– Ausschussvorlage INA 20/75 –
– öffentlich –

Stellungnahmen der Anzuhörenden
zur mündlichen Anhörung des Innenausschusses

Sitzung am 15. Mai 2023

Gesetzentwurf
Landesregierung
Hessisches Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG)
– Drucks. 20/10752 –

NExT e. V.
Prinzessinnenstr. 8-14
10969 Berlin

Telefon: 030 18681 17435
E-Mail: info@next-netz.de
Internet: next-netz.de

NExT e. V. Prinzessinnenstr. 8-14, 10969 Berlin

Hessischer Landtag
Schlossplatz 1-3
65183 Wiesbaden

Ansprechpartnerin
Ann Cathrin Riedel
E-Mail: anncathrin.riedel@next-netz.de

Berlin, 12. Mai 2023

Stellungnahme zum Hessisches Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG)

1. Ausgangslage und Auftrag

Zum o.a. Gesetzesentwurf wird eine Kurz-Stellungnahme aus Sicht von Anwenderunternehmen / Behörden gewünscht. Aus Termingründen steht vsl. kein NExT-Vortrag der Stellungnahme im örtlichen Präsenz-Anhörungsverfahren zu erwarten.

2. Vorgehen

Aufgrund der Ausgangslage (vgl. 1.) wird eine Kurz-Stellungnahme angeboten. Diese verzichtet auf die übliche systematische und daher umfangreiche Analyse des Gesetzentwurfs, und beschränkt sich deshalb auf kursorische Feststellungen zu wesentlichen Aspekten nach Durchsicht des Entwurfs.

3. Tenor

Der Gesetzentwurf ist aus Sicht der seitens NExT vertretenen Akteur:innen hinsichtlich Inhalt und Struktur dem Grunde nach zu begrüßen. Die vorgesehenen Regelungen geben dem zunehmend existenziellen Thema Cybersecurity einen verbindlichen Gestaltungsrahmen, der einerseits die Themen-Wahrnehmung auf allen Adressat:innen-Ebenen stärkt und strategisch wie taktisch Verantwortlichen als auch operativ Ausführenden das Bereitstellen bzw. Einfordern geeigneter Ressourcen in gebotenem Umfang erlaubt.

Der Entwurf leidet jedoch aufgrund der extrem volatilen Entwicklungen im IuK- und ganz besonders im Cybersecurity-Umfeld trotz erreichter Regelungs-Abstraktion unter seiner rechtsstaatlich erforderlichen Fixierung. Das kann erwarten lassen, dass er früher als erwartet entweder realen Entwicklungen nachhängt oder häufiger Novellierung bedarf – die aufgrund erforderlicher Anforderungen an geordnete Legislativprozesse wiederum nachhängen könnten.

NExT e. V.
Prinzessinnenstr. 8-14
10969 Berlin

Telefon: 030 18681 17435
E-Mail: info@next-netz.de
Internet: next-netz.de

Auf o.a. Punkte geht die nachfolgende Kurzanalyse exemplarisch ein.

4. Ausgewählte Einzelaspekte aus der Perspektive adressierter / verpflichteter Akteur:innen

4.1 Geltungsbereich (§ 1 Abs. 1)

Es erscheint hilfreich, den Begriff „elektronische Verwaltungstätigkeit“ in die Legal-Definitionsliste des § 2 aufzunehmen (oder einen Verweis auszubringen, soweit der Begriff anderweitig legal definiert vorliegt). Cybersicherheit umfasst mit wachsender Vernetzung aller digitalisierter Verfahren auch alle Verwaltungstätigkeiten, unabhängig von Fiskal- oder Verwaltungshandeln, ebenso unabhängig von Digitalverfahren in der Bandbreite von internen Verfahren, Außenanbindungen oder bis zu E-Mail oder Social-Media-Aktivitäten – was durch den Begriff „Verwaltung“ auch anderweitiger i.S.e. engeren Verständnisses offen stünde. Darüber hinaus ist fraglich, ob die Begrenzung auf „elektronische“ Tätigkeiten genügt: zunehmende sog. „social engeneering“-Angriffe können klassische analoge Kanäle mit dem Ziel prä-adressieren, Informationen zum Zugang auf „digitale“ Kanäle zu erlangen und damit den eigentlichen Angriff zu starten.

4.2 Referenzierung auf Standards und Methoden (§ 3)

Die Bezugnahme auf BSI-Standards sowie IT-PLR Beschlüsse ist zielführend. Fraglich erscheint, ob eine landesspezifische Öffnungsklausel ergänzend hilfreich wäre, damit in begründeten Einzelfällen entweder vorab oder ergänzende bzw. abweichende Regelungen zu ermöglichen. Die Öffnungsklausel könnte bspw. im Verordnungswege dem zuständigen Ressort die entsprechenden Kompetenzen – ggf. unter zeitlicher Begrenzung – übertragen. Damit würden taktische und operative Entscheidungsträger:innen immer dann eine Handlungsgrundlage erhalten können, wenn grundlegende neue Entwicklungen großen Ausmaßes vorab unabsehbare Maßnahmen erfordern. Der Ansatz schließt konsequent an § 4 Abs. 3 an und überbrückt Zeiträume zwischen Anordnungen des CISO bis zu ggf. nötigen Nachsteuerungen im HITSiG für neue Cybersecurity-Aspekte. Retrospektiv sei exemplarisch auf das volatile Angreifer-Verhalten bei Ransomware-Vorfällen verwiesen, welches mit Zeitverlauf der letzten Monate unterschiedliche Einschätzungen zum Verhalten wie bspw. Lösegeldzahlungen vs. Cyberversicherungs-Bedingungen hervorbrachte, was wiederum jeweils zeitnaher und ggf. strategischer (Landes-)Festlegungen bedarf.

4.3 Verpflichtung der Behördenleitungen (§ 3 Abs. 3)

Die Verpflichtung ist sinnstiftend und zielführend, insbes. auch aufgrund der damit einhergehenden personellen und monetären Ausstattung. Das darf jedoch nicht darüber hinwegtäuschen, dass bereits die Rekrutierung und Bindung hinreichend digital kompetenter Fachkräfte die Verwaltungsbehörden vor massive Vollzugsprobleme stellt (Fachkräftemangel, MINT-Berufe, Demografie-Schere, Vergütungsstrukturen, tech war of

NExT e. V.
Prinzessinnenstr. 8-14
10969 Berlin

Telefon: 030 18681 17435
E-Mail: info@next-netz.de
Internet: next-netz.de

talents); im Cybersecurity-Umfeld gilt diese Problematik nochmals verstärkt. Deshalb steht zu befürchten, dass der Maßnahmenvollzug schleppend und ggf. unterkompetent anläuft. Als Gegenmaßnahme sollte den Behördenleitungen daher ein gesetzlicher Anspruch auf Unterstützungsmaßnahmen zur Expert:innen-Fortbildung eingeräumt werden, bspw. durch geeignete Akademie-Fortbildungen des Landes, ggf. in Kooperation mit privatrechtlichen Anbietern unter Fokussierung auf die Besonderheiten der öffentlichen Hand in Hessen. Dabei darf im Übrigen die damit verbundene Daueraufgabe nicht unterschätzt werden: geeignetes Fachpersonal wird sich idealerweise halbjährlich, mindestens jedoch jährlich testierten (!) Fortbildungsmaßnahmen unterwerfen müssen, damit die Fachkompetenz den volatilen Cybersecurity-Entwicklungen halbwegs zeitnah nachgeführt werden kann. Daneben sind mindestens monatliche, besser wöchentliche Wissensupdates zur abstrakten und konkreten Gefährdungslage nötig, worauf Behörden und deren Verantwortlichen (Leitung, ITSiBe) ebenfalls Zugriffe legislativ verbindlich zugestanden werden sollten. Dafür könnte bspw. der Aufgabenkanon des CISO gem. § 4 Abs. 2 um eine zusätzliche Ziffer 6 oder das ZfIS gem. § 5 Abs. 2 um eine zusätzliche Ziffer 11 „Bereitstellung der Aus- und Fortbildung für Stellen gem. § 1 Abs. 1 und 2“ (Arbeitstitel) erweitert werden.

4.4 Verschlüsselter Datenverkehr (§§ 8 – 11)

In der arbeitstäglichen Sicherheitspraxis erweist sich die Antipoden zwischen Datenschutzbedarf einerseits und Sicherheitsniveau andererseits seit Jahren als hochproblematisch. Bspw. treffen verschlüsselte Verbindungen nach dem TLS-Standard (Transport Layer Security, u.a. Basis für HTTPS_Standardverbindungen) auf technische Systeme, die diese Verschlüsselung als sog. „incerpetion“ aufbrechen, Inhaltsdaten analysieren und anschließend wieder verschlüsseln, was als permanenter und gewollter „man in the middle“-Angriff der Empfängerseite – oder schlimmer: zwischengeschalteter Transportsysteme außerhalb eigener Sphäre – gewertet werden kann. Je nach TLS-Version einerseits und (jeweils!) eingesetzten Sicherheitskomponenten treffen solche und ähnliche Konstellationen mehr oder minder in der heutigen Praxis zu. Daraus erwachsen grundlegende Auswirkungen auf und deshalb strategische Bedeutung für ein ausgewogenes Verhältnis zwischen Datenschutz und Informationssicherheit. Eine verbindliche Festschreibung dieses Verhältnisses ist nach gegenwärtiger Kenntnis nicht aus den referenzierten Standards und Methoden (vgl. oben 4.2) abzuleiten, sondern festzulegen. Deshalb liegt hier ein (weiterer) Beispielfall vor, der mittels untergesetzlicher Verordnung auf Ressortebene ebenso verbindlich wie flexibel geregelt werden kann. Im Übrigen könnten solche Festlegungen im Verordnungswege das ZfIS bzw. den CISO vor anlassbezogenen Massenanfragen wirksam schützen und zur Vollzugssicherheit beitragen.

