20. Wahlperiode

Drucksache **20/10752**

HESSISCHER LANDTAG

14. 03. 2023

Plenum

Gesetzentwurf

Landesregierung

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

Die Landesregierung legt mit Schreiben vom 13. März 2023 den nachstehenden, durch Kabinettsbeschluss vom 13. März 2023 gebilligten und festgestellten Gesetzentwurf dem Landtag zur Beschlussfassung vor. Der Gesetzentwurf wird vor dem Landtag von dem Hessischen Minister des Innern und für Sport vertreten.

A. Problem

Die Nutzung informationstechnischer Systeme durchdringt Staat, Wirtschaft und Gesellschaft in immer größerem Maße. Die Handlungsfähigkeit der öffentlichen Verwaltung aller Ebenen hängt heute in hohem Maße von Informations- und Kommunikationstechnologien ab. Informationssicherheit und Datenschutz sind elementare Voraussetzungen für die weitere erfolgreiche Digitalisierung der Verwaltung. Nur wenn Unternehmen und Bürger darauf vertrauen, dass ihre Daten sicher sind, werden neue digitale Prozesse angenommen und genutzt.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt in seinem Bericht zur Lage der IT-Sicherheit in Deutschland 2022 die Gefährdungslage als so hoch wie noch nie. Die voranschreitende Digitalisierung und Vernetzung bietet den Cyber-Angreifern immer neue Einfallstore und weitreichende Möglichkeiten, Informationen auszuspähen, Geschäfts- und Verwaltungsprozesse zu sabotieren oder sich anderweitig auf Kosten Dritter kriminell zu bereichern. Zunehmend gerät auch die Verwaltung in den Fokus der Angreifer. In der im Jahr 2021 vorgestellten neuen nationalen Cyber-Sicherheitsstrategie stellt die Bundesregierung fest, dass die Gewährleistung einer angemessenen Cybersicherheit eine gesamtstaatliche Aufgabe ist, die nur gelingen kann, wenn·Bund, Länder und Kommunen eng zusammenarbeiten.

Mit dem Hessen CyberCompetenceCenter (Hessen3C) wurde eine zentrale Stelle zur Unterstützung aller öffentlichen Stellen eingerichtet, um starke Cyber-Expertisen und neue Fähigkeiten zum Schutz der eigenen Informations- und Kommunikationstechnik gebündelt aus- und aufzubauen sowie die hierfür erforderliche Technik bereitzustellen. Hierdurch wurden Strukturen geschaffen, die es jederzeit ermöglichen, angemessen den vielschichtigen Bedrohungen im Cyberraum zu begegnen.

Bislang fehlt es an einer umfassenden Rechtsgrundlage für die Befugnisse beziehungsweise Datenzugriffe, die für den umfänglichen Betrieb des Hessen3C als Zentrum zum Schutz der Informationstechnik in der Verwaltung vor Angriffen aus dem Cyberraum erforderlich sind.

Der Bund und andere Länder haben entsprechende Instanzen aufgebaut und die nötigen Rechtsgrundlagen geschaffen.

B. Lösung

Mit dem vorliegenden Entwurf eines Hessischen Gesetzes zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz - HITSiG) sollen die rechtlichen Grundlagen zur Steigerung der Sicherheit in der Informationstechnik in Hessen geschaffen werden. Der Gesetzentwurf hat folgende Schwerpunkte:

Eingegangen am 14. März 2023 · Eilausfertigung am 14. März 2023 · Ausgegeben am 4. April 2023
Herstellung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden · www.Hessischer-Landtag.de

Zentrum für Informationssicherheit

Erstmals werden einer Zentralstelle Befugnisse eingeräumt, zur Erhöhung der IT-Sicherheit in der Landesverwaltung und zur Abwehr von Gefahren für die Informationstechnik des Landes eigenständig, ohne Amtshilfeersuchen anderer Landesbehörden, operativ tätig zu werden. Der Aufgabenbereich des Zentrums für Informationssicherheit reicht von der Prävention durch Lagebeobachtung, Sammlung und Auswertung von Informationen zu Sicherheitsrisiken, Schwachstellen und Schadprogrammen, über Informationen, Warnungen und Empfehlungen an Behörden und auch an die Öffentlichkeit bis hin zur aktiven Abwehr von konkreten Gefahren. Für Kommunen und sonstige Stellen kann das Zentrum für Informationstechnik im Wege der Auftragsverarbeitung entsprechende Dienstleistungen (je nach Kapazitäten) erbringen.

Eingebunden in das Zentrum für Informationssicherheit wird das bereits bestehende Computer Emergency Response Team, CERT, das Teile der Aufgaben des Zentrums für Informationssicherheit wahrnimmt. Das CERT ist außerdem zentrale Kontaktstelle nach § 8b Abs. 2 Nr. 4c des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG).

Regelungen zu Eingriffs- und Abwehrmaßnahmen

Das Zentrum für Informationssicherheit erhält die Befugnis, zu Zwecken der Abwehr von Gefahren für die Sicherheit in der Informationstechnik, Daten zu analysieren. Erforderlich waren hierzu Regelungen soweit personenbezogene Daten betroffen sind.

Des Weiteren erhält das Zentrum für Informationssicherheit die Möglichkeit, Daten im Landesdatennetz sowie auf informationstechnischen Systemen gespeicherten Daten im Hinblick auf Gefahren für die IT-Sicherheit zu untersuchen. Dabei werden je nach Tiefe des Eingriffs in Grundrechte Dritter (Fernmeldegeheimnis, Schutz personenbezogener Daten) gestaffelt Einschränkungen der möglichen Maßnahmen (Pseudonymisierung, automatisierte Auswertung, Beschränkung der Speichermöglichkeit etc.) festgelegt.

Flankiert werden diese Regelungen durch Anforderungen an die Gewährleistung der Datensicherheit und des Datenschutzes, an die Benachrichtigung der Betroffenen sowie die Einschränkungen zu Übermittlungsmöglichkeiten von personenbezogenen oder dem Fernmeldegeheimnis unterliegenden Daten.

Die Einrichtung einer Zentralstelle für Informationssicherheit entbindet die einzelnen Stellen der öffentlichen Verwaltung in Hessen nicht von ihrer Pflicht, selbständig für eine angemessene Sicherheit bei dem Betrieb ihrer informationstechnischen Systeme zu sorgen. Insbesondere ist die Informationssicherheitsleitlinie für die hessische Landesverwaltung in der jeweils gültigen Fassung in der gesamten hessischen Landesverwaltung zu·beachten. Das Zentrum für Informationssicherheit soll die Landesbehörden bei den aus dieser Leitlinie folgenden Aufgaben und Pflichten im Bereich der Prävention und Gefahrenabwehr durch Aufbau und Einsatz entsprechender Expertisen unterstützen. Die Regelungen der Informationssicherheitsleitlinie ergänzen die Regelungen dieses Gesetzes.

Zentrale Beauftragte oder zentraler Beauftragter für Informationssicherheit (Chief, Information Security Officer - CISO)

Die Position der zentralen Beauftragten oder des zentralen Beauftragten für Informationssicherheit (Chief Information Security Officer - CISO) wird gesetzlich verankert. Die Aufgaben und Befugnisse des CISO sind dem Grunde nach in der Informationssicherheitsleitlinie für die hessische Landesverwaltung beschrieben. Gesetzlich geregelt werden die ressortübergreifenden Eingriffsbefugnisse bei Gefahren für die Sicherheit in der Informationstechnik der Landesverwaltung, entsprechende Berichtspflichten sowie die Koordinierung des IT-Krisenmanagements der Landesverwaltung.

C. Befristung

Das HITSiG ist nach Ziffer 2.1.1., Erster Teil, des Leitfadens für das Vorschriften-Controlling (StAnz. 2018, S. 2) auf sieben Jahre befristet. Ein Ausnahmetatbestand ist nicht ersichtlich.

D. Alternativen

Die Alternative zu dem vorliegenden Gesetzesentwurf wäre die Beibehaltung der bisherigen Rechtslage. Die möglichen Maßnahmen zur Gewährleistung der Sicherheit in der Informationstechnik wären beschränkt auf die vorhandenen Rechtsgrundlagen. Die Analyse von Daten in dem für eine schlagkräftige Abwehr von Bedrohungen aus dem Cyberraum

erforderlichen Maße wäre (weiterhin) rechtlich nur eingeschränkt zulässig, da hier die Interessen des Datenschutzes (Sicht des Betroffenen) und der IT-Sicherheit (Schutz der Systeme) miteinander konkurrieren. Die erforderlichen fachlichen Expertisen sowie die technische Ausstattung für den Schutz der Informationstechnik müssten für jede Dienststelle separat aufgebaut und vorgehalten werden.

E. Finanzielle Auswirkungen

1. Auswirkungen auf die Finanz-, Vermögens- und Erfolgsrechnung

   Die neu zu schaffenden Befugnisse des Zentrums für Informationssicherheit sind mit einem entsprechenden Umsetzungsaufwand verbunden. Dessen Umfang und damit die Höhe der Vollzugskosten sind maßgeblich von der zukünftigen Entwicklung der IT-Sicherheitslage abhängig und daher nicht exakt zu beziffern.

   Einen Teil der zukünftig anfallenden administrativen Aufgaben erfüllt das Zentrum für Informationssicherheit bereits heute durch das CERT. Um die Möglichkeit der Untersuchung, Daten im Landesdatennetz sowie auf informationstechnischen Systemen gespeicherten Daten im Hinblick auf Gefahren für die IT-Sicherheit, nutzen zu können, sind einmalige Sachkosten für das Implementieren zusätzlicher Datenquellen in Höhe von 3,3 Millionen Euro sowie laufende Personalkosten i. H. v. rund einer Million Euro jährlich in der Entwicklungsphase und im Wirkbetrieb obligatorisch.

   Die Haushaltsmittel für diese Kosten sind beim Hessischen Ministerium des Innern und für Sport bereits etatisiert.

	Liquidität		**Ergebnis**	
	Ausgaben	Einnahmen	Aufwand	Ertrag
Einmalig im Haushaltsjahr 2023	3.300.000 €			
Einmalig in künftigen Haushaltsjahren				
Laufend ab Haushaltsjahr 2023			1.000.000 €	

2. Auswirkungen auf die mittelfristige Finanz- und Entwicklungsplanung

   Die Auswirkungen des HITSiG auf die mittelfristige Finanz- und Entwicklungsplanung können zurzeit nicht beurteilt werden.

3. Auswirkungen für hessische Gemeinden und Gemeindeverbände

   Das HITSiG statuiert für hessische Gemeinden und Gemeindeverbände keine Verpflichtungen, die über die bereits bestehenden Verpflichtungen zur IT-Sicherheit hinausgehen.

F. Unmittelbare oder mittelbare Auswirkungen auf die Chancengleichheit von Frauen und Männern

Das HITSiG hat keine diesbezüglichen Auswirkungen.

G. Besondere Auswirkungen auf Menschen mit Behinderungen

Das HITSiG wurde am Maßstab der UN-Behindertenrechtskonvention überprüft.
Es bestand kein Änderungsbedarf.

Der Landtag wolle das folgende Gesetz beschließen:

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

Vom

ERSTER TEIL
Allgemeine Vorschriften

§ 1
Geltungsbereich

Soweit andere Rechtsvorschriften nicht entgegenstehen, gilt dieses 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.

§ 2
Begriffsbestimmungen

Im Sinne dieses Gesetzes

1. ist Informationstechnik jedes technische Mittel zur elektronischen Verarbeitung oder Übertragung von Informationen,
2. ist Informationssicherheit die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität oder Vertraulichkeit (Schutzziele) von Informationen betreffen, durch Sicherheitsvorkehrungen
   a) in informationstechnischen Systemen, Komponenten oder Prozessen oder
   b) bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen,
3. sind Schadprogramme Programme und sonstige informationstechnische Routinen und Verfahren, die dem Zweck dienen, unbefugt
   a) Daten zu nutzen oder zu löschen oder
   b) auf sonstige informationstechnische Abläufe einzuwirken,
4. sind Sicherheitslücken Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen der Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können,
5. sind Übergabe- und Knotenpunkte IT-Systeme, über die der Datenverkehr in ein anderes Netz fließt (Übergabepunkt) oder innerhalb eines Netzes verteilt wird (Knotenpunkt),
6. sind Protokolldaten Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind; Protokolldaten können Verkehrsdaten nach § 3 Nr. 70 des Telekommunikationsgesetzes vom 23. Juni 2021 (BGBl. I S. 1858), zuletzt geändert durch Gesetz vom 20. Juli 2022 (BGBl. I

S. 1166), und Nutzungsdaten nach § 2 Abs. 2 Nr. 3 des Telekommunikation-Telemedien-Datenschutz-Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045), zuletzt geändert durch Gesetz vom 12. August 2021 (BGBl. I S. 3544; 2022 I S. 1045), enthalten.

§ 3
Grundsätze der Informationssicherheit

(1) Die Stellen nach § 1 Nr. 1 und 2, mit Ausnahme der Schulen in öffentlicher Trägerschaft sowie genehmigter und anerkannter Ersatzschulen im Sinne des Hessischen Schulgesetzes, treffen angemessene organisatorische und technische Vorkehrungen sowie sonstige Maßnahmen zur Gewährleistung der Informationssicherheit. Für technische Maßnahmen soll der Stand der Technik maßgeblich sein. Maßnahmen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den möglichen Folgen der Verletzung der Schutzziele steht. Um die Erreichung und Aufrechterhaltung eines angemessenen Informationssicherheitsniveaus zu gewährleisten, haben die Stellen nach § 1 Nr. 1 und 2 sich an der IT-Grundschutzmethodik des Bundesamtes für Sicherheit in der Informationstechnik zu orientieren und setzen ein Informationssicherheitsmanagementsystem um.

(2) Die jeweils geltenden Standards und das jeweils geltende IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik werden zur Anwendung empfohlen. Werden dem Land Hessen Informationssicherheitsstandards verbindlich durch Beschlüsse des IT-Planungsrates nach Art. 91c Abs. 2 Satz 1 des Grundgesetzes für die Bundesrepublik Deutschland i. V. m. § 1 Abs. 1 Satz 1 Nr. 2 des IT-Staatsvertrages vom 30. Oktober 2009 bis 30. November 2009 (GVBl. I 2010 S. 65, 66), geändert durch Staatsvertrag vom 15. März 2019 bis 21. März 2019 (GVBl. S. 150, 151), vorgeschrieben oder nach § 5 des Onlinezugangsgesetzes vom 14. August 2017 (BGBl. I S. 3122, 3138), zuletzt geändert durch Gesetz vom 28. Juni 2021 (BGBl. I S. 2250), in der jeweils geltenden Fassung, festgelegt, sind diese Standards durch die Stellen nach § 1 Nr. 1 und 2 bei den von ihnen eingesetzten informationstechnischen Systemen einzuhalten.

(3) Die Verantwortung für die Gewährleistung der Informationssicherheit im Sinne des Abs. 1 trägt die jeweilige Leiterin oder der Leiter der Stelle für ihren oder seinen jeweiligen Verantwortungsbereich. Sie oder er stellt im Rahmen der ihr oder ihm zugewiesenen Aufgaben und Befugnisse die erforderlichen personellen und finanziellen Ressourcen zur Verfügung. Für jede Stelle nach § 1 Nr. 1 und 2 ist eine Informationssicherheitsbeauftragte oder ein Informationssicherheitsbeauftragter und deren oder dessen Vertretung zu benennen. Für die Geschäftsbereiche der Staatskanzlei und der Ministerien der hessischen Landesverwaltung sind jeweils zentrale Informationssicherheitsbeauftragte des Geschäftsbereichs (Ressort-ISB) zu benennen; diese unterstützen die Leitung des Geschäftsbereichs in Belangen der Informationssicherheit.

(4) Wesentliche Änderungen an den informationstechnischen Systemen einer Stelle nach § 1 Nr. 1 und 2 dürfen nur im Benehmen mit der oder dem nach Abs. 3 Satz 3 benannten Informationssicherheitsbeauftragten durchgeführt werden.

(5) Den Stellen nach § 1 Nr. 3 und den Schulen in öffentlicher Trägerschaft sowie den genehmigten und anerkannten Ersatzschulen im Sinne des Hessischen Schulgesetzes wird die Einhaltung der Grundsätze nach Abs. 1 bis 4 empfohlen.

ZWEITER TEIL
Organisation

§ 4
Die oder der Zentrale Informationssicherheitsbeauftragte der Landesverwaltung

(1) Auf Vorschlag der für IT- und Cybersicherheit in der Landesverwaltung zuständigen Ministerin oder des hierfür zuständigen Ministers setzt die Landesregierung zur Gewährleistung der Informationssicherheit in der Landesverwaltung eine Zentrale Informationssicherheitsbeauftragte oder einen Zentralen Informationssicherheitsbeauftragten (Chief Information Security Officer, CISO) ein. Die oder der CISO ist ressortübergreifend tätig, hat ein umfassendes Informationsrecht und ist von den Dienststellen der Landesverwaltung bei ihrer oder seiner Aufgabenerfüllung zu unterstützen, soweit Rechtsvorschriften nicht entgegenstehen. Er oder sie koordiniert ressortübergreifende Informationssicherheitsthemen und nimmt die Außenvertretung der hessischen Landesverwaltung in Belangen der Informationssicherheit wahr.

(2) Die Aufgaben der oder des CISO umfassen insbesondere

1. die Fortschreibung der Informationssicherheitsleitlinie der hessischen Landesverwaltung in Abstimmung mit der Staatskanzlei und den Ministerien und die kontinuierliche Verbesserung der Informationssicherheit in der Landesverwaltung,

2. die Beratung der Beauftragten oder des Beauftragten der Landesregierung für E-Government und Informationstechnik (CIO), der Staatskanzlei und der Ministerien sowie die Entwicklung von Empfehlungen in Fragen der Informationssicherheit,

3. die Koordinierung der Abwehrmaßnahmen nach § 5 Abs. 2 Satz 1 Nr. 2,

4. regelmäßige Berichte an die Landesregierung über den Sachstand der Informationssicherheit in der Landesverwaltung sowie über Maßnahmen und Anordnungen nach Abs. 3,

5. die Koordinierung des IT-Krisenmanagements der Landesverwaltung.

