Oberverwaltungsgericht NRW, 4 B 473/22

Datum:	28.04.2022
Gericht:	Oberverwaltungsgericht NRW
Spruchkörper:	4. Senat
Entscheidungsart:	Beschluss
Aktenzeichen:	4 B 473/22
ECLI:	ECLI:DE:OVGNRW:2022:0428.4B473.22.00

Vorinstanz:	Verwaltungsgericht Köln, 1 L 466/22
Schlagworte:	Informationshandeln Warnung Empfehlung Information Amtliche Äußerung Willkürverbot Verhältnismäßigkeit Sachlichkeitsgebot Neutralitätsgebot Grundrechtsbindung Hinreichende Anhaltspunkte Sicherheit in der Informationstechnik Sicherheitslücke Sicherheitsstandards Sicherheitsvorkehrungen Virenschutzprogramm Virenschutzsoftware Cyberangriff Cybersicherheitslage
Normen:	BSIG § 2 Abs. 2 Satz 4; BSIG § 2 Abs. 6; BSIG § 3 Abs. 1 Satz 2 Nr. 14; BSIG § 3 Abs. 1 Satz 2 Nr. 14a; BSIG § 7 Abs. 1 Satz 1 Nr. 1 Buchst. a);; BSIG § 7 Abs. 1 Satz 1 Nr. 2; BSIG § 7 Abs. 2 Satz 1; GG Art. 12 Abs. 1

Leitsätze:

Unabhängig davon, inwieweit staatliches Informationshandeln einfachgesetzlicher Normierung zugänglich ist, besteht eine Grundrechtsbindung aus Art. 12 Abs. 1 GG, wenn solches Handeln zwar die Berufstätigkeit nicht unmittelbar berührt, aber Rahmenbedingungen der Berufsausübung verändert und in Zielsetzung und mittelbar-faktischen Wirkungen einem Grundrechtseingriff als funktionales Äquivalent gleichkommt.

2.
Die Grundrechtsbindung hindert staatliche Stellen nicht daran, sich überhaupt zu grundrechtlich geschützten Bereichen – auch kritisch – zu äußern. Grundrechte schützen nicht vor der Verbreitung von inhaltlich zutreffenden und unter Beachtung des Gebots der Sachlichkeit sowie mit

angemessener Zurückhaltung formulierten Informationen durch einen Träger der Staatsgewalt.

3.
Angesichts der Vielgestaltigkeit möglicher Risiken für die Sicherheit in der Informationstechnik ist es verfassungsrechtlich unbedenklich, dass der Gesetzgeber den Begriff der Sicherheitslücke im Sinne des § 2 Abs. 6 BSIG gerade als Tatbestandsvoraussetzung für eine amtliche Warnung weit gefasst hat, um bislang unvorhersehbare Fallgestaltungen abzudecken.

4.
Liegen hinreichende Anhaltspunkte dafür vor, dass die Sicherheitsstandards insbesondere zum Schutz der Verfügbarkeit, Integrität und Vertraulichkeit von Informationen (§ 2 Abs. 2 Satz 4 BSIG) nicht mehr gewährleistet werden können, sind zugleich hinreichende Anhaltspunkte dafür gegeben, dass von dem betroffenen Programm oder informationstechnischen System eine Gefahr für die Sicherheit in der Informationstechnik ausgeht.

5.
Ob hinreichende Anhaltspunkte dafür vorliegen, dass von einem Produkt aufgrund einer Sicherheitslücke Gefahren für die Sicherheit in der Informationstechnik ausgehen, ist anhand aller mit vernünftigem Aufwand feststellbaren Umstände oder Ereignisse zu beurteilen, die nachteilige Auswirkungen auf die Sicherheit von Informationssystemen haben können. Mit Blick auf das mit dem BSIG verfolgte Ziel der umfassenden Gewährleistung der Sicherheit der Informationstechnik sind sowohl technische Kriterien als auch staatliche Sicherheitsinformationen einzubeziehen.

Tenor:

Die Beschwerde der Antragstellerin gegen die Versagung vorläufigen Rechtsschutzes durch den Beschluss des Verwaltungsgerichts Köln vom 1.4.2022 wird zurückgewiesen.

Die Antragstellerin trägt die Kosten des Beschwerdeverfahrens.

Der Streitwert wird auch für das Beschwerdeverfahren auf 100.000,00 Euro festgesetzt.

Gründe:

I. 1

Die Antragstellerin, eine 100%ige Tochter der L. Labs Limited, London, vertreibt auf der Grundlage eines Vertriebsvertrags mit ihrer Schwestergesellschaft in der Schweiz die Virenschutzsoftware von L. in Deutschland. Sie wendet sich gegen die behördliche Warnung des Bundesamts für Sicherheit in der Informationstechnik – Bundesamt – vom 15.3.2022, die folgenden Wortlaut hat: 2

„**BSI-Warnung gemäß BSIG § 7** 3

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht die vorliegende Warnung im Rahmen seines gesetzlichen Auftrags […]. 4

Virenschutzsoftware des Herstellers L. 5

Risikostufe […]: 4 - hoch 6

1 Sachverhalt 7

Virenschutzsoftware, einschließlich der damit verbundenen echtzeitfähigen Clouddienste, ist essentiell zum Schutz von IT-Systemen. Wenn Zweifel an der Zuverlässigkeit des Herstellers bestehen, birgt aber gerade Virenschutzsoftware ein besonderes Risiko für eine zu schützende IT-Infrastruktur. Um einen aktuellen und wirksamen Schutz vor Schadsoftware zu gewährleisten, verfügt sie über weitreichende Systemberechtigungen und muss systembedingt (zumindest für Aktualisierungen) eine dauerhafte, verschlüsselte und nicht prüfbare Verbindung zu Servern des Herstellers unterhalten. Daher ist Vertrauen in die Zuverlässigkeit und den Eigenschutz eines Herstellers sowie seiner authentischen Handlungsfähigkeit entscheidend für den sicheren Einsatz solcher Systeme. Virenschutzsoftware ist ein exponiertes Ziel von offensiven Operationen im Cyberraum, um potentielle Gegner auszuspionieren, die Integrität ihrer Systeme zu beeinträchtigen oder sogar die Verfügbarkeit der darauf gespeicherten Daten vollständig einzuschränken. 8

Das Vorgehen militärischer und/oder nachrichtendienstlicher Kräfte in Russland sowie die im Zuge des aktuellen kriegerischen Konflikts jüngst von russischer Seite ausgesprochenen Drohungen gegen die EU, die NATO und die Bundesrepublik Deutschland sind mit einem erheblichen Risiko eines erfolgreichen IT-Angriffs mit weitreichenden Konsequenzen verbunden. 9

Ein russischer IT-Hersteller kann selbst offensive Operationen durchführen, gegen seinen eigenen Willen gezwungen werden, Zielsysteme anzugreifen, oder selbst als Opfer einer Cyber-Operation ohne seine Kenntnis ausspioniert oder als Werkzeug für Angriffe gegen seine eigenen Kunden missbraucht werden. 10

2 Auswirkung 11

Durch Manipulationen an der Software oder den Zugriff auf bei L. gespeicherte Daten können Aufklärungs- oder Sabotageaktionen gegen Deutschland, einzelne Personen oder bestimmte Unternehmen oder Organisationen durchgeführt oder zumindest unterstützt 12

werden.

Alle Anwender und Nutzerinnen der Virenschutzsoftware können je nach Ihrer strategischen Bedeutung von einer schädigenden Operation betroffen sein. Abgestuft ist damit zu rechnen, dass Einrichtungen des Staates, der Kritischen Infrastrukturen, der Unternehmen im besonderen öffentlichen Interesse, des produzierenden Gewerbes sowie wichtiger gesellschaftlicher Bereiche betroffen sein können. Privatanwender ohne wichtige Funktion in Staat, Wirtschaft und Gesellschaft stehen möglicherweise am Wenigsten im Fokus, können aber in einem erfolgreichen Angriffsfall auch Opfer von Kollateralauswirkungen werden. 13

3 Betroffene Produkte 14

Betroffen ist das Portfolio von Virenschutzsoftware des Unternehmens L. . 15

4 Handlungsempfehlung 16

Virenschutzsoftware des Unternehmens L. sollte durch alternative Produkte ersetzt werden. 17

Unternehmen und Behörden mit besonderen Sicherheitsinteressen/Rahmenbedingungen und Einrichtungen Kritischer Infrastrukturen sind in besonderem Maß gefährdet. Sie haben die Möglichkeit, sich von den zuständigen Verfassungsschutzbehörden bzw. vom BSI beraten zu lassen. 18

Allgemeiner Hinweis: Der Wechsel wesentlicher Bestandteile einer IT-Sicherheitsinfrastruktur muss im Enterprise-Bereich immer sorgfältig geplant und durchgeführt werden. Würden IT-Sicherheitsprodukte (also insbesondere Virenschutzsoftware) ohne Vorbereitung abgeschaltet, wäre man Angriffen aus dem Internet möglicherweise schutzlos ausgeliefert. Der notfallmäßige Umstieg auf andere Produkte ist auf jeden Fall mit vorübergehenden Komfort-, Funktions- und Sicherheitseinbußen verbunden. 19

Das BSI empfiehlt daher in jedem Fall eine individuelle Bewertung und Abwägung der aktuellen Situation sowie in einem erforderlichen Migrationsfall, Experten zur Umsetzungsplanung und -durchführung hinzuzuziehen.“ 20

Das Bundesamt hat die Warnung in einem internen Vermerk im Wesentlichen damit begründet, es lägen seit dem russischen Angriff auf die Ukraine, der von der UNO-Vollversammlung mit großer Mehrheit scharf verurteilt worden sei, hinreichende Anhaltspunkte dafür vor, dass Gefahren für die Sicherheit in der Informationstechnik von der Virenschutzsoftware der Firma L. ausgingen. Sicherheitseigenschaften von Produkten könnten sich auch aus der Struktur des Anbieters ergeben. Um die gewollte Funktionalität bieten zu können, liefen Virenschutzprogramme mit hohen Systemrechten, schützten sich vor Veränderungen und hätten Zugriff auf das gesamte Filesystem. Durch die hohe Updatefrequenz, die für einen einwandfreien Betrieb notwendig sei, könnten theoretisch beliebige Funktionalitäten unbemerkt hinzugefügt werden. Mit feindlichen Übergriffen aus Russland auf deutsche Institutionen, Unternehmen und lT-Infrastrukturen sei zu rechnen. Russland sehe Deutschland durch die Beteiligung an Sanktionen und Waffenlieferungen als Kontrahent an. Der russische Angriff auf die Ukraine werde mit hybriden Mitteln – also auch im Cyberraum – geführt. Russische Unternehmen wie L. könnten zum einen für die Unterstützung der russischen Streitkräfte instrumentalisiert werden und zum anderen selbst Ziel massiver Cyberangriffe werden. Es müsse damit gerechnet werden, dass L. nicht mehr die uneingeschränkte Kontrolle über seine Software und IT-Systeme habe bzw. diese in 21

