Verwaltungsgericht Köln, 1 L 466/22

Datum:	01.04.2022
Gericht:	Verwaltungsgericht Köln
Spruchkörper:	1. Kammer
Entscheidungsart:	Beschluss
Aktenzeichen:	1 L 466/22
ECLI:	ECLI:DE:VGK:2022:0401.1L466.22.00

Rechtskraft: nicht rechtskräftig

Tenor:

1.

Der Antrag wird abgelehnt.

Die Antragstellerin trägt die Kosten des Verfahrens.

2.

Der Wert des Streitgegenstands wird auf 100.000,00 Euro festgesetzt.

Gründe 1

Der nach § 123 Abs. 1 S. 2 Verwaltungsgerichtsordnung (VwGO) gestellte Antrag, 2

im Wege der einstweiligen Anordnung 3

1. der Antragsgegnerin bei Vermeidung eines vom Gericht für jeden Fall der Zuwiderhandlung festzusetzenden Ordnungsgeldes (und für den Fall, dass dieses nicht beigetrieben werden kann, Ordnungshaft) oder einer Ordnungshaft bis zu 6 Monaten (Ordnungsgeld im Einzelfall höchstens EUR 250.000,00, Ordnungshaft insgesamt höchstens 2 Jahre), zu vollziehen jeweils gegen die Bediensteten, die gegen den nachfolgenden Unterlassungstatbestand verstoßen, zu untersagen, vor der von der Antragstellerin vertriebenen Virenschutzsoftware zu warnen wie geschehen mit Schreiben vom 15. März 2022, 4

5

2. der Antragsgegnerin aufzugeben, die mit Schreiben vom 15. März 2022 ausgesprochene Warnung zu widerrufen,

hilfsweise, 6

die Warnung mit der als Anlage ASt 2 vorgelegten E-Mail unverzüglich, spätestens innerhalb eines Monats nach Veröffentlichung der Warnung, zu archivieren, 7

hat keinen Erfolg. 8

Der Antrag nach § 123 Abs. 1 S. 2 VwGO ist zulässig, insbesondere statthaft, da in der Hauptsache eine allgemeine Leistungsklage zu erheben wäre. Die Antragstellerin ist antragsbefugt (§ 42 Abs. 2 VwGO analog), da sie als Unternehmen des L. -Konzerns, das Virenschutzprodukte von L. u.a. in Deutschland vertreibt, durch die streitgegenständliche Warnung in eigenen Rechten betroffen ist. 9

Der Antrag ist jedoch nicht begründet. 10

Nach § 123 Abs. 1 S. 2 VwGO kann eine einstweilige Anordnung zur Regelung eines vorläufigen Zustands in Bezug auf ein streitiges Rechtsverhältnis nur erlassen werden, wenn dies zur Abwendung wesentlicher Nachteile, zur Verhinderung drohender Gewalt oder aus anderen Gründen nötig erscheint. Die Notwendigkeit der vorläufigen Regelung (Anordnungsgrund) und der geltend gemachte Anspruch (Anordnungsanspruch) sind glaubhaft zu machen (§ 123 VwGO i.V.m. § 920 Abs. 2, § 294 Zivilprozessordnung – ZPO –). 11

Führt der Erlass der begehrten einstweiligen Anordnung – wie hier – zu einer Vorwegnahme der Hauptsache, sind an das Vorliegen von Anordnungsgrund und Anordnungsanspruch hohe Anforderungen zu stellen. 12

Nach diesen Maßstäben liegt hier kein Anordnungsanspruch vor. Die Antragstellerin hat einen öffentlich-rechtlichen Unterlassungsanspruch nicht glaubhaft gemacht. 13

Der öffentlich-rechtliche Anspruch auf Unterlassung (der Wiederholung) einer amtlichen Äußerung setzt voraus, dass diese rechtswidrig in subjektive Rechte des Betroffenen eingreift und die konkrete Gefahr ihrer Wiederholung droht. Fehlt es – wie hier – an einer spezialgesetzlichen Grundlage für den Unterlassungsanspruch, leitet sich dieser aus einer grundrechtlich geschützten Position des Betroffenen ab. Die Grundrechte schützen vor rechtswidrigen Beeinträchtigungen jeder Art, auch solchen durch schlichtes Verwaltungshandeln. Der Betroffene kann daher, wenn ihm eine derartige Rechtsverletzung droht, gestützt auf das jeweilige Grundrecht Unterlassung verlangen. 14

Vgl. BVerwG, Urteil vom 20. November 2014 – 3 C 27.13 –, juris Rn. 11 m.w.N. 15

Diese Voraussetzungen sind hier nicht gegeben. Zwar greift die streitgegenständliche Warnung des Bundesamts für Sicherheit in der Informationstechnik (im Folgenden: BSI) vom 15. März 2022 in das Grundrecht der Antragstellerin aus Art. 12 Abs. 1, 19 Abs. 3 Grundgesetz (GG) ein (dazu I.). Der Eingriff ist jedoch gerechtfertigt, weil die Warnung sich nach summarischer Überprüfung im Verfahren des vorläufigen Rechtsschutzes als rechtmäßig erweist (dazu II.). 16

I. 17

18

Die auf § 7 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) gestützte hoheitliche Warnung stellt einen Eingriff in das aus Art. 12 Abs. 1 i.V.m. 19 Abs. 3 GG folgende subjektiv-öffentliche Recht der Antragstellerin dar. Die Antragstellerin kann sich als inländische juristische Person auf die Berufsfreiheit aus Art. 12 GG berufen.

Vgl. *Mann*, in: Sachs (Hrsg.), Grundgesetz, 9. Aufl. 2021, Art. 12 Rn. 37. 19

Die Berufsfreiheit schützt grundsätzlich nicht vor bloßen Veränderungen von Marktdaten und Rahmenbedingungen unternehmerischer Tätigkeit. Marktteilnehmer haben keinen grundrechtlichen Anspruch darauf, dass die Wettbewerbsbedingungen für sie gleich bleiben. Insbesondere gewährleistet das Grundrecht keinen Anspruch auf eine erfolgreiche Marktteilhabe oder künftige Erwerbsmöglichkeiten. Vielmehr unterliegen die Wettbewerbsposition und damit auch die erzielbaren Erträge dem Risiko laufender Veränderung je nach den Verhältnissen am Markt und damit nach Maßgabe seiner Funktionsbedingungen. Regelungen, die die Wettbewerbssituation der Unternehmen lediglich im Wege faktisch-mittelbarer Auswirkungen beeinflussen, berühren den Schutzbereich von Art. 12 Abs. 1 GG grundsätzlich nicht. Demgemäß ist nicht jedes staatliche Informationshandeln, das die Wettbewerbschancen von Unternehmen am Markt nachteilig verändert, ohne weiteres als Grundrechtseingriff zu bewerten. Eine staatliche Informationstätigkeit, die sich nachteilig auf die unternehmerische Wettbewerbsposition auswirken und den Markterfolg des Unternehmers behindern kann, stellt aber jedenfalls dann eine Beeinträchtigung des Grundrechts aus Art. 12 Abs. 1 GG dar, wenn sie in der Zielsetzung und ihren Wirkungen Ersatz für eine behördliche Maßnahme ist, die als Grundrechtseingriff zu qualifizieren wäre. Von einem solchen funktionalen Äquivalent ist jedenfalls dann auszugehen, wenn die Informationstätigkeit direkt auf die Marktbedingungen konkret individualisierter Unternehmen zielt, indem sie die Grundlagen der Entscheidungen am Markt zweckgerichtet beeinflusst und so die Markt- und Wettbewerbssituation zum wirtschaftlichen Nachteil der betroffenen Unternehmen verändert. 20

