RECHTSWISSENSCHAFTLICHE FAKULTÄT
UNIVERSITÄT DES SAARLANDES

Lehrstuhl
für Rechtsinformatik

Prof. Dr. Christoph Sorge

Postfach 15 11 50
66041 Saarbrücken

Besucheranschrift:
Campus C3 1, Raum 1.25
66123 Saarbrücken

Tel. 0 681 / 302-51 20
E-Mail christoph.sorge@uni-saarland.de
Web www.legalinf.de

Universität des Saarlandes, Postfach 15 11 50, 66041 Saarbrücken

Hessischer Landtag
Innenausschuss
Schlossplatz 1–3
65183 Wiesbaden

Saarbrücken, 9. Mai 2023

Stellungnahme zum Gesetzentwurf der Landesregierung für ein Hessisches Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG)

Für die Gelegenheit zur Stellungnahme zum Entwurf eines Hessischen IT-Sicherheitsgesetz bedanke ich mich. An der Stellungnahme haben die wissenschaftlichen Mitarbeiter Dipl.-Jur. Maximilian Leicht, LL. M. und Dr. rer. nat. Frederik Möllers, LL. M. mitgewirkt.

Die Stellungnahme ist wie folgt gegliedert: Im ersten Teil (vgl. A.) werden übergreifende Aspekte des vorliegenden Gesetzentwurfs diskutiert. Im zweiten Teil (vgl. B.) werden die einzelnen Regelungen thematisiert.

A. Übergreifende Aspekte

Grundsätzlich ist das Anliegen des Landesgesetzgebers begrüßenswert, die IT-Sicherheit der elektronischen Verwaltung zu stärken. Hierfür erscheint die Einrichtung eines Zentrums für Informationssicherheit zweckmäßig. Dies gilt jedenfalls insoweit, wie dieses Zentrum mit entsprechenden, die anderen Stellen des Landes unterstützenden, Eingriffs- und Abwehrbefugnissen ausgestattet wird. Auch die Schaffung eines bzw. einer zentralen Beauftragten für Informationssicherheit kann hierfür zweckmäßig sein.

Die im Folgenden skizzierten, übergreifenden Kritikpunkte sind im Kontext dieser vorangestellten Anmerkung zu begreifen.

I. Fehlende Regelung zu Responsible Disclosure

Der Entwurf befasst sich richtigerweise auch mit dem Umgang mit etwaigen Sicherheitslücken der eingesetzten Programme bzw. IT-Systeme. In diesem Kontext ist es dringend zu empfehlen, ein Verfahren zu sog. Coordinated Vulnerability Disclosure (CVD) zu regeln. Es besteht aus der Perspektive der technischen Fachcommunity Einigkeit, dass die koordinierte Offenlegung von Sicherheitslücken mittels CVD-Prozessen zielführend ist. Die dadurch erst ermöglichte, möglichst weitgehende Beseitigung der Sicherheitslücken ist dabei gesamtgesellschaftlich wünschenswert, sie fördert die IT-Sicherheit sowohl von staatlichen Infrastrukturen wie von privaten Akteuren.[1] Daher erscheint es erforderlich, auch im hier vorliegenden Entwurf eine Regelung zum verantwortungsbewussten Umgang mit IT-Sicherheitslücken aufzunehmen.

Dies gilt auch deshalb, weil die europäische NIS-2-Richtlinie (mehr hierzu vgl. Abschnitt A.II.) ebenso Regelungen zur koordinierten Offenlegung von Schwachstellen enthält. Jedenfalls zwingend erscheint es, zu regeln, dass dem Zentrum für Informationssicherheit bekannt gewordene Sicherheitslücken einem CVD-Prozess zugeführt werden.

Umsetzbar wäre dies etwa durch Regelung einer weiteren Aufgabe des Zentrums in § 5 Abs. 2 des Entwurfs. Das vorsätzliche oder fahrlässige Zurückhalten von Sicherheitslücken bei staatlichen Behörden gilt es angesichts der Auswirkungen auf die gesamtgesellschaftliche IT-Sicherheit sowie angesichts des drohenden Vertrauensverlusts in Bevölkerung und Fachcommunity in jedem Fall zu vermeiden.

II. NIS-2-Richtlinie

Der Unionsgesetzgeber hat kürzlich die sog. NIS-2-Richtlinie[2] erlassen. Die Richtlinie ist von den Mitgliedstaaten bis zum 17.10.2024 umzusetzen. Hierfür dürfte sich auch landesrechtlicher Änderungsbedarf ergeben. Soweit erkennbar, geht der vorliegende Gesetzentwurf bisher nicht auf die durch die NIS-2-RL gestellten Anforderungen ein. Angesichts der Umsetzungsfrist ist dies auch nicht zwingend erforderlich; es sei jedoch an dieser Stelle auf ggf. erforderliche Änderungen angesichts der NIS-2-RL hingewiesen.

---

1 Für einen Überblick zu Relevanz und Status quo des verantwortungsbewussten Umgangs mit IT-Sicherheitslücken vgl. überblicksartig: Oliver Vettermann, Manuela Wagner, Maximilian Leicht und Felix Freiling: Lücken schließen: Der verantwortungsbewusste Umgang mit IT-Sicherheitslücken, bidt Impulse Nr. 5, bidt – Bayerisches Forschungsinstitut für Digitale Transformation, 2023, abrufbar: `https://doi.org/10.35067/b0bj-im05`; sowie ausführlich: Wagner/Vettermann et al., Verantwortungsbewusster Umgang mit IT-Sicherheitslücken, Whitepaper, Schriftenreihe digital | recht – Staat und digitale Gesellschaft, 2023, abrufbar: `https://doi.org/10.25353/ubtr-xxxx-8597-6cb4`.

