abrufbar. Es war Teil hineingehackter englischsprachiger Unter-

seiten, die über das Backend der Internetseite der Antragsgegnerinnen gespeichert worden waren. Diese Unterseiten wiesen ein anderes Layout auf als die übrigen Webseiten der Antragsgegnerinnen. Es war nicht möglich, von der Internetseite der Antragsgegnerinnen auf die beanstandeten Inhalte und das streitgegenständliche Foto zu gelangen, weder durch eine Verlinkung noch durch die interne Suchfunktion auf der Seite. Auf den hinzugefügten Unterseiten war ein sog. Backlink auf die Startseite der Internetseite der Antragsgegnerinnen gesetzt.

Durch Eingabe der Bilddaten in eine -Bildersuche wurde der Antragsteller auf die beanstandeten Unterseiten der Webseite der Antragsgegnerinnen aufmerksam und ließ die Antragsgegnerinnen mit Anwaltsschreiben vom 20.06.2018 abmahnen. Diese entfernten sofort danach die hineingehackten Unterseiten, deaktivierten die theoretisch anfälligen Komponenten im System und setzten die relevanten Passwörter neu. Eine Unterlassungsverpflichtungserklärung gaben sie nicht ab.

Bei den Antragsgegnerinnen werden Webserver-Logdateien nicht länger als 14 Tage gespeichert, so dass ihnen eine genaue Rückverfolgung der Speicherung der Unterseiten nicht möglich war.

Der Antragsteller hat behauptet, er habe das streitgegenständliche Foto erstellt.

Er ist der Auffassung gewesen, ihm komme die Vermutungswirkung des § 10 Abs. 1 UrhG zugute. Die Antragsgegnerinnen hätten sein Foto widerrechtlich vervielfältigt und öffentlich zugänglich gemacht.

Hauptweise hat der Antragsteller in erster Instanz sein Unterlassungsbegehren auf täterschaftliches Handeln der Antragsgegnerinnen gestützt, entweder durch aktives Tun oder Unterlassen. Hilfsweise sei eine Störerhaftung der Antragsgegnerinnen gegeben, weil diese es versäumt hätten, ihren Server hinreichend zu schützen, insbesondere die notwendigen Updates aufzuspielen. Die Antragsgegnerinnen hätten ihre Internetseite bewusst mit einem pflegebedürftigen OpenSource-Programm betrieben, dies zwischenzeitlich aus finanziellen Gründen ohne Programmpflege. Sie hätten bewusst auf Sicherheitsupdates für das -Kernprogramm verzichtet. Das Bestehen von Sicherheitslücken hätte den Antragsgegnerinnen bekannt sein müssen. Sie hätten billigend in Kauf genommen, dass Dritte sich ihres Systems bemächtigten und dort rechtswidrige Inhalte platzierten. Es sei zu befürchten, dass ein vermeintlicher Hacker nur auf die nächste Schwachstelle im System der Antragsgegnerinnen warte und sich der Vorfall wiederhole. Das Abschalten ihrer Internetseite wäre kostenlos möglich sowie zumutbar gewesen und hätte als mögliche Alternative zum Betrieb einer unsicheren Plattform gewählt werden müssen. Die Antragsgegnerinnen hätten ihre Internetseite nicht unter Inkaufnahme von Schäden für Dritte weiterbetreiben dürfen. Bei einer sog. OpenSource-Software wie bestehe die Möglichkeit, gezielt nach Sicherheitslücken zu suchen und sog. Exploits, also ausnutzende Schadsoftware, zu

erstellen. Es sei daher erforderlich, vorhandene Schwachstellen unverzüglich zu schließen, indem Updates aufgespielt werden. Anderenfalls werde ein Programm mit einer für jedermann erkennbaren und ausnutzbaren Schwachstelle betrieben, was eine Einladung für Hacker darstelle. Bei regelmäßiger und zeitnaher Installation aller Security-Updates wären Hackerangriffe nicht erfolgreich. Die Antragsgegnerinnen hätten gegen grundsätzliche Anforderungen verstoßen und billigend in Kauf genommen, dass Dritte die vorhandenen Sicherheitslücken ausnutzen, um Schadcode einzuschleusen und so unerkannt Urheberrechtsverletzungen begehen.

Der Antragsteller hat beantragt,

der Antragsgegnerin zu 1. und der Antragsgegnerin zu 2. im Wege einstweiliger Verfügung bei Meidung eines vom Gericht für jeden Fall der Zuwiderhandlung festzusetzenden Ordnungsgeldes von bis zu € 250.000,-, ersatzweise Ordnungshaft bis zu 6 Monaten, oder Ordnungshaft bis zu 6 Monaten, Ordnungshaft jeweils zu vollstrecken an den jeweiligen Rektoren und Präsidenten

zu untersagen,

ohne Zustimmung des Antragstellers das von diesem hergestellte Lichtbild/Lichtbildwerk mit dem Namen „ “ wie in Anlage K1 abgebildet über Internetseiten öffentlich zugänglich zu machen, ohne dazu berechtigt zu sein, wie im Internetauftritt http:// .php geschehen.

Die Antragsgegnerinnen haben beantragt,

den Antrag auf Erlass einer einstweiligen Verfügung zurückzuweisen.

Sie haben behauptet, die hineingehackten Unterseiten seien, was im Berufungsverfahren unstreitig geworden ist, ohne ihre Kenntnis unter Manipulation zweier Standardsystemdateien im „Backend“ ihrer Internetseite gespeichert worden.

Für den Betrieb der neueren Version von ab April 2017 wären erhebliche Anpassungsarbeiten notwendig gewesen. Jedes Update sei für sie mit Arbeitsaufwand und Kosten für ihren IT-Dienstleister (p) verbunden.

Bezogen auf den ihnen vorgeworfenen Verstoß sei zu berücksichtigen, dass die Webseite http:// .php - was unstreitig ist - von keiner anderen Webseite verlinkt und auch in Suchmaschinen nicht indexiert gewesen sei. Internetnutzer hätten die genaue URL kennen müssen, um die beanstandeten Inhalte aufrufen zu können.

