– Ausschussvorlage INA 20/75 –
– öffentlich –

Stellungnahmen der Anzuhörenden zur mündlichen Anhörung des Innenausschusses und des Ausschusses für Soziales und Integration

Sitzung am 15. Mai 2023

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

Fraport AG
Frankfurt Airport Services Worldwide

25.04.2023

Hallo zusammen,

wie versprochen anbei das Feedback zu dem Entwurf.

Positiv:

- Etablierung formale Rolle CISO für Land Hessen
- Bündelung der Kompetenzen im Zentrum für Informationssicherheit
- Angebot des CERT seine Dienstleistungen auch privaten Unternehmen im Land Hessen anzubieten, sofern die Kapazität ausreicht (§ 5 Nr. (3))

Zu überdenken:

- §8 (1): Mit der Auflistung der 6 Systembereiche schränkt man sich ggf. zu sehr ein. Es können auch weitere Protokolldateien wichtig werden (bspw. Applikationslogs, die nicht im Betriebssystemlog protokolliert werden oder Intrusion Prevention Systeme (Fallen meines Erachtens in keine der Kategorien, da sie keine Schadsoftware, aber bösartige Anfragen blocken)). Müsste man dann immer erst das Gesetz anpassen, um diese auszuwerten?
- $11: Bei der Auswertung von Inhaltsdaten sollte wie in §10 (ohne Inhaltsdaten) auch der „Verdacht eines Angriffs“ aufgenommen werden. Hier rein auf Schadprogramme zu referenzieren könnte zu sehr einschränken. Auch bei Angriffen ohne Schadprogramme müssen ggf. Inhaltsdaten analysiert werden.
- § 18: Müssen in (2) so viele Stellen von der Meldepflicht ausgenommen werden? Warum sollten bspw. Hochschulen nicht auch Melden, wenn bedeutsame Gefahren bestehen?

Aktuell nicht zu bewerten auf Grund fehlenden Wissens meinerseits:

- Gibt es Stellen im Geltungsbereich, die bereits anderen Regularien unterliegen (bspw. aus dem BSIG)? Dann sollte ggf. dargestellt werden, welche Regulierung höherwertig anzusehen ist, um Doppel-Regulierung zu vermeiden. Zumindest sollte eine einheitliche Nachweisführung berücksichtigt werden.

Viele Grüße
Alexander Döhne

Informations- und Telekommunikationsdienstleistungen
Leiter Cyber Security und IT-Governance, IUK-CI

Universität Bremen

IGMR
Institut für Informations-,
Gesundheits- und Medizinrecht

Universität Bremen | Postfach 33 04 40, 28334 Bremen
IGMR | FB06

Hessischer Landtag
Innenausschuss
Schlossplatz 1-3
65183 Wiesbaden

nachrichtlich per E-Mail

Bremen 26. April 2023

Fachbereich 06
Rechtswissenschaft

Prof. Dr. jur. Dennis-Kenji Kipker

GW 1
Universitätsallee
28359 Bremen

Tel. 0421 5905 5465
Fax 0421 218 66052
kipker@uni-bremen.de

www.igmr.uni-bremen.de
igmr@uni-bremen.de

Prof. Dr. jur. Dennis-Kenji Kipker

Schriftliche Stellungnahme

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

Universität Bremen

IGMR
Institut für Informations-, Gesundheits- und Medizinrecht

I. Vorbemerkung und rechtspolitischer Hintergrund

Eine Interpretation und Bewertung des vorliegenden Gesetzentwurfs muss vor dem Hintergrund der gesetzgeberischen und politischen Regelungsintention vorgenommen werden. Einerseits beschreibt das BSI in seinem Bericht zur Lage der IT-Sicherheit in Deutschland 2022 die Gefährdungslage als so hoch wie noch nie, andererseits nimmt die Nutzung und Vernetzung von IT rapide zu. So ergeben sich zwar die Bedarfe für die Digitalisierung, es wachsen jedoch auch die technischen Digitalisierungsrisiken gleichzeitig exponentiell an. Insbesondere die öffentliche Verwaltung steht unter einem zunehmenden Digitalisierungszwang, um die Erwartungen von Bürgerinnen und Bürgern an eine zeitgemäße und interessengerechte behördliche Infrastruktur zu erfüllen. Gleichzeitig wird von der Bevölkerung nicht nur erwartet, dass die digitalisierte Verwaltung im Sinne der Verfügbarkeit fehlerfrei funktioniert, sondern auch, dass (sensible) Bürgerdaten hinreichend vor unbefugter Offenlegung und Manipulation geschützt sind (Authentizität, Integrität und Vertraulichkeit). In diesem Spannungsverhältnis bewegt sich auch der vorliegende Gesetzentwurf, denn eine Gewähr für Cybersicherheit existiert nicht – umso wichtiger ist es daher auch, vor allem präventive Strukturen zu errichten.

Diese Aufgabe erfüllen soll auch das Hessen CyberCompetenceCenter (Hessen3C) im Zuständigkeitsbereich des Hessischen Ministeriums des Innern und für Sport, das als zentraler Ansprechpartner zum Thema Cybersicherheit in Hessen fungiert. Eingerichtet wurde Hessen3C im April 2019 innerhalb der Abteilung Cyber- und IT-Sicherheit, Verwaltungsdigitalisierung und steht seither der hessischen Landesverwaltung, hessischen Kommunen und hessischen Unternehmen in beratender Funktion zur Verfügung. Hessen3C hat ein breit gefasstes Aufgabenspektrum, das nicht nur den Schutz der Landesverwaltung vor Cyberbedrohungen umfasst. Ebenso fällt in den Aufgabenbereich die Unterstützung der Sicherheitsbehörden bei der Ausbildung von Fachkräften, die Bekämpfung von Cybercrime und Cyberspionage sowie die Beratung von Kommunen, Wirtschaft und KRITIS. In letztgenanntem Zusammenhang ist Hessen3C zentra-

le Kontaktstelle zur Entgegennahme landesbezogener KRITIS-Meldungen. Aufgrund des weit gefassten Funktionszuschnitts besteht überdies eine enge Zusammenarbeit mit der Landespolizei und dem Landesamt für Verfassungsschutz. Folgende Leistungen erbringt Hessen3C konkret:

- **Leistungen für die Landesverwaltung:** Unterstützung und Koordinierung der Bearbeitung von Cybersicherheitsvorfällen in der Landesverwaltung. Zentrale Ansprechstelle bei IT-Sicherheitsvorfällen.
- **Leistungen für Kommunen:** Hessische Kommunen können die Leistungen des Hessen3C auf freiwilliger Basis und unter Wahrung des Selbstverwaltungsprinzips kostenfrei nutzen.
- **Leistungen für KRITIS:** Inanspruchnahme des Hessen3C durch KRITIS ist bei Bedarf kostenlos, ergebnisoffen und produktneutral möglich.
- **Leistungen für KMU:** Inanspruchnahme des Hessen3C durch KMU ist bei Bedarf kostenlos, ergebnisoffen und produktneutral möglich.

Mit dem Entwurf für ein HITSiG werden die umfangreichen Befugnisse des Hessen3C an eine Rechtsgrundlage angeknüpft, was gemessen am skizzierten Aufgaben- und Befugnisumfang sinnvoll, sachgerecht und juristisch notwendig erscheint – insbesondere auch deshalb, weil es bislang an einer umfassenden Rechtsgrundlage für Befugnisse und Datenzugriffe in Hessen fehlt, die jedoch dringend erforderlich ist, um Rechtssicherheit und Betroffenenschutz zu gewährleisten, da die Befugnisse teils Grundrechtsrelevanz besitzen. Überdies erfolgt die staatliche Gewährleistung der Cybersicherheit rechtlich nicht im „luftleeren Raum“ – vielmehr kann es zur Gewährleistung der Cybersecurity auch notwendig sein, andere und ebenfalls grundrechtlich geschützte Positionen inhaltlich zu verkürzen, sodass ein gesetzlich skizzierter Interessenausgleich sachgerecht ist. Ein behördliches Tätigwerden ohne entsprechende gesetzliche Grundlage wäre folglich nicht möglich bzw. rechtswidrig. Kernaspekte der zu treffenden Regulierung betreffen nachfolgende thematische Schwerpunkte:

Universität Bremen

IGMR
Institut für Informations-, Gesundheits- und Medizinrecht

- **Zentrum für Informationssicherheit:** U.a. Möglichkeit zum eigenständigen operativen Tätigwerden des Hessen3C in den Bereichen Prävention, Informationssammlung und -auswertung, Erarbeitung von Warnungen und Empfehlungen für Behörden und Öffentlichkeit, aktive Abwehr von Cybergefahren, Dienstleistungen/Auftragsverarbeitung für Kommunen, Einbindung des CERT.
- **Eingriffs- und Abwehrmaßnahmen:** U.a. Befugnis zur Datenanalyse zu Zwecken der Abwehr von Gefahren für die Cybersicherheit, insb. unter Einbeziehung personenbezogener Daten. Des Weiteren Möglichkeiten zur Untersuchung von im Landesdatennetz sowie von in IT-Systemen gespeicherten Daten mit Grundrechtsrelevanz (Fernmeldegeheimnis, informationelle Selbstbestimmung) unter Heranziehung von eingriffsmildernden Verfahrensvorkehrungen und Betroffenenrechten.
- **Zentraler Beauftragter für Informationssicherheit (CISO):** Gesetzliche Verankerung der Position des CISO im Hinblick auf Eingriffsbefugnisse zur Abwehr von Cybergefahren, sowie zu Berichtspflichten und zur Koordinierung des IT-Krisenmanagements.

II. Zu den Vorschriften im Einzelnen

1. § 2 Nr. 1 HITSiG-E – Begriffsbestimmungen

Ausweislich der Entwurfsbegründung basieren die herangezogenen Begriffsbestimmungen auf dem BSIG. Unklar ist, weshalb im Entwurf des HITSiG geringfügig von den entsprechenden BSI-Bestimmungen abgewichen wird, da dies einem einheitlichen systematischen Begriffsverständnis im deutschen IT-Sicherheitsrecht abträglich ist, ohne dass dafür ein sachlich nachvollziehbarer Grund bestehen würde. Datenschutzrechtlich ist die Übermittlung bzw. Übertragung überdies eine Form der Verarbeitung. Die Bestimmung sollte deshalb wie folgt formuliert werden: „Die Informationstechnik im Sinne dieses Gesetzes umfasst alle technischen Mittel zur Verarbeitung von Informationen“.

Universität Bremen

IGMR
Institut für Informations-, Gesundheits- und Medizinrecht

2. § 2 Nr. 2 HITSiG-E – Begriffsbestimmungen

Der Begriff der „Informationssicherheit“ als solcher wird im BSIG nicht definiert. Hier fehlt es gegenwärtig noch an einem klaren begrifflichen Verständnis des hessischen Regelungsvorschlags, da die Begriffe „IT-Sicherheit“, „Cybersicherheit“ und „Informationssicherheit“ eine unterschiedliche Bedeutung haben.[1] Da es im vorliegenden Gesetz wie in der Regelungsintention in Abschnitt I. dieser Stellungnahme um die Sicherheit von vernetzten IT-Systemen geht, wäre zumindest der Begriff der „IT-Sicherheit“ angemessener (die „Cybersicherheit“ findet sich bereits begrifflich nicht in der Gesetzesbezeichnung wieder wie es beispielsweise für Baden-Württemberg mit dem Cybersicherheitsgesetz in Anbetracht der skizzierten technischen Bedrohungslage treffender wäre). Überdies sollten die Schutzziele der IT-Sicherheit abschließend aufgeführt werden, mithin eine Ergänzung um Authentizität und Nichtabstreitbarkeit vorgenommen werden. Fraglich ist überdies, wie in der begrifflich engen Definition, die sich auf das IT-System und dessen Anwendung beschränkt, externe Dienste und Herausforderungen der digitalen Lieferkette angemessen Berücksichtigung finden sollen.

3. § 2 Nr. 3 HITSiG-E – Begriffsbestimmungen

Für die Definition der Schadprogramme wäre in Erweiterung der BSIG-Definition denkbar, zusätzlich den Begriff der Verarbeitung zu ergänzen, soweit dieser nicht unter die unbefugte „Nutzung“ und „Löschung“ von Daten fällt.

4. § 2 Nr. 4 HITSiG-E – Begriffsbestimmungen

Der rechtliche Begriff der „Sicherheitslücke“ ist spätestens seit den Entwicklungen zum Russland-Ukraine-Krieg im Jahr 2022 hoch politisiert und, wie von manch einem Autor behauptet wird, „verbrannt“. Dies ist vornehmlich auf einen juristisch bislang nicht korrigierten Auslegungsfehler des BSI bei der Anwen-

[1] Siehe zu den Begriffen im Einzelnen *Kipker*, Rechtshandbuch Cybersecurity, S. 2 f.

dung der Warnbestimmung zurückzuführen.[2] Wünschenswert wäre deshalb, die Begriffsbestimmung insoweit zu ergänzen bzw. umzuformulieren, sodass deutlich wird, dass es sich bei „Sicherheitslücken“ nicht um politisch zugängliche Wertungen, sondern um originär technisch-organisatorische und damit fachliche Beurteilungen handelt. Ansonsten führt dieser Begriff in der Folge zu einer erheblichen und im Praxisgebrauch weiter perpetuierten Rechtsunsicherheit, wie es aktuell bedauerlicherweise auch im BSIG der Fall ist.