2 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie).

Insbesondere sollten (hierzu bereits Abschnitt A.I.) die grundsätzlichen Wertungen der NIS-2-RL hinsichtlich der koordinierten Offenlegung von Schwachstellen bzw. IT-Sicherheitslücken berücksichtigt werden. Nach Art. 7 Abs. 1 NIS-2-RL müssen die Mitgliedstaaten jeweils eine nationale Cybersicherheitsstrategie erlassen. Im Rahmen der Strategie muss nach Art. 7 Abs. 2 lit. c NIS-2-RL u. a. ein Konzept für „das Vorgehen bei Schwachstellen, das die Förderung und Erleichterung der koordinierten Offenlegung von Schwachstellen nach Artikel 12 Absatz 1 umfasst“ angenommen werden. Art. 12 NIS-2-RL sieht die koordinierte Offenlegung von Schwachstellen vor, wobei die Mitgliedstaaten hierfür eine Stelle als Koordinator für diese Zwecke festlegen müssen. Der Koordinator soll sodann eine vertrauenswürdige Vermittlerposition einnehmen. Die Normen sehen daher nicht unmittelbar eine Verpflichtung der Behörden zur Teilnahme an CVD-Prozessen vor; sie lassen jedoch die grundsätzlichen Wertungen der NIS-2-RL erkennen.

III. Sonderrolle von Schulen und Stellen nach § 1 Nr. 3 des Entwurfs

Insbesondere § 3 des Entwurfs enthält gestufte Regelungen, welche für die Stellen nach § 1 Nr. 3 – und damit v.a. Behörden und sonstige öffentliche Stellen von Gemeinden und Gemeindeverbänden – sowie Schulen in öffentlicher Trägerschaft sowie genehmigte und anerkannte Ersatzschulen im Sinne des Hessischen Schulgesetzes deutliche Erleichterungen im Vergleich zu Stellen nach § 1 Nr. 1, 2 des Entwurfs bedeuten. Diesen Stellen werden die in § 3 Abs. 1–4 des Entwurfs geregelten Grundsätze lediglich empfohlen. Gerade bei Behörden der Gemeinden und Gemeindeverbände sowie bei Schulen werden jedoch sensible personenbezogene Daten verarbeitet. Die Absicherung der IT-Infrastruktur sowie der Arbeitsfähigkeit dieser öffentlichen Stellen ist daher zentral.
Es ist daher zu begrüßen, dass diese Stellen im Aufgabenkatalog des Zentrums für Informationssicherheit in § 5 Abs. 2 des Entwurfs ausdrücklich adressiert werden. Dennoch empfiehlt es sich, zeitnah zu evaluieren, ob die reine Empfehlung der Einhaltung der Grundsätze zielführend ist oder ob der Empfehlung zusätzliche, ggf. auch finanzielle Regelungen zur Seite gestellt werden sollten.

IV. Privatnutzung und BYOD

In der Praxis kann die Privatnutzung dienstlicher Geräte und umgekehrt die dienstliche Nutzung mitgebrachter Geräte („Bring your own device, BYOD“) erhebliche Auswirkungen auf die Sicherheit eines Datennetzes haben. Sind Privatnutzungen zugelassen, ergeben sich aus der größeren Bandbreite an Nutzungen zusätzliche Sicherheitsrisiken, und rechtliche Wertungen im Rahmen der Auswertung des Datenverkehrs ändern sich. Werden andererseits private Geräte dienstlich genutzt, ist der Zugriff von Systemadministratoren auf die Geräte ggf. eingeschränkt. Beides hat Auswirkungen auf die im Entwurf jedenfalls implizit angelegte Entschlüsselung verschlüsselten Datenverkehrs; ohne administrativen Zugriff

auf den Kommunikationsendpunkt wird dieser sogar unmöglich (vgl. dazu die Ausführungen zu § 9 in Abschnitt B.VII., S. 9). Diese Problematiken erfordern nicht zwingend eine gesetzliche Regelung, sind jedoch bei der praktischen Anwendung des Entwurfs zu berücksichtigen.

V. Einbeziehung zusätzlicher Kontrollmechanismen

Angesichts der – insbesondere durch das Aufbrechen verschlüsselter Verbindungen – teilweise tiefen Eingriffe und des potentiellen Missbrauchpotentials der geregelten Befugnisse wäre es überlegenswert, eine explizite Kontrolle durch Personalvertretungen oder behördliche Datenschutzbeauftragte vorzusehen.

B. Aspekte ausgewählter Regelungen

I. Zu § 1

Der Begriff der elektronischen Verwaltungstätigkeit ist im vorliegenden Entwurf nicht definiert. Jedenfalls kann der Begriff so verstanden werden, dass nur die IT-bezogenen Aspekte der Informationssicherheit geregelt werden sollen. Risiken für die Informationssicherheit gibt es aber auch bei noch nicht bzw. nicht vollständig digitalisierten Prozessen (etwa den nachlässigen Umgang mit Papierakten). Es wäre daher zu erwägen, diese Prozesse in den Anwendungsbereich des Gesetzes mit einzubeziehen.

