Leonie Sterz/Christoph Werner/Prof. Dr. Oliver Raabe

Intelligente Verkehrssysteme – IT-Sicherheit in offenen Infrastrukturen Teil 2

Durch die zunehmende Verbreitung offener Infrastrukturen wie beispielsweise Intelligente Verkehrssysteme (IVS) ergeben sich in tatsächlicher und rechtlicher Hinsicht neue Fragestellungen. Nachdem im ersten Teil des Beitrags (RDV 2022, 291) die Rechtslage zur IT-Sicherheit in IVS dargestellt und vereinzelte Probleme angerissen wurden, werden diese im vorliegenden Beitrag vertieft. Hierzu gehört unter anderem die Verteilung der Verantwortlichkeit für die IT-Sicherheit (II.), sowie ein Vorschlag zum Austausch des verteilten Wissens in offenen IVS (III.).

I. Einleitung

Für die IT-Sicherheit von Intelligenten Verkehrssystemen (IVS) sind grundsätzlich sowohl das KRITIS-Recht (BSIG und BSI-KritisV), als auch das fahrzeugspezifi sche Typengenehmigungsrecht (VO (EU) 2018/858) und insbesondere die UN-R 155 und das IVS-spezifi sche Recht (IVS-RL mit ihren delegierten VOen) relevant. Wie im ersten Teil des Beitrags herausgearbeitet wurde, weisen diese drei Rechtsregime Überschneidungen und verschiedene Defizite auf.

In allen Regimen besteht das im ersten Teil des Beitrags dargestellte Problem, dass eine gesetzlich verankerte Methodik zum Umgang mit IT-Sicherheitsrisiken entweder gänzlich fehlt, oder sich die Verweise auf private Normung als unzureichend erweisen. So wurde identifiziert, dass die durch die Risikomethodik zu schützenden Rechtsgüter an-

gepasst sowie die Möglichkeit individueller Risikoakzeptanz ausgeschlossen werden müsste.

Außerdem wurde gezeigt, dass die drei Regelungsregime im Hinblick auf IVS jeweils drei unterschiedliche Adressaten als Verantwortlichen für die Gewähr von IT-Sicherheit aufweisen: Das KRITIS-Recht richtet sich an den Betreiber eines IVS, das Typengenehmigungsrecht ist auf den Fahrzeughersteller zugeschnitten und die IT-Sicherheitspflichten aus der gescheiterten del. VO 2019/1789 adressieren den Betreiber von sog. C-ITS-Stationen. Angesichts der vorherrschenden Unsicherheit in offenen IVS soll der Frage nachgegangen werden, ob einem und wenn ja, welchem Beteiligten die Verantwortlichkeit für eine umfassende Gewähr von Ende-zu-Ende IT-Sicherheit zugeschrieben werden sollte. Hierfür kommt in erster Linie der IVS-Betreiber als Adressat des BSIG in Betracht, da er auch für das funktionale Dienstangebot einstehen muss. Dabei stellen sich aber schon die Fragen, inwieweit dieser tatsächlich vom Anwendungsbereich des BSIG erfasst ist (II. 1., 2., 3.) und ob das die Anwendbarkeit bedingende Schwellenwertkonzept für den offenen und verteilten Charakter des IVS sachgerecht ist (II. 4.).

Insgesamt fehlt in der Risikomethodik zur IT-Sicherheit bisher gänzlich ein sachgerechter Umgang mit der Unsicherheit, die sich daraus ergibt, dass besonders ein offenes, verteiltes IVS eine Vielzahl von sich ständig ändernden Beteiligten haben kann, die gleichzeitig keine Kenntnisse über die Gewährleistung der IT-Sicherheit bei den jeweils anderen beteiligten Rollen haben. Insbesondere kann bislang kein Beteiligter absehen, wie und welche Ereignisse bei anderen Teilsystemen auf die eigenen Systeme einwirken können und welche Schadfolgen umgekehrt die eigenen ggf. korrumpierten Systeme in den anderen Teilsystemen nach sich ziehen können.

Angesichts der bedeutenden betroffenen Schutzgüter bei IVS wie Leben und Gesundheit der Verkehrsteilnehmer/-innen sollte jedoch durch einen Wissensaustausch die Ende-zu-Ende IT-Sicherheit verbessert werden. Hierfür soll unter Abschnitt III. ein Ansatz vorgestellt werden.

Dieser Ansatz ist als Antwort auf die Frage nach der Optimierung der Informationsgrundlagen bei Entscheidungen unter Unsicherheit, mithin nach dem Risikowissen und der Verantwortlichkeit in der IT-Sicherheit, insofern generalisierbar, als zunehmend ein Wandel von geschlossenen Zentralsystemen zu den genannten verteilten und offenen Systemen zu beobachten ist (Systems of Systems). In diesen Fällen ist eine paradigmatische Anpassung der gesetzgeberischen Vorstellungsbilder und der insofern gesetzlich verankerten Methoden und Rollenmodelle vermutlich unumgänglich.

II. Verantwortlichkeit für die IT-Sicherheit in IVS

Der Datenfluss im IVS kann schematisch in die Prozessschritte Erfassung, Übermittlung, Auswertung und Ausgabe eingeteilt werden, wobei es bei jedem Prozessschritt einen oder mehrere Beteiligte geben kann.[1]

Die Daten können durch Sensoren oder Eingabemöglichkeiten von Fahrzeugen, Smartphones oder Smartphone-Apps erfasst werden, aber auch durch Straßeninfrastruktur, die durch die öffentliche Hand oder Private betrieben werden kann. Anschließend werden die Daten durch einen Beteiligten gesammelt und verarbeitet. Dies kann durch Fahrzeughersteller, öffentliche oder private Infrastrukturbetreiber, Smartphone-Hersteller, App-Anbieter oder durch Rundfunkanstalten geschehen. Schließlich werden die verarbeiteten Daten durch den Schritt der Ausgabe nutzbar gemacht. Hierfür kommen beispielsweise das Human-Machine-Interface (HMI) im Fahrzeug, eine automatisierte Reaktion des Fahrzeugs, eine Smartphone-App, vernetzte Verkehrszeichen oder der Rundfunk mit den jeweiligen Verantwortlichkeiten in Betracht. Für die Kommunikation können je nach verwendeter Technologie die Fahrzeug- und Smartphonehersteller, die Infrastrukturbetreiber oder Mobilfunkanbieter relevant sein. Die Beteiligten können einem IVS auch nur temporär beitreten, wodurch die Zusammensetzung der Beteiligten dynamisch ist. Dies ist schematisch in Abbildung 1 dargestellt.

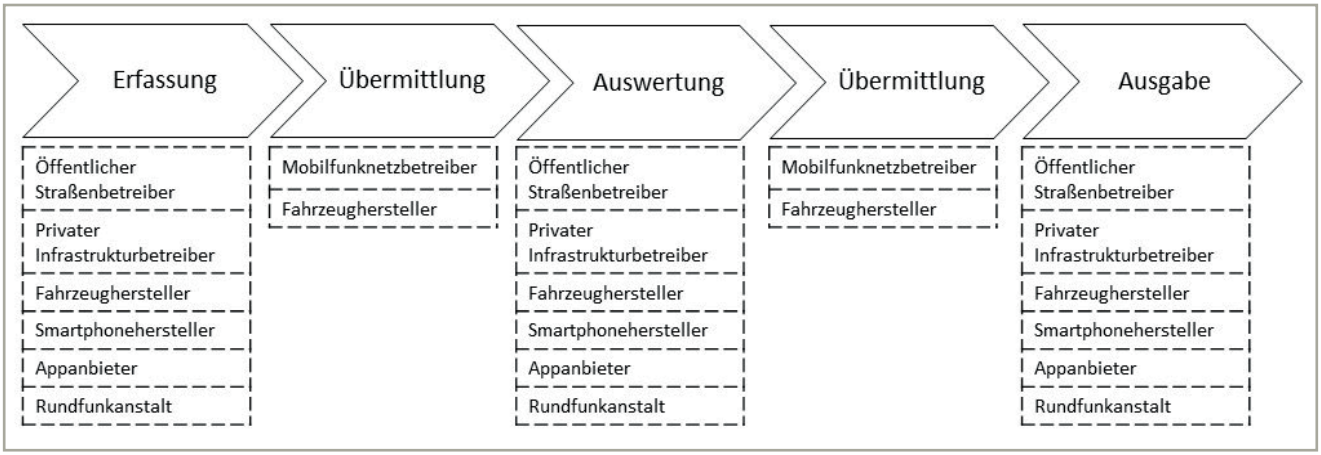

Abbildung 1: Matrix IVS-Beteiligte, angelehnt an BASt, Matrix von Lösungsvarianten Intelligenter Verkehrssysteme (IVS) im Straßenverkehr, Fahrzeugtechnik Heft F 97, S. 18 Bild 11.