5. § 3 HITSiG-E – Grundsätze der Informationssicherheit

Abs. 1 bestimmt grds. für die Stellen nach § 1 Nr. 1 und Nr. 2, dass angemessene organisatorische und technische Vorkehrungen sowie „sonstige Maßnahmen“ zur Gewährleistung der Informationssicherheit zu treffen sind. Was unter diesen „sonstigen Maßnahmen“ zu verstehen sein soll und inwieweit diese über die vorgeschlagenen TOM hinausgehen sollen, erschließt sich nicht. Empfohlen wird deshalb die Streichung dieser Ergänzung. Überdies wird wie folgt konkretisiert: „Für technische Maßnahmen soll der Stand der Technik maßgeblich sein“. Diese einengende Formulierung wird nicht empfohlen, auch findet sich keine Entsprechung in der bundesrechtlichen Bestimmung, in welcher der „Stand der Technik“ vielmehr auch die organisatorischen Maßnahmen einbezieht. Das erscheint an dieser Stelle sinnvoll, da der nachfolgende Verweis auf die IT-Grundschutzmethodik die Umsetzung eines ISMS verlangt, das eben nicht nur aus rein technischen Maßnahmen besteht. Auch „organisatorische Maßnahmen“ sind einer Bewertung nach dem Stand der Technik zugänglich, soweit sie im Kontext der IT-Sicherheit eingesetzt werden.

Abs. 3 bestimmt die Gewährleistungsverantwortung der Informationssicherheit für die jeweiligen Geschäftsbereiche. Vorgeschrieben wird die Benennung von ISBs. Hier sollte ergänzt werden, dass der ISB die erforderliche Qualifikation besitzen sollte, um die Aufgaben und Anforderungen seines Tätigkeitsbereichs angemessen zu erfüllen.

[2] Dazu im Detail *Kipker*, „Die Sicherheitslücke im BSIG – Möglichkeiten und Grenzen der juristischen Auslegung eines Rechtsbegriffs“, MMR 2023, 93 ff.

Abs. 4 legt fest, dass die ISBs an wesentlichen Änderungen von IT-Systemen zu beteiligen sind. Solche „wesentlichen Änderungen“ sollten spezifiziert werden, beispielsweise im Hinblick auf Funktionsauswirkungen, ihrem Bezugspunkt in der Hard- und Software oder mit Blick auf potenzielle Folgen für die Cybersicherheit. Unklar ist außerdem, welche Folge die Beteiligung des ISBs letztlich haben kann. Im Sinne der Informationssicherheit anzudenken wäre beispielsweise ein „Vetorecht“ des ISBs, falls bestimmte Änderungsvorschläge der IT-Infrastruktur grundlegende Sicherheitsbedenken zur Folge haben.

Für Abs. 5 wäre außerdem eine leichte begriffliche Verschärfung anzudenken, ohne damit die kommunale Selbstverwaltungsautonomie über Gebühr einzuschränken: Anstelle von „empfohlen“ die Formulierung „nahegelegt“.

6. § 4 HITSiG-E – Die oder der Zentrale Informationssicherheitsbeauftragte der Landesverwaltung

Der Zentrale Informationssicherheitsbeauftragte der Landesregierung ist für die Herstellung der ressortübergreifenden Informationssicherheit zuständig und nimmt in diesem Zusammenhang u.a. die Außenvertretung der hessischen Landesverwaltung in den Belangen der Informationssicherheit wahr. Die Aufgabenbeschreibung in Abs. 2 ist nicht abschließend, jedoch sollte hier noch stärker als in der bislang vorgeschlagenen Fassung der präventive Aspekt der Informationssicherheit, die Förderung von Cybersecurity Awareness und der Informationsaustausch als zentraler Stelle in den Mittelpunkt gestellt werden. Auch wäre es sinnvoll, die Abgrenzung zu weiteren IT-bezogenen Ämtern im Bereich der Landesverwaltung in Kürze zu skizzieren und begrifflich darzustellen. Im Hinblick auf die Befugnisse des CISO nach Abs. 3 ist die Anordnungsbefugnis zu IT-Sicherheitsmaßnahmen bei Gefahr im Verzug sinnvoll. Ergänzend wäre noch eine Begründungspflicht der Dienststellen im Allgemeinen anzudenken, sollten sie den Empfehlungen des CISO nicht folgen bzw. eigene Maßnahmen zur Cybersicherheit ergreifen.

Universität Bremen

IGMR
Institut für Informations-, Gesundheits- und Medizinrecht

7. § 5 HITSiG-E – Zentrum für Informationssicherheit

Das Zentrum für Informationssicherheit ist durch den für die IT- und Cybersicherheit in der Landesverwaltung zuständigen Minister einzurichten. Die Aufgaben sind vielfältig und betreffen in erster Linie eine aktive Koordinierungsfunktion sowie Aufgaben der Sammlung und Auswertung cybersicherheitsrelevanter Informationen. Insgesamt sollte dabei deutlich werden, dass das Zentrum für Informationssicherheit zuvorderst eine präventive Rolle für den Aufbau effektiver Informationssicherheitsinfrastrukturen darstellt, so werden in der Entwurfsfassung bislang keine Fragen des Informationssicherheitsmanagements begrifflich deutlich adressiert. Ebenso fehlen in der Aufgabenbeschreibung Vorgaben zur Zusammenarbeit mit privaten Stellen (insb. public private partnerships) zur Verbesserung der Effektivität nach dem HITSiG getroffener und zu treffender Maßnahmen. Hier sollte noch stärker als bislang die multidimensionale Bedrohungslage Berücksichtigung finden, da Bedrohungen für den privaten Sektor auch für den öffentlichen Sektor relevant sein können und eine Zusammenarbeit an dieser Stelle deshalb sinnvoll erscheint – dies insbesondere auch vor dem Hintergrund, dass Bestandteil des Zentrums für Informationssicherheit das CERT ist, das die Funktion als zentrale Kontaktstelle nach dem BSIG wahrnimmt und seine Leistungen auch gegenüber privaten Unternehmen erbringen kann.

8. § 6 HITSiG-E – Zentraler IT-Dienstleister des Landes

Die Hessische Zentrale für Datenverarbeitung (HZD) ist zentraler IT-Dienstleister für Informations- und Kommunikationstechnik für alle Behörden, Gerichte und sonstigen öffentlichen Stellen des Landes Hessen. Die HZD ist für den sicheren Betrieb für den Teil der IT-Infrastruktur der Landesverwaltung verantwortlich, den sie beeinflussen kann. Ein umfassender, dauerhafter und zügiger Informationsaustausch zwischen der HZD und dem Zentrum für Informationssicherheit ist deshalb essenziell für eine effektive Cybersecurity. Laut Gesetzeswortlaut ist dieser Informationsaustausch bislang vor allem einseitiger Natur und geht primär von der HZD in Richtung Zentrum für Informationssicherheit

und CISO. Hier sollte eine gesetzliche Informationsparität dergestalt hergestellt werden, als dass auch ein Informationsaustusch in Richtung der HZD möglich ist, indem explizit Anfragen an diese gestellt werden können. Unklar ist außerdem, weshalb die an sich wünschenswerte Vorgabe „Erkenntnisse im Zusammenhang mit der Informationssicherheit unverzüglich zu teilen“ nur Eingang in die Entwurfsbegründung, nicht aber in den eigentlichen Wortlaut der Vorschrift gefunden hat.

9. § 7 HITSiG-E – Datenverarbeitung

Systematisch ist im Hinblick auf diese Vorschrift generell anzumerken, dass ihre Rolle im Gesamtgefüge der Datenverarbeitungsvorschriften nicht klar definiert ist, da daneben auch weitere Datenverarbeitungstatbestände existieren, in deren Rahmen die Verarbeitung von personenbezogenen Daten nicht ausgeschlossen werden kann und die auch nicht klar als solche gekennzeichnet sind. Fraglich ist somit, welcher Tatbestand in welchen Fällen gilt. In jedem Falle handelt es sich bei § 7 aber um eine Vorschrift zur Verarbeitung von personenbezogenen Daten, sodass sich diese Angabe auch im Titel bzw. der Gesetzesbezeichnung wiederfinden sollte.

Abs. 1 bestimmt, dass das Zentrum für Informationssicherheit personenbezogene Daten zur Erfüllung seiner im öffentlichen Interesse liegenden Aufgaben verarbeiten darf. Dies sollte dergestalt konkretisiert werden, als dass zumindest ein Verweis auf die (abschließende) Aufgabenbeschreibung nach § 5 Abs. 2 HITSiG-E gegeben ist.

Die Ergebnisse der Interessenabwägung nach Abs. 2 sind zu dokumentieren.

Abs. 3 regelt die Anonymisierung der personenbezogenen Daten für eine Datenverarbeitung nach Abschluss des Auswertungsvorgangs. Da unterschiedliche Anonymisierungstechniken zur Verfügung stehen, sollte ergänzt werden, dass die Anonymisierung nach dem „Stand der Technik“ zu erfolgen hat. Im Übrigen entbindet eine Anonymisierung nicht vollständig von der datenschutzrechtlichen Verantwortlichkeit. Deshalb sollte die Vorschrift um einen zusätzlichen Passus

Universität Bremen

IGMR
Institut für Informations-, Gesundheits- und Medizinrecht

ergänzt werden, der eine regelmäßige Überprüfung des verwendeten Anonymisierungsverfahrens und alternativ eine Datenlöschung vorschreibt. Begrifflich sollte Abs. 3 S. 2 korrigiert werden, der irreführend von „anonymisierten personenbezogenen Daten“ spricht.

Abs. 4 bestimmt, dass, soweit es die Datenauswertungen ergeben, ein Schadprogramm identifiziert wurde, dieses jederzeit beseitigt werden kann oder in seiner Funktionsweise gehindert werden kann. Dies betrifft auch Fälle des § 303a StGB. Es mutet befremdlich an, dass sich eine derartige Befugnisgrundlage in einer Datenverarbeitungs- bzw. Datenschutzvorschrift befindet. Eine vergleichbare Regelung wurde im Cybersicherheitsgesetz Baden-Württemberg im Rahmen der Gefahrenabwehr für die Cybersicherheit getroffen. Ohnehin ist im Sinne der technischen IT-Sicherheit fraglich, ob die Vorschrift in dieser Weite formuliert wirklich sinnstiftend ist, da keinerlei Hinweise auf die Art der Gefahr, ihren Umfang und ihre Herkunft gegeben werden. Außerdem unklar ist, welche technischen Eingriffe in ein IT-System mit einer solchen „Beseitigung“ verbunden sein sollen.

10. § 8 HITSiG-E – Verwendung von auf informationstechnischen Systemen gespeicherten Daten

Grundsätzlich ist es im Sinne der Informationssicherheit sinnvoll, Protokolldaten bzw. Metadaten automatisiert zu verarbeiten. Eine entsprechende Rechtsgrundlage sollte deshalb im HITSiG vorgesehen werden. Dabei berücksichtigt werden muss jedoch auch, dass derartige Metadaten einen Personenbezug enthalten bzw. enthalten können (beispielsweise durch Kumulierung der Daten oder weil es sich um im konkreten Anwendungskontext einzigartige Daten handelt). Diese Eigenschaft berücksichtigt § 8 in der gegenwärtig vorliegenden Fassung nicht ausreichend, indem z.B. technisch-organisatorische Schutzvorkehrungen und Überprüfungen vorgeschlagen werden. Zwar enthält die systematisch nachfolgende Regelung des § 14 HITSiG-E Anforderungen an die Gewährleistung von Informationssicherheit und Datenschutz, hilfreich wäre hier jedoch schon an

dieser Stelle ein Verweis auf diese flankierende Verfahrensvorschrift. In dem vorgenannten Zusammenhang ist deshalb auch das systematische Verhältnis zu § 7 HITSiG-E unklar.

Eine vergleichbare Problematik haftet der Vorschrift § 9 HITSiG-E (Erhebung und Auswertung des Datenverkehrs im Landesdatennetz) an, da die Regelungen inhaltlich ähnlich ausgestaltet sind.