II. Zu § 2

Die Definitionen orientieren sich an denjenigen aus § 2 BSIG. Dies ist aus Sicht des Rechtsanwenders zu begrüßen. Es fehlt jedoch eine Definition des Begriffs „Landesdatennetz“. Da an anderer Stelle darauf Bezug genommen wird, sollte eine solche Definition noch ergänzt werden. Sie könnte sich an der Definition orientieren, die in der Begründung zu § 12 Abs. 1 (S. 29 des Dokuments) zu finden ist.

Zu den einzelnen Definitionen ist Folgendes anzumerken:

- Nr. 2: Die Definition nimmt Bezug auf Informations*technik*, wohingegen Sicherheitsprobleme auch außerhalb der IT auftreten. Die Bezugnahme auf Prozesse erweitert den Begriff, nicht digitalisierte Prozesse werden aber nach hiesigem Verständnis nicht erfasst (vgl. Bemerkung zu § 1). Erwägenswert wäre außerdem die Einbeziehung weiterer Schutzziele neben Verfügbarkeit, Integrität und Vertraulichkeit; allerdings wären keine großen praktischen Auswirkungen zu erwarten.

- Nr. 5: Der Begriff „anderes Netz“ ist aus technischer Sicht nicht scharf definiert. Was ein anderes Netz ist, ist eine Frage der Perspektive, da Netze hierarchisch unterteilt sein können – aus einer Außenperspektive könnte etwa ein Universitätsnetz als „ein Netz“ angesehen werden, wohingegen aus einer Binnensicht von verschiedenen Netzen der Fakultäten und Lehrstühle gesprochen werden könnte. Die Begründung stellt klar, dass auch Übergänge zwischen virtuellen Netzen (gemeint sind wohl sogenannte VLANs – Virtual Local Area Networks, bei denen die Trennung zwischen verschiedenen lokalen Netzen nicht physisch, sondern auf gemeinsamer Hardware hergestellt wird) erfasst sein sollen. Eine Präzisierung im Normtext wäre aber wünschenswert.
- Nr. 6: Die in der Begründung wiedergegebene Definition entspricht nicht derjenigen des Normtexts; es liegt nah, dass eigentlich die Begriffsdefinition aus der Begründung gemeint ist. In diesem Fall wäre eine Anpassung des Gesetzestextes zwingend. Zum Vergleich: § 2 Abs. 8 und 8a BSIG führen eine Unterscheidung zwischen Protokolldaten (definiert wie in § 2 Nr. 6 des vorliegenden Entwurfs) und Protokollierungsdaten („Aufzeichnungen über technische Ereignisse oder Zustände innerhalb informationstechnischer Systeme“) ein. Der Begriff der Protokolldaten umfasst auch in großem Umfang Daten, die typischerweise nicht protokolliert werden. Gleichzeitig ist der Begriff sehr breit, da bei Kommunikationsvorgängen in der Praxis immer mehrere Protokolle in verschiedenen Schichten[3] ablaufen; die Sensibilität in verschiedenen Protokollen anfallender Protokolldaten kann sehr unterschiedlich sein.
  Umgekehrt können Protokollierungsdaten sich auch auf Vorgänge außerhalb eines Kommunikationsprotokolls beziehen. Eine Differenzierung zwischen Protokoll- und Protokollierungsdaten in Anlehnung an das BSI-Gesetz wäre daher sinnvoll. Insbesondere scheint der Gesetzentwurf den Begriff „Protokolldaten“ zu verwenden, wenn sich die folgenden Regelungen jedoch sinnvollerweise auf „Protokollierungsdaten“ beziehen sollten, vgl. die Stellungnahme zu § 8 in Abschnitt B.VI., S. 8.

III. Zu § 3

Die in § 3 Abs. 1 des Entwurfs getroffene Regelung, die eine Orientierung an der IT-Grundschutzmethodik des BSI vorsieht, ist zu begrüßen. Der IT-Grundschutz enthält etablierte und regelmäßig aktuell gehaltene Schutzmaßnahmen. Eine vollständige Umsetzung dürfte jedoch nicht in jedem Fall gleichermaßen zielführend sein, sodass die grundsätzliche Orientierung sinnvoll ist. Sie lässt den Normadressaten angemessenen Freiraum, pragmatisch davon abzuweichen. Dies gilt gerade für die Einführung eines Informationssicherheitsmanagementsystems, welches je nach Größe der Stelle in unterschiedlicher Ausprägung sinnvoll sein dürfte – ohne, dass hiermit eine Absenkung des Schutzniveaus verbunden sein muss.

[3] Nach Schichtenmodellen der Kommunikation wie dem TCP/IP-Modell.

§ 3 Abs. 1 S. 2 des Entwurfs – nach dem der Stand der Technik für technische Maßnahmen „maßgeblich“ sein „soll“ – lässt jedoch Interpretationsspielraum zu: *Müssen* die Maßnahmen dem Stand der Technik *entsprechen*? *Muss* der Stand der Technik nur – vergleichbar zu Art. 32 DSGVO – gemeinsam mit anderen Kriterien *berücksichtigt* werden? Vorschriften über die Informations- bzw. IT-Sicherheit stellen üblicherweise – so wie hier – ohnehin hohe Anforderungen an die Rechtsanwender, die konkrete Umsetzungsmaßnahmen identifizieren müssen. Daher sollte eine Verstärkung der Rechtsunsicherheit aufgrund unklarer Formulierungen zum Stand der Technik vermieden, mithin eine Klarstellung der Anforderung vorgenommen werden.