Im Folgenden soll die Frage beantwortet werden, welcher dieser Beteiligten nach dem KRITIS-Recht als Betreiber des IVS zu qualifizieren und somit verantwortlich für die Einhaltung der Pflichten nach § 8a Abs. 1 BSIG ist, technische und organisatorische Vorkehrungen zur Vermeidung von Störungen

1 Vgl. BASt, Matrix von Lösungsvarianten Intelligenter Verkehrssysteme (IVS) im Straßenverkehr, Fahrzeugtechnik Heft F 97, S. 8.

der IT-Sicherheit der Anlage zu treffen. Der Betreiber ist nach § 1 Abs. 1 Nr. 2 BSI-KritisV die Person, die einen bestimmenden Einfl uss auf die Beschaffenheit und den Betrieb einer Anlage oder Teile davon ausübt. Dabei sind nur solche IVS-Betreiber adressiert, deren Anlage den Schwellenwert von 500.000 angeschlossenen oder durchschnittlich im Versorgungsgebiet versorgten Nutzer/-innen erreicht.

Um zu klären, welcher Beteiligte im Fall von IVS bestimmenden Einfl uss auf die Anlage ausübt, muss zunächst betrachtet werden, was in einem IVS genau als eine Anlage zu qualifi zieren ist.

1. Anlagenbegriff

Nach der Definition in § 1 Abs. 1 Nr. 1 BSI-KritisV sind Anlagen
a) Betriebsstätten und sonstige ortsfeste Einrichtungen,
b) Maschinen, Geräte und sonstige ortsveränderliche Einrichtungen oder
c) Software und IT-Dienste, die für die Erbringung einer kritischen Dienstleistung notwendig sind.

Im Grunde setzten sich IVS aus Software und Hardware wie Sensoren, Road Side Units (RSUs) oder Ausgabeeinheiten zusammen. Bei offenen, verteilten IVS ist fraglich, ob die für jeden der Prozessschritte Erfassung, Übermittlung, Auswertung und Ausgabe relevanten Bestandteile zu einer Anlage gehören. Dies soll mit Hilfe des bereits im ersten Teil des Beitrags beschriebenen Beispiels eines virtuellen Blaulichts erläutert werden. In diesem Beispiel werden V2X-Nachrichten durch einen Rettungswagen als „virtuelles Blaulicht" ausgesendet,[2] damit betroffene Fahrzeuge und andere Verkehrsteilnehmer/-innen direkt oder durch die Weiterleitung über RSUs[3] über das HMI eine Warnung erhalten. Weiterhin könnten diese Nachrichten auch über entsprechende Server auf Smartphones betroffener Fußgänger- und Radfahrer/-innen übertragen werden. Hierdurch ist diesen gegebenenfalls schneller eine Reaktion möglich als dies bei einer Warnung durch das analoge Blaulicht der Fall gewesen wäre.

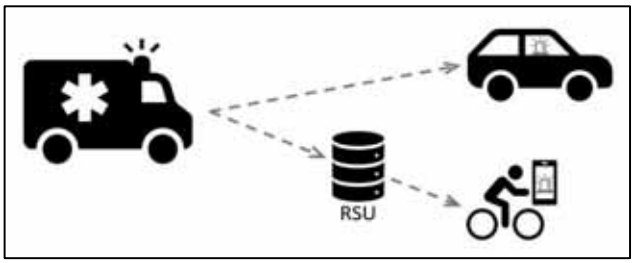

Abbildung 2: Instanz eines Virtuellen Blaulichts

Es stellt sich sodann die Frage, ob sowohl der Rettungswagen, der das virtuelle Blaulicht als V2X-Nachricht erstellt (Erfassung), die im Fahrzeug verbaute Funktechnik (Übermittlung) als auch ein beteiligter Server (Auswertung) sowie die Endgeräte einschließlich der empfangenden Fahrzeuge (Ausgabe) eine einzige Anlage im Sinne des § 1 Abs. 1 Nr. 1 BSI-KritisV darstellen.

Alternativ könnte jedes der Teilsysteme für sich eine Anlage darstellen, sodass das virtuelle Blaulicht aus mehreren Anlagen besteht, die eine gemeinsame Anlage i.S.d. Ziff. 4. Teil 1 Anhang 7 BSI-KritisV darstellen könnten. Dagegen spricht jedoch, dass nur bei einer gemeinsamen Betrachtung aller Teilsysteme die kritische Dienstleistung gefördert wird. Die RSU als solche versorgt nicht die Allgemeinheit mit Leistungen zum Transport von Personen und Gütern (§ 8 Abs. 1 BSI-KritisV) sondern kann ihre fördernde Wirkung auf die kritische Dienstleistung nur im Zusammenwirken mit den anderen Teilsystemen entfalten. Dies streitet dafür, dass das gesamte virtuelle Blaulicht eine einzige Anlage darstellt. Auch der Verordnungsgeber ging von einem weiten Anlagenbegriff aus, indem er sich hierfür am Anlagenbegriff des Immissionsschutzrechts orientierte.[4]

Hinzu kommt, dass auch der Begriff IVS weit verstanden wird und diese eine Anlagenkategorie darstellen. In Ziff. 1.22) des Anhang 7 der BSI-KritisV wird für die Defi nition der Anlagenkategorie IVS auf die Defi nition im IVSG Bezug genommen. Nach § 2 Nr. 1 IVSG werden IVS als Systeme defi niert, bei denen Informations- und Kommunikationstechnologien im Straßenverkehr und an Schnittstellen zu anderen Verkehrsträgern eingesetzt werden. Die Defi nition aus der IVS-RL wurde nur teilweise übernommen, denn dort wird in Art. 4 Nr. 1 klargestellt, dass zum Straßenverkehr sämtliche Infrastrukturen, Fahrzeuge und Nutzer/-innen gehören. Da danach auch Fahrzeuge, in denen IKT eingesetzt werden, zu IVS gehören und diese in vielen Fällen die Rolle des Datenlieferanten einnehmen, spricht dies dafür auch den Anlagenbegriff auf diese zu beziehen und so insgesamt von einem holistischen Anlagenbegriff auszugehen.