NExT e. V.
Prinzessinnenstr. 8-14
10969 Berlin

Telefon: 030 18681 17435
E-Mail: info@next-netz.de
Internet: next-netz.de

4.5 Grenzen der Trennung von Informationssicherheit und IT-Betrieb (§ 14)

Eine „harte“ Trennung von Informationssicherheit und IT-Betrieb (Operations) ist insbes. im Netze-Bereich generell problembehaftet, weil – spätestens – in diesem Handlungssegment systematisch fließende Grenzen vorherrschen. Daher wird ein gestuftes Trennungskonzept empfohlen, welches neben technischen insbes. auch auf organisatorische Maßnahmen (sog. TOMs) wie bspw. besondere Verpflichtungen für dort eingesetztes Personal aus beiden o.g. Bereichen enthält. Im Übrigen gilt bei Informationssicherheit wie bei allen Sicherheitsfragen immer, dass verlängerte Wege aufgrund unüberwindbarer Formalgrenzen bei Sicherheitsvorfällen in aller Regel Auswirkungen auf die Reaktionszeiten und damit auf das Schadensbild entfalten. Deshalb kann bspw. aus etablierten und daher praktisch bewährten Regeln aus dem BOS-Bereich (Behörden und Organisationen mit Sicherheits-/Sonderaufgaben, sog. „Blaulicht-Behörden“) Nutzen gezogen werden, in dem einige Elemente daraus auf die o.g. Rechtslage im Tayloring-Verfahren abgebildet werden und damit möglichst kurze Wege erhalten bleiben.

4.6 Ergänzungsempfehlungen:

4.6.1 DevSecOps

Der Ansatz aus 4.5 kann auf die – im Entwurf nicht näher ausgeführten – Prozesse sicherer Softwareentwicklung bzw. der Beschaffung hinreichend sicher entwickelter IuK-Produkte ausgeweitet werden, was bspw. durch eine geeignete Ergänzung in den o.g. Vorschriften um den als allgemein anerkannt geltenden DevSecOps-Zyklus möglich ist.

4.6.2 Folgen aus Verbandsklagerecht

Mit dem neuerdings vorgesehenen Verbandsklagerecht ist derzeit noch offen, ob davon „nur“ Datenschutz- oder auch Cybervorfälle betroffen sind, wobei im konkreten Einzelfall beide Aspekte fließend ineinander übergehen werden und daher schwer trennbar sind. Jedenfalls wird aus dem Verbandsklagerecht eine Steigerung der Verbandsklagen erwartet. Sofern dies auch auf Verwaltungsvorgänge („Verbraucherbegriff“?) ausgeweitet werden würde, ist empfehlenswert, monetäre Enthaftungs-Vorsorge für behördliche Verantwortliche im Gesetzentwurf (oder an anderer Stelle) zu schaffen: andernfalls steht zu befürchten, dass spätestens mit diesem drohende Risiko neben der problembehafteten Fachkräfterekrutierung (vgl. oben) kein geeignetes Fachpersonal in hinreichender Anzahl mehr bereit wäre, die notwendigen Funktionen in Behörden zu verantworten.

Sinngemäß Ähnliches gilt für die aktuell zu beobachtende Entwicklung, dass Schadenersatzklagen nach Cyberattacken nach US-Modell zunehmend auf (zunächst noch privatrechtliche) EU- und damit auch nationale Behörden übergreifen. Im Übrigen sei auf die laufende EuGH-Entwicklung verwiesen, hier anlässlich des Auftauchens von Daten im sog. Darknet nach Cyberangriff(en).

NExT e. V.
Prinzessinnenstr. 8-14
10969 Berlin

Telefon: 030 18681 17435
E-Mail: info@next-netz.de
Internet: next-netz.de

Diese Thematik schließt den Kreis zu 4.6.1, denn Cyberschäden aufgrund Produktmängeln (wie bspw. verschwiegener oder lange verschleppter Sicherheitslücken) bedürfen eines Nachweises, um ggf. eintretende Haftungsfälle wirksam abzuwehren, in dem verantwortliche Hersteller bzw. Dienstleister in die Pflicht genommen werden (Leistungsstörungsnachweis). Dafür nötige Dokumentationen enthalten bereits die §§ 17 – 19 des Entwurfs, die dafür auf den vollständigen Produktlebenszyklus von Auswahl und Beschaffung bis zur Außerbetriebnahme einschließlich Entsorgung auszuweiten wäre, also eine 360-Grad-Perspektive über den konkreten Schadensfall hinaus enthalten würde. Damit einhergehender (personeller) Aufwand wird jedoch erheblich sein.

4.6.3 Folgen aus EU-Gesetzgebung

Mit der national unmittelbar bevorstehenden Umsetzung der sog. NIS2-RL, des sog. CRA (Cyber Resiliance Act) als auch weiterer (Bundes-)Gesetze wir bspw. das angekündigte sog. „Dachgesetz“ des BMI sind Auswirkungen auf a) die Anzahl sog. KRITIS-(Behörden) also auch auf b) persönliche Haftungsfolgen für Verantwortliche verbunden, deren Art und Umfang sich derzeit noch nicht abschätzen lässt. Es wird daher empfohlen, die Wiedervorlage-Frist des HITSchiG in Anbetracht dieser Entwicklungen zu verkürzen und es mit Vorliegen der o.g. Regelungen dem Normenscreening zu unterziehen, bspw. zum 31.12.2024.

5. Fachjuristische Aspekte

Auf fachjuristische Betrachtungen wurde aufgrund des eingangs skizzierten Scopes dieser Stellungnahme bewusst verzichtet.

ekom21 – KGRZ Hessen · Postfach 42 02 08 · 34071 Kassel

Hessischer Landtag
Ausschuss für Digitales und Datenschutz
Der Vorsitzende
Schlossplatz 1 - 3
65183 Wiesbaden

per E-Mail an:
c.lingelbach@ltg.hessen.de
m.mueller@ltg.hessen.de

Olaf Orth
Olaf.Orth@ekom21.de
+49 561 204 1203
09.05.2023

Stellungnahme zum Gesetzentwurf
eines Hessischen Gesetzes zum Schutz der elektronischen Verwaltung
(Hessisches IT-Sicherheitsgesetz)
Öffentliche Anhörung

Sehr geehrter Herr Vorsitzender,
sehr geehrte Damen und Herren,

für die Gelegenheit und das Vertrauen, zu dem vorgelegten Kabinettentwurf Stellung nehmen zu können, bedanken wir uns.

Die ekom21 ist ein nach dem Datenverarbeitungsverbundgesetz (DV-VerbundG) als Körperschaft des öffentlichen Rechts errichtetes Kommunales Gebietsrechenzentrum. Für die hessischen Kommunalverwaltungen stellen wir seit über 50 Jahren Informations- und Kommunikationstechnik aller Art bereit. Seit 2009 ist die ekom21 ununterbrochen vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach ISO 27001 auf Basis von IT-Grundschutz zertifiziert. Mit unseren Dienstleistungen (z.B. KDLZ-CS) und unserer Expertise unterstützen wir die hessischen Kommunalverwaltungen umfassend im Themenfeld der Informations- und Cybersicherheit.

Zu dem vorgelegten Gesetzentwurf der Landesregierung nehmen wir daher vorrangig aus Sicht eines öffentlichen IT-Dienstleisters Stellung, der die angeschlossenen Kommunalverwaltungen im Bereich der IT-Sicherheit unterstützt.

I. Einordnung des Gesetzes

Die Digitalisierung durchdringt alle privaten Lebensbereiche und jedes staatliche Handeln. Die Lage der IT-Sicherheitslage hingegen verschärft sich seit Jahren besorgniserregend. Zuletzt im besonderen Maße durch terroristische und geopolitische Konflikte sowie die massive Zunahme krimineller Handlungen. Die Cyber- und Informationssicherheit ist damit ein essentieller Vertrauensanker für Verwaltungen, Bürgerinnen und Bürger sowie die Wirtschaft. Mit den Regelungen für Telemediendienste in § 19 Abs. 4 TTDSG und den Regelungen zur Datensicherheit in Art. 32 der Datenschutzgrundverordnung (DS-GVO) sind bereits gewisse IT-Sicherheitsanforderungen hinaus in weiteren Bereichen der Wirtschaft und Verwaltung etabliert. Sie verpflichten viele Unternehmen, risikoangemessene und dem Stand der Technik entsprechende IT-Sicherheitsmaßnahmen zu ergreifen und Vorfälle zu melden.