Ausdrücklich begrüßt wird, dass § 3 Abs. 3 des Entwurfs die Verantwortung für Informationssicherheit explizit der Leitungsebene zuweist. Damit wird auch in der öffentlichen Verwaltung Informationssicherheit zur „Chefsache“.

Auch die Einbeziehung des Informationssicherheitsbeauftragten bei wesentlichen Änderungen an den IT-Systemen nach § 3 Abs. 3 des Entwurfs ist zu begrüßen. Überlegenswert wäre des Weiteren eine Regelung, nach der jegliche Verringerung des Informationssicherheitsniveaus als „wesentliche Änderung“ gilt.

IV. Zu § 5

Der in § 5 Abs. 2 des Entwurfs geregelte Aufgabenkatalog des Zentrums für Informationssicherheit stellt eine mögliche Stelle dar, an der geregelt werden könnte, dass dem Zentrum bekannte IT-Sicherheitslücken bzw. Schwachstellen einem CVD-Prozess zugeführt werden müssen (vgl. hierzu bereits Abschnitt A.I. auf S. 2).

§ 5 Abs. 3 des Entwurfs wird ausdrücklich begrüßt, insbesondere hinsichtlich der Möglichkeit, dass auch Dienstleistungen für private Stellen ermöglicht werden. Überlegenswert wäre außerdem eine Regelung, welche dem CERT (bzw. dem Zenturm für Informationssicherheit) auferlegt, eine Rolle als erster Ansprechpartner für Cybersecurityvorfälle zu übernehmen. Denkbar wären etwa erste Hilfestellungen für Betroffene von Ransomware-Angriffen. Den Verfassern ist jedoch der IT-Fachkräftemangel sowie die Herausforderungen insbesondere für die öffentliche Verwaltung, geeignete IT-Fachkräfte zu gewinnen, bewusst. Die Anmerkung ist daher unter Vorbehalt einer Prüfung der (vorgesehenen) Kapazitäten im Einzelfall zu verstehen.

V. Zu § 7

Die Begründung zu § 7 des Entwurfs ist fehlerhaft, jedenfalls dürfte die Bezugnahme auf die Absätze des § 7 im Text zu Abschnitt „Zu § 7 (Datenverarbeitung), zu Abs. 1 und 2“ zumindest missverständlich sein.

§ 7 des Entwurfs orientiert sich an § 3a BSIG, welcher erst durch das 2. DSAnpUG-EU neu in das BSIG aufgenommen wurde, um das BSIG an die DSGVO anzupassen. Ebenso wie im BSIG sollen die Abs. 1, 2 der Norm nur gelten, soweit nicht die folgenden, spezielleren Normen (§§ 8 ff. des Entwurfs) die entsprechende Verarbeitung umfassen.

Anders als das BSIG werden die im vorliegenden Entwurf in § 5 definierten Aufgaben jedoch nicht explizit als solche im öffentlichen Interesse bezeichnet, sodass der Verweis in § 7 Abs. 1 des Entwurfs sich insoweit von dem in § 3a Abs. 1 BSIG unterscheidet.

Vergleichbar zu § 3a Abs. 1 BSIG erschöpft sich der Gehalt von § 7 Abs. 1 des Entwurfs in einer unwesentlich abgewandelten Wiederholung des Wortlautes von Art. 6 Abs. 1 lit. e DSGVO.[4] Damit ist § 7 Abs. 1 des Entwurfs allerdings überflüssig und bietet keinen erkennbaren eigenen Mehrwert. Dies gilt insbesondere nach dem kürzlich ergangenen Urteil des EuGH zu § 23 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes[5]. Vergleichbar zur dort relevanten Öffnungsklausel in Art. 88 DSGVO („spezifische Vorschriften“) setzt die hier relevante Öffnungsklausel in Art. 6 Abs. 2, 3 DSGVO voraus, dass „spezifische Bestimmungen“ bzw. „spezifische Anforderungen“ geregelt werden. In Bezug auf Art. 88 DSGVO stellte der EuGH jedoch in der genannten Entscheidung fest, dass es sich nicht um spezifische Vorschriften handelt, wenn lediglich der Wortlaut der DSGVO wiederholt wird.[6]