2. Bestimmender EinflussaufdasIVS

Zur Begründung der Verantwortlichkeit müsste nach § 1 Abs. 1 Nr. 2 BSI-KritisV ein Betreiber bestimmenden Einfl uss auf die Beschaffenheit und den Betrieb dieser Anlage haben. Ob ein Beteiligter bestimmenden Einfl uss auf die Anlage IVS hat, ist nach dieser Vorschrift anhand rechtlicher, wirtschaftlicher und tatsächlicher Umstände zu ermitteln. Auch für diesen Begriff rekurriert der Verordnungsgeber auf das Verständnis des Immissionsschutzrechts, wonach die Weisungsfreiheit maßgeblich ist, welche regelmäßig mit der tatsächlichen Sachherrschaft einhergeht.[5]

In einem offenen, verteilten IVS hat grundsätzlich jeder Beteiligte einen gewissen Einfl uss auf das IVS, denn sowohl die Prozessschritte Datenerfassung, als auch die Übermittlung und Auswertung der Daten sowie die Ausgabe sind zwingende Voraussetzung für den Dienst. Welche dieser Einfl üsse als bestimmend zu qualifi zieren sind, soll anhand des virtuellen Blaulichts erläutert werden. Dort beeinfl usst zum einen der Hersteller des Rettungswagens die Schritte Erfassung und Übermittlung der Daten, da er die technischen Voraussetzungen für die Fähigkeit des Rettungswagens zum Aussenden der entsprechenden V2X-Nachrichten schaffen muss. Der Halter des Rettungswagens (etwa das Krankenhaus) schafft eine zwingende Voraussetzung für das virtuelle Blaulicht, indem er sich dafür entscheidet, ein Fahrzeug mit der für das virtuelle Blaulicht erforderlichen Technik anzuschaffen. Die jeweiligen Fahrer/-innen des Rettungswagens

2 Zu effektiven Umsetzungsmöglichkeiten von V2X-Nachrichten im Straßenverkehr für Einsatzfahrzeuge siehe Bieker-Walz, Verkehrsmanagement für Einsatzfahrzeuge, S. 15 ff.

3 Zum technischen Aufbau eines Fahrzeug-Ad-hoc-Netzwerks siehe Verma et al., Analysis of Attacks on Vehicular Networks, S. 4 f.

4 Referentenentwurf BSI-KritisV, Stand 13.01.2016, S. 25.

5 Referentenentwurf BSI-KritisV, Stand 13.01.2016, S. 26.

könnten das virtuelle Blaulicht beeinflussen, indem sie den Versand der V2X-Nachrichten ein- oder ausschalten.

Halter- und Fahrer/-innen des Rettungswagens haben zwar einen Einfl uss darauf, ob das virtuelle Blaulicht in einer konkreten Situation aktiviert wird. Art und Weise der Funktion können sie jedoch nicht beeinfl ussen. Damit ist ihr Einfl uss nicht als bestimmend einzuordnen.

Der Rettungswagenhersteller aus dem Beispiel erfasst die Daten und stellt sie zur Übermittlung bereit, wobei er die Zwecke kennt, für die seine Daten durch andere Beteiligte verwendet werden können. Durch die Auswahl der Datenquellen und -formate bestimmt er die Möglichkeiten und Qualität der Ausgestaltung des IVS wesentlich mit. Beispielsweise könnte er die auszusendenden Nachrichten so gestalten, dass auch die Route des Rettungswagens mitgesendet wird, um eine genauere und frühzeitigere Warnung der Verkehrsteilnehmer/-innen zu ermöglichen. Der Beteiligte, der die Daten erfasst, auf denen das IVS basiert, hat somit bestimmenden Einfl uss.

Durch den Prozessschritt der Auswertung fi ndet die Wertschöpfung aus den Daten statt. Der hierfür Zuständige entscheidet unabhängig von den vor- und nachgelagerten Beteiligten, welche Daten er für welche Zwecke sammelt, einschließlich der Auswahl der Datenquellen und der Anforderungen an diese, und wie die Daten verarbeitet werden. Er hat somit einen bestimmenden Einfl uss auf das IVS. So ist im Beispielsfall der Fahrzeughersteller des Pkw derjenige, der entscheidet, ob und wie er die durch den Rettungswagen ausgesendeten Nachrichten verarbeitet. Beispielsweise könnte er den Algorithmus zur Verarbeitung der Daten so gestalten, dass die räumliche Entfernung des Rettungswagens berechnet wird oder die Zeit, die den Fahrer/-innen für eine Reaktion verbleibt.

Zugleich ist der Hersteller des Pkw im Beispielsfall zuständig für den Schritt der Ausgabe an die Nutzer/-innen. Er entscheidet, wie die Informationen an die Nutzer/-innen ausgegeben werden, ob und wie dies durch ein akustisches oder optisches Signal geschieht. Dadurch hat er auch in dieser Rolle einen bestimmenden Einfl uss auf das IVS.

Die V2X-Nachrichten werden je nach verwendeter Technologie beispielsweise durch den Fahrzeughersteller, den Infrastrukturbetreiber oder den Mobilfunkanbieter übermittelt. Diese haben in dieser Rolle jedoch keinen Einfl uss auf den Inhalt der Nachrichten und somit auch keinen bestimmenden Einfl uss auf die Anlage IVS.

Nachdem festgestellt wurde, dass sowohl die an den Prozessschritten Erfassung, Auswertung und Ausgabe Beteiligten Betreiber i.S.v. § 1 Abs. 1 Nr. 2 BSI-KritisV sind, stellt sich die Frage nach der Verteilung der Verantwortlichkeit. Anders als in Outsourcing-Fällen, bei denen der Betreiber IT-Dienstleister einsetzt, was jedoch nichts an seiner Betreibereigenschaft ändert,[6] besteht gerade kein Weisungsrecht eines Beteiligten gegenüber einem anderen. Daher könnten alle Beteiligten als gemeinsame Betreiber einer Anlage i.S.v. § 1 Abs. 2 S. 3 BSI-KritisV gesehen werden. Hierauf wird unter II. 5. genauer eingegangen.

3. Erreichung der Schwellenwerte

Wie oben erwähnt müsste für die Anlage außerdem der entsprechende Schwellenwert überschritten werden, damit sie in den Anwendungsbereich des KRITIS-Rechts fällt. Wie im ersten Teil des Beitrags angedeutet, könnte sich das Erreichen des geforderten Schwellenwerts von 500.000 angeschlossenen oder durchschnittlich im Versorgungsgebiet versorgten Nutzer/-innen bei offenen, verteilten IVS jedoch als schwierig darstellen. Hierbei stellt sich die Frage, wie die Anzahl der Nutzer/-innen von IVS zu bemessen ist.

a) Bemessung der Anzahl von Nutzer/-innen

Die Bemessung der Zahl von Nutzer/-innen in einem IVS soll am Beispiel des virtuellen Blaulichts erörtert werden. Es kommen drei Möglichkeiten für die Zählweise in Betracht.

aa) Möglichkeit 1: Anzahl konkret versorgter Nutzer/-innen

Als erste Möglichkeit könnte entscheidend sein, wie viele Nutzer/-innen im konkreten Fall tatsächlich versorgt sind, wie viele also das virtuelle Blaulicht des einen konkreten Rettungswagens empfangen. Hierfür müssten 500.000 Fahrer/-innen auf der Route des Rettungsfahrzeugs die Nachricht empfangen können. Diese Zahl wird regelmäßig nicht erreicht werden.

Dagegen spricht, dass es auch sonst im KRITIS-Recht nicht darauf ankommt, wie viele Nutzer/-innen oder Haushalte im Moment eines Ausfalls die kritische Dienstleistung gerade verwenden, sondern wie viele im Falle eines Ausfalls betroffen sein könnten.[7] Außerdem ist anders als bei einem Verkehrsschild oder einer Ampel der/die Vorbeifahrende nicht nur Nutzer/-in im Moment des Vorbeifahrens an einem Rettungsfahrzeug, dass das virtuelle Blaulicht aktiviert hat. Vielmehr profitieren die Fahrer:innen dauerhaft von der Funktion des virtuellen Blaulichts , da sie sich auch wenn sich gerade kein Rettungsfahrzeug nähert, auf das Ausbleiben einer Warnung verlassen können. Dieses Vertrauen wird in dem Moment geschädigt, in dem die Fahrer/-innen von einem erfolgreichen Angriff auf das System erfahren.

bb) Möglichkeit 2: Anzahl lokal durchschnittlich versorgter Nutzer/-innen

Als zweite Möglichkeit könnte es darauf ankommen, wie viele Nutzer/-innen in einem konkreten Umkreis durchschnittlich versorgt sind. Das Versorgungsgebiet wäre die Gemeinde oder das Gebiet, für das die mit virtuellem Blaulicht ausgestatteten Rettungswägen eines Krankenhauses zuständig sind. Entscheidend wäre dann die Anzahl der sich durchschnittlich in diesem Gebiet befindlichen Pkw. Weiterhin stellt sich die Frage, ob hierbei nur die Pkw zählen, die das virtuelle Blaulicht auch empfangen können.