Die Regelungen zur Verbesserung des Schutzes der Bundesverwaltung und der Kommunikationstechnik des Bundes sind im Großen und Ganzen im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) geregelt, z.B. in §§ 4, 4a und 4b, 5a und 5b.

Grundsätzlich begrüßen wir daher ausdrücklich, dass die Cyber- und IT-Sicherheit neben den bisherigen Aktivitäten (z.B. für den kommunalen Bereich das KDLZ-CS) nun auch auf landesgesetzgeberischer Ebene verstärkt bearbeitet wird.

Mit dem vorgelegten Gesetzentwurf zum Schutz der elektronischen Verwaltung (HITSiG-E) sollen primär die gesetzlichen Grundlagen für eine rechtliche Absicherung der Aufgaben und Befugnisse des neuen Zentrums für Informationssicherheit geschaffen werden, um den Schutz der Informations- und Kommunikationstechnologie der Landesverwaltung zu gewährleisten. Ferner ist nach dem Gesetzesentwurf das Computer Emergency Response Team (CERT) künftig Bestandteil des Zentrums für Informationssicherheit. Darüber hinaus soll das Zentrums für Informationssicherheit die Zusammenarbeit mit den für die Informationssicherheit zuständigen zentralen Stellen in Bund, Ländern und Kommunen fördern. Eingebettet in diesen Kontext darf es auf Ersuchen der kommunalen Stellen bei der Erkennung, Untersuchung und Abwehr von Gefahren für die Informationssicherheit unterstützend tätig werden und seine Dienstleistungen der Wirtschaft anbieten.

Neben dem Zentrum für Informationssicherheit wird die Position der Zentralen oder des Zentralen Informationssicherheitsbeauftragten für die hessische Landesverwaltung (Chief Information Security Officer, CISO) einschließlich Zuständigkeiten und Befugnissen und Pflichten für die Stellen der hessischen Landesverwaltung gesetzlich verankert.

Mit den §§ 7ff HITSiG-E schafft der Gesetzesentwurf – soweit ersichtlich – erstmals ausdrückliche landesrechtliche Grundlagen für die Ver- und Weiterverarbeitung von (personenbezogenen) Daten, die im Rahmen von IT-Sicherheits- und Cyberabwehrmaßnahmen bei Stellen nach § 1 HITSiG-E anfallen (können). Insbesondere ermöglicht § 8 HITSiG-E die Verarbeitung bereits auf den IT-Systemen vorhandener (Protokoll-)Daten zu Zwecken der IT-Sicherheit und Cyberabwehr. Die §§ 10, 11 HITSiG-E hingegen schaffen einen rechtlichen Rahmen für die Auswertung von (personenbezogenen) Daten zu IT-Sicherheitsmaßnahmen. Damit wird ein geeigneter Rechtsrahmen für die erforderlichen Verarbeitungen geschaffen.

II. Konkretisierungsbedarfe

Die im HTSiG vorgesehen Regelungen sind aus Sicht der ekom21 ein wichtiger Baustein, um das Zielbild einer sicheren elektronischen Verwaltung in Hessen zu erreichen. Allerdings bedarf der Gesetzesentwurf einiger punktueller Konkretisierungen.

Nach § 1 HITSiG-E gilt das Gesetz für die elektronische Verwaltungstätigkeit

> *„1. der Behörden und sonstigen öffentlichen Stellen des Landes sowie nicht öffentlicher Stellen, soweit sie hoheitliche Aufgaben unter Aufsicht der vorgenannten Stellen wahrnehmen,*
>
> *2. der nicht unter Nr. 3 fallenden der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen ungeachtet ihrer Rechtsform sowie nicht öffentlicher Stellen, soweit sie hoheitliche Aufgaben unter Aufsicht der vorgenannten Stellen wahrnehmen,*
>
> *3. der Behörden und sonstigen öffentlichen Stellen der Gemeinden und Gemeindeverbände sowie nicht öffentlicher Stellen, soweit sie hoheitliche Aufgaben unter Aufsicht der vorgenannten Stellen wahrnehmen.*"

Der Gesetzesentwurf unterscheidet damit zwischen der unmittelbaren Landesverwaltung (Nr. 1), der Aufsicht des Landes unterstehenden juristischen Personen (Nr. 2) und dem Kommunalbereich (Nr. 3). Diese Unterscheidung wirkt sich im Gesetzentwurf an mehreren Stellen erheblich aus. Denn anknüpfend an diese Differenzierung wird im Gesetzesentwurf hinsichtlich des Umfangs der rechtlichen Befugnisse und Verpflichtungen unterschieden. Beispielhaft sind hier die §§ 3, 5 Abs. 1 Nr. 2, 12 Abs. 1 und 2 HITSiG-E anzuführen, die zwischen den Stellen nach § 1 Nr. 1 und 2 oder Nr. 3 unterscheiden. Besonders deutlich wird dies in § 3 HITSiG-E. Nach dessen Absatz 4 darf eine Stelle nach § 1 Nr. 1 und 2 wesentliche Änderungen an informationstechnischen Systemen nur im Benehmen mit der oder dem Informationssicherheitsbeauftragten durchführen. Stellen nach § 1 Nr. 3 sowie den hessischen Schulen wird hingegen nur „empfohlen", die Grundsätze nach Abs. 1 bis 4 HITSiG-E einzuhalten.

Im Hinblick auf die Einordnung der ekom21 in die Systematik nach § 1 HITSiG-E ergeben sich für uns Unklarheiten, die aus den vorgenannten Gründen zu erheblichen praktischen Auswirkungen führen können. Einerseits hat der Gesetzgeber in § 2 Abs. 5 DV-VerbundG entschieden, die (Rechts-)Aufsicht für die ekom21 dem Regierungs-

präsidium Gießen zu übertragen. Auf den ersten Blick könnte damit die ekom21 nach der Systematik des Gesetzesentwurfs § 1 Nr. 2 HITSiG-E unterfallen. Andererseits ist die ekom21 nach § 2 Abs. 1 DV-VerbundG eine Körperschaft des öffentlichen Rechts auf die die für Zweckverbände geltenden Vorschriften des Gesetzes über kommunale Gemeinschaftsarbeit (KGG) Anwendung. Das KGG wiederum verweist in § 7 Abs. 2 im Falle von Regelungslücken subsidiär auf die Hessische Gemeindeordnung (HGO). Für die Wirtschaftsführung und das Rechnungswesen gelten nach § 2 Abs. 4 DV-VerbundG ebenfalls kommunale Vorschriften, nämlich das kommunale Eigenbetriebsrecht. Nach der Intention und im Lichte der Regelungen des DV-VerbundG ist die ekom21 aber primär dem kommunalen (§ 1 Nr. 3 HITSiG-E) und nicht dem staatlichen Bereich (§ 1 Nr. 1 und 2 HITSiG-E) zuzuordnen.

Um hier jedoch jeglicher rechtlichen Unsicherheit zu begegnen, regen wir an, entweder im Gesetz oder in der Gesetzesbegründung eine entsprechende Klarstellung dahingehend aufzunehmen, dass die ekom21 als Stelle im Sinne von § 1 Nr. 3 HITSiG-E zu qualifizieren ist.

Ausweislich von § 1 Abs. 1 Satz 1 HITSiG-E, gilt das Gesetz „für die elektronische Verwaltungstätigkeit". Weit überwiegend sind jedoch zentrale IT-Infrastrukturmaßnahmen- und Systeme betroffen, die – so unsere Einschätzung - nicht nur zur Abwicklung der elektronischen Verwaltungstätigkeit eingesetzt und genutzt werden, sondern auch für die sonstigen Tätigkeiten der öffentlichen Hand. Dies könnte etwa der (zivilrechtliche) Verkauf von Holz durch HessenForst oder den Verkauf von Veranstaltungstickets betreffen. Hierbei handelt es sich nicht um „klassische Verwaltungstätigkeit" sondern um sonstige Tätigkeiten der öffentlichen Hand. Weil die vom Gesetz betroffenen IT-Systeme und Maßnahmen ggf. sowohl für Verwaltungstätigkeit als auch die sonstigen Handlungen der betroffenen öffentlichen Einrichtung genutzt werden können, sollte im Gesetz oder in der Gesetzesbegründung klargestellt werden, dass der Begriff der Verwaltungstätigkeit weitgefasst ist und auch die sonstigen Tätigkeiten umfasst, die von den Behörden ausgeübt werden. Denn auf der Ebene der eingesetzten IT-Systeme und Maßnahmen kann – wie bereits festgehalten wurde – nicht nach dem „Einsatzzweck" differenziert werden.