§ 7 Abs. 2 S. 1 des Entwurfs dürfte angesichts der vergleichsweise niedrigen Anforderungen der Öffnungsklausel in Art. 6 Abs. 4 DSGVO unionsrechtskonform sein. Zweifel können dagegen bei der in § 7 Abs. 2 S. 2 des Entwurfs getroffenen Regelung zu besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO bestehen. Ausweislich der Begründung wird die Norm auf die Öffnungsklausel des Art. 9 Abs. 2 lit. g DSGVO gestützt. Dieser erfordert allerdings u. a., dass das Recht des Mitgliedstaats „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht“. Offenbar um dieses Erfordernis zu erfüllen, verweist § 7 Abs. 2 S. 3 des Entwurfs auf § 20 Abs. 2 S. 2 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes. Ob dies ausreicht, darf allerdings bezweifelt werden. So stellt *Hornung* zurecht fest, dass § 20 Abs. 2 S. 2 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes „dem Rechtsanwender an keiner Stelle spezifischere Handlungsanweisungen gibt als die Verordnung“,[7] und verweist für mögliche Konkretisierungen beispielhaft auf § 17 Abs. 3 des Niedersächsischen Datenschutzgesetzes. Angesichts dieser existierenden Kritik in der Literatur ist dem Gesetzgeber im Hinblick auf den vorliegenden Entwurf zu empfehlen, den Verweis in § 7 Abs. 2 S. 3 zu streichen und durch einen Katalog an spezifischeren Maßnahmen zu ersetzen. Ansonsten droht zum einen ein Verstoß gegen die Anforderungen des Art. 9 Abs. 2 lit. g DSGVO und damit die Unionsrechtswidrigkeit. Zum anderen

---

4 Vgl. zu § 3a BSIG: Brandenburg, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit, § 3a BSIG, Rn. 3, 4.

5 EuGH v. 30.03.2023, Rs. C-34/21, ECLI:EU:C:2023:270.

6 Vgl. EuGH v. 30.03.2023, Rs. C-34/21, ECLI:EU:C:2023:270, Rn. 65, 71.

7 Hornung, in: Roßnagel, Hessisches Datenschutz- und InformationsfreiheitsG, 1. Aufl. 2021, § 20 Rn. 29.

sind spezifischere Maßnahmen auch für die Praxis der Rechtsanwender und den Schutz der Betroffenen zweckmäßiger.

Hinsichtlich § 7 Abs. 5 des Entwurfs verstehen die Verfasser den Gesetzgeber wie folgt: Daten, welche nicht dem Fernmeldegeheimnis unterfallen oder personenbezogen sind, weisen keinen Schutzbedarf auf. Folglich bestehen für solche Daten keine Verwendungsbeschränkungen, etwa hinsichtlich des Zwecks der Verarbeitung dieser nicht schutzbedürftigen Daten. Mit „Verwendungsbeschränkungen“ bezeichnet der Gesetzgeber die Beschränkung der Zwecke, für welche die Daten verarbeitet werden sollen. So ist die Auswertung von Inhaltsdaten – soweit sie personenbezogen sind oder dem Fernmeldegeheimnis unterfallen – im Falle des § 11 Abs. 3 des Entwurfs auf Schadprogramme begrenzt, was nach der Begründung einer möglichen „ausufernden“ Nutzung entgegenwirken soll. Soweit es also (Inhalts-)Daten gibt, die nicht personenbezogen sind und nicht dem Fernmeldegeheimnis unterfallen, so können diese ungeachtet davon verarbeitet werden, ob Schadprogramme, Sicherheitslücken oder eine allgemeine zu erkennende Störung vorliegt. Dieses Verständnis drängt sich nach Auffassung der Verfasser allerdings nicht unmittelbar auf. Es wird daher empfohlen, den Gesetzestext zu konkretisieren, um Rechtsanwender nicht vor zu hohe Hürden zu stellen. Hierfür wäre bspw. eine konkretere Benennung der Verwendungsbeschränkungen hilfreich.

VI. Zu § 8

§ 8 Abs. 1 erlaubt die Auswertung bereits – aufgrund von Rechtsgrundlagen außerhalb des vorliegenden Entwurfs – gespeicherter Protokolldaten. Es ist davon auszugehen, dass tatsächlich nicht (nur) Protokolldaten im Sinne von § 2 Nr. 6 gemeint sind, sondern Protokollierungsdaten, wie sie in § 2 Abs. 8a BSIG definiert sind (vgl. dazu die Stellungnahme zu § 2 Nr. 6). Andernfalls bliebe jedenfalls unklar, welche Protokolldaten der Betriebssoftware von Computersystemen gemeint sein könnten. Die Begründung geht offenbar ebenfalls davon aus, dass auch Log-Dateien ohne direkten Kommunikationsbezug ausgewertet werden können.

In der Praxis könnte sich zudem die Abgrenzung von Protokoll- bzw. Protokollierungsdaten einerseits und Inhaltsdaten andererseits als problematisch herausstellen. Aus Sicht der Telekommunikation bzw. des Betriebs von Kommunikationsnetzen sind Daten der Anwendungsprotokolle wie HTTP etwa bereits Inhaltsdaten, doch werden gewisse Inhalte der HTTP-Kopfzeilen oft in Log-Dateien protokolliert. Auch können Protokolldaten bereits sehr sensibel sein. Da eine separate Rechtsgrundlage für die Speicherung erforderlich ist und zudem § 8 Abs. 1 lediglich eine automatisierte Auswertung erlaubt, ist die Norm insgesamt dennoch sachgerecht.

Denkbar wäre jedoch noch, in § 8 Abs. 1 an die Aufgabendefinition aus § 5 Abs. 2 anzuknüpfen. Dies gilt auch für die folgenden Befugnisse. Überlegenswert wäre jeweils ein

konkreter Verweis auf die einzelnen in § 5 Abs. 2 definierten Aufgaben. Dies könnte die Lesbarkeit des Gesetzes für den Rechtsanwender verbessern.