Für diese Möglichkeit spricht das dem BSIG zugrundeliegende lokale Verständnis. Wie der Anlagenbegriff in § 1 Abs. 1 Nr. 1a) BSI-KritisV zeigt, geht das Gesetz grundsätzlich von ortsfesten Einrichtungen aus. Zwar gehören zu Anlagen auch ortsveränderliche und ortsunabhängige Einheiten wie Geräte und Software (§ 1 Abs. 1 Nr. 1b, c BSI-KritisV). Wie die Anlagenkategorien beispielsweise im Wasser- oder Energiesektor zeigen (Erzeugungsanlage, Gewinnungsanalage, Aufbereitungsanlage), bestand jedoch ursprünglich die Vor-

6 Hornung/Schallbruch, IT-Sicherheitsrecht, S. 310.

7 Vielmehr ging der Verordnungsgeber von einer Binarität bei der Versorgungssituation aus, vgl. Referentenentwurf BSI-KritisV, Stand 13.01.2016, S. 27.

stellung, dass zentraler Orientierungspunkt die räumlich abgrenzbare Betriebsstätte ist und dieser die ortsveränderlichen und ortsunabhängigen Einheiten und Komponenten zugeordnet werden können. Im vorliegenden Szenario kommt einer abgrenzbaren Betriebsstätte am ehesten das zum Rettungsfahrzeug gehörende Krankenhaus gleich. Dies spräche somit dafür, dass das Versorgungsgebiet des Krankenhauses entscheidend ist.

cc) Möglichkeit 3: Anzahl global potenzieller Nutzer/-innen

Als dritte Möglichkeit kommt die Anzahl der global potenziellen Teilnehmer/-innen in Betracht. Demnach käme es darauf an, wie viele Nutzer/-innen bundesweit Pkw haben, die das virtuelle Blaulicht empfangen können.

Für die dritte Möglichkeit spricht, dass prägend und zentrale Voraussetzung für das virtuelle Blaulicht die in den Pkw verbaute Software ist (Zentralität durch Software). Die Pkw müssen nicht nur in der Lage sein, die V2V-Nachrichten zu empfangen, sondern müssen auch die Nachrichten zu einer optischen oder akustischen Meldung an den/die Fahrer/-in verarbeiten können. Auch für etwaige Plausibilitätsprüfungen und die Überprüfung der Authentizität durch Rückverfolgung des in der Nachricht enthaltenen Zertifikats entlang der Vertrauenskette ist die im Fahrzeug enthaltene Software maßgeblich. Die Software wird durch den Hersteller entwickelt und ist, eventuell mit leichten Abweichungen je nach Version und Variante des Fahrzeugtyps, flottenübergreifend enthalten.

Hieraus ergibt sich, dass sich etwaige Schwachstellen des IVS, die aus einer Schwachstelle in der Fahrzeugsoftware resultieren, nicht nur lokal im Zuständigkeitsbereich eines Krankenhauses, sondern bundesweit über die gesamte Flotte des Herstellers auswirken. Derartige Schwachstellen sollte das KRITIS-Recht daher nicht lokal, sondern bundesweit einheitlich adressieren.

b) Zwischenfazit

Da durch eine flottenübergreifende Behebung von Schwachstellen am effektivsten eine Ende-zu-Ende IT-Sicherheit erreicht werden kann, vermag die dritte Möglichkeit am ehesten zu sachgerechten Ergebnissen zu führen.

Unabhängig vom Ergebnis der obigen Diskussion über die Bemessung der Zahl von Nutzer/-innen eines IVS konnte jedenfalls gezeigt werden, dass sich die Bemessung anhand der bestehenden rechtlichen Kriterien als schwierig gestaltet. Es stellt sich daher die Frage, ob das Schwellenwertkonzept de lege lata, welches nur systemische Effekte zentraler Systeme reflektiert, überhaupt ein geeignetes Kriterium für die Kritikalität von IVS darstellt und ob nicht auch IVS, die die Schwellenwerte nicht erreichen, als kritische Infrastruktur qualifiziert werden sollten.

4. Exkurs: Schwellenwertkonzept als geeignetes Kriterium für die Kritikalität von IVS?

Die Kritikalität eines Dienstes wird nach § 2 Abs. 10 BSIG grundsätzlich nach der Bedeutung für das Funktionieren des Gemeinwesens bemessen. Der Schwellenwert ist dabei nach § 10 Abs. 1 BSIG derzeit das Maß für den als bedeutend anzusehenden Versorgungsgrad. Bei der Bestimmung der Kritikalität ist es wichtig zwischen dem Dienst und der sog. „kritischen Infrastruktur“ zu differenzieren. Anknüpfungspunkt für die Kritikalität im Sinne des Potenzials schwerer Folgen bei einem Ausfall ist im KRITIS-Recht stets der Dienst selbst, nicht die dahinterstehende Infrastruktur.[8] Das Ziel von Interventionen ist daher die Verhinderung von Ausfällen oder Beeinträchtigungen der Dienste, um daraus folgende erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit in den betreffenden Sektoren zu verhindern.[9]

Nun kann die Kritikalität eines Dienstes sowohl systemischer als auch symbolischer Natur sein.[10] Systemische Kritikalität zeichnet sich durch das sich aus der infrastrukturellen Vernetzung ergebende Potenzial von Kaskadeneffekten aus.[11] Das Schwellenwertkonzept und die Betonung des bedeutenden Versorgungsgrades in § 2 BSIG zeigen, dass das BSIG mit dem technischen Kriterium der großflächigen statischen Vernetzung primär auf die systemische Kritikalität abzielt.[12] Aber auch auf der Folgenseite, welche die gesellschaftliche Ebene der Kritikalität umfasst, wird durch das mit dem Schwellenwertkonzept mittelbar verknüpften Merkmal des „erheblichen Versorgungsengpasses“ ein eher quantitatives Kriterium bemüht, mithin auf die systemischen Auswirkungen im Sinne der Anzahl nicht (mehr) versorgter Nutzer/-innen abgestellt.

Die symbolische Kritikalität wird häufig anknüpfend an o.g. Missverständnis als das Vertrauen in Infrastrukturen an sich interpretiert.[13] Dieses Vertrauen sei besonders hoch, soweit diese Infrastrukturen „kulturelle oder identitätsstiftende Bedeutung“ innehätten und „ihre Zerstörung eine Gesellschaft emotional erschüttern und psychologisch nachhaltig aus dem Gleichgewicht bringen“ könne.[14] Der Vertrauenstatbestand ist aber im KRITIS-Recht tatsächlich nicht auf eine bestimmte Infrastruktur, sondern auf die ständige Verfügbarkeit eines Dienstes bezogen.[15] Wird dieses Vertrauen erschüttert, so sind die Nutzer/-innen gezwungen, Alternativen zur Nutzung der Dienste zu finden. Im Falle des virtuellen Blaulichts würde dies etwa dazu führen, dass die Nutzer/-innen sich nicht mehr auf dieses verlassen könnten und wieder verstärkt selbst den Verkehr beobachten müssten. Im Falle unauthentischer Blaulicht-Meldungen könnte dies sogar zu einer Ignoranz des Dienstes führen.

8 So aber mit einem erweiterten Verständnis von kritischen Infrastrukturen: BMI, Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), 2009, S.5.