11. § 10 HITSiG-E – Auswertung ohne Inhaltsdaten

§ 10 HITSiG-E stellt eine flankierende Vorschrift zur Datenauswertung zu Zwecken der Informationssicherheit (ohne Inhaltsdaten) gem. §§ 8 und 9 HITSiG-E dar, die offensichtlich wie dargestellt von einem Personenbezug der in diesem Kontext verarbeiteten Daten ausgeht. Dies sollte deshalb begrifflich nicht nur in § 10, sondern auch schon in den §§ 8 und 9 des Gesetzes deutlich werden.
Im Sinne des Datenschutzes hingegen positiv hervorzuheben ist der Fokus auf der automatisierten Auswertung der Daten, um die Intensität eines eventuellen Grundrechtseingriffs gemäß den bundesverfassungsrechtlichen Vorgaben zu reduzieren. Für eine manuelle oder personenbezogene Datenauswertung werden Einschränkungstatbestände formuliert. Fraglich ist in diesem Zusammenhang, welche weiteren Verarbeitungsvorgänge über Abs. 1 hinausgehend relevant sein sollen, wie die Formulierung „insbesondere“ nahelegt. Zwar formuliert Abs. 2 einschränkende Anforderungen für die über Abs. 1 hinausgehende Datenverarbeitung, die aber nicht ausreichend sind, da sie – eben weil es sich um personenbezogene Daten handelt – die verfassungsrechtlich geschützten Rechtspositionen des durch die Datenverarbeitung Betroffenen nicht angemessen berücksichtigen, so beispielsweise im Zuge einer kumulativen Interessenabwägung der widerstreitenden Rechtsgüter. Allein die eingeschränkte Anordnungsbefugnis der Auswertungsmaßnahmen vermag dieses datenschutzrechtliche Defizit nicht auszugleichen.

Universität Bremen

IGMR
Institut für Informations-, Gesundheits- und Medizinrecht

12. § 11 HITSiG-E – Auswertung von Inhaltsdaten

§ 11 befasst sich im Kern mit der Auswertung von Inhaltsdaten. Auch diese Vorschrift leidet jedoch an den systematischen Mängeln des Datenschutz- bzw. Maßnahmenteils des HITSiG-E. Unklarerweise wird in Abs. 1 zunächst – obwohl es laut Titel bzw. Bezeichnung um eine Auswertung von Inhaltsdaten gehen soll, wieder auf die Auswertung von Metadaten nach §§ 8 und 9 abgestellt, wobei sich inhaltliche Überschneidungen insbesondere zu § 8 ergeben. Nicht deutlich wird dabei die Abgrenzung zwischen den nach den jeweiligen Vorschriften möglichen Maßnahmen, so z.B. auch für die unverzügliche Löschpflicht, die inhaltsgleich bereits in § 8 Abs. 2 S. 2 HITSiG-E geregelt ist. Auch für Abs. 3 fehlt es an einer dokumentierten Abwägung der widerstreitenden Interessen.

Im Übrigen ergibt sich aus Abs. 1-3 nicht, worin die Unterscheidung zwischen Verkehrs- und Inhaltsdaten liegen soll, wie die Bezeichnung der Vorschrift eigentlich erwarten lassen sollte.

Unvermittelt trifft Abs. 4 eine – juristisch zwar erforderliche – Regelung zum Kernbereichsschutz, ohne dass jedoch überhaupt deutlich wird, was unter Inhaltsdaten im Sinne des Gesetzes zu verstehen sein soll und aus welcher Quelle diese stammen.

13. § 14 HITSiG-E – Gewährleistung der Informationssicherheit und des Datenschutzes

Auch eine gesetzliche Vorschrift, die die Informationssicherheit befördern will, muss den Datenschutz und die Vorgaben an die Datensicherheit beachten, soweit sie zu diesem Zweck (personenbezogene) Daten auswertet. Deshalb ist zu begrüßen, dass die gegenwärtige Entwurfsfassung eine ausdrückliche Regelung hierzu beinhaltet. Gleichwohl wäre zur Klarstellung schon ein Verweis aus den vorangehenden und bezugnehmenden Vorschriften heraus auf § 14 HITSiG sinnvoll. Wie bereits im Rahmen der Begriffsbestimmungen angemerkt, sollte für Abs. 2 Nr. 4 erwogen werden, weitere Schutzziele der IT-Sicherheit zu ergänzen, da gerade im Rahmen einer verlässlichen Datenauswertung die Authentizität

Universität Bremen

IGMR
Institut für Informations-, Gesundheits- und Medizinrecht

und Nichtabstreitbarkeit unerlässlich sind. Lobenswert ist die ausdrückliche Verankerung des Vier-Augen-Prinzips beim Datenzugriff, die Anordnung der getrennten Datenhaltung sowie die Protokollierung der entsprechenden Datenverarbeitung inklusive eines Berechtigungsmanagements. Ebenso positiv hervorzuheben ist die Erstellung eines Sicherheitskonzepts gem. § 15 HITSiG-E – in dem Zusammenhang ist anzumerken, dass wesentliche Veränderungen der IT-Systeme auch die ihrer Nutzung zugrundeliegende Software betreffen können.

14. § 16 HITSiG-E – Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen der Beeinträchtigung

Abs. 4 enthält einen redaktionellen Fehler, richtig müsste es heißen: „[…] nur mit Einwilligung der ersuchenden Stelle nach Abs. 1 übermitteln […]“.

Abs. 5 regelt die Einbeziehung Dritter in die Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme. Dabei werden jedoch keinerlei weitere Anforderungen an die Dritten selbst, deren Befähigung und das Rechtsverhältnis zueinander festgelegt.

15. § 17 HITSiG-E – Information der Betroffenen

Die datenschutzrechtlichen und systematischen Unzulänglichkeiten des vorliegenden Gesetzentwurfs setzen sich bei der Information der Betroffenen als wichtiger verfassungsrechtlicher Gewährleistung fort (gerade auch im Hinblick auf das Zitiergebot als Beleg für den Grundrechtseingriff). Weshalb eine Betroffeneninformation nur in den Fällen des § 10 Abs. 2 oder des § 11 Abs. 3 einschlägig sein soll, wird nicht weiter ausgeführt. Dies ist rechtlich problematisch, denn es können – wie bereits angeführt wurde – auch im Kontext der anderen Verarbeitungsszenarien zur IT-Sicherheit nach diesem Gesetz personenbezogene Daten anfallen, die behördlich verarbeitet werden.

Universität Bremen

IGMR
Institut für Informations-,
Gesundheits- und Medizinrecht

Bremen, den 26. April 2023

Prof. Dr. jur. Dennis-Kenji Kipker

Deutsche Universität für Verwaltungswissenschaften Speyer

Deutsche Universität für Verwaltungswissenschaften Speyer
Postfach 14 09 – D-67324 Speyer
Hessischer Landtag
Der Vorsitzende des Innenausschusses
Schlossplatz 1-3
65183 Wiesbaden

Universitätsprofessor
Dr. David Roth-Isigkeit

Lehrstuhl für Öffentliches Recht, insbesondere Recht der Digitalisierung

Freiherr-vom-Stein-Str. 2
67346 Speyer
Telefon: ++49(0)6232-654-149
E-Mail: ls-oer@uni-speyer.de

02. Mai 2023

Stellungnahme im Rahmen der öffentlichen mündlichen Anhörung
am 15. Mai 2023 des
Innenausschusses des Hessischen Landtags
zum Gesetzentwurf

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

I. Allgemeines

Die Digitalisierung des täglichen Lebens und insbesondere der Arbeitsweise in der öffentlichen Verwaltung rückt die Sicherheit im digitalen Raum aus einer bereichsspezifischen Nische in einen zentralen Fokus der Sicherheitspolitik. Diese Statusveränderung fordert insbesondere die Länder rechtlich und politisch heraus.

Die Sicherheit informationstechnischer Systeme stellt besondere Anforderungen, die sich von klassischer Sicherheitspolitik stark unterscheiden. Cyberangriffe werden punktuell und meist weit entfernt von ihrem eigentlichen Wirkungsort ausgeführt, sind dann allerdings systemseitig kaum zu vermeiden und nur unter größten Schwierigkeiten zu konkreten Verursachern zurückzuverfolgen. Ähnlich wie die Bekämpfung organisierter Kriminalität ist die Cybersicherheit ein Feld, auf dem es sowohl auf Spitzentechnologie als auch auf speziell ausgebildetes Personal ankommt.

Das Land Hessen reagiert dementsprechend auf die wachsenden Gefahren durch die zunehmende Vernetzung und versucht der Bedrohung durch die Einrichtung eigener Verwaltungsstellen sowie gefahrenabwehrrechtlicher Eingriffsgrundlagen entgegenzuwirken. Dies ist ein grundsätzlich begrüßenswertes Anliegen. Kompetenzen im Bereich der Cybersicherheit werden auf allen Ebenen benötigt.

Die immer größer werdende Bedeutung der Cybersicherheit setzt die klassische, dezentrale Sicherheitsarchitektur im Bund und in den Ländern unter Druck. Eine wachsende Anzahl von Bundesländern hat Cybersicherheitsgesetze erlassen und entsprechende Verwaltungsstellen eingerichtet. Gleichzeitig ist die Cybersicherheitspolitik ein eher atypisches Feld der Sicherheitspolitik, weshalb die nun geschaffenen und noch zu schaffenden Sicherheitsgesetze der Länder perspektivisch noch einer Harmonisierung und Überarbeitung bedürfen.

Das Land Hessen folgt damit einer allgemeinen Entwicklung unter den Ländern, wenngleich die notwendige Bündelung von Kompetenzen und die Verfügbarkeit von Spitzentechnologie strukturell eher für die Einrichtung zentraler Behörden auf Bundesebene spricht. Diese spiegelt sich konsequenterweise in einer Verschiebung von Cybersicherheitskompetenzen auf der Ebene der Europäischen Union und der intensiven Zusammenarbeit mit globalen starken Partnern wie etwa den Vereinigten Staaten und dem Vereinigten Königreich.

Welche Lücke in der Cybersicherheitsarchitektur ist angesichts der Aktivitäten auf Bundes- und EU-Ebene nun den Ländern zur eigenen Verantwortung gelassen? Richtig begründet der Entwurf, dass die spezielle Konstellation des Schutzes der *Systeme der Landesverwaltung* es erfordert, auch in den Ländern Behörden zum Schutz der IT-Infrastruktur einzurichten. Geschützt ist damit nicht die Cybersicherheit „allgemein“, wenngleich die geplante Stelle auch private Unternehmen unterstützen dürfen soll, sondern die Sicherheit in der hessischen Landesverwaltung.

Da sich die Cyberbedrohungslage in der Hessischen Landesverwaltung nicht von der Lage im Bund oder in der Privatwirtschaft unterscheidet, wird es eine zentrale Herausforderung darstellen, in der geplanten Organisation eine ähnliche Kompetenzdichte wie auf Bundesebene zu erreichen. Die Aufgabe ist es dann, die Zusammenarbeit mit den zentralen Stellen, insbesondere dem Bundesamt für Sicherheit in der Informationstechnik (BSI), richtig herzustellen.

In der folgenden Stellungnahme gehe ich nur kurz auf mE wesentliche Aspekte ein.

Zur Behördenstruktur (unten II.)

Die Schaffung ressortübergreifender und auf die Binnenstruktur der Verwaltung bezogener Kompetenzen im Innenministerium ist ein atypischer Sonderfall, der der Rechtfertigung bedarf. Diese Rechtfertigung ist mE noch nicht gut genug herausgearbeitet.

Zur „automatisierten Verarbeitung“ der anfallenden personenbezogenen Daten (unten III.)

Der Entwurf spricht nur abstrakt von der automatisierten Verarbeitung personenbezogener Daten, stellt aber nicht hinreichend klar, welchen Grad der Automatisierung diese Bestimmung meint. An welcher Stelle das Eingreifen eines Menschen erfolgt, bzw. wie es ausgelöst wird, bleibt unklar.

II. Zur Behördenstruktur

Der Gesetzentwurf sieht eine Verwaltungsstelle mit ressortübergreifenden Eingriffskompetenzen vor, die gleichzeitig im Geschäftsbereich des Innenministeriums angesiedelt ist. Dadurch werden zwei verschiedene Formen des Behördenaufbaus miteinander verschliffen. Eine solche (atypische) Kombination ist zwar grundsätzlich möglich, verlangt aber nach rechtfertigenden Gründen. Diese spezifischen Gründe, warum die Stelle beim Innenministerium angesiedelt sein soll, und nicht wie bei

ressortübergreifenden Kompetenzen üblich, jenseits einer konkreten Ministerialstruktur, sind mE noch nicht ersichtlich.

Dem Zentrum für Informationssicherheit (ZfIS), inkl. der darin folgende Einbindung der Computer Emergency Response Teams (CERT), sowie des Zentralbeauftragten für Informationssicherheit (CISO) sollen weitreichende Kompetenzen zugewiesen werden. Der Gesetzentwurf sieht ressortübergreifende Kompetenzen vor, die sich insbesondere aus § 5 Abs. 2 Nr. 2 des Gesetzentwurfes ergeben. Das geplante ZfIS soll für die gesamte Landesverwaltung „ohne Amtshilfeersuchen“ eine entsprechende Sicherheitsstruktur bereitstellen.