VII. Zu § 9

Eine explizite Regelung über die Erhebung und Auswertung von Datenverkehr ist zu begrüßen. Allerdings wäre wünschenswert, damit verbundene praktische Schwierigkeiten noch genauer zu berücksichtigen.

In der Praxis ist seit einigen Jahren ein Großteil des Datenverkehrs in Kommunikationsnetzen (transport-)verschlüsselt. Für diesen Zweck kommt das TLS-Protokoll zum Einsatz, das die Kopfzeilen (Header) und Inhalte von Protokollen der Anwendungsschicht schützt. Zu diesen Protokollen der Anwendungsschicht gehört auch das im World Wide Web verwendete HTTP. Folglich wird in § 9 Abs. 1 Nr. 2 auch ausdrücklich HTTPS – die Kombination von HTTP mit TLS – benannt. Aufgrund der Verschlüsselung ist eine Auswertung der Kopfdaten von HTTP und anderen Anwendungsschicht-Protokollen nicht ohne weiteres möglich: Die Verschlüsselung ist gerade dazu bestimmt, die Inhalte vor sämtlichen Auswertungen auf dem Übertragungsweg zu schützen.

Da andererseits eine automatisierte Überprüfung, wie sie in § 9 Abs. 1 vorgesehen ist, oft als notwendig angesehen wird, ist in Unternehmensnetzen ein Aufbrechen verschlüsselter Verbindungen weit verbreitet. Firewalls und ähnliche Systeme erhalten also die Möglichkeit, den Datenverkehr in beide Richtungen zu entschlüsseln, auf Auffälligkeiten zu überprüfen und dann neu zu verschlüsseln. Das ist aufgrund der Sicherheitsgarantien von TLS nur möglich, wenn einer der Kommunikationspartner mitwirkt. Konkret müsste also der im Landesdatennetz befindliche Kommunikationsendpunkt so konfiguriert werden, dass er das Mitlesen durch die Firewall zulässt.[8] Die Folge ist aber, dass scheinbar Ende-zu-Ende-verschlüsselte Kommunikation tatsächlich in Gänze auf dem entsprechenden Firewall-System entschlüsselt werden kann. Auch können neue Sicherheitsrisiken entstehen, wenn das technische Konzept für die Entschlüsselung nicht mit größter Sorgfalt erstellt und umgesetzt wird – denn am eigentlichen Kommunikationsendpunkt im Landesnetz sind Informationen über verwendete Zertifikate des Kommunikationspartners nicht mehr sichtbar. Zusätzliche Schwierigkeiten ergeben sich, wenn Nutzer eigene Endgeräte ins Landesdatennetz einbringen („Bring your own device, BYOD“) oder dienstliche Geräte privat nutzen können (vgl. hierzu bereits Abschnitt A.IV., S. 3).

Das bedeutet nicht, dass das beschriebene Vorgehen per se abzulehnen wäre, denn es sprechen gute Argumente für die Analyse des Datenverkehrs wie in § 9 Abs. 1 beschrieben. Aufgrund der weiten Verbreitung verschlüsselter Kommunikation ist eine solche Analyse

[8] Aus technischer Sicht erhält die Firewall den privaten Schlüssel zu einem Zertifikat, das auf den Rechnern im Landesdatennetz dann als vertrauenswürdiges Stammzertifikat einzurichten wäre. Fortschrittlichere Sicherheitsmaßnahmen, die sich zunehmend verbreiten, erfordern noch weitergehende Anpassungen auf den Endgeräten.

aber kaum sinnvoll, wenn nicht auch verschlüsselte Daten mit einbezogen werden können. Angesichts der weitreichenden Folgen wäre jedoch eine explizite Regelung der Entschlüsselung von Datenverkehr zu empfehlen.

Wünschenswert wäre weiterhin, im Normtext klarzustellen, dass bei der automatisierten Auswertung die Kenntnisnahme durch natürliche Personen auszuschließen ist. Das ergibt sich zwar aus der Begründung, aber jedenfalls nicht selbstverständlich aus dem Begriff.

Im Einzelnen ist weiterhin anzumerken:

- Der in § 9 Abs. 1 Nr. 1 verwendete Begriff des „Netzwerkpakets“ könnte missverständlich sein. In der Fachsprache der Informatik dürfte er sich ausschließlich auf Dateneinheiten der Vermittlungsschicht beziehen – konkret also IP-Pakete, aber ohne Berücksichtigung von Informationen aus anderen Schichten (wie der TCP-Kopf, aus dem also nur Portnummern erhoben werden dürfen). Es könnte aber hilfreich sein, dies klarzustellen.
- Auch wäre in § 9 Abs. 1 Nr. 1 eine Klarstellung hilfreich, dass jeweils beide Portnummern (von Absender- und Empfängerseite eines TCP- oder UDP-Segments) gemeint sind.
- Der in § 9 Abs. 1 Nr. 1 verwendete Begriff der „Statusdaten von Netzwerkpaketen“ ist unklar.
- § 9 Abs. 1 Nr. 1 sieht ebenfalls die Erhebung von Domänennamen vor. Domänennamen können entweder – etwa im Fall von HTTP – aus Kopfzeilen ausgelesen werden oder ein einer IP-Adresse zugeordneter Domänenname durch eine sogenannte Reverse-DNS-Anfrage im Domain Name System aufgelöst werden. Die Aussage beider Varianten ist unterschiedlich. Die Begründung scheint auf die zweite Variante hinzudeuten; die erste ist für den Fall von HTTP von Nr. 2 umfasst. Eine Klarstellung im Normtext könnte für den Rechtsanwender aber jedenfalls hilfreich sein.
- § 9 Abs. 1 Nr. 1 sieht die Erhebung von MAC-Adressen vor. Diese dürften praktisch eher selten relevant werden, da MAC-Adressen nur innerhalb eines lokalen Netzes übertragen werden. Das spricht aber nicht gegen eine Verarbeitung.
- Die in § 9 Abs. 1 Nr. 2 erwähnte URL ergibt sich aus den Kopfdaten, womit eine separate Erwähnung nicht notwendig sein dürfte.
- In § 9 Abs. 1 Nr. 2 ist nur HTTP als Anwendungsprotokoll erwähnt. Tatsächlich hat HTTP in der Praxis eine herausgehobene Rolle; ggf. könnte aber erwogen werden, die Norm zu verallgemeinern, da auch andere Protokolle sicherheitsrelevant sein können.