Vgl. zu alledem BVerfG Beschluss vom 21. März 2018 – 1 BvF 1/13 –, juris Rn. 27 f.; BVerwG, Urteil vom 20. November 2014 – 3 C 27.13 –, juris Rn. 14 jeweils m.w.N. 21

In Anwendung dieses Maßstabs stellt die Warnung vom 15. März 2022 ein funktionales Äquivalent zu einem Eingriff in die Berufsfreiheit der Antragstellerin dar. Sie ist ihrem Inhalt nach darauf gerichtet, die Öffentlichkeit vor Gefahren zu warnen, die aus Sicht des BSI mit der Nutzung der von der Antragstellerin vertriebenen Virenschutzsoftware verbunden sind und empfiehlt ausdrücklich, Virenschutzsoftware der Antragstellerin bzw. des Unternehmens L. durch andere Produkte zu ersetzen. Hierdurch wird der Antragstellerin das Agieren am Markt faktisch erschwert. Die mit der Warnung verbundene Veränderung der Marktbedingungen stellt keinen bloßen Reflex einer abstrakten Verbraucherinformation dar; vielmehr ist die Warnung gezielt darauf ausgerichtet, das Marktverhalten der Adressaten zu beeinflussen. 22

II. 23

Ist danach ein funktionales Äquivalent zu einem Eingriff in Art. 12 GG gegeben, hängt die Rechtmäßigkeit der Veröffentlichung der Warnung davon ab, dass die für Grundrechtseingriffe maßgeblichen rechtlichen Anforderungen erfüllt sind. 24

Vgl. BVerwG, Urteil vom 20. November 2014 – 3 C 27.13 –, juris Rn. 14 m.w.N. 25

26

Dies ist hier der Fall. Die Warnung ist auf eine gesetzliche Ermächtigungsgrundlage gestützt (dazu 1.). Beachtliche Verfahrensfehler liegen nicht vor (dazu 2.). Die Tatbestandsvoraussetzungen der Ermächtigungsgrundlage sind erfüllt (dazu 3.). Ermessensfehler sind nicht gegeben, insbesondere wahrt die Warnung den Verhältnismäßigkeitsgrundsatz (dazu 4.).

1. 27

Rechtsgrundlage für die streitgegenständliche Warnung ist § 7 Abs. 1 S. 1, Abs. 2 S. 1 BSIG. 28

Nach § 7 Abs. 1 S. 1 Nr. 1 Buchstabe a) BSIG kann das BSI zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 und 14a Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten an die Öffentlichkeit oder an die betroffenen Kreise richten und nach § 7 Abs. 1 S. 1 Nr. 2 BSIG Sicherheitsmaßnahmen sowie den Einsatz bestimmter Sicherheitsprodukte empfehlen. 29

Gemäß § 7 Abs. 2 S. 1 BSIG kann das BSI zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 und 14a die Öffentlichkeit unter Nennung der Bezeichnung und des Herstellers des betroffenen Produkts und Dienstes vor Sicherheitslücken in informationstechnischen Produkten und Diensten und vor Schadprogrammen warnen, wenn hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Sicherheit in der Informationstechnik hiervon ausgehen, oder Sicherheitsmaßnahmen sowie den Einsatz bestimmter informationstechnischer Produkte und Dienste empfehlen. 30

Darauf, ob im Fall einer Warnung vor einer Sicherheitslücke unter ausdrücklicher Nennung des Namens des Herstellers des betroffenen Produkts neben § 7 Abs. 2 S. 1 auch § 7 Abs. 1 S. 1 Nr. 1 Buchstabe a) einschlägig ist, 31

von ersterem wohl nicht ausgehend *Buchberger*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 7 BSIG Rn. 2; nach *Leisterer*/*Schneider*, K&R 2015, 681 (683, 688), ist das Verhältnis von Abs. 1 zu Abs. 2 unklar bzw. müssen die Voraussetzungen stets kumulativ vorliegen, 32

kommt es hier nicht an, da § 7 Abs. 1 S. 1 Nr. 1 Buchstabe a) BSIG keine Tatbestandsvoraussetzungen enthält, die über die des § 7 Abs. 2 S. 1 BSIG hinausgehen. 33

Ob die streitgegenständliche Warnung wie von der Antragsgegnerin geltend gemacht auch auf § 7 Abs. 1 S. 1 Nr. 1 Buchstabe d) BSIG gestützt werden könnte, der das BSI zur Veröffentlichung von Informationen über sicherheitsrelevante IT-Eigenschaften von Produkten ermächtigt, kann hier offen bleiben, da die Voraussetzungen von § 7 Abs. 1 S. 1 Nr. 1 Buchstabe a) bzw. Abs. 2 S. 1 BSIG für die Warnung vor einer Sicherheitslücke vorliegen (dazu unten). 34

2. 35

Zur Rechtswidrigkeit der Warnung führende Verfahrensfehler, auf die sich die Antragstellerin berufen kann, liegen nicht vor. 36

Nach § 7 Abs. 1a BSIG sind die Hersteller betroffener Produkte rechtzeitig vor Veröffentlichung der Warnungen zu informieren (Satz 1). Diese Informationspflicht besteht nicht, wenn hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks gefährdet wird oder wenn berechtigterweise davon ausgegangen werden kann, dass der Hersteller an einer vorherigen Benachrichtigung kein Interesse hat (Satz 2).Unabhängig von dem 37

Verständnis des Verhältnisses von § 7 Abs. 1 BSIG zu § 7 Abs. 2 BSIG besteht die in § 7 Abs. 1a BSIG normierte Informationspflicht auch für die in § 7 Abs. 2 BSIG ausdrücklich genannten Warnungen unter Nennung des Namens des Herstellers, da diese Warnungen gegenüber denjenigen ohne Bezug zu einem konkreten Hersteller erst recht einen Grundrechtseingriff darstellen.