Insbesondere gilt dies nicht nur in Bezug auf die eigentlich unproblematische Leistung von Assistenz bei der Gewährleistung von Informationssicherheit vertraulicher Daten. Das ZfIS darf nach dem vorliegenden Entwurf eben auch von sich aus Überprüfungen der Gewährleistung der Informationssicherheit initiieren. Besonders hervorzuheben sind die Eingriffsgrundlagen nach § 4 Abs. 2 und 3 des Gesetzentwurfes.

Eine ressortübergreifende Tätigkeit verlangt in der Regel nach einem Legitimationsweg, der nicht nur über ein einzelnes Ressort führt. Für übergreifende Fragen ist in der Regel die Landesregierung zuständig, arg. ex. Art. 104 Abs. 3 der Hessischen Verfassung. § 4 Abs. 1 des Gesetzesentwurfes sieht hier aber nur die für IT- und Cybersicherheit in der Landesverwaltung zuständige Ministerin oder den hierfür zuständigen Ministers vor. Damit werden die für eine ressortübergreifende Tätigkeit notwendigen breiten Legitimations- und Kontrollstränge auf das Innenressort beschränkt.

Das Ressortprinzip gewährleistet in der Regel, dass Ministerinnen und Minister den ihnen zufallenden Geschäftsbereich in eigener Verantwortung leiten. Dazu gehört auch die Kommunikationsinfrastruktur der Ministerien. Im vorliegenden Entwurf wird dieses Ressortprinzip im Hinblick auf einen wesentlichen Teilbereich der Informationssicherheit durchbrochen und schlägt diese Kompetenzen in ihrer gesamten Breite dem Innenressort zu.

Das ist nicht unproblematisch, da über das Ressortprinzip die Gewährleistung demokratischer Legitimation und Kontrolle erfolgt. Die Hausleitung und die Sicherstellung der wesentlichen Arbeitsgrundlagen gehören strukturell jeweils umfassend in den Kompetenzbereich eines Ministers/einer Ministerin, die hierfür auch die politische Verantwortung tragen. Im vorliegenden Entwurf wird diese politische Verantwortlichkeit zum Innenministerium verschoben. Nach der hier gewählten Gestaltung müsste der Innenminister bzw. die Innenministerin die politische Verantwortung für Mängel in der Cybersicherheitsarchitektur tragen. Das kann aber gerade deshalb nicht sein, da diese nach der Grundkonstruktion der Hessischen Verfassung in den Geschäftsbereich der einzelnen Ministerien fallen und die Kompetenzen des ZfIS nur punktuell wirken.

Auch wenn der Gesetzentwurf in seiner Begründung formuliert: „Die Einrichtung einer Zentralstelle für Informationssicherheit entbindet die einzelnen Stellen der öffentlichen Verwaltung nicht von ihrer Pflicht, selbständig für eine angemessene Sicherheit bei dem Betrieb ihrer informationstechnischen Systeme zu sorgen“ scheint dies in der Praxis unrealistisch. Tatsächlich, dafür sprechen auch die umfassenden Eingriffsgrundlagen, wird diese Aufgabe der Zentralstelle überantwortet. Die in § 12 Abs. 1 und Abs. 2 des Gesetzentwurfes vorgenommene Begrenzung im Hinblick auf Fälle, in denen das Landesdatennetz betroffen ist, überzeugt nicht. Denn in der Praxis werden die Stellen (wie auch die Gesetzesbegründung zu Abs. 2 feststellt) wohl auf das Datennetz zur Erfüllung ihrer Aufgaben zurückgreifen.

Querschnittsaufgaben, d.h. solche Aufgaben die ressortübergreifend erledigt werden müssen, vertragen sich schlecht mit dem klassischen Muster des Behördenaufbaus in Deutschland.

Cybersicherheitspolitik und insbesondere die Abwehr von Gefahren für die Informationssysteme in der Landesverwaltung ist eine solche Querschnittsaufgabe. Die Komplexität der in der modernen Gesellschaft anfallenden Aufgaben tendiert dazu, die klassischen Aufbaumuster des Behördenaufbaus in Frage zu stellen. Dies ist im Hinblick auf die wichtige Funktion von Legitimation und Kontrolle, die dieser Aufbau im verfassungsrechtlichen Schema übernimmt, nicht unproblematisch. Gleiches gilt für die Systeme der Kommunen und die Garantie der kommunalen Selbstverwaltung.

Insbesondere im Hinblick auf die ressortübergreifende Tätigkeit wäre ein Modell wie in Baden-Württemberg mit der Einrichtung einer (rechtlich ungenau bezeichneten) „Cybersicherheitsagentur“ als Landesoberbehörde zu präferieren gewesen. Denn selbst, wenn dem Innenministerium die Fachaufsicht über eine unabhängige Behörde zugewiesen wird, ist dies der Struktur der ressortübergreifenden Tätigkeit näher als eine unmittelbare Integration in die Verwaltungsstruktur eines anderen Ressorts. Gerade im digitalen Bereich haben sich solche „Beauftragten“, die jenseits der Ministerialstruktur stehen, bewährt.

Abgemildert werden könnte das Problem der ressortübergreifenden Kompetenzen durch klare Vorgaben für parlamentarische Berichtspflichten und parlamentarische Kontrollen. Diese könnten, insbesondere wenn Einzelfälle betroffen sind, dem § 5 Abs. 10 BSIG oder, wenn es um allgemeine Berichtspflichten der parlamentarischen Kontrolle geht, aus § 13 BSIG entnommen werden. Eine klarere Strukturierung im Hinblick auf die durchaus beträchtlichen Eingriffskompetenzen der Behörde im Hinblick auf Legitimation und parlamentarische Kontrolle wäre wünschenswert und durch verhältnismäßig einfache Anpassungen möglich.

III. Zur „automatisierten Verarbeitung“ der anfallenden personenbezogenen Daten

Soweit das Gesetz ein abgestuftes Verfahren vorsieht, das im ersten Schritt eine automatisierte, rein technische Auswertung der anfallenden Daten vorsieht, im zweiten Schritt eine manuelle Bearbeitung erlaubt, so ist der Begriff einer automatisierten Verarbeitung genauer zu definieren.

Automatisierung kennt, wie aus der rechtlichen Diskussion insbesondere im Verwaltungsverfahrensrecht klar geworden sein sollte, verschiedene Stufen. Die vollständig automatisierte Verarbeitung sieht keinerlei Eingreifen eines/-r menschlichen Bearbeiter/-in mehr vor. Bei einer teilweise oder teilautomatisierten Bearbeitung sind an den einzelnen Schritten, insbesondere der Definition von Kriterien, noch Menschen beteiligt. Diese Unterscheidung ist jedoch nicht binär, sondern kennt viele Zwischenschritte, die etwa daran anknüpfen, an welcher Stelle im Arbeitsprozess durch einen Menschen Kriterien definiert werden können.

Im Gesetzentwurf ist der Grad der Automatisierung und insbesondere die Tiefe der Automatisierung noch unbestimmt. Das könnte letzten Endes auch verfassungsrechtlich bedenklich sein. Denn in Fragen der Automatisierung ließe sich etwa schärfen, an welchem Punkt, insbesondere an welchem Zeitpunkt, die automatisierte Verarbeitung beginnt und nach welchen Kriterien sie sich richtet. Können Kriterien für die automatisierte Verarbeitung schon mit Blick auf ein bestimmtes Verdachtsmoment erstellt werden, das dann wiederum erlauben würde, auf konkrete Fälle rückzuschließen. Eine mögliche Schärfung dieses Passus ließe sich etwa aus § 8a Absatz 1 BSI-G entnehmen, der die automatisierte Verarbeitung zumindest etwas bestimmter beschreibt.

HESSISCHER STÄDTETAG

Hessischer Städtetag · Frankfurter Straße 2 · 65189 Wiesbaden

Hessischer Landtag
Vorsitzender des Innenausschusses
Schlossplatz 1 - 3
65183 Wiesbaden

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

Anhörung zum Gesetzentwurf zum Hessischen Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG)

Ihre Nachricht vom:
03.04.2023

Ihr Zeichen:
I 2.2

Unser Zeichen:
TA 048.0 Wi/In

Durchwahl:
0611/1702-21

E-Mail:
anja.wiesmeier@hess-staedtetag.de

Datum:
08.05.2023

Stellungnahme Nr.:
049-2023

Sehr geehrter Herr Ausschussvorsitzender Heinz,
sehr geehrte Damen und Herren,

wir bedanken uns für die Möglichkeit der Stellungnahme.
Grundsätzlich ist der Gesetzentwurf positiv zu bewerten.
Vor dem Hintergrund, dass die Gesetzesbegründung, die aus unserer Sicht die durchaus folgerichtige Erläuterung enthält, „dass die Gewährleistung einer angemessenen Cybersicherheit eine gesamtstaatliche Aufgabe ist, die nur gelingen kann, wenn Bund, Länder und Kommunen eng zusammenarbeiten", greift der Gesetzentwurf aus unserer Sicht mit Blick auf die Zusammenarbeit nicht weit genug.
Die Informationssicherheit im kommunalen Bereich spielt nicht nur für selbstverwaltende Aufgaben, sondern auch bei der Übernahme staatlicher Aufgaben durch Kommunen eine

Verband der kreisfreien und kreisangehöriger Städte im Lande Hessen

Frankfurter Straße 2
65189 Wiesbaden

Telefon: 0611/1702-0
Telefax: 0611/1702-17

posteingang@hess-staedtetag.de
www.hess-staedtetag.de

bedeutende Rolle. Aus unserer Sicht sind hierbei einheitliche und verbindliche IT-Sicherheitsstandards sinnvoll, da im Rahmen staatlicher Aufgabenerfüllung – durch Kommune oder Land – nicht unterschiedliche Sicherheitsniveaus zugrunde liegen sollten.

Das Zentrum für Informationssicherheit könnte hierbei als zentrale hessenübergreifende Instanz fungieren, die hessenweite verpflichtende Sicherheitsstandards für alle im Geltungsbereich des Gesetzentwurfs genannten Akteure (§ 1 HITSiG) entwickelt, dazu regelmäßig in den Dialog tritt und generell mit Expertise zur Seite steht.
An den Grundgedanken der engeren Zusammenarbeit anknüpfend ist eine finanzielle Unterstützung der Kommunen zur dauerhaften Aufrechterhaltung von Sicherheitsstandards notwendig. Ebenso ist auch das Zentrum für Informationssicherheit insoweit mit entsprechend höheren Ressourcen auszustatten, um auch die kommunale Ebene umfänglich einzubeziehen.

Mit freundlichen Grüßen

gez.
Stephan Gieseler
Direktor

Kassel documenta Stadt
Magistrat
Personal- und Organisationsamt
Informationstechnologie

Jens Lange
jens.lange@kassel.de
it@kassel.de
Telefon 0561 787 2318
Fax 0561 787 882318
IBAN DE16 5205 0353 0000 0110 99
BIC HELADEF1KAS

Rathaus
Obere Königsstraße 8
34117 Kassel
Zimmer E1.217
Montag – Donnerstag
9 – 15 Uhr
Freitag
9 – 12.30 Uhr
und nach Vereinbarung

Behördennummer 115
Rechtshinweise
zur elektronischen
Kommunikation
im Impressum unter
www.kassel.de

34112 Kassel documenta Stadt

Hessischer Landtag
Der Vorsitzende des Innenausschusses
Herr Christian Heinz
Schlossplatz 1-3
65183 Wiesbaden

Kassel documenta Stadt

Öffentliche Anhörung im Innenausschuss des Hessischen Landtags
Stellungnahme zum Gesetzentwurf HITSiG

5. Mai 2023
1 von 7

Sehr geehrter Herr Heinz,
sehr geehrte Mitglieder des Innenausschusses des Hessischen Landtags,

ich möchte mich zunächst herzlich für Ihre Anfrage bedanken, eine Stellungnahme zum Gesetzentwurf „Hessisches Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz - HITSiG) - Drucks. 20/10752 –“ abzugeben. Es ist mir eine große Ehre, dass Sie meinem Fachwissen und meiner Meinung in dieser Angelegenheit vertrauen. Ich schätze Ihre Bereitschaft, verschiedene Perspektiven bei der Erstellung und Verabschiedung wichtiger Gesetze zu berücksichtigen.

Nach eingehender Prüfung des vorliegenden Gesetzentwurfs möchte ich nachfolgend meine Stellungnahme abgeben. Zusammenfassend begrüße ich die Bemühungen der Landesregierung des Landes Hessen, die rechtlichen Grundlagen zur Steigerung der Sicherheit in der Informationstechnik in Hessen anzugehen. Ich hoffe, dass meine Stellungnahme dazu beiträgt, die Diskussion zu bereichern und die Entscheidungsfindung zu unterstützen. Ich stehe gerne für weitere Fragen oder Diskussionen zur Verfügung, um den Gesetzentwurf bestmöglich zu optimieren. Bitte zögern Sie nicht, mich zu kontaktieren, wenn Sie weitere Informationen oder Klarstellungen benötigen. Ich bin jederzeit bereit, meine Expertise und Kenntnisse mit Ihnen zu teilen, um den Gesetzgebungsprozess bestmöglich zu unterstützen. Ich wünsche Ihnen viel Erfolg bei der weiteren Bearbeitung und Verabschiedung des Gesetzentwurfs.