(3) Die oder der CISO ist berechtigt, zur Erfüllung der Aufgaben nach Abs. 2, insbesondere bei dienststellenübergreifenden informationstechnischen Sicherheitsvorfällen, unter Einbeziehung des jeweils betroffenen Geschäftsbereichs Maßnahmen zu empfehlen. Bei unmittelbaren und erheblichen Gefahren für die Informationssicherheit in der Landesverwaltung kann er oder sie erforderliche Sicherheitsmaßnahmen anordnen; die betroffenen Stellen sind unverzüglich zu informieren.

(4) Die oder der CISO hat ein Vortragsrecht bei der für IT- und Cybersicherheit in der Landesverwaltung zuständigen Ministerin oder dem hierfür zuständigen Minister und bei der oder dem CIO. Bei schwerwiegenden Anlässen hat die oder der CISO ein Vortragsrecht bei den Staatssekretärinnen oder Staatssekretären der Ministerien und bei der Chefin oder dem Chef der Staatskanzlei.

§ 5
Zentrum für Informationssicherheit

(1) Die für IT- und Cybersicherheit in der Landesverwaltung zuständige Ministerin oder der hierfür zuständige Minister richtet zur Förderung der Informationssicherheit ein Zentrum für Informationssicherheit ein.

(2) Das Zentrum für Informationssicherheit nimmt folgende Aufgaben wahr:

1. die Zusammenarbeit mit den für die Informationssicherheit zuständigen zentralen Stellen des Bundes, der anderen Länder und der Kommunen, unbeschadet besonderer Zuständigkeiten anderer Stellen,

2. die Erkennung, Untersuchung und Abwehr von Gefahren für die Informationssicherheit der Stellen nach § 1 Nr. 1 und 2,

3. die Unterstützung bei der Erkennung, Untersuchung und Abwehr von Gefahren für die Informationssicherheit der Stellen nach § 1 Nr. 3 auf deren Ersuchen,

4. die Unterstützung bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen der Beeinträchtigung nach § 16,

5. die technische Unterstützung und Beratung auf Ersuchen

   a) der Polizei- und Strafverfolgungsbehörden,

   b) des Landesamts für Verfassungsschutz,

   c) der oder des Hessischen Beauftragten für Datenschutz und Informationsfreiheit

   im Zusammenhang mit Tätigkeiten oder Ereignissen, die gegen die Informationssicherheit gerichtet sind oder die unter Nutzung der Informationstechnik erfolgen,

6. die Unterstützung des Krisenstabs der Landesregierung,

7. die Sammlung und Auswertung von Informationen über Risiken, Beeinträchtigungen, Störungen und Vorkehrungen zur Abwehr von Gefahren für die Informationssicherheit,

8. die Information der Stellen nach § 1 sowie Dritter über die nach Nr. 7 gewonnenen Erkenntnisse, soweit dies zur Erfüllung ihrer staatlichen Aufgaben oder zur Wahrung ihrer Sicherheitsinteressen erforderlich ist,

9. die Beratung, Warnung und Empfehlung in Fragen der Informationssicherheit, einschließlich der Erstellung einer werktäglichen Übersicht, sowie im Zusammenhang mit Tätigkeiten oder Ereignissen, die die öffentliche Sicherheit oder Ordnung beeinträchtigen und unter Nutzung der Informationstechnik erfolgen,

10. die Entgegennahme von Sofortmeldungen aus der Landesverwaltung und die Koordinierung der Bearbeitung von Sicherheitsvorfällen,

11. die Untersuchung von Sicherheitsrisiken bei der Anwendung der Informationstechnik sowie der Test von vorhandenen Verfahren und Werkzeugen sowie deren Entwicklung zur Erkennung und Abwehr von Gefahren für die Informationssicherheit in Zusammenarbeit mit Wissenschaft und Forschung.

Ersuchen nach Satz 1 Nr. 5 sind durch das Zentrum für Informationssicherheit aktenkundig zu machen.

(3) Bestandteil des Zentrums für Informationssicherheit ist das Computer Emergency Response Team (CERT), durch das Teile der in Abs. 2 genannten Aufgaben wahrgenommen werden. Das CERT ist zentrale Kontaktstelle nach § 8b Abs. 2 Nr. 4 Buchst. c des BSI-Gesetzes in der Fassung der Bekanntmachung vom 14. August 2009 (BGBl. I S. 2821), zuletzt geändert durch Gesetz vom 23. Juni 2021 (BGBl. I S. 1982). Das CERT unterhält Mobile Incident Response Teams (MIRTs), die die Stellen nach § 1 bei der Wiederherstellung ihrer IT-Systeme nach § 16 unterstützen. Das CERT kann seine Dienstleistungen neben den in § 1 genannten Stellen auch privaten Unternehmen im Land Hessen anbieten, sofern die Kapazitäten des CERT dies erlauben; ein Anspruch privater Unternehmen auf eine Dienstleistung seitens des CERT besteht nicht.

§ 6
Zentraler IT-Dienstleister des Landes

Der zentrale IT-Dienstleister des Landes gewährleistet die Informationssicherheit im Landesdatennetz und der von ihm betriebenen informationstechnischen Systeme und berät das Zentrum für Informationssicherheit bei der Erledigung seiner Aufgaben, soweit diese die Informationssicherheit in der Landesverwaltung betreffen. Er berichtet der oder dem CISO zum Stand der Informationssicherheit in der Landesverwaltung.

DRITTER TEIL
Maßnahmen

§ 7
Datenverarbeitung

(1) Das Zentrum für Informationssicherheit darf personenbezogene Daten verarbeiten, wenn die Verarbeitung zur Erfüllung seiner im öffentlichen Interesse liegenden Aufgaben erforderlich ist.

(2) Die Verarbeitung personenbezogener Daten durch das Zentrum für Informationssicherheit zu anderen Zwecken als demjenigen, zu dem die Daten ursprünglich erhoben wurden, ist unbeschadet des Art. 6 Abs. 4 der Datenschutz-Grundverordnung und des § 21 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes zulässig, wenn

1. die Verarbeitung erforderlich ist
   a) zur Sammlung, Auswertung oder Untersuchung von Informationen über Risiken oder Vorkehrungen für die Informationssicherheit oder
   b) zur Unterstützung, Beratung oder Warnung in Fragen der Informationssicherheit und
2. kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

Eine Verarbeitung von besonderen Kategorien personenbezogener Daten durch das Zentrum für Informationssicherheit ist abweichend von Art. 9 Abs. 1 der Datenschutz-Grundverordnung und unbeschadet des § 20 Abs. 1 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes zulässig, wenn

1. die Verarbeitung erforderlich ist zur Abwehr einer erheblichen Gefahr für die Informationssicherheit,
2. ein Ausschluss dieser Daten von der Verarbeitung die Erfüllung der Aufgaben des Zentrums für Informationssicherheit unmöglich machen oder diese erheblich gefährden würde und
3. kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss dieser Daten von der Verarbeitung überwiegt.

Im Fall des Satz 2 sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person nach § 20 Abs. 2 Satz 2 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes vorzusehen.

(3) Ist die Verarbeitung der Daten über den Abschluss des Auswertungsvorgangs hinaus erforderlich, sind darin enthaltene personenbezogene Daten unverzüglich automatisiert zu anonymisieren. Ist eine Verarbeitung der Daten im Sinne des Satz 1 mit anonymisierten personenbezogenen Daten nicht möglich, sind für die weitere Verarbeitung der personenbezogenen Daten die §§ 10, 11, 13 und 17 entsprechend anzuwenden.

(4) Soweit die Auswertungen nach §§ 7 bis 11 ein Schadprogramm identifizieren, kann dieses jederzeit beseitigt oder in seiner Funktionsweise gehindert werden.

(5) Die Verwendungsbeschränkungen nach § 7 Abs. 3 und §§ 8 bis 11 betreffen nur Daten, die dem Fernmeldegeheimnis aus Art. 10 des Grundgesetzes für die Bundesrepublik Deutschland unterliegen oder einen Personenbezug aufweisen.

§ 8
Verwendung von auf informationstechnischen Systemen gespeicherten Daten

(1) Die auf den informationstechnischen Systemen der Stellen nach § 1 sowie auf sonstigen informationstechnischen Systemen, die mit dem Landesdatennetz verbunden sind, gespeicherten Protokolldaten von

1. Firewall-Systemen,
2. Systemen zur Erkennung und Beseitigung von Schadsoftware,
3. Systemen zur Erkennung von unerwünschten E-Mails,
4. Datenbankservern,
5. Web-, Proxy- und Anwendungsservern und
6. der Betriebssoftware von Computersystemen

dürfen automatisiert ausgewertet werden, soweit dies zum Erkennen, Eingrenzen, Nachverfolgen oder Beseitigen von Störungen oder Fehlern oder zum Erkennen und Abwehren von Gefahren für die Informationssicherheit durch Sicherheitslücken, Schadprogramme oder erfolgte oder versuchte Angriffe auf die Informationstechnik der Stellen nach § 1 erforderlich ist.

(2) Eine Auswertung von während der automatisierten Verarbeitung nach Abs. 1 anfallenden Inhaltsdaten ist nur unter den Voraussetzungen des § 11 zulässig. Die Daten der Auswertung nach Abs. 1 sind nach ihrer automatisierten Auswertung unverzüglich zu löschen, es sei denn, §§ 10 oder 11 sehen eine weitere Verwendung vor.

§ 9
Erhebung und Auswertung des Datenverkehrs im Landesdatennetz

(1) Soweit dies zum Erkennen und Abwehren von Gefahren für die Informationssicherheit durch Sicherheitslücken, Schadprogramme oder erfolgte oder versuchte Angriffe auf die Informationstechnik der Stellen nach § 1 erforderlich ist, darf der an den Übergabe- und Knotenpunkten des Landesdatennetzes anfallende Datenverkehr automatisiert erhoben und dürfen

1. der Erhebungszeitpunkt, die IP-Adresse einschließlich der Subnetzmaske, die Präfixlänge, der Port und die Medienzugriffskontrolladresse (Media-Access-Control-Address, MAC-Adresse), der vollständige Domänenname sowie die Kopf- und Statusdaten von Netzwerkpaketen für ein- und ausgehende Verbindungen,
2. für ein- und ausgehende Verbindung auf Basis der Hypertext-Übertragungsprotokolle (Hypertext Transfer Protocol, HTTP, und Hypertext Transfer Protocol Secure, HTTPS) zusätzlich zu Nr. 1 der vollständige einheitliche Ressourcenzeiger (Uniform Resource Locator, URL) und die Kopfdaten exklusive Cookie,

unverzüglich automatisiert ausgewertet werden.

(2) Eine Auswertung des während der automatisierten Erhebung des Datenverkehrs nach Abs. 1 anfallenden Inhalts der Kommunikation ist nur unter den Voraussetzungen des § 11 zulässig. Die nach Abs. 1 erhobenen Daten sowie die Daten der Auswertung sind nach der automatisierten Auswertung unverzüglich zu löschen, es sei denn, die §§ 10 oder 11 sehen eine weitere Verwendung vor.

§ 10
Auswertung ohne Inhaltsdaten

(1) Soweit die automatisierte Auswertung nach § 8 Abs. 1 oder § 9 Abs. 1 zureichende tatsächliche Anhaltspunkte dafür bietet, dass bestimmte Daten zur Abwehr von Gefahren im Sinne von § 8 Abs. 1 oder § 9 Abs. 1 erforderlich sind, dürfen diese für höchstens 90 Tage gespeichert werden. Die Daten sind unverzüglich automatisiert zu pseudonymisieren, soweit dies technisch möglich ist und die Daten nicht bereits pseudonym vorliegen. Die weitere Auswertung der nach Satz 1 gespeicherten Daten erfolgt nur automatisiert.

(2) Eine über Abs. 1 hinausgehende, insbesondere nicht automatisierte oder direkt personenbezogene Verarbeitung der Daten nach § 8 Abs. 1 und § 9 Abs. 1 ist nur zulässig, soweit und solange

1. hinreichende tatsächliche Anhaltspunkte den Verdacht begründen, dass
   a) die Daten ein Schadprogramm enthalten,
   b) die Ursache in einem Angriff oder einem Schadprogramm liegt oder
   c) sich aus den Daten Hinweise auf einen Angriff oder ein Schadprogramm ergeben können und
2. die Datenverarbeitung zur Abwehr des Schadprogramms oder Angriffs, zur Abwehr von Gefahren, die von dem Schadprogramm oder Angriff ausgehen, oder zur Erkennung und Abwehr anderer Schadprogramme oder Angriffe erforderlich ist.

Die Datenverarbeitung nach Satz 1 bedarf der Anordnung durch die Leiterin oder den Leiter der nach § 12 zur Ergreifung der Maßnahme zuständigen Stelle. Sofern das Zentrum für Informationssicherheit zuständige Stelle ist, darf die Anordnung nur durch eine Beschäftigte oder einen Beschäftigten des für IT- und Cybersicherheit in der Landesverwaltung zuständigen Geschäftsbereichs mit der Befähigung zum Richteramt getroffen werden.

§ 11
Auswertung von Inhaltsdaten

(1) Nach § 8 Abs. 1 und § 9 Abs. 1 verarbeitete Daten dürfen unverzüglich automatisiert nach technischen Indikatoren für Schadprogramme ausgewertet werden. Die nach Satz 1 ausgewerteten Daten sind nach ihrer automatisierten Auswertung unverzüglich zu löschen, es sei denn, die nachfolgenden Absätze sehen eine weitere Verwendung vor.

(2) Soweit die automatisierte Auswertung nach Abs. 1 zureichende tatsächliche Anhaltspunkte dafür bietet, dass bestimmte Daten zum Schutz vor Schadprogrammen erforderlich sind, dürfen diese für höchstens 90 Tage gespeichert werden. Die Daten sind unverzüglich automatisiert zu pseudonymisieren, soweit sie nicht bereits pseudonym sind. Die weitere Auswertung der nach Satz 1 und 2 gespeicherten Daten erfolgt nur automatisiert. Die Datenverarbeitung nach Satz 1 bedarf der Anordnung durch die Leiterin oder den Leiter der nach § 12 zur Ergreifung der Maßnahme zuständigen Stelle. Sofern das Zentrum für Informationssicherheit zuständige Stelle ist, darf die Anordnung nur durch eine Beschäftigte oder einen Beschäftigten des für IT- und Cybersicherheit in der Landesverwaltung zuständigen Geschäftsbereichs mit der Befähigung zum Richteramt getroffen werden.

(3) Eine über die Abs. 1 und 2 hinausgehende, insbesondere nicht automatisierte oder direkt personenbezogene Auswertung der Daten nach Abs. 1 Satz 1 ist nur zulässig, soweit und solange

1. hinreichende tatsächliche Anhaltspunkte den Verdacht begründen, dass
   a) die Ursache in einem Schadprogramm liegt oder
   b) sich aus den Daten Hinweise auf ein Schadprogramm ergeben und
2. die Datenverarbeitung zur Abwehr des Schadprogramms, zur Abwehr von Gefahren, die von dem Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich ist.

Die Datenverarbeitung nach Satz 1 ebenso wie eine erforderliche Wiederherstellung des Personenbezugs bereits pseudonymisierter Daten bedarf der Anordnung durch die Leiterin oder den Leiter der nach § 12 zur Ergreifung der Maßnahme zuständigen Stelle. Sofern das Zentrum für Informationssicherheit zuständige Stelle ist, darf die Anordnung nur durch eine Beschäftigte oder einen Beschäftigten des für IT- und Cybersicherheit in der Landesverwaltung zuständigen Ministeriums mit der Befähigung zum Richteramt getroffen werden.

(4) Soweit möglich, ist bei der Datenverarbeitung nach Abs. 1 bis 3 technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Werden aufgrund der Maßnahmen nach Abs. 1 bis 3 Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt, dürfen diese nicht verwendet werden. Auswertungsergebnisse, die den Kernbereich privater Lebensgestaltung betreffen, sind unverzüglich zu löschen. Dies gilt auch in Zweifelsfällen. Die Erlangung und Löschung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der nachträglichen Überprüfung der Rechtmäßigkeit der Verarbeitung verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch zum Ablauf des Kalenderjahres, das dem Jahr der Dokumentation folgt. Satz 1 bis 6 gelten nicht, sofern für die Verarbeitung der in Satz 1 bis 3 genannten Daten eine Ausnahmeregelung nach Art. 9 Abs. 2 oder 3 der Datenschutz-Grundverordnung oder nach dem Hessischen Datenschutz- und Informationsfreiheitsgesetz greift.

§ 12
Zuständigkeit

(1) Soweit das Landesdatennetz einschließlich der Übergabe- und Knotenpunkte oder die informationstechnischen Systeme der Stellen nach § 1 Nr. 1 und 2 betroffen sind, ist das Zentrum für Informationssicherheit für die Ergreifung der Maßnahmen nach §§ 8 bis 11 zuständig. Dies betrifft alle Systeme, Verfahren und Plattformen, die beim zentralen IT-Dienstleister des Landes betrieben und für mehrere Geschäftsbereiche bestimmt sind. Die Bereitstellung von Daten oder von Analyseergebnissen zu Daten, die nicht vom zentralen IT-Dienstleister verarbeitet werden oder für einen einzelnen Geschäftsbereich verarbeitet werden, sind in einer Landesrichtlinie zu regeln. Daten des Hessischen Landtags, des Hessischen Rechnungshofs, des Hessischen Beauftragten für Datenschutz und Informationsfreiheit, der Gerichte und Staatsanwaltschaften sowie der Hochschulen nach § 2 des Hessischen Hochschulgesetzes dürfen nur einvernehmlich mit diesen verarbeitet werden. Daten, die dem richterlichen, staatsanwaltschaftlichen oder rechtspflegerischen Arbeitsprozess oder der Abgeordnetentätigkeit zuzurechnen sind, dürfen von dem Zentrum für Informationssicherheit nicht verarbeitet werden.