Sie sind der Ansicht gewesen, sie seien nicht als sog. Störer für die hier gegenständliche Urheberrechtsverletzung verantwortlich. Eine Störerhaftung könne nicht darauf gestützt werden, dass

sie ihre Internetseite im Verletzungszeitpunkt mit einem Content-Management-System betrieben hätten, das sich nicht auf aktuellstem Stand befunden habe. Sie hätten auch keine Pflichten nach § 13 Abs. 7 TMG verletzt, indem sie beim Betrieb ihrer Internetseite (zwischenzeitlich) nicht die neueste -Version eingesetzt und Erweiterungen nicht geupdatet hätten. Diese Maßnahmen hätten nicht in einem angemessenen Verhältnis zum angestrebten Schutzzweck gestanden und seien ihnen wirtschaftlich nicht zumutbar gewesen. Zwischen April 2017 und Juni 2018 hätten ihnen wegen ausgelaufener Drittmittel die finanziellen Mittel dafür gefehlt, auf die aktuellste -Version umzusteigen oder die Erweiterungen upzudaten bzw. zu deinstallieren. Sie müssten als Diensteanbieter Sicherheitsvorkehrungen nur dann vornehmen, wenn diese in einem angemessenen Verhältnis zum angestrebten Schutzzweck stünden. Da ihre Webseite nur Informationszwecken diene und man dort nichts bestellen könne, sei es nicht angemessen, ständig die neueste Version des Content-Management-Systems einzuspielen. Derartige Anforderungen könne man nur an Online-Shops oder sog. kritische Infrastrukturen stellen. Es sei zu berücksichtigen, dass § 13 Abs. 7 TMG durch das am 24.07.2015 verkündete IT-Sicherheitsgesetz eingeführt wurde, welches vor allem dem Schutz von sog. kritischen Infrastrukturen diene, wozu sie, die Antragsgegnerinnen, nicht gehörten.

Das Landgericht hat durch Urteil vom 22.01.2019 den Antrag auf Erlass einer einstweiligen Verfügung zurückgewiesen. Dem Antragsteller stehe gem. § 97 Abs. 1 UrhG weder aufgrund täterschaftlicher Verantwortlichkeit der Antragsgegnerinnen noch aufgrund einer Störerhaftung ein Verfügungsanspruch zu. Wegen der Einzelheiten wird auf das Urteil Bezug genommen.

Mit seiner form- und fristgerecht eingelegten Berufung erstrebt der Antragsteller unter Abänderung des landgerichtlichen Urteils den Erlass der einstweiligen Untersagungsverfügung.

Er meint, das Landgericht habe zu Unrecht die Störerhaftung der Antragsgegnerinnen wegen fehlender Kausalität abgelehnt. Die erstinstanzliche Entscheidung beruhe auf einer Verletzung der richterlichen Hinweispflicht gem. § 139 ZPO. Er habe erst aus dem landgerichtlichen Urteil erfahren, dass er zur Kausalität hätte vortragen müssen. Unzutreffend habe das Landgericht ihm den Nachweis der Kausalität auferlegt. Die Antragsgegnerinnen hätten unzureichend Auskunft erteilt, so dass er habe darauf vertrauen dürfen, dass das Gericht die Antragsgegnerinnen zu entsprechenden Auskünften anhalten werde. Eine Pflichtverletzung der Antragsgegnerinnen sei unstreitig und ergebe sich aus dem Betrieb eines unsicheren Content-Management-Systems mit Sicherheitslücken. Es sei die Rechtsprechung des BGH in Filesharing-Fällen zum Betrieb eines nicht ausreichend gesicherten WLAN-Anschlusses bei Privatpersonen übertragbar. Hiernach sei nicht gänzlich unwahrscheinlich, dass unberechtigte Dritte einen unzureichend gesicherten WLAN-Anschluss dazu benutzten, urheberrechtlich geschützte Musiktitel im Internet in Tauschbörsen ein-

zustellen. Es genüge für die Störerhaftung nach der Rechtsprechung des BGH somit, dass es nicht gänzlich unwahrscheinlich sei, dass unberechtigte Dritte einen unzureichend gesicherten Server dazu benutzten, urheberrechtlich geschützte Werke im Internet einzustellen. Die Unterlassung ausreichender Sicherungsmaßnahmen habe auf dem Willen der Antragsgegnerinnen beruht. Es liege eine Verletzung der Prüfpflicht mit der Folge der Störerhaftung vor, wenn die gebotenen Sicherungsmaßnahmen unterblieben. Die Antragsgegnerinnen seien verpflichtet gewesen, ein aktuelles Content-Management-System mit aktuellen Modulen aufzusetzen.

Die Störerhaftung der Antragsgegnerinnen ergebe sich auch aus ihrem Verhalten nach der Abmahnung. Indem die Antragsgegnerinnen – was unstreitig ist – nach Erhalt der Abmahnung eine Strafanzeige erstattet hätten, hätten sie unberechtigt und mittels unangemessenen Drucks versucht, ihn, den Antragsteller mit dem Ziel einzuschüchtern, ihn von weiterer Rechtsverfolgung abzuhalten.

Der Antragsteller beantragt,

> unter Abänderung des Urteils des Landgerichts Hamburg vom 22.01.2019, Az. 310 O 219/18, der Antragsgegnerin zu 1. und der Antragsgegnerin zu 2. bei Meidung eines vom Gericht für jeden Fall der Zuwiderhandlung festzusetzenden Ordnungsgeldes von bis zu € 250.000,-, ersatzweise Ordnungshaft bis zu 6 Monaten, oder Ordnungshaft bis zu 6 Monaten, Ordnungshaft jeweils zu vollstrecken an den jeweiligen Rektoren und Präsidenten
>
> zu untersagen,
>
> Dritten zu ermöglichen, ohne Zustimmung des Antragstellers das von diesem hergestellte Lichtbild/Lichtbildwerk mit dem Namen „ “ wie in Anlage K1 abgebildet über das Internet öffentlich zugänglich zu machen, ohne dazu berechtigt zu sein,
>
> wie im Internetauftritt http:// .php mittels des zum Zeitpunkt der Installation veralteten Content Management Systems und mittels zum Zeitpunkt der Installation veralteter Module zu diesem Content Management System namentlich geschehen.