9 Insofern ist die Terminologie der BSI-KritisV zutreffend, wenn in § 1 Abs. 1 Nr. 2, 3 von Betreibern von Anlagen, die zur Erbringung der kritischen Dienstleistung notwendig sind, gesprochen wird; demgegenüber ist die Terminologie Betreiber kritischer Infrastrukturen in § 8a BSIG ungenau.

10 BMI, Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), 2009, S.5; Metzger, Das Konzept “Schutz kritischer Infrastrukturen” hinterfragt in: Bulletin 2004 zur schweizerischen Sicherheitspolitik, S. 73, 77; wobei auf die Kritikalität der Infrastruktur und nicht des Dienstes abgestellt wird, hierzu sogleich.

11 BMI, Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), 2009, S.5; Metzger, Das Konzept “Schutz kritischer Infrastrukturen” hinterfragt in: Bulletin 2004 zur schweizerischen Sicherheitspolitik, S. 73, 77; Folkers, Was ist kritisch an kritischer Infrastruktur? S. 133.

12 Vgl. Folkers, Was ist kritisch an kritischer Infrastruktur? S. 132 f.

13 BMI, Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), 2009, S.5; Metzger, Das Konzept „Schutz kritischer Infrastrukturen“ hinterfragt in: Bulletin 2004 zur schweizerischen Sicherheitspolitik, S. 73, 77; Folkers, Was ist kritisch an kritischer Infrastruktur? S. 133.

14 BMI, Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), 2009, S. 5.

15 Etwa das Vertrauen in die Verfügbarkeit von Strom, nicht in die Unversehrtheit eines (einzelnen) Kraftwerks.

Insofern stellt sich aber die Frage, ob dieser Fokus des BSIG auf systemische Kritikalität mit dem Aufkommen zunehmend verteilter, offener Systeme, die teilweise die geschlossenen Zentralsysteme klassischer KRITIS substituieren oder mit ihnen temporär verschmelzen, noch allein zukunftsfähig ist. Dies ergibt sich daraus, dass die Gefahren emergenter Effekte erfolgreicher Angriffe auf die IT-Sicherheit nicht nur technisch in Netzwerken vermittelt werden können. Erfolgreiche Angriffe auf Teilsysteme eines IVS[16] können insbesondere bei physischem Leid der Betroffenen durch branchenweite Vertrauensverluste vergleichbare Effekte zeigen. Diese Vertrauensverluste und die Folgen dezentraler Wirkungen können jedoch durch das Schwellenwertkonzept nicht erfasst werden.

In dem genannten Beispiel des virtuellen Blaulichts könnte ein erfolgreicher Angriff auf die IT zu erheblichen Gefahren für die körperliche Unversehrtheit der beteiligten Akteure führen. Medial vermittelt wäre ein derartiger Vorfall sicher auch für vergleichbare Dienste aus der Vertrauensperspektive nachteilig wirksam, zumal wenn ein entsprechendes Informationssicherheitsmanagement nicht etabliert wäre. Dies zeigt, dass Vertrauensverluste ebenso erhebliche Auswirkungen haben können wie Angriffe, deren Auswirkungen sich durch technische Infrastrukturen großfl ächig ausbreiten.

Hinzu kommt, dass der Schwellenwert von 500.000 Nutzer/-innen der kritischen Dienstleistung auf die Kompensationsfähigkeit einer Anlage abzielt. So ging der Verordnungsgeber der BSI-KritisV davon aus, dass ab 500.000 versorgten Personen der Ausfall einer Anlage nicht mehr durch Notfallkapazitäten wie Feuerwehr, Bundeswehr oder für den Notfall vorgehaltene Systeme, wie beispielsweise ein Notbrunnensystem, kompensiert werden kann.[17] Im Gegensatz zu geschlossenen zentralen kritischen Infrastrukturen kann die Dienstleistung eines offenen, verteilten IVS nicht kompensiert werden. Dies zeigt sich auch beim virtuellen Blaulicht: fällt dieses IVS aus, würde man allenfalls auf bisherige, analoge Systeme zurückfallen, wie etwa das analoge Blaulicht. Hierdurch wird jedoch das eigentliche Ziel des IVS, nämlich die Erhöhung der Straßenverkehrssicherheit durch eine frühere Warnung vor dem nahenden Rettungswagen als bisher, nicht mehr erreicht. Digitale Dienstleistungen sind in der Regel nicht derart durch analoge Mittel kompensationsfähig, wie das bei klassischen analogen kritischen Dienstleistungen, wie beispielsweise der Wasser- oder Energieversorgung, der Fall ist.

Insgesamt bestehen somit Zweifel, ob das KRITIS-Schwellenwertkonzept bei der Fortentwicklung zu offenen, verteilten IVS noch schutzgutangemessen ist. Das KRITIS-Schwellenwertkonzept sollte daher überdacht und auch die symbolische Kritikalität berücksichtigt werden.

5. Zwischenfazit, Rechtsfolge und Kritik

Die Begründung einer Verantwortlichkeit für das gesamte IVS nach dem KRITIS-Recht erweist sich als schwierig. Im Beispielszenario kommen als Betreiber die für die Prozessschritte Erfassung, Auswertung und Ausgabe Beteiligten in Betracht. Zudem wurde dargestellt, dass das Schwellenwertkonzept sowohl in seiner konkreten Anwendung als auch in seiner generellen Zweckmäßigkeit für IVS Zweifel weckt.

Selbst wenn die einzelnen Voraussetzungen vorliegen, erscheint die Rechtsfolge mit dem an den Anlagenbegriff anknüpfenden Rollenmodell zweifelhaft. Wie unter II. 2. erwähnt, könnten die für die Erfassung, Auswertung und Anzeige zuständigen Beteiligten de lege lata als gemeinsame Betreiber zu qualifizieren sein. Dies hätte nach § 1 Abs. 2 S. 3 BSI-KritisV zur Folge, dass jeder Betreiber für die Einhaltung der Pflichten verantwortlich wäre. Unklar bleibt, ob der Verordnungsgeber mit der Einfügung der gemeinsamen Betreiber durch die 2. Verordnung zur Änderung der BSI-KritisV vom 06.09.2021[18] bezwecken wollte, dass jeder Betreiber für die Einhaltung aller Pflichten ähnlich einer Gesamtschuld verantwortlich ist.[19]

Gegen ein solches Ergebnis spricht jedoch, dass dies nicht den tatsächlichen Verantwortungsbereichen entspricht und somit auch nicht sachgerecht ist. Denn auch wenn das Zusammenwirken der Beteiligten für das IVS zwingend notwendig ist, lassen sich die Verantwortungsbereiche klar voneinander abgrenzen. Da ohnehin nur jeder Beteiligte technisch-organisatorische Vorkehrungen für das von ihm beherrschte Teilsystem ergreifen kann, wäre es nicht zweckmäßig, wenn jeder Beteiligte auch für die Pflichten des Anderen verantwortlich gemacht werden könnte.

Zusammenfassend hat damit ein IVS als eine Anlage zwar jedenfalls mehrere Betreiber, diese sollten jedoch nicht für die Pflichten in Bezug auf die anderen Teilsysteme einstehen müssen.[20] Auch wenn dieses Rollenmodell dem BSIG bislang fremd sein sollte, da in klassischen kritischen Infrastrukturen im Falle mehrerer Betreiber diese nach § 1 Abs. 2 BSI-KritisV wohl stets gemeinsame Betreiber sind, erscheint diese Auslegung für das Sachphänomen der offenen und verteilten IVS für eine bestmögliche Ende-zu-Ende IT-Sicherheit sachgerecht.

