DENNIS-KENJI KIPKER

Die „Sicherheitslücke“ im BSIG

Möglichkeiten und Grenzen der juristischen Auslegung eines Rechtsbegriffs

Produktwarnung

Gem. § 7 Abs. 1 BSIG hat das BSI die Befugnis, zur Erfüllung seiner Aufgaben nach § 3 Abs. 1 S. 2 Nr. 14 und Nr. 14a BSIG Warnungen und Informationen an die Öffentlichkeit oder an die betroffenen Kreise zu richten sowie Sicherheitsmaßnahmen und den Einsatz bestimmter Produkte zu empfehlen. Seit der Veröffentlichung der Warnung des BSI vor Antivirus-Produkten des russischen Herstellers Kaspersky im März 2022 ist eine öffentliche, rechtliche und rechtspolitische Diskussion darüber entbrannt, wie der Rechtsbegriff der „Sicherheitslücke“ zu interpretieren ist, der zentrale tatbestandliche Voraussetzung zum Aussprechen einer allgemeinen Produktwarnung sowohl nach § 7 Abs. 1 BSIG als auch für die qualifizierte Produktwarnung unter Bezeichnung des Herstellers nach § 7 Abs. 2 BSIG ist. Der Beitrag will anhand einer formaljuristischen Analyse eine Einordnung über Möglichkeiten und Grenzen der juristischen Auslegung des Rechtsbegriffs der Sicherheitslücke geben. Lesedauer: 15 Minuten

I. Weit gefasste Auslegungsmöglichkeit der „Sicherheitslücke"

Die Warnbefugnis in § 7 Abs. 1 S. 1 Nr. 1 lit. a BSIG definiert den Begriff der Sicherheitslücke nicht. Jedoch enthält § 2 Abs. 6 BSIG eine Legaldefinition, die zur Auslegung der Vorschrift herangezogen werden kann: „Sicherheitslücken im Sinne des BSIG sind 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."

Der Gesetzgeber wollte die Sicherheitslücke auf Grund der Vielgestaltigkeit von potenziellen Sachverhalten und Bedrohungsszenarien weit verstanden wissen[1] und konkretisiert ihn in der Begründung zum Gesetz deshalb wie folgt: „Sicherheitslücken sind ... 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."[2]

Der Gesetzeswortlaut wie auch die Gesetzesbegründung beschränken sich folglich nicht auf bestimmte Arten von Schadsoftware oder Angriffsvektoren, was iSe Kasuistik im Hinblick auf die sich schnell fortentwickelnde Bedrohungslage weder praktikabel noch angebracht wäre. Zu Recht wird deshalb festgestellt, dass sich die IT-Sicherheit durch ein „komplexes und intransparentes Geflecht" beteiligter Akteure auszeichnet und hieraus das dringende Erfordernis erwächst, schnell und flexibel auf neue Gefahrenszenarien reagieren zu können.[3]

II. Kritik aus der rechtswissenschaftlichen Literatur am weiten Verständnis

Jedoch wird ein solches an sich notwendiges weites Verständnis der Sicherheitslücke in der rechtswissenschaftlichen Literatur in Teilen kritisiert. Dabei hat sich die juristische Debatte primär an der durch das BSI ausgesprochenen Kaspersky-Warnung[4] entzündet, deren rechtliche Grundlage die in § 7 Abs. 1 und Abs. 2 BSIG beschriebene und vorausgesetzte Sicherheitslücke ist.[5] So stellen die Autoren Deutsch und Eggendorfer im Hinblick auf die Entscheidung des OVG NRW, das die Kaspersky-Warnung im Eilrechtsschutz in zweiter Instanz zu beurteilen hatte, wie folgt fest: „Es sei ‚bemerkenswert, dass das Gericht [OVG NRW] eine bestimmungsgemäße Softwarefunktion (nämlich das Entfernen erkannter Schadsoftware) unter das Tatbestandsmerkmal „Sicherheitslücke" subsumiert, weil die Funktion – technisch bedingt – verschiedene Zugriffsrechte auf dem IT-System voraussetzt (zB Root-Berechtigungen).'[6] Die polizei- und ordnungsrechtliche Gefahr, die die Warnung voraussetzt, sei letzten Endes jedoch nicht aus technischen Gegebenheiten ergangen, sondern aus der Befürchtung, die bestimmungsgemäße Funktion der Antivirus-Software könne auf Grund des Russland-Ukraine-Kriegs zweckwidrig eingesetzt werden. Hierdurch sei der technisch besetzte Begriff der Sicherheitslücke „verbrannt" worden, indem nicht-technische Sachverhalte wie die politische Gefahrenlage in das Tatbestandsmerkmal hineingelesen wurden".[7]