Die Antragsgegnerinnen beantragen,

> die Berufung zurückzuweisen.

Die Antragsgegnerinnen verteidigen das angegriffene Urteil unter Wiederholung und Vertiefung ihres erstinstanzlichen Vorbringens.

Ergänzend machen sie geltend, dass sie nicht wüssten, wer ihre Webseite gehackt habe. Ein Anfangsverdacht für einen Hackerangriff habe vorgelegen (abweichendes Layout, abweichende Sprache, fehlende Verlinkung). Strafanzeige sei gegen „unbekannt" erstattet worden.

Eine Verletzung der Hinweispflicht gem. § 139 ZPO liege nicht vor. Das Landgericht habe zu Recht eine Störerhaftung mangels Sorgfaltspflichtverletzungen der Antragsgegnerinnen verneint. Der Gesetzgeber habe die Störerhaftung beim gewerblichen WLAN-Betreiber grundsätzlich abgeschafft. Der Antragsteller versuche, ihnen obliegende Sorgfaltspflichten zu erfinden. Soweit sich diese aus § 13 Abs. 7 TMG ergäben, seien sie von ihnen beachtet worden. Sie seien nicht verpflichtet gewesen, die jeweils neueste -Version einzusetzen und die Erweiterungen sofort zu updaten, wenn diese Maßnahmen in keinem angemessenen Verhältnis zum Schutzzweck stünden und ihnen wirtschaftlich nicht zumutbar seien.

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die zwischen den Parteien gewechselten Schriftsätze nebst Anlagen sowie die Protokolle zur mündlichen Verhandlung vor dem Landgericht vom 15.11.2018 sowie vor dem Senat vom 29.04.2020 Bezug genommen.

II.

1. Die zulässige Berufung des Antragstellers bleibt in der Sache ohne Erfolg.

a. Ein Verfügungsanspruch auf Unterlassung steht dem Antragsteller gegen die Antragsgegnerinnen im Zusammenhang mit dem streitgegenständlichen Hackerangriff – überwiegend wahrscheinlich – weder aus §§ 97 Abs. 1, 15, 16, 19a UrhG noch aus § 1004 BGB analog zu (§§ 935, 936, 920 Abs. 2 ZPO). Eine Verantwortlichkeit der Antragsgegnerinnen aus dem im Berufungsverfahren gegenständlichen Haftungsgrund als Störer besteht nicht.

aa. Da der Antragsteller den geltend gemachten Unterlassungsanspruch auf Wiederholungsgefahr gestützt hat, ist sein Begehren nur begründet, wenn das beanstandete Verhalten der Antragsgegnerinnen sowohl zum Zeitpunkt seiner Vornahme rechtswidrig als auch zum Zeitpunkt des Schlusses der mündlichen Verhandlung vor dem Senat rechtswidrig war (stRspr; BGH, NJW 2018, 3779 Rn. 37 – Dead Island).

bb. Von der Urheberschaft und damit der Aktivlegitimation des Antragstellers ist im vorliegenden einstweiligen Verfügungsverfahren auszugehen, weil sich aus dem glaubhaft gemachten Antragstellervortrag hinreichende Indizien für dessen Urheberschaft ergeben, die von den Antragsgegnerinnen nicht erheblich angegriffen worden sind.

cc. Anzunehmen ist auch, dass ein öffentliches Zugänglichmachen des streitgegenständlichen Lichtbildes gem. § 19a UrhG vorlag. Ein urheberrechtlich geschütztes Werk ist bereits dann im Internet öffentlich zugänglich gemacht iSd § 19a UrhG, wenn es durch Eingabe einer

URL erreichbar ist; eine Verlinkung mit der Homepage des Verletzers ist nicht notwendig (Senat, Beschl. v. 08.02.2010, 5 W 5/10, NJOZ 2010, 2111). Auch stellt das Heraufspielen einer Datei auf einen Server, der die Datei dann im Internet bereithält, eine Vervielfältigung gem. § 16 UrhG dar (Wandtke/Bullinger/Heerma, 5. Aufl., UrhG § 16 Rn. 19).

dd. Jedoch besteht eine Passivlegitimation der Antragsgegnerinnen im Ergebnis nicht.

aaa. Eine täterschaftliche Haftung der Antragsgegnerinnen ist nicht gegeben und wird vom Antragsteller nicht mehr geltend gemacht. Im Berufungsverfahren beschränkt sich der Vorwurf des Antragstellers darauf, die Antragsgegnerinnen hätten ihren Internetauftritt .de mittels eines veralteten Content-Management-Systems und mittels veralteter Module bzw. Erweiterungen zu diesem Content-Management-System betrieben und es hierdurch ermöglicht, dass Hacker das streitgegenständliche Lichtbild auf dem Server der Internetseite hochluden, so dass dieses öffentlich zugänglich gemacht wurde. Hierin liegt keine täterschaftliche Begehung der vorgeworfenen Urheberrechtsverletzung durch die Antragsgegnerinnen, da die Verletzung derartiger Verkehrspflichten keine Täterhaftung gem. § 97 Abs. 1 UrhG begründet.