Freundliche Grüße
Im Auftrag

Jens Lange
Informationssicherheitsbeauftragter

Stellungnahme zum Gesetzentwurf HITSiG

Anlass

Der Innenausschuss des Hessischen Landtags hat mich durch ein Schreiben vom 3. April 2023 darüber informiert, dass ich sowohl schriftlich als auch mündlich zu dem Gesetzentwurf „Hessisches Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG) – Drucks. 20/10752 –“ der Landesregierung angehört werde. Aus diesem Anlass habe ich die nachfolgende schriftliche Stellungnahme verfasst.

Vorbemerkung

In meiner Funktion als Informationssicherheitsbeauftragter der Stadtverwaltung Kassel und als Mitglied diverser Arbeitsgruppen der kommunalen Spitzenverbände (z. B. AG kommunale Basis-Absicherung, AG BCM Länder/Kommunen, AG Handreichung Informationssicherheitsleitlinie), werde ich meine Betrachtung des Gesetzentwurfs auf die kommunalen Aspekte aus dieser Sichtweise fokussieren.

Zusammenfassung der wichtigsten Punkte

Die Schaffung einer rechtlichen Grundlage zur Steigerung der Informationssicherheit in Hessen ist begrüßenswert und notwendig. Die Einrichtung einer Zentralstelle und einer oder eines Beauftragten für Informationssicherheit mit Regelungen zu den Aufgaben und Befugnissen ist sinnvoll und angemessen. Nach sorgfältiger Prüfung des Gesetzentwurfs möchte ich im Folgenden die zentralen Punkte aufzeigen, die meiner Meinung nach im Gesetzentwurf fehlen oder nicht ausreichend berücksichtigt wurden:

1. Pflicht für das Land Hessen, ein System zur Meldung von IT-Sicherheitsvorfällen für Kommunen bereitzustellen.
2. Meldepflicht für Kommunen von IT-Sicherheitsvorfällen über das vom Land Hessen bereitgestellte System.
3. Pflicht für das Land Hessen, die Kommunen über die Erkenntnisse zu informieren, die aus Sammlung und Auswertung von Informationen über Risiken, Beeinträchtigungen, Störungen und Vorkehrungen zur Abwehr von Gefahren für die Informationssicherheit gewonnen werden.
4. Pflicht für das Land Hessen, zur Unterstützung der Kommunen bei der Erkennung, Untersuchung und Abwehr von Gefahren für die Informationssicherheit auf deren Ersuchen.
5. Pflicht für Kommunen zur Erstellung einer „Leitlinie zur Informationssicherheit“, in der der Stellenwert, die verbindlichen Prinzipien und das anzustrebende Niveau der Informationssicherheit dokumentiert werden.
6. Pflicht für Kommunen eine/n zentralen Ansprechpartner/in (Informationssicherheitsbeauftragte/n) zu benennen.

Die vorgeschlagenen Pflichten für das Land Hessen und die Kommunen tragen gemeinsam dazu bei, die Informationssicherheit zu verbessern. Während das Land durch die Maßnahmen eine gestärkte Zusammenarbeit zwischen den verschiedenen Verwaltungsebenen erreicht, ermöglichen die Pflichten für die Kommunen einen systematischen und strukturierten Ansatz zur Gewährleistung eines angemessenen Schutzniveaus für ihre IT-Systeme und -Dienste.

Begründung und Aspekte im Einzelnen

Meldung von IT-Sicherheitsvorfällen
(Punkt 1 und 2 der Zusammenfassung)

Die Pflicht für das Land Hessen, ein System zur Meldung von IT-Sicherheitsvorfällen für Kommunen bereitzustellen (Punkt 1) und die Meldepflicht für Kommunen (Punkt 2) sind zusammenhängend zu betrachten. Deutschlandweit sind 2023 bereits 12 IT-Sicherheitsvorfälle von Kommunalverwaltungen öffentlich bekannt geworden (davon drei in Hessen)[1]. Im Jahr 2022 waren es 18 und im Jahr 2021 sogar 32 Vorfälle. Ein tatsächliches kommunales Lagebild zur Informationssicherheit ist jedoch nicht bekannt. Das Land Hessen sollte aus diesem und den folgenden Gründen ein System zur Meldung von IT-Sicherheitsvorfällen für Kommunen bereitstellen und die Kommunen dazu verpflichten, IT-Sicherheitsvorfälle über dieses System an das Land zu melden:

1. Zentralisierte Erfassung: Durch ein zentrales Meldesystem können IT-Sicherheitsvorfälle effizienter erfasst und analysiert werden. Dies ermöglicht einen besseren Überblick über die Häufigkeit, Art und Schwere der Vorfälle in der gesamten Region.
2. Schnellere Reaktionszeiten: Durch das zentrale Meldesystem kann das Land Hessen rascher auf Sicherheitsvorfälle reagieren und angemessene Maßnahmen ergreifen. Dies kann dazu beitragen, Schäden zu minimieren und die Auswirkungen auf betroffene Kommunen zu reduzieren.
3. Erfahrungsaustausch und Best Practices: Ein zentrales Meldesystem ermöglicht es, Informationen und Erfahrungen zwischen den Kommunen und dem Land Hessen auszutauschen. Dadurch können Best Practices und Lösungsansätze gemeinsam entwickelt und angewendet werden, um die IT-Sicherheit in der gesamten Region zu stärken.
4. Ressourceneffizienz: Ein gemeinsames Meldesystem reduziert den Verwaltungsaufwand und die Kosten für die Kommunen, da sie keine eigenen Systeme entwickeln und betreiben müssen. Gleichzeitig profitieren sie von der Expertise des Landes Hessen in Bezug auf IT-Sicherheit.
5. Gesetzliche Vorgaben und Compliance: Durch die Verpflichtung zur Meldung von IT-Sicherheitsvorfällen können gesetzliche Vorgaben eingehalten und die Compliance in Bezug auf IT-Sicherheit gewährleistet werden. Dies ist insbesondere wichtig, um den Schutz sensibler Daten und die Funktionsfähigkeit kritischer Infrastrukturen sicherzustellen.

Informationspflicht des Landes Hessen
(Punkt 3 der Zusammenfassung)

Das Land Hessen sollte aus folgenden Überlegungen die Pflicht haben, die Kommunen über die Erkenntnisse zu informieren, die aus der Sammlung und Auswertung von Informationen über Risiken, Beeinträchtigungen, Störungen und Vorkehrungen zur Abwehr von Gefahren für die Informationssicherheit gewonnen werden:

[1] Siehe https://kommunaler-notbetrieb.de

1. Proaktive Risikominimierung: Durch das Teilen von Erkenntnissen können die Kommunen proaktiv Maßnahmen ergreifen, um Risiken zu minimieren und ihre IT-Sicherheit zu verbessern, bevor potenzielle Sicherheitsvorfälle eintreten.
2. Effektive Ressourcennutzung: Die Weitergabe von Informationen ermöglicht es den Kommunen, ihre Ressourcen effektiver einzusetzen, indem sie auf bereits gewonnene Erkenntnisse und Erfahrungen zurückgreifen können, anstatt diese selbst erarbeiten zu müssen.
3. Gemeinsame Strategieentwicklung: Die Kommunikation zwischen dem Bundesland und den Kommunen fördert die Entwicklung gemeinsamer Strategien und Vorgehensweisen zur Verbesserung der Informationssicherheit. Dies stärkt die Zusammenarbeit und führt zu einem kohärenten Ansatz in der gesamten Region.
4. Sensibilisierung und Schulung: Die Weitergabe von Erkenntnissen trägt dazu bei, das Bewusstsein für Informationssicherheit in den Kommunen zu erhöhen und deren Mitarbeiter entsprechend zu schulen. Dies ist eine wichtige Voraussetzung für die Umsetzung wirksamer Sicherheitsmaßnahmen.
5. Transparenz und Vertrauen: Die Offenlegung von Erkenntnissen über Risiken und Vorkehrungen zur Abwehr von Gefahren für die Informationssicherheit schafft Transparenz und fördert das Vertrauen zwischen dem Bundesland und den Kommunen. Dies ist für eine erfolgreiche Zusammenarbeit und den Schutz kritischer Infrastrukturen von zentraler Bedeutung.

Unterstützung der Kommunen bei Gefahren für die Informationssicherheit
(Punkt 4 der Zusammenfassung)

Das Land Hessen sollte unter Berücksichtigung der nachfolgenden Faktoren die Pflicht haben, die Kommunen bei der Erkennung, Untersuchung und Abwehr von Gefahren für die Informationssicherheit auf deren Ersuchen zu unterstützen:

1. Expertise und Ressourcen: Ein Bundesland verfügt in der Regel über umfangreichere Expertise und Ressourcen im Bereich der Informationssicherheit als die einzelnen Kommunen. Durch die Unterstützung des Bundeslandes können die Kommunen von diesem Wissen und den verfügbaren Ressourcen profitieren, um ihre Sicherheit effektiv zu erhöhen.
2. Konsistente Sicherheitsstandards: Die Unterstützung durch das Bundesland trägt dazu bei, dass einheitliche und hohe Sicherheitsstandards in der gesamten Region etabliert und eingehalten werden. Dies ist insbesondere wichtig, um kritische Infrastrukturen und sensible Daten zu schützen.
3. Effiziente Reaktion auf Sicherheitsvorfälle: Im Falle eines IT-Sicherheitsvorfalls kann die Hilfe des Bundeslandes dazu beitragen, dass die Kommunen schneller und effektiver auf den Vorfall reagieren können. Dies kann dazu führen, dass Schäden minimiert und die Auswirkungen auf betroffene Systeme und Daten reduziert werden.
4. Kostenersparnis: Die Unterstützung durch das Bundesland kann den Kommunen helfen, Kosten zu sparen, indem sie auf die Expertise und Ressourcen des Bundeslandes zurückgreifen, anstatt eigene Fachkräfte einzustellen oder externe Dienstleister zu beauftragen.

5. Stärkung der Zusammenarbeit: Die Unterstützung des Bundeslandes bei der Erkennung, Untersuchung und Abwehr von Gefahren für die Informationssicherheit fördert die Zusammenarbeit zwischen den verschiedenen Verwaltungsebenen und stärkt das Vertrauen zwischen den Kommunen und dem Bundesland. 5 von 7

Pflicht für Kommunen zur Erstellung einer „Leitlinie zur Informationssicherheit“
(Punkt 5 der Zusammenfassung)

Die Kommunen des Landes Hessen sollten aufgrund der nachstehenden Aspekte die Pflicht zur Erstellung einer „Leitlinie zur Informationssicherheit“ haben, in der der Stellenwert, die verbindlichen Prinzipien und das anzustrebende Niveau der Informationssicherheit dokumentiert werden:

1. Strategische Orientierung: Die Leitlinie zur Informationssicherheit gibt den Kommunen eine klare und strukturierte Vorgabe für die Ausrichtung ihrer IT-Sicherheitsstrategie. Sie dient als Grundlage für die Planung, Umsetzung und Überwachung von Sicherheitsmaßnahmen.
2. Verbindlichkeit: Die Dokumentation der verbindlichen Prinzipien und des anzustrebenden Sicherheitsniveaus schafft Verbindlichkeit und Verantwortlichkeit innerhalb der Kommunalverwaltung. Dadurch wird sichergestellt, dass alle Beteiligten sich an den Vorgaben orientieren und ihren Aufgaben im Bereich der Informationssicherheit nachkommen.
3. Kontinuität und Nachvollziehbarkeit: Eine Leitlinie zur Informationssicherheit trägt zur Kontinuität und Nachvollziehbarkeit der Sicherheitsmaßnahmen bei. Sie ermöglicht es, den Fortschritt der Sicherheitsinitiativen zu verfolgen und gegebenenfalls Anpassungen vorzunehmen, um das angestrebte Sicherheitsniveau zu erreichen oder zu erhalten.
4. Sensibilisierung und Schulung: Die Leitlinie zur Informationssicherheit unterstützt die Sensibilisierung und Schulung der Mitarbeiterinnen und Mitarbeiter in den Kommunen. Sie informiert über die Relevanz der Informationssicherheit, die geltenden Prinzipien und das angestrebte Schutzniveau, sodass alle Beteiligten ein gemeinsames Verständnis entwickeln können.
5. Rechtliche und regulatorische Anforderungen: Die Erstellung einer Leitlinie zur Informationssicherheit hilft den Kommunen, gesetzliche und regulatorische Anforderungen im Bereich der IT-Sicherheit zu erfüllen. Sie dient als Nachweis für die Einhaltung von Vorschriften und kann im Falle von Sicherheitsvorfällen oder Audits als Referenz herangezogen werden.