Ebenso thematisiert der Autor Dittrich die für den o.g. Kaspersky-Fall aufgeworfene Frage der inhaltlichen Reichweite der Sicherheitslücke unter dem Gesichtspunkt der „Vertrauenswürdigkeit" des russischen Herstellers.[8] So stützen sowohl das BSI[9] als auch die Gerichte ihre Ausführungen im Hinblick auf die Definition der Sicherheitslücke primär auf das im Zuge des Russland-Ukraine-Kriegs nicht mehr in ausreichendem Umfang bestehende Herstellervertrauen und das Fehlen einer eigenen, authentischen Handlungsfähigkeit des Unternehmens im Angesicht eines autoritär und zunehmend unkalkulierbar handelnden russischen Staatsapparats. Dies sei für eine Software, die ihrer Zwecksetzung folgend schon über weite Systemberechtigungen verfügt, nicht hinnehmbar und hätte nicht mehr berechenbare Sicherheitsrisiken im Einsatz zur Folge. Möglicherweise durch den Hersteller ergriffene technisch-organisatorische Gegenmaßnahmen, wie eine Verlagerung zentraler Rechenzentren in die Schweiz, USA und Kanada oder Möglichkeiten zur Einsichtnahme in Quellcode seien nicht ausreichend, um die Bedrohung im gesetzlich geforderten Rahmen zu unterbinden.[10]

Dittrich stellt im Hinblick auf diese zunächst durchaus berechtigt erscheinenden Erwägungen des BSI die Frage, ob nicht erst die Warnung der IT-Sicherheitsbehörde zu einem Vertrauensverlust der Nutzer von Kaspersky-Antivirus-Produkten geführt haben könnte. Zur Begründung wird angeführt, dass es fernliegend erscheine, zumindest bei Verbrauchern automatisch von einem Vertrauensverlust im Zuge des Kriegsgeschehens auszugehen. So herrsche eine „unglaubliche Informationsflut, die gepaart wird mit gegenseitigen Vorwürfen der Desinformation". Ein Verbraucher würde überdies auch keine Gefährdungsanalyse in den sozialen Netzwerken durchführen, ob Mitarbeiter eines russischen Unternehmens im Zuge des Kriegsgeschehens noch über realistische eigene Handlungsoptionen verfügen oder vielmehr durch Akteure des autoritär handelnden russischen Staates fremdgesteuert werden. Dittrich gelangt deshalb abschließend in seiner juristischen Bewertung der Sicherheitslücke zu dem Ergebnis, dass zumindest bei der Zielgruppe der Verbraucher ein Zirkelschluss des BSI und damit auch des diese These im Eilrechtsschutz stützenden erstinstanzlichen Urteils des VG Köln vorliegt.

III. Durchgriff juristischer Bedenken zur tatbestandlichen Reichweite der „Sicherheitslücke"?

Fraglich jedoch ist, ob diese in der rechtswissenschaftlichen Literatur geäußerten Bedenken im Hinblick auf eine eingrenzende Auslegung des Begriffs der Sicherheitslücke durchgreifen können bzw. nicht vielmehr dem gesetzgeberisch angeordneten und in der bisherigen Rechtsprechung im Eilrechtsschutz bestätigten weiten Verständnis des Rechtsbegriffs widersprechen. Zur Klärung dieser Frage bedarf es einer formaljuristischen Be-

1 So auch VG Köln MMR 2022, 503 (505).
2 BT-Drs. 16/11967, 12.
3 Hierzu detailliert VG Köln MMR 2022, 503 (505).
4 BSI-Warnung gem. § 7 BSIG: Virenschutzsoftware des Herstellers Kaspersky, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Warnungen-nach-P7_BSIG/Archiv/2022/BSI_W-004-220315.pdf.
5 Dies stellen richtigerweise sowohl das VG Köln MMR 2022, 503 (504) als auch das OVG NRW MMR 2022, 695 fest.
6 Taeger/Pohle (Hrsg.), Computerrechts-HdB/Deutsch/Eggendorfer, 37. EL Mai 2022, 50.1 IT-Sicherheit, Rn. 410.
7 Taeger/Pohle (Hrsg.), Computerrechts-HdB/Deutsch/Eggendorfer, 37. EL Mai 2022, 50.1 IT-Sicherheit, Rn. 410.
8 Dittrich NJW 2022, 2971.
9 BSI-Warnung gem. § 7 BSIG: Virenschutzsoftware des Herstellers Kaspersky, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Warnungen-nach-P7_BSIG/Archiv/2022/BSI_W-004-220315.pdf.
10 VG Köln MMR 2022, 503 (505 f.); OVG NRW MMR 2022, 695.

trachtung, bei der auch die bisherige Auslegungspraxis des BSI als zuständiger Behörde Berücksichtigung finden sollte.