(1) Im Urheberrecht beurteilt sich eine täterschaftliche Haftung grundsätzlich nach den im Strafrecht entwickelten Rechtsgrundsätzen (BGH, MMR 2018, 303, 304 – Konferenz der Tiere). Als Täter einer Urheberrechtsverletzung haftet deshalb nur, wer selbst, in mittelbarer Täterschaft oder in Mittäterschaft die Merkmale einen der handlungsbezogenen Verletzungstatbestände erfüllt (vgl. BGH, GRUR 2013, 1229, 1231 – Kinderhochstühle im Internet II; BGH, GRUR 2010, 633 Rn. 13 – Sommer unseres Lebens; Wandtke/Bullinger/v. Wolff, 5. Aufl., UrhG § 97 Rn. 14). Im Berufungsverfahren ist unstreitig, dass die Antragsgegnerinnen nicht selbst das streitgegenständliche Foto auf ihre Internetseite hochgeladen und damit die Verletzungshandlung des § 16 UrhG begangen haben. Damit haben sie auch die Handlung des öffentlichen Zugänglichmachens iSd § 19a UrhG nicht selbst begangen. Denn durch das Einstellen eines Fotos wird den Besuchern der Webseite, auf der die Einstellung erfolgt ist, der Zugang zum betreffenden Foto auf dieser Webseite ermöglicht (BGH, GRUR 2019, 813 Rn. 40 – Cordoba II). Das Zugänglichmachen liegt in dem Einstellen ins Internet (Dreier/Schulze/Dreier, 6. Aufl. 2018, UrhG § 19a Rn. 6), welches die Antragsgegnerinnen nach dem zugrunde zu legenden Sachverhalt nicht vorgenommen haben.

(2) Die Verletzung von Verkehrspflichten begründet hingegen keine täterschaftliche Haftung gem. § 97 Abs. 1 UrhG (BGH, GRUR 2011, 1018 Rn. 18 – Automobil-Onlinebörse; BGH, GRUR 2010, 633 Rn. 13 – Sommer unseres Lebens). Im vorliegenden Fall müsste das Verhalten der Antragsgegnerinnen – also der Betrieb einer Internetseite mit einem Content-Management-System, das Sicherheitslücken aufweist – den Tatbestand der öffentlichen Zugänglichmachung (§ 19a UrhG) oder der Vervielfältigung (§ 16 UrhG) des in Rede stehenden urheberrechtlichen Werkes erfüllen

(vgl. BGH, 2010, 633 Rn. 13 – Sommer unseres Lebens). Dies ist jedoch nicht der Fall.

bbb. Im vorliegenden Fall haften die Antragsgegnerinnen entgegen der Auffassung des Antragstellers auch nicht nach den Grundsätzen der Störerhaftung, so dass die landgerichtliche Entscheidung im Ergebnis nicht zu beanstanden ist.

Als Betreiber einer Internetseite und als Diensteanbieter gem. § 2 Satz 1 Nr. 1 TMG trafen die Antragsgegnerinnen bis zur Kenntnis von der Rechtsverletzung keine anlasslosen Prüf- und Überwachungspflichten. Aus Anforderungen zur IT-Sicherheit, etwa § 13 Abs. 7 TMG, ergibt sich eine urheberrechtliche Störerhaftung für den hier gegenständlichen Verletzungsfall ebenfalls nicht.

(1) Die mittelbare Verursachung von Urheberrechtsverletzungen wird von der deutschen Rechtsprechung insbesondere im Rahmen der sog. Störerhaftung erfasst. Diese Haftungsfigur ist auf die Verletzung absoluter Rechte begrenzt und wird mit einem Analogieschluss zu § 1004 BGB begründet (Leistner in Schricker/Loewenheim, UrhG, 6. Aufl., § 97 Rn. 72). Als Störer kann auf Unterlassung und Beseitigung in Anspruch genommen werden, wer – ohne Täter oder Teilnehmer zu sein – in irgendeiner Weise willentlich und adäquat-kausal zur Verletzung des geschützten (absoluten) Rechts beiträgt (vgl. BGH, GRUR 2017, 617 Rn. 11 – WLAN-Schlüssel; Wandtke/Bullinger/v. Wolff, 5. Aufl., UrhG § 97 Rn. 15). Dabei kann als Beitrag auch die Unterstützung oder Ausnutzung der Handlung eines eigenverantwortlich handelnden Dritten genügen, sofern der in Anspruch Genommene die rechtliche und tatsächliche Möglichkeit zur Verhinderung dieser Handlung hatte (BGH, GRUR 2017, 617 Rn. 11 – WLAN-Schlüssel). Da die Störerhaftung nicht über Gebühr auf Dritte erstreckt werden darf, die weder als Täter noch als Teilnehmer für die begangene Urheberrechtsverletzung in Anspruch genommen werden können, setzt die Haftung als Störer die Verletzung zumutbarer Verhaltenspflichten, insbesondere von Prüfpflichten voraus (BGH, GRUR 2017, 617 Rn. 11 – WLAN-Schlüssel; Nordemann in Fromm/Nordemann, UrhG, 12. Aufl., § 97 Rn. 157). Die Feststellung einer solchen Prüfpflichtverletzung bedarf einer umfassenden Interessenabwägung und wertenden Risikozuweisung, ob die Prüfpflicht zumutbar war (Nordemann in Fromm/Nordemann, UrhG, 12. Aufl., § 97 Rn. 157). Weiter bestimmt sich nach den jeweiligen Umständen des Einzelfalls unter Berücksichtigung von Funktion und Aufgabenstellung des als Störer in Anspruch Genommenen sowie mit Blick auf die Eigenverantwortung desjenigen, der die rechtswidrige Beeinträchtigung selbst unmittelbar vorgenommen hat, ob und inwieweit dem als Störer in Anspruch Genommenen eine Verhinderung der Verletzungshandlung des Dritten zuzumuten ist (vgl. BGH, GRUR 2017, 617 Rn. 11 – WLAN-Schlüssel). Hierbei kann auch auf gesetzlich normierte Pflichten zurückgegriffen werden (z.B. § 832 BGB, vgl. Nordemann in Fromm/Nordemann, UrhG, 12. Aufl., § 97 Rn. 157). Auch das Geschäftsmodell des als Störer in Anspruch Genommenen ist von Bedeutung; wer ohne Gewinnerzielungsabsicht im öffentlichen

Interesse handelt, wird großzügiger behandelt als Störer, die aus der Verletzung Gewinn ziehen (Nordemann in Fromm/Nordemann, UrhG, 12. Aufl., § 97 Rn. 157).