(2) Die Stellen nach § 1 sind für die Ergreifung der Maßnahmen nach §§ 8 bis 11 für ihren Verantwortungsbereich zuständig. Sie können das Zentrum für Informationssicherheit mit den erforderlichen Maßnahmen nach §§ 8 bis 11 im Wege der Auftragsverarbeitung im Sinne von Art. 28 der Datenschutz-Grundverordnung betrauen, sofern die Kapazitäten des Zentrums für Informationssicherheit dies erlauben. Ein Anspruch auf Übernahme der Maßnahmen durch das Zentrum für Informationssicherheit besteht nicht.

§ 13
Übermittlung personenbezogener oder dem Fernmeldegeheimnis unterliegender Daten

(1) Die nach § 12 zuständigen Stellen können die jeweils von ihnen nach § 10 Abs. 2 und § 11 Abs. 3 verarbeiteten personenbezogenen oder dem Fernmeldegeheimnis unterliegenden Daten an die für den Betrieb der Informationstechnik der Verwaltung zuständigen Stellen oder damit beauftragte Dritte übermitteln, wenn und soweit dies zur Abwehr oder Beseitigung von Gefahren für die Informationssicherheit erforderlich ist.

(2) Die nach § 12 zuständigen Stellen können die jeweils von ihnen nach § 10 Abs. 2 und § 11 Abs. 3 verarbeiteten personenbezogenen oder dem Fernmeldegeheimnis unterliegenden Daten an die Strafverfolgungsbehörden zur Verfolgung einer mittels eines Schadprogramms begangenen Straftat nach den §§ 202a, 202b, 202c, 269, 271, 274 Abs. 1 Nr. 2, §§ 303a, 303b und 348 des Strafgesetzbuches übermitteln. Sie können diese Daten ferner übermitteln

1. zur Abwehr einer Gefahr für die öffentliche Sicherheit, die unmittelbar von einem Schadprogramm ausgeht, an die Polizeibehörden,
2. zur Unterrichtung über Tatsachen, die sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht oder einen internationalen kriminellen, terroristischen oder staatlichen Angriff mittels Schadprogrammen oder vergleichbaren schädlich wirkenden informationstechnischen Mitteln auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland oder zum Land Hessen erkennen lassen, an das Landesamt für Verfassungsschutz Hessen.

(3) Für sonstige Zwecke können die nach § 12 zuständigen Stellen übermitteln

1. an die Strafverfolgungsbehörden zur Verfolgung einer Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere einer in § 100a Abs. 2 der Strafprozessordnung bezeichneten Straftat,
2. an die Polizeibehörden zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates oder für Leib, Leben oder Freiheit einer Person oder für Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist.

Die Übermittlung nach Satz 1 bedarf der vorherigen gerichtlichen Zustimmung. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Zuständig ist das Amtsgericht, in dessen Bezirk die nach § 12 zuständige Stelle ihren Sitz hat.

(4) Ist das Zentrum für Informationssicherheit in den Fällen des Abs. 2 zuständige Stelle nach § 12, darf es die nach § 10 Abs. 2 und § 11 Abs. 3 verarbeiteten personenbezogenen oder dem Fernmeldegeheimnis unterliegenden Daten auch abweichend von § 10 Abs. 2 und § 11 Abs. 3 bis zur Beendigung der Unterstützung der Behörden, an die die Daten übermittelt wurden, weiterverarbeiten. § 11 Abs. 4 bleibt unberührt.

§ 14
Gewährleistung der Informationssicherheit und des Datenschutzes

(1) Die nach §§ 8 bis 11 erhobenen oder gespeicherten Daten sind durch technische und organisatorische Maßnahmen nach dem Stand der Technik gegen unbefugte Kenntnisnahme, Veränderung und Verwendung zu schützen. Bei der Umsetzung dieser Maßnahmen ist ein besonders hohes Maß an Informationssicherheit zu gewährleisten.

(2) Die zu treffenden Maßnahmen umfassen insbesondere

1. die organisatorische Trennung von den für die üblichen Aufgaben des IT-Betriebs verantwortlichen Organisationseinheiten,
2. die technische Trennung von den für die üblichen Aufgaben des IT-Betriebs vorgehaltenen informationstechnischen Systemen, insbesondere die Speicherung in gesonderten, von den für die üblichen betrieblichen Aufgaben getrennten Speichereinrichtungen,
3. besondere Sicherungsmaßnahmen gegen unberechtigte Zugriffe aus anderen Netzen, insbesondere aus dem Internet,
4. die Umsetzung von Maßnahmen nach dem Stand der Technik zur Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit der gespeicherten Daten,
5. die Beschränkung des Zutritts zu den und des Zugriffs auf die Datenverarbeitungsanlagen auf Personen, die durch die jeweilige Leitung der Stelle hierzu besonders ermächtigt sind, und
6. das Zusammenwirken von mindestens zwei Personen beim Zugriff auf die Daten.

(3) Zum Zwecke der Datenschutzkontrolle ist jeder Zugriff auf die Datenverarbeitungsanlagen, insbesondere das Lesen, Kopieren, Ändern, Löschen und Sperren von den nach §§ 8 bis 11 erhobenen oder gespeicherten Daten, in einem Protokoll aufzunehmen. Das Protokoll hat Zeitpunkt und Art des Zugriffs sowie eine eindeutige Kennung der auf die Daten zugreifenden Personen zu enthalten. Das Protokoll darf ausschließlich zum Zwecke der Rechtmäßigkeitskontrolle verwendet werden. Die Einträge in das Protokoll sind nach zwölf Monaten zu löschen.

(4) Der oder dem Hessischen Datenschutzbeauftragten ist durch das Zentrum für Informationssicherheit einmal im Jahr eine Aufstellung über die nach den §§ 8 bis 11, 13 und 16 erfolgten Verarbeitungen vorzulegen. Inhalt und Frist der Aufstellung erfolgen im Einvernehmen mit der oder dem Hessischen Datenschutzbeauftragten. Soweit Daten der hessischen Justiz betroffen sind, ist eine Aufstellung über die betreffenden Verarbeitungen zusätzlich dem Kontrollgremium bei der IT-Stelle der hessischen Justiz vorzulegen. Das Kontrollgremium ist berechtigt, Auskünfte zu verlangen und Einsicht in die Datenverarbeitungen durch das Zentrum für Informationssicherheit zu nehmen.

§ 15
Sicherheitskonzept

Maßnahmen nach den §§ 7 bis 11 dürfen nur ergriffen werden, wenn ein Sicherheitskonzept erstellt wurde und die Umsetzung aller darin vorgesehenen technischen und organisatorischen Maßnahmen von der zuständigen Stelle aktenkundig gemacht wurde. Das Sicherheitskonzept ist vor jeder wesentlichen Veränderung der eingesetzten technischen Systeme zu aktualisieren und alle zwei Jahre einer Revision zu unterziehen. Für jede wesentliche Veränderung des Sicherheitskonzeptes gilt Satz 1 entsprechend.

§ 16
Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen der Beeinträchtigung

(1) Handelt es sich bei einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer Stelle nach § 1 um einen herausgehobenen Fall, so kann das Zentrum für Informationssicherheit auf Ersuchen der betroffenen Stelle die Maßnahmen treffen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind. Sofern Notfallkonzepte bei der betroffenen Stelle vorhanden sind, ist auf diese zurückzugreifen.

(2) Ein herausgehobener Fall nach Abs. 1 liegt insbesondere dann vor, wenn es sich um einen Angriff von besonderer technischer Qualität handelt oder die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems von besonderem öffentlichen Interesse ist.

(3) Das Zentrum für Informationssicherheit darf bei Maßnahmen nach Abs. 1 personenbezogene oder dem Fernmeldegeheimnis unterliegende Daten verarbeiten, soweit dies zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich und angemessen ist. Die Daten sind unverzüglich zu löschen, sobald sie für die Wiederherstellung der Sicherheit oder Funktionsfähigkeit des informationstechnischen Systems nicht mehr benötigt werden. Wenn die Daten nach Abs. 4 an eine andere Behörde zur Erfüllung von deren gesetzlichen Aufgaben übermittelt worden sind, darf das Zentrum für Informationssicherheit die Daten abweichend von Satz 2 bis zur Beendigung der Unterstützung dieser Behörde weiterverarbeiten. Eine Nutzung zu anderen Zwecken ist unzulässig. § 11 Abs. 4 ist entsprechend anzuwenden. Im Übrigen sind die Regelungen der Datenschutz-Grundverordnung und des Hessischen Datenschutz- und Informationsfreiheitsgesetzes anzuwenden.

(4) Das Zentrum für Informationssicherheit darf Informationen, von denen es im Rahmen dieser Vorschrift Kenntnis erlangt, nur mit Einwilligung der ersuchenden Stelle nach Abs. 1 übermitteln, es sei denn, die Informationen lassen keine Rückschlüsse auf die Identität des Ersuchenden zu oder die Informationen können nach § 13 übermittelt werden. Zugang zu den in Verfahren nach Abs. 1 geführten Akten wird Dritten nicht gewährt.

(5) Das Zentrum für Informationssicherheit kann sich bei Maßnahmen nach Abs. 1 mit der Einwilligung der ersuchenden Stelle nach Abs. 1 der Hilfe Dritter bedienen, wenn dies zur rechtzeitigen oder vollständigen Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich ist. Die hierdurch entstehenden Kosten hat die ersuchende Stelle zu tragen. Das Zentrum für Informationssicherheit kann die ersuchende Stelle auch auf Dritte verweisen. Das Zentrum für Informationssicherheit und von der ersuchenden Stelle oder vom Zentrum für Informationssicherheit nach Satz 1 beauftragte Dritte können einander bei Maßnahmen nach Abs. 1 mit der Einwilligung der ersuchenden Stelle Daten übermitteln. Hierfür gilt Abs. 3 entsprechend.

(6) Soweit es zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des informationstechnischen Systems erforderlich ist, kann das Zentrum für Informationssicherheit vom Hersteller des informationstechnischen Systems verlangen, an der Wiederherstellung der Sicherheit oder Funktionsfähigkeit mitzuwirken.

(7) In begründeten Einzelfällen kann das Zentrum für Informationssicherheit auch bei nicht in § 1 genannten Einrichtungen tätig werden, wenn es darum ersucht wurde und es sich um einen herausgehobenen Fall im Sinne des Abs. 2 handelt und soweit Rechtsvorschriften dem nicht entgegenstehen.

VIERTER TEIL
Informations- und Dokumentationspflichten

§ 17
Information der Betroffenen

Die von Maßnahmen nach § 10 Abs. 2 oder § 11 Abs. 3 Betroffenen sind spätestens nach dem Erkennen und der Abwehr eines Schadprogramms oder von Gefahren, die von einem Schadprogramm ausgehen, zu informieren, wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßigen Aufwand möglich ist und wenn das Interesse des Verantwortlichen der Datenverarbeitung an der Nichterteilung der Information das Informationsinteresse der oder des Betroffenen

nicht überwiegt. Die Information kann unterbleiben, wenn hierdurch der Ermittlungszweck eines Straf- oder Disziplinarverfahrens oder die Tätigkeit der Verfassungsschutzbehörden gefährdet würde. Im Falle einer Übermittlung der Daten nach § 13 Abs. 2 erfolgt die Information durch die dort genannten Behörden in entsprechender Anwendung der für diese Behörden geltenden Vorschriften. Enthalten diese keine Bestimmungen zu Informationspflichten, sind die Vorschriften der Strafprozessordnung entsprechend anzuwenden.

§ 18
Meldepflichten

(1) Werden den Stellen nach § 1 Nr. 1 und 2 Informationen bekannt, die zur Abwehr von Gefahren für die Informationssicherheit von Bedeutung sind, unterrichten diese das Zentrum für Informationssicherheit unverzüglich hierüber, soweit andere Vorschriften oder Vereinbarungen mit Dritten nicht entgegenstehen.

(2) Die Pflicht gilt nicht für den Hessischen Landtag, den Hessischen Rechnungshof, den Hessischen Beauftragten für Datenschutz und Informationsfreiheit, die Gerichte und Staatsanwaltschaften sowie die Hochschulen nach § 2 des Hessischen Hochschulgesetzes.

§ 19
Dokumentationspflichten

Anordnungen nach § 10 Abs. 2 Satz 2, § 11 Abs. 2 Satz 4 und § 11 Abs. 3 Satz 2 sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der nachträglichen Überprüfung der Rechtmäßigkeit der Verarbeitung der Daten verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch zum Ablauf des Kalenderjahres, das dem Jahr der Dokumentation folgt.

FÜNFTER TEIL
Schlussvorschriften

§ 20
Einschränkung von Grundrechten

Das Fernmeldegeheimnis nach Art. 10 des Grundgesetzes für die Bundesrepublik Deutschland, Art. 12 der Verfassung des Landes Hessen und das Recht auf informationelle Selbstbestimmung nach Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 des Grundgesetzes für die Bundesrepublik Deutschland, Art. 12a der Verfassung des Landes Hessen werden durch die §§ 7 bis 11, 13 und 16 eingeschränkt.

§ 21
Inkrafttreten, Außerkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft. Es tritt mit Ablauf des 31. Dezember 2030 außer Kraft.

Begründung

A. Allgemeiner Teil

1. Zweck und Inhalt des Gesetzes

Die Nutzung informationstechnischer Systeme und des Internets mit seinen vielfältigen Angeboten durchdringen Staat, Wirtschaft und Gesellschaft in immer größerem Maße. Auch und gerade die Handlungsfähigkeit der öffentlichen Verwaltung aller Ebenen hängt wesentlich von Informations- und Kommunikationstechnologien (IKT) ab.

Umso wichtiger ist es, dass sich alle auf eine jederzeit sichere IKT verlassen können, die stabil funktioniert und Cyberangriffen standhält. Informationssicherheit und Datenschutz sind elementare Voraussetzungen für die weitere erfolgreiche Digitalisierung der Verwaltung. Nur wenn Unternehmen und Bürger darauf vertrauen, dass ihre Daten sicher sind, werden neue digitale Prozesse angenommen und genutzt.

Die zuständigen staatlichen Stellen beschäftigen sich regelmäßig mit Angriffen gegen IT-Infrastrukturen. Die Medien berichten immer wieder über Cyber-Kriminalität, gestohlene Passwörter und Kundendaten, Angriffe auf IT-Infrastrukturen, Beeinflussung politischer Wahlen durch Cyber-Spionage und Social Bots sowie über massive Eingriffe in die Privatsphäre, zum Beispiel in und durch soziale Netzwerke.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat zuletzt mit dem am 21. Oktober 2021 vorgestellten Bericht zur Lage der IT-Sicherheit in Deutschland, die Ursachen von Cyber-Angriffen sowie die verwendeten Angriffsmittel und -methoden beschrieben und analysiert[1]. Demnach bieten die zunehmende Digitalisierung und Vernetzung den Cyber-Angreifern immer neue Angriffsflächen und weitreichende Möglichkeiten, Informationen auszuspähen, Geschäfts- und Verwaltungsprozesse zu sabotieren oder sich anderweitig auf Kosten Dritter kriminell zu bereichern. Hierbei ist nicht nur ein rasanter Anstieg neuer Schadsoftwarevarianten zu verzeichnen, auch die Qualität der Angriffe nimmt beträchtlich zu. Folgerichtig stuft das BSI die IT-Sicherheitslage erstmalig als angespannt bis kritisch ein. In der im Jahr 2021 vorgestellten nationalen Cyber-Sicherheitsstrategie für Deutschland[2] stellt die Bundesregierung fest, dass die Gewährleistung einer angemessenen Cybersicherheit eine gesamtstaatliche Aufgabe ist, die nur gelingen kann, wenn Bund, Länder und Kommunen eng zusammenarbeiten.

Der Bund (u. a. mit dem personellen Ausbau des BSI) und andere Länder (z. B. Bayern mit dem Landesamt für Sicherheit in der Informationstechnik) haben entsprechende Instanzen aufgebaut.

Hessen steht daher vor großen Herausforderungen. Zum Schutz der Informations- und Kommunikationstechnologie in Hessen sind die erforderlichen Kompetenzen und die Technik für den Betrieb einer Kompetenzstelle für Cybersicherheit auf- bzw. auszubauen und dauerhaft zu installieren. Der Markt in Bezug auf die erforderlichen Fachkräfte ist sehr stark umkämpft durch immense Bedarfe in Bund, Ländern und der Wirtschaft. Die erforderliche Technik ist komplex und teuer. Kooperationen mit dem Bund und den anderen Ländern zur Gewährleistung der Cybersicherheit sind unumgänglich, es müssen entsprechende Fähigkeiten und Services aufgebaut werden, damit Hessen als kompetenter Partner auf Augenhöhe seinen Beitrag hierfür leisten kann.

Um diesen Herausforderungen mit einer effizienten Lösung begegnen zu können, soll ein Zentrum für Informationssicherheit aufgebaut werden. Hier werden neue Fähigkeiten zum Schutz der eigenen IKT und starke Cyber-Expertisen aus- und aufgebaut. Für den Schutz der eigenen IT, aber auch für eine Unterstützung und Beratung anderer öffentlicher Stellen, werden entsprechende Services bereitgestellt sowie Strukturen geschaffen, die es jederzeit ermöglichen, angemessen den vielschichtigen Bedrohungen im Cyberraum zu begegnen. Die Vernetzung mit der einschlägigen Forschung, eine zielgerichtete Vergabe von Forschungsanliegen und entsprechend abrufbares Wissen zu "dem Stand der Technik" sollen dabei sicherstellen, dass die eigenen Cyberkompetenzen jederzeit aktuell bleiben. Die erforderlichen technischen Voraussetzungen werden durch Auf- und Ausbau des Zentrums für Informationssicherheit unter Einbeziehung des bereits bestehenden Sicherheits- und Computer-Notfallteams (Computer Emergency Response Team, CERT) sichergestellt.