Bislang veröffentlichte das BSI basierend auf der Rechtsgrundlage des § 7 BSIG zwei zentrale Warnungen, die sich mit der tatbestandlichen Voraussetzung der Sicherheitslücke auseinandersetzen, namentlich bereits o.g. Kaspersky-Warnung v. 15.3.2022 sowie am 10.8.2022 eine Warnung vor einem Funk-Türschlossantrieb des deutschen Herstellers ABUS.[11] Obwohl sich sowohl die Kaspersky-Warnung als auch die ABUS-Warnung auf die Rechtsgrundlage nach § 7 BSIG stützen, wird in beiden Fällen ausdrücklich nicht auf die jeweils einschlägige tatbestandliche Alternative verwiesen, sondern nur die allgemeine Rechtsgrundlage genannt. Gerichtlich jedoch wurde die Warnung vor Antivirus-Produkten des Herstellers Kaspersky auf den bereits bekannten § 7 Abs. 1 S. 1 Nr. 1 lit. a BSIG als tatbestandliche Alternative gestützt, der die Sicherheitslücke in informationstechnischen Produkten und Diensten zum Gegenstand hat.[12] Dies erscheint vor dem Hintergrund des gegebenen Sachverhalts auch als naheliegendste bzw. juristisch einzig mögliche Alternative. Auch für die mit einer „Schwachstelle" beschriebene Warnung vor dem Funk-Türschlossantrieb des Herstellers ABUS erscheint § 7 Abs. 1 S. 1 Nr. 1 lit. a BSIG somit als grundsätzlich geeignete Ermächtigungsgrundlage für das Handeln des BSI. Daraus folgt, dass die tatbestandlichen Voraussetzungen beider Warnungen rechtlich vergleichbar sein sollten – entscheidend ist somit die juristische Auslegung des Rechtsbegriffs der Sicherheitslücke. Dennoch zeigt der inhaltliche Vergleich beider BSI-Warnungen bei gleicher tatbestandlicher Rechtsgrundlage eine unterschiedliche Argumentationsführung der Behörde auf. Diese stellt sich für die BSI-Warnung vor Antivirus-Produkten des Herstellers Kaspersky im Wesentlichen wie folgt dar: „Virenschutzsoftware, einschließlich der damit verbundenen echtzeitfähigen Clouddienste, ist essenziell 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 den Servern des Herstellers unterhalten. Daher ist Vertrauen in die Zuverlässigkeit und den Eigenschutz des Herstellers sowie seiner authentischen Handlungsfähigkeit entscheidend für den sicheren Einsatz solcher Systeme. ... 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. 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."[13]

Die Begründung des BSI zur Warnung vor der Schwachstelle in einem Produkt des Unternehmens ABUS lautet im Kern wie folgt: „Das BSI hat Erkenntnisse über eine Schwachstelle in dem Produktset Funk-Türschlossantrieb HomeTec Pro CFA3000 und Wireless remote control CFF3000 (Funkfernbedienung für das Produkt CFA3000) erlangt. Das Unternehmen bestätigte die Schwachstelle gegenüber dem BSI und teilte zusätzlich mit, dass die Schwachstelle im Funk-Türschlossantrieb HomeTec Pro CFA3000 (bei dieser Produktgeneration) nicht behoben werden kann, da keine Updatemöglichkeiten für den Kunden bestehen. ... Angreifende können durch diese Schwachstelle die Ver- und Entriegelung des Produkts ... vornehmen, wodurch sich Zugang zu Gebäuden, Büroräumen oder Wohnungen/Häusern verschafft werden kann."[14]