(2) Zwar sind bei der Prüfung, welche zumutbaren Prüf- oder Verhaltenspflichten einem als Störer in Anspruch Genommenen obliegen, die Haftungsprivilegien der §§ 7 ff. TMG zu berücksichtigen (vgl. BGH, GRUR 2013, 1030 Rn. 30 – File-Hosting-Dienst; BeckOK UrhR/Reber, 27. Ed. 20.04.2018, UrhG, § 97, Rn. 56). Insoweit hat das Europäische Recht wesentlichen Einfluss auf die Haftung für Rechtsverletzungen, indem die Haftungsprivilegien für Provider nach der E-Commerce-RL (Richtlinie 2000/31/EG) in Deutschland in den Sonderregeln des TMG für die unterschiedlichen Internetprovider umgesetzt worden sind (Leistner in Schricker/Loewenheim, UrhG, 6. Aufl., § 97 Rn. 55). Einer allgemeinen proaktiven Prüf- und Überwachungspflicht von Diensteanbietern i.S.d. §§ 8 bis 10 TMG für die von ihnen gespeicherten Informationen steht dabei § 7 Abs. 2 Satz 1 TMG entgegen (vgl. BGH, GRUR, 2013, 1030 Rn. 30 – File-Hosting-Dienst; BGH, GRUR 2016, 268 Rn. 21 – Störerhaftung des Access-Providers). Betreffende Diensteanbieter sind nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen proaktiv zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hindeuten (vgl. BGH, GRUR 2013, 1030 Rn. 30 – File-Hosting-Dienst; BGH, GRUR 2016, 268 Rn. 21 – Störerhaftung des Access-Providers).

Jedoch sind die Antragsgegnerinnen keine Provider i.S.d. §§ 8 bis 10 TMG. Sie betreiben mit ihrer Internetseite keinen Dienst, über den von einem Nutzer eingegebene Informationen in einem Kommunikationsnetz übermittelt oder der Zugang zu einem Kommunikationsnetz vermittelt werden (§ 8 TMG, vgl. Gersdorf/Paal, BeckOK Informations- und Medienrecht, 28. Ed. 01.02.2020, TMG § 8 Rn. 3). Die Webseite der Antragsgegnerinnen ist auch nicht darauf angelegt, fremde Informationen bzw. Informationen von Nutzern zu speichern (vgl. § 10 TMG). Wesentlicher Privilegierungsgrund des § 10 TMG ist die Beschränkung der Tätigkeit von Diensteanbietern im Rahmen des Hosting auf den technischen Vorgang der Speicherung von fremden Informationen (Gersdorf/Paal, BeckOK Informations- und Medienrecht, 28. Ed. 01.02.2020, TMG § 10 Rn. 3). Die Antragsgegnerinnen sind jedoch in diesem Sinne keine Host-Provider. Sie stellen ihren Nutzern keinen Speicherplatz zur Verfügung, um Inhalte ins Internet hochzuladen oder zu posten. Zwar wurden die hier beanstandeten Inhalte auf der Internetseite der Antragsgegnerinnen hochgeladen und gespeichert. Dies geschah jedoch durch einen Hackerangriff und nicht über Nutzern zur Verfügung gestellten Speicherplatz.

(3) Als Webseite-Betreiber bzw. Domaininhaber haften die Antragsgegnerinnen zwar grundsätzlich für die Inhalte ihrer Homepage täterschaftlich, wenn sie die Inhalte der Webseite kontrollieren (dann ggf. über §§ 31, 89 BGB, vgl. Nordemann in Fromm/Nordemann, UrhG, 12. Aufl., § 97 Rn.

169). Aus diesem Haftungsgrund scheidet eine Haftung für die Inhalte der hier gegenständlichen, über einen Hackerangriff zugefügten Seiten jedoch aus. Nutzer können auf der Internetseite der Antragsgegnerinnen, die Informationszwecken dient, nichts hochladen. Bei den unbemerkt im Rahmen eines Hackerangriffs abgelegten Inhalten handelt es sich um keine von den Antragsgegnerinnen kontrollierten Inhalte.

(4) Durch die Begrenzung der Störerhaftung aufgrund des Erfordernisses der Verletzung zumutbarer Verkehrspflichten, insbesondere Prüfpflichten, ist in der Regel Voraussetzung einer Störerhaftung, dass der Störer zuvor auf eine konkrete, klare Rechtsverletzung hingewiesen worden ist (Leistner in Schricker/Loewenheim, UrhG, 6. Aufl., § 97 Rn. 79). Erst nach einem Hinweis auf einen konkreten Rechtsverstoß ist der Störer verpflichtet, diese konkrete Rechtsverletzung abzustellen und gegebenenfalls im Rahmen des Möglichen und Zumutbaren bestimmte gleichartige zukünftige Rechtsverletzungen durch spezifische Vorabprüfungen zu unterbinden (Leistner in Schricker/Loewenheim, UrhG, 6. Aufl., § 97 Rn. 79). Auch über diesen Gesichtspunkt lässt sich im vorliegenden Fall eine Störerhaftung der Antragsgegnerinnen nicht begründen. Im Zusammenhang mit der streitgegenständlichen Rechtsverletzung ist ein Hinweis auf die konkrete Rechtsverletzung verbunden gewesen. Jedoch begründet dieser erstmalige Hinweis keine Störerhaftung gerade für den Rechtsverletzungsfall, auf den hingewiesen worden ist, sondern nur für einen etwaigen Folgefall. Um einen solchen geht es hier jedoch nicht.

(5) Schließlich ergibt sich eine Störerhaftung der Antragsgegnerinnen für die hier geltend gemachte Rechtsverletzung auch nicht aus einer Verletzung von Pflichten gem. § 13 Abs. 7 TMG.