Mit diesem Gesetz sollen auch die rechtlichen Grundlagen für eine umfängliche Absicherung der Aufgaben und Befugnisse des Zentrums für Informationssicherheit geschaffen werden. Damit werden einer Zentralstelle Befugnisse eingeräumt, zur Erhöhung der IT-Sicherheit in der Landesverwaltung und zur Abwehr von Gefahren für die Informationstechnik des Landes eigenständig, ohne Amtshilfeersuchen anderer öffentlicher Stellen, operativ tätig zu werden. Der Aufgabenbereich des Zentrums für Informationssicherheit reicht von der Prävention durch Lagebeobachtung, Sammlung und Auswertung von Informationen zu Sicherheitsrisiken, Schwachstellen und

[1] Die Lage der IT-Sicherheit in Deutschland 2021, Bundesamt für Sicherheit in der Informationstechnik (BSI), Stand September 2021, ➔ www.bsi.bund.de, BSI-LB21/510.

[2] Cybersicherheitsstrategie für Deutschland 2021, Bundesministerium des Innern und für Heimat (BMI), Stand August 2021, ➔ www.bmi.bund.de.

Schadprogrammen, über Informationen, Warnungen und Empfehlungen an Behörden und auch an die Öffentlichkeit bis hin zur aktiven Abwehr von konkreten Gefahren.

Für die aufgelisteten Aufgaben sind Rechtsgrundlagen erforderlich. Insbesondere der Schutz des hessischen Behördennetzes bedarf einer umfangreichen Analyse des Datenverkehrs an den Übergängen zum Internet. Anders kann eine hinreichende Sicherheit des Netzes nicht erreicht werden. Allerdings unterliegt eine entsprechende Regelung wegen der mit ihr verbundenen möglichen Grundrechtseingriffe strengen Anforderungen. Die zuständigen Stellen sind hierbei auf Rechtssicherheit beim Einsatz von aktuellen Sicherheitslösungen angewiesen. Die kontinuierliche Auswertung der Protokolldaten und des Datenverkehrs im Landesnetz kann eine Beeinträchtigung des informationellen Selbstbestimmungsrechts der Beschäftigten und der mit der Landesverwaltung kommunizierenden Dritten sowie einen Eingriff in das Fernmeldegeheimnis darstellen. Andererseits stärkt diese Maßnahme den Schutz vor Angriffen auf die IT-Systeme. Dies wiederum dient auch dem Schutz der Nutzer dieser Systeme vor einer Verletzung ihrer Grundrechte durch unbefugte Zugriffe und Missbrauch ihrer Daten. Es geht bei den hier zu schaffenden Rechtsgrundlagen also letztlich um die Abwägung, ob der Eingriff durch die vorgesehenen Maßnahmen in Anbetracht der Risiken für eine Verletzung der Rechte der Betroffenen durch Angriffe auf die IT-Systeme als verhältnismäßig zu bewerten ist. Dies wird aufgrund des vorgesehenen abgestuften Verfahrens gewährleistet, das zunächst eine automatisierte, rein technische Auswertung der anfallenden Daten vorsieht, der sich nur im Falle hinreichender tatsächlicher Anhaltspunkte für eine Gefahrenlage eine manuelle Prüfung anschließen kann. Darüber hinaus bleiben die zusätzlichen datenschutzrechtlichen Anforderungen, insb. aus der DS-GVO und dem HDSIG, unberührt.

Die vorgesehene Zusammenarbeit des Zentrums für Informationssicherheit mit den für die Informationssicherheit zuständigen Stellen von Bund und Ländern (z. B. IT-Planungsrat, eGOV-VR, CISO, AK Informationssicherheit), die Möglichkeit der Unterstützung von Kommunen und sonstigen öffentlichen Stellen bis hin zu privaten Unternehmen, schließt den Kreis der vom Bund angestrebten Bündelung der Kräfte und Vernetzung über Bundes- und Landesgrenzen hinweg zur Erreichung eines möglichst hohen Sicherheitsniveaus von Netz- und Informationssystemen und damit zu mehr Cyber-Sicherheit von der „kleinsten“ bis zur „größten“ europäischen Einheit – von den Kleinunternehmen bis zur Europäischen Union.

Die Einrichtung eines Zentrums für Informationssicherheit entbindet die einzelnen Stellen der öffentlichen Verwaltung in Hessen nicht von ihrer Pflicht, selbständig für eine angemessene Sicherheit bei dem Betrieb ihrer informationstechnischen Systeme zu sorgen. Insbesondere ist die Informationssicherheitsleitlinie für die hessische Landesverwaltung in der jeweils geltenden Fassung in der gesamten hessischen Landesverwaltung zu beachten. Das Zentrum für Informationssicherheit soll die Landesbehörden bei den aus dieser Leitlinie folgenden Aufgaben und Pflichten im Bereich der Prävention und Gefahrenabwehr durch Aufbau und Einsatz entsprechender Expertisen unterstützen. Dafür ist es maßgeblich auf eine vertrauensvolle Zusammenarbeit und insbesondere auch auf die Erfüllung der Informationspflichten der Informationssicherheitsleitlinie angewiesen. Die Regelungen der Informationssicherheitsleitlinie ergänzen dementsprechend die Regelungen dieses Gesetzes.

Neben dem Zentrum für Informationssicherheit (mit CERT) wird auch die Position der Zentralen oder des Zentralen Informationssicherheitsbeauftragten für die hessische Landesverwaltung (Chief Information Security Officer, CISO) gesetzlich verankert, deren oder dessen Aufgaben und Befugnisse dem Grunde nach in der Informationssicherheitsleitlinie für die hessische Landesverwaltung (2021), veröffentlicht im StAnz. 47/2021 S. 1517, beschrieben werden. Gesetzlich geregelt werden hier insbesondere die ressortübergreifenden Befugnisse bei Gefahren für die Informationssicherheit der Landesverwaltung, entsprechende Berichtspflichten sowie die koordinierende Funktion im IT-Krisenmanagement der Landesverwaltung.

2. Finanzielle Auswirkungen

a) für die Verwaltung des Landes Hessen

Die neu zu schaffenden Befugnisse des Zentrums für Informationssicherheit sind mit einem entsprechenden Umsetzungsaufwand verbunden. Dessen Umfang und damit die Höhe der Vollzugskosten sind maßgeblich von der zukünftigen Entwicklung der IT-Sicherheitslage abhängig und daher nicht exakt zu beziffern.

Einen Teil der zukünftig anfallenden administrativen Aufgaben erfüllt das Zentrum für Informationssicherheit bereits heute durch das Hessen CyberCompetenceCenter (Hessen3C). Die neuen Dienste (Ausbau von Sensorik und Log-Auswertung, Forensik sowie Mobile Incident Response Teams für die hessischen Kommunen) führen zur Erhöhung des Umsetzungsaufwands.

Die neuen oder zukünftig aufgrund dieses Gesetzes in größerem Umfang wahrzunehmenden Aufgaben erfordern beim Zentrum für Informationssicherheit ab dem Jahr 2023 einmalige Sachkosten in Höhe von 3,3 Millionen Euro sowie laufende Personal- und Sachkosten in Höhe von ca. einer Million Euro jährlich.

Sie resultieren insbesondere aus den neu geschaffenen Aufgaben nach § 5 Abs. 2 Satz 1 Nr. 2 und 3 (Abwehr von Gefahren für die Sicherheit in der Informationstechnik), nach § 5 Abs. 2 Satz 1 Nr. 4 i. V. m. § 16 (Unterstützung bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen) nach § 5 Abs. 2 Satz 1 Nr. 5 (technische Unterstützung der Sicherheitsbehörden und der oder des HBDI), sowie der Entwicklung von Verfahren und Werkzeugen zur Erkennung und Abwehr von Gefahren für die Sicherheit in der Informationstechnik (§ 5 Abs. 2 Satz 1 Nr. 11). Die Mittel stehen hierfür bereits zur Verfügung. Zusätzliche Kosten sind nicht zu erwarten.

Weiterer Umsetzungsaufwand für die Landesverwaltung ist nicht ersichtlich, da keine weiteren kostenrelevanten, über die Verpflichtungen zur Informationssicherheit in der Informationssicherheitsleitlinie des Landes hinausgehenden Regelungen getroffen werden.

b) für hessische Gemeinden und Gemeindeverbände

Das Gesetz statuiert für hessische Gemeinden und Gemeindeverbände keine Verpflichtungen, die über die bereits bestehenden Verpflichtungen zur IT-Sicherheit hinausgehen.

c) für die Wirtschaft

Das Gesetz statuiert für Wirtschaftsunternehmen keine Verpflichtungen, so dass hier keine besonderen finanziellen Auswirkungen veranlasst durch dieses Gesetz zu erwarten sind.

d) für Bürgerinnen und Bürger

Das Gesetz statuiert für Bürgerinnen und Bürger keine Verpflichtungen, so dass hier keine besonderen finanziellen Auswirkungen veranlasst durch dieses Gesetz zu erwarten sind.

B. Besonderer Teil

Zu § 1 (Geltungsbereich)

§ 1 regelt den Geltungsbereich dieses Gesetzes. Das Gesetz gilt für Behörden und sonstige öffentliche Stellen des Landes und der Kommunen sowie der sonstigen der Aufsicht des Landes unterliegenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts und deren Vereinigungen ungeachtet ihrer Rechtsform. Das Gesetz gilt ebenso für Beliehene dieser Stellen. Damit soll sichergestellt werden, dass die zur Gewährleistung der IT-Sicherheit unumgänglich erforderlichen Befugnisse der §§ 8 bis 11 für alle Stellen im Land Hessen genutzt werden können.

Zu § 2 (Begriffsbestimmungen)

Diese Vorschrift dient zur Klarstellung solcher Rechtsbegriffe, die für das Verständnis und die Anwendung dieses Gesetzes von Bedeutung sind.

Sie lehnen sich an die Definitionen im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) in der Fassung der Bekanntmachung vom 14. August 2009 (BGBl. I S. 2821), zuletzt geändert durch Gesetz vom 23. Juni 2021 (BGBl. I S. 1982), an.

Zu Nr. 1

Die Definition der Informationstechnik ist bewusst allgemein gefasst, um alle technischen Ausgestaltungen und denkbaren künftigen Entwicklungen auf dem Gebiet der Informationstechnik abzudecken. Unter „technische Mittel" sind alle heutigen und zukünftigen Arten von Hard- und Software- oder Cloudlösungen zu verstehen. Der Begriff „Verarbeitung" schließt alle Vorgänge wie Erfassung, Darstellung, Speicherung oder Übermittlung ein. Eine Bekanntgabe von Informationen an Dritte ist dabei nicht erforderlich. Erfasst werden alle Arten von Informationen, ein Personenbezug ist dabei nicht erforderlich.

Zu Nr. 2

Mit Informationssicherheit ist kein absoluter, sondern lediglich ein relativer Sicherheitsbegriff vorgegeben. Welche Sicherheit im Einzelfall erreicht sein muss, hängt von den jeweiligen Sicherheitserfordernissen ab. Daher ist in der Definition von der „Einhaltung bestimmter Sicherheitsstandards" die Rede. Die „Verfügbarkeit von Informationen" erfordert Sicherheitsvorkehrungen, um die Informationen in der vorgesehenen Weise verarbeiten oder übertragen und damit nutzen zu können. Die „Integrität von Informationen" erfordert Sicherheitsvorkehrungen, um deren Inhalt und Form vor unzulässigem Verändern zu schützen. Die „Vertraulichkeit von Informationen" erfordert Sicherheitsvorkehrungen, um einen unbefugten Informationsgewinn über die Informationstechnik und einen ungewollten Abfluss der mit ihr verarbeiteten oder übertragenen Informationen zu verhindern. Die Sicherheit umfasst sowohl den technischen Sicherheitsstandard (z. B. automatische Verschlüsselung gespeicherter oder zu übertragender Informationen) als auch – ergänzend oder alternativ – Sicherheitsvorkehrungen bei Anwendung der Informationstechnik (z. B. baulicher oder organisatorischer Art). Es ist Aufgabe des jeweiligen Anwenders, die Sicherheitstechnik durch erforderliche Umfeldmaßnahmen zu ergänzen.

Zu Nr. 3 und 4

Gefahren für die Informationssicherheit gehen insbesondere von Schadprogrammen sowie von Sicherheitslücken in informationstechnischen Systemen aus, die in den Nr. 3 und 4 legaldefiniert werden. Die Definition von Schadprogrammen in Nr. 3 entspricht im Wesentlichen der in der Informationstechnik üblichen Terminologie. Maßgeblich ist, dass die Programme dem Zweck dienen, unbefugt unerwünschte Funktionen auszuführen. Nicht erfasst sind damit unbeabsichtigte Sicherheitslücken in normalen Programmen. Schadprogramme können typischerweise Schäden verursachen, dies ist aber keine zwingende Voraussetzung. Moderne Schadprogramme zeichnen sich gerade dadurch aus, dass sie möglichst unauffällig und klein sind. Schadfunktionen sind zunächst nicht enthalten, können aber ggf. nachgeladen werden. Auch der Versand von Spam, also die massenhafte Versendung unerwünschter E-Mails, oder sogenannte DDoS-Angriffe (Distributed Denial of Service; Massenanfragen, um Server durch Überlastung lahmzulegen) sind informationstechnische Routinen, die geeignet sind, unbefugt informationstechnische Prozesse zu beeinflussen. Sicherheitslücken sind hingegen unerwünschte Eigenschaften von informationstechnischen Systemen, insbesondere Computerprogrammen, die es Dritten erlauben, gegen den Willen der Berechtigten deren Informationstechnik zu beeinflussen. Eine Beeinflussung muss nicht zwingend darin bestehen, dass sich der Dritte Zugang zum System verschafft und dieses dann manipulieren kann. Es genügt auch, dass die Funktionsweise in sonstiger Weise beeinträchtigt werden kann, z. B. durch ein ungewolltes Abschalten. Der Begriff ist notwendigerweise weit gefasst, da Sicherheitslücken in den unterschiedlichsten Zusammenhängen, oftmals abhängig von der Konfiguration oder Einsatzumgebung, entstehen können.

Zu Nr. 5

Mit den Begriffen „Übergabe- und Knotenpunkte“ sind die Übergänge beschrieben, an denen aus Gründen der IT-Sicherheit eine Auswertung von Daten notwendig ist bzw. sein kann. Davon erfasst sind Übergänge zwischen den IT-Systemen der Landesverwaltung inklusive der Übergänge zwischen virtuellen Netzen sowie zwischen einzelnen internen Behördennetzen oder den Netzen einer Gruppe von Behörden (Knotenpunkte) einerseits und zum Internet und anderen nicht der Landesverwaltung zuzurechnenden Netzen (Übergabepunkte) andererseits.

Zu Nr. 6

Protokolldaten sind historische Aufzeichnungen über die Art und Weise, wie IT-Systeme genutzt wurden und wie diese miteinander kommuniziert haben. Hieraus ergeben sich wesentliche Rückschlüsse für die Erkennung und Abwehr von Angriffen auf die Informationstechnik. Besonders bedeutsam sind in diesem Zusammenhang die Kopfdaten der gängigen Kommunikationsprotokolle. Kommunikationsinhalte sind nicht Bestandteil der Protokolldaten.

Zu § 3 (Grundsätze der Informationssicherheit)

Zu Abs. 1 - 3

Die Verantwortung für eine angemessene Informationssicherheit trägt die jeweilige Stelle innerhalb ihres Zuständigkeitsbereichs selbst. Hierbei sind für die Stellen nach § 1 Nr. 1 und 2 die Standards des Bundesamts für die Sicherheit in der Informationstechnik (BSI) zu berücksichtigen bzw. für die übrigen Stellen empfohlen. Die bindenden Beschlüsse des IT-Planungsrates sind einzuhalten.

Für die hessische Landesverwaltung werden zur Unterstützung der jeweiligen Leitung Informationssicherheitsbeauftragte sowohl für jede Dienststelle als auch für jedes Ressort benannt. Aufgaben und Befugnisse der Beauftragten regelt die Informationssicherheitsleitlinie für die hessische Landesverwaltung.

Zu Abs. 4

Die jeweiligen Informationssicherheitsbeauftragten sind bei wesentlichen Änderungen an informationstechnischen Systemen zu beteiligen.

Zu Abs. 5

Den in Abs. 5 genannten Stellen wird zur Erreichung und Aufrechterhaltung eines angemessenen Informationssicherheitsniveaus empfohlen, diese Grundsätze anzuwenden und einzuhalten.

Zu § 4 (Die oder der Zentrale Informationssicherheitsbeauftragte der Landesverwaltung)

Zu Abs. 1

Mit der Regelung wird eine Zentrale Informationssicherheitsbeauftragte oder ein Zentraler Informationssicherheitsbeauftragter (Chief Information Security Officer, CISO) in der Landesverwaltung gesetzlich verankert. Die Vorschrift ist notwendig, um das informationstechnische Sicherheitsniveau in der Landesverwaltung zu stärken und permanent zu kontrollieren. Dieser gesetzliche Auftrag ist an die Ministerin oder den Minister adressiert, die bzw. der nach Beschluss über

die Zuständigkeit der einzelnen Ministerinnen und Minister nach Art. 104 Abs. 2 der Verfassung des Landes Hessen vom 4. April 2019 (GVBl. S. 56) für IT- und Cybersicherheit in der Landesverwaltung zuständig ist. Damit wird die gebotene Sachnähe sichergestellt.