In einer solchen Pflicht für die Kommunen zur Erstellung einer „Leitlinie zur Informationssicherheit“ sollten in Anbetracht der nachfolgenden Punkte zunächst keine Mindeststandards gefordert werden:

1. Flexibilität und Anpassungsfähigkeit: Indem keine Mindeststandards vorgeschrieben werden, erhalten die Kommunen die Flexibilität, ihre Leitlinien an ihre spezifischen Bedürfnisse und Ressourcen anzupassen. Dies ermöglicht es ihnen, die Informationssicherheit auf eine Weise zu gestalten, die ihren individuellen Gegebenheiten und Herausforderungen gerecht wird.

2. Autonomie der Kommunen: Die Kommunen verfügen über eigene Zuständigkeiten und Verantwortungsbereiche. Indem keine Mindeststandards auf Landesebene vorgegeben werden, wird die Autonomie der Kommunen gewahrt und ihre Entscheidungsfreiheit bei der Ausgestaltung ihrer Informationssicherheitsstrategie respektiert.
3. Anreiz zur Selbstverantwortung: Ohne vorgegebene Mindeststandards werden die Kommunen dazu angehalten, selbst aktiv zu werden und eigene Vorgehensweisen für ihre Informationssicherheit zu entwickeln. Dies fördert die Selbstverantwortung der Kommunen und motiviert sie, ihre IT-Sicherheit kontinuierlich zu verbessern.
4. Berücksichtigung von Best Practices und Branchenstandards: Die Kommunen haben die Möglichkeit, ihre Leitlinien zur Informationssicherheit an bestehenden Best Practices und Standards (z. B. IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung) auszurichten, ohne dass ihnen von Landesebene spezifische Vorgaben gemacht werden. Dies ermöglicht eine flexible und effektive Anwendung von bewährten Sicherheitsmaßnahmen.

Pflicht für Kommunen zur Benennung einer/s Ansprechpartner/in
(Punkt 6 der Zusammenfassung)

Die Kommunen des Landes Hessen sollten basierend auf den folgenden Überlegungen die Pflicht zur Benennung einer/s zentralen Ansprechpartner/in (Informationssicherheitsbeauftragte/n) haben:

1. Klare Zuständigkeiten: Die Benennung eines zentralen Ansprechpartners schafft klare Zuständigkeiten und Verantwortlichkeiten in Bezug auf Informationssicherheit. Dies erleichtert die Steuerung und Koordination von Sicherheitsmaßnahmen und gewährleistet, dass Entscheidungen und Aktivitäten im Bereich der IT-Sicherheit effizient umgesetzt werden.
2. Kompetenzbündelung: Die Benennung eines Informationssicherheitsbeauftragten fördert die Bündelung von Kompetenzen und Expertise in der Kommunalverwaltung. Der/die Informationssicherheitsbeauftragte ist die zentrale Anlaufstelle für Fragen rund um die Informationssicherheit und kann so gezielte und fachkundige Beratung und Unterstützung für die verschiedenen Abteilungen und Mitarbeiter/innen anbieten.
3. Kommunikation und Zusammenarbeit: Ein/e zentrale/r Ansprechpartner/in dient als Schnittstelle zwischen den verschiedenen Verwaltungseinheiten, dem Bundesland und ggf. externen Partnern. Dadurch wird die Kommunikation und Zusammenarbeit in Fragen der Informationssicherheit verbessert, und es entsteht ein gemeinsames Verständnis für die Bedeutung und Umsetzung von Sicherheitsmaßnahmen.
4. Kontinuierliche Verbesserung: Der/die Informationssicherheitsbeauftragte überwacht und bewertet regelmäßig die Wirksamkeit der eingesetzten Sicherheitsmaßnahmen und identifiziert Verbesserungspotenziale. Dies gewährleistet eine kontinuierliche Anpassung und Optimierung der Informationssicherheit in der Kommunalverwaltung.

5. Schulung und Sensibilisierung: Der/die Informationssicherheitsbeauftragte kann verantwortlich für die Schulung und Sensibilisierung der Mitarbeiter/innen hinsichtlich der Informationssicherheit sein. Dies trägt dazu bei, das Sicherheitsbewusstsein zu erhöhen und die Einhaltung von Sicherheitsrichtlinien und -verfahren in der gesamten Organisation zu fördern. 7 von 7

Schriftliche Stellungnahme

Pierre Gronau

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

daal
information security & compliance

Contents

Inhalt

Chapter 1

Einführung

Um den vorliegenden Gesetzentwurf angemessen zu interpretieren und zu bewerten, müssen wir die legislativen und politischen Absichten berücksichtigen. Einerseits hat das BSI in seinem Bericht zur Lage der IT-Sicherheit in Deutschland 2022 festgestellt, dass die Bedrohungslage so hoch wie nie zuvor ist. Andererseits nimmt die Nutzung und Vernetzung von IT rapide zu. Während also die Nachfrage nach digitler Transformation steigt, steigen auch die technischen Risiken exponentiell an. Insbesondere die öffentliche Verwaltung steht unter starkem Druck, sich zu digital zu transformieren, um die Erwartungen der Bürgerinnen und Bürger an eine moderne und kundenorientierte behördliche Infrastruktur zu erfüllen. Gleichzeitig erwarten die Menschen, dass ihre sensiblen Daten vor unbefugter Offenlegung und Manipulation geschützt sind (Authentizität, Integrität und Vertraulichkeit). Im Kontext dieser Herausforderungen bewegt sich auch der vorliegende Gesetzentwurf, da es letztendlich keine Garantie für Cybersicherheit gibt. Es ist daher umso wichtiger, präventive Strukturen aufzubauen.

Das Hessen CyberCompetenceCenter (Hessen3C), das dem Hessischen Ministerium des Innern und für Sport untersteht, fungiert als zentraler Ansprechpartner für das Thema Cybersicherheit in Hessen und erfüllt die Aufgabe, präventive Strukturen im Bereich Cybersicherheit aufzubauen. Seit seiner Gründung im April 2019 in der Abteilung Cyber- und IT-Sicherheit sowie digitler Verwaltungstransformtion bietet Hessen3C beratende Unterstützung für die hessische Landesverwaltung, hessische Kommunen und hessische Unternehmen an. Das Aufgabenspektrum von Hessen3C ist breit gefasst und beinhaltet nicht nur den Schutz der Landesverwaltung vor Cyberbedrohungen, sondern auch die Unterstützung von Sicherheitsbehörden bei der Ausbildung von Fachkräften, die Bekämpfung von Cybercrime und Cyberspionage sowie die Beratung von Kommunen, Wirtschaft und KRITIS. Hessen3C ist auch die zentrale Kontaktstelle für die Entgegennahme landesbezogener KRITIS-Meldungen. Zusammen mit der Landespolizei und dem Landesamt für Verfassungsschutz arbeitet Hessen3C eng zusammen. Hessen3C erbringt konkret folgende Leistungen:

- **Landesverwaltung**: Unterstützung und Koordinierung der Bearbeitung von Cybersicherheitsvorfällen in der Landesverwaltung und ist die zentrale Ansprechstelle bei IT-Sicherheitsvorfällen.
- **Kommunen**: Kostenfreie Nutzung der Leistungen für hessische Kommunen auf freiwilliger Basis unter Wahrung des Selbstverwaltungsprinzips.
- **KRITIS und NIS-2**: Bei Bedarf kostenlose, ergebnisoffene und produktneutrale Inanspruchnahme durch KRITIS und NIS-2.
- **KMU**: Bei Bedarf kostenlose, ergebnisoffene und produktneutrale Inanspruchnahme durch KMU.

Durch den Entwurf eines HITSiG werden die umfangreichen Befugnisse des Hessen3C an eine Rechtsgrundlage geknüpft. Dies ist notwendig, da bislang keine umfassende Rechtsgrundlage für Befugnisse und Datenzugriffe in Hessen vorhanden war, obwohl einige Befugnisse Grundrechtsrelevanz besitzen. Eine gesetzliche Regelung ist notwendig, um Rechtssicherheit und Betroffenenschutz zu gewährleisten. Die staatliche Gewährleistung der Cybersicherheit erfordert einen Interessenausgleich zwischen grundrechtlich geschützten Positionen, was sachgerecht und juristisch notwendig ist. Ohne eine entsprechende gesetzliche Grundlage wäre ein behördliches Tätigwerden folglich nicht möglich bzw. rechtswidrig. Die zu treffende Regulierung betrifft insbesondere das Zentrum für Informationssicherheit, Eingriffs- und Abwehrmaßnahmen sowie den zentralen Beauftragten für Informationssicherheit (CISO), der gemäß IT-SiG 2.0 und NIS-2 üblicherweise Informationssicherheitsbeauftragter bezeichnet wird. Der Entwurf sieht u.a.

- die Möglichkeit zum eigenständigen operativen Tätigwerden des Hessen3C in den Bereichen Prävention, Informationssammlung und -auswertung, Erarbeitung von Warnungen und Empfehlungen für Behörden

und Öffentlichkeit, aktive Abwehr von Cybergefahren, Dienstleistungen/Auftragsverarbeitung für Kommunen, Einbindung des CERT vor.

- Auch **Eingriffs- und Abwehrmaßnahmen** wie die Befugnis zur Datenanalyse zu Zwecken der Abwehr von Gefahren für die Cybersicherheit sowie die Untersuchung von im Landesdatennetz und IT-Systemen gespeicherten Daten mit Grundrechtsrelevanz werden geregelt.
- Zusätzlich wird die **Position des CISO** gesetzlich verankert, einschließlich seiner Eingriffsbefugnisse zur Abwehr von Cybergefahren, Berichtspflichten und Koordinierung des IT-Krisenmanagements.

Chapter 2

Zu den Vorschriften im Einzelnen

Angesichts der am 27. Dezember 2022 verabschiedeten **NIS-2 EU-Richtlinie** (EU 2022/2555), die ihre Kraft am 16. Januar 2023 entfaltet, plant der Bund konsequenterweise ein **NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz** (NIS2UmsuCG).

2.1 § 2 Nr. 1 HITSiG-E – Begriffsbestimmungen

Gemäß der Entwurfsbegründung stützen sich die verwendeten Begriffsbestimmungen im Entwurf des HITSiG auf das BSIG. Allerdings bleibt unklar, warum im Entwurf des **HITSiG** leicht von den entsprechenden BSI-Bestimmungen oder die durch NIS-2 Richtlinie (wurde am 27.12.2022 im Amtsblatt L333 der Europäischen Union veröffentlicht) abgewichen wird. Dies ist problematisch für ein einheitliches und systematisches Begriffsverständnis im deutschen IT-Sicherheitsrecht, insbesondere wenn hierfür kein sachlich nachvollziehbarer Grund besteht. Darüber hinaus sollte berücksichtigt werden, dass die Übermittlung oder Übertragung von Informationen eine Form der Datenverarbeitung darstellt. Daher wäre es angemessener, die Bestimmung wie folgt zu formulieren: “Die Informationstechnik im Sinne dieses Gesetzes umfasst alle technischen Mittel zur Verarbeitung von Informationen”.

2.2 § 2 Nr. 2 HITSiG-E – Begriffsbestimmungen

Im BSIG fehlt eine Definition des Begriffs “Informationssicherheit”. Daher besteht derzeit keine klare begriffliche Abgrenzung im vorgeschlagenen hessischen Regelungsentwurf, da die Begriffe “IT-Sicherheit”, “Cybersicherheit” und “Informationssicherheit” unterschiedliche Bedeutungen haben. Da der Regelungsentwurf sich jedoch auf die Sicherheit vernetzter IT-Systeme bezieht, wäre zumindest der Begriff “IT-Sicherheit” angemessener. Um eine umfassendere Definition zu schaffen, sollten die Schutzziele der IT-Sicherheit ergänzt werden, insbesondere um Authentizität und Nichtabstreitbarkeit. Es ist fraglich, wie externe Dienste und Herausforderungen in der digitalen Lieferkette in die enge Definition einbezogen werden sollen, die sich nur auf das IT-System und dessen Anwendung beschränkt.

Auch hier wären die Formulierungen aus NIS-2 bzw. NIS2UmsuCG hilfreich.

2.3 § 2 Nr. 3 HITSiG-E – Begriffsbestimmungen

Es könnte in Betracht gezogen werden, die Definition der Schadprogramme im Hinblick auf das BSIG zu erweitern, indem der Begriff “Verarbeitung” hinzugefügt wird, sofern er nicht bereits unter die unbefugte “Nutzung” und “Löschung” von Daten fällt.