Kürze verlieren werde. Wenn die L. -Produkte für Angriffe entweder durch Anweisung der russischen Regierung oder durch staatliches Eindringen in deren Systeme instrumentalisiert würden, sei es daher möglich, dass auf die Systeme, auf denen L. -Produkte installiert seien, unberechtigt zugegriffen oder Einfluss genommen werden könne. L. sei sich dieser schon in der Vergangenheit bestehenden Gefahren bewusst und habe diverse Maßnahmen zur Vertrauensbildung ergriffen, die aber alle nicht geeignet seien, die aktuelle veränderte Gefahrenlage zu entschärfen. Obwohl die Dateninfrastruktur für Kunden aus Europa, den Vereinigten Staaten und Kanada in zwei Rechenzentren in Zürich betrieben werde und Sitz der Holding des global agierenden privaten Unternehmens London sei, habe L. seinen Hauptsitz in Moskau und weise eine russische Eigentümerstruktur auf. AIs eines der wichtigsten lT-Security-Unternehmen Russlands arbeite L. eng mit Ermittlungsbehörden zusammen. Wesentliche Teile der Belegschaft arbeiteten in Russland oder hätten familiäre Bindungen in Russland und seien daher dem direkten Einfluss und Druck der Behörden ausgesetzt. Angesichts der nunmehr offenen Konfrontation Russlands mit der EU und den NATO-Staaten und der Hinnahme selbst existenzvernichtender Sanktionen für russische Unternehmen seien die eigenen Schutzmaßnahmen von L. nicht mehr ausreichend. Nunmehr sei davon auszugehen, dass die russische Regierung in der jetzigen Situation keine Rücksicht mehr auf das internationale Geschäft und die Reputation von L. nehmen würde. Zudem lägen aktuelle Informationen eines vertrauenswürdigen Partners vor, dass es bald zu einer Lageverschärfung mittels Cyber-Angriffen auf Hochwertziele kommen könnte.

II. 22

Die Beschwerde der Antragstellerin ist unbegründet. 23

Das Verwaltungsgericht hat ihren Antrag, 24

im Wege der einstweiligen Anordnung 25

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 sechs Monaten (Ordnungsgeld im Einzelfall höchstens 250.000,00 Euro, 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 15.3.2022, 26

2. der Antragsgegnerin aufzugeben, die mit Schreiben vom 15.3.2022 ausgesprochene Warnung zu widerrufen, 27

hilfsweise, 28

die Warnung unverzüglich, spätestens innerhalb eines Monats nach Veröffentlichung der Warnung, zu archivieren, 29

im Wesentlichen mit der Begründung abgelehnt, die Antragstellerin habe einen öffentlich-rechtlichen Unterlassungsanspruch wegen einer rechtswidrigen Beeinträchtigung einer grundrechtlich geschützten Position aus Art. 12 Abs. 1, 19 Abs. 3 GG nicht glaubhaft gemacht. Rechtsgrundlage für die streitgegenständliche Warnung sei § 7 Abs. 1 Satz 1, Abs. 2 Satz 1 BSIG. Der Begriff der Sicherheitslücke sei grundsätzlich weit zu verstehen. Maßgeblich sei, dass Eigenschaften von Programmen (aus)genutzt würden, um sich 30

unbefugt („gegen den Willen des Berechtigten“) Zugang zu verschaffen oder Funktionen eines Systems zu beeinflussen. Im Fall der L. Virenschutzsoftware sei das hohe Maß an Vertrauen in die Integrität der Software derzeit nicht mehr gegeben, weil die Einflussnahme russischer Akteure auf die Virenschutzprogramme drohe. Das Unternehmen L. habe seinen Hauptsitz in Moskau und beschäftige dort über 2.000 Mitarbeiter, einschließlich des Chief Technology Officers. Die zentralen operativen Voraussetzungen des IT-Dienstleistungsangebots von L. würden am Standort Moskau erbracht. Angesichts der geopolitischen Lage bzw. Russlands Angriffs auf die Ukraine, der auch als Cyberkrieg geführt werde, sei nicht auszuschließen, dass russische Entwicklerteams aus eigenem Antrieb oder unter dem Druck anderer russischer Akteure die technischen Möglichkeiten der Virenschutzprogramme ausnutzten, um Computersysteme in anderen Staaten zu korrumpieren. Dabei handele es sich um im Wirtschaftsleben bereits konkret in Betracht gezogene Bedrohungsszenarien. Es erscheine zwar plausibel, dass es grundsätzlich im Unternehmensinteresse von L. liege, jegliche Schadsoftware, auch solche von Staaten, zu enttarnen. Allerdings sei nicht davon auszugehen, dass das Unternehmen in der Lage wäre, seine in Russland ansässigen Mitarbeiter vor Einflussnahme und Zwang staatlicher Stellen in Russland hinreichend zu schützen. Etwas anderes folge nicht aus der Information Security Policy von L. . Die unternehmensinternen Vorgaben und Standards verlören an Wert, wenn der Hersteller in einem Staat ansässig sei, in dem eine Einflussnahme staatlicher Stellen auf das Unternehmen drohe. Aus diesem Grund böte auch die regelmäßige Zertifizierung der unternehmensinternen Sicherheitsprozesse durch unabhängige Institutionen und die Transparenzinitiative von L. keine Gewähr dafür, dass die Virenschutzsoftware nicht für Cyberangriffe missbraucht werden könne. Die großen zu verarbeitenden Datenmengen, der komplexe Programmcode, die erforderlichen häufigen Updates, die vielfältigen Angriffsmöglichkeiten und der geringe Aufwand für erfolgreiche Angriffe auf Virenschutzsoftware mache eine Qualitätssicherung durch Kunden oder externe Experten – die permanent erfolgen müsste – praktisch unmöglich. Ebenso lägen hinreichende Anhaltspunkte dafür vor, dass von der Sicherheitslücke Gefahren für die Sicherheit in der Informationstechnik ausgingen. Insbesondere mit Blick auf die Sanktionen westlicher Staaten sei es wahrscheinlich, dass auch (Hochwert-)Ziele in Deutschland von aus Russland geführten Cyberangriffen bedroht seien. Von russischen Stellen initiierte Cyberangriffe könnten staatliche Stellen und kritische Infrastruktur in den Fokus nehmen und zu (Kollateral-) Schäden für weite Teile der Bevölkerung führen. Ermessensfehler lägen nicht vor. Die Erforderlichkeit einer Sicherheitswarnung könne nicht losgelöst von der jeweiligen Cybersicherheitslage in dem betreffenden Staat getroffen werden. Die Einschätzung der Antragsgegnerin, die Warnmeldung werde mit hoher Wahrscheinlichkeit zwar spürbare Folgen für die wirtschaftliche Tätigkeit von L. in Deutschland haben, der Schutz der Allgemeinheit überwiege aber aufgrund der besonderen Schwere des Schadensrisikos das Interesse des Herstellers, sei rechtlich nicht zu beanstanden. Die Antragsgegnerin habe mit der Formulierung der Warnung 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. sei, sondern die drohende Einflussnahme des russischen Staats auf den Hersteller.

Das hiergegen gerichtete Beschwerdevorbringen, auf dessen Prüfung der Senat gemäß § 146 Abs. 4 Satz 6 VwGO beschränkt ist, gibt keinen Anlass zu einer anderen Beurteilung. 31

Die Einwände der Antragstellerin gegen die Annahme des Verwaltungsgerichts, die materiellen Voraussetzungen für den Erlass einer Warnung zu den Antivirenprogrammen von L. seien vorliegend erfüllt, greifen nicht durch. 32

33

Staatliches Informationshandeln unterliegt verfassungsrechtlichen Vorgaben, die sich auch in der einfachrechtlichen Ermächtigungsgrundlage für die Herausgabe einer Warnung und Empfehlung nach § 7 Abs. 1 Nr. 1 Buchst. a), Satz 1 Nr. 2, Abs. 2 Satz 1 BSIG widerspiegeln, und bei der Beurteilung der Rechtmäßigkeit zu beachten sind (hierzu unten 1.). Auf der Grundlage der Ermächtigungsgrundlage und des maßgeblichen Verfassungsrechts ist die streitgegenständliche Warnung rechtmäßig (hierzu unten 2.).

1. Amtliche Äußerungen müssen die hierfür geltenden verfassungsrechtlichen Grenzen einhalten. Soweit sie einer Grundrechtsbindung unterliegen, haben sie sich an den allgemeinen Grundsätzen für rechtsstaatliches Verhalten in der Ausprägung des Willkürverbots und des Verhältnismäßigkeitsgrundsatzes zu orientieren [hierzu unten a)]. Im Rahmen dieser Vorgaben kann das Bundesamt unter den Voraussetzungen von § 7 Abs. 1 Nr. 1 Buchst. a), Satz 1 Nr. 2, Abs. 2 Satz 1 BSIG die Öffentlichkeit hersteller- und produktbezogen vor Sicherheitslücken in informationstechnischen Systemen warnen und Sicherheitsmaßnahmen empfehlen [hierzu unten b)]. 34

a) Grundsätzlich schützt das Grundrecht aus Art. 12 Abs. 1 GG in der bestehenden Wirtschaftsordnung nicht vor der Verbreitung zutreffender und sachlich gehaltener Informationen am Markt, die für das wettbewerbliche Verhalten der Marktteilnehmer von Bedeutung sein können. Das Grundrecht vermittelt einem Unternehmen auch nicht ein Recht, nur so von anderen dargestellt zu werden, wie es gesehen werden möchte oder wie es sich und seine Produkte selber sieht. 35

Vgl. BVerfG, Beschluss vom 26.6.2002 – 1 BvR 558/91 –, BVerfGE 105, 252 = juris, Rn. 42 ff. 36

Eine rechtzeitige öffentliche Information kann etwa die Bewältigung von Konflikten in Staat und Gesellschaft erleichtern. Auf diese Weise kann neuen, oft kurzfristig auftretenden Herausforderungen entgegengetreten und auf Krisen sowie auf Besorgnisse der Bürger schnell und sachgerecht reagiert werden, um diesen zu Orientierungen zu verhelfen. Derart motivierte Informationen, Empfehlungen und Warnungen des Staates zielen regelmäßig nicht auf eine Grundrechtsbeeinträchtigung. Eine solche Wirkung entsteht häufig vielmehr mittelbar-faktisch erst aufgrund der Reaktionen auf das staatliche Informationshandeln. 37

Vgl. BVerfG, Beschluss vom 26.6.2002 – 1 BvR 670/91 –, BVerfGE 105, 279 = juris, Rn. 75 ff. 38

Die Unterrichtung der Öffentlichkeit über Vorgänge und Entwicklungen, die für den Bürger und das funktionierende Zusammenwirken von Staat und Gesellschaft von Wichtigkeit sind, kann im Rahmen verfassungsrechtlicher Aufgabenzuweisungen oder gesetzlicher Ermächtigungen auch dann zulässig sein, wenn mit dem Informationshandeln mittelbar-faktische Grundrechtsbeeinträchtigungen verbunden sind. Sofern oder soweit sich mittelbar-faktische Wirkungen staatlichen Informationshandelns einer Normierung entziehen, etwa weil das Vorgehen durch den konkreten Anlass der Äußerung bestimmt wird, der oft kurzfristig entsteht, sich unter Umständen schnell wieder ändert und deshalb vielfach ebenfalls nicht prognostiziert werden kann, verlangt der Gesetzesvorbehalt nicht einmal eine über die Aufgabenzuweisung hinausgehende gesetzliche Ermächtigung. Angesichts der zwangsläufig weiten und unbestimmten Fassung einer einfachgesetzlichen Ermächtigung zum Informationshandeln wäre in Fällen dieser Art mit einer solchen Ermächtigung eine Entscheidung zur Sache in Wirklichkeit nicht verbunden. 39

40

Vgl. BVerfG, Beschluss vom 26.6.2002 – 1 BvR 670/91 –, BVerfGE 105, 279 = juris, Rn. 76 ff.