Die Sätze 2 und 3 beschreiben den funktionellen Status der beauftragten Person innerhalb der Landesverwaltung. Sie ist ressortübergreifend zuständig für die Einhaltung der Informationssicherheit und besitzt ein diesbezügliches Informationsrecht. In Erfüllung ihrer in Abs. 2 aufgeführten Aufgaben kann die beauftragte Person über die Ressort-ISB alle die Informationssicherheit betreffenden Unterlagen einsehen sowie von Dienststellen der Landesverwaltung Auskünfte und erbetene Unterlagen anfordern. Die Dienststellen der Landesverwaltung sind vorbehaltlich entgegenstehender Rechtsvorschriften verpflichtet, die beauftragte Person in der Wahrnehmung ihres Auftrags umfassend zu unterstützen. Unterstützung in diesem Sinne bedeutet, dass ihr die Dienststellen der Landesverwaltung Zugang zu ihren Einrichtungen, Anlagen und sonstigen Gegenständen ermöglichen.

Zu Abs. 2 und 3

Die Abs. 2 und 3 benennen nicht abschließend die Aufgaben und Befugnisse der oder des CISO. Die in Nr. 7.12 der weiterhin ergänzend anwendbaren Informationssicherheitsleitlinie für die hessische Landesverwaltung beschriebenen wesentlichen Aufgaben und Kompetenzen der oder des CISO werden damit gesetzlich normiert.

Insbesondere die ressortübergreifenden erheblichen Befugnisse der beauftragten Person bei Gefahr im Verzug für die Sicherheit in der Informationstechnik der Landesverwaltung einschließlich entsprechender Berichtspflichten gegenüber der Landesregierung sollen einer gesetzlichen Regelung zugeführt werden.

Nach Abs. 2 obliegt der beauftragten Person die Fortschreibung der Informationssicherheitsleitlinie des Landes (Nr. 1).

Die beauftragte Person soll insbesondere den Beauftragten oder die Beauftragte der Landesregierung für E-Government (CIO), sowie die Staatskanzlei und die Ministerien beraten und Empfehlungen in Fragen der Informationssicherheit entwickeln (Nr. 2) sowie das Zentrum für Informationssicherheit in den Fällen der Gefahrenabwehr nach § 5 Abs. 2 Satz 1 Nr. 2 steuern (Nr. 3).

Neben der regelmäßigen Berichterstattung über den Sachstand der Informationssicherheit in der Landesverwaltung ist die Landesregierung über jede Maßnahme nach Abs. 2 Nr. 3 zu informieren (Nr. 4).

In Fällen ressortübergreifender Cybersicherheitslagen koordiniert die beauftragte Person das IT-Krisenmanagement der Landesverwaltung. Die nähere Ausgestaltung ist durch die Informationssicherheitsleitlinie für die hessische Landesverwaltung zu regeln (Nr. 5).

Abs. 3 regelt die zur Erfüllung der Aufgaben notwendigen Befugnisse bei unmittelbaren und erheblichen Gefahren. Die beauftragte Person kann bei dringenden dienststellenübergreifenden informationstechnischen Sicherheitsvorfällen – korrespondierend zur Aufgabe nach Abs. 2 Nr. 3 und zur Aufgabe der Zentralstelle für Informationssicherheit nach § 5 Abs. 2 Satz 1 Nr. 2 – Maßnahmen zur Gefahrenabwehr anordnen (bspw. die Datenverbindung zum Landesdatennetz trennen oder ein IT-Verfahren abschalten lassen). Im Rahmen der Abwägung der zu treffenden Maßnahmen, sind insbesondere ressortspezifische Auswirkungen zu berücksichtigen. Dies wird durch die Einbeziehung des betreffenden Ressorts sichergestellt.

Zu Abs. 4

Abs. 4 räumt der oder dem CISO ein Vortragsrecht bei der für IT- und Cybersicherheit zuständigen Ministerin oder dem hierfür zuständigen Minister sowie bei der Beauftragten oder dem Beauftragten der Landesregierung für E-Government (CIO) ein. Darüber hinaus besteht ein solches Vortragsrecht bei den Staatssekretärinnen und Staatssekretären der Ministerien und der Chefin oder dem Chef der Staatskanzlei, soweit schwerwiegende Anlässe dies erfordern. Gemeint sind damit besonders hervorgehobene Defizite in der Informationssicherheit des betreffenden Bereichs. Hierdurch soll sichergestellt werden, dass wichtige Belange der Cybersicherheit in der Landesverwaltung ohne Verzögerung auf entscheidungsbefugter politischer Ebene kommuniziert werden können.

Zu § 5 (Zentrum für Informationssicherheit)

Diese Regelung enthält die rechtliche Grundlage zur Einrichtung eines Zentrums für Informationssicherheit zur Förderung der Informationssicherheit der gesamten Verwaltung in Hessen. Aufgrund der aktuellen und auch in Zukunft aller Voraussicht nach nicht schwächer werdenden Bedrohungslage im „Cyberraum“ ist der Aufbau einer schlagkräftigen Präventions- und Gefahrenabwehrorganisation für die IT-Sicherheit in Hessen unumgänglich.

Zu Abs. 1

Abs. 1 Satz 1 regelt, dass das Zentrum für Informationssicherheit im Zuständigkeitsbereich der für IT- und Cybersicherheit in der Landesverwaltung zuständigen Ministerin oder des hierfür zuständigen Ministers eingerichtet wird. Dieser gesetzliche Auftrag ist an die Ministerin oder den Minister adressiert, die bzw. der nach Beschluss über die Zuständigkeit der einzelnen Ministerinnen und Minister nach Art. 104 Abs. 2 der Verfassung des Landes Hessen vom 4. April 2019 (GVBl. S. 56) für IT- und Cybersicherheit in der Landesverwaltung zuständig ist. Damit wird die gebotene Sachnähe sichergestellt.

Zu Abs. 2

In Abs. 2 werden die konkreten Aufgaben des Zentrums für Informationssicherheit zur Erfüllung des in Abs. 1 beschriebenen Auftrags – die Förderung der Informationssicherheit der gesamten Verwaltung in Hessen – aufgezählt.

Zu Nr. 1

Das Zentrum für Informationssicherheit soll mit den für die Informationssicherheit zuständigen zentralen Stellen in Bund, Ländern und Kommunen zusammenarbeiten, denn die Bedrohungen im Cyberraum machen vor keiner Grenze halt und sind für alle für die Sicherheit in der Informationstechnik zuständigen Stellen gleich.

Zu Nr. 2

Diese Aufgabe (Erkennung, Untersuchung und Abwehr von Gefahren für die Informationssicherheit) bildet die Grundlage für die in den §§ 7 bis 11 beschriebenen Befugnisse, von denen das Zentrum für Informationssicherheit gemäß § 12 Abs. 1 zentral für alle Stellen nach § 1 Nr. 1 und 2 zum Schutz der Informationstechnik der Landesverwaltung Gebrauch macht. Abwehr ist dabei im Sinne einer passiven Cyberabwehr zu verstehen.

Zu Nr. 3

Stellen nach § 1 Nr. 3 können das Zentrum für Informationssicherheit um Unterstützung bitten bei der Erkennung, Untersuchung und Abwehr von Gefahren für ihre IT-Systeme.

Unter „zuständige Stellen" sind die für die Informationssicherheit zuständigen Verwaltungsstellen bei den Stellen nach § 1 Nr. 3 zu verstehen. Art und Umfang der Unterstützung richten sich nach dem jeweiligen Bedarf.

Zu Nr. 4

Diese Aufgabe korrespondiert mit den Befugnissen nach § 16 dieses Gesetzes. Es werden Maßnahmen, die von Mobilen Einsatzgruppen, sogenannten Mobile Incident Response Teams (MIRTs) durchgeführt werden, in den Aufgabenkatalog des Zentrums für Informationssicherheit aufgenommen. Mit den MIRTs soll das Zentrum für Informationssicherheit durch das Sicherheits- und Computer-Notfallteam (Computer Emergency Response Team, CERT), dem die MIRTs zugeordnet werden, andere Stellen bei der Wiederherstellung ihrer IT-Systeme bei Cyber-Angriffen unterstützen.

Zu Nr. 5

Das Zentrum für Informationssicherheit unterstützt und berät Polizei- und Strafverfolgungsbehörden sowie das Landesamt für Verfassungsschutz auf deren Ersuchen, beispielsweise bei der Durchführung von technischen Untersuchungen oder Datenverarbeitung. Die Unterstützung soll dabei helfen, allgemein kriminell oder extremistisch motivierte Angriffe auf oder Einbrüche in informationstechnische Systeme möglichst frühzeitig zu erkennen, ihre Auswirkungen zu bewerten und Möglichkeiten der analytischen Untersuchung oder der sächlichen Beweisführung im Rahmen der Strafverfolgung aufzuzeigen. Eine technische Unterstützung kommt insbesondere bei großen Verfahren mit umfangreichen technischen Beweismitteln in Betracht, bspw. im Bereich der Erkennung von kinderpornographischen Schriften. Das Zentrum für Informationssicherheit unterstützt und berät insbesondere auch bezüglich der Verwendung von Produkten, hinsichtlich fachspezifischer Aus- und Weiterbildung sowie durch die Bereitstellung einer Wissensplattform.

Der HBDI ist aufgrund der ihm übertragenen Aufgaben und Befugnisse (vgl. Art. 57, 58 DS-GVO, §§ 13 und 14 HDSIG) als Aufsichtsbehörde selbst an der Aufklärung von IT-Sicherheitsvorfällen beteiligt, etwa im Zusammenhang mit Meldungen von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO. Zur Sachverhaltsaufklärung gehören auch technische Datenschutzprüfungen, wobei der HBDI durch das Zentrum für Informationssicherheit unterstützt werden kann.

Nach § 5 Abs. 2 Satz 2 sind solche Ersuchen in den Akten zu vermerken.

Zu Nr. 6

Die Einschätzung der IT-Sicherheitslage durch das Zentrum für Informationssicherheit als Expertenteam für Cybersicherheit ist unabdingbare Voraussetzung für Entscheidungen durch den Krisenstab der Landesregierung.

Zu Nr. 7 bis 10

Die Aufgaben nach den Nr. 7 bis 10 sind im Zusammenhang zu lesen und entsprechen im Wesentlichen den bislang durch das CERT wahrgenommenen Aufgaben. Die hieraus gewonnenen Erkenntnisse werden den Stellen nach § 1 zum Schutz ihrer IT-Infrastruktur zur Verfügung gestellt und tragen damit wesentlich zur Erhöhung des gesamtstaatlichen Informationssicherheitsniveaus bei, indem Schwachstellen erkannt und geschlossen werden können. Die Aufgaben gehören in den Bereich der Prävention. Befugnisse zum Eindringen in fremde IT-Systeme zur Beschaffung solcher Informationen werden hierdurch nicht verliehen.

Insbesondere die Aufgabe der Sammlung und Auswertung von Informationen über Risiken, Beeinträchtigungen, Störungen und Vorkehrungen wird maßgeblich durch die Befugnis zur Auswertung von Daten aus allgemein zugänglichen Quellen unterstützt.

Neben Fragen der Informationssicherheit soll das Zentrum für Informationssicherheit auch bei Tätigkeiten oder Ereignissen unter Nutzung der Informationstechnik eigenständig beratend, warnend oder empfehlend tätig werden, soweit die öffentliche Sicherheit oder Ordnung beeinträchtigt wird. Hiermit soll eine Möglichkeit geschaffen werden, auf neuartige Phänomene der Digitalisierung zu reagieren, wie dies beispielsweise bei den in sozialen Netzwerken verbreiteten sog. Hasskommentaren der Fall ist. Die öffentliche Ordnung ist in solchen Fällen unterhalb der Grenze zur strafrechtlichen Relevanz betroffen. Die originären Zuständigkeiten der Gefahrenabwehrbehörden werden davon nicht berührt.

Zu Nr. 11

Im Zentrum für Informationssicherheit sollen im Sinne einer umfassenden Prävention durch die dort an zentraler Stelle eingesetzten Experten Sicherheitsrisiken analysiert und Kriterien, Werkzeuge und Verfahren untersucht und auch selbst entwickelt werden, um Gefahren für die IT-Sicherheit besser erkennen und abwehren zu können. Hierbei ist eine enge Zusammenarbeit mit Wissenschaft und Forschung vorgesehen.

Zu Abs. 3

Das bereits heute eingesetzte CERT wird in das Zentrum für Informationssicherheit integriert, weiter ausgebaut und übernimmt in diesem Rahmen wesentliche Teile der Aufgaben des Zentrums für Informationssicherheit.

Das CERT bleibt auch weiterhin zentrale Kontaktstelle i. S. v. § 8b Abs. 2 Nr. 4 Buchst. c des BSI-Gesetzes.

Im CERT werden MIRTs aufgebaut, die entsprechend den Regelungen in § 16 die Stellen nach § 1 bei der Wiederherstellung ihrer IT-Systeme nach Cyberattacken unterstützen.

Das CERT wird weiter ausgebaut, so dass es seine Dienstleistungen nicht nur den Stellen nach § 1 des Gesetzes anbieten kann, sondern auch Dritten bis hin zu privaten Unternehmen.

Ein Anspruch auf die Dienstleistungen des CERT besteht aus Kapazitätsgründen nicht.

Zu § 6 (Zentraler IT-Dienstleister des Landes)

Die Hessische Zentrale für Datenverarbeitung (HZD) ist gem. § 1 Abs. 1 Satz 1 DV-VerbundG zentraler IT-Dienstleister für Informations- und Kommunikationstechnik für alle Behörden, Gerichte und sonstigen öffentlichen Stellen des Landes Hessen. Sie ist für den sicheren Betrieb für den Teil der IT-Infrastruktur der Landesverwaltung verantwortlich, den sie beeinflussen kann. Die Befugnisse des Zentrums für Informationssicherheit lassen diese Verantwortlichkeit unberührt.

Eine enge Kooperation und ein intensiver Informationsaustausch zwischen der HZD und dem Zentrum für Informationssicherheit ist unerlässlich. Die HZD berät das Zentrum bei dessen Aufgabenerledigung. Das Zentrum wiederum teilt seine Erkenntnisse im Zusammenhang mit der Informationssicherheit der Landesverwaltung unverzüglich mit der HZD.

Zu §§ 7 bis 17

In den §§ 7 ff. dieses Gesetzes werden die Befugnisse der Stellen, die für die Sicherheit der informationstechnischen Systeme der Verwaltung in Hessen gemäß § 12 zuständig sind, geregelt. Neben den Maßnahmen in §§ 7 bis 11 und 16 finden sich Regelungen zur Datenübermittlung (§ 13), zur Gewährleistung von Datensicherheit und Datenschutz (§§ 14 und 15) sowie zur Benachrichtigung der Betroffenen (§ 17).

Unabhängig von der gewählten Form der Datenverarbeitung findet eine Verarbeitung zu Zwecken der Verhaltens- oder Leistungskontrolle nicht statt.

Zu § 7 (Datenverarbeitung)

Zu Abs. 1 und 2

Abs. 1 und 2 sind dem § 3a BSI-Gesetz nachgebildet und geringfügig an die hessischen Verhältnisse angepasst. Mit Abs. 2 wird, auf Basis von Art. 6 Abs. 1 UA. 1 lit. e und Abs. 3 S. 1 lit. b der Datenschutz-Grundverordnung, eine klare Rechtgrundlage für das Zentrum für Informationssicherheit zur Verarbeitung von personenbezogenen Daten geschaffen. Das Zentrum fördert die Informationssicherheit nach § 5 Abs. 1 und nimmt zu diesem Zweck die in § 5 Abs. 2 aufgeführten Aufgaben wahr. Zur Erfüllung dieser im wichtigen öffentlichen Interesse liegenden Aufgaben ist das Zentrum auf datenschutzrechtliche Ermächtigungen zur Verarbeitung personenbezogener Daten angewiesen. Damit wird sichergestellt, dass das Zentrum seine gesetzlichen Aufgaben erfüllen kann, insbesondere auch informationssicherheitsrelevante Daten erhalten und analysieren zu können. Abs. 2 gilt nur für die Aufgaben und Tätigkeiten, die nicht unmittelbar durch die speziellen datenschutzrechtlichen Ermächtigungen (wie z. B. §§ 8 ff.) erfasst werden.

Durch Abs. 2 Satz 1 wird klargestellt, dass das Zentrum zur Wahrnehmung seiner Aufgaben personenbezogene Daten verarbeiten kann. Die Regelung trägt dem Erfordernis Rechnung, dass das Zentrum neben den bestehenden Möglichkeiten zur Weiterverarbeitung von Daten nach §§ 8 ff. für die Erfüllung seiner gesetzlichen Aufgaben eine datenschutzrechtliche Rechtsgrundlage benötigt, um personenbezogene Daten zum Zwecke der Sammlung, Auswertung und Untersuchung von Informationen über Sicherheitsrisiken oder Sicherheitsvorkehrungen für die Informationssicherheit und zur Unterstützung, Beratung und Warnung in Fragen der Informationssicherheit zu verarbeiten.

Abs. 2 Satz 2 stellt eine gemäß Art. 6 Abs. 4 Var. 2 der Datenschutz-Grundverordnung erforderliche Rechtsgrundlage für diese Weiterverarbeitungen dar. Das Zentrum muss in der Lage sein, zur Erfüllung seiner Aufgaben aus § 5 Abs. 2 alle ihm aus öffentlichen, privaten, staatlichen, bekannten oder anonymen Quellen erlangten und zur Verfügung gestellten Daten auszuwerten, um vor möglichen Sicherheitsrisiken für die Informationstechnik zu warnen und entsprechende Sicherheitsvorkehrungen, insbesondere zum Schutz der Landesverwaltung, zu entwerfen oder zu etablieren, um die nationale und öffentliche Sicherheit sowie den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses sicherzustellen. Hierzu ist allerdings auch eine Interessenabwägung erforderlich.