Eine weitere Konkretisierung erachten wir in § 8 Abs. 1 HITSiG-E für erforderlich. Weder Wortlaut noch die Gesetzesbegründung ermöglichen eine ausreichende Abgrenzung, welche Fallgestaltungen, Daten und Systeme genau gemeint sind. Ausweislich der Gesetzesbegründung bleibt offen, welche Daten genau genutzt werden können, „die nicht Gegenstand einer Datenübermittlung im Landesdatennetz sind (z. B. Transaktionsprotokolle von Datenbankservern oder Betriebszustände von Serversystemen), jedoch für den Betrieb eines wirksamen informationstechnischen Sicherheitssystems erforderlich sind, um Gefahren zu erkennen.

Zu eng gefasst ist nach unserer Ansicht § 10 Abs. 1 S. 1 HITSiG-E. Dieser gibt vor, dass Daten die zur Abwehr von Gefahren erforderlich sind, höchstens für 90 Tage gespeichert werden dürfen. Im Gesetz sollte jedoch klargestellt werden, dass diese Speicherbegrenzung anderen rechtlichen Vorgaben nicht entgegensteht, die ggf. eine längere Speicherdauer ermöglichen oder vorgeben.

Nach § 10 Abs. 2 S. 2 HITSiG-E sind die Daten „unverzüglich automatisiert zu pseudoanonymisieren, soweit dies technisch möglich ist und die Daten nicht bereits pseudonym vorliegen. Aus Sicht und Erfahrung der ekom21 ist dies Anforderung in der Praxis häufig nur sehr schwierig und mit erheblichen (wirtschaftlichen) Aufwand zu realisieren. Im Gesetz sollte daher dahingehend präzisiert werden, dass die Pseudoanonymisierung unter dem Vorbehalt der Implementierungskosten und der praktischen Realisierbarkeit steht.

Mit freundlichen Grüßen
im Auftrag

Olaf Orth
(Leiter Fachbereich
Recht & Verträge)

HSGB
HESSISCHER STÄDTE- UND GEMEINDEBUND

Hessischer Städte- und Gemeindebund · Postfach 1351 · 63153 Mühlheim/Main

Hessischer Landtag
Vorsitzender des Innenausschusses
Herrn Christian Heinz
Schlossplatz 1-3
65183 Wiesbaden

c.lingelbach@ltg.hessen.de
m.mueller@ltg.hessen.de

Geschäftsführer
Dr. David Rauber
Unser Zeichen Dr.R/Eh.

Telefon 06108 6001-20
Telefax 06108 6001-57
E-Mail hsgb@hsgb.de

Ihr Zeichen
Ihre Nachricht vom

Datum 04.05.2023

Entwurf eines Hessischen Gesetzes zum Schutz der elektronischen Verwaltung

(Hessisches IT-Sicherheitsgesetz, HITSiG)

Sehr geehrter Herr Vorsitzender,
sehr geehrte Damen und Herren,

für die uns eingeräumte Gelegenheit zur Stellungnahme danken wir herzlich. Aufgrund der frühzeitigen Vorabinformation im Rahmen der Regierungsanhörung erheben wir keine Einwände aufgrund der verkürzten Anhörungsfrist.

Zum Gesetzentwurf selbst ist aus Sicht der von uns vertretenden kreisangehörigen Städten und Gemeinden folgendes auszuführen:

I. Bedeutung des Themas für die Städte, Gemeinden und Landkreise

Die Gewährleistung eines angemessenen IT-Sicherheitsniveaus ist angesichts nur begrenzt verfügbaren Fachpersonals eine Aufgabe des Landes, die das Land auch für die Gemeinden und Gemeindeverbände mit wahrnehmen muss. Denn die Leistungen beider Ebenen sind in der Praxis und auch rechtlich vielfältig aufeinander bezogen und auch technisch verknüpft bis hin zum Portalverbund. Nur mit einer zentralen Rolle des Landes kann das notwendige einheitliche Sicherheitsniveau für die öffentlichen Verwaltungen

von Land und Kommunen und für die in ihrer Verantwortung betriebenen kritischen Infrastrukturen zuverlässig gewährleistet werden.

Daher müssen die Kapazitäten des Zentrums für Informationssicherheit ausreichend dimensioniert werden. Gebraucht wird, was das Gesetz auch in weitem Umfang regelt – Befugnisse der Gefahrenabwehr für eine spezialisierte Behörde (Zentrum für Informationssicherheit) und eine Art Cyber-Feuerwehr (CERT und die zugeordneten MIRTs).

Die Gewährleistungsverantwortung des Landes umfasst auch ein ausreichendes und leicht zugängliches Informations-, Schulungs- und Fortbildungsangebot zur IT-Sicherheit. Diese hat das Land mit dem Arbeitskreis kommunale Cybersicherheit und Schulungsprogrammen auch bereits aktiv aufgegriffen; diese Initiativen müssen beibehalten und jeweils bedarfsgerecht weiterentwickelt werden.

II. Zu Vorschriften im Einzelnen

Soweit aus unserer Sicht Anmerkungen zu einzelnen Vorschriften zu machen sind, erfolgen diese nachstehend:

1. Befreiende Wirkung einer Beauftragung geeigneter Dritter (§ 3)

Das Gesetz sollte um eine ausdrückliche Regelung ergänzt werden, wonach bei Beauftragung eines geeigneten Dritten, der die Einhaltung der Grundsätze nach § 3 Abs. 1 bis 4 des Entwurfs mit Ausnahme der Bestellung eines IT-Sicherheitsbeauftragten gewährleistet, die Anforderungen des Gesetzes durch die beauftragende / betrauende juristische Person als erfüllt gelten. Mit der Beauftragung gelten sinnvollerweise auch die Anforderungen an das Sicherheitskonzept als erfüllt.

2. Betrauung des Zentrums für Informationssicherheit (§ 12)

Kommunen sollten das Zentrum für Informationssicherheit oder geeignete Dritte, die der Aufsicht des Landes unterstehen bereits mit Inkrafttreten des Gesetzes mit der Durchführung erforderlicher Maßnahmen betrauen können.

3. Zulässigkeit von Abwehrmaßnahmen (§ 15)

Abwehrmaßnahmen dürfen entgegen § 15 des Entwurfs nicht erst dann zulässig sein, wenn die von sicherheitsrelevanten Vorfällen betroffene Stelle ein Sicherheitskonzept hat.

HSGB
HESSISCHER STÄDTE- UND GEMEINDEBUND

4. **Ergänzungsbedarf: Aufgabenbeschreibung (§ 1 oder § 3)**

Auch mit Blick auf die Umsatzbesteuerung der öffentlichen Hand (§ 2b UStG) sollte – entsprechend dem Vorschlag für ein Versorgungskassengesetz – ausdrücklich klargestellt werden, dass Vorhaltung, Betrieb und ein angemessenes Sicherheitsniveau der für die Aufgabenwahrnehmung erforderlichen IT-Systeme zu den Aufgaben des Landes, der Gemeinden und Gemeindeverbände gehören.

5. **Vorgesehene Befristung (§ 21)**

IT-Sicherheit ist eine Aufgabe, die auf unabsehbare Zeit bestehen wird. Daher ist die vorgesehene Befristung des Gesetzes nicht sinnvoll.

Aus terminlichen Gründen ist es uns leider nicht möglich, an der Anhörung teilzunehmen.

Mit freundlichen Grüßen

GEZ.
Dr. David Rauber
Geschäftsführer

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.

VERBAND KOMMUNALER UNTERNEHMEN e.V.
LANDESGRUPPE HESSEN

VKU Geschäftsstelle Hessen • Frankfurter Straße 2 • 65189 Wiesbaden

Hessischer Landtag
Innenausschuss
Schlossplatz 1-3
65183 Wiesbaden

per E-Mail

Frankfurter Str. 2
65189 Wiesbaden

Fon +49 611.1702-29
Fax +49 611.1702-30

Vorsitzender:
RA Ralf Schodlok

Geschäftsführer:
Dipl.-Pol. Martin Heindl
heindl@vku.de

Hauptgeschäftsstelle

Invalidenstrasse 91
10115 Berlin

Fon +49 30.58580-0
Fax +49 30.58580-100

www.vku.de
info@vku.de

Stellungnahme zum Gesetzentwurf eines Hessischen Gesetzes zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz) 10.05.2023

Sehr geehrter Herr Abgeordneter Heinz,
sehr geehrte Damen und Herren Abgeordnete,

wir bedanken uns für die Möglichkeit zur Stellungnahme zum Gesetzentwurf der Landesregierung für ein Hessisches Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz).

In unserer zunehmend digitalisierten Welt sind nahezu alle Bereiche des gesellschaftlichen und wirtschaftlichen Lebens auf die stets zuverlässige Funktion der notwendigen Informations- und Kommunikationstechnik angewiesen. Deren Ausfall oder Beeinträchtigung kann zu erheblichen Störungen oder im schlimmsten Fall sogar zum völligen Ausfall der wirtschaftlichen und administrativen Leistungsfähigkeit und damit der gesellschaftlichen Lebensgrundlagen führen.