Unabhängig davon, inwieweit staatliches Informationshandeln einfachgesetzlicher Normierung zugänglich ist, besteht eine Grundrechtsbindung aus Art. 12 Abs. 1 GG jedoch dann, wenn solches Handeln zwar die Berufstätigkeit nicht unmittelbar berührt, aber Rahmenbedingungen der Berufsausübung verändert und in Zielsetzung und mittelbar-faktischen Wirkungen einem Grundrechtseingriff als funktionales Äquivalent gleichkommt. Dies kann jedenfalls dann der Fall sein, wenn eine amtliche Information 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. 41

Vgl. BVerfG, Beschlüsse vom 21.3.2018 – 1 BvF 1/13 –, BVerfGE 148, 40 = juris, Rn. 28, und vom 26.6.2002 – 1 BvR 558/91 –, BVerfGE 105, 252 = juris, Rn. 62, sowie – 1 BvR 670/91 –, BVerfGE 105, 279 = juris, Rn. 76. 42

Soweit hiernach eine Grundrechtsbindung besteht, haben sich amtliche Äußerungen an den allgemeinen Grundsätzen für rechtsstaatliches Verhalten in der Ausprägung des Willkürverbots und des Verhältnismäßigkeitsgrundsatzes zu orientieren. Mitgeteilte Tatsachen müssen objektiv zutreffend wiedergegeben werden. Werturteile dürfen nicht auf sachfremden Erwägungen beruhen, d. h. sie müssen bei verständiger Beurteilung auf einem im Wesentlichen zutreffenden oder zumindest sachgerecht und vertretbar gewürdigten Tatsachenkern beruhen, und dürfen zudem den sachlich gebotenen Rahmen nicht überschreiten. 43

Vgl. BVerfG, Beschlüsse vom 15.8.1989 – 1 BvR 881/89 –, juris, Rn. 7 sowie 15, und vom 26.6.2002 – 1 BvR 558/91 –, BVerfGE 105, 252 = juris, Rn. 61; BVerwG, Beschluss vom 11.11.2010 – 7 B 54.10 –, juris, Rn. 14. 44

Die Grundrechtsbindung hindert zuständige staatliche Stellen aber nicht daran, sich überhaupt zu grundrechtlich geschützten Bereichen – auch kritisch – zu äußern. Grundrechte schützen nicht vor der Verbreitung von inhaltlich zutreffenden und unter Beachtung des Gebots der Sachlichkeit sowie mit angemessener Zurückhaltung formulierten Informationen durch einen Träger von Staatsgewalt. 45

Vgl. BVerfG, Beschlüsse vom 26.6.2002 – 1 BvR 670/91 –, BVerfGE 105, 279 = juris, Rn. 54 (zu staatlichem Informationen über das tatsächliche Verhalten einer religiösen oder weltanschaulichen Gruppierung), und vom 26.6.2002 – 1 BvR 558/91 –, BVerfGE 105, 252 = juris, Rn. 59 (zu marktbezogenem Informationshandeln). 46

Die zuständige Behörde kann zur Verbreitung von Informationen, wozu auch Empfehlungen oder Warnungen gehören, unter besonderen Voraussetzungen auch dann berechtigt sein, wenn ihre Richtigkeit noch nicht abschließend geklärt ist. In solchen Fällen hängt die Rechtmäßigkeit der staatlichen Informationstätigkeit davon ab, ob der Sachverhalt vor seiner Verbreitung im Rahmen des Möglichen sorgsam und unter Nutzung verfügbarer Informationsquellen, gegebenenfalls auch unter Anhörung Betroffener, sowie in dem Bemühen um die nach den Umständen erreichbare Verlässlichkeit aufgeklärt worden ist. Verbleiben dennoch Unsicherheiten in tatsächlicher Hinsicht, ist der Staat an der Verbreitung der Informationen gleichwohl jedenfalls dann nicht gehindert, wenn es im öffentlichen Interesse liegt, dass die Marktteilnehmer über einen für ihr Verhalten wichtigen Umstand, etwa ein Verbraucherrisiko, aufgeklärt werden. In solchen Fällen wird es angezeigt sein, die 47

Marktteilnehmer auf verbleibende Unsicherheiten über die Richtigkeit der Information hinzuweisen, um sie in die Lage zu versetzen, selbst zu entscheiden, wie sie mit der Ungewissheit umgehen wollen. Im Übrigen ist die Verbreitung von Informationen unter Berücksichtigung möglicher nachteiliger Wirkungen für den Betroffenen auf das zur Informationsgewährung Erforderliche zu beschränken.

Vgl. BVerfG, Beschluss vom 26.6.2002 – 1 BvR 558/91 –, BVerfGE 105, 252 = juris, Rn. 56 f., 60 f. 48

b) Die Voraussetzungen für die Herausgabe von Warnungen vor Sicherheitslücken in informationstechnischen Systemen und Empfehlungen von Sicherheitsmaßnahmen durch das Bundesamt für Sicherheit in der Informationstechnik hat der Gesetzgeber in § 7 Abs. 1 Nr. 1 Buchst. a), Satz 1 Nr. 2, Abs. 2 Satz 1 BSIG normiert. Das Bundesamt ist die zentrale Stelle für Informationssicherheit auf nationaler Ebene (§ 1 Satz 2 BSIG). In seinen Aufgabenbereich fallen gemäß § 3 Abs. 1 Satz 2 Nr. 14, 14a BSIG 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 (Nr. 14) sowie der Verbraucherschutz und die Verbraucherinformation im Bereich der Sicherheit in der Informationstechnik, insbesondere durch Beratung und Warnung von Verbrauchern in Fragen der Sicherheit in der Informationstechnik und unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen (Nr. 14a). Gemäß § 7 Abs. 1 BSIG kann das Bundesamt zur Erfüllung seiner Aufgaben nach § 3 Abs. 1 Satz 2 Nr. 14 und 14a BSIG unter anderem Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten an die Öffentlichkeit oder an die betroffenen Kreise richten [Satz 1 Nr. 1 Buchst. a)] und Sicherheitsmaßnahmen sowie den Einsatz bestimmter Sicherheitsprodukte empfehlen (Satz 1 Nr. 2). Unter Nennung der Bezeichnung und des Herstellers des betroffenen Produkts kann es nach § 7 Abs. 2 Satz 2 BSIG zur Erfüllung seiner Aufgaben nach § 3 Abs. 1 Satz 2 Nr. 14, 14a BSIG die Öffentlichkeit unter anderem vor Sicherheitslücken [hierzu unten aa)] in informationstechnischen Produkten und Diensten warnen oder Sicherheitsmaßnahmen sowie den Einsatz bestimmter Sicherheitsprodukte empfehlen, wenn hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Sicherheit in der Informationstechnik hiervon ausgehen [hierzu unten bb)]. 49

aa) Nach § 2 Abs. 6 BSIG sind Sicherheitslücken Eigenschaften von Programmenoder 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. Die Gesetzesbegründung macht deutlich, dass allein maßgeblich sein soll, ob ein informationstechnisches System über eine solche – grundsätzlich unerwünschte – Beeinflussungsmöglichkeit durch Dritte verfügt. Der Begriff ist notwendigerweise weit gefasst, weil Sicherheitslücken in den unterschiedlichsten Zusammenhängen, oftmals abhängig von der Konfiguration oder Einsatzumgebung, entstehen können. 50

Vgl. BT-Drs. 16/11967, S. 12. 51

Damit hat sich der Gesetzgeber bewusst dagegen entschieden, den Begriff der Sicherheitslücke auf Fehlkonfigurationen der Hard- oder Software zu beschränken. Die entsprechende Empfehlung im Gesetzgebungsverfahren hat er nicht aufgegriffen. 52

53

Vgl. Pohl, Hochschule Bonn-Rhein-Sieg, Stellungnahme an den Innenausschuss des Deutschen Bundestages vom 5.5.2009, A-Drs. 16(4)570 C, S. 3.

Angesichts der Vielgestaltigkeit möglicher Risiken für die Sicherheit in der Informationstechnik ist es auch verfassungsrechtlich unbedenklich, dass der Gesetzgeber den Begriff der Sicherheitslücke gerade als Tatbestandsvoraussetzung für eine amtliche Warnung weit gefasst hat, um bislang unvorhersehbare Fallgestaltungen abzudecken. Die Bedrohungsszenarien für die Sicherheit in der Informationstechnologie sind vielgestaltig und außerordentlich dynamisch. 54

bb) Eine Produktwarnung im Sinne von § 7 Abs. 2 Satz 1 BSIG ist aber nur dann gerechtfertigt, wenn hinreichende Anhaltspunkte dafür vorliegen, dass von einer Sicherheitslücke Gefahren für die Sicherheit in der Informationstechnik ausgehen. Die Sicherheit in der Informationstechnik und der damit verbundene Schutz von Informationen und informationsverarbeitenden Systemen vor Angriffen und unautorisierten Zugriffen erfordert die Einhaltung bestimmter Sicherheitsstandards zur Gewährleistung der informationstechnischen Grundwerte und Schutzziele durch Sicherheitsvorkehrungen in informationstechnischen Systemen, Komponenten oder Prozessen oder bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen (vgl. § 2 Abs. 2 Sätze 3 und 4 BSIG). 55

Liegen hinreichende Anhaltspunkte dafür vor, dass die Sicherheitsstandards insbesondere zum Schutz der Verfügbarkeit, Integrität und Vertraulichkeit von Informationen (§ 2 Abs. 2 Satz 4 BSIG), 56

vgl. zu den informationstechnischen Grundwerten Grimm/Waidner, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 1. Aufl. 2021, S. 39 ff., Kap. 2 Rn. 17 ff. 57

nicht mehr gewährleistet werden können, sind zugleich hinreichende Anhaltspunkte dafür gegeben, dass von dem betroffenen Programm oder informationstechnischen System eine Gefahr für die Sicherheit in der Informationstechnik ausgeht. 58

Ob hinreichende Anhaltspunkte dafür vorliegen, dass von einem Produkt aufgrund einer Sicherheitslücke Gefahren für die Sicherheit in der Informationstechnik ausgehen, ist anhand aller mit vernünftigem Aufwand feststellbaren Umstände oder Ereignisse zu beurteilen, die nachteilige Auswirkungen auf die Sicherheit von Informationssystemen haben können. Mit Blick auf das mit dem BSIG verfolgte Ziel der umfassenden Gewährleistung der Sicherheit der Informationstechnik sind sowohl technische Kriterien als auch staatliche Sicherheitsinformationen einzubeziehen. 59

Vgl. zur Berücksichtigung von staatlichen Sicherheitsinformationen schon bei der Entwicklung von Sicherheitskriterien, Prüfverfahren und Prüfwerkzeugen: BT-Drs. 11/7029, S. 6. 60

Dem steht § 1 Satz 3 BSIG nicht entgegen. Danach führt das Bundesamt Aufgaben gegenüber den Bundesministerien auf Grundlage wissenschaftlich-technischer Erkenntnisse durch. Der Satz wurde im Rahmen der Neufassung des § 1 BSIG durch Art. 1 Nr. 1 des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18.5.2021 (BGBl. I S. 1122) aufgenommen und dient der Klarstellung, dass das Bundesamt Aufgaben der Beratung und Unterstützung als neutrale Stelle durchführt. 61

Vgl. BT-Drs. 19/28844, S. 39. 62

63

Eine Einschränkung hinsichtlich der zu berücksichtigenden Umstände bei der Beurteilung, ob hinreichende Anhaltspunkte für das Bestehen einer Gefahrenlage für die Sicherheit der Informationstechnik gegeben sind, liegt hierin nicht.