(a) Die nationale Regelung des § 13 Abs. 7 TMG wurde durch das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz, BGBl. I 2015, 1324) mit Wirkung zum 25.07.2015 in das Telemediengesetz eingefügt. Durch technische und organisatorische Maßnahmen, die dem Stand der Technik zu entsprechen haben, ist durch Anbieter von Telemediendiensten sicherzustellen, dass kein unerlaubter Zugriff auf die genutzten technischen Einrichtungen möglich ist und diese gegen die Verletzung des Schutzes personenbezogener Daten (§ 13 Abs. 7 Nr. 2a TMG) und gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind, gesichert sind (§ 13 Abs. 7 Nr. 2b TMG) (Spindler/Schmitz, TMG, 2. Aufl., TMG § 13 Rn. 77). Im Rahmen ihrer jeweiligen Verantwortlichkeit und unter dem Vorbehalt der technischen Möglichkeit und wirtschaftlichen Zumutbarkeit trifft geschäftsmäßige Diensteanbieter die Pflicht, rechtswidrige Angriffe zu vermeiden (Spindler/Schmitz, TMG, 2. Aufl., TMG § 13 Rn. 83). In diesem Rahmen sind von einem Diensteanbieter Schutzvorkehrungen zu treffen, deren Kosten in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen, wobei die jeweiligen Anforderungen im Einzelfall zu berücksichtigen sind (BT-Drucks. 18/4096, S. 34). § 13 Abs. 7

TMG ist eine Regelung im vierten Abschnitt des Telemediengesetzes unter der Überschrift „Datenschutz". Gesetzgeberisches Ziel der Einfügung des § 13 Abs. 7 TMG ist u.a. die Eindämmung der Hauptverbreitungswege von Schadsoftware (BT-Drucks. 18/4096, S. 34). Je nach Sensibilität und Umfang der verarbeiteten Daten kann das erforderliche Schutzniveau dabei unterschiedlich sein (BT-Drucks. 18/4096, S. 34). Hieraus folgt, dass es um den Schutz der Nutzerdaten geht.

(b) Dahinstehen kann im vorliegenden Fall, ob § 13 TMG durch die Bestimmungen der Datenschutz-Grundverordnung (DS-GVO, Verordnung (EU) 2016/679), die seit dem 25.05.2018 gilt, verdrängt worden ist (vgl. OLG Stuttgart, GRUR-RS 2020, 2392 Rn. 31). Die DS-GVO beansprucht gemäß Art. 288 Absatz 2 AEUV unmittelbare Geltung und verdrängt im Kollisionsfall das nationale Recht. Den Mitgliedstaaten ist es untersagt, (auch gleichlaufende) Regelungen zu erlassen, die den Anwendungsbereich der Verordnung verschleiern und damit die Auslegungshoheit des Europäischen Gerichtshofs über das Unionsrecht in Frage stellen (EuGH, Urteil vom 10.10.1973, C-34/73, Rn. 11; vgl. OLG Stuttgart, GRUR-RS 2020, 2392 Rn. 31). Die auf den Datenschutz bezogenen Pflichten des Diensteanbieters richten sich daher seit ihrem Inkrafttreten allein nach der DS-GVO, nicht nach § 13 TMG (vgl. OLG Stuttgart, GRUR-RS 2020, 2392 Rn. 31). Im vorliegenden Fall beanstandet der Antragsteller jedoch, dass die Antragsgegnerinnen den hier gegenständlichen rechtswidrigen Angriff auf ihre geschäftsmäßig betriebene Internetseite nicht vermieden haben und es hierdurch zu einer Urheberrechtsverletzung gekommen ist.

(c) Gegenüber dem Antragsteller, der kein Nutzer der Internetseite der Antragsgegnerinnen ist, indem er dort nichts hoch- oder heruntergeladen hat, sind jedoch auch etwaige Verkehrspflichten aus § 13 Abs. 7 TMG nicht verletzt worden. Ein Pflichtwidrigkeitszusammenhang zwischen dem nicht verhinderten Hackerangriff und der im vorliegenden Fall gegenständlichen Urheberrechtsverletzung im Hinblick auf Pflichten aus § 13 Abs. 7 TMG besteht nicht.

(aa) § 13 Abs. 7 TMG stellt Anforderungen „im Rahmen der jeweiligen Verantwortlichkeit" der betreffenden Diensteanbieter auf, wobei sich die Verantwortung aus den §§ 7 ff. TMG ergibt. Eine sich hieraus ergebende Privilegierung ist zu berücksichtigen.

Die Antragsgegnerinnen sind hinsichtlich des Betriebs ihrer Internetseite als geschäftsmäßige Telemediendiensteanbieter i.S.d. § 13 Abs. 7 TMG anzusehen. Die weitere Voraussetzung, dass die Verpflichtung der Anbieter von Telemedien nach § 13 Abs. 7 TMG nur „im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien" gilt (vgl. Spindler/Schmitz, TMG, 2. Aufl., § 13 TMG Rn. 83), ist nicht erfüllt. Diese Verantwortung besteht danach für die eigenen oder sich zu eigen gemachten Inhalte des Anbieters (vgl. Spindler/Schmitz, TMG, 2. Aufl., § 13 TMG Rn. 83). Der Anbieter ist grundsätzlich für die Inhalte und die Webseiten verantwortlich, für die er als Anbieter auftritt und damit kongruent zu seiner Eigenschaft als Anbieter dieser Tele-

medien (vgl. Spindler/Schmitz, TMG, 2. Aufl., § 13 TMG Rn. 83). Wenn ein rechtswidriger Angriff gerade darin liegt, dass Seiten des Anbieters von Dritten unberechtigt um neue Seiten erweitert werden, so ist der Anbieter sicherheitstechnisch jedenfalls dann nicht verantwortlich, wenn sich klar ergibt, dass dies nicht seine Inhalte sind (vgl. Spindler/Schmitz, TMG, 2. Aufl., § 13 TMG Rn. 83). Wird es hingegen für den Nutzer nicht erkennbar, dass es sich um unautorisierte Inhalte handelt, dann soll sich eine Verantwortung des Anbieters auch für Sicherheitsmaßnahmen nach § 13 Abs. 7 TMG ergeben (vgl. Spindler/Schmitz, TMG, 2. Aufl., § 13 TMG Rn. 83). Rechtswidrig eingestellte Inhalte können dem Anbieter nicht ohne weiteres zugerechnet werden, es sei denn, er muss diese kennen oder kennt diese, ohne diese zu entfernen oder sich zu distanzieren (vgl. Spindler/Schmitz, TMG, 2. Aufl., § 13 TMG Rn. 83). Nach Kenntnis ist auch eine weitergehende Verantwortlichkeit möglich.