Vgl. zu § 7 Abs. 1 S. 3 BSIG a.F.: *Buchberger*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 7 BSIG Rn. 8; *Leisterer*/*Schneider*, K&R 2015, 681 (683). 38

Bei der Feststellung der Reichweite der Informationspflicht in § 7 Abs. 1a S. 1 BSIG ist zu berücksichtigen, dass diese (auch) den Zweck verfolgt, den Herstellern vor Veröffentlichung einer Sicherheitslücke in Form einer technischen Schwachstelle Gelegenheit zu geben, diese durch technische Maßnahmen wie bspw. den Kunden zur Verfügung gestellte Sicherheits-Updates abzustellen (sog. Prinzip der verantwortungsvollen Weitergabe bzw. *responsible disclosure*). 39

Vgl. dazu Bundestags-Drucksache 16/13259, S. 7. 40

Die Antragsgegnerin ist von einer Informationspflicht nach § 7 Abs. 1a S. 1 BSIG ausgegangen und hat am 14. März 2022 ein an L. F. Headquarters in M1. sowie nachrichtlich an Herrn K. N. von der Antragstellerin („- Von der Darstellung des nachfolgenden Textes wird abgesehen –„) adressiertes Schreiben versandt. 41

Die Antragstellerin, die nach ihren eigenen Angaben auf der Grundlage eines Vertriebsvertrags mit der L. M. T. GmbH mit Sitz in A. Virenschutzsoftwareprodukte von L. in Deutschland vertreibt, ist jedoch schon nicht „Herstellerin“ im Sinne des § 7 Abs. 1a S. 1 BSIG. Auf eine Verletzung der Informationspflicht gegenüber dem Hersteller der Virenschutzsoftware kann sich die Antragstellerin nicht berufen, da sie dadurch nicht in eigenen Rechten verletzt wird. 42

Selbst wenn man eine Informationspflicht gegenüber der Antragstellerin annimmt, wäre ein Verstoß gegen diese Pflicht jedenfalls geheilt. 43

Dass das BSI die Antragstellerin im Sinne von § 7 Abs. 1a S. 1 BSIG rechtzeitig vor Veröffentlichung der Warnung informiert hat, erscheint zweifelhaft. Die Antragstellerin macht insofern geltend, die E-Mail habe sie nicht vor Veröffentlichung der Warnung erreicht. 44

Das BSI hat am Montag, den 14. März 2022 um 13:52 Uhr ein an L. F. Headquarters in M1. sowie nachrichtlich an Herrn K. N. von der Antragstellerin adressiertes Schreiben per E-Mail an die Adressen „info@L. .com“ und „L. .“Bezugsquelle wurde entfernt“ versandt, in dem es auf die beabsichtigte Veröffentlichung der Warnung am 15. März 2022, 9:00 Uhr hingewiesen und Gelegenheit zur Stellungnahme bis zum 14. März 2022, 17:00 Uhr gegeben hat. Die E-Mail enthielt als Anlage auch den Entwurf der Warnmeldung. 45

Die E-Mail Adresse „info@L. .com“ ist auf der Internetpräsenz von L. als allgemeine Kontaktadresse nicht nur für die F. Headquarters in M1. , sondern auch für die Headquarters Russia, Middle East, Turkey, Africa, Americas und Latin America angegeben, 46

vgl. https://www.L. .com/about/contact; zuletzt abgerufen am 31. März 2022, 47

so dass damit zu rechnen war, dass die Weiterleitung an die zuständige Person einige Zeit benötigen würde. Die allgemeine E-Mail Kontaktadresse der Antragstellerin ist auf der 48

deutschen Internetpräsenz von L. zudem nicht mit „info@L. .com“, sondern mit „info@L. .de“ angegeben.

Vgl. https://www.L. .de/legal; zuletzt abgerufen am 31. März 2022; dies ist auch die allgemeine Kontaktadresse der L. GmbH (auf der Internetpräsenz von L. aufgeführt unter „Headquarter Deutschland“) vgl. https://www.L. .de/about; zuletzt abgerufen am 31. März 2022. 49

Darüber hinaus war dem BSI die persönliche E-Mail Adresse des Herrn K. N. von der Antragstellerin bekannt, der das BSI ab dem 26. Februar 2022 mehrfach bezüglich einer Stellungnahme des BSI zur Sicherheit von L. per E-Mail („K. N. @L. .com“) kontaktiert hatte. Mit Blick auf die sehr kurze Stellungnahmefrist hätte es jedenfalls nahegelegen, das Informations- bzw. Anhörungsschreiben vom 14. März 2022 auch an diese dem BSI bekannte E-Mail Adresse von Herrn N. zu versenden und nicht nur an die Adresse „- Von der Darstellung des nachfolgenden Textes wird abgesehen –„ die Herr N. im November 2021 zur Einladung zu einem Online-Seminar genutzt hatte. 50

Ob aus der Verwendung dieser E-Mail-Adressen ein Verstoß gegen die Informationspflicht nach § 7 Abs. 1a S. 1 BSIG folgt, kann aber offen bleiben, weil ein solcher jedenfalls geheilt wäre. Die Heilungsvorschrift des § 45 Abs. 1 Nr. 3, Abs. 2 Verwaltungsverfahrensgesetz (VwVfG) ist auf einen Realakt in Form staatlichen Informationshandelns zwar nicht unmittelbar (vgl. § 9 VwVfG), jedoch dem Rechtsgedanken nach anwendbar. 51

Vgl. BVerfG, Nichtannahmebeschluss vom 6. Dezember 2002 – 1 BvR 1919/95 –, juris Rn. 27; BVerwG, Urteil vom 23. Mai 1989 – 7 C 2.87 –, juris Rn. 82; BayVGH, Beschluss vom 28. November 2019 – 20 CE 19.1995 –, juris Rn. 44 und Beschluss vom 14. Februar 2003 – 5 CE 02.3212 –, juris Rn. 34; VG Köln, Beschluss vom 22. März 2021 – 1 L 307/21 – n.v. 52

Demnach ist ein Anhörungs- bzw. Informationsmangel unbeachtlich, wenn die erforderliche Anhörung oder Information eines Beteiligten bis zum Abschluss der ersten Instanz eines verwaltungsgerichtlichen Verfahrens nachgeholt wird. Für den Fall der Anhörung ist höchstrichterlich entschieden, dass eine Heilung nach dieser Vorschrift voraussetzt, dass die Anhörung ordnungsgemäß durchgeführt und ihre Funktion für den Entscheidungsprozess der Behörde uneingeschränkt erreicht wird. Diese Funktion besteht nicht allein darin, dass der Betroffene seine Einwendungen vorbringen kann und diese von der Behörde zur Kenntnis genommen werden, sondern schließt vielmehr ein, dass die Behörde ein etwaiges Vorbringen bei ihrer Entscheidung in Erwägung zieht. 53

Vgl. BVerwG, Beschluss vom 17. August 2017 – 9 VR 2.17 –, juris, Rn. 10, sowie Urteile vom 17. Dezember 2015 – 7 C 5.14 –, juris, Rn. 17, vom 22. März 2012 – 3 C 16.11 –, juris, Rn. 18, und vom 24. Juni 2010 – 3 C 14.09 –, juris, Rn. 37; OVG NRW, Urteil vom 6. November 2018 – 5 A 470/17 –, n.v. 54

Hier ist von einer Heilung in diesem Sinne auszugehen. Kurz nach Veröffentlichung der Warnung hat das BSI in einem von der Antragstellerin initiierten Telefongespräch am 15. März 2022 erklärt, dass die Antragstellerin jederzeit eine Stellungnahme zusenden könne. Die Antragstellerin hat mit E-Mail an das BSI vom 15. März 2022 eine Stellungnahme mit weiteren Unterlagen vorgelegt, in der sie im Wesentlichen geltend gemacht hat, dass die Warnung nicht auf einer objektiven technischen Analyse der Risiken beim Einsatz von L. -Software beruhe und das Risiko staatlicher Eingriffe durch die russische Regierung mit Blick auf die von L. ergriffenen, von unabhängigen Organisationen zertifizierten Maßnahmen zur Gewährleistung der Transparenz und Sicherheit der Produkte deutlich geringer als bei 55

allen anderen Cybersicherheitsunternehmen der Welt sei. L. sei gesetzlich auch nicht verpflichtet, Informationen mit staatlichen Stellen in Russland zu teilen; dies werde durch eine unabhängige rechtliche Bewertung bestätigt. Das BSI hat sich nach interner Abstimmung mit am 17. März 2022 per E-Mail übersandtem Schreiben mit den in der Stellungnahme der Antragstellerin aufgeführten Argumenten auseinandergesetzt und erklärt, gleichwohl (derzeit) an der Warnung festzuhalten. Auch im Rahmen dieses Verfahrens auf Gewährung einstweiligen Rechtsschutzes hatte die Antragstellerin nochmals Gelegenheit, ihren Standpunkt zu vertreten. Die Antragsgegnerin hat nach Auseinandersetzung mit den Argumenten der Antragstellerin erneut erklärt, an der Warnung festzuhalten.