2. Nach diesen Maßstäben ist die streitgegenständliche Warnung und Empfehlung rechtmäßig. Die Tatbestandsvoraussetzungen von § 7 Abs. 1 Nr. 1 Buchst. a), Satz 1 Nr. 2, Abs. 2 Satz 1 BSIG sind gegeben [hierzu unten a)]. Ermessensfehler liegen nicht vor, insbesondere hat die Antragsgegnerin das Verhältnismäßigkeitsgebot gewahrt [hierzu unten b)]. 64

a) Das Bundesamt ist rechtlich zutreffend davon ausgegangen, dass bei den von der Antragstellerin vertriebenen Virenschutzprogrammen schon aufgrund ihrer konkreten Funktionsweise eine Sicherheitslücke im Sinne des § 2 Abs. 6 BSIG besteht [hierzu unter aa)]. Aufgrund der veränderten geopolitischen Lage seit Beginn des Angriffskriegs Russlands auf die Ukraine und der von der russischen Regierung ausdrücklich erklärten Einordnung der Staaten der Europäischen Union als „unfreundliche Staaten“, 65

vgl. Russland zahlt nur noch Rubel an „unfreundliche Staaten“, Spiegel, 8.3.2022, abgerufen am 27.4.2022 unter: https://www.spiegel.de/wirtschaft/russland-zahlt-nur-noch-rubel-an-unfreundliche-staaten-a-c99d1fdb-6e26-487d-89b1-1c0ea8116f60, 66

besteht mit Blick auf Missbrauchsmöglichkeiten und Schadenspotential von Virenschutzprogrammen russischer IT-Hersteller mit einem beachtlichen Marktanteil in Deutschland ein besonderes Informationsbedürfnis der Öffentlichkeit, welchem das Bundesamt in sachlicher Weise nachgekommen ist. Insbesondere hat es hinreichende tatsächliche Anhaltspunkte, die so gravierend sind, dass sie eine Warnung rechtfertigen, dafür angeführt, dass von diesen Virenschutzprogrammen derzeit Gefahren für die Sicherheit in der Informationstechnik ausgehen [hierzu unter bb)]. 67

aa) Virenschutzprogramme – auch die von der Antragstellerin vertriebenen – weisen per se eine Sicherheitslücke im Sinne von § 2 Abs. 6 BSIG auf, weil sie über Eigenschaften verfügen, 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. Dies ist nach den fachkundigen Erwägungen des Bundesamts in seiner Warnung und der hierfür gegebenen Begründung der Fall, weil Virenschutzsoftware über weitreichende Systemberechtigungen verfügt und systembedingt (zumindest für Aktualisierungen) eine dauerhafte, verschlüsselte und nicht prüfbare Verbindung zu Servern des Herstellers unterhalten muss. Die in der Warnung beschriebenen Angriffsvektoren haben ausweislich der Begründung in der Vergangenheit bereits zu zahlreichen Vorfällen bei allen Herstellern von Virenschutzprogrammen geführt, in denen Fehlfunktionen IT-Systeme blockiert haben und Daten unbemerkt an den Hersteller übertragen worden sind. Nach aktenkundigen Erkenntnissen des Bundesamts kann die systembedingt vorhandene Root-Berechtigung zum Zugriff auf die eigentlich durch das Virenschutzprogramm zu schützende IT-Infrastruktur für maliziöse Aktivitäten missbraucht werden, ohne dass es zum Ausspionieren des Nutzers einer sog. Hintertür (backdoor) bedarf, also undokumentierter, alternativer Zugänge zu einem IT-System. Durch die hohe Updatefrequenz, die für einen einwandfreien Betrieb notwendig ist, können theoretisch beliebige Funktionalitäten unbemerkt hinzugefügt werden. Manipulationen lassen sich nach fachlicher Einschätzung des Bundesamts auch temporär vornehmen und dadurch sehr gut tarnen. 68

69

So auch unabhängige externe Fachleute, z. B. Shulman, Digitale Souveränität und der Fall L. , Tagesspiegel, 24.3.2022, abgerufen am 27.4.2022 unter: https://background.tagesspiegel.de/cybersecurity/digitale-souveraenitaet-und-der-fall-L. (eAkte VG, Bl. 223 ff.); Schmid, Warnung vor L. : Experten erklären, was die russische Software so riskant macht, 19.4.2022, abgerufen am 27.4.2022 unter: https://www.chip.de/news/Warnung-vor-L. -1-Experten-erklaeren-was-die-russische-Software-so-riskant-macht_184168547.html

(eAkte OVG, Bl. 79 ff.). 70

Diese technischen Möglichkeiten für Manipulationen durch Dritte über Virenschutzprogramme werden von der Antragstellerin nicht durchgreifend in Zweifel gezogen, obwohl sie hierzu über Expertenwissen aus erster Hand verfügt. Auf systembedingte Manipulationsmöglichkeiten zur Beurteilung der Frage abzustellen, ob eine Sicherheitslücke gegeben ist, ist nicht deshalb ausgeschlossen, weil nach diesem Begriffsverständnis auch andere Programme aufgrund ihrer Funktionsweise und der ihnen eingeräumten Zugriffsrechte von vornherein Sicherheitslücken aufweisen können. 71

Maßgeblich ist allein, dass ein informationstechnisches System – wie hier – Eigenschaften aufweist, 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. Bereits in diesem Fall sind dem informationstechnischen System – hier der Virenschutzsoftware – Angriffsvektoren immanent, die eine individuelle Risikoabschätzung im Hinblick auf die Nutzungssicherheit erfordern. Entscheidend für den sicheren Einsatz solcher Systeme ist, wovon auch das Bundesamt in seiner Warnung nachvollziehbar ausgeht, die Zuverlässigkeit und der Eigenschutz eines Herstellers sowie seine authentische Handlungsfähigkeit. 72

Vgl. hierzu auch die Antwort der Bundesregierung auf die Kleine Anfrage zum behördliche Umgang mit L. Software, BT-Drs. 19/6048, S. 5. 73

bb) Es liegen hinreichende Anhaltspunkte dafür vor, dass durch die Nutzung der von der Antragstellerin vertriebenen Virenschutzsoftware derzeit eine Gefahr für die Sicherheit in der Informationstechnik besteht. Die von dem Bundesamt in der Warnung zunächst wiedergegebenen allgemeinen Feststellungen sind auf der Grundlage verfügbarer Erkenntnisse in der Sache zutreffend oder zumindest vertretbar gewürdigt [hierzu unten (1)]. Auch die Annahmen, durch Manipulationen an der Software oder den Zugriff auf bei L. gespeicherte Daten könnten Aufklärungs- oder Sabotageaktionen gegen Deutschland, einzelne Personen oder bestimmte Unternehmen oder Organisationen durchgeführt oder zumindest unterstützt werden, ein russischer IT-Hersteller könne selbst offensive Operationen durchführen, gegen seinen eigenen Willen gezwungen werden, Zielsysteme anzugreifen, oder selbst als Opfer einer Cyber-Operation ohne seine Kenntnis ausspioniert oder als Werkzeug für Angriffe gegen seine eigenen Kunden missbraucht werden, werden durch ausreichend gewichtige Anhaltspunkte gestützt [hierzu unten (2)]. 74

(1) Zunächst beruht die Annahme des Bundesamts, das Vorgehen militärischer und/oder nachrichtendienstlicher Kräfte in Russland sowie die im Zuge des aktuellen kriegerischen Konflikts jüngst von russischer Seite ausgesprochenen Drohungen gegen die EU, die NATO und die Bundesrepublik Deutschland seien mit einem erheblichen Risiko eines erfolgreichen IT-Angriffs mit weitreichenden Konsequenzen verbunden, auf hinreichenden Erkenntnissen zur aktuellen Cybersicherheitslage. 75

76

Allgemein wird bereits seit einigen Jahren angenommen, dass der Cyberraum heutzutage für Kriegsführung – sei es allein im Cyberraum oder im Rahmen eines hybriden Ansatzes – genutzt wird.

Vgl. EU-Kommission, Gemeinsame Mitteilung an das Europäische Parlament und den Rat – Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen, BR-Drs. 654/17, S. 2; European Union Agency for Cybersecurity (ENISA), Threat Landscape 2021, S. 21, 27.10.2021, abgerufen am 27.4.2022 unter: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021. 77

Nach den vom Bundesamt zur Begründung der Warnung herangezogenen Erkenntnissen besteht derzeit eine hoch dynamische Cybersicherheitslage gerade auch mit Blick auf mögliche Angriffe, die von der russischen Regierung gesteuert werden. Diese ist nach Erkenntnissen von Cybersicherheitsspezialisten und offiziellen amerikanischen Regierungsstellen seit langem in Cyberangriffe auf staatliche und privatwirtschaftliche Einrichtungen involviert und verfügt über umfassende Fähigkeiten zur Cyberkriegsführung, die in vielfältiger Weise, vor allem in der Ukraine, aber auch in den USA sowie in Europa jenseits der Ukraine, bereits gezielt eingesetzt worden sind, unter anderem um technische Anlagen abzuschalten und kritische Infrastrukturen komplett lahmzulegen. 78

Vgl. hierzu US Cybersecurity & Infrastructure Security Agency (CISA), Russia Cyber Threat Overview and Advisories, mit zahlreichen Nachweisen, abgerufen am 27.4.2022 unter: https://www.cisa.gov/uscert/russia; bpb, Hintergrund aktuell: Welche Rolle spielt der Cyberkrieg beim Überfall auf die Ukraine, 10.3.2022, abgerufen am 27.4.2022 unter: https://www.bpb.de/kurz-knapp/hintergrund-aktuell/506109/welche-rolle-spielt-der-cyberkrieg-beim-ueberfall-auf-die-ukraine/; Freidel, Russlands Trumpfkarte ist der Cyberkrieg, FAZ, 1.4.2022, aktualisiert am 4.4.2022, abgerufen am 27.4.2022 unter: https://www.faz.net/aktuell/politik/ausland/cyberkrieg-usa-warnen-vor-hackerangriffen-aus-russland-17927853.html; US-Department of Justice, Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide, 24.3.2022, abgerufen am 27.4.2022 unter: https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical. 79