Als VKU-Landesgruppe Hessen begrüßen wir daher grundsätzlich das Vorhaben der Hessischen Landesregierung, mit dem Hessischen IT-Sicherheitsgesetz wichtige Maßnahmen zur Sicherheit der Informations- und Kommunikationstechnologien in der hessischen Verwaltung gesetzlich festzuschreiben. Mit dem Zentrum für Informationssicherheit wird zudem eine Kompetenzstelle geschaffen, um die zum Schutz der Informations- und Kommunikationstechnologie in Hessen erforderlichen Kompetenzen und die Technik auf- bzw. auszubauen und dauerhaft zu installieren.

Auch die kommunalen Unternehmen nutzen die Digitalisierung und die Möglichkeiten digitaler Transformation, um ihre Leistungen jederzeit erbringen zu können. Hierbei werden immer mehr Anlagen und Maschinen digital vernetzt. Damit steigt zugleich das Risiko: Je mehr Anlagen und Maschinen digital vernetzt sind, desto mehr Angriffspunkte entstehen, desto vulnerabler wird das Gesamtsystem. Die kommunalen Unternehmen arbeiten bei der IT-Sicherheit täglich daran, technologisch gut aufgestellt zu sein und erfüllen entsprechende gesetzliche Standards.

Hauptgeschäftsführer:
Ingbert Liebing

Registergericht:
Amtsgericht Charlottenburg
Registernummer:
VR 27941 B

VERBAND KOMMUNALER UNTERNEHMEN e.V.
LANDESGRUPPE HESSEN

So unterliegen zum Beispiel Energieversorger dem IT-Sicherheitskatalog und müssen somit ein Informationssicherheitsmanagementsystem (ISMS) nach ISO 27001 nachweisen. Für Wasserversorger ab einer gewissen Größe gelten die Vorgaben der KRITIS Verordnung des BSI. Mit dem Hessischen IT-Sicherheitsgesetz wird ein weiterer wichtiger Baustein ergänzt, jedoch sollte auch eine mögliche Vereinheitlichung der unterschiedlichen Begrifflichkeiten, Definitionen und Normen dabei nicht aus dem Blick verloren werden.

Dennoch möchten wir darauf hinweisen, dass es IT-Sicherheit nicht zum Nulltarif gibt. Von Audits durch externe Sachverständige über die Anschaffung von Hardware bis zur Sensibilisierung der Mitarbeiter: Alle diese Maßnahmen sind mit hohen Kosten verbunden und müssen refinanziert werden. Es muss deshalb über eine entsprechende Förderung der betroffenen Unternehmen und Kommunen nachgedacht werden.

Ergänzt werden muss dieser Ansatz durch eine Unterstützung in der Fachkräftegewinnung und -ausbildung. Qualifizierte Fachkräfte im Bereich der IT-Sicherheit sind rar und gerade für kommunale Unternehmen und Kommunen nicht leicht zu gewinnen, vor allem dann, wenn diese abseits attraktiver Metropolen ansässig sind. Die kommunalen Unternehmen, Betriebe und Verbände sowie die Kommunen sollten auch dabei unterstützt werden, ein ISMS einzuführen und zu betreiben. Insbesondere die interkommunale Zusammenarbeit im Bereich der IT-Sicherheit sollte finanziell unterstützt werden.

Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen

Martin Heindl
Geschäftsführer

EBS UNIVERSITÄT

EBS Universität, Gustav-Stresemann-Ring 3, 65189 Wiesbaden

An den Innenausschuss
des Hessischen Landtags

Prof. Dr. Matthias Friehe
Qualifikationsprofessur für
Staats- und Verwaltungsrecht

EBS Law School
T +49 611 7102 2207
matthias.friehe@ebs.edu

10. Mai 2023

Stellungnahme zum Gesetzentwurf

der Landesregierung für ein Hessisches Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG) auf Drs. 20/10752

Sehr geehrter Herr Vorsitzender,
sehr geehrte Damen und Herren Abgeordnete,

vielen Dank für die Gelegenheit, zum vorgenannten Gesetzentwurf Stellung zu nehmen.

Der Entwurf für ein Hessisches IT-Sicherheitsgesetz (E-HITSiG) regelt in organisatorischer Hinsicht die Einrichtung eines Zentralen Informationssicherheitsbeauftragten – Chief Information Security Officer, CISO – (§§ 4-6 E-HITSiG) und in materieller Hinsicht verschiedene Ermächtigungsgrundlagen zur Überwachung der landeseigenen IT-Sicherheitsinfrastruktur zum Zwecke der Abwehr von IT-Sicherheitsgefahren (§§ 7-19 E-HITSiG). Dementsprechend ist auch die Zweckrichtung des Gesetzentwurfs eine doppelte: Zum einen geht es um organisatorische Maßnahmen, um Kompetenzen für IT-Sicherheit zu bündeln. Zum anderen geht es um die nötigen Rechtsgrundlagen für die Schutzmaßnahmen zugunsten der landeseigenen IT-Systeme.

Zu beiden Aspekten werde ich kurz Stellung beziehen, wobei ich mich auf wesentliche Aspekte beschränke.

EBS UNIVERSITÄT

I. Organisatorische Maßnahme: Einrichtung eines Zentralen Informationssicherheitsbeauftragten

Die – für eine deutsche Behörde ungewöhnliche – englische Titulierung als Chief Information Security Officer scheint bereits an und für sich ein Signal setzen zu wollen: Das Land Hessen bekommt eine Art digitalen „Sheriff", der Angriffe auf die IT-Sicherheit abwehren soll. Dabei steht außer Frage, dass die öffentliche Hand mehr in die IT-Sicherheit ihrer Informationssysteme investieren muss. Die Politik ist zu Recht entschlossen, die Digitalisierung der Verwaltung voranzutreiben und so Verwaltungsabläufe zu vereinfachen. Je mehr sich der Staat auf digitale bzw. digitalisierte Verwaltungsverfahren einlässt und verlässt, desto größer wird allerdings auch das Risiko, dass einzelne Verwaltungsbereiche teilweise oder sogar ganz ausfallen, weil sie Opfer von Cyberattacken geworden sind. Die Bedrohung geht zum einen von kriminellen Banden aus, die beispielsweise IT-Systeme mit erpresserischer Zielsetzung angreifen, zum anderen von staatlichen Akteuren, die spionieren oder sogar gezielt sabotieren.

Die Abwehr derartiger Gefahren kann nicht von einer zentralen Stelle allein erfolgen. Auch der Gesetzentwurf betont insofern die Verantwortung des jeweiligen Behördenleiters, in seinem Bereich für die IT-Sicherheit zu sorgen, wozu auch jeweils lokale IT-Sicherheitsbeauftragte bestimmt werden sollen (§ 3 Abs. 3 E-HITSiG). Gleichwohl ist der Gesetzentwurf eher auf eine Zentralisierung der Cyberabwehr ausgelegt. Das hat Vor- und Nachteile. Zu den Vorteilen gehört eine Bündelung von Kompetenzen und Expertise sowie eine klare Verantwortlichkeit für das Thema IT-Sicherheit. Nachteilig kann sich hingegen auswirken, dass eine zentrale Steuerung der IT durch zentrale Systeme und Vorgaben den Schaden im Schadensfalle vergrößern kann. Zentral gesteuerte Systeme sind „attraktiver" für Cyberangriffe als dezentrale Systeme.

Organisatorisch bemerkenswert ist, dass der CISO nach derzeitigem Geschäftsverteilungsplan der Landesregierung (GVBl. 2019, 56) im Innenministerium angesiedelt ist. Das ist einerseits folgerichtig, da das Innenministerium für allgemeine Fragen der Verwaltungsorganisation sowie für die Gefahrenabwehr zuständig ist. Fragen der Cybersicherheit von Behörden haben starke sachliche Bezüge zu beiden Bereichen. Andererseits besteht in Hessen seit 2019 ein „Digitalministerium", das bisher über keinen „echten" Geschäftsbereich verfügt. Hier bestünde die Chance, das Digitalministerium jenseits von Fototerminen bei innovativen Unternehmen mit echten eigenen Verwaltungskompetenzen auszustatten. Dies wäre auch im Sinne einer klaren politisch zuordbaren Verantwortung für „Cyberunfälle".

Klarstellen sollte das Gesetz, dass sich die Zuständigkeit des CISO nicht auf die Landtagsverwaltung und den Rechnungshof erstreckt, da dies mit der Unabhängigkeit dieser Verfassungsorgane unvereinbar erscheint. Beide Institutionen sind zwar nach § 18 Abs. 2 E-HITSiG von Meldepflichten bei IT-Störfällen ausgenommen, um dieser Unabhängigkeit gerecht zu werden.

EBS UNIVERSITÄT

Vorzugswürdig wäre allerdings eine Klarstellung in § 1, dass beide Organe insgesamt vom Geltungsbereich des Gesetzes ausgenommen sind.

Abschließend hierzu möchte ich unterstreichen, dass sich IT-Sicherheit nicht allein durch Regelung einer angemessenen Behördenstruktur sicherstellen lässt. Erforderlich sind vor allem ausreichende personelle und sachliche Ressourcen. Insofern steht das Land vor der fortlaufenden Aufgabe, in einem schwierigen Arbeitsmarktumfeld ausreichend attraktiv für entsprechende IT-Fachkräfte zu sein.