Im vorliegenden Fall steht einer Verantwortlichkeit der Antragsgegnerinnen entgegen, dass die rechtswidrig zugefügten Seiten nach dem unstreitigen Sachverhalt deutlich abweichend und in englischer Sprache gestaltet sind, während die übrigen Internetseiten der Antragsgegnerinnen in deutscher Sprache verfasst sind. Auch das Layout ist unstreitig gänzlich abweichend gestaltet. Bereits hieraus ergibt sich, dass es sich für einen Nutzer erkennbar um keine Inhalte der Antragsgegnerinnen handelt. Die hinzugefügten Seiten waren unstreitig nicht über die Internetseite der Antragsgegnerinnen verlinkt. Selbst wenn aufgrund des Backlinks auf den rechtswidrig zugefügten Seiten eine Zuordnung beim Gelangen auf die zugefügten Seiten möglich ist, so scheitert eine Zurechnung daran, dass die Antragsgegnerinnen die zugefügten Internetseiten bis zur Abmahnung nicht kannten und nach Kenntnis sofort entfernten.

(bb) Der Antragsteller ist im Hinblick auf die gegenständliche Rechtsverletzung nicht vom Schutzbereich des § 13 Abs. 7 TMG erfasst.

§ 13 Abs. 7 TMG gewährt u.a. einen spezifischen Nutzerschutz, wobei der Verkehr, der im Zusammenhang mit dem Betrieb der konkreten Internetseite eröffnet worden ist, geschützt ist. Die erforderlichen Schutzvorkehrungen hängen von der Sensibilität und dem Umfang der verarbeiteten Daten ab (BT-Drucks. 18/4096 S. 34, 35). Der Gesetzgeber hat den Schutz von Urhebern bei der Einführung des § 13 Abs. 7 TMG durch das IT-Sicherheitsgesetz nicht im Blick gehabt. Insofern besteht ein Unterschied zu § 7 Abs. 4 TMG nF. Nach der Begründung zum Regierungsentwurf des Dritten Gesetzes zur Änderung des Telemediengesetzes mit Wirkung vom 13.10.2017 wurde mit dem Sperranspruch gem. § 7 Abs. 4 TMG nF ein Verfahren geschaffen, mit dem „abseits der viel kritisierten Störerhaftung“ zugunsten der Rechtsinhaber die Möglichkeit gerichtlicher Anordnungen gegen Vermittler vorgesehen wird, deren Dienste von einem Dritten zur Verletzung eines Urheberrechts oder verwandter Schutzrechte genutzt werden (BGH, GRUR 2018, 1044 Rn.

43 – Dead Island). Anders als die Vorschrift des § 7 Abs. 4 TMG nF bezwecken die Bestimmungen des § 13 Abs. 7 TMG und der DS-GVO nicht den Schutz von Inhabern von Urheberrechten oder verwandten Schutzrechten. Während bei Access-Providern und WLAN-Betreibern, für die § 7 Abs. 4 TMG nF gilt, die Gefahr von Urheberrechtsverletzungen durch Dritte besteht, da deren Dienste darauf abzielen, Nutzerinformationen durchzuleiten (§ 8 TMG), ist die Gefahr von Urheberrechtsverletzungen bei einem Betreiber einer Internetseite, die nur Informationszwecken dient und auf die Nutzer keine Inhalte einstellen oder durchleiten können, nur im Falle eines Hackerangriffs gegeben. Vom Schutzzweck des § 13 Abs. 7 TMG ist der durch einen Hackerangriff geschädigte Inhaber von Urheberrechten bzw. verwandten Schutzrechten nicht erfasst.

Zwar ist gesetzgeberisches Ziel der Einführung des § 13 Abs. 7 TMG gewesen, die Verbreitung von Schadsoftware einzudämmen bzw. zu verhindern, indem geschäftsmäßigen Diensteanbietern Pflichten zur IT-Sicherheit auferlegt worden sind (BT-Drucks. 18/4096, S. 34). Der im vorliegenden Fall erfolgte Hackerangriff stellt einen Angriff auf die IT-Sicherheit der von den Antragsgegnerinnen betriebenen Internetseite dar. Jedoch folgt aus einem Verstoß gegen § 13 Abs. 7 TMG kein urheberrechtlicher Unterlassungsanspruch. Die Vorschrift des § 13 Abs. 7 TMG ist keine selbstständige Anspruchsgrundlage, sondern so einzuordnen, dass sie zusätzliche anspruchsbegründende Merkmale für eine Verantwortlichkeit des Diensteanbieters enthält (so zu § 5 Abs. 2 TDG a.F.: BGH, GRUR 2004, 74, 75 – rassistische Hetze). Der Antragsteller ist kein Vertragspartner der Antragsgegnerinnen, so dass eine etwaige Verletzung von Pflichten aus § 13 Abs. 7 TMG nicht als Pflichtverletzung i.S.d. § 280 BGB angesehen werden kann (vgl. hierzu Spindler/Schmitz, TMG, 2. Aufl., TMG § 13 Rn. 125). Soweit es sich bei § 13 Abs. 7 TMG um ein Schutzgesetz i.S.d. § 823 Abs. 2 BGB handelt (Spindler/Schmitz, TMG, 2. Aufl., TMG § 13 Rn. 125), stehen dem Antragsteller Ansprüche aus § 823 Abs. 2 BGB nicht zu, weil er nicht in den Schutzbereich der verletzten Norm fällt.

Der gesetzgeberische Schutzzweck ist auch im Rahmen eines Anspruchs aus §§ 823 Abs. 1, 1004 BGB analog zu berücksichtigen, da sich Verkehrspflichten nur insoweit ergeben können, als ein Verkehr eröffnet worden ist. Die streitgegenständliche Rechtsverletzung ist nicht über den mit dem Betrieb der Internetseite der Antragsgegnerinnen eröffneten Verkehr geschehen, sondern über eine von Hackern entdeckte Sicherheitslücke im sog. Backend, einem passwortgeschützten Bereich der Internetseite, zu dem Nutzer keinen Zugang haben. Es ist nicht der Nutzerverkehr betroffen, den § 13 Abs. 7 TMG schützt. Dem Kläger als Inhaber von Urheberrechten bzw. verwandten Schutzrechten betreffend rechtswidrig hinzugefügte Internetseiten ist insoweit kein Schutz zuzusprechen, den ihm der Gesetzgeber mit der Einführung des § 13 Abs. 7 TMG nicht geben wollte.