3. 56

Die Tatbestandsvoraussetzungen des § 7 Abs. 2 S. 1 BSIG sind gegeben. Das BSI erfüllt mit der streitgegenständlichen Warnung seine Aufgaben nach § 3 Abs. 1 S. 2 Nr. 14 und 14a BSIG (dazu a.), es liegen eine Sicherheitslücke im Sinne der Vorschrift (dazu b.) sowie hinreichende Anhaltspunkte dafür vor, dass hiervon Gefahren für die Sicherheit in der Informationstechnik ausgehen (dazu c.). 57

a. 58

Gemäß § 3 Abs. 1 S. 2 Nr. 14 BSIG ist Aufgabe des BSI die Beratung, Information und Warnung der Stellen des Bundes, der Länder sowie der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik, insbesondere unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen. 59

Zudem nimmt das BSI nach § 3 Abs. 1 S. 2 Nr. 14a BSIG die Aufgabe des Verbraucherschutzes und der Verbraucherinformation im Bereich der Sicherheit in der Informationstechnik wahr, insbesondere durch Beratung und Warnung von Verbrauchern in Fragen der Sicherheit in der Informationstechnik und unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen. 60

Die an die Öffentlichkeit bzw. Verbraucher gerichtete streitgegenständliche Warnung dient der Erfüllung dieser Aufgaben, da sie sich auf eine Frage der Sicherheit in der Informationstechnik bezieht. Soweit die Antragstellerin geltend macht, für fehlende oder unzureichende Sicherheitsvorkehrungen im Sinne der Vorschriften lägen bei ihr bzw. L. tatsächlich keine Anhaltspunkte vor, ist dies keine Frage der Aufgabenzuweisung nach § 3 Abs. 1 S. 2 Nr. 14 und 14a BSIG, sondern im Rahmen der einschlägigen Befugnisnorm zu prüfen. 61

b. 62

Es liegt auch eine Sicherheitslücke im Sinne von § 7 Abs. 1 und 2 BSIG vor. Nach § 2 Abs. 6 BSIG sind Sicherheitslücken im Sinne dieses Gesetzes Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können. 63

Der Begriff der Sicherheitslücke im Sinne des § 2 Abs. 6 BSIG ist grundsätzlich weit zu verstehen (dazu aa.). Virenschutzsoftware stellt aufgrund der ihr eingeräumten weitreichenden Berechtigungen zu Eingriffen in das jeweilige Computersystem jedenfalls dann eine Sicherheitslücke dar, wenn das erforderliche hohe Maß an Vertrauen in den 64

Hersteller nicht (mehr) gewährleistet ist (dazu bb.). Dies ist vorliegend der Fall, da die Möglichkeit einer Einflussnahme russischer Akteure auf die Virenschutzsoftware des russischen Herstellers L. nicht hinreichend sicher auszuschließen ist (dazu cc.).

aa. 65

Der Begriff der Sicherheitslücke ist weit zu verstehen. Der Gesetzeswortlaut ist nicht auf bestimmte Arten von Schadsoftware – Viren, Würmer, Trojaner – beschränkt, sondern stellt allein darauf ab, dass Eigenschaften von Programmen (aus)genutzt werden, um sich unbefugt („gegen den Willen des Berechtigten“) Zugang zu verschaffen oder Funktionen eines Systems zu beeinflussen. 66

Der Gesetzgeber wollte den Begriff der Sicherheitslücke bewusst weit verstanden wissen. In der Gesetzesbegründung heißt es: 67

„Sicherheitslücken sind hingegen unerwünschte Eigenschaften von informationstechnischen Systemen, insbesondere Computerprogrammen, die es Dritten erlauben, gegen den Willen des Berechtigten dessen Informationstechnik zu beeinflussen. Eine Beeinflussung muss nicht zwingend darin bestehen, dass sich der Angreifer Zugang zum System verschafft und dieses dann manipulieren kann. Es genügt auch, dass die Funktionsweise in sonstiger Weise beeinträchtigt werden kann, z.B. durch ein ungewolltes Abschalten. Der Begriff ist notwendigerweise weit gefasst, da Sicherheitslücken in den unterschiedlichsten Zusammenhängen, oftmals abhängig von der Konfiguration oder Einsatzumgebung, entstehen können.“ 68

Vgl. Bundestags-Drucksache 16/11967, S. 12. 69

Die weite Auslegung des Begriffs der Sicherheitslücke entspricht zudem auch dem Sinn und Zweck des § 7 Abs. 1 und 2 BSIG i.V.m. § 2 Abs. 6 BSIG. Dabei ist zu berücksichtigen, dass es sich bei den Warnungen vor Sicherheitslücken um Gefahrenabwehr handelt und sich die Einschätzung der Gefahrenlage sowie Art und Ausmaß der Bedrohungsszenarien im Bereich der IT-Sicherheit schnell ändern können, wie derzeit mit Blick auf die geopolitische Situation zu beobachten ist. Da die IT-Sicherheit durch ein komplexes und intransparentes Geflecht aus handelnden Regierungen, Nachrichtendiensten, Hackergruppen und Cyberkriminellen bedroht wird, ist es erforderlich, schnell und flexibel auf neu entstehende Gefahrenszenarien reagieren zu können. Dies wird durch ein weites Verständnis des Begriffs der Sicherheitslücke ermöglicht. 70

bb. 71

Dem derart weit verstandenen Begriff der Sicherheitslücke unterfällt Virenschutzsoftware aufgrund der ihr eingeräumten weitreichenden Berechtigungen zu Eingriffen in das jeweilige Computersystem jedenfalls dann, wenn das erforderliche hohe Maß an Vertrauen in den Hersteller nicht (mehr) gewährleistet ist. 72

Virenschutzprogramme weisen gegenüber anderer Software mehrere Besonderheiten auf. Entscheidend sind vor allem die weitreichenden (System-)Berechtigungen, die diesen Programmen eingeräumt sind. Diese ermöglichen einen Zugriff auf Teile des Systems, die dem normalen Benutzer und sogar mit Administratorrechten ausgeführten Programmen nicht ohne Weiteres zugänglich sind. Es kommt hinzu, dass Virenschutzprogramme ständig Programmupdates und Updates der Erkennungsmerkmale der zu detektierenden Schadsoftware durchführen und sich hierzu notwendigerweise regelmäßig mit Servern des 73

Herstellers verbinden müssen. Sie erfüllen damit dem weiten Wortlaut nach alle Voraussetzungen für das Vorliegen einer Sicherheitslücke im Sinne des § 2 Abs. 6 BSIG, da es sich um Programme handelt, die nach ihrer technischen Ausgestaltung grundsätzlich dazu geeignet sein können, Dritten unbefugten Zugang zu einem Computersystem zu ermöglichen.