In Abs. 2 Satz 3 wird die Verarbeitung besonderer Kategorien personenbezogener Daten geregelt. Grundsätzlich verarbeitet das Zentrum keine besonderen Kategorien personenbezogener Daten. Es ist jedoch nicht auszuschließen, dass dies im Einzelfall vorkommt. Sofern für das Zentrum im konkreten Einzelfall keine andere Möglichkeit besteht, eine Aufgabe aus § 5 Abs. 2 zu erfüllen, ermöglicht Abs. 2 Satz 3 dem Zentrum auf Grundlage des Art. 9 Abs. 2 lit. g der Datenschutz-Grundverordnung die Verarbeitung dieser Daten. Zum Schutz besonderer Kategorien personenbezogener Daten ist hierfür ein erhebliches öffentliches Interesse erforderlich. Ein erhebliches öffentliches Interesse liegt insbesondere bei Hilfe-, Beratungs- und Unterstützungsleistungen eines IT-Sicherheitsvorfalls in der Landesverwaltung vor. Im Einzelfall kann ein erhebliches öffentliches Interesse jedoch auch bei Schadens- oder Störfällen in anderen Bereichen nicht vollständig ausgeschlossen werden. Die Interessen der von der Verarbeitung betroffenen Person werden vor der Verarbeitung besonderer Kategorien personenbezogener Daten darüber hinaus durch das Erfordernis einer zusätzlichen Verhältnismäßigkeitsprüfung besonders geschützt. Erst wenn das Zentrum im konkreten Einzelfall zu dem Ergebnis gelangt, dass die nicht zu vermeidende Verarbeitung der personenbezogenen Daten besonderer Kategorien keine unverhältnismäßige Beeinträchtigung der betroffenen Person darstellt, ist eine Datenverarbeitung zulässig.

Zum Schutz der betroffenen Person sieht das Zentrum angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vor, Abs. 2 Satz 4. Hierzu zählt neben den in § 20 Abs. 2 Satz 2 Nr. 2 und Nr. 5 HDSIG genannten Maßnahmen (Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind sowie Pseudonymisierung personenbezogener Daten), auch die Anonymisierung personenbezogener Daten, soweit dies angemessen ist und die Aufgabenwahrnehmung nicht gefährdet.

Zu Abs. 3

Enthalten die Daten personenbezogene Informationen, sind diese vor einer weiteren Verarbeitung unverzüglich automatisiert zu anonymisieren. Ist eine Anonymisierung im Hinblick auf die Zielsetzung der Erkennung und Abwehr von Gefahren für die Informationssicherheit der Landesverwaltung nicht möglich, richtet sich die weitere Verarbeitung der personenbeziehbaren Daten nach den Regelungen in §§ 10, 11, 13 und 17 dieses Gesetzes.

Zu Abs. 4

Abs. 4 stellt für das gesamte Gesetz klar, dass Schadprogramme zu jeder Zeit durch die jeweils betroffene Stelle gelöscht oder unbrauchbar gemacht werden dürfen. Dies gilt auch dann, wenn dem Schutz des § 303a StGB unterliegende Daten mit dem Schadprogramm untrennbar zusammenhängen. Eine Strafbarkeit nach § 303a StGB kommt in diesem Fall nicht in Betracht.

Zu Abs. 5

Mit Abs. 5 wird klargestellt, dass die sich aus den §§ 8 bis 11 ergebenden Verwendungsbeschränkungen ausschließlich für Daten gelten, die dem Fernmeldegeheimnis aus Art. 10 des Grundgesetzes unterliegen oder die einen Personenbezug aufweisen und somit den Einschränkungen der Datenschutzregelungen unterfallen.

Zu § 8 (Verwendung von auf informationstechnischen Systemen gespeicherten Daten)

Zu Abs. 1

Abs. 1 erlaubt die Auswertung von Daten, die bereits aufgrund anderer Rechtsgrundlagen, etwa der Vorschriften über technisch-organisatorische Sicherungsmaßnahmen des Hessischen Datenschutz- und Informationsfreiheitsgesetzes oder der Datenschutz-Grundverordnung, vorliegen. Da diese Daten grundsätzlich nur im Rahmen ihres Erhebungszwecks verarbeitet werden dürfen (Art. 6 Datenschutz-Grundverordnung), enthält Abs. 1 die Erlaubnis, diese Daten auch für die in Abs. 1 konkret genannten weiteren Zwecke auszuwerten.

Eine Auswertung ist zum einen zum Erkennen, Nachverfolgen oder Beseitigen von Störungen oder Fehlern des informationstechnischen Systems erlaubt.

Zum anderen ist die Auswertung zulässig zur Abwehr von Gefahren für die Grundwerte der Informationssicherheit (namentlich der Vertraulichkeit, Verfügbarkeit und Integrität von Daten), die von Sicherheitslücken, Schadprogrammen oder erfolgten bzw. versuchten Angriffen ausgehen.

Es ist sowohl die Erkennung von Angriffen als auch die Beseitigung ihrer Folgen, wie auch die Prävention vor weiteren Angriffen umfasst.

Eine Datenerhebung ist nach dieser Vorschrift nicht vorgesehen. Sie dient allein der Zweckänderung der Verarbeitung bereits auf den IT-Systemen gespeicherter Daten. Damit können auch Daten genutzt werden, 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.

Umfasst werden sowohl die Daten, die auf den informationstechnischen Systemen der Stellen nach § 1 gespeichert sind, als auch die Daten auf informationstechnischen Systemen, die mit dem jeweiligen Datennetz der entsprechenden Stelle verbunden sind, unabhängig von ihrem zivilrechtlichen Eigentum, der Zuordnung zu einer bestimmten Behörde oder Organisationseinheit, ihrem konkreten Einsatzzweck und der Erlaubnis zur Verbindung mit dem Datennetz.

In Bezug auf das Landesdatennetz bedeutet dies, dass auch Geräte der Bediensteten oder von Fremdfirmen erfasst werden, soweit diese Geräte mit dem Landesdatennetz verbunden sind. Verbunden mit dem Landesdatennetz ist ein IT-System, wenn es mit einem nichtöffentlichen Datennetzwerk verbunden ist, welches durch oder im Auftrag des Landes betrieben wird.

Die Vorschrift ermöglicht die Zweckänderung von bereits durch die bestehenden informationstechnischen Systeme erhobenen Daten (sog. Protokolldaten, „log files“). In diesen Protokolldaten sind stets der Zeitpunkt des aufgezeichneten Ereignisses verzeichnet, welches für die Korrelation von Ereignissen auf verschiedenen Systemen ebenso bedeutsam ist, wie die in einem Protokoll regelmäßig verzeichnete IP-Adresse mit dem korrespondieren Domänennamen zur Identifikation eines für einen (mutmaßlichen) Angriff genutzten und eines angegriffenen Systems.

Zu Nr. 1

Erhoben werden dürfen Protokolldaten von Firewall-Systemen einschließlich Erhebungszeitpunkt, IP-Adresse und Port sowie vollständigem Domänennamen von ein- und ausgehenden Verbindungen sowie die durch die Firewall durchgeführte Aktion. Eine Firewall ist ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt. Die Firewall dient der Beschränkung des Netzwerkzugriffs auf Basis eines Regelwerks, auf der Basis von Absender, Empfänger und Dienst bzw. Port einer Verbindung. Auf Basis dieses Regelwerks entscheidet die Firewall, ob sie eine Verbindung zulässt oder verhindert. Insbesondere aus den abgelehnten Verbindungen können Aussagen über Angriffe abgeleitet werden.

Zu Nr. 2

Erhoben werden dürfen Protokolldaten von Systemen zur Erkennung und Beseitigung von Schadsoftware einschließlich Erhebungszeitpunkt, IP-Adresse und vollständigem Domänennamen des betroffenen Systems, ausgegebener Meldung sowie Informationen über die Schadsoftware und die als Schadprogramm erkannten Daten. Ein System zur Erkennung und Beseitigung von Schadsoftware (sog. „Antivirenprogramm“) versucht auf Basis von Signaturen bekannter Schadsoftware und Heuristiken Schadprogramme auf einem IT-System zu erkennen, deren Ausführung zu verhindern und möglichst zu beseitigen. Überdies werden genaue Informationen über den Typ des erkannten Schadprogramms verzeichnet sowie ggf. die vom Schadprogramm betroffenen Daten selbst.

Zu Nr. 3

Erhoben werden dürfen Protokolldaten von Systemen zur Erkennung von unerwünschten E-Mails einschließlich Erhebungszeitpunkt, IP-Adresse und vollständigem Domänennamen von ein- und ausgehenden Verbindungen, E-Mailadresse des Absenders und Empfängers einer Nachricht, deren Größe und eindeutiger Identifikationsnummer sowie Fehler- und sonstige Statusmeldungen und die als Schadprogramm erkannten Daten. Ein System zur Erkennung von unerwünschten E-Mails (sog. „Spam-Filter“) versucht insbesondere auf Basis von bekannten unerwünschten E-Mails oder Absendern oder auf Basis eines selbstlernenden Filters unerwünschte Werbe- und Betrugsmails und Mails mit Schadprogrammen aus den eingehenden E-Mails vor der Zustellung an den Adressaten insgesamt herauszufiltern. Die dabei entstehenden Protokolldaten geben Aufschluss über mögliche Angriffe, insbesondere wenn Schadsoftware per E-Mail verteilt wird.

Zu Nr. 4

Erhoben werden dürfen Protokolldaten von Datenbankservern einschließlich Erhebungszeitpunkt, Anmeldename, IP-Adresse und vollständigem Domänennamen von Verbindungen und die Identifikationsnummer der ausgegebenen Meldung und deren Klartext. Datenbankserver liefern häufig Daten für die Ausgabe durch Webserver, welche ihrerseits häufige Angriffsziele sind. Aus den (gescheiterten) Zugriffen auf Datenbankserver lassen sich insoweit Anhaltspunkte für Angriffe entnehmen. Beim Anmeldenamen handelt es sich um einen Benutzernamen, der zur Authentisierung des zugreifenden Benutzers notwendig ist. Häufungen von abgelehnten Authentisierungsversuchen sind oft ein Zeichen für einen Angriff.

Zu Nr. 5

Erhoben werden dürfen Protokolldaten von Web- und Proxyservern einschließlich Erhebungszeitpunkt, IP-Adresse und vollständigem Domänenamen von ein- und ausgehenden Verbindungen sowie dem einheitlichen Ressourcenzeiger (Uniform Ressource Locator, URL) und Kopfdaten exklusive dem Cookie einer ein- oder ausgehenden Verbindung auf Basis der Hypertext-Übertragungsprotokolle (HTTP, HTTPS). Webserver sind häufig Ziel von Angriffen. Dabei versuchen Angreifer vor allem über speziell präparierte Abfragen an Webserver erweiterte Rechte zu erlangen, weswegen diese Angriffe die Auswertung der URL und der Kopfdaten erfordern. Zudem kommuniziert Schadsoftware überwiegend per http-Protokoll mit ihren Zielsystemen, um dorthin Daten zu exfiltrieren. Um diese Form der Folge von Angriffen zu entdecken und zu verhindern ist ebenfalls eine Auswertung der URL und der Kopfdaten erforderlich.

Bei der Auswertung dieser Daten können in Einzelfällen Inhaltsdaten als Bestandteile von URL, Kopfdaten oder Cookies enthalten sein. Die Erhebung dieser Parameter soll weitmöglichst ausgeschlossen und bei der weiteren Verarbeitung nicht verwertet werden. Dies ist durch entsprechende technisch-organisatorische Maßnahmen im Datenschutzkonzept, vgl. § 14, zu gewährleisten.

Zu Nr. 6

Erhoben werden dürfen Protokolldaten der Betriebssoftware von Computersystemen einschließlich Erhebungszeitpunkt, IP-Adresse und vollständigem Domänennamen des betroffenen Computersystems, Namen des Programms oder Systemdienstes sowie dessen Typ, die Identifikationsnummer der ausgegebenen Meldung und deren Klartext. Jede Betriebssoftware speichert Protokolldateien von erfolgreichen und fehlgeschlagenen Aktionen und Programmaufrufen, welche ebenfalls Anhaltspunkte für einen Angriff oder eine Schadsoftware liefern können. Um Angriffe erkennen zu können, ist es erforderlich, die Meldungen der Computersysteme und die sie erzeugenden Programme zu erfassen.

Zu Abs. 2

Nach Satz 1 dürfen gespeicherte Inhalte von Kommunikationsvorgängen nur unter den engen Voraussetzungen des § 11 ausschließlich zur Abwehr von Schadprogrammen ausgewertet werden.

Satz 2 bestimmt, dass Ergebnisse der Verarbeitung unverzüglich zu löschen sind, soweit nicht zureichende oder hinreichende tatsächliche Anhaltspunkte gemäß § 10 oder die Sonderregelung zu Inhaltsdaten in § 11 eine andere Behandlung rechtfertigen. Dadurch wird dem Grundsatz der Datensparsamkeit Rechnung getragen und die Eingriffsintensität gesenkt.

Zu § 9 (Erhebung und Auswertung des Datenverkehrs im Landesdatennetz)

Während § 8 die Auswertung bereits erhobener und gespeicherter Daten regelt, stellt § 9 die Rechtsgrundlage dar für eine Durchsuchung des Datenverkehrs im Landesdatennetz nach Auffälligkeiten.

Zu Abs. 1

Satz 1 garantiert eine strenge Zweckbindung und stellt klar, dass der Datenverkehr ausschließlich zur Abwehr von Gefahren für die Grundwerte der Informationssicherheit, namentlich der Vertraulichkeit, Verfügbarkeit und Integrität von Daten ausgewertet werden darf, die von Sicherheitslücken, Schadprogrammen oder erfolgten bzw. versuchten Angriffen ausgehen; es ist also sowohl die Erkennung von Angriffen als auch die Beseitigung ihrer Folgen, wie auch die Prävention vor weiteren Angriffen umfasst.

Auffälliger Datenverkehr ergibt sich beispielsweise aus einem Abweichen von einer festgelegten „Regel“ oder aus der Entdeckung von Schadsoftware.

Die Auswertung darf ausschließlich automatisiert erfolgen, so dass eine Kenntnisnahme durch natürliche Personen ausgeschlossen wird. Überdies wird die Verarbeitung der Daten auf die benannten Datenkategorien begrenzt:

Zu Nr. 1

Diese Vorschrift sieht die Auswertung der im IP-Datenstrom benötigten Informationen für die Steuerung der einzelnen Datenpakete vor. Zu diesen Informationen gehört insbesondere, welches System das Datenpaket gesendet hat und welches es empfängt, auf welchen menschenlesbaren Domänennamen sich diese Adressen auflösen lassen (z. B. www.hessen.de statt einer Zahlenkombination wie 12.123.45.67) sowie technische Steuerinformationen des Datenpakets.

Zu Nr. 2

Diese Regelung sieht für Verbindungen auf Basis der Hypertext-Übertragungsprotokolle (HTTP, HTTPS) vor, dass über die bereits in Nr. 1 vorgesehenen Daten hinaus auch der vollständige einheitliche Ressourcenzeiger (Uniform Ressource Locator, URL) verarbeitet werden darf. Bei der URL handelt es sich um den von einem Nutzer mittels Webbrowser oder von einem Computerprogramm, insbesondere von einer Schadsoftware getätigten Seitenaufruf. Dabei werden neben dem Protokoll (HTTP, HTTPS) und dem Domänennamen (Hostnamen) auch alle weiteren Elemente des Seitenaufrufs erfasst. Automatisiert verarbeitet werden dürfen auch die Kopfdaten der http-Verbindung jedoch unter Ausschluss des sog. Cookies, d. h. kleiner Datenmengen, welche von einem Webserver zur Speicherung auf dem Endgerät des Nutzers vorgesehen sind.

Zu Abs. 2

Nach Satz 1 dürfen die gemäß Abs. 1 erhobenen Inhalte der Kommunikation nur unter den engen Voraussetzungen des § 11 ausschließlich zur Abwehr von Schadprogrammen ausgewertet werden.

Da in § 9 neue Daten erhoben werden, sind diese unverzüglich zu löschen, soweit eine automatisierte Auswertung keine Anhaltspunkte für Auffälligkeiten bietet (§ 10) oder die besonderen Voraussetzungen des § 11 vorliegen.

Zu § 10 (Auswertung ohne Inhaltsdaten)

§ 10 regelt die über §§ 8 Abs. 1 oder 9 Abs. 1 hinausgehende Möglichkeit der Datenauswertung, soweit es sich nicht um Inhaltsdaten handelt. Daten über den Inhalt werden ausschließlich unter den Voraussetzungen des § 11 ausgewertet.

Die Auswertungsmöglichkeiten sind zweistufig aufgebaut, entsprechend der Qualität der Anhaltspunkte für eine Gefährdung der Informationssicherheit.

Zu Abs. 1

Da Schadprogramme regelmäßig erst mit einer zeitlichen Verzögerung identifiziert werden können, müssen auffällige Daten gespeichert werden können. Dies ist jedoch nur im Falle des Vorliegens von zureichenden tatsächlichen Anhaltspunkten erlaubt. Zureichende tatsächliche Anhaltspunkte liegen vor, wenn ein Anfangsverdacht im Sinne des § 152 StPO für eine Gefahr für die Vertraulichkeit, Verfügbarkeit oder Integrität von Daten in der Informations- und Kommunikationsinfrastruktur des Landes durch Sicherheitslücken, Schadprogramme und erfolgte oder versuchte Angriffe vorliegt. In diesem Fall dürfen die Daten für höchstens 90 Tage gespeichert werden. Sollte sich der Anfangsverdacht bereits vor Ablauf der 90 Tage als nicht fundiert erweisen, sind die Daten umgehend zu löschen. Für eine zulässige Speicherung von 90 Tagen wird der Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen nach § 8 Abs. 1 Satz 1 BSI-Gesetz (Stand 25. Dezember 2021) in Verbindung mit der Protokollierungsrichtlinie Bund herangezogen. Hiernach beträgt die Speicherfrist in Abstimmung mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit für alle Protokolldaten 90 Tage. Soweit andere Vorschriften eine längere Speicherdauer vorsehen, bleiben diese unberührt.