VIII. Zu § 10

Der Grundgedanke, Daten unverzüglich zu pseudonymisieren, ist zu begrüßen. Pseudonymisierung kann eine wirksame Schutzmaßnahme sein, da sie in vielen Fällen versehentliche Kenntnisnahme von Identitäten verhindern und auch gezielte Zuordnung von Datensätzen zu Personen zumindest erschweren kann.

Fraglich ist jedoch, wie eine solche Pseudonymisierung von allen verantwortlichen Stellen wirksam umgesetzt werden kann. In der Praxis ergeben sich bei der Pseudonymisierung immer wieder große Herausforderungen. So kam es bereits in zahlreichen Fällen dazu, dass pseudonymisierte Daten nachträglich und ohne Hinzunahme weiterer Informationen wieder einer natürlichen Person zugeordnet werden konnten.[9] Pseudonymisierung ist also nicht mit Anonymisierung gleichzusetzen.

Es erscheint daher sachgemäß, eine Richtlinie zur Pseudonymisierung zu erstellen, um den verantwortlichen Stellen die Umsetzung einer sinnvollen Pseudonymisierung zu erleichtern. Eine solche Richtlinie könnte etwa vom Zentrum für Informationssicherheit erstellt und für alle weiteren verantwortlichen Stellen verbindlich festgelegt werden. So kann ein einheitlicher Standard und eine einheitliche Qualität der Pseudonymisierung sichergestellt werden.

In § 10 Abs. 2 Nr. 1 Buchst. b) des Entwurfs ist unklar, auf welches Ereignis sich der Begriff „Ursache“ bezieht. Naheliegend ist, dass die Ursache einer Auffälligkeit gemeint ist, die im Rahmen der Auswertung nach § 8 Abs. 1 oder § 9 Abs. 1 aufgetreten ist. Dafür spricht auch die Formulierung in der Begründung zu Abs. 2 („dass die Daten durch einen Angriff oder ein Schadprogramm verursacht wurden“). Jedenfalls fehlt eine klare Nennung des Umstandes in der Norm.

Das Prinzip des § 10 Abs. 2, Entscheidungen über tiefe Eingriffe in die Privatsphäre von Beschäftigten nur durch Verantwortliche in entsprechender Position nach einer Angemessenheitsprüfung treffen zu lassen, erscheint zielführend. Allerdings erfordert die Prüfung neben juristischer auch technische Kompetenz, um die praktische Relevanz konkret erhobener Daten prüfen zu können. Daher regen wir an, zu prüfen, wie konkret technischer Sachverstand in eine solche Prüfung eingebracht werden könnte und ob umgekehrt ein Verzicht auf die Befähigung zum Richteramt bei entsprechender interdisziplinärer Kompetenz – gerade angesichts der Schwierigkeit bei der Gewinnung doppeltqualifizierten Personals – sinnvoll sein könnte.

---

[9] Vgl. dazu C. Christine Porter: De-identified Data and Third Party Data Mining: The Risk of Re-identification of Personal Information, Washington Journal of Law, Technology & Arts, 2008 (abrufbar unter `https://digitalcommons.law.uw.edu/wjlta/vol5/iss1/3`) sowie Arvind Narayanan und Vitaly Shmatikov: Robust De-anonymization of Large Sparse Datasets, 2008 IEEE Symposium on Security and Privacy (abrufbar unter `https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf`).

Die Überschrift des § 10 spricht von einer Auswertung *ohne* Inhaltsdaten. Aus dem Text der Norm wird dies jedoch nicht klar. Es kann etwa vorkommen, dass auch Protokolldaten nach § 8 Abs. 1 oder Datenverkehr nach § 9 Abs. 1 Inhaltsdaten enthalten oder zumindest Rückschlüsse auf diese ermöglichen.

IX. Zu § 11

In § 11 Abs. 3 Nr. 1 Buchst. a) wiederholt sich die bereits angesprochene Problematik aus § 10 Abs. 2 Nr. 1 Buchst. b): Der Bezug des Wortes „Ursache“ ist unklar.