Auch und gerade das militärische Vorgehen Russlands gegen die Ukraine wird durch Cyberangriffe begleitet. Nach aktuellen Schätzungen von IT-Sicherheitsforschern sind die Cyberaktivitäten gegen ukrainische Ziele zehnmal so hoch wie in Friedenszeiten. 80

Vgl. hierzu Bundesamt für Verfassungsschutz, Sicherheitshinweis für Politik & Verwaltung 01/2022 vom 11.4.2022, Krieg in der Ukraine, S. 2, abgerufen am 27.4.2022 unter: 81

https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/wirtschafts-wissenschaftsschutz/2022-04-11-Sicherheitshinweis-pv-1.pdf. 82

Ein besonderes Augenmerk der russischen Cyberangriffe liegt nach Erkenntnissen der Cybersicherheitsbehörden der USA, Großbritanniens und Deutschlands seit mehreren Jahren auf westlichen Versorgungseinrichtungen im Wege der Kompromittierung von Software-Supply-Chains. 83

Siehe hierzu BSI, Bericht zur Lage der IT-Sicherheit in Deutschland 2021, BT-Drs. 20/24, S. 9 f., 30 f.; Freidel, Russlands Trumpfkarte ist der Cyberkrieg, FAZ, 1.4.2022, aktualisiert am 4.4.2022, abgerufen am 27.4.2022 unter: https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical; CISA, 84

Alerts (AA22-011A) Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure, 11.1.2022, aktualisiert am 1.3.2022, abgerufen am 27.4.2022 unter: https://www.cisa.gov/uscert/ncas/alerts/aa22-011a und (AA22-110A), Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure, 20.4.2022, abgerufen am 27.4.2022 unter: https://www.cisa.gov/uscert/ncas/alerts/aa22-110a.

Seit Kriegsbeginn hat sich die Gefahrenlage nach den dem Bundesamt vorliegenden Erkenntnissen zwar noch nicht derart verdichtet, dass bestimmte Cyberangriffe der russischen Regierung auf Ziele in der Bundesrepublik Deutschland konkret vorhergesagt werden könnten. Allerdings ist es danach bereits auch in Deutschland zu wenigen unzusammenhängenden IT-Sicherheitsvorfällen gekommen, weshalb die Einschätzung nachvollziehbar ist, diese Bewertung könne sich jederzeit ändern und erhöhte Vorsicht sei geboten. 85

Siehe hierzu auch BSI, Einschätzung der aktuellen Cyber-Sicherheitslage in Deutschland nach dem russischen Angriff auf die Ukraine vom 4.3.2022, abgerufen am 27.4.2022 unter: 86

https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220225_Angriff-Ukraine-Statement.html. 87

Zudem liegen dem Bundesamt über das Nationale Cyber-Abwehrzentrum Informationen vor, nach denen es bald zu einer Lageverschärfung mittels Cyberangriffen – auch gegen deutsche Hochwertziele – kommen könnte. Auch aus Sicht des Bundesamts für Verfassungsschutz besteht ein erhöhtes Risiko von Cyberangriffen gegen deutsche Stellen – insbesondere in Reaktion auf die jüngsten Sanktionen und militärischen Unterstützungszusagen. Bei länger anhaltenden und/oder sich verschärfenden Kampfhandlungen sei von einem vermehrten Einsatz von Cyberwerkzeugen auszugehen. Es könne nicht ausgeschlossen werden, dass Ziele in Deutschland auch indirekt im Zuge von Spill-Over-Effekten und Kollateralschäden betroffen würden. Dies treffe insbesondere auf die Sektoren Energie, Telekommunikation, Transport, Finanzen, Medien und Rüstung zu. 88

Vgl. Bundesamt für Verfassungsschutz, Sicherheitshinweis für die Wirtschaft 01/2022 vom 4.3.2022, Krieg in der Ukraine, abgerufen am 27.4.2022 unter: https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/DE/2022/2022-03-01-wis.html. 89

Die jüngst von der Behörde für Cybersicherheit in den USA herausgegebene Warnung bestätigt diese Einschätzung. Nach den dort vorliegenden Erkenntnissen besteht ein erhöhtes Risiko von Cyberangriffen aus Russland auf die westlichen Länder als Reaktion auf die Wirtschaftssanktionen sowie deren Unterstützung der Ukraine durch Waffenlieferungen. 90

Vgl. CISA, Alert (AA22-110A), Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure, 20.4.2022, abgerufen am 27.4.2022 unter: https://www.cisa.gov/uscert/ncas/alerts/aa22-110a. 91

Als erster sog. Cyber-Kollateralschaden in Deutschland seit Beginn des russischen Angriffs auf die Ukraine ist – wie auch das Bundesamt im Rahmen der aktuellen Lagebeurteilung in den Blick genommen hat – der Cyberangriff auf den Satellitendienst des US-amerikanischen Netzbetreibers W. vom 24.2.2022 – dem Tag der russischen Invasion in die Ukraine – zu verzeichnen, durch welchen Satelliten-Modems funktionsunfähig gemacht worden sind, wovon auch tausende Windenergieanlagen in Deutschland betroffen waren, die für die Entstörung nicht mehr im Wege der Fernüberwachung erreichbar waren. 92

Vgl. hierzu auch Ohlig, Attacke auf W. – eine gezielte Cyberaktion, Tagesspiegel, 4.4.2022, abgerufen am 27.4.2022 unter: https://background.tagesspiegel.de/cybersecurity/attacke-auf-viasat-eine-gezielte-cyberaktion. 93

Bekannt sind ferner Angriffe der Russland zugeordneten Cybergruppierung GHOSTWRITER auf deutsche Ziele. Die Gruppierung ist erst Anfang März erneut aktiv geworden, indem es E-Mail-Adressen aus dem politischen Raum mit dem Ziel angegriffen hat, über diese Mailkonten Falschinformationen in den sozialen Medien zu platzieren. 94

Vgl. Bundesamt für Verfassungsschutz, Sicherheitshinweis für Politik & Verwaltung 01/2022 vom 11.4.2022, Krieg in der Ukraine, S. 2, abgerufen am 27.4.2022 unter: 95

https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/wirtschafts-wissenschaftsschutz/2022-04-11-Sicherheitshinweis-pv-1.pdf. 96

Weiter beobachtet das Bundesamt auf Basis öffentlicher Quellen und seiner Dienstleister aktuell vielfältige Formen des „Hacktivismus“, also dezentrale Cyber-Aktivitäten von Aktivisten gegen (symbolträchtige) Ziele. Bisher hätten diese Aktivitäten aus Sicht des Bundesamts über Symbolkraft hinaus zwar keine signifikanten Auswirkungen im Konflikt gehabt. Die wachsende Anzahl von nicht-staatlichen Akteuren verbunden mit unklaren Auftraggebern gestalte die Lage im Informationsraum aber zunehmend unübersichtlich. Nicht-öffentliche Quellen berichteten zudem über eine Zunahme von Scans russischer Gruppen, die nach Schwachstellen in westlichen Netzwerken suchten. 97

Auch Bitkom e. V., der Branchenverband der deutschen Informations- und Telekommunikationsbranche, sowie der Fachbeirat der Deutschen Cyber-Sicherheitsorganisation GmbH (DCSO), warnen vor der zunehmenden Gefahr durch Cyberangriffe für die deutsche Wirtschaft. Letzterer hat – bereits vor Erlass der streitgegenständlichen Warnung des Bundesamts – angesichts der aktuellen geopolitischen Lage die Nutzung der Virenschutzprogramme von L. als hoch problematisch eingeschätzt. Die Einbeziehung dieser Stellungnahmen bei Beurteilung der Sicherheitslage entspricht der Obliegenheit des Bundesamts, eine öffentliche Warnung möglichst sorgsam und unter Nutzung aller verfügbaren Informationsquellen zu erstellen. Fachliche Zweifel mit Blick auf die Aussagen insbesondere auch des DCSO bestehen nicht und wurden auch von der Antragstellerin nicht substantiiert dargelegt. Die Einbeziehung der fachlichen Lagebeurteilung durch das DCSO durch das Bundesamt entspricht zudem dem auf europäischer Ebene gesetzten Ziel, in Zusammenarbeit mit Unternehmen in wichtigen Wirtschaftssektoren die Abwehrfähigkeit bei Cyberangriffen und die Cybersicherheit insgesamt zu stärken. 98

Vgl. Erwägungsgrund 35 der Richtlinie (EU) 2016/1148; Erwägungsgrund 30 sowie Art. 4 Abs. 4 der Verordnung (EU) 2019/881; Europäische Kommission, Gemeinsame Mitteilung an das Europäische Parlament und den Rat – Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen, BR-Drs. 654/17, S. 3, 8 f. 99

Das Bundesamt geht in seiner Warnung weiter sachlich nachvollziehbar davon aus, dass Virenschutzsoftware aufgrund der ihr immanenten Angriffsvektoren ein exponiertes Ziel von offensiven Operationen im Cyberraum ist, um potentielle Gegner auszuspionieren, die Integrität ihrer Systeme zu beeinträchtigen oder sogar die Verfügbarkeit der darauf gespeicherten Daten vollständig einzuschränken. 100

101

Vgl. hierzu auch it-daily.net, Antivirus-Lösungen als Ursprung eines Cyberangriffs?, 26.1.2021, abgerufen am 27.4.2022 unter: https://www.it-daily.net/it-sicherheit/cybercrime/26975-antivirus-loesungen-als-ursprung-eines-cyberangriffs.