In den Fällen, in denen ein direkter Personenbezug vorliegt, etwa im Regelfall bei der Verarbeitung von E-Mail- oder IP-Adressen, sind diese unverzüglich, das heißt ohne schuldhaftes Zögern, zu pseudonymisieren, soweit dies technisch und ohne unverhältnismäßigen Aufwand möglich ist.

Jegliche Verarbeitung nach Abs. 1, das heißt sowohl die Pseudonymisierung als auch die Auswertung, erfolgt automatisiert. Hierdurch wird die Eingriffsintensität verringert und dem Grundsatz der Datensparsamkeit wird entsprochen.

Zu Abs. 2

Nur soweit die Auswertung nach Abs. 1 hinreichende tatsächliche Anhaltspunkte dafür bietet, dass die betreffenden Daten ein Schadprogramm enthalten, durch einen Angriff oder ein Schadprogramm verursacht wurden oder sich aus ihnen entsprechende Hinweise ergeben, kommt eine nichtautomatisierte oder direkt personenbezogene Auswertung der Daten in Betracht. Zudem muss die weitere Datenverarbeitung zur Abwehr des Schadprogramms oder Angriffs, zur Abwehr von Gefahren, die von dem Schadprogramm oder Angriff ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme oder Angriffe erforderlich sein.

Hinreichende tatsächliche Anhaltspunkte liegen vor, wenn ein hinreichender Tatverdacht im Sinne von § 170 StPO bejaht werden kann. Es müssen also Anhaltspunkte vorliegen, die das Szenario, dass die Daten durch einen Angriff oder ein Schadprogramm verursacht wurden oder sich aus ihnen entsprechende Hinweise ergeben, wahrscheinlicher erscheinen lassen, als das Szenario, dass dies nicht der Fall ist.

Die Datenverarbeitung nach Satz 1 bedarf der Anordnung durch die Leiterin oder den Leiter der nach § 12 zur Ergreifung der Maßnahme ermächtigten Stelle, im Falle des Tätigwerdens des Zentrums für Informationssicherheit darf die Anordnung nur durch eine Beschäftigte oder einen Beschäftigten des für IT- und Cybersicherheit in der Landesverwaltung zuständigen Ministeriums mit der Befähigung zum Richteramt getroffen werden. Da die Maßnahme nach Abs. 2 keine heimliche, inhaltsbezogene Überwachung darstellt, sondern lediglich die Suche nach Schadprogrammen oder Angriffen zum Gegenstand hat, bedarf sie keiner richterlichen Anordnung. Gleichwohl stellt sie einen intensiven Eingriff in die Grundrechte der Bediensteten und/oder Dritter dar und muss daher durch eine oder einen Beschäftigten in einer dieser Entscheidung angemessenen Position getroffen werden. Da die Maßnahmen durch alle in § 1 genannten Stellen ergriffen werden können (vgl. § 12) und kleinere Kommunen evtl. keine Personen mit Befähigung zum Richteramt beschäftigen, die die Anordnung treffen könnten, wurde von einer generellen Forderung nach einer solchen Befähigung abgesehen. Da das Zentrum für Informationssicherheit für die gesamte Landesverwaltung tätig wird, mit entsprechendem Zugriff auf sehr große Datenmengen, wird für ein Tätigwerden des Zentrums für Informationssicherheit jedoch die Anordnung durch eine Person mit Befähigung zum Richteramt gefordert.

Durch das Erfordernis der Anordnung soll die Durchführung einer Rechtmäßigkeitsprüfung der weiteren Auswertung gewährleistet werden. Aus diesem Grunde und auch aus Gründen der Transparenz ist die Entscheidung zu dokumentieren und nach § 14 Abs. 4 in die jährliche Aufstellung an die Hessische Beauftragte oder den Hessischen Beauftragten für Datenschutz und Informationssicherheit aufzunehmen. Die Dokumentation darf für andere Zwecke als der nachträglichen Überprüfung der Rechtmäßigkeit der Verarbeitung nicht verwendet werden und ist zu löschen, wenn sie nicht mehr erforderlich ist, spätestens jedoch zum Ablauf des Kalenderjahres, das dem Jahr der Dokumentation folgt.

Zu § 11 (Auswertung von Inhaltsdaten)

Zu Abs. 1

Erhobene Inhaltsdaten, also solche, die den Inhalt einer Kommunikation betreffen, werden ausschließlich nach dieser Vorschrift ausgewertet. Abs. 1 Satz 1 erlaubt die unverzügliche Auswertung von im Rahmen von § 8 Abs. 1 und § 9 Abs. 1 angefallener Inhaltsdaten zum Schutz der Daten vor Schadprogrammen. Hinsichtlich der Erläuterungen zum Zweck der Maßnahme und zu den Gefahren für die Daten in der Informations- und Kommunikationsinfrastruktur des Landes wird auf die Erläuterungen zu § 8 Abs. 1 verwiesen.

Nach Satz 2 sind Inhaltsdaten nach ihrer Auswertung ohne schuldhaftes Zögern zu löschen, soweit die folgenden Absätze keine weitere Verwendung vorsehen.

Zu Abs. 2

Abs. 2 regelt die weitere Auswertung von Inhaltsdaten im Falle von zureichenden tatsächlichen Anhaltspunkten und entspricht weitestgehend § 10 Abs. 1, auf dessen Erläuterungen verwiesen wird. Da es sich um Inhaltsdaten handelt, deren Verarbeitung einen intensiveren Grundrechtseingriff begründet, ist aber bereits die Speicherung der Daten – anders als nach § 10 Abs. 1 – unter den Vorbehalt einer Anordnung gestellt. Hinsichtlich der Anordnung kann auf die Erläuterungen zu § 10 Abs. 2 verwiesen werden. Gleiches gilt für die Dokumentation.

Zu Abs. 3

Abs. 3 regelt die weitere Auswertung von Inhaltsdaten bei Vorliegen hinreichender tatsächlicher Anhaltspunkte. Da nunmehr auch eine über die 90-Tage-Frist hinausgehende, nicht-automatisierte Verarbeitung ermöglicht und damit der Grundrechtseingriff weiter intensiviert wird, verlangt Abs. 3 erneut eine Anordnung der Maßnahme. Hiermit und mit der Beschränkung der Auswertung auf Schadprogramme soll dem Ausnahmeverhältnis des Abs. 3 gegenüber der automatisierten Verarbeitung Rechnung getragen und einer möglichen „ausufernden" Nutzung entgegengewirkt werden.

Im Übrigen wird auf die Erläuterungen zum Vorliegen hinreichender tatsächlicher Anhaltspunkte, zur Erforderlichkeit der Verarbeitung und der Anordnung im Rahmen des § 10 Abs. 2 verwiesen.

Zu Abs. 4

Abs. 4 trägt dem Umstand Rechnung, dass Inhaltsdaten immer auch Aufschluss über den Kernbereich privater Lebensgestaltung geben können, der über Art. 1 Abs. 1 GG absolut geschützt wird und durch hinreichende Vorkehrungen geschützt werden muss, auch wenn ein Eingriff in den Kernbereich privater Lebensgestaltung durch eine Maßnahme nach § 11 eher unwahrscheinlich ist, da diese vor allem die Analyse der Umstände der Kommunikation im Fokus hat und gerade nicht auf eine Ausspähung des Inhaltes zielt.

Soweit möglich, ist nach Satz 1 bereits technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Sollten sie doch und wenn auch nur im Zweifel, erlangt werden, dürfen sie nicht verwendet werden und sind unverzüglich, das heißt ohne schuldhaftes Zögern, zu löschen. Auf eine Kernbereichskontrolle wurde verzichtet, da dies eine inhaltliche Auswertung in Bezug auf kernbereichsrelevante Aspekte erfordern würde und der Eingriff damit erheblich intensiver würde, als die Maßnahme ihn vorsieht. Um aber eine nachträgliche Rechtmäßigkeitsprüfung zu gewährleisten, ist die Tatsache der Erlangung und unverzüglichen Löschung kernbereichsrelevanter Daten zu dokumentieren und darf ausschließlich zu diesem Zweck verwendet werden. Die Dokumentation ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch zum Ablauf des Kalenderjahres, das dem Jahr der Dokumentation folgt.

Zu § 12 (Zuständigkeit)

Zu Abs. 1

Sofern das Landesdatennetz (einschließlich der Übergabe- und Knotenpunkte) betroffen ist oder IT-Systeme der Stellen nach § 1 Nr. 1 und 2, ist das Zentrum für Informationssicherheit zuständig, die in den §§ 8 bis 11 beschriebenen Maßnahmen für diese Stellen durchzuführen. Diese Stellen erhalten darüber hinaus die Möglichkeit, eigene Auswertungen für ihren Verantwortungsbereich durchzuführen (Abs. 2). Ziel hiervon ist neben einem landeseinheitlichen Lagebild der Informationssicherheit auch spezifische umfassende Lagebilder zu ermöglichen, bspw. das Lagebild zu einem einzelnen Ressort. Die hierfür nötigen technischen und organisatorischen Schnittstellen regelt die Landesrichtlinie.

Das Landesdatennetz ist das vom Land in eigener Verantwortung betriebene Datennetz. Es verbindet die einzelnen lokalen Netzwerke der Dienststellen zu einem landesweiten Netz und wird bei der Hessischen Zentrale für Datenverarbeitung (HZD) betrieben. Datennetze, die im Auftrag einer Dienstelle von einem Dritten (Service-Provider) betrieben werden und nicht mit dem Landesdatennetz verbunden sind, unterfallen hingegen nicht dem Landesdatennetz.

Das Zentrum für Informationssicherheit ist in Bezug auf die Maßnahmen nach §§ 8 bis 11 damit zentral und primär zuständig für das Landesdatennetz und die IT-Systeme der hessischen Landesverwaltung. Hierdurch wird ein landeseinheitliches Lagebild der Informationssicherheit in der Landesverwaltung gewährleistet. Die konkrete Bereitstellung der Daten, über die bei der HZD betriebenen und für mehrere Ressorts bestimmte Systeme, Verfahren und Plattformen hinaus, wird in einer Landesrichtlinie geregelt. Damit wird ermöglicht, auf infrastrukturelle und technische Änderungen zu reagieren und ressortspezifische Anforderungen zu berücksichtigen. Unabhängig vom Erlass der Richtlinie findet die Erhebung und Auswertung zentraler Daten, wie an zentralen E-Mail-Servern, Virenschutz und artverwandten Sicherheitssystemen (bspw. Endpoint-Security-Systeme) sowie an Netzübergängen zu Netzen außerhalb des Landesdatennetzes durch das Zentrum für Informationssicherheit statt.

Zur Wahrung der besonderen Rechtsstellung der in Abs. 1 Satz 4 genannten Stellen, findet eine Datenverarbeitung durch das Zentrum für Informationssicherheit nur im Einvernehmen mit der Leitung der jeweiligen Stelle statt.

Zur Gewährleistung der richterlichen Unabhängigkeit werden Daten, die diesem Arbeitsprozess unterliegen, durch das Zentrum für Informationssicherheit nicht verarbeitet. Dies gilt auch für Zweifelsfälle. Die Kontrolle der Einhaltung dieser Vorschrift erfolgt durch die bei der IT-Stelle der Justiz eingerichtete IT-Kontrollkommission nach § 14 Abs. 4 Satz 3. Ebenso erfolgt keine Verarbeitung von Daten, die der Mandatstätigkeit von Abgeordneten des Hessischen Landtags zuzurechnen sind.

Zu Abs. 2

Soweit der jeweilige Verantwortungsbereich der Stellen nach § 1 betroffen ist, können diese Stellen selbst die in den §§ 8 bis 11 beschriebenen Maßnahmen ergreifen. Da diese Stellen aber unter Umständen nicht die erforderliche Kompetenz oder technische Ausstattung besitzen, um von dieser Ermächtigung Gebrauch zu machen, ermöglicht es Satz 2 diesen Stellen das Zentrum für Informationssicherheit im Wege der Auftragsverarbeitung mit Maßnahmen nach den §§ 8 bis 11 zu beauftragen. Ebenso können die Stellen nach § 1 das Zentrum für Informationssicherheit beauftragen, die Maßnahmen nach §§ 8 bis 11 bei solchen Datennetzen zu ergreifen, die im Auftrag dieser Stellen durch Dritte betrieben werden (bspw. das nPOL-Leitstellennetz).

Ein Anspruch auf Übernahme der Maßnahmen durch das Zentrum für Informationssicherheit besteht aus Kapazitätsgründen nicht.

Zu § 13 (Übermittlung personenbezogener oder dem Fernmeldegeheimnis unterliegender Daten)

Zu Abs. 1

Werden im Rahmen der Maßnahmen nach §§ 7 bis 11 tatsächliche Gefahren für die Vertraulichkeit, Verfügbarkeit oder Integrität von Daten in der Informations- und Kommunikationsinfrastruktur des Landes ermittelt, dürfen die zur Abwehr oder Beseitigung erforderlichen Daten an die für den tatsächlichen Betrieb der informationstechnischen Systeme verantwortliche Stellen im Land übermittelt werden. Nach §§ 9 Abs. 3 und 10 Abs. 2 verarbeitete personenbezogene Daten (i. d. R. die IP-Adresse des betroffenen informationstechnischen Systems und der Umstand der Beeinträchtigung) oder dem Fernmeldegeheimnis unterliegende Daten dürfen ebenfalls übermittelt werden, allerdings nur zu den in § 8 Abs. 1 bzw. § 9 Abs. 1 genannten Zwecken und sind auf das absolut notwendige Maß zu beschränken.

Zu Abs. 2 und 3

Abs. 2 und 3 regeln die Möglichkeiten der Übermittlung von personenbezogenen Daten an Polizei- und Verfassungsschutzbehörden. Sie sind § 5 Abs. 5 und 6 BSI-Gesetz nachempfunden.

Angriffe auf die Informationstechnik mittels Schadprogrammen stellen zugleich auch Straftaten oder eine Gefahr für die öffentliche Sicherheit dar. Abs. 2 gestattet der jeweils ermächtigten Stelle daher, die Daten auch an die insoweit zuständigen Behörden zu übermitteln, sofern dies zur Verfolgung einer Straftat einer mittels Telekommunikation begangenen Straftat erforderlich ist. Außerdem darf das BSI Daten im Rahmen des ursprünglichen Verwendungszwecks übermitteln, wenn eine Gefahr für die öffentliche Sicherheit unmittelbar von dem gefundenen Schadprogramm ausgeht oder wenn ein nachrichtendienstlicher Hintergrund vorliegt.

Eine zweckändernde Übermittlung möglicher Zufallsfunde nach Abs. 3 an die Polizei- oder Verfassungsschutzbehörden ist hingegen nur unter den engen Voraussetzungen dieses Absatzes zulässig. Diese bedarf der gerichtlichen Zustimmung. Da Ziel der Maßnahmen die Suche nach Schadprogrammen, also technischen Inhalten, aber nicht die Auswertung der eigentlichen Kommunikationsinhalte ist, ist ein Richtervorbehalt nur bei dieser zweckändernden Übermittlung erforderlich.

Zu § 14 (Gewährleistung der Informationssicherheit und des Datenschutzes)

§ 14 regelt zusätzliche und explizite Anforderungen an die Informationssicherheit und den Datenschutz. Weitere Anforderungen, die sich bereits aus anderen Vorschriften, insbesondere aus der Datenschutz-Grundverordnung und dem HDSIG, ergeben, bleiben unberührt. Die Maßnahmen sind in einem Datenschutzkonzept zu regeln. Die Gewährleistung eines besonders hohen Maßes an Informationssicherheit folgt aus dem regelmäßig hohen Schutzbedarf der Informationen gemäß BSI-Grundschutz.

Zu Abs. 1

Abs. 1 stellt klar, dass die erhobenen und gespeicherten Daten durch technische und organisatorische Maßnahmen, die dem Stand der Technik entsprechen, zu sichern sind. Unter „Stand der Technik“ wird der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen verstanden, der nach herrschender Auffassung führender Fachleute das Erreichen des gesetzlich vorgegebenen Zieles gesichert erscheinen lässt. Verfahren, Einrichtungen und Betriebsweisen oder vergleichbare Verfahren, Einrichtungen und Betriebsweisen müssen sich in der Praxis bewährt haben oder sollten – wenn dies noch nicht der Fall ist – möglichst im Betrieb mit Erfolg erprobt worden sein.

Zu Abs. 2

Abs. 2 konkretisiert die abstrakte Verpflichtung aus Abs. 1 durch eine nicht abschließende Aufzählung von zu treffenden Maßnahmen.

Zu Nr. 1

Die organisatorische Trennung der Organisationseinheiten für die Datenverarbeitung nach §§ 8 bis 11 von den für die üblichen betrieblichen Aufgaben verantwortlichen Organisationseinheiten ist angezeigt, um zu verhindern, dass andere als die dafür ermächtigten Personen von den sensiblen Daten Kenntnis erhalten.

Zu Nr. 2

Das gleiche Ziel wird durch die technische Trennung der informationstechnischen Systeme für die Datenverarbeitung nach §§ 8 bis 11 von den für die üblichen betrieblichen Aufgaben vorgehaltenen informationstechnischen Systemen verfolgt. Insbesondere sind die Speichereinrichtungen zu separieren.

Zu Nr. 3

Ein angemessenes Datenschutzniveau erfordert auch die besondere Sicherung vor unberechtigten Zugriffen aus anderen Netzen, so dass ein versehentlicher oder beabsichtigter Zugriff durch nicht berechtigte Personen über das Netz ausgeschlossen wird.