Dass der Einsatz dieser Programme dennoch empfohlen wird, beruht letztlich allein auf einem hohen Maß an Vertrauen in die Kompetenz und Zuverlässigkeit des Herstellers und seines Entwicklungsteams sowie in die Integrität der Produktionsumgebung. Hierzu gehört zunächst das Vertrauen, dass weder der Hersteller selbst noch sein Entwicklungsteam die ihnen eingeräumten Befugnisse ausnutzen, und dass der Hersteller zudem ausreichende Vorkehrungen dagegen trifft, dass Dritte sein System ohne sein Wissen unbefugt nutzen können. Des Weiteren gehört hierzu aber auch das Vertrauen, dass der Hersteller keiner Einflussnahme durch Dritte, insbesondere auch keinem Druck oder Zwang, ausgesetzt sein wird. 74

Wird dieses Vertrauen erschüttert, können Virenschutzprogramme als Sicherheitslücke einzustufen sein. Auf ein Verschulden des Herstellers kommt es dabei nicht an. 75

cc. 76

Im Fall der Virenschutzsoftware von L. ist das dargestellte hohe Maß an Vertrauen in die Integrität der Software derzeit nicht mehr gegeben. Die Annahme der drohenden Einflussnahme russischer Akteure auf das Virenschutzprogramm von L. , von der das BSI bei seiner Warnung ausgegangen ist, ist vielmehr berechtigt. 77

Dabei ist zu berücksichtigen, dass das Unternehmen seinen Hauptsitz in N3. hat und dort nach den von der Antragsgegnerin vorgelegten Rechercheergebnissen einer Abfrage des Online-Karrierenetzwerks LinkedIn über 2.000 Mitarbeiter beschäftigt sind, darunter der Chief Technology Officer. Nach dem unwidersprochenen Vorbringen der Antragsgegnerin werden die zentralen operativen Voraussetzungen des IT-Dienstleistungsangebots von L. am Standort N3. erbracht. 78

Angesichts der geopolitischen Lage bzw. Russlands Angriff auf die Ukraine, der auch als „Cyberkrieg“ geführt wird, ist nicht auszuschließen, dass russische Entwicklerteams aus eigenem Antrieb oder unter dem Druck anderer russischer Akteure die technischen Möglichkeiten der Virenschutzprogramme ausnutzen, um Computersysteme in anderen Staaten zu korrumpieren. Es handelt sich dabei auch nicht nur um fernliegende Vermutungen, sondern um im Wirtschaftsleben bereits konkret in Betracht gezogene Bedrohungsszenarien. So wird innerhalb der Deutschen Cyber-Sicherheitsorganisation (DCSO) nach einem Vermerk des BSI allgemein damit gerechnet, dass Personen aus Russland unter Druck gesetzt oder Firmen von Spezialkräften durchsucht werden könnten; einige fürchteten sogar Enteignungen. Es seien daher umfangreiche IT-Sicherheitsmaßnahmen ergriffen worden. Auch die Deutsche Telekom scheint von einer drohenden Einflussnahme auf russische Mitarbeiter auszugehen und hat nach Presseberichten entschieden, ihre Software-Entwicklerstandorte in Russland zu schließen und russische Entwickler des Konzerns nur weiter zu beschäftigen, wenn sie das Land verlassen. 79

Vgl. etwa https://www.golem.de/news/ukrainekrieg-telekom-entlaesst-umzugsunwillige-entwickler-in-russland-2203-164243.html; https://www.handelsblatt.com/technik/it-internet/ukraine-krieg-deutsche-telekom-zieht-sich-nun-doch-aus-russland-zurueck/28197714.html; zuletzt abgerufen am 31. März 2022. 80

Dieses Bedrohungsszenario und der damit verbundene Vertrauensverlust kann derzeit von L. nicht in ausreichendem Umfang entkräftet werden. 81

Es erscheint zwar plausibel, dass es grundsätzlich im Unternehmensinteresse von L. liegt, jegliche Schadsoftware, auch solche von Staaten, zu enttarnen. 82

Vgl. den Beitrag von *Eva Wolfnagel* in Spektrum der Wissenschaft vom 17. März 2022, die dazu mit dem Direktor des Global Research and Analysis Team von L. gesprochen hat; abrufbar unter: https://www.spektrum.de/news/it-sicherheit-ist-L. -wirklich-ein-problem/2000236; zuletzt abgerufen am 31. März 2022. 83

Davon, dass das Unternehmen L. in der Lage wäre, seine Mitarbeiter vor Einflussnahme und Zwang staatlicher Stellen in Russland hinreichend zu schützen, ist aber nicht auszugehen. Angesichts des bekannten Verhaltens der russischen Regierung gegenüber Regimekritikern und Oppositionellen, das vor Gewaltanwendung nicht zurückschreckt, ist in der derzeitigen zugespitzten Situation nicht davon auszugehen, dass sich der IT-Sektor oder auch ein führendes IT-Unternehmen der Kontrolle durch die russische Regierung entziehen kann. Es ist vielmehr davon auszugehen, dass Unternehmen direktem Druck ausgesetzt werden, der Regierung benötigte Dienste zur Verfügung zu stellen und mit dem Staat zu kooperieren, auch wenn dies nicht mit Unternehmensinteressen vereinbar ist (so auch die Einschätzung des BSI in dem Vermerk zur Begründung der Warnung). 84

Auf das Vorbringen der Antragstellerin, es sei abwegig, dass sie dem Einfluss staatlicher Stellen in Russland ausgesetzt sei, da die russische L. -Gesellschaft zunächst Einfluss auf die britische Holding – L. Labs Limited UK mit Sitz in M1. , an der Eugene L. mit 82,98% beteiligt ist – nehmen müsste, deren 100%-ige Tochter die Antragstellerin ist, und die britische Holding dann wiederum Einfluss auf die Antragstellerin, kommt es nicht an. Denn das BSI warnt nicht vor der Antragstellerin, sondern der Virenschutzsoftware von L. . Im Übrigen hilft die geltend gemachte gesellschaftsrechtliche Ausgestaltung auch nicht darüber hinweg, dass Entwickler bzw. Programmierer der Software in Russland ansässig und damit der Einflussnahme des russischen Staates ausgesetzt sind. 85

Soweit die Antragstellerin unter Verweis auf ein Gutachten von L2. I. (Universität Uppsala, Schweden) vom 31. Januar 2019 geltend macht, L. unterfalle nicht bestimmten russischen Gesetzen, die in Russland operierende Unternehmen zur Weitergabe von Informationen an staatliche Stellen bzw. den russischen Geheimdienst verpflichten, führt dies zu keiner anderen Bewertung. Zum einen ist insbesondere angesichts des völkerrechtswidrigen Angriffskriegs auf die Ukraine nicht gesichert, dass staatliche Stellen in Russland sich in rechtstaatlicher Weise an die Vorgaben dieser Gesetze halten; zum anderen ist auch eine schnelle Schaffung entsprechender Rechtsgrundlagen denkbar wie etwa hinsichtlich der kürzlich erfolgten massiven Beschränkung der Pressefreiheit in Russland. 86