Bei einem inhaltlichen Vergleich der Argumentationsführung des BSI für die Kaspersky-Warnung und die ABUS-Warnung, wobei für erstgenannte die Auslegung des Begriffs der Sicherheitslücke im Eilrechtsschutz gerichtlich bestätigt wurde, ergeben sich zunächst folgende Feststellungen: Obwohl sich äußerlich beide Warnungen als Produktwarnungen darstellen, für die § 7 BSIG grundsätzlich die geeignete Rechtsgrundlage darstellt, argumentiert das BSI für die Kaspersky-Warnung nahezu ausschließlich mit herstellerrelevanten Argumenten, die erst in einem zweiten Schritt auf das Produkt Antivirus-Software durchschlagen, da der Hersteller nicht (mehr) die für das Produkt notwendige Zuverlässigkeit besitzen soll. Die ABUS-Warnung hingegen orientiert sich in ihren inhaltlichen Ausführungen ausschließlich am Produkt Funk-Türschlossantrieb, Aussagen über das Unternehmen selbst und dessen Zuverlässigkeit werden nicht getroffen. So gesehen stellt sich die BSI-Warnung vor Antivirus-Software des Herstellers Kaspersky folglich primär als eine Herstellerwarnung dar, wohingegen es sich bei der ABUS-Warnung primär um eine produktbezogene Warnung handelt.

IV. Produkt- oder Herstellerwarnung: Rechtliche Folgen einer unterschiedlichen Argumentationslinie

Festzustellen ist, welche rechtlichen Folgen diese Erkenntnis für die Auslegung des Rechtsbegriffs der Sicherheitslücke hat. Wie bereits festgestellt, wird die Sicherheitslücke in § 2 Abs. 6 BSIG legaldefiniert als Eigenschaft 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. Wie ebenfalls dargelegt wurde, ergänzt die Gesetzesbegründung diese Definition um den weiteren Aspekt der „unerwünschten Eigenschaft"[15]. Unerwünscht ist zB eine Eigenschaft eines Programms regelmäßig dann, wenn sie nicht dem Willen seines Nutzers entspricht. Eine formaljuristische Auslegung der Sicherheitslücke legt somit zunächst ein technisches Verständnis selbiger nahe. Fraglich aber ist, ob eine extensive Auslegung der Sicherheitslücke auch die Möglichkeit offenlässt, argumentativ eine primär hersteller- und nicht produkt- oder dienstbezogene Schwachstelle anzunehmen.

Dagegen sprechen zunächst verschiedene Hinweise aus Gesetzesbegründungen im IT-Sicherheitsrecht. Insbesondere der Entwurf zum IT-Sicherheitsgesetz 2.0 referenziert an zahlreichen Stellen auf den Begriff der Sicherheitslücke und konkretisiert damit dessen Auslegung in technischer Hinsicht:

- „Sicherheitslücken im Bereich der Portkommunikation durch Software- und Konfigurationsfehler sind häufig."[16]

11 BSI-Warnung gem. § 7 BSIG: Funk-Türschlossantrieb HomeTec Pro CFA3000 des Herstellers ABUS, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Warnungen-nach-P7_BSIG/2022/BSI_W-005-220810.pdf.

12 VG Köln MMR 2022, 503 (504 f.).

13 BSI-Warnung gem. § 7 BSIG: Virenschutzsoftware des Herstellers Kaspersky, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Warnungen-nach-P7_BSIG/Archiv/2022/BSI_W-004-220315.pdf.

14 BSI-Warnung gem. § 7 BSIG: Funk-Türschlossantrieb HomeTec Pro CFA3000 des Herstellers ABUS, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Warnungen-nach-P7_BSIG/2022/BSI_W-005-220810.pdf.

15 BT-Drs. 16/11967, 12.

16 BT-Drs. 19/26106, 69.

- „Je nach Typ der Sicherheitslücke (des Systemfehlers) kann das gescannte informationstechnische System gegebenenfalls auch ungewollt gespeicherte Daten zurückliefern."[17]
- „Bei einem Honeypot handelt es sich um ein informationstechnisches System, das vom Bundesamt in öffentlichen Netzen betrieben wird und bewusst Sicherheitslücken aufweist."[18]
- „Bei den technischen Befehlen handelt es sich beispielsweise um Programme, die dazu dienen, eine Sicherheitslücke zu schließen ... ."[19]
- „Für bestimmte technische Einrichtungen (z.B. Router, IoT-Geräte) übernimmt der Diensteanbieter bereits heute auch die Verantwortung, dass diese von Sicherheitslücken oder Schadprogrammen bereinigt werden."[20]
- „Hierzu kann es erforderlich sein, dass – wenn die IT-Sicherheit durch eine Sicherheitslücke in der verwendeten Hard- oder Software gefährdet wird – der Hersteller des betroffenen Produkts schnell und nachhaltig zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit beiträgt – etwa durch das zeitnahe Bereitstellen eines Sicherheitspatches."[21]