Dies gilt auch und gerade für staatlich gelenkte oder sonst veranlasste Cyberangriffe. So haben nach Angaben eines französischen Senior Security Researchers bei L. staatliche Akteure regelmäßig ein großes Interesse daran, die Funktionsweise der Antivirenprodukte zu verstehen und sich selbst vor Entdeckung zu schützen. 102

Vgl. Wolfangel, Ist L. wirklich ein Problem?, Spektrum, 17.3.2022, abgerufen am 27.4.2022 unter: https://www.spektrum.de/news/it-sicherheit-ist-L. -wirklich-ein-problem/2000236#:~:text=Das%20Bundesamt%20f%C3%BCr%20Sicherheit%20in,unsicher%20zu%20b 103

Mögliche Angriffsszenarien sind aus fachlicher Sicht des Bundesamts, dass das Virenschutzprogramm absichtlich Schadsoftware „übersieht“, Schadsoftware zwar detektiert, aber absichtlich nicht blockt oder Alarme unterdrückt, oder wichtige Systemkomponenten oder -dateien blockiert, die fälschlicherweise als Virus erkannt werden, um so einen Systemausfall zu verursachen. 104

(2) Für die von dem Bundesamt in seiner Warnung beschriebenen Bedrohungsszenarien – dass durch Manipulationen an der Software oder den Zugriff auf bei L. gespeicherte Daten Aufklärungs- oder Sabotageaktionen gegen Deutschland, einzelne Personen oder bestimmte Unternehmen oder Organisationen durchgeführt oder zumindest unterstützt werden könnten, ein russischer IT-Hersteller selbst offensive Operationen durchführen kann, gegen seinen eigenen Willen gezwungen werden kann, Zielsysteme anzugreifen, oder selbst als Opfer einer Cyber-Operation ohne seine Kenntnis ausspioniert oder als Werkzeug für Angriffe gegen seine eigenen Kunden missbraucht werden kann – liegen ebenso hinreichende Anhaltspunkte vor. Wenngleich Unsicherheiten über den möglichen Kausalverlauf und die Wahrscheinlichkeit eines solchen Cyberangriffs bestehen, beruht die Risikobewertung des Bundesamts nicht auf bloßen Spekulationen, sondern stützt sich auf eine ausreichend fundierte Tatsachengrundlage. 105

Die Virenschutzprogramme von L. bieten sich nach Einschätzung des Bundesamts für die russische Regierung gerade deshalb als Angriffsmittel im Rahmen eines Cyberkriegs in besonderer Weise an, weil sie weltweit verbreitet sind und eine hohe Marktdurchdringung gerade auch in Deutschland verzeichnen können. Es gibt nach den sorgfältigen und schlüssigen Recherchen des Bundesamts kein anderes auf dem deutschen Markt in gleicher Weise verbreitetes Virenschutzprogramm, welches für die russische Regierung für Cyberangriffe ähnlich attraktiv sein könnte. Aufgrund der hohen Marktdurchdringung bergen die Virenschutzprogramme von L. bei missbräuchlicher Verwendung ein enormes Angriffspotenzial, weil zeitgleich – insbesondere durch maliziöse Updates – eine Vielzahl von Softwarenutzern angegriffen und Daten abgegriffen oder ein weitreichender Zugang zu Systemen erlangt werden kann. 106

Vgl. zu den möglichen enormen Auswirkungen manipulierter Updates BSI, Bericht zur Lage der IT-Sicherheit in Deutschland 2021, BT-Drs. 20/24, S. 30 f. (zu der Angriffskampagne durch manipulierte Software-Installationsdateien oder -Updates der Software Orion des amerikanischen Herstellers SolarWinds). 107

Das Bundesamt hat ferner die in der Vergangenheit dokumentierte Einflussnahme der russischen Regierung auf die in Russland agierenden IT-Unternehmen, insbesondere auch auf L. , berücksichtigt und daraus nachvollziehbar gefolgert, dass hinreichende 108

Anhaltspunkte für die Gefahr bestehen, die russische Regierung werde auch im Rahmen des von ihr geführten Angriffskriegs auf die Ukraine eine Instrumentalisierung russischer Softwareunternehmen zur Durchführung eines Cyberangriffs nicht nur auf ukrainische, sondern auch auf andere westliche Ziele vornehmen.

Die russische Regierung ist seit längerem um eine stärkere Kontrolle über den IT-Sektor bemüht und auch L. steht als eines der führenden IT-Unternehmen Russlands unter direktem Druck, mit der russischen Regierung zu kooperieren. Zwar hat die Dachgesellschaft – L. Labs Limited – ihren Sitz inzwischen in London, Großbritannien. Zutreffend weist das Bundesamt aber darauf hin, dass mit der L. Lab ZAO nicht nur eine von vielen Tochterfirmen der L. Lab Limited in Russland ansässig ist. Im Gegenteil: Die drei Gesellschafter der L. Labs Limited sind russische Staatsbürger, die Konzernzentrale befindet sich weiterhin in Moskau, Russland. Dort beschäftigt L. nach unbestrittenen Ermittlungen des Bundesamts mehr als 2.000 Mitarbeiter, darunter zahlreiche Softwareentwickler. Zudem sitzen dort nicht nur der Chief Technology Officer von L. , sondern auch die Leitung des Global Research & Analysis Teams (GReAT). 109

Vgl. hierzu 110

https://www.L. .de/about/team/great (abgerufen am 27.4.2022). 111

Alle relevanten strategischen und operativen Aufgaben werden damit jedenfalls auch am Hauptsitz des Unternehmens in Moskau wahrgenommen. Das Unternehmen hat bewusst davon abgesehen, nicht nur seinen offiziellen Firmensitz außerhalb von Russland zu verlegen, sondern auch die Forschung und Entwicklung vollständig außerhalb von Russland zu betreiben. 112

So vergibt etwa der Bundesverband IT-Sicherheit e. V. das Vertrauenszeichen „IT Security made in EU“ an IT-Security Unternehmen, die nicht nur ihren offiziellen Firmensitz im EU-Raum haben, sondern auch ausschließlich im EU-Raum forschen und entwickeln, siehe hierzu die Pressemitteilung vom 2.11.2021, abgerufen am 27.4.2022 unter: 113

https://www.teletrust.de/startseite/pressemeldung/?tx_ttnews%5Btt_news%5D=1420&cHash=8214 7fd2c6 114

Weiter hat das Bundesamt in seine Erwägungen einbezogen, dass L. nach eigenen Angaben im Bereich der Cyberkriminalität (auch) mit russischen Behörden, insbesondere dem Innenministerium und dem Inlandsgeheimdienst FSB, zusammenarbeitet. 115

Vgl. auch die Angaben hierzu auf der Homepage von L. unter dem Titel „Unsere Grundsätze zur Zusammenarbeit mit Strafverfolgungsbehörden, kommerziellen und öffentlichen Einrichtungen“, abrufbar unter: https://www.L. .de/about/law-enforcement-cooperation, sowie unter dem Blog-Eintrag „Drei hartnäckige Mythen über L. “, abrufbar unter: https://www.L. .de/blog/L. -lab-mythbusters/17346/ (jeweils abgerufen am 27.4.2022). 116

Eine Distanzierung hiervon angesichts des rechtswidrigen Angriffskriegs Russlands auf die Ukraine, dem Druck, der seitens der russischen Regierung auch auf heimische Unternehmen und die Bevölkerung ausgeübt wird, und der auch sonst in Russland herrschenden Rechtsunsicherheiten hat L. bis heute nicht erklärt. Es hat sich zudem – ausweislich der Begründung des Bundesamts anders als viele andere Unternehmen – bereits in der Vergangenheit den von der russischen Regierung angestoßenen Maßnahmen zur Kontrolle des Internets gefügt. Im Jahr 2019 etwa blockierte die russische Telekom-Aufsichtsbehörde 117

Roskomnadzor mehrere VPN-Dienste in Russland, weil diese sich geweigert hatten, ihren Datenverkehr an die staatlichen IT-Systeme für Filterlisten zu koppeln, die der Durchsetzung der Blockade unerwünschter Websites und Messengerdienste dient. Neun der zehn aufgeforderten VPN-Anbieter haben hierauf ihre Server in Russland heruntergefahren, nur L. hat sein Produkt Secure Connection an das staatliche Informationssystem FGIS angeschlossen.

Vgl. Heise online, News 06/2019, Russland droht VPN-Diensten mit Blockade, abgerufen am 27.4.2022 unter:

https://www.heise.de/newsticker/meldung/Russland-droht-VPN-Diensten-mit-Blockade-4442975.html.

Ereignisse aus der Vergangenheit wie aktuelle Geschehnisse verdeutlichen ferner, dass die russische Regierung nicht davor zurückschreckt, zur Durchsetzung eigener Interessen Drohkulissen gegenüber in Russland ansässigen Unternehmen aufzubauen.

Vgl. aktuell etwa FAZ, Die Angst vor Putins Willkür, 20.4.2022, abgerufen am 27.4.2022 unter: https://www.faz.net/aktuell/wirtschaft/unternehmen/angst-vor-wladimir-putins-willkuer-deutsche-konzerne-in-russland-17970643.html?GEPC=s9&premium=0x8db4b663d68c78788853ecd644c156da.

Auch der IT-Hersteller L. war hiervon in der Vergangenheit bereits betroffen. Nach den vom Bundesamt herangezogenen Erkenntnissen war es etwa im Jahr 2017 unter unklaren Umständen zur Verhaftung und späteren Verurteilung eines hochrangigen Mitarbeiters von L. wegen Hochverrats gekommen. Vermutet wurde, dass hinter dem Verfahren die Motivation Russlands stand, die Zusammenarbeit zwischen russischen IT-Sicherheitsexperten und westlichen Stellen im Bereich der Cyberkriminalität zu unterbinden und L. mit der Verhaftung unter Druck zu setzen. Auch aktuell befürchtet ein Vertreter der Antragstellerin mögliche Repressalien für in Russland ansässige Mitarbeiter bei aus Regierungssicht nicht opportunem Verhalten. Das Unternehmen sei daher bemüht, die Mitarbeiter vor möglichen Vergeltungsmaßnahmen des russischen Staates zu schützen, etwa indem es sich nicht öffentlich gegen den Angriffskrieg Russlands gegen die Ukraine positioniere.

Die Tatsache, dass L. nach einem Gutachten von Prof. Dr. Hobér nicht dem russischen System of Operational Investigative Measures (SORM) oder anderen ähnlichen Gesetzen unterliegt und daher rechtlich nicht verpflichtet ist, Informationen zu teilen, entkräftet die von dem Bundesamt aufgezeigten Bedrohungsszenarien nicht.

Vgl. Hobér, Report, 31.1.2019, abgerufen am 27.4.2022 unter:

https://media.L. daily.com/wp-content/uploads/sites/92/2015/02/02060120/REPORT-OF-PROF-DR-KAJ-HOBER.pdf.

Denn durch Gesetz legitimiertes Handeln der russischen Regierung ist nicht Gegenstand der Warnung des Bundesamts.

Das Bundesamt hat ferner schlüssig dargelegt, aus welchen Gründen aus seiner fachkundigen Sicht die von L. eingeführten Sicherheitsvorkehrungen – die mögliche Einsichtnahme in den Quellcode, die für alle Mitarbeiter geltende Information Security Policy sowie die Zertifizierung der Sicherheit und Zuverlässigkeit der Programme – in der aktuellen

Situation nicht genügen, um den aufgezeigten Bedrohungen hinreichend entgegenzuwirken.