Hier der Formulierungsvorschlag: “„Schadprogramme“ Programme und sonstige informationstechnische Routinen und Verfahren, die dem Zweck dienen, unbefugt Daten zu nutzen oder zu löschen oder die dem Zweck dienen, unbefugt auf sonstige informationstechnische Abläufe einzuwirken”

2.4 § 2 Nr. 4 HITSiG-E – Begriffsbestimmungen

Der Begriff der “Sicherheitslücke” ist aufgrund politischer Entwicklungen, insbesondere des Russland-Ukraine-Konflikts im Jahr 2022, hoch umstritten und wird von einigen Autoren als “verbrannt” bezeichnet. Dies liegt hauptsächlich an einer bisher nicht korrigierten Auslegung der Warnbestimmung durch das BSI. Um eine klare Unterscheidung zwischen politischen Wertungen und technisch-organisatorischen Bewertungen zu schaffen, wäre es wünschenswert, die Definition der “Sicherheitslücke” entsprechend zu ergänzen oder zu ändern. Andernfalls besteht weiterhin erhebliche Unsicherheit bei der Anwendung dieses Begriffs in der Praxis, wie es derzeit leider im BSIG der Fall ist.

Hier der Formulierungsvorschlag: „Schwachstelle“ eine Schwäche, Anfälligkeit oder Fehlfunktion von IKT-Produkten oder IKT-Diensten, die bei einer Cyberbedrohung ausgenutzt werden kann (Umsetzung Art. 6 Ziff. 15 NIS2. Der Begriff der „Sicherheitslücke“)

2.5 § 3 HITSiG-E – Grundsätze der Informationssicherheit

Im Absatz wird festgestellt, dass Absatz 1 für die Stellen nach § 1 Nr. 1 und Nr. 2 vorsieht, angemessene organisatorische und technische Vorkehrungen sowie “sonstige Maßnahmen” zur Gewährleistung der Informationssicherheit zu treffen. Es bleibt unklar, was unter diesen “sonstigen Maßnahmen” zu verstehen ist und inwiefern sie über die vorgeschlagenen technischen und organisatorischen Maßnahmen hinausgehen sollen. Daher wird angeregt, diese Ergänzung zu streichen.

Es wird angeregt, die Formulierung “Für technische Maßnahmen soll mindestens der Stand der Technik maßgeblich sein” nicht einzuschränken, da dies nicht nur den technischen, sondern auch den organisatorischen Maßnahmen gerecht werden sollte. Der nachfolgende Verweis auf die IT-Grundschutzmethodikerfordert die Umsetzung eines ISMS, das nicht nur aus technischen, sondern auch aus organisatorischen Maßnahmen besteht. Es ist daher sinnvoll, dass auch organisatorische Maßnahmen mindestens gemäß dem Stand der Technik bewertet werden, wenn sie im Kontext der IT-Sicherheit eingesetzt werden.

Es wird vorgeschrieben, dass für jeden Geschäftsbereich ein Informationssicherheitsbeauftragter (ISB) benannt werden muss, der für die Gewährleistung der Informationssicherheit verantwortlich ist (Abs. 3). Es wird empfohlen, dass der ISB über die erforderliche Qualifikation verfügen sollte, um seine Aufgaben und Anforderungen angemessen zu erfüllen.

Absatz 4 legt fest, dass die ISBs bei wesentlichen Änderungen von IT-Systemen beteiligt werden müssen. Es wäre sinnvoll, diese “wesentlichen Änderungen” genauer zu definieren, beispielsweise unter Berücksichtigung ihrer Auswirkungen auf Funktionen, Hardware und Software sowie potenzieller Cybersicherheitsrisiken. Es ist unklar, welche Konsequenzen die Beteiligung des ISBs haben wird. Um die Informationssicherheit zu gewährleisten, sollte darüber nachgedacht werden, dem ISB beispielsweise ein “Vetorecht” zu geben, falls bestimmte Änderungen der IT-Infrastruktur erhebliche Sicherheitsbedenken aufwerfen.

Eine geringfügige Verstärkung der Formulierung in Absatz 5 sollte in Erwägung gezogen werden, um die kommunale Selbstverwaltungsautonomie nicht übermäßig einzuschränken. Statt “empfohlen” könnte die Formulierung “nahegelegt” verwendet werden.

Auch finanzielle Argumente dürfen kein Maßstab für eine Risikoübernahme darstellen, da kritische Infrastrukturen unabweisbare Anforderungen besitzen.

2.6 § 4 HITSiG-E – Die oder der Zentrale Informationssicherheitsbeauftragte der Landesverwaltung

Der Zentrale Informationssicherheitsbeauftragte der Landesregierung hat die Verantwortung, die ressortübergreifende Informationssicherheit sicherzustellen und vertritt die hessische Landesverwaltung in Angelegenheiten der Informationssicherheit nach außen. Die Aufgabenbeschreibung in Absatz 2 sollte erweitert werden, um den präventiven Aspekt der Informationssicherheit, die Förderung der Cybersecurity Awareness und den Informationsaustausch als zentrale Funktionen stärker zu betonen. Es wäre auch sinnvoll, die Unterscheidung zu anderen IT-bezogenen Positionen in der Landesverwaltung kurz zu skizzieren und begrifflich zu erläutern. In Bezug auf die Befugnisse des CISO gemäß Absatz 3 wäre es vernünftig, ihm die Anordnungsbefugnis für IT-Sicherheitsmaßnahmen bei Gefahr im Verzug zu geben. Zusätzlich könnte eine Begründungspflicht für die Dienststellen in Erwägung gezogen werden, wenn sie den Empfehlungen des CISO nicht folgen oder eigene Maßnahmen zur Cybersicherheit ergreifen.

2.7 § 5 HITSiG-E – Zentrum für Informationssicherheit

Der für IT- und Cybersicherheit in der Landesverwaltung zuständige Minister hat die Aufgabe, das Zentrum für Informationssicherheit zu errichten. Die vielfältigen Aufgaben des Zentrums betreffen hauptsächlich die aktive Koordination und die Sammlung sowie Auswertung cybersicherheitsrelevanter Informationen. Es sollte jedoch deutlicher herausgestellt werden, dass das Zentrum für Informationssicherheit in erster Linie eine präventive Rolle für den Aufbau effektiver Informationssicherheitsinfrastrukturen einnimmt und somit Fragen des Informationssicherheitsmanagements im Entwurf nicht ausreichend adressiert werden. Zudem fehlen Vorgaben zur Zusammenarbeit mit privaten Stellen, insbesondere im Rahmen von Public-Private-Partnerships, um die Effektivität von getroffenen und noch zu treffenden Maßnahmen gemäß HITSiG zu verbessern. Die multidimensionale Bedrohungslage sollte stärker berücksichtigt werden, da Bedrohungen für den privaten Sektor auch für den öffentlichen Sektor relevant sein können und eine Zusammenarbeit sinnvoll erscheint. Hierbei sollte insbesondere berücksichtigt werden, dass das CERT Teil des Zentrums für Informationssicherheit ist und somit die Funktion als zentrale Kontaktstelle nach dem BSIG wahrnimmt und seine Leistungen auch gegenüber privaten Unternehmen erbringen kann.

2.8 § 6 HITSiG-E – Zentraler IT-Dienstleister des Landes

Die Hessische Zentrale für Datenverarbeitung (HZD) ist der zentrale IT-Dienstleister für alle Behörden, Gerichte und öffentlichen Stellen des Landes Hessen in Bezug auf Informations- und Kommunikationstechnik. Die HZD ist für einen sicheren Betrieb des Teils der IT-Infrastruktur der Landesverwaltung verantwortlich, den sie beeinflussen kann. Ein effizienter, effektiver und kontinuierlicher Informationsaustausch zwischen der HZD und dem Zentrum für Informationssicherheit ist unerlässlich für eine erfolgreiche Cybersecurity. Gemäß dem Gesetzeswortlaut ist der Informationsaustausch derzeit hauptsächlich einseitig und geht vorrangig von der HZD in Richtung des Zentrums für Informationssicherheit und ISB. Es sollte jedoch eine gesetzliche Parität hergestellt werden, die es ermöglicht, auch Anfragen an die HZD zu stellen und somit den Informationsaustausch in beide Richtungen zu ermöglichen. Es ist unklar, warum die wünschenswerte Vorgabe, “Erkenntnisse im Zusammenhang mit der Informationssicherheit unverzüglich zu teilen”, nur in der Entwurfsbegründung und nicht im eigentlichen Wortlaut der Vorschrift enthalten ist.

2.9 § 7 HITSiG-E – Datenverarbeitung

Es lässt sich allgemein feststellen, dass die Rolle der Vorschrift in Bezug auf die Gesamtheit der Datenschutzvorschriften nicht klar definiert ist, da es auch andere Datenverarbeitungstatbestände gibt, in denen die Verarbeitung personenbezogener Daten nicht ausgeschlossen ist und die nicht eindeutig als solche gekennzeichnet sind. Es bleibt unklar, welche Vorschrift in welchen Fällen gilt. In jedem Fall handelt es sich jedoch bei § 7 um eine Vorschrift zur Verarbeitung personenbezogener Daten, die auch im Titel oder der Gesetzesbezeichnung deutlich werden sollte.

Gemäß Absatz 1 darf das Zentrum für Informationssicherheit personenbezogene Daten zur Erfüllung seiner im öffentlichen Interesse liegenden Aufgaben verarbeiten. Es wäre jedoch wünschenswert, dass zumindest ein Verweis auf die (abschließende) Aufgabenbeschreibung nach § 5 Absatz 2 HITSiG-E gegeben wird, um diese Aufgaben genauer zu konkretisieren.

Die Ergebnisse der Interessenabwägung gemäß Absatz 2 müssen dokumentiert werden.

Die Vorschrift in Absatz 3 regelt die Anonymisierung von personenbezogenen Daten nach Abschluss der Datenauswertung. Da es verschiedene Techniken zur Anonymisierung gibt, sollte klargestellt werden, dass die Anonymisierung nach dem aktuellen “Stand der Technik” erfolgen muss. Außerdem sollte ein zusätzlicher Passus hinzugefügt werden, der eine jährliche Überprüfung des verwendeten Anonymisierungsverfahrens vorschreibt und alternative Maßnahmen wie die Löschung der Daten ermöglicht, da eine Anonymisierung nicht vollständig von der datenschutzrechtlichen Verantwortung entbindet. Die Formulierung i n Absatz 3 Satz 2 sollte korrigiert werden, da sie irreführend von “anonymisierten personenbezogenen Daten” spricht.

Ungeachtet dessen geht der Autor davon aus, das nach jetzigen wissenschaftlichen Erkenntnissen eine Anonymisierung dieser Daten praktisch unmöglich ist.

In Absatz 4 wird festgelegt, dass bei Feststellung eines Schadprogramms dieses jederzeit beseitigt oder dessen Funktion eingeschränkt werden kann, sofern es durch die Datenanalyse entdeckt wurde. Dies gilt auch für Fälle, die unter § 303a StGB fallen. Es erscheint ungewöhnlich, dass eine solche Regelung in einer Datenschutzvorschrift enthalten ist, da sie sich auf die technische IT-Sicherheit bezieht. Eine ähnliche Vorschrift wurde im Cybersicherheitsgesetz Baden-Württemberg erlassen, um Gefahren für die Cybersicherheit abzuwehren. Es bleibt fraglich, ob die aktuelle Formulierung sinnvoll ist, da keine Angaben zur Art, dem Umfang und der Herkunft der Gefahr gemacht werden. Darüber hinaus ist unklar, welche technischen Eingriffe erforderlich sind, um eine solche “Beseitigung” vorzunehmen.

2.10 § 8 HITSiG-E – Verwendung von auf informationstechnischen Systemen gespeicherten Daten

Es wäre zweckmäßig, im HITSiG eine Rechtsgrundlage für die automatisierte Verarbeitung von Protokolldaten und Metadaten zu schaffen, da dies zur Informationssicherheit beitragen kann. Allerdings muss beachtet werden, dass solche Daten fast immer personenbezogene Informationen enthalten, insbesondere wenn sie kumuliert werden oder einzigartig sind. Derzeit berücksichtigt § 8 HITSiG-E diese Eigenschaft nicht hinlänglich, da er nur technisch-organisatorische Schutzvorkehrungen und Überprüfungen vorschlägt. Es wäre daher hilfreich, einen Verweis auf die flankierende Verfahrensvorschrift § 14 HITSiG-E einzufügen, um sicherzustellen, dass angemessene Schutzmaßnahmen ergriffen werden. Das Verhältnis von § 8 HITSiG-E zu § 7 HITSiG-E ist unklar und sollte unbedingt geklärt werden. Ähnliche Probleme bestehen bei § 9 HITSiG-E, der ebenfalls Regelungen zur Erhebung und Auswertung von Datenverkehr im Landesdatennetz enthält.

Das Damoklesschwert einer verstecken verfassungswidrigen Vorratsdatenspeicherung droht.

2.11 § 10 HITSiG-E – Auswertung ohne Inhaltsdaten

§ 10 HITSiG-E ist eine ergänzende Vorschrift zur Datenauswertung im Sinne der Informationssicherheit (ohne Inhaltsdaten) gemäß § 8 und § 9 HITSiG-E, die offensichtlich davon ausgeht, dass die in diesem Kontext verarbeiteten Daten einen Personenbezug haben. Um dies deutlicher zu machen, sollte dies nicht nur in § 10, sondern auch schon in den § 8 und § 9 des Gesetzes klargestellt werden.