Offenkundig ist somit, dass auch der Gesetzgeber grundsätzlich von einer technischen Behebbarkeit der Sicherheitslücke ausgeht. Diese Auslegung wird gestützt durch das ebenfalls in der Gesetzesbegründung beschriebene und allgemein genutzte „responsible disclosure"-Verfahren zur Behebung von Sicherheitslücken, dessen Rechtsgedanke sich auch in § 7 Abs. 1a BSIG wiederfindet: „Nach dem in der IT-Wirtschaft geübten Prinzip der verantwortungsvollen Weitergabe („responsible disclosure") werden in der Regel zunächst die Hersteller betroffener Produkte über entdeckte Sicherheitslücken informiert, um diesen Gelegenheit zu geben, Sicherheits-Updates zu entwickeln und ihre Kunden zur Verfügung zu stellen. Dieses Prinzip soll auch iRd § 7 Abs. 1 [BSIG] Beachtung finden."[22]

Die technische Behebbarkeit der Sicherheitslücke wurde mit Blick auf die gerichtliche Argumentation zur Kaspersky-Warnung des BSI jedoch verneint, da es nicht auf das Produkt, sondern auf die faktischen geopolitischen Umstände ankomme, denen der Hersteller ausgesetzt sei. Es wurde vielmehr dargelegt, dass keinerlei durch den Hersteller ergriffenen technischen Maßnahmen ausreichend seien, um das Vertrauen in ihn wieder herzustellen.[23] Diese zur Begründung der Warnung angeführten ausschließlich geopolitischen Umstände sind jedoch gerade keine „Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen", wie durch die Legaldefinition der Sicherheitslücke in § 2 Abs. 6 BSIG vorausgesetzt wird. Erst recht sind sie keine „unerwünschten Eigenschaften", weil sie sich nicht auf den Willen des Nutzers der Antivirus-Software beziehen, sondern von diesem und damit vom eigentlichen Produkt völlig losgelöste Eigenschaften betreffen.[24]

Einer im geopolitischen Sinne weit verstandenen Auslegung der Sicherheitslücke stehen überdies erhebliche rechtssystematische Bedenken entgegen. So ist die Sicherheitslücke im Kontext derjenigen Rechtsvorschriften zu sehen, innerhalb derer sie relevant ist, dh Rechtswirkungen entfalten kann. Hier darf es bei Vorliegen der tatbestandlichen Voraussetzungen nicht zu widersprüchlichen Rechtsfolgen kommen. Im Hinblick auf die vorgenannte Warntätigkeit des BSI ist § 7 BSIG einschlägig. Wie ebenfalls bereits dargelegt wurde, bestimmt sich der gerichtliche Prüfmaßstab für die materielle Rechtmäßigkeit des Handelns des BSI nach § 7 Abs. 1 S. 1 Nr. 1 lit. a BSIG.[25] Hiernach kann das BSI eine Warnung vor Sicherheitslücken in informationstechnischen Produkten und Diensten aussprechen. In der Zusammenschau von § 2 Abs. 6 BSIG und § 7 Abs. 1 S. 1 Nr. 1 lit. a BSIG ergibt sich bei Annahme einer geopolitisch und ausschließlich auf die individuellen Umstände des Herstellers begründeten Sicherheitslücke und damit verbundenen Warnung folgendes Problem: Eine Sicherheitslücke, die ihre Gefährdungsbeurteilung allein aus der besonderen Situation des in Rede stehenden Unternehmens ableitet, kann in der Rechtsfolge bereits nicht zu einer Warnung nach § 7 Abs. 1 S. 1 Nr. 1 lit. a BSIG führen, da sie keine „Sicherheitslücke in informationstechnischen Produkten oder Diensten" darstellt, wie es durch den Wortlaut der Befugnisgrundlage für das BSI jedoch gerade vorausgesetzt wird. Im Hinblick auf die technischen Eigenschaften eines Produkts selbst wird gerade keine abweichende IT-sicherheitsrelevante Aussage getroffen – für den Fall „Kaspersky" bedeutet dies, dass die Antivirus-Software mit ihren beschriebenen und dokumentierten technischen Eigenschaften an sich bestimmungsgemäß und auch dem Erwartungshorizont ihrer Nutzer entsprechend funktioniert. Etwas Anderes wurde bislang weder durch das BSI noch durch die im Eilrechtsschutz befassten Gerichte nachgewiesen oder behauptet. Gestützt wird dieses technische Verständnis des Rechtsbegriffs der „Sicherheitslücke" auch durch das BVerfG in einer entsprechenden Entscheidung: So differenziert das Gericht zwischen N-Day- und Zero-Day-Sicherheitslücken. Die einen sind dem Hersteller bekannt, die anderen nicht – beide sind aber als technische Programmeigenschaften grundsätzlich patchbar.[26]