II. Materielle Maßnahme: Rechtsgrundlagen für Grundrechtseingriffe

Die §§ 7-16 sollen als Rechtsgrundlagen für Grundrechtseingriffe dienen, die mit IT-Sicherheitsmaßnahmen verbunden sind. § 7 regelt dabei allgemein die Verarbeitung personenbezogener Daten, § 8 die automatisierte Auswertung von Meta- und Protokolldaten und § 9 die Erhebung und Auswertung des Datenverkehrs innerhalb des Landesdatennetzes. Die §§ 10 und 11 regeln die Speicherung und Auswertung von Daten bei konkreten Anhaltspunkten für eine Cybergefahr. § 13 enthält eine Übermittlungsbefugnis. Besonders bemerkenswert ist insofern die Möglichkeit zur Übermittlung an die Strafverfolgungsbehörden, insbesondere bei Anhaltspunkten für eine Katalogstraftat (§ 13 Abs. 3 Nr. 1 HITSiG).

Die Annahme des Gesetzgebers, dass in Grundrechte eingegriffen wird, wenn der Datenverkehr innerhalb der Behörden-IT des Landes ausgewertet wird, ist nicht von vornherein selbstverständlich. Soweit es um dienstliche Telekommunikation geht, dürften sich die für das Land Hessen handelnden Amtsträger nicht auf Grundrechte berufen können. Denn Grundrechte sind Abwehrrechte des Bürgers gegen den Staat, weshalb der Staat als solcher nicht grundrechtsberechtigt, sondern grundrechtsverpflichtet ist. Das gilt auch für seine Amtsträger in Ausübung ihres Dienstes, weil sich die Grundrechtsbindung des Staates nur durch die Grundrechtsbindung seiner Amtsträger verwirklichen lässt. Soweit Behörden mit Außenstehenden – nämlich mit den Bürgern – kommunizieren, können sich zwar diese auf Grundrechte berufen. Wenn die Bürger aber selbst eine Behörde beispielsweise per Email anschreiben, so liegt in der Kenntnisnahme dieser Email durch die Behörde kein Eingriff in Art. 10 GG vor. Dies würde die Zweckrichtung des Grundrechts, die vertrauliche Kommunikation zwischen Bürgern zu schützen, völlig verfehlen. Jedenfalls willigt der Bürger, der eine Behörde elektronisch kontaktiert, in die Kenntnisnahme dieser Kommunikation ein, weil dies gerade Zweck seiner Nachricht ist. Insofern scheint es mir auch nicht grundrechtlich rechtfertigungsbedürftig, wenn die Metadaten einer solchen Kommunikation zwischen Bürger und Behörde automatisiert zur Abwehr etwaiger Cyberangriffe ausgewertet wird.

Aus meiner Sicht ist die Überwachung der verwaltungseigenen IT deswegen eher in untypischen Konstellationen mit Grundrechtseingriffen verbunden, etwa bei der Versendung privater Emails

EBS UNIVERSITÄT

vom Dienstcomputer aus (Grundrechtseingriff bejaht für die Überwachung eines Diensttelefons bei privaten Gesprächen *Jarass*, in: Jarass/Pieroth, Art. 10 Rn. 27). Diese Grundrechtseingriffe lassen sich jedenfalls im Grundsatz mit dem Ziel der Abwehr von Cyberangriffen auf die IT-Infrastruktur des Landes rechtfertigen, zumal es sich hierbei um ein überragend wichtiges Gemeinschaftsgut handelt, weil es um den Schutz der Funktionsfähigkeit der staatlichen Verwaltung geht. Dem Gewicht etwaiger Grundrechtseingriffe tragen die einzelnen Ermächtigungsgrundlagen durch verfahrensrechtliche Absicherungen Rechnung. Hervorzuheben sind insofern die im Einzelnen mit steigender Eingriffsintensität qualifizierteren Gefahrbegriffe (vgl. etwa § 10 Abs. 2 E-HITSiG). Überdies führt die im Regelfall vorgesehene Automatisierung der Auswertung dazu, dass die meisten Daten nur technisch ausgewertet werden, was eine geringere Eingriffsintensität bedeutet als die Prüfung von Telekommunikationsvorgängen durch Verwaltungsmitarbeiter.

Für klärungsbedürftig halte ich indes die Frage, unter welchen Voraussetzungen Inhaltsdaten gesammelt und ausgewertet werden dürfen. Seiner Überschrift nach regelt § 11 E-HITSiG die Auswertung von Inhaltsdaten. Der Verweis in § 11 Abs. 1 E-HITSiG verweist in die Erhebung von Metadaten. Insofern ist mir nicht klar, an welcher Stelle genau die Inhaltsdaten erhoben werden.

III. Schlussbemerkung

Das Ziel, die IT-Sicherheit der hessischen Verwaltung zu stärken, ist uneingeschränkt zu begrüßen. Im Hinblick auf die Ermächtigungsgrundlagen für etwaige Grundrechtseingriffe mögen diese zusätzliche Rechtssicherheit in bestimmten Fallkonstellationen schaffen. Die Überwachung von dienstlicher Kommunikation zwischen Verwaltung und Bürgern und erst Recht die Überwachung innerdienstlicher Kommunikation dürfte aber regelmäßig ohnehin keinen rechtfertigungsbedürftigen Eingriff in Art. 10 GG begründen. Die Bündelung von Kompetenz in einer zentralen Stelle wie dem CISO ist grundsätzlich sinnvoll, darf aber nicht dazu führen, dass sich die einzelnen Behörden allein auf den CISO verlassen. IT-Sicherheit ist grundsätzlich auch dezentral zu gewährleisten. Entscheidend sind dabei nicht allein Verwaltungsstrukturen, sondern fortlaufend ausreichende Investitionen in personelle und sächliche Ressourcen im Bereich der IT-Sicherheit.

Mit freundlichen Grüßen

Matthias Friehe

Professor Dr. Matthias Friehe

Gemeinsame Stellungnahme zu dem Vorschlag eines Hessischen Gesetzes zum Schutz der elektronischen Verwaltung (HITSiG)

Prof. Dr. Haya Shulman

Institut für Informatik, Goethe-Universität Frankfurt am Main,

Fraunhofer-Institut für Sichere Informationstechnologie SIT

und

Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE

Prof. Dr. Michael Waidner

Fachbereich Informatik, Technische Universität Darmstadt,

Fraunhofer-Institut für Sichere Informationstechnologie SIT

und

Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE

Sehr geehrte Damen und Herren,

gerne kommen wir hiermit Ihrer Bitte um Stellungnahme des vom Kabinett mit Beschluss vom 16. Januar 2023 gebilligten Entwurfes eines Gesetzes zum Schutz der elektronischen Verwaltung (HITSiG) nach.

1. Zum Zweck und Inhalt des Vorschlages eines Hessischen Gesetzes zum Schutz der elektronischen Verwaltung (HITSiG)

Nachdem das Land Hessen bereits in den 1970er Jahren eine Vorreiterrolle im Datenschutz eingenommen und maßgeblich die Gesetzgebung in diesem Bereich mitbestimmt hat, ist es sehr zu begrüßen, dass es auch im Bereich der IT-Sicherheit der öffentlichen Verwaltung ein hohes Schutzniveau anstrebt.

Der Gesetzesentwurf erkennt richtigerweise, dass die Handlungsfähigkeit der öffentlichen Verwaltung auf allen Ebenen immer stärker von Informations- und Kommunikationstechnologien abhängt, die durch Cyberkriminalität in unterschiedlichen Ausprägungen (z.B. Eingriffe in die Privatsphäre der Bürgerinnen und Bürger, Beeinflussung von Wahlen, Wirtschaftsspionage) bedroht wird.[1] Es ist vor diesem Hintergrund wichtig und richtig, dass sich das Land Hessen mit dem Schutz dieser Technologien – inklusive der mit ihrer Hilfe verarbeiteten personenbezogenen und nicht personenbezogenen Informationen – gegen unberechtigte Zugriffe und sonstige Einflussnahmen befasst.

Um diese Aufgabe effizienter als bisher erfüllen zu können, soll in Hessen das Zentrum für Informationssicherheit entstehen, das mit anderen relevanten und für die Informationssicherheit zuständigen Stellen des Bundes und der Länder zusammenarbeiten soll. Der Auf- und Ausbau des Zentrums – insbesondere hinsichtlich erforderlicher technischer Voraussetzungen – soll unter Einbeziehung des bestehenden Sicherheits- und Computer-Notfallteams (CERT) erfolgen, welches in das Zentrum für Informationssicherheit integriert werden soll. Zusätzlich soll durch den HITSiG-Gesetzesentwurf die Position der oder des Zentralen Informationssicherheitsbeauftragten der Hessischen Landesverwaltung (CISO) etabliert und gesetzlich verankert werden.[2]

Die dadurch erfolgende Stärkung der Informationssicherheit, einschließlich der Etablierung und Vernetzung der vorgenannten Stellen und Funktionen, ist zielführend und zu begrüßen. Es ist zu erwarten, dass durch den Aus- und Aufbau dieser Stellen und Funktionen die Informationssicherheit innerhalb Hessens deutlich gestärkt werden wird und im Ergebnis das Vertrauen in sowie die Bereitschaft zur Nutzung (neuer) Technologien durch Bürgerinnen, Bürger und Unternehmen wachsen wird, ohne dass natürliche Personen durch die durch den Gesetzesentwurf neu geschaffenen Stellen, Funktionen und Befugnisse unangemessene Eingriffe in ihre Rechte und Freiheiten hinnehmen müssen.