Im Sinne des Datenschutzes ist es positiv zu bewerten, dass der Fokus auf der automatisierten Auswertung der Daten liegt, um die Intensität eines möglichen Grundrechtseingriffs entsprechend den Vorgaben des Bundesverfassungsgerichts zu reduzieren. Für manuelle oder personenbezogene Datenauswertungen werden Einschränkungen formuliert. Allerdings ist unklar, welche weiteren Verarbeitungsvorgänge über Absatz 1 hinaus relevant sein sollen, wie die Formulierung “insbesondere” nahelegt. Obwohl Absatz 2 einschränkende Anforderungen für die über Absatz 1 hinausgehende Datenverarbeitung formuliert, sind diese nicht ausreichend, da sie - aufgrund der personenbezogenen Daten - die verfassungsrechtlich geschützten Rechtspositionen der Betroffenen nicht ausreichend berücksichtigen, beispielsweise im Rahmen einer kumulativen Interessenabwägung der widerstreitenden Rechtsgüter. Die eingeschränkte Anordnungsbefugnis der Auswertungsmaßnahmen kann dieses datenschutzrechtliche Defizit allein nicht ausgleichen.

2.12 § 11 HITSiG-E – Auswertung von Inhaltsdaten

Der Kern von § 11 bezieht sich auf die Auswertung von Inhaltsdaten. Trotzdem weist auch diese Vorschrift systematische Mängel im Datenschutz- und Maßnahmenteil des HITSiG-E auf. Absatz 1 bezieht sich zunächst auf die Auswertung von Metadaten gemäß § 8 und § 9, obwohl es sich laut Titel um die Auswertung von Inhaltsdaten handeln soll. Es gibt auch inhaltliche Überschneidungen, insbesondere mit § 8, und es ist nicht klar, wie die jeweiligen Maßnahmen voneinander abgegrenzt werden sollen, einschließlich der unverzüglichen Löschpflicht, die bereits in § 8 Abs. 2 Satz 2 HITSiG-E geregelt ist. Absatz 3 fehlt es an einer dokumentierten Abwägung der widerstreitenden Interessen. Darüber hinaus ist aus Absatz 1 bis 3 nicht ersichtlich, was die Unterscheidung zwischen Verkehrs- und Inhaltsdaten sein soll, obwohl dies der Titel der Vorschrift erwarten lässt. Absatz 4 enthält eine juristisch notwendige Regelung zum Kernbereichsschutz, jedoch ist unklar, was unter Inhaltsdaten im Sinne des Gesetzes zu verstehen ist und aus welcher Quelle diese stammen.

Das Damoklesschwert einer verstecken verfassungswidrigen Vorratsdatenspeicherung droht erneut.

2.13 § 14 HITSiG-E – Gewährleistung der Informationssicherheit und des Datenschutzes

Eine gesetzliche Regelung, die die Informationssicherheit verbessern möchte, muss auch den Datenschutz und die Anforderungen an die Datensicherheit berücksichtigen, wenn sie (personenbezogene) Daten auswertet. Es ist daher zu begrüßen, dass die derzeitige Entwurfsfassung eine ausdrückliche Regelung zu diesem Thema enthält. Um die Klarheit zu verbessern, wäre jedoch ein Verweis auf § 14 HITSiG aus den vorhergehenden und darauf bezogenen Vorschriften sinnvoll. Wie bereits in den Definitionen angemerkt, sollten weitere Schutzziele der IT-Sicherheit in Absatz 2 Nummer 4 in Betracht gezogen werden, da die Authentizität und Nichtabstreitbarkeit bei einer zuverlässigen Datenanalyse unerlässlich sind. Es ist lobenswert, dass der Datenzugriff durch das Vier-Augen-Prinzip, die getrennte Datenhaltung und die Protokollierung der entsprechenden Datenverarbeitung einschließlich des Berechtigungsmanagements gesichert wird. Die Erstellung eines Sicherheitskonzepts gemäß § 15 HITSiG-E ist ebenfalls positiv zu bewerten. In diesem Zusammenhang ist zu beachten, dass wesentliche Änderungen an IT-Systemen auch die genutzte Software betreffen können.

2.14 § 16 HITSiG-E – Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen der Beeinträchtigung

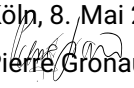
Ein redaktioneller Fehler findet sich in Absatz 4, der korrekterweise lauten sollte: "[…] nur mit Einwilligung der ersuchenden Stelle gemäß Absatz 1 übermitteln […]". Absatz 5 regelt die Einbindung von Dritten in die Wiederherstellung der Sicherheit oder Funktionsfähigkeit von IT-Systemen. Allerdings werden in diesem Absatz keine weiteren Anforderungen an die Dritten selbst, deren Qualifikation oder das Rechtsverhältnis untereinander festgelegt.

2.15 § 17 HITSiG-E – Information der Betroffenen

Die Mängel des vorliegenden Gesetzentwurfs in Bezug auf den Datenschutz und die Systematik setzen sich auch bei der Informationspflicht gegenüber Betroffenen fort, die eine wichtige verfassungsrechtliche Garantie darstellt (insbesondere im Hinblick auf das Zitiergebot als Nachweis für den Eingriff in Grundrechte). Es wird nicht erklärt, warum die Informationspflicht nur in den Fällen des § 10 Abs. 2 oder des § 11 Abs. 3 relevant sein soll. Dies ist rechtlich problematisch, da im Zusammenhang mit anderen Verarbeitungsszenarien zur IT-Sicherheit nach diesem Gesetz auch personenbezogene Daten anfallen können, die von Behörden verarbeitet werden.

Darüber hinaus wurde die NIS-2 Richtlinie sowie die anstehende NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz noch nicht berücksichtigt.

Köln, 8. Mai 2023



Pierre Gronau

Kontakt

ndaal Gesellschaft für Sicherheit in der Informationstechnik mbH & Co KG

Adolf-Grimme-Allee 3, D 50829 Köln, Deutschland.

e.: info@ndaal.eu

t.: +49 221 650 86 200

w.: https://ndaal.eu

Amtsgericht Köln, HRA 35474

Komplementärin XSTeam Beteiligungs GmbH

Geschäftsführer Carsten Dingendahl

Amtsgericht Köln, HRB 105499

bitkom

Stellungnahme

Stellungnahme zum Gesetz zur Erhöhung der IT-Sicherheit in der hessischen Verwaltung

7. Mai 2023

Simran Mann
Referentin
Sicherheitspolitik

M +49 30 27576-214
s.mann@bitkom.org

Albrechtstraße 10
10117 Berlin

Cybersicherheit in Hessen stärken

Das Gesetz zur Erhöhung der IT-Sicherheit in der hessischen Verwaltung ist grundsätzlich zu begrüßen. **Die Sicherheit der digitalen Systeme und Daten der Verwaltung ist von zentraler Bedeutung für die Wirtschaft und die Gesellschaft.** Das Gesetz zielt darauf ab, das Hessen CyberCompetenceCenter (Hessen3C) zu einer Zentralstelle für die Informationssicherheit in Hessen durch eine Rechtsgrundlage auszubauen. Dies ist ein wichtiger Schritt, um das Vertrauen in die digitale Verwaltung zu stärken und die gesellschaftliche Widerstandsfähigkeit gegenüber Cyberbedrohungen zu erhöhen.

Das Gesetz sieht verschiedene Maßnahmen vor, um die Informationssicherheit zu gewährleisten, wie beispielsweise das Entfallen der Amtshilfeersuchen zur Erfüllung der Aufgaben des Zentrums für Informationssicherheit sowie das Vortragsrecht der/des Landes-CISO. **Diese Maßnahmen sind essenziell, um der flexiblen Gefahrenlage im Cyberraum zu begegnen.** Sie tragen dazu bei, dass die hessische Verwaltung besser auf aktuelle und zukünftige Bedrohungen vorbereitet ist.

Dennoch sollte das Gesetz an einigen Punkte geschärft werden. Dazu gehört u.a. die rechtlich geschützte Unterstützung der Kommunen durch das Hessen3C, die Inkludierung der Schulen in den Geltungsbereich des Gesetzes sowie die Aufnahme der Meldepflicht für die gesamte hessische Verwaltung.

- Es ist zu begrüßen das zukünftig das Hessische Zentrum für Informationssicherheit (Hessen3C) **ohne Amtshilfeersuchen** anderer Landesbehörden operativ tätig sein kann.

- Auf Grund der vielfältigen Aufgaben des Hessen3C, Prävention durch Lagebeobachtung, Sammlung und Auswertung von Informationen zu Sicherheitsrisiken, Schwachstellen und Schadprogrammen, Informationen, Warnungen und Empfehlungen an Behörden und der Öffentlichkeit sowie die aktive Abwehr von konkreten Gefahren, ist es notwendig, dass Zentrum mit **ausreichenden finanziellen und personellen Ressourcen** auszustatten. Dabei sind auf Grund des Fachkräftemangel auch **attraktive und wettbewerbsfähige Arbeitsangebote für IT-Fachkräfte** zu bedenken.

- Die Kommunen in Deutschland sind den Bürgerinnen und Bürger am nächsten und sind auch für wichtige alltägliche Funktionen wie die Müllentsorgung, das Auszahlen von Wohn- und Sozialgeld zuständig. Daher ist es wichtig die **Unterstützung der Kommunen** in den Auftrag des Hessen3C zu inkludieren. Eine Inkludierung nach Kapazität ist dazu unzureichend.

- Es ist zu begrüßen, dass das Landes-CSIRT, welches die Rolle einer zentralen Kontaktstelle für das Bundesamt für Sicherheit in der Informationstechnik übernimmt, in das Hessen3C eingebunden wird. In der Bekämpfung von Cyberangriffen stellt ein **regelmäßiger Informationsaustausch** eine zentrale Rolle dar.

- Es ist zu begrüßen, dass die einzelnen Stellen der öffentlichen Verwaltung weiterhin in der **Pflicht** sind, selbstständig für eine **angemessene Sicherheit ihrer informationstechnischen Systeme** zu gewährleisten.

- Es ist zu begrüßen, dass die/der **zentrale Beauftragte oder zentraler Beauftragter für Informationssicherheit** (Chief Information Security Officer, CISO) **ressortübergreifende Eingriffsbefugnisse erhält**. Die **Unabhängigkeit** des CISOs ist essenziell zur Erfüllung ihrer/seiner Aufgaben.

- **§3(1) Schulen** in öffentlicher Trägerschaft sollten **nicht aus der Verpflichtung genommen werden angemessene organisatorische und technische Vorkehrungen sowie weitere Maßnahmen zur Gewährleistung der Informationssicherheit umzusetzen.** Schulen verfügen über sensible Daten der Schülerinnen und Schüler und führen eine grundlegende gesellschaftliche Tätigkeit aus. Eine Empfehlung zur

Einhaltung der Grundsätze ist dahingehen unzureichend. Der Datenschutz kann nur durch Informationssicherheit gewährleistet werden.

- **§3(3)** Es ist zu begrüßen, dass jede Stelle eine/n **Informationssicherheitsbeauftragten** benennen muss. Dabei muss auch sichergestellt werden, dass sie/er, gleich des CISOs, über **die notwendigen ressortübergreifenden Eingriffsbefugnisse verfügt**.

- **§7** Es ist zu begrüßen, dass zum Zwecke der Arbeitstätigkeit des Hessen3C eine **Analyse von Daten** möglich gemacht wird und auch die Wertung der Daten sowie mögliche Maßnahmen zum Schutz der Daten **konstruktiv reguliert** wird.

- **§18 Zum Schutz aller ist es von Interesse, dass auch der Hessische Landtag, der Hessische Rechnungshof, der Hessische Beauftragte für Datenschutz und Informationsfreiheit, die Gerichte und Staatsanwaltschaften sowie die Hochschulen dem Zentrum für Informationssicherheit Informationen, welche der Abwehr von Gefahren dienen, melden**. Nur durch eine vollständige Informationsgrundlage kann das Zentrum seine Aufgabe erfolgreich erfüllen und übergreifende Cyberangriffskampagnen aufgedeckt werden. Dies sollte die Unabhängigkeit dieser Stellen in ihrer Aufgabenausführung nicht gefährden, sondern die Aufgabenerfüllung absichern.

- Im Rahmen der Weiterentwicklung der Tätigkeiten des Hessen3C ist ein **Erhalt der Unterstützung von Kommunen und kommunale Eigenbetriebe, KRITIS-Einrichtungen sowie hessischen Unternehmen bei der Bewältigung von Cyberangriffen zu begrüßen.** Dazu sollte der **Informationsaustausch** über z.B. Lagebewertungen zwischen dem Zentrum der Informationssicherheit und der hessischen Wirtschaft eingeführt werden.