Dies entspricht auch mehr dem Gedanken von Annex 4 des Entwurfs für die del. VO 2019/1789, wonach jeder Betreiber einer C-ITS Station ein ISMS betreiben muss (s. im ersten Teil des Beitrags). Dem liegt der Gedanke zugrunde, dass die Absicherung jedes einzelnen Teilschritts eines IVS automatisch die Ende-zu-Ende Sicherheit mit sich bringt. Bei einer isolierten Verantwortlichkeit jedes einzelnen Beteiligten darf jedoch nicht wie in der der del. VO 2019/1789 die Perspektive des Gesamtsystems und etwaige Abhängigkeiten und Wechselwirkungen der Teilsysteme untereinander außer Acht gelassen werden. Dies schließt insbesondere ein, dass die im Beitrag bereits angedeuteten Wissensdefizite durch eine geeignete Methodik ausgeglichen werden.

III. Ansatz für eine Ende-zu-Ende Sicherheit

Grundsätzlich sind für die Risikobetrachtung und Maßnahmenwahl durch ein ISMS Kenntnisse über die Eintrittswahrscheinlichkeit von potenziell schädigenden Ereignissen sowie über die schädlichen Auswirkungen eines Ereignisses erforderlich.

Durch die zunehmende Verbreitung von offenen IVS ist das für eine umfassende Risikobetrachtung erforderliche Wissen zu Schadereignissen und Schadfolgen unter den verschiedenen Beteiligten verteilt. Zugleich muss dieses verteilte Wissen in einer einheitlichen, dem normativen Schutz-

16 Vgl. zu den Arten von Angriffen Verma et al., Analysis of Attacks on Vehicular Networks, Appl. Sci. 2021, 11, 4682.

17 Referentenentwurf BSI-KritisVO, Stand 13.01.2016, S. 28.

18 BGBl. 2021, 4163.

19 So Bitkom, Stellungnahme zur Änderung der BSI-Kritisverordnung, 17.05.2021, S. 4.

20 Sollte § 1 Abs. 2 S. 3 BSI-KritisV dahingehend auszulegen sein, ist eine entsprechende teleologische Reduktion vorzunehmen.

auftrag angemessenen Methodik zusammengeführt und zur Risikominderung durch technisch-organisatorische Maßnahmen von sämtlichen Beteiligten verwendet werden, um trotz der dezentralen Struktur des IVS auch Ende-zu-Ende Sicherheit zu gewährleisten.

1. Wissensdefizite

Das vorgenannt beschriebene Problem der Wissensdefi zite weist einen im bestehenden Rechtsrahmen normativ angelegten und einen tatsächlichen Anteil auf: Der produktbezogene Fokus im Typengenehmigungs- und IVS-Recht erweist sich als unzureichend, weil er den Blick auf die Schädigung einzelner Komponenten des IVS lenkt und schädigende Folgewirkungen in den anderen Komponenten des IVS ausblendet. Ein umfassender Dienstbegriff (wie im KRITIS-Recht) muss hingegen immanent alle Systembestandteile und soziotechnischen Faktoren in den Untersuchungsbereich von Risikobewertungen aufnehmen, die für die Diensterbringung notwendig sind. Gerade in einem verteilten System wie dem IVS kann aber hinsichtlich der tatsächlichen Fähigkeit der verantwortlichen Akteure ein solch normativer Appell einer umfassenden Prüfung von Ereignissen und Folgen bei allen an der Diensterbringung beteiligten Teilsystemen faktisch ins Leere laufen. Dies lässt sich wie folgt illustrieren.

Die tatsächliche Verteilung der Wissensbestände um Ereignisse und deren Schadfolgen wird besonders bei einer Betrachtung der o.g. Prozessschritte Erfassung, Übermittlung, Auswertung und Ausgabe deutlich. Für jeden Teilschritt kann wie oben dargestellt ein anderer Beteiligter verantwortlich sein, der lediglich Wissen über die Wahrscheinlichkeit potenziell schädigender Ereignisse und Auswirkungen in Bezug auf sein Teilsystem hat.

Ein potenziell schädigendes Ereignis kann in allen Prozessschritten auftreten und sich auf alle darauffolgenden Schritte auswirken. Hier kommt es darauf an, inwiefern ein Schritt das potenziell schädigende Ereignis aus einem vorherigen Prozessschritt abfangen kann, sodass es sich nicht auf die darauffolgenden Schritte auswirkt. Der tatsächliche Schaden wird erst durch den letzten Prozessschritt, die Ausgabe und die damit verbundene Verhaltenssteuerung der Nutzer/-innen unmittelbar verursacht. Hieraus ergibt sich, dass für ein Ende-zu-Ende Risikomanagement Wissen um Schadereignisse und -folgen aus allen Prozessschritten erforderlich ist.

Wie gezeigt wurde, adressieren die bisherigen Regelungen für die Schutzmaßnahmen hingegen stets nur eine Teilmenge der Beteiligten am IVS und verlangen (zumindest im Fall fehlenden Wissens über Auswirkungen auf andere Teilsysteme) von ihnen lediglich, die unmittelbaren Auswirkungen auf ihre Teilsysteme zu betrachten. Der Beteiligte, der die Daten erfasst, kann derzeit nur vom Datumstyp auf die potenziellen Verwendungsmöglichkeiten und damit auf die potenziellen Auswirkungen eines schädigenden Ereignisses schließen. Allerdings bieten viele Datentypen zu vielfältige Verwendungsmöglichkeiten, als dass Auswirkungen antizipiert werden könnten. Beispielsweise können Standort- und Geschwindigkeitsdaten sowohl für ein IVS wie das virtuelle Blaulicht mit entsprechend hohen betroffenen Schutzgütern als auch für ein Parkleitsystem mit vergleichsweise geringen betroffenen Schutzgütern verwendet werden. Kennt ein IVS-Beteiligter aber die betroffenen Schutzgüter nicht, kann er den nächsten Schritt der Abwägung hinsichtlich angemessener Maßnahmen nicht so exakt, wie es mit umfassendem Wissen möglich wäre, durchführen.

Die Beteiligten, die von anderen stammende Daten auswerten oder ausgeben, haben wiederum regelmäßig keine Kenntnisse hinsichtlich der Wahrscheinlichkeit schädigender Ereignisse in den vorhergehenden Prozessschritten. Sie könnten auf die Qualität der verwendeten Daten lediglich anhand von Plausibilitätsprüfungen schließen. Hierdurch ist die Bestimmung des Risikos jedoch nicht so exakt möglich, wie es bei umfassendem Wissen über die Wahrscheinlichkeit von potenziell schädigenden Ereignissen der Fall wäre. Keinem der am IVS Beteiligten und jeweils gesetzlich Adressierten ist daher eine vollständige Risikobetrachtung möglich.

Lediglich die (nicht verbindliche) C-ITS Sicherheitsstrategie verpfl ichtet die Betreiber von C-ITS, andere relevante Beteiligte zu ermitteln, knüpft hieran jedoch keine Maßnahmen. Unter diesen Umständen ist eine Ende-zu-Ende Sicherheit entlang der IVS-Wertschöpfungskette nicht möglich.

2. Methodik zur Ende-zu-Ende Wissensvermittlung

Für eine Ende-zu-Ende IT-Sicherheit muss jedem IVS-Beteiligten auch das Wissen über für ihn nicht ersichtliche Risiken und Schadauswirkungen zur Verfügung gestellt und so entsprechende Wissensdefi zite ausgeglichen werden. Eine hierfür geeignete Methodik muss dabei zwei Herausforderungen bewältigen: Erstens muss ermittelt werden, welcher Beteiligte von wem welches Wissen benötigt. Denn während in bisherigen IVS in der Regel feste, langwierige Verträge bestehen, sodass sich die Beteiligten bereits kennen, wird dies in zukünftigen offenen IVS nicht der Fall sein.[21] Wie oben dargestellt weiß der Fahrzeughersteller, dessen Fahrzeuge periodisch V2X-Nachrichten aussenden, nicht immer, wer diese Daten empfängt und für welche Zwecke er sie weiterverarbeitet.[22] Zudem kann sich dies zeitlich schnell ändern: je nachdem, wo das Fahrzeug fährt, empfangen andere Straßenbetreiber die Daten durch RSUs und verarbeiten sie unter Umständen zu anderen Zwecken.