(cc) Offenbleiben kann, ob auch aus Zumutbarkeitsgesichtspunkten im vorliegenden Fall eine Störerhaftung der Antragsgegnerinnen ausscheidet.

Eine urheberrechtliche Störerhaftung aus Gründen der Anforderungen an die IT-Sicherheit steht unter einem zweifachen Zumutbarkeitsvorbehalt: Die Haftung Dritter aus § 97 Abs. 1 UrhG, die nicht Täter oder Teilnehmer sind, für eine begangene Urheberrechtsverletzung kommt nur in Betracht, wenn zumutbare Verhaltenspflichten verletzt worden sind (BGH, GRUR 2017, 617 Rn. 11 – WLAN-Schlüssel). Daneben stehen die Anforderungen an die IT-Sicherheit aus § 13 Abs. 7 TMG unter einem Zumutbarkeitsvorbehalt (vgl. BT-Drucks 18/4096 S. 34); durch das Kriterium der Zumutbarkeit soll sichergestellt werden, dass von dem Diensteanbieter nur solche Vorkehrungen zu treffen sind, deren Kosten zum angestrebten Schutzzweck in einem angemessenen Verhältnis stehen. Es ist die Verhältnismäßigkeit von Sicherungsmaßnahmen zu berücksichtigen (vgl. Spindler/Schmitz, TMG, 2. Aufl., § 13 TMG Rn. 97; BT-Drucks 18/4096 S. 34). Nach den Gesetzesmaterialien soll durch das Kriterium der Zumutbarkeit in § 13 Abs. 7 TMG eine flexible Anpassung der jeweiligen Anforderungen im Einzelfall ermöglicht werden (BT-Drucks 18/4096 S. 34). Der Umfang von Verkehrspflichten wird zudem durch eine spezifische Gefahrgeneigtheit des Geschäftsmodells mitbestimmt (Leistner in Schricker/Loewenheim, UrhG, 6. Aufl., § 97 Rn. 129).

Hier ist zu berücksichtigen, dass die Antragsgegnerinnen eine Internetseite betreiben, die nicht den Dienst anbietet, von Nutzern bereitgestellte Informationen zu speichern. Eine Bearbeitung der Web-Inhalte ist nur über das passwortgeschützte Backend der Webseite möglich und steht damit Nutzern der Internetseite nicht zur Verfügung. Die Internetseite der Antragsgegnerinnen dient Informationszwecken und man kann über sie nichts bestellen, so dass keine Kundendaten über sie gespeichert werden. Die Antragsgegnerinnen stellen auf ihrer Internetseite im wissenschaftlichen Bereich Informationen zur Verfügung. Sieht man den angestrebten Schutzzweck in der Vermeidung eines rechtswidrigen Angriffs, mit dem Seiten hinzugefügt werden, die rechtswidrige Inhalte enthalten, so ist die Gefahr eines solchen Angriffs bei einem Betrieb einer Open-Source-Software mit Sicherheitslücken gegeben. Das erforderliche Schutzniveau hängt jedoch auch davon ab, ob und in welchem Umfang sensible Daten auf der betreffenden Internetseite verarbeitet werden. Ob Letzteres dazu führt, dass das Aufspielen der jeweils aktuellen Updates der verwendeten Open-Source-Software im Zeitraum zwischen April 2017 und Juni 2018 im Hinblick auf einen damit verbundenen Kostenaufwand den Antragsgegnerinnen nicht zumutbar war, kann im vorliegenden Fallen dahinstehen, da ein Anspruch aus den oben unter (bb) genannten Gründen nicht gegeben ist.

(d) Auch auf eine Erstbegehungsgefahr kann der geltend gemachte Unterlassungsanspruch nicht gestützt werden. Der Umfang der Handlungspflichten, die sich aus einem Unterlassungsgebot

wegen Erstbegehungsgefahr ergeben, bestimmt sich danach, inwieweit dieses auf die Gefahr gestützt ist, dass bestimmte zumutbare Maßnahmen zur Vorbeugung gegen erneute derartige Rechtsverletzungen unterlassen werden (vgl. BGH GRUR 2011, 152 Rn. 38 ff. – Kinderhochstühle im Internet; Wandtke/Bullinger/v. Wolff, 5. Aufl. 2019 Rn. 28, UrhG § 97 Rn. 28). Die Antragsgegnerinnen entfernten jedoch die rechtswidrigen Inhalte und aktualisierten die Software nach Kenntniserlangung von dem Angriff. Es ist unstreitig, dass nach Erhalt der Abmahnung die zwei aufgefundenen Sicherheitslücken behoben wurden. Die Internetseite wird nunmehr geändert betrieben. Dass die Antragsgegnerinnen insoweit weiter Sicherheitslücken zuließen oder noch zulassen, ist weder dargetan noch ersichtlich. Eine Erstbegehungsgefahr liegt nicht vor.

ccc. Entgegen der Ansicht des Antragstellers lässt sich eine Störerhaftung für den hier gegenständlichen Verstoß aus dem Verhalten der Antragsgegnerinnen nach dem Verstoß ebenfalls nicht herleiten. In der Anzeigeerstattung gegen „unbekannt" kann eine Druckausübung gegenüber dem Antragsteller nicht gesehen werden. Es dürfte im Interesse des Antragstellers als Urheber gelegen haben, dass die hier zugrundeliegende Rechtsverletzung aufgeklärt wird. Hierin eine Erpressung zu sehen, erscheint fernliegend.

ee. Das Vorliegen eines Verfügungsgrundes kann offenbleiben, weil es bereits am Verfügungsanspruch fehlt.

2. Die Kostenentscheidung ergibt sich aus § 97 ZPO.

Vorsitzender Richter am Oberlandesgericht	Richter am Oberlandesgericht	Richterin am Oberlandesgericht