Das Gesetz bietet eine Grundlage für einen Strukturaufbau, der Vorbildwirkung für andere Bundesländer entfalten kann. Dies gelingt allerdings nur, wenn die Umsetzung so erfolgt, dass sich

[1] Abschnitt A. 1. der Begründung des HITSiG-Gesetzesentwurfes (S. 14 f.).
[2] § 5 Abs. 3 des HITSiG-Gesetzesentwurfs; Abschnitt A. 1. und B. zu § 5 der Begründung des HITSiG-Gesetzesentwurfes (S. 15, 22).

die neu geschaffenen Strukturen nahtlos in die Cybersicherheitsarchitektur Deutschlands integrieren und in die Meldewege und Prozesse einheitlich, zielführend und schlank einpassen lassen.

2. Zu einzelnen Aspekten des Vorschlages eines Hessischen Gesetzes zum Schutz der elektronischen Verwaltung (HITSiG)

Der Gesetzesentwurf sieht eine Vernetzung mit der Cybersicherheitsforschung, bspw. Im Bereich der Untersuchung von Sicherheitsrisiken bei Anwendung der Informationstechnik sowie Tests von vorhandenen Verfahren und Werkzeugen sowie deren Entwicklung zur Erkennung und Abwehr von Gefahren für die Informationssicherheit in Zusammenarbeit mit Wissenschaft und Forschung vor. Es wird angeregt, die Verknüpfung noch stärker im Gesetz zum Ausdruck zu bringen und auf weitere Bereiche auszudehnen, z.B. durch eine Festschreibung der Möglichkeit der Einbeziehung der angewandten Forschung in Fällen akuter Cybersicherheitsbedrohungen und -vorfälle, in denen (Schutz-)Maßnahmen des Standes der Technik nicht ausreichen. Gerade in Hessen existiert mit dem Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENE eine exzellente, agil handlungsfähige und große Forschungseinrichtung, die nachweislich ihre Expertise bei Vorfällen nutzbringend eingesetzt hat. Zusätzlich erscheinen an dieser Stelle das Festschreiben von Schulungsmaßnahmen zu Schutzmaßnahmen des Standes der Technik und der Forschung zielführend.

Die in § 8 Abs. 1 und 9 Abs. 1 HITSiG beschriebenen Technologien und Systeme sind abschließend beschrieben. Die Norm lässt so keinen Spielraum für Änderungen am Stand der eingesetzten Technik und erscheint zu dem in Hinblick auf Cloud-Services, KI-Anwendungen und Security-Appliances nicht vollständig. Dies könnte beispielsweise hinderlich für die Auswertungsmöglichkeiten bei der Vorfallsbearbeitung sein. Eine Lösungsmöglichkeit wäre es, eine abstrakte Beschreibung der Technik an den Beginn der Aufzählung zu stellen und danach alles, was jetzt schon genannt wird (und genannt werden kann), als eine nicht abschließende Liste von Beispielen wiederzugeben.

Der § 8 Abs. 1 spezifiziert nicht, von wem die Protokolldaten automatisiert ausgewertet werden dürfen. Es bleibt offen, ob z. B. auch der Anbieter oder Hersteller der IT-Systeme oder ein Dienstleister die Auswertung vornehmen darf. Wenn die Auswertungen extern vorgenommen werden und man sich auf die Ergebnisse eines Dienstleisters verlässt, ergeben sich weitere Fragen der Cybersicherheit und des Datenschutzes.

Der/die Chief Information Security Officer (CISO) kann Sicherheitsmaßnahmen anordnen (§ 4 Abs. 3), dies ist eine weitgehende Befugnis. Möglicherweise könnte diese Befugnis noch genauer umschrieben werden. Wiederum scheinen die Befugnisse des/der CISO hinsichtlich des zentralen IT-Dienstleisters eingeschränkt zu sein:

- Der/die CISO hat im Regelbetrieb keinen Zugriff auf die Protokolldaten des zentralen IT-Dienstleisters – dies scheint erst in einer Krise oder einem Vorfall über das Zentrum für Informationssicherheit möglich zu werden.
- Die Kompetenzverteilung zwischen den in lit. a und lit. b von § 5 Abs. 2 Nr. 5 genannten Stellen ist unklar: Haben diese Stellen Anspruch auf die Unterstützung durch das Zentrum für Informationssicherheit, oder haben sie diesem gegenüber Weisungsrechte?

Ferner möchten wir die Möglichkeit der Stellungnahme für einige perspektivische Anmerkungen nutzen. IT-Sicherheit ist sowohl technisch als auch legislativ ein schnelllebiger Bereich. Es ist zu vermuten, dass das HITSiG bereits vor dem im Entwurf vorgesehenen Außerkrafttreten im Dezember 2030 eine Novellierung erfahren wird. Folgende Themen sind bereits jetzt Gegenstand umfangreicher Forschungsvorhaben und sollten bei künftigen Gesetzesaktualisierungen berücksichtigt werden.

Aktive Cyberabwehr

Unter aktiver Cyberabwehr ist eine Reihe von Technologien und Maßnahmen zu verstehen, die Strafverfolgungsbehörden dabei unterstützen können, Straftaten im Cyberraum zu verhindern, abzumindern oder zu verfolgen. Aktive Cyberabwehr wird in der Öffentlichkeit häufig mit Hackbacks gleichgesetzt. Unter einem Hackback versteht man allerdings einen digitalen Vergeltungsangriff gegen den Cyberangreifer, also eine Maßnahme, die auf Rache angelegt ist, nicht auf die Verfolgung und Vereitelung von Straftaten.[3] Es ist absehbar, dass Maßnahmen der passiven Cyberabwehr ihre Grenzen erreichen, während (erste) Maßnahmen der aktiven Cyberabwehr in den kommenden Jahren zum Stand der Technik zählen werden.

Vor diesem Hintergrund ist es zu begrüßen, dass in der Gesetzesbegründung die Möglichkeit der aktiven Cyberabwehr unter Zugrundelegung des o.g. Begriffsverständnisses aufgeführt wird. In künftigen Gesetzesnovellierungen sollte das Thema Aktive Cyberabwehr in den Gesetzestext einfließen.

Zero Trust

Ein technisch höheres Cybersicherheitsniveau für die Landesverwaltung kann künftig durch eine Zero-Trust-Architektur erreicht werden. Zero Trust bedeutet zunächst, ein IT-System so abzusichern, dass nichts oder zumindest möglichst wenig über die Sicherheit anderer IT-Systeme angenommen werden muss. Ganz kann das natürlich nicht gelingen, einzelne Komponenten eines IT-Systems können immer korrumpiert werden, etwa wenn ein Angreifer erfolgreich den Hersteller der Komponente angreift. Das zweite Ziel von Zero Trust ist deshalb, es dem Angreifer zumindest so schwer wie irgend möglich zu machen, sich nach einem erfolgreichen Angriff auf eine Komponente weiter im IT-System auszubreiten.

Prävention

Der aktuelle Gesetzentwurf geht mehr auf Reaktion ein als auf präventive Maßnahmen. In späteren Fassungen könnten beispielsweise Forensic Readiness und Übungen festgeschrieben werden:

- **Forensic Readiness** kann im Falle eines Vorfalls eine effektive und effiziente Untersuchung ermöglichen. Im Idealfall gelingt es schnell den Ursprungsort der Ausbreitung des Vorfalls zu finden und betroffene von nicht betroffenen Systemen zu unterscheiden. Die Ausfallzeit wird auf diese Weise minimiert und die Handlungsfähigkeit des Landes bleibt zu jeder Zeit bestehen. Der zweite essenzielle Aspekt der Forensic Readiness ist die Schaffung von

[3] Shulman/Waidner, Aktive Cyberabwehr (ATHENE-Whitepaper, Darmstadt 2022), S. 3.

digitalen Indizien bis hin zu Beweismitteln, so dass eine Beweiskette erstellt werden kann, die von der Strafverfolgung verwendet werden kann.

- **Übungen** und kontinuierliches Training sind die Basis für zielführendes Handeln bei realen Vorkommnissen. Dies gilt für die Polizei, die Feuerwehr, das Technische Hilfswerk, die Bundeswehr und im gleichen Maße für alle, die potenziell in Cybersicherheitsvorfälle involviert werden könnten. Im Bereich des Cybersicherheitstrainings muss Cybersicherheitshandeln aktiv und praktisch geübt werden. Neben der Schulung von Verteidigungstechniken (defensiver Herangehensweisen) trägt auch die Vermittlung von Hacking-Techniken (offensiver Fähigkeiten) zur Steigerung zielführenden Handelns im Ernstfall bei.