Zweitens muss das Wissen zwischen den ermittelten relevanten Betreibern ausgetauscht werden. Hierbei muss unterschieden werden zwischen dem Wissen, das für das initiale Risikomanagement erforderlich ist und dem Wissen im Falle eines einzelnen Sicherheitsvorfalls.

a) Ermittlung der relevanten Beteiligten

Für eine generelle Erfassung aller potenziell relevanten Beteiligten wäre eine Registrierungspfl icht jedes IVS-Beteiligten denkbar. Hierbei könnten auch Angaben darüber gemacht werden, welche Datentypen in welchem räumlichen Bereich auf welche Art und Weise erfasst, verarbeitet oder ausgegeben werden.[23] Auf dieser Grundlage gäbe es zwei Möglichkeiten, wie die relevanten Beteiligten für eine Prozesskette

21 Vgl. BASt, Matrix von Lösungsvarianten Intelligenter Verkehrssysteme (IVS) im Straßenverkehr, Fahrzeugtechnik Heft F 97, S. 19.

22 Hier nicht näher betrachtet werden soll das sich daraus auch ergebende datenschutzrechtliche Problem der Einhaltung des Zweckbindungsgrundsatzes (Art. 5 Abs. 1 lit. b) DS-GVO) und der Anforderungen an die Einwilligung (nach Art. 4 Nr. 11 DS-GVO muss die Einwilligung u.a. für den bestimmten Fall abgegeben werden).

23 Die Normierung einer solchen Berichtspflicht könnte sich an § 12 Abs. 3b EnWG orientieren, wonach Betreiber von Übertragungsnetzen gegenüber der Behörde bestimmte Berichtspflichten haben, wobei die Behörde die Berichte zunächst anfordern muss.

ermittelt werden könnten. Entweder könnte jeder Beteiligte selbst die für ihn relevanten Beteiligten identifi zieren, indem er auf die durch die Registrierungs- und Berichtspfl icht erfassten Informationen beispielsweise über eine Datenbank zugreifen kann. Die andere Möglichkeit wäre die Identifizierung der relevanten Beteiligten durch eine Behörde wie beispielsweise die Bundesanstalt für Straßenwesen (BASt), die ihre Ergebnisse den einzelnen Beteiligten mitteilen würde. Dies hätte den Vorteil, dass nicht alle IVS-Beteiligten auf alle Daten zugreifen müssten, wodurch dem Interesse an der Geheimhaltung von Geschäfts- und Betriebsgeheimnissen besser Rechnung getragen werden könnte.[24]

b) Wissensaustausch

Für den Wissensaustausch im Rahmen des initialen Risikomanagements müsste eine Kooperation aller an einer IVS-Prozesskette Beteiligten erfolgen. Neben eines Wissensaustauschs durch gemeinsame Gespräche käme insbesondere der Wissensaustausch durch den Zugriff auf eine Datenbank in Betracht.[25]

Hinsichtlich einer Datenbank gäbe es verschiedene Gestaltungsmöglichkeiten. Die Betreiberrolle könnte entweder durch die Behörde oder eine unabhängige dritte Partei, wie einem Datenintermediär als treuhänderischen Verwalter, erfüllt werden.[26] Die Daten könnten die IVS-Beteiligten selbst eintragen und bearbeiten oder dies könnte dem Datenbankbetreiber vorbehalten sein. Es könnte ein Informationsauskunftsanspruch eines IVS-Beteiligten normiert werden.[27] Ein Zugriff könnte auch davon abhängig gemacht werden, dass ein IVS-Beteiligter zunächst selbst Informationen teilt.

Hinsichtlich des Wissensaustausches in Bezug auf einzelne Angriffe oder Sicherheitslücken kommen insbesondere Meldepflichten[28] oder -möglichkeiten in Betracht. Dies schließt insbesondere Wissen über Sicherheitslücken, erfolgte Angriffe, deren Auswirkungen und ggf. bereits getroffene Maßnahmen mit ein.[29] Auch das in den Meldungen enthaltene Wissen könnte über die bereits für den Wissensaustausch für das initiale Risikomanagement verwendete Datenbank erfolgen. Hier muss stets eine Abwägung zwischen der Nützlichkeit der Information für das Risikomanagement der anderen IVS-Beteiligten und der Gefahr der Ausnutzung der Informationen durch Angreifer erfolgen. Aus diesem Grund sollten die Informationen erst nach der Überprüfung durch den Betreiber der Datenbank freigeschaltet werden.

3. Verwendung des Wissens

Das durch den Austausch erlangte Wissen muss jeder Beteiligte auch in seiner Risikobetrachtung und -bewältigung verwenden, anderenfalls würde der Wissensaustausch ins Leere führen. Hierfür muss der Beteiligte das Wissen über die Wahrscheinlichkeit von Schadereignissen sowie über die Auswirkungen in seine Maßnahmenwahl einfließen lassen. Dies impliziert, dass das Wissen nicht nur bei der initialen Maßnahmenwahl berücksichtigt wird, sondern auch neues Wissen über die kontinuierliche Überprüfung und Verbesserung der getroffenen Maßnahmen im Rahmen der Risikomethodik in die Maßnahmenwahl einfl ießen kann.

Hierdurch entsteht letztlich eine dauerhafte Kooperation zwischen den Beteiligten. Dies führt am Ende nicht nur zu einer Erhöhung des insgesamten Sicherheitsniveaus, da zusätzliche Risiken berücksichtigt werden können, vielmehr wird auch die Effektivität der Bewältigung des Gesamtrisikos sichergestellt.

Sofern etwa bei einem Fahrzeughersteller Schwachstellen bestehen und somit beispielsweise eine Korruption der ausgesendeten Daten möglich ist, muss der Dienstanbieter diesem Risiko durch eigene Maßnahmen begegnen (im genannten Beispiel etwa Plausibilitätsprüfungen oder der Abgleich mit anderen Datenquellen). Kann der Fahrzeughersteller hingegen ein hohes Maß an Sicherheit gewährleisten, darf sich der Diensteanbieter auch in höherem Maß auf die Qualität[30] der gelieferten Daten verlassen und kann in der Folge seine eigenen Maßnahmen zumindest reduzieren. Hätte der Diensteanbieter dagegen kein Wissen über die relativ hohe Qualität der Daten des Fahrzeugherstellers, wäre er bei entsprechend hohen Auswirkungen auf Schutzgüter verpflichtet, erhöhte Maßnahmen zu ergreifen. Durch die Verwendung des ausgetauschten Wissens kann somit insgesamt auch dem Prinzip der Verhältnismäßigkeit besser Rechnung getragen werden.

4. Zwischenfazit

Angesichts der vielfältigen Möglichkeiten zur Wissensvermittlung sollten der nationale und der europäische Gesetzgeber diese genau prüfen. Dabei sollten auch die verschiedenen Interessen der Beteiligten wie das Interesse an Wirtschaftlichkeit, am Schutz von Geschäftsgeheimnissen und am Schutz vor Missbrauch des Wissens durch Angreifer sowie IT-Sicherheitsinteressen berücksichtigt werden. Letztlich sollte der Modus der Wissensvermittlung gesetzlich verankert werden, der die Interessen der Beteiligten bestmöglich miteinander in Einklang bringt. Gleichzeitig muss das verfügbare Wissen von allen Beteiligten in einer geeigneten Methodik genutzt werden. Die Wissensvermittlung führt indes nicht zur Annahme einer gemeinsamen Betreibereigenschaft i.S.v. § 1 Abs. 2 S. 3 BSI-KritisV, sondern es bleibt bei den oben dargestellten getrennten Verantwortungsbereichen.