Die Möglichkeit der Einsichtnahme in den Quellcode, die Software-Updates und die Regeln zur Erkennung von Bedrohungen im Transparency Center in Zürich mag danach zur Förderung des Vertrauens in den Hersteller der Virenschutzprogramme geeignet sein und die Chance erhöhen, dass unabhängige Forscher mögliche backdoors entdecken. Es bleiben jedoch nach aktenkundiger Einschätzung des Bundesamts im Prozess der Binärcodeerstellung, der Softwareverteilung, aber auch durch den Umfang und die Dynamik der Software- und Signatur-Updates umfassende „weiße Flecken“, die technisch faktisch nicht überprüfbar sind. Diese Einschätzung wird von unabhängigen Fachleuten geteilt. 128

Vgl. hierzu beispielsweise Shulman, Digitale Souveränität und der Fall L. , Tagesspiegel, 24.3.2022, abgerufen am 27.4.2022 unter: https://background.tagesspiegel.de/cybersecurity/digitale-souveraenitaet-und-der-fall-L. (Beiakte 5, Bl. 61 ff.); Wolfangel, Ist L. wirklich ein Problem?, Spektrum, 17.3.2022, abgerufen am 27.4.2022 unter: https://www.spektrum.de/news/it-sicherheit-ist-L. -wirklich-ein-problem/2000236#:~:text=Das%20Bundesamt%20f%C3%BCr%20Sicherheit%20in,unsicher%20zu%20b 129

Für die in Rede stehenden Bedrohungsszenarien ist es ferner unerheblich, dass L. seine Dateninfrastruktur zur Verarbeitung und Speicherung von Cyberbedrohungsdaten von Kunden u. a. aus Europa in zwei Rechenzentren nach Zürich verlegt hat und für die Bereitstellung von Updates/Virensignaturen bei Bedarf verschiedene Server in Europa zur Verfügung stehen, unter anderem in Frankfurt. Das Bundesamt hat hierzu überzeugend dargelegt, allein entscheidend sei, wer Sourcecodeänderungen vornehmen und Signaturdaten erstellen könne und wie diese qualitätsgesichert und geprüft würden. Eine einzige getarnte VPN-Verbindung wäre nach Einschätzung des Bundesamts ausreichend, dem Personal aus Russland einen Fernzugriff auf die Rechenzentren in Zürich zu ermöglichen. Auch wäre das Einspielen eines schadhaften Codes manuell über einen USB-Stick technisch nicht nachweisbar. Der Einwand der Antragstellerin, ein von Russland aus gesteuerter Cyberangriff unter Nutzung eines der Virenschutzprogramme von L. sei aufgrund der nach den Firmengrundsätzen (Information Security Policy) nur restriktiv zu vergebenden Zugriffsmöglichkeiten und breit gefächerten Verantwortlichkeiten nicht möglich, greift nicht durch. Die in der Information Security Policy vorgesehenen Schutzmechanismen können nicht isoliert davon betrachtet werden, dass L. mit einem großen Teil seiner Mitarbeiter in einem Staat ansässig ist, in dem eine Einflussnahme staatlicher Stellen auf das Unternehmen droht. An der Erstellung von Updates sind nach den Angaben der Antragstellerin jedenfalls auch Experten beteiligt, die in Russland ansässig sind. Aus den von ihr vorgelegten Unterlagen geht nicht hervor, dass der Zugriff auf das Virenschutzprogramm oder die damit verbundenen Clouddienste stets der Kontrolle durch im Ausland sitzende Entwicklungsteams unterliegt, die einen missbräuchlichen Eingriff in jedem Fall unterbinden könnten, zumal der Chief Technology Officer von L. und die Leitung des Global Research & Analysis Teams in Moskau sitzen. Etwas anderes folgt auch nicht daraus, dass es nach dem Vortrag der Antragstellerin für einen umfassenden Zugriff auf die Software nicht ausreichend sei, lediglich in Russland auf die entsprechenden Personen Einfluss zu nehmen, sondern es auch der Einflussnahme auf die Entwicklungsteams im Ausland bedürfe. Es ist nichts dafür ersichtlich, dass für einen Cyberangriff ein „umfassender“ Zugriff auf die Software erforderlich ist. Dass die Schutzmechanismen auch die vom Bundesamt in den Blick genommenen Angriffsszenarien ausreichend sicher abwehren können, erschließt sich aus den Angaben der Antragstellerin und sonstigen vorliegenden Unterlagen nicht. 130

131

Ohne Erfolg rügt die Antragstellerin in diesem Zusammenhang, die Antiviren-Datenbanken sowie die Updates würden vor der Ausspielung an Kunden mit einer digitalen Signatur versehen und es sei ohne weiteres möglich, die Updates von einer unabhängigen Organisation verifizieren zu lassen. Ungeachtet dessen, dass nicht ersichtlich ist, ob eine solche Verifizierung derzeit überhaupt erfolgt, lassen sich Manipulationen auf staatliche Veranlassung unter Umgehung der Sicherheitsstandards des Unternehmens hierdurch gerade nicht verhindern. Dass jeder unautorisierte Zugriffsversuch auf das System nachvollzogen werden kann, dient lediglich der Aufklärung, vermag aber keine Angriffe im Vorhinein zu verhindern.

Eine abweichende Beurteilung musste sich dem Bundesamt auch nicht deshalb aufdrängen, weil die Sicherheit und Zuverlässigkeit der technischen und organisatorischen Verfahren sowie Datendienste von L. in der Vergangenheit von zwei externen, unabhängigen Prüforganisationen bestätigt worden sind. Eine fundamentale Herausforderung der Zertifizierung ist es gerade, dass Software dynamisch ist und kontinuierlich Updates zum Schließen von Schwachstellen oder zur Verbesserung ihrer Funktionalität erfordert. Die Zertifizierung ist im Grundsatz statisch. Sie sagt, wie das Bundesamt zutreffend in seiner Begründung zur Warnung ausführt, nur etwas über den Soll-Zustand zum Zeitpunkt des Audits aus, ist aber keine Garantie für den Ist-Zustand. 132

Vgl. hierzu auch Skiera, in: Hornung/Schallbruch (Hrgs.), IT-Sicherheitsrecht, 1. Aufl. 2021, S. 179 f., Kap. 8 Rn. 108. 133

Dies wird ? ohne dass es hierauf entscheidungserheblich ankommt ? bestätigt durch den auf der Homepage von L. veröffentlichten Vulnerability Report, wonach erst jüngst entdeckte Fehler in seinen Virenschutzprogrammen zu Cyberangriffen hätten genutzt werden können. 134

Vgl. L. , Vulnerability Report: List of Advisories, Advisory issued on March 31, 2022, abgerufen am 27.4.2022 unter: https://support.L. .com/general/vulnerability.aspx?el=12430#310322_1; zur Gefahreneinschätzung auch CISA, Bulletin (SB22-101) vom 11.4.2022, abgerufen am 27.4.2022 unter: 135

https://www.cisa.gov/uscert/ncas/bulletins/sb22-101. 136

Weiter steht der aktuellen Bewertung der Sicherheitslage nicht entgegen, dass das Bundesamt die von L. in den letzten Jahren eingeführten Sicherheitsvorkehrungen in der Vergangenheit als ausreichend erachtet hat, um die Sicherheit der Informationstechnologie zu gewährleisten. Insbesondere gab es für das Bundesamt in der Vergangenheit keinen Anlass, die Sicherheitsvorkehrungen unter Berücksichtigung des Einsatzes der Software im Rahmen eines auch als Cyberkrieg geführten Angriffskriegs Russlands zu bewerten. Insofern ist es nachvollziehbar, dass sich das Bundesamt etwa im Jahr 2017 allein zur Vertrauenswürdigkeit des Unternehmens und Erkenntnissen zu etwaigen technischen Schwachstellen geäußert hat. 137

Vgl. BSI-Stellungnahme zu Medienberichten über AV-Software vom 11.10.2017, abgerufen am 27.4.2022 unter: 138
https://web.archive.org/web/20171201184645/https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Pre
_11102017.html.

Dass das Bundesamt in Sachen Cybersicherheit die Zusammenarbeit mit L. unabhängig von der streitgegenständlichen Warnung fortführen möchte, lässt ebenfalls keinen anderen Rückschluss zu, weil diese nicht den Einsatz der Virenschutzprogramme von L. betrifft. 139

Nur insofern aber, wegen der gegebenen Anhaltspunkte für vom russischen Staat veranlasste Cyberangriffe unter Einbeziehung russischer IT-Unternehmen, stehen der noch ausreichende Eigenschutz von L. und dessen authentische Handlungsfähigkeit in Frage.

Die vorstehende Lagebeurteilung wird konkret in Bezug auf das Risiko der Nutzung von Virenschutzprogrammen der Firma L. durch die in anderen Ländern herausgegebenen Warnungen und Handlungsempfehlungen zur aktuellen Cybersicherheit bestätigt, wenngleich sich die Risikoeinschätzungen nicht in jeder Hinsicht decken. So haben die USA bereits im Jahr 2017 behördlichen Einrichtungen untersagt, IT-Produkte der Firma L. zu nutzen und Ende März 2022 L. als ein inakzeptables Risiko für die nationale Sicherheit der USA und für die Sicherheit der amerikanischen Bürger eingestuft. 140

Vgl. FCC, Presseinformation vom 25.3.2022, Az. DA 22-320, abgerufen am 27.4.2022 unter: https://docs.fcc.gov/public/attachments/DA-22-320A1.docx. 141

Auch in den Niederlanden ist die Nutzung von L. -Software wegen Sicherheitsbedenken in Behörden der Regierung seit 2018 untersagt. 142

Vgl. Brief van de Minister Van Justitie en Veiligheid aan de Voorzitter von de Tweede Kamer der Staten-Generaal, 14.5.2018, abgerufen am 27.4.2022 unter: https://www.tweedekamer.nl/downloads/document?id=a30541a9-8c7e-45b5-932d-cd7f2916b9a9. 143

Ebenso hat das Europäische Parlament 2018 die EU aufgefordert, die Software, die IT-Kommunikationsgeräte sowie die entsprechenden Infrastrukturen, die in den Organen eingesetzt werden, einer umfassenden Überprüfung zu unterziehen, um die Verwendung potenziell gefährlicher Programme und Geräte auszuschließen und die Verwendung als böswillig eingestufter Programme und Geräte wie L. Lab zu verbieten. 144

Vgl. Entschließung des Europäischen Parlaments vom 13.6.2018 zur Cyberabwehr (2018/2004 (INI)), Rn. 76, abgerufen am 27.4.2022 unter: https://www.europarl.europa.eu/doceo/document/TA-8-2018-0258_DE.html. 145

Frankreich und Tschechien haben nach Kriegsbeginn jeweils Warnungen bezogen auf die Nutzung von Produkten russischer IT-Hersteller, insbesondere L. , ausgesprochen, 146

CERT-FR, Rapport Menaces et Incidents du CERT-FR, 2.3.2022, zuletzt aktualisiert am 12.4.2022, abgerufen am 27.4.2022 unter: https://cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-001/; NUKIB, Warning, 21.3.2022, File reference: 350-401/2022, Case No.: 3381/2022-NUKIB-E-350, abgerufen am 27.4.2022 unter: https://nukib.cz/download/aktuality/en_2022-03-21_warning.pdf, 147

und auch Großbritannien hat seine Empfehlungen mit Blick auf den Einsatz von Software russischer IT-Hersteller aktualisiert. 148

Vgl. UK National Cyber Security Centre, Use of Russian technology products and services following the invasion of Ukraine, 29.3.2022, abgerufen am 27.4.2022 unter: https://www.ncsc.gov.uk/blog-post/use-of-russian-technology-products-services-following-invasion-ukraine. 149

b) Das Bundesamt hat die Entscheidung, die Warnung herauszugeben, ermessensfehlerfrei getroffen und dabei insbesondere den Grundsatz der Verhältnismäßigkeit gewahrt. 150

151

Die Warnung ist nicht aufgrund sachfremder Erwägungen herausgegeben worden, insbesondere war sie weder politisch motiviert noch stellt sie reine Symbolpolitik dar.