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Der Vizepräsident
Bundesamt für Sicherheit in der Informationstechnik, 53175 Bonn

Hessischer Landtag
- Innenausschuss -
Schlossplatz 1-3
65183 Wiesbaden
-per E-Mail-

Dr. Gerhard Schabhüser
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189
53175 Bonn

Postanschrift:
Postfach 20 03 63
53133 Bonn

Tel. +49 228 99 9582-5210
Fax +49 228 99 10 9582-5210

vizepraesident@bsi.bund.de

www.bsi.bund.de

Betreff: Öffentliche Anhörung im Innenausschuss des Hessischen Landtags am 15.05.2023

Bezug: Ihr Schreiben I 2.2, vom 03.04.2023
Az.: BL22 – 001 00 08
Datum: 11.05.2023
Seite 1 von 1

Sehr geehrter Herr Vorsitzender Heinz,
Sehr geehrte Damen und Herren Abgeordnete,
Sehr geehrte Frau Lingelbach,
Sehr geehrter Frau Müller,

vielen Dank für Ihre Anfrage. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterstützt und fördert den Ausbau einer gesamtstaatlichen Cybersicherheitsarchitektur. Aus diesem Grund setzen wir uns für die Errichtung einer Zentralstelle im Bund-Länder-Verhältnis beim BSI ein, um in Zusammenarbeit mit den Ländern ganzheitliche Cyber-Sicherheit für Staat, Wirtschaft und Gesellschaft weiter auszubauen. Momentan sind die Ressourcen für die Unterstützung der Länder des BSI aufgrund von verfassungsrechtlicher Schranken hier sehr begrenzt.

Gerne äußern wir uns nachfolgend zu dem von Ihnen vorgelegtem Gesetzentwurf der hessischen Landesregierung „Hessisches Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz HITSiG)“ in Form von rechtlichen Anmerkungen. Bitte haben Sie Verständnis, dass diese lediglich das Ergebnis einer im Umfang begrenzten Prüfung sind.

Bei § 1 erscheint die Bezugnahme auf „elektronische Verwaltungstätigkeit“ unpräzise, da diese im nachfolgenden § 2 nicht aufgegriffen und definiert wird. Zur Vermeidung von Unklarheiten sollte hier ggf. von „Verwaltungstätigkeit mittels Informationstechnik“ gesprochen werden.

Auch zu § 5 gibt es Anmerkungen seitens des BSI. So fehlt in Absatz 2 der Anker zu § 7. Wichtig ist, dass alle gesetzlichen Aufgaben „im öffentlichen Interesse“ liegen, um von bestimmten Verarbeitungserleichterungen zu profitieren. Bei Absatz 2 Nr. 5 stellt sich im Sinne der Doppeltür-Rechtsprechung des BVerfG die Frage, ob die Übermittlung von Daten von und an die Polizeien und Nachrichtendienste ausreichend klar geregelt sind. In der Praxis werden nämlich erfahrungsgemäß umfangreiche Daten übermittelt und ausgetauscht. In Absatz 2 Nr. 9 erweckt die Formulierung „werktägliche Übersicht“ den Eindruck, als würde die Lage nicht durchgängig und tagesaktuell beobachtet. Vor dem Hintergrund, dass Gefährdungen der Informationssicherheit rund um die Uhr auftreten können, sollte das überdacht werden.

Zu § 10 ist generell anzumerken, dass die Norm davon ausgeht, dass bereits eine automatisierte Auswertung nach §§ 8 oder 9 zu zureichenden tatsächlichen Anhaltspunkten für das Vorliegen eines Angriffs führen kann. Aus der Praxis des BSI kann berichtet werden, dass dies nicht der Fall ist. Deshalb ermöglicht § 5 Abs. 2 und Abs. 3 BSIG eine Depseudonymisierung von Daten, um „den Verdacht [auf Vorliegen eines Schadprogramms] zu bestätigen oder zu widerlegen“. Oftmals verbleiben nach der automatisierten Analysestrecke nämlich Zweifel, weshalb genau eine bestimmte Signatur angeschlagen hat und diese Zweifelsfälle müssen durch manuelle Analyse durch Zuhilfenahme von depseudonymisierten Daten geklärt werden – erst danach steht fest, ob hinreichende tatsächliche Anhaltspunkte vorliegen oder nicht. Im letzteren Fall konnte der vermutete Verdacht widerlegt werden. Diese Möglichkeit fehlt den §§ 10 und 11. Hierdurch dürfte die Praxistauglichkeit der Normen stark vermindert sein.

Zwischen § 16 HITSiG und § 5b BSIG dürfte ein Konflikt bestehen. Das BSI darf gem. § 5b Abs. 7 BSIG auch Stellen der Länder unterstützen. Wenn allerdings bereits Unterstützung durch ein MIRT gem. § 16 HTSiG geleistet wird, so müsste wohl ein herausgehobener Fall gem. § 5b Abs. 2 BSIG und damit ein begründeter Einzelfall verneint werden. Eine zusätzliche Unterstützung durch ein BSI MIRT wäre dann vermutlich nicht möglich.

Bei § 18 empfiehlt es sich, nach Möglichkeit eine Verpflichtung zur Meldung von sog. „Nicht-Meldungen“ aufzunehmen. Also die Anzahl derjenigen Fälle, die von bestimmten Stellen nicht übermittelt worden ist. Auf diese Art und Weise können „Meldungslücken“ und „blinde Flecken“ durch Zahlenmaterial belegt werden, wodurch ein exekutives oder gesetzgeberisches Gegensteuern ermöglicht werden kann.

Falls es Ihrerseits zukünftig weitere konkrete Fragen zur Cyber-Sicherheit geben sollte, kommen Sie gerne wieder auf das BSI zu. Auch stehen mein Haus und ich gerne für sämtliche Fragen rund um die angestrebte Zentral-

Bundesamt
für Sicherheit in der
Informationstechnik

stellenfunktion zur Verfügung. Diese würde es ermöglichen, die Zusammenarbeit zwischen dem BSI und dem Land Hessen, die derzeit im Rahmen einer Kooperationsvereinbarung erfolgt, dauerhaft zu vertiefen.

Mit freundlichen Grüßen

Dr. Gerhard Schabhüser

DER HESSISCHE BEAUFTRAGTE
FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT

DER HESSISCHE BEAUFTRAGTE
FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT
Postfach 31 63 · 65021 Wiesbaden

Vorsitzender des Innenausschusses
des Hessischen Landtags
Herrn Christian Heinz
Schlossplatz 1-3
65183 Wiesbaden

Aktenzeichen *Bitte bei Antwort angeben*	15.52:Schriftverkehr-hk
zuständig	Frau Horlbeck
Durchwahl 14 08 -	146
Ihr Zeichen	
Ihre Nachricht vom	03.04.2023
Datum	03.05.2023

Anhörung zum Hessischen Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG) – Drucks. 20/10752 –

Sehr geehrter Herr Vorsitzender,

vielen Dank für die Möglichkeit der Stellungnahme zum Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG).

Das Vorblatt zum Gesetzesentwurf führt zutreffend aus, dass Informationssicherheit und Datenschutz elementare Voraussetzungen für eine erfolgreiche Digitalisierung sowie das Vertrauen von Bürgerinnen und Bürgern in staatliches Handeln sind. Diesem Leitgedanken folgend wurde meine Behörde zeitig und umfassend bei der Ausarbeitung des nunmehr vorgelegten Gesetzesentwurfs der Landesregierung beteiligt. Die von meiner Behörde eingebrachten Änderungsvorschläge wurden überwiegend berücksichtigt und umgesetzt. Für die enge Abstimmung und den konstruktiven Austausch möchte ich mich daher ausdrücklich bedanken.

Aufgrund der frühen Einbindung und der Berücksichtigung meiner Anregungen bestehen datenschutzrechtliche Bedenken lediglich mit Blick auf die in § 17 Satz 1 HITSiG enthaltene Interessenabwägung zur Information der Betroffenen. Die DS-GVO kennt

Gustav-Stresemann-Ring 1 · 65189 Wiesbaden · Telefon (06 11) 14 08-0
E-Mail poststelle@datenschutz.hessen.de · DE-Mail: poststelle@datenschutz-hessen.de-mail.de
Internet www.datenschutz.hessen.de
Bankverbindung: Kontoinhaber HCC/Kanzlei Hess.Landtag/DB · IBAN DE67 5005 0000 0001 0053 62 · BIC HELADEFFXXX
USt IdNr: DE812021807

keine Interessenabwägung bei der Informationspflicht nach Art. 13 und 14 DS-GVO. Zwar sieht Art. 23 DS-GVO die Möglichkeit der Beschränkung vor. Dies jedoch nur dann, „*sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt*“. Die aktuelle Formulierung stellt jedoch lediglich auf das überwiegende Interesse des Verantwortlichen ab. Weder der Wortlaut des Gesetzes noch die Gesetzesbegründung enthalten ergänzende Hinweise zur Auslegung. Sowohl für den Rechtsanwender als auch für die Betroffenen bietet die aktuell gewählte Formulierung daher Potential für Unsicherheiten bei der Rechtsanwendung.

Mit freundlichen Grüßen

Prof. Dr. A. Roßnagel