Außerdem sollte über eine Kooperation der relevanten Behörden wie BASt, KBA und BSI[31] nachgedacht werden, um sicherzustellen, dass auch dort das vorhandene Wissen bestmöglich genutzt wird. So ist das KBA aufgrund seines Aufga-

24 Vgl. für eine Lösung des Spannungsverhältnisses zwischen Interesse am Wissensaustausch und sonstige private Interessen § 9 Umweltinformationsgesetz.

25 Hierfür könnten bspw. die über den Nationalen Zugangspunkt nach § 2 Nr. 11 IVSG gesammelten Daten auch auf für die IT-Sicherheit relevante Daten ausgeweitet werden. So wird der Nationale Zugangspunkt bereits auch für die Bereitstellung von Mobilitätsdaten nach dem Personenbeförderungsgesetz verwendet, vgl. § 3a PBefG in Verbindung mit der Mobilitätsdatenverordnung. Der Nationale Zugangspunkt wird durch die BASt im Auftrag des Bundesministeriums für Digitales und Verkehr betrieben. Die sog. Mobilithek soll zukünftig den bisherigen Mobilitätsdatenmarktplatz als Nationalen Zugangspunkt ablösen, vgl. https://mobilithek.info/ABOUT, abgerufen am 15.12.2022.

26 Vgl. für anonyme Daten Selzer/Timm, Potenziale anonymer Datenverarbeitungen nutzen, DuD 2021, 816.

27 Vgl. §§ 3,4 Umweltinformationsgesetz; ähnlich konzipiert sind das Informationsfreiheitsgesetz und das Verbraucherinformationsgesetz.

28 Vgl. bspw. § 4b BSIG.

29 Vgl. Bräutigam/Wilmer, Big brother is watching you? – Meldepflichten im geplanten IT-Sicherheitsgesetz, ZRP 2015, 38, 40 f.

30 Datenqualität umfasst sowohl die Integrität i.S. der Manipulationsfreiheit als auch die „Richtigkeit" i.S. der Übereinstimmung mit der Realität.

31 Eine Verwaltungsvereinbarung zwischen KBA und BSI existiert bereits, https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/KBA-BSI_autonomes-Fahren_121020.html, abgerufen am 15.12.2022.

benbereichs Fahrzeugen als wichtigem IVS-Bestandteil thematisch näher und hat nicht zuletzt wegen Prüfungen nach der neuen UN-R 155 Wissen über mögliche Schwachstellen der Fahrzeuge, die sich auch auf IVS-Dienste auswirken können.

IV. Ausblick

Insgesamt konnten die im ersten Teil aufgeworfenen Fragestellungen vertieft sowie zwei Lösungsvorschläge aufgezeigt werden.

Zunächst wurde dargestellt, dass die Adressierung des IVS-Anbieters als übergreifend für die IT-Sicherheit Verantwortlichen i.S. eines Betreibers einer kritischen Infrastruktur i.S.d. § 2 Abs. 10 BSIG nicht sachgerecht ist. Der Grund dafür ist im Kern, dass das KRITIS-Recht nicht auf offene und verteilte Systeme wie IVS zugeschnitten ist.

Weiterhin hat sich das Konzept der Schwellenwerte für IVS als nicht hinreichend ergeben und sollte deshalb im KRITIS-Recht insbesondere mit Blick auf die symbolische Kritikalität grundsätzlich überdacht werden. Denkbar wäre es, als Alternative neben den Schwellenwerten bestimmte Dienste unabhängig von der Zahl der Nutzer/-innen nach Art und Zweck in den Anwendungsbereich des KRITIS-Rechts einzuschließen. So könnten sowohl zentrale IVS, die der Architektur klassischer Infrastrukturen entsprechen, als auch offene und verteilte IVS wie das virtuelle Blaulicht angemessen erfasst werden.

Eine generelle Abkehr von dem Prinzip starrer Schwellenwerte ist jedoch mit Blick auf die kürzlich verabschiedete 2-RL nicht in Sicht. Danach wird die Festlegung der Schwellenwerte nicht mehr den Mitgliedstaaten überlassen, sondern sektorübergreifend anhand der Beschäftigtenanzahl, die 50 überschreiten, sowie dem Jahresumsatz, der mindestens 10 Mio. EUR betragen muss, vereinheitlicht.[32] Allerdings ist die Anwendbarkeit der NIS-2-RL unter bestimmten Voraussetzungen auch unabhängig von der Erreichung der Schwellenwerte gegeben, insbesondere bei entsprechender Kritikalität der Dienste und deren Auswirkungen auf die öffentliche Sicherheit und Ordnung.[33] Mittelbar kann so, wie unter II. 3. a) cc) vertreten, an die Größe des globalen, potenziellen Kreises von Nutzer/-innen angeknüpft werden (Zentralität durch Software), da bei einer entsprechenden Zahl von Nutzer/-innen die Auswirkungen auf die öffentliche Ordnung, Sicherheit und Gesundheit umso wesentlicher sein können. Auch kann hierdurch bei IVS, die die Schwellenwerte nicht erreichen, eine Anwendbarkeit sachgerecht von der Art des Dienstes abhängig gemacht werden. So können im Einzelfall kritische Dienste erfasst und solche Dienste ausgeschlossen werden, bei denen keine erheblichen Auswirkungen auf die öffentliche Ordnung, Sicherheit oder Gesundheit in Betracht kommen (wie beispielsweise bei Parkplatzleitsystemen).

Zudem ergibt sich aus dem offenen und verteilten Charakter von IVS das Problem einer stark segmentierten Wissensverteilung um Schadereignisse und -folgen. Hierfür wurde eine methodische Lösung angeboten, um bei Überschneidungen in der Risikobetrachtung jedem Beteiligten das hierfür notwendige Wissen zur Verfügung zu stellen. U.a. wurde die Möglichkeit einer treuhänderisch verwalteten Datenbank aufgezeigt.

Der europäische Gesetzgeber sollte daher zumindest nach Inkrafttreten der IVS2-RL eine del. VO zur IT-Sicherheit in C-ITS erlassen. Sofern man sich hierfür an der del. VO 2019/1789 orientiert und auf die ISO 27001 verweist, sollte jedoch der Katalog der Schutzgüter angepasst und die individuelle Risikoakzeptanz ausgeschlossen werden. Außerdem sollte sich der europäische Gesetzgeber auch um eine methodische Implementierung des Wissensaustauschs bemühen. Hierfür spricht auch die staatliche Schutzpflicht: indem der Gesetzgeber die Einführung von IVS fördert, trägt er auch ungewollt zur Erhöhung der IT-Risiken im Straßenverkehr bei. Daraus folgt eine Pflicht zur Kompensation der IT-Risiken, die sich aus Wissensdefiziten ergeben. Dieser Schutzpflicht könnte er nachkommen, indem er eine der oben dargestellten Methodik entsprechende Kooperationspflicht zum Zwecke des Wissensaustauschs erlässt.

Leonie Sterz
arbeitet am ZAR/KIT (Zentrum für an-gewandte Rechtswissenschaft am Karlsruher Institut für Technologie) und forscht schwerpunktmäßig im Datenschutz- und IT-Sicherheitsrecht mit besonderem Fokus auf den Be-reich Smart Mobility.

Christoph Werner
arbeitet am ZAR/KIT (Zentrum für an-gewandte Rechtswissenschaft am Karlsruher Institut für Technologie) und forscht schwerpunktmäßig im Datenschutz- und IT-Sicherheitsrecht.

Prof. Dr. Oliver Raabe arbeitet am ZAR/KIT (Zentrum für an-gewandte Rechtswissenschaft am Karlsruher Institut für Technologie) und forscht schwerpunktmäßig im Daten-schutz- und IT-Sicherheitsrecht mit Querbezügen zur Rechtsinformatik und besonderem Fokus auf den Bereich Smart Mobility.

32 Art. 2 Abs. 1 NIS-2-RL i.V.m. Art. 2 den Anhangs der Empfehlung der EU-Kommission 2003/361/EG.

33 Art. 2 Abs. 2 lit. b)-e NIS-2-RL.