Vgl. dazu etwa https://www.tagesschau.de/ausland/europa/russland-gesetz-fakenews-strafen-103.html; zuletzt abgerufen am 31. März 2022. 87

Auch wirtschaftliche Interessen bieten keine Gewähr dafür, dass es nicht zu einer Einflussnahme staatlicher Stellen in Russland auf L. kommt. Die Antragsgegnerin hat insoweit überzeugend ausgeführt, dass die Hinnahme angedrohter Sanktionen gezeigt hat, dass die russische Regierung zur Erreichung ihrer (geopolitischen) Ziele bereit ist, wirtschaftliche Verluste russischer Unternehmen hinzunehmen. 88

89

Die von der Antragstellerin angeführte *Information Security Policy* von L. , die alle Mitarbeiter durch die Unterzeichnung einer Vertraulichkeits- und Geheimhaltungsvereinbarung (*Non Disclosure Agreement*) akzeptieren müssten, führt ebenfalls nicht zu einer anderen Bewertung. Die darin vorgesehenen Schutzmechanismen wie die Auffächerung von Befugnissen und Kontrollen zwischen einzelnen Betriebseinheiten, Regeln zum Umgang mit Passwörtern und die Beschränkung von Zugriffsrechten auf das Informationssystem des Unternehmens sind zwar bei der Bewertung der Zuverlässigkeit eines Herstellers zu berücksichtigen. Die unternehmensinternen Vorgaben und Standards können aber nicht isoliert davon betrachtet werden, in welchem Umfeld das Unternehmen agiert bzw. inwieweit rechtstaatliche Garantien eine schädigende Einflussnahme staatlicher Stellen ausschließen. Die unternehmensinternen Vorgaben und Standards verlieren mit anderen Worten an Wert, wenn der Hersteller – wie L. – in einem Staat ansässig ist, in dem eine Einflussnahme staatlicher Stellen auf das Unternehmen droht, die seine Mitarbeiter dazu zwingt, gegen die unternehmensinternen Standards zu verstoßen. Aus diesem Grund bietet auch die regelmäßige Zertifizierung der unternehmensinternen Sicherheitsprozesse durch unabhängige Institutionen keine Gewähr dafür, dass die Virenschutzsoftware von L. nicht für Cyberangriffe missbraucht werden kann.

Gleiches gilt für die von der Antragstellerin angeführte sog. Transparenzinitiative von L. , 90
in deren Rahmen das Unternehmen die Speicherung und Verarbeitung von Daten u.a. europäischer Nutzer auf Server in der Schweiz verlagert hat und die die Möglichkeit bietet, den Quellcode, Updates und die Softwarearchitektur einzusehen. Allein die vom Head of Information Security and Compliance Europe von L. eidesstattlich versicherte Beteiligung von Teams außerhalb Russlands (etwa in den USA und Europa) an der Erstellung von Updates garantiert nicht, dass russische Stellen über in Russland ansässige Programmierer keinen Einfluss nehmen können. Gleiches gilt, soweit dieser versichert, alle nicht autorisierten Zugriffsversuche würden nachvollzogen, da dies einen Angriff nicht präventiv verhindert. Das BSI hat in der im gerichtlichen Verfahren vorgelegten sachverständigen Erklärung überzeugend ausgeführt, dass die von L. angeführten Maßnahmen keinen ausreichenden Schutz vor möglichen Angriffen von außen bzw. durch staatliche Stellen in Russland bieten, da die großen zu verarbeitenden Datenmengen, der komplexe Programmcode, die erforderlichen häufigen Updates, die vielfältigen Angriffsmöglichkeiten und der geringe Aufwand für erfolgreiche Angriffe auf Virenschutzsoftware eine Qualitätssicherung durch Kunden oder externe Experten – die permanent erfolgen müsste – praktisch unmöglich mache. Es sei zudem nicht plausibel, dass ein Rechenzentrum in Westeuropa vollständig ohne Personal, Daten oder Softwarekomponenten aus dem Hauptquartier in Russland arbeitsfähig sei. Ein Fernzugriff über das Internet, das Einspielen von Softwarekomponenten oder Datenbanken, die in Russland erstellt oder durch russische Stellen beeinflusst würden sowie Aktionen durch einen Innentäter, der direkt oder indirekt über Zugriff auf IT-Systeme des Rechenzentrums verfügt, wären nicht oder nur nach langwieriger forensischer Analyse im Nachhinein nachweisbar.

Experten außerhalb des BSI weisen im Zusammenhang mit dem Fall L. zudem darauf 91
hin, dass es sehr unwahrscheinlich sei, eingebaute Hintertüren (*backdoors*), in IT-Produkten zu finden, die dazu genutzt werden könnten, ein System über das Internet komplett zu steuern oder beliebige Daten abzugreifen. Dies gelte selbst bei vollem Zugriff auf den Quellcode. Antivirensoftware benötige zudem noch nicht einmal eine Hintertür, um den Nutzer auszuspionieren, da sie ohnehin vollen Zugriff auf das überwachte System habe. Wer Antivirensoftware kontrolliere, könne sehr einfach dafür sorgen, dass bestimmte Schadprogramme nicht erkannt werden. Die Vertrauenswürdigkeit eines IT-Produkts hänge damit nicht nur von dessen technischer Qualität ab, sondern auch davon, ob der Hersteller

Druck durch staatliche Stellen ausgesetzt ist bzw. für Cyberangriffe missbraucht werden kann.

Vgl. *Haya Shulman*, Professorin für Informatik an der Goethe-Universität Frankfurt am Main, Kolumne im Tagesspiegel vom 24. März 2022, abrufbar unter:https://background.tagesspiegel.de/cybersecurity/digitale-souveraenitaet-und-der-fall- L. ; zuletzt abgerufen am 31. März 2022. 92

c. 93

Es liegen auch hinreichende Anhaltspunkte dafür vor, dass von der Sicherheitslücke Gefahren für die Sicherheit in der Informationstechnik ausgehen. Bei der Beurteilung, wie konkret und sicher die Anhaltspunkte sein müssen, ist maßgeblich zu berücksichtigen, welcher Schaden für die IT-Sicherheit droht. Je weitgehender und existenzieller der drohende Schaden ist, umso geringere Anforderungen sind an das Vorliegen hinreichender Anhaltspunkte zu stellen. Nach diesem Maßstab ist zu berücksichtigen, dass eine Manipulation von Virenschutzsoftware es wegen des vollen Zugriffs der Software auf das überwachte System und der ständigen Aktualisierung erlaubt, mit relativ wenig Einsatz großen Schaden für die IT-Sicherheit anzurichten. 94

Klarzustellen ist zudem, dass Maßstab der Prüfung an dieser Stelle nicht diejenigen Gefahren sind, die bereits im Rahmen der Frage, ob eine Sicherheitslücke vorliegt, zu prüfen waren. Die Frage einer drohenden Einflussnahme Russlands stellt sich mit anderen Worten schon im Rahmen der Prüfung, ob eine Sicherheitslücke vorliegt und entgegen der Annahme der Antragstellerin nicht erst bei der Prüfung, ob hinreichende Anhaltspunkte für eine von der Sicherheitslücke ausgehende Gefahr für die Sicherheit in der Informationstechnik gegeben sind. 95