Darüber hinaus ist die in § 11 Abs. 3 verwendete Formulierung der „Wiederherstellung des Personenbezugs“ irreführend, da Rechtsanwender die Norm so interpretieren könnten, dass pseudonyme Daten regelmäßig keinen Personenbezug aufwiesen. Missverständnissen kann etwa vorgebeugt werden, wenn statt „Wiederherstellung des Personenbezugs“ die Formulierung „Zusammenführung“ von pseudonymisierten Daten und den Daten über die Pseudonyme verwendet wird.

Ähnlich wie in § 10 ist nur in der Überschrift von § 11 die Rede von Inhaltsdaten. Auch in Verweisen auf § 11 (Bspw. in § 8 Abs. 2) findet sich die Nennung von Inhaltsdaten. Insbesondere im Sinne der Verständlichkeit der Norm für Rechtsanwender wäre es jedoch sinnvoll, diesen Umstand auch innerhalb der Norm explizit zu nennen.

X. Zu § 12

Es ist zu begrüßen, dass das Zentrum für Informationssicherheit auch im Wege der Auftragsverarbeitung tätig werden kann sowie, dass die datenschutzrechtlichen Rahmenbedingungen hierfür explizit im Gesetzentwurf angesprochen werden. Praktisch hilfreich könnte es darüber hinaus sein, die datenschutzrechtliche Verantwortlichkeit des Zentrums für Informationssicherheit zu adressieren. Art. 4 Nr. 7 Hs. 2 DSGVO ermöglicht es den Mitgliedstaaten, den Verantwortlichen bzw. bestimmte Kriterien seiner Benennung gesetzlich festzulegen, soweit die Zwecke und Mittel der Datenverarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben sind. Dabei sollte der Rechtsgedanke des Art. 26 Abs. 2 S. 1 DSGVO berücksichtigt werden, sodass die gesetzliche Regelung die jeweiligen tatsächlichen Funktionen und Beziehungen der (ggf. gemeinsam) Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegelt. Eine Klarstellung der datenschutzrechtlichen Rolle des Zentrums für Informationssicherheit bietet sich sowohl im Verhältnis zu Beteiligten am Landesdatennetz bzw. zur Hessischen Zentrale für Datenverarbeitung an als auch zu weiteren möglichen Dritten, etwa einzelnen öffentlichen Stellen des Landes. Dies ist zum einen relevant für die Sicherstellung der datenschutzrechtlichen Compliance der jeweiligen Stellen. Zum anderen muss es nach den Wertungen der DSGVO

für Betroffene stets transparent sein, an wen sie sich bei der Geltendmachung ihrer Betroffenenrechte wenden können. Für beide Aspekte erscheint eine gesetzliche Klarstellung zweckmäßig.

XI. Zu § 14

§ 14 regelt einige wichtige – und aus Sicht der Verfasser begrüßenswerte – Maßnahmen, welche zur Wahrung der Informationssicherheit bei den verantwortlichen Stellen selbst getroffen werden müssen. Insbesondere das 4-Augen-Prinzip des § 14 Abs. 2 Nr. 6 für den Zugriff auf sensible Daten kann das Risiko von Fehlern, Datenlecks und Missbrauch signifikant reduzieren.

Da die Daten aller Voraussicht nach an wenigen Orten zentral gespeichert werden, erscheint es sinnvoll, auch eine Maßnahme wie die Datenträgerverschlüsselung bzw. allgemein die Verschlüsselung von persistent gespeicherten Daten in die Norm aufzunehmen. So kann unbeabsichtigten Datenabflüssen etwa durch Angriffe oder durch nicht sachgemäße Außerbetriebnahme von Hardware vorgebeugt werden.

Die Protokollierung von Zugriffen nach § 14 Abs. 3 kann das Risiko von missbräuchlicher Nutzung der erfassten Daten reduzieren. Wünschenswert wären jedoch auch verbindliche Angaben etwa zu stichprobenartigen Kontrollen des Protokolls. Diese könnten bspw. in regelmäßigen Abständen durch die jeweiligen behördlichen Datenschutzbeauftragten erfolgen.

XII. Zu § 15

Die Regelung des § 15 ist begrüßenswert. Allerdings wird nicht konkretisiert, welche Inhalte ein Sicherheitskonzept haben soll oder wie der Prozess zur Erstellung eines solchen Konzepts aussehen soll. Denkbar wäre etwa eine Anlehnung an BSI-Vorgaben wie den BSI-Standard 200-1. Für andere öffentliche Stellen als das Zentrum für Informationssicherheit wäre zu erwägen, ob Sicherheitskonzepte in Abstimmung mit dem Zentrum erstellt werden sollten.

XIII. Zu § 17

Die Information der Betroffenen ist aus Sicht des Datenschutzes sehr zu begrüßen. Insbesondere in Zusammenhang mit der Entschlüsselung verschlüsselten Datenverkehrs (vgl. oben § 9), die für Betroffene im Regelfall unerwartet sein dürfte, wäre aber eine explizite Regelung auch für im Vorfeld zu erteilende Informationen wünschenswert. Die Verpflichtung zur Erteilung entsprechender Informationen könnte sich zwar in bestimmten Fällen

bereits aus Art. 13, 14 DSGVO ergeben. Eine Klarstellung und Konkretisierung hinsichtlich der Entschlüsselung des Datenverkehrs im Rahmen des HITSiG dürfte aber die Rechtssicherheit sowie die Transparenz für Betroffene erhöhen.