Zur öffentlichen Diskussion hierzu vgl. Kipker, Durfte das BSI vor russischer Virenschutz-Software warnen, LTO, 8.4.2022, abgerufen am 27.4.2022 unter: https://www.lto.de/recht/kanzleien-unternehmen/k/L. -ovg-nrw-warnung-bsi-gute-chanchen-sicherheitsluecke-bewertung/?r=rss (eAkte OVG, Bl. 23 ff.); Herpig/Atug, L. -Produktwarnung: Reine Symbolpolitik?, Tagesspiegel, 7.4.2022, abgerufen am 27.4.2022 unter: https://background.tagesspiegel.de/cybersecurity/L. -produktwarnung-reine-symbolpolitik (eAkte OVG, Bl. 29 ff.). 152

Angesichts der aufgezeigten Bedrohungslage dient sie allein dazu, das Risiko von Angriffsmöglichkeiten auf die Sicherheit in der Informationstechnik zu reduzieren. Hierzu war sie geeignet und erforderlich. Mit der Warnung erhöht das Bundesamt signifikant das Bewusstsein für potentiell mögliche Gefahren, die sich aus dem Einsatz der Virenschutzprogramme von L. aktuell ergeben und empfiehlt nach individueller Risikobewertung einen Ersatz durch alternative Produkte. Zugleich hat es die Warnung unter Beachtung des Zurückhaltungsgebots formuliert und auf das Erforderliche beschränkt. 153

Das Bundesamt hat zu Beginn des Warntextes unter „Sachverhalt“ das allgemeine Gefahrenpotenzial von Virenschutzprogrammen beschrieben, die aktuelle Bedrohungslage, aufgrund derer mit einem erheblichen Risiko eines erfolgreichen IT-Angriffs zu rechnen ist, benannt und sodann – abstrakt – die Möglichkeiten aufgezählt, wie ein Missbrauch von Virenschutzprogrammen eines russischen IT-Herstellers erfolgen kann. Die bestehenden Unsicherheiten über den möglichen Kausalverlauf und die Wahrscheinlichkeit eines solchen Cyberangriffs werden durch diesen Aufbau und die gewählte Formulierung hinreichend zum Ausdruck gebracht. Zugleich wird der Eindruck vermieden, es lägen bereits konkrete Hinweise dafür vor, dass mit Hilfe der Virenschutzprogramme von L. Daten unberechtigt abgegriffen würden oder sonst Tatsachen bekannt seien, durch die Software sei bereits Missbrauch erfolgt. Ebenfalls deutlich wird, dass die Warnung nicht auf konkreten technischen Mängeln an den von der Antragstellerin vertriebenen Virenschutzprogrammen beruht. 154

Noch ausreichend deutlich wird auch, dass das Bundesamt dem Unternehmen L. bislang nicht das Vertrauen insgesamt entzogen hat. Zwar weist es (sachlich zutreffend) auch darauf hin, ein russischer IT-Hersteller könne selbst offensive Operationen durchführen. Dies gilt ebenso – das wird im Kontext der Warnung deutlich – für den russischen IT-Hersteller L. . Zugleich kommt aber hinreichend zum Ausdruck, dass Anhaltspunkte für das Drohen derartiger Operationen nur wegen der befürchteten direkten oder indirekten Einwirkung des russischen Staates gesehen werden. 155

Das Bundesamt hat weiter ausdrücklich auf das abgestufte Risiko eines Cyberangriffs hingewiesen, wobei Unternehmen und Behörden mit besonderen Sicherheitsinteressen/Rahmenbedingungen und Einrichtungen kritischer Infrastrukturen in besonderem Maße gefährdet seien. Eine Beschränkung auf eine Warnung allein von staatlichen Stellen und Einrichtungen kritischer Infrastrukturen war hingegen nicht angezeigt, weil darüber hinaus – mit abgestuftem Risiko – auch Unternehmen im besonderen öffentlichen Interesse, des produzierenden Gewerbes sowie wichtiger gesellschaftlicher Bereiche und eine große Zahl von Privatanwendern betroffen sein können. Insofern hat das Bundesamt darauf hingewiesen, dass Letztere möglicherweise am Wenigsten im Fokus stehen, aber in einem erfolgreichen Angriffsfall auch Opfer von Kollateralauswirkungen werden können. Die Nutzung von Virenschutzsoftware der Firma L. hat es gerade nicht 156

untersagt, sondern ausdrücklich von einer Abschaltung des Virenschutzprogramms ohne Vorbereitung abgeraten und empfohlen, bezogen auf den empfohlenen Wechsel zu anderen Produkten in jedem Fall eine individuelle Bewertung und Abwägung der aktuellen Situation durchzuführen.

Der Einwand der Antragstellerin, eine andere Formulierung – wie etwa die von Frankreich verwandte Formulierung in dem CERT-FR Bericht über Bedrohungen und Vorfälle vom 2.3.2022, zuletzt aktualisiert am 12.4.2022, 157

CERT-FR, Rapport Menaces et Incidents du CERT-FR, vom 2.3.2022, zuletzt aktualisiert am 12.4.2022, abgerufen am 27.4.2022 unter: https://cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-001/, 158

wäre aus ihrer Sicht für sie milder gewesen, greift schon deshalb nicht durch, weil Art. 12 Abs. 1 GG kein Recht des Unternehmens vermittelt, nur so von anderen dargestellt zu werden, wie es gesehen werden möchte oder wie es sich und seine Produkte selber sieht. 159

Angesichts der seit Jahren bekannten Bedrohungslage durch hochprofessionelle Cyberangriffe, gelenkt durch die russische Regierung mit besonderem Fokus auf Einrichtungen westlicher Staaten und kritischer Infrastrukturen, dem äußerst konfrontativen und aggressiven Vorgehen Russlands gegenüber dem Westen, der weiter zunehmenden Rechtsunsicherheiten innerhalb Russlands sowie des Umstands, dass Cyberangriffe in zeitlicher und örtlicher Hinsicht weitgehend unvorhersehbar sind, wäre eine zurückhaltender formulierte Warnung aber auch nicht in gleicher Weise geeignet gewesen, das notwendige Bewusstsein für potentiell mögliche Gefahren durch die Verwendung der von L. entwickelten Virenschutzsoftware in allen Bereichen der Gesellschaft zu wecken. Insbesondere ein Verzicht auf die Empfehlung, alternative Produkte zu verwenden, wäre zur Erreichung des gegenwärtig legitimen Schutzziels, verbreitete und besonders geeignete Angriffsmöglichkeiten für den russischen Staat in Deutschland durch deutliche Sensibilisierung verschiedenster Nutzerkreise spürbar zu begrenzen, nicht ebenso geeignet. 160

Bei der Entscheidung, ob und in welcher Form die Warnung erfolgen soll, hat das Bundesamt schließlich in nicht zu beanstandender Weise eine Folgenabwägung getroffen und dabei das durch Art. 12 Abs. 1 GG geschützte Interesse der Antragstellerin an der freien Ausübung ihres Gewerbes mit dem staatlichen Interesse an einem effektiven Schutz der Informationen sowie informationsverarbeitenden Systeme, Komponenten und Prozesse abgewogen. Dabei hat es zutreffend berücksichtigt, dass die produktbezogene Warnung mit hoher Wahrscheinlichkeit deutlich spürbare Folgen auf die wirtschaftliche Tätigkeit der Antragstellerin hat, zugleich aber Ungewissheiten bestehen, ob es zu einem Cyberangriff unter Nutzung der von L. entwickelten Virenschutzprogramme kommen wird. Dass es im Ergebnis dem Schutz der Allgemeinheit den Vorrang gegeben hat, ist rechtlich nicht zu beanstanden. Die Sicherheit in der Informationstechnik ist besonders schützenswert (vgl. § 2 Abs. 2 Satz 1 BSIG), zumal im konkreten Fall von einem möglichen Cyberangriff eine Vielzahl von zu schützenden Rechtsgütern betroffen sein kann. Dies gilt zunächst für Einrichtungen des Staates und kritische Infrastrukturen, also Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind. Durch ihren Ausfall oder ihre Beeinträchtigung würden erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten (vgl. § 2 Abs. 10 Satz 1 BSIG). Die Warnung dient ferner dem Schutz der bei einem erfolgreichen Cyberangriff in ihrer Gewerbeausübung betroffenen Unternehmen sowie dem Datenschutz aus Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG. Zugleich sind die möglichen Folgen eines 161

Cyberangriffs Russlands unter Missbrauch der in Deutschland auch unter Privatanwendern weit verbreiteten Virenschutzprogramme von L. unüberschaubar groß. In der aktuellen Situation aber ist zu befürchten, dass Russland jederzeit von der Möglichkeit eines Cyberangriffs unter Ausnutzung der Virenschutzprogramme von L. auch auf deutsche Ziele Gebrauch machen könnte.

Die Warnung erfolgte schließlich nicht willkürlich. Dass das Bundesamt aufgrund der aktuellen geopolitischen Lage und den damit verbundenen Risiken eines russischen Cyberangriffs vor der Nutzung der Virenschutzsoftware des Herstellers L. warnt, stellt keine Ungleichbehandlung gegenüber anderen Herstellern von Virenschutzprogrammen im Sinne von Art. 3 Abs. 1 GG dar. Bei den IT-Produkten anderer russischer Hersteller konnte das Bundesamt bislang kein vergleichbares Gefährdungspotential erkennen. Auch die Verflechtungen des chinesischen Staates mit dort ansässigen IT-Unternehmen und den daraus folgenden Sicherheitsbedenken sind nicht mit dem vorliegenden Sachverhalt in einer Weise vergleichbar, dass das Bundesamt gehalten wäre, in gleicher Weise zu agieren. Ungeachtet der Frage, in welcher Art und Weise chinesische Softwareprogramme als Angriffsmittel für Cyberattacken genutzt werden können, ist der Verzicht auf einen mit der hier streitgegenständlichen Warnung vergleichbaren Hinweis bezüglich der Nutzung von Softwareprodukten chinesischer IT-Hersteller schon deshalb nicht willkürlich, weil die chinesische Regierung die Bundesrepublik Deutschland nicht zum unfreundlichen Staat erklärt hat und bezogen auf Deutschland keine hinreichenden Anhaltspunkte für die Gefahr chinesischer Cyberangriffe im Rahmen einer kriegerischen Auseinandersetzung ersichtlich sind. Gleiches gilt für den pauschalen Einwand der Antragstellerin, eine Warnung müsse auch mit Blick auf die Nutzung von Software aus den USA gelten. 162

Die Kostenentscheidung folgt aus § 154 Abs. 2 VwGO. 163

Die Festsetzung des Streitwerts beruht auf §§ 47 Abs. 1, 53 Abs. 2 Nr. 1 und 52 Abs. 1 GKG und folgt der erstinstanzlichen Streitwertfestsetzung. 164

Dieser Beschluss ist gemäß § 152 Abs. 1 VwGO, § 68 Abs. 1 Satz 5 i. V. m. § 66 Abs. 3 Satz 3 GKG unanfechtbar. 165

Justiz NRW
Rechtsprechungsdatenbank ONLINE