Die Frage, ob es hinreichende Anhaltspunkte dafür gibt, dass von der im oben genannten Sinne verstandenen Sicherheitslücke Gefahren für die Sicherheit in der Informationstechnik ausgehen, zielt darauf ab, ob ein Ausnutzen der Sicherheitslücke durch tatsächliche Cyberangriffe Russlands zu einer Gefahr für die Sicherheit in der Informationstechnik in Deutschland führt. Davon ist aufgrund hinreichender Anhaltspunkte auszugehen. Insbesondere mit Blick auf die Sanktionen westlicher Staaten ist es wahrscheinlich, dass auch Ziele in Deutschland von aus Russland geführten Cyberangriffen bedroht sind, zumal Experten Deutschland im Vergleich zu anderen westlichen Staaten für ein besonders verwundbares Ziel halten. Nach inzwischen allgemein über Presseberichte verbreiteten Informationen könnte es alsbald zu einer verschärften Lage hinsichtlich Cyberangriffen auf deutsche (Hochwert-) Ziele kommen 96

Vgl. dazu https://www.tagesschau.de/investigativ/swr/cyberkrieg-ukraine-putin-101.html; https://www.spiegel.de/netzwelt/warnung-der-bundesregierung-cyberangriff-auf-deutsche-hochwertziele-koennte-schon-bald-starten-a-3d80a9a1-7558-4fd4-873b-070fd6ceec0f; zuletzt abgerufen am 31. März 2022. 97

Es ist zudem davon auszugehen, dass von russischen Stellen initiierte Cyberangriffe staatliche Stellen in Deutschland und kritische Infrastruktur in den Fokus nehmen würden, die zu (Kollateral-) Schäden für weite Teile der Bevölkerung führen können. 98

Da damit auch hinreichende Anhaltspunkte für eine von der Sicherheitslücke ausgehende Gefahr für die Sicherheit in der Informationstechnik vorliegen, kommt es auf den von der Antragstellerin angeführten Vergleich mit § 40 Abs. 1a Lebensmittel- und 99

Futtermittelgesetzbuch (LFGB) nicht an. Dies gilt unabhängig von der Frage, wie zielführend dieser Vergleich mit Blick auf die in § 40 Abs. 1 und 1a LFGB genutzte uneinheitliche Terminologie („hinreichender Verdacht“, „hinreichend begründeter Verdacht“, „durch Tatsachen hinreichend begründeter Verdacht“) überhaupt sein könnte.

4. 100

Dass die Antragsgegnerin das ihr durch § 7 Abs. 2 S. 1, Abs. 1 S. 1 Nr. 1 Buchstabe a) BSIG eingeräumte Ermessen falsch ausgeübt hat, ist nicht ersichtlich. 101

Soweit die Antragstellerin geltend macht, es liege ein Ermessensmissbrauch vor, weil es sich bei der Warnung um eine rein politische Entscheidung handle, ist dem entgegenzuhalten, dass nach den obigen Ausführungen die Tatbestandsvoraussetzung der „Sicherheitslücke“ im Sinne von § 7 Abs. 1 und 2 BSIG i.V.m. § 2 Abs. 6 BSIG auch dann gegeben ist, wenn wie hier keine technischen Fehler eines Programms Anlass für die Warnung sind, sondern eine drohende Einflussnahme eines ausländischen Staates auf den Hersteller. Die Einschätzung der Gefahr einer Einflussnahme auf den Hersteller kann nicht unabhängig von der geopolitischen Situation getroffen werden. Bei der Entscheidung, die Gefahr einer Einflussnahme des russischen Staates auf L. nach dem Angriffskrieg Russlands auf die Ukraine neu zu bewerten, handelt das BSI demnach im Rahmen seiner ihm durch das BSIG eingeräumten Kompetenzen. Inwiefern die Berücksichtigung dieser politischen Veränderung einen Ermessensmissbrauch darstellen sollte, ist vor diesem Hintergrund nicht ersichtlich. 102

Ermessenfehler sind auch im Übrigen nicht ersichtlich, insbesondere verstößt die Warnung nicht gegen den Grundsatz der Verhältnismäßigkeit. 103

Die Warnung ist geeignet und erforderlich, um der drohenden Gefahr von Cyberangriffen Russlands durch einen Missbrauch der Virenschutzsoftware von L. zu begegnen. Soweit die Antragstellerin geltend macht, andere europäische Staaten hätten nicht vor der Virenschutzsoftware von L. gewarnt, ist dem entgegen zu halten, dass die Cybersicherheitsbehörde in Frankreich am 15. März 2022 jedenfalls erklärt hat, im aktuellen Kontext könne die Nutzung bestimmter digitaler Tools, insbesondere der Tools der Firma L. , aufgrund ihrer Verbindung zu Russland in Frage gestellt werden. 104

Vgl. https://cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-001/; zuletzt abgerufen am 31. März 2022. 105

Nach den von den Prozessbevollmächtigten der Antragsgegnerin in ihrem Schriftsatz vom 28. März 2022 zitierten Presseberichten arbeitet Italien daran, Software von L. aus der öffentlichen Verwaltung zu entfernen. Die USA, Großbritannien, die Niederlande und Litauen haben den Einsatz von Virenschutzsoftware von L. in Behörden bereits 2017 bzw. 2018 verboten oder davor gewarnt; in Litauen gilt das Verbot auch für Unternehmen der kritischen Infrastruktur. 106

Vgl. zum Verbot in Litauen https://www.heise.de/security/meldung/Litauische-Behoerden-setzen-Nutzung-von-L. -Software-aus-3952578.html; zuletzt abgerufen am 31. März 2022. 107

Ebenfalls bereits 2018 hat das Europäische Parlament die EU dazu aufgefordert, die Verwendung „bestätigt böswilliger“ Programme und Geräte wie L. N1. . in ihren eigenen Institutionen und Organen zu verbieten. 108

109

„*The F. Parliament [c]alls on the EU to perform a comprehensive review of software, IT and communications equipment and infrastructure used in the institutions in order to exclude potentially dangerous programmes and devices, and to ban the ones that have been confirmed as malicious, such as L. N1. . .*“

Vgl. Report on Cyber Defense vom 25. Mai 2018, Ziffer 76; abrufbar unter: https://www.europarl.europa.eu/doceo/document/A-8-2018-0189_EN.html?redirect; zuletzt abgerufen am 31. März 2022. 110

Daraufhin hat auch die ungarische Regierung Behörden und Unternehmen in Staatsbesitz angewiesen, die Virenschutzsoftware von L. nicht mehr zu nutzen. 111

Vgl. https://www.handelsblatt.com/politik/international/virenschutz-ungarns-regierung-verbannt-L. -software-aus-behoerden/22913120.html; zuletzt abgerufen am 31. März 2022. 112

Im Übrigen ist zu berücksichtigen, dass die Frage, ob eine Warnung erforderlich ist, nicht losgelöst von der jeweiligen Cybersicherheitslage in dem betreffenden Staat getroffen werden kann, so dass Vergleiche mit anderen Staaten ohnehin nur eine begrenzte Aussagekraft haben. 113

Soweit die Antragstellerin vorbringt, die mit der Warnung ausgesprochene Empfehlung, Virenschutzsoftware von L. durch andere Produkte zu ersetzen, sei nicht erforderlich, ist dem entgegenzuhalten, dass diese Empfehlung verhindert, dass Nutzer (auch nur kurzfristig) komplett ohne Virenschutz sind; dies würde ebenfalls eine Bedrohung der Cybersicherheit darstellen. 114