V. Kritik und Fazit

Diese rechtliche Feststellung bedeutet im Ergebnis, dass nicht nur keine geopolitisch verstandene weite Auslegung der Sicherheitslücke iSv § 2 Abs. 6 BSIG juristisch möglich ist,[27] sondern ebenso eine argumentativ ausschließlich auf den Hersteller und dessen Situation gestützte BSI-Warnung vom gesetzlichen Erlaubnistatbestand des § 7 BSIG nicht gedeckt wird. § 7 Abs. 1 S. 1 Nr. 1 lit. a BSIG ermöglicht nämlich gerade keine allgemeine Herstellerwarnung der Öffentlichkeit, sondern – und dies beschreibt auch der Wortlaut der Vorschrift – ausschließlich eine Warnung vor informationstechnischen Produkten und Diensten. IT-Produkte werden in § 2 Abs. 9a BSIG definiert als „Software, Hardware sowie alle einzelnen oder miteinander verbundenen Komponenten, die Informationen informationstechnisch verarbeiten". Eine ausschließlich herstellerbezogene Regelung findet sich hingegen in § 9b BSIG (Untersagung des Einsatzes kritischer Komponenten, auch bekannt als „lex Huawei"), der unter Einbeziehung des Bundesinnenministeriums wiederum gänzlich andere tatbestandliche Voraussetzungen enthält (zB, ob der Hersteller mittelbar von der Regierung eines Drittstaats kontrolliert wird; einbezogen werden kann laut Gesetzeswortlaut auch dessen Organisationsstruktur) sowie unterschiedliche Rechtsfolgen aufweist und sich ausschließlich auf kritische Komponenten im KRITIS-Sektor bezieht. Eine allgemeine und unterschiedslose Herstellerwarnung durch das BSI ist somit auch nach dieser Vorschrift nicht möglich.

17 BT-Drs. 19/26106, 70.
18 BT-Drs. 19/26106, 71.
19 BT-Drs. 19/26106, 74.
20 BT-Drs. 19/26106, 74.
21 BT-Drs. 19/26106, 90.
22 BT-Drs. 16/13259, 7.
23 S. für sämtliche vorgeschlagenen technischen Maßnahmen zur Ausräumung geopolitischer Bedenken ausf. OVG NRW MMR 2022, 695.
24 So im Ergebnis auch die Erwägungen von Dittrich NJW 2022, 2971 (2973).
25 Zu den einschlägigen tatbestandsmäßigen Voraussetzungen detailliert Ritter (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes: Kommentar zum IT-Sicherheitsgesetz 2.0/Schulte, S. 144 ff.
26 BVerfG ZD 2021, 685 Rn. 7 mAnm Petri – IT-Sicherheitslücken.
27 Dies fälschlicherweise annehmend Shulman/Waidner, Wie Deutschland mit nicht vertrauenswürdiger Informationstechnik besser umgehen kann, F.A.Z. v. 24.10.2022.

Schnell gelesen ...

- Die Sicherheitslücke iSv § 2 Abs. 6 BSIG ist technisch zu verstehen. Eine geopolitisch-strategisch weite Interpretation wird weder durch den Willen des Gesetzgebers noch durch eine formaljuristische und systematische Auslegung gedeckt.
- § 7 Abs. 1 S. 1 Nr. 1 lit. a BSIG ist keine tatbestandliche Grundlage für eine allgemeine Herstellerwarnung durch das BSI, sondern bezieht sich in seinem Wortlaut ausschließlich auf „informationstechnische Produkte und Dienste". Eine andere rechtliche Wertung hätte systemimmanente gesetzliche Widersprüche zur Folge.

Professor Dr. Dennis-Kenji Kipker
ist Mitglied des Vorstands der EAID und Mitherausgeber der MMR.