Die Warnung ist auch verhältnismäßig im engeren Sinne. Wie sich dem in den beigezogenen Verwaltungsvorgängen befindlichen Vermerk zur Begründung der Warnung vom 14. März 2022 entnehmen lässt, hat das BSI sich bereits vor Veröffentlichung der Warnung mit den von L. angeführten Maßnahmen zur Vertrauensbildung (Serververlagerung in die Schweiz, Zertifizierung durch unabhängige Prüforganisationen) und der Angabe von L. , nicht bestimmten russischen Gesetzen unterworfen zu sein, die Unternehmen zur Weitergabe von Informationen an staatliche Stellen verpflichten, auseinandergesetzt und auch die Interessen von L. in die Ermessensentscheidung einbezogen. Das BSI ist insoweit ermessensfehlerfrei zu dem Ergebnis gelangt, dass die Warnmeldung mit hoher Wahrscheinlichkeit zwar spürbare Folgen für die wirtschaftliche Tätigkeit von L. in Deutschland hätte, allerdings überwiege der Schutz der Allgemeinheit aufgrund der besonderen Schwere des Schadensrisikos das Interesse des einzelnen Herstellers. Diese Einschätzung ist mit Blick darauf, dass russische Cyberangriffe staatliche Stellen und kritische Infrastruktur in Deutschland im Fokus haben dürften, rechtlich nicht zu beanstanden. 115

Das BSI hat mit der Formulierung der Warnung nach Auffassung der Kammer zudem noch hinreichend deutlich zum Ausdruck gebracht, dass Anlass für die Warnung nicht eine neu bekannt gewordene technische Schwachstelle bzw. die technische Qualität der Virenschutzsoftware von L. ist, sondern die drohende Einflussnahme des russischen Staates auf den Hersteller. Die Formulierung, „ein russischer IT-Hersteller kann selbst offensive Operationen durchführen“ erscheint zwar mit Blick darauf, dass für einen eigeninitiativ, d.h. ohne Einflussnahme staatlicher Stellen von L. ausgeführten Cyberangriff keine konkreten Anhaltspunkte vorliegen dürften, sehr weitgehend, ist aber angesichts der Intention des BSI, an dieser Stelle sämtliche theoretisch denkbaren Angriffsszenarien zu verdeutlichen, noch vertretbar. 116

Die Warnung spiegelt schließlich auch die unterschiedliche Gefährdung von staatlichen Stellen und kritischer Infrastruktur auf der einen und Privatanwendern auf der anderen Seite wider, indem sie darauf hinweist, dass Privatanwender ohne wichtige Funktion in Staat, Wirtschaft und Gesellschaft möglicherweise am wenigsten im Fokus stehen, aber im Falle eines erfolgreichen Angriffs auch Opfer von Kollateralauswirkungen werden können. 117

Da die Warnung insgesamt rechtmäßig ist, hat die Antragstellerin unabhängig von der Frage, ob ein solcher auf § 7 Abs. 2 S. 2 BSIG oder den allgemeinen öffentlich-rechtlichen Folgenbeseitigungsanspruch gestützt werden könnte, auch keinen Anspruch auf den Widerruf der Warnung bzw. die hilfsweise beantragte Archivierung der Warnung nach spätestens einem Monat. 118

Die Kostenentscheidung beruht auf § 154 Abs. 1 VwGO. 119

Die Festsetzung des Streitwerts beruht auf §§ 53 Abs. 2 Nr. 1, 52 Abs. 1 Gerichtskostengesetz (GKG). Sie entspricht der Bedeutung der Sache für die Antragstellerin. Eine Reduzierung des Streitwerts in diesem Verfahren des vorläufigen Rechtschutzes erscheint wegen der beantragten Vorwegnahme der Hauptsache nicht angemessen. 120

Rechtsmittelbelehrung 121

Gegen Ziffer 1 dieses Beschlusses kann innerhalb von zwei Wochen nach Bekanntgabe schriftlich bei dem Verwaltungsgericht Köln, Appellhofplatz, 50667 Köln, Beschwerde eingelegt werden. 122

Die Beschwerdefrist wird auch gewahrt, wenn die Beschwerde innerhalb der Frist schriftlich bei dem Oberverwaltungsgericht für das Land Nordrhein-Westfalen, Aegidiikirchplatz 5, 48143 Münster, eingeht. 123

Die Beschwerde ist innerhalb eines Monats nach Bekanntgabe der Entscheidung zu begründen. Die Begründung ist, sofern sie nicht bereits mit der Beschwerde vorgelegt worden ist, bei dem Oberverwaltungsgericht schriftlich einzureichen. Sie muss einen bestimmten Antrag enthalten, die Gründe darlegen, aus denen die Entscheidung abzuändern oder aufzuheben ist und sich mit der angefochtenen Entscheidung auseinander setzen. 124

Auf die ab dem 1. Januar 2022 unter anderem für Rechtsanwälte, Behörden und juristische Personen des öffentlichen Rechts geltende Pflicht zur Übermittlung von Schriftstücken als elektronisches Dokument nach Maßgabe der §§ 55a, 55d Verwaltungsgerichtsordnung – VwGO – und der Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (Elektronischer-Rechtsverkehr-Verordnung – ERVV) wird hingewiesen. 125

Im Beschwerdeverfahren müssen sich die Beteiligten durch Prozessbevollmächtigte vertreten lassen; dies gilt auch für die Einlegung der Beschwerde und für die Begründung. Als Prozessbevollmächtigte sind Rechtsanwälte oder Rechtslehrer an einer staatlichen oder staatlich anerkannten Hochschule eines Mitgliedstaates der Europäischen Union, eines anderen Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum oder der Schweiz, die die Befähigung zum Richteramt besitzen, für Behörden und juristische Personen des öffentlichen Rechts auch eigene Beschäftigte oder Beschäftigte anderer Behörden oder juristischer Personen des öffentlichen Rechts mit Befähigung zum Richteramt zugelassen. Darüber hinaus sind die in § 67 Abs. 4 der Verwaltungsgerichtsordnung im Übrigen bezeichneten ihnen kraft Gesetzes gleichgestellten Personen zugelassen. 126

Gegen Ziffer 2 dieses Beschlusses kann innerhalb von sechs Monaten, nachdem die Entscheidung in der Hauptsache Rechtskraft erlangt oder das Verfahren sich anderweitig erledigt hat, Beschwerde eingelegt werden. Ist der Streitwert später als einen Monat vor Ablauf dieser Frist festgesetzt worden, so kann sie noch innerhalb eines Monats nach Zustellung oder formloser Mitteilung des Festsetzungsbeschlusses eingelegt werden. 127

Die Beschwerde ist schriftlich oder zu Protokoll des Urkundsbeamten der Geschäftsstelle bei dem Verwaltungsgericht Köln, Appellhofplatz, 50667 Köln, einzulegen. 128

Die Beschwerde ist nur zulässig, wenn der Wert des Beschwerdegegenstandes 200 Euro übersteigt. 129

Die Beschwerdeschrift sollte zweifach eingereicht werden. Im Fall der Einreichung eines elektronischen Dokuments bedarf es keiner Abschriften. 130