Zu Nr. 4

Bei der Datenverarbeitung sind die nach dem jeweils aktuellen Stand der Technik erforderlichen Maßnahmen zu ergreifen, um die Daten vor Missbrauch und Kenntnisnahme durch unbefugte Personen zu schützen. Eine solche Maßnahme kann z. B. der Einsatz eines als besonders sicher geltenden Verschlüsselungsverfahrens sein.

Zu Nr. 5

Aufgrund der Sensibilität der Daten darf der Zutritt zu den und der Zugriff auf die Datenverarbeitungsanlagen nur mit Ermächtigung der Leitung der Stelle erfolgen. Die restriktive Regelung soll gewährleisten, dass der Kreis der Personen, die Zugriff auf die sensiblen Daten haben, möglichst klein bleibt. Überdies soll sichergestellt werden, dass die ermächtigten Personen regelmäßig über die Sensibilität der ihnen anvertrauten Daten belehrt werden können.

Zu Nr. 6

Das Prinzip des Zusammenwirkens von mindestens zwei Personen soll die Gefahr der unrechtmäßigen Kenntnisnahme von personenbezogenen Daten minimieren.

Zu Abs. 3

Alle Zugriffe auf die im Rahmen der §§ 8 bis 11 gespeicherten Daten sind in einem Protokoll zu vermerken. Das Führen einer Protokolldatei ist erforderlich, um unberechtigte Zugriffe zu erkennen und abzuwehren. Sie kann auch als automatisierte Datei geführt werden.

Zu Abs. 4

Um die Wahrung der Verhältnismäßigkeit zwischen Datenschutz und Datensicherheit zu sichern, ist der oder dem Hessischen Datenschutzbeauftragten einmal jährlich eine Auswertung über die nach den §§ 8 bis 11, 13 und 16 erfolgten Verarbeitungsvorgänge vorzulegen. Diese Berichtspflicht soll gewährleisten, dass der Zugriff, die Nutzung und die Verarbeitung von personenbezogenen Daten auf das Notwendige beschränkt werden. Inhalt und Frist zur Vorlage des Berichts sind mit der oder dem Hessischen Datenschutzbeauftragten abzustimmen.

Zur nachträglichen Kontrolle zum Schutz vor unbefugter Einsichtnahme in Daten, die der richterlichen Unabhängigkeit unterliegen, ist der IT-Kontrollkommission der hessischen Justiz nach Satz 2 eine Aufstellung über die erfolgten Datenverarbeitungen aus dem Bereich der Justiz vorzulegen. Hiermit soll unter Mitwirkung gewählter Vertreter des betroffenen Kreises sichergestellt werden, dass Einflussnahmen durch die Exekutive verhindert und die Integrität und Vertraulichkeit von Verfahrensdaten gewahrt werden. Zur Wahrnehmung der Kontrollfunktion werden Einsichts- und Auskunftsrechte hinsichtlich der Verarbeitung von Justizdaten gewährt.

Zu § 15 (Sicherheitskonzept)

Sicherheitskonzepte dienen der Ermittlung und Analyse von Risiken beim Betrieb von IT-Systemen und der darauf basierenden Bestimmung von Maßnahmen zur Risikobehandlung mit dem Ziel der weitgehenden Risikominimierung. Mit dem Sicherheitskonzept soll gewährleistet werden, dass die beim Betrieb der zur Zweckerreichung des Gesetzes eingesetzten IT-Systeme entstehenden Risiken nach dem Stand der Technik behandelt werden und davon ausgehende Gefahren für die Grundrechtspositionen der Betroffenen so weit wie möglich ausgeschlossen werden.

Zu Satz 1

Satz 1 stellt klar, dass die in §§ 7 bis 11 geregelten Ermächtigungen nur nach vorheriger Erstellung eines Sicherheitskonzepts ergriffen werden dürfen. Ferner darf von diesen Ermächtigungen erst dann Gebrauch gemacht werden, wenn die im Sicherheitskonzept vorgesehenen technischen und organisatorischen Maßnahmen auch tatsächlich umgesetzt werden und die zuständige Behörde dies auch aktenkundig gemacht hat.

Zu Satz 2

Um dies dauerhaft zu gewährleisten, ist das Sicherheitskonzept entsprechend der Fortentwicklung der Technik spätestens nach zwei Jahren zu aktualisieren; bei maßgeblichen Veränderungen am IT-System allerdings auch früher. Softwareaktualisierungen dienen der Erhaltung der Funktionsfähigkeit eines bestehenden IT-Systems und stellen grundsätzlich keine wesentliche Veränderung dar. Veränderungen an der IT-Architektur oder am Funktionsumfang erfordern hingegen in der Regel die Aktualisierung des Sicherheitskonzeptes.

Zu § 16 (Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen)

Mit § 16 wird die rechtliche Grundlage geschaffen, auf der das Zentrum für Informationssicherheit, konkret die MIRTs des CERT, erforderliche Maßnahmen zur Unterstützung und Wiederherstellung der Sicherheit oder Funktionsfähigkeit der von Cyber-Angriffen betroffenen informationstechnischen Systeme von Stellen nach § 1 - auf Ersuchen der betroffenen Stellen - vor Ort treffen kann. Vorhandene Notfallkonzepte der betroffenen Stellen sind hierbei heranzuziehen.

Da es bei einem vor Ort Einsatz nicht im Einzelnen absehbar ist, auf welche Daten zur Gefahrenabwehr zugegriffen werden muss, insbesondere nicht ausgeschlossen werden kann, dass hierbei auf personenbezogene Daten oder dem Fernmeldegeheimnis unterfallende Daten zugegriffen werden muss, ggf. auch nicht nur automatisiert oder pseudonymisiert, ist für diese Einsätze eine eigene Rechtsgrundlage erforderlich.

§ 16 ist dem § 5a des BSI-Gesetzes nachgebildet und geringfügig an die hessischen Verhältnisse angepasst. Die hessischen MIRTs haben so die gleichen Unterstützungsmöglichkeinen für die hessische Verwaltung wie die BSI-MIRTs für die Bundesbehörden und die Betreiber einer Kritischen Infrastruktur. Indem im Land Hessen vergleichbare Kompetenzen aufgebaut werden wie im Bund, kann (über den CERT-Verbund) der gewünschte und erforderliche Erfahrungsaustausch zwischen Bund und Ländern auf Augenhöhe realisiert werden.

Entsprechend der Nachbildung der Norm ist auch in der Begründung überwiegend wörtlich die Erläuterung zu § 5a des Gesetzentwurfs zur Änderung des BSI-Gesetz übernommen worden.

Zu Abs. 1

Nach Abs. 1 ist Voraussetzung für einen MIRT-Einsatz, dass es sich um einen herausgehobenen Fall handelt. Des Weiteren können die MIRTs nur auf Ersuchen der betroffenen Einrichtung tätig werden. Es soll der Entscheidung der Einrichtung überlassen bleiben, ob sie die Dienste eines MIRT in Anspruch nimmt.

Aufgabe der MIRTs ist dabei zunächst die kurzfristige Unterstützung der betroffenen Einrichtung bei der Schadensbegrenzung und der Sicherstellung eines Notbetriebes vor Ort. Danach sollen die Betroffenen aber auch bei der forensischen Untersuchung des Vorfalles, der Beseitigung der Ursachen und damit der Wiederherstellung des Normalbetriebes unterstützt werden dürfen.

Die Ausgestaltung als „Kann-Regelung“ stellt klar, dass eine Pflicht des Zentrums für Informationssicherheit zum Tätigwerden nicht besteht. Ein Ersuchender hat also keinen Anspruch auf ein Tätigwerden des Zentrums für Informationssicherheit. Diesem steht ein Ermessensspielraum zu, der insbesondere auch von den vorhandenen Kapazitäten abhängig ist.

Die vom Zentrum für Informationssicherheit zu ergreifenden Maßnahmen können unterschiedlicher Natur sein. Neben Analysen der betroffenen informationstechnischen Systeme und des Netzwerkverkehrs können dazu insbesondere auch aktive Sicherungsmaßnahmen gehören, wie etwa das Blockieren der Netzwerkverbindungen zu den Quellen der Gefährdung (z. B. zu den Kontrollservern des Angreifers oder zu den Ausgangspunkten von DDoS-Angriffen).

Zu Abs. 2

In Abs. 2 wird festgelegt, wann ein herausgehobener Fall vorliegt, bei dem um Unterstützung durch die MIRTs des Zentrums für Informationssicherheit ersucht werden kann. Ein herausgehobener Fall liegt insbesondere dann vor, wenn es sich um einen Angriff von besonderer technischer Qualität handelt oder die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems im besonderen öffentlichen Interesse liegt.

Angriffe besonderer Qualität liegen etwa dann vor, wenn zumindest der Verdacht auf sogenannte Advanced Persistent Threats besteht, die sich dadurch auszeichnen, dass Standardsicherheitsmaßnahmen zur Abwehr nicht ausreichen. Eine besondere Qualität kann auch sogenannten DDoS-Angriffen zugeschrieben werden, sofern sie mit einer außergewöhnlichen Bandbreite oder Technik ausgeführt werden. Wird zum Beispiel ein Verschlüsselungstrojaner eingesetzt, kann es sein, dass der erste Angriff als außergewöhnlich einzustufen ist; diese Einstufung würde aber für spätere Fälle nicht mehr gelten, wenn in diesen Fällen keine neuen Techniken verwendet wurden und Anleitungen zum Umgang mit den Vorfällen bereits verfügbar sind.

Ein besonderes öffentliches Interesse an der zügigen Wiederherstellung der Sicherheit oder Funktionsfähigkeit des informationstechnischen Systems wird jedenfalls dann anzunehmen sein, wenn dessen Ausfall oder Beeinträchtigung spürbare Auswirkungen auf die Arbeitsfähigkeit von Stellen des Landes oder der Kommunen haben kann, z. B. wenn staatliche informationstechnische Systeme durch Angreifer kompromittiert sind und dadurch die Funktionsfähigkeit und Vertraulichkeit des Verwaltungshandelns nicht mehr sichergestellt ist.

Zu Abs. 3

In Abs. 3 ist der Umgang mit den personen- und kommunikationsbezogenen Daten geregelt, die das Zentrum für Informationssicherheit bei seiner Unterstützung erheben und verarbeiten muss. Zur Analyse eines Cyber-Angriffes müssen Logdaten der betroffenen Systeme und Netze analysiert werden, um den Angriff und die Aktivitäten des Täters nachvollziehen zu können. Üblicherweise verbleiben Täter nicht nur auf einem IT-System, sondern versuchen, sich im Netz des Angegriffenen auszubreiten. Die Aufklärung eines solchen Angriffs und die Bereinigung der infizierten Systeme können nur mittels umfassender Analyse der Log- und Kommunikationsdaten ermöglicht werden. Die personen- und kommunikationsbezogenen Daten, die das Zentrum für Informationssicherheit erhoben hat, sind nach Beendigung der Unterstützung zu löschen. Ausnahmen gelten nur dann, wenn die Daten mit Einwilligung der betroffenen Stelle oder entsprechend § 13 an eine andere Behörde zur Erfüllung ihrer gesetzlichen Aufgaben weitergegeben worden sind.

Zu Abs. 4

Nach Abs. 4 dürfen Informationen, von denen das Zentrum für Informationssicherheit Kenntnis erlangt, von diesem nur mit Einwilligung des Ersuchenden übermittelt werden, es sei denn, die weiterzugebenden Informationen lassen keine Rückschlüsse auf die Identität des Ersuchenden zu oder die Informationen können entsprechend § 13 übermittelt werden. Diese Regelung dient dem Schutz der Interessen der unterstützten Einrichtung. Sofern die Ergebnisse und Fakten bekannt würden, die bei der Analyse und Wiederherstellung der Sicherheit oder Funktionsfähigkeit der informationstechnischen Systeme erarbeitet wurden, könnten Angreifer daraus wertvolle Informationen für neue Angriffe auf die Sicherheit dieser Systeme erhalten. Außerdem setzt die Einschaltung des Zentrums für Informationssicherheit das Zutrauen der zu unterstützenden Stellen in die vertrauliche Behandlung des Vorfalles voraus. Da sich allerdings aus den erhobenen und verarbeiteten Daten auch für Strafverfolgungsbehörden, Polizei und Verfassungsschutzbehörden wichtige Erkenntnisse für ihre Aufgabenwahrnehmung ergeben können, gelten zur Übermittlung dieser Daten die Regelungen nach § 13. Satz 2 regelt ferner, dass zum Schutz des öffentlichen Interesses an der Bewältigung der hier in Rede stehenden Sicherheitsvorfälle, der hierfür zu treffenden Maßnahmen sowie der schutzwürdigen Interessen der ersuchenden Stelle oder Einrichtung ein Zugang für Dritte (beispielsweise auf Grundlage einer Informationsfreiheitsregelung) zu den Akten von Verfahren nach § 16 Abs. 1 ausgeschlossen wird. Soweit das Zentrum für Informationssicherheit andere Behörden unterstützt, bleibt das Recht auf Informationszugang gegenüber diesen Behörden unberührt.

Zu Abs. 5

Abs. 5 stellt klar, dass das Zentrum für Informationssicherheit nicht nur mit eigenen Mitteln unterstützen kann, sondern mit Zustimmung des Ersuchenden und auf dessen Kosten auch auf externe Unterstützung zurückgreifen darf. Gerade im Hinblick auf die notwendige Verarbeitung personenbezogener und dem Fernmeldegeheimnis unterfallender Daten ist diese Klarstellung erforderlich. Die Einbindung Dritter durch das Zentrum für Informationssicherheit kann in verschiedenen Formen geschehen. Zum einen kann das Zentrum für Informationssicherheit selbst externe Experten und Dienstleister mit der Wahrnehmung bestimmter Tätigkeiten beauftragen. Zum anderen kann es aber auch Dritte einbinden, die von der ersuchenden Stelle bestimmt wurden. Dies gilt insbesondere bei Vorfällen mit Spezial-IT, zu der im Zentrum für Informationssicherheit keine ausreichenden Fachkenntnisse für eine rasche Unterstützung vorliegen. Es kann mit den Dritten auch Daten austauschen. Hierbei sind die Vorgaben des Abs. 3 einzuhalten.

Anstelle der oder zusätzlich zur eigenen Unterstützung kann das Zentrum für Informationssicherheit betroffene Stellen auch auf qualifizierte Dritte verweisen, die bei der Wiederherstellung der Sicherheit der informationstechnischen Systeme herangezogen werden können. Die Auswahl des Dritten obliegt der betroffenen Stelle selbst.

Zu Abs. 6

Das Zentrum für Informationssicherheit kann die Hersteller der betroffenen informationstechnischen Systeme auffordern, bei der Analyse und Wiederherstellung der Sicherheit oder Funktionsfähigkeit mitzuwirken. Insbesondere wenn die IT-Sicherheit durch eine Sicherheitslücke in der verwendeten Hard- oder Software gefährdet wird, kann in erster Linie der Hersteller des jeweiligen Produktes schnell und nachhaltig zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit beitragen – etwa durch das zeitnahe Bereitstellen eines Sicherheitspatches. Aus Gründen der Verhältnismäßigkeit darf der Hersteller nicht zur kostenlosen Mitwirkung herangezogen werden, wenn die ersuchende Stelle Soft- oder Hardware einsetzt, deren Supportzeitraum bereits abgelaufen ist und der Hersteller das Ende des Supportzeitraumes rechtzeitig angekündigt hat. In diesem Fall hat die ersuchende Einrichtung dem Hersteller die entstandenen Kosten zu ersetzen. Die Mitwirkungspflicht des Herstellers bleibt davon unberührt.

Zu Abs. 7

In Abs. 7 wird dem Zentrum für Informationssicherheit die Möglichkeit eingeräumt, in begründeten Einzelfällen auch andere Einrichtungen bei der Analyse und Wiederherstellung der Sicherheit oder Funktionsfähigkeit ihrer informationstechnischen Systeme zu unterstützen. Ein begründeter Einzelfall liegt dann vor, wenn (neben den sonstigen Voraussetzungen des Abs. 1) ein vergleichbares öffentliches Interesse an der Behebung des Sicherheitsvorfalls besteht, auch wenn die betroffene Einrichtung nicht zu dem Adressatenkreis des Abs. 1 zählt. Zwar soll der Einsatz der MIRTs primär auf den Adressatenkreis des Abs. 1 beschränkt bleiben. Dem Zentrum für Informationssicherheit soll aber die Möglichkeit eröffnet werden, ausnahmsweise auch in anderen Fallkonstellationen tätig werden zu können. Dies kann etwa dann der Fall sein, wenn Anlagen oder Systeme von Organisationen betroffen sind, deren Ausfall oder Beeinträchtigung ähnlich weitreichende Auswirkungen hätte wie der Ausfall Kritischer Infrastrukturen. Durch die starke Vernetzung wirken sich erfolgreiche Angriffe nicht nur auf das unmittelbar angegriffene, sondern auf viele assoziierte Unternehmen aus. In Betracht kommen aber auch Einrichtungen, deren besondere politische, wirtschaftliche oder gesellschaftliche Bedeutung im Fall eines erheblichen Angriffs staatliches Eingreifen erforderlich erscheinen lässt. Daneben kann auch die besondere technische Qualität des Angriffs ein solches staatliches Eingreifen rechtfertigen, insbesondere sofern zu befürchten ist, dass ein gleichgelagerter Angriff auch Stellen nach § 1 bedroht.

Zu § 17 (Information der Betroffenen)

Im Hinblick auf die mit einer automatisierten Auswertung von personenbezogenen Daten verbundenen Grundrechtseingriffe sind an den Datenschutz hohe Anforderungen zu stellen. § 17 regelt daher die Informationspflichten bei den Maßnahmen nach §§ 8 bis 11. Die Vorschriften aus der Datenschutz-Grundverordnung und dem HDSIG bleiben daneben unberührt. Soweit das Zentrum für Informationssicherheit andere Maßnahmen, insbesondere nach § 7 Abs. 2, trifft, gelten die §§ 31, 32 HDSIG.

Zu Satz 1

Satz 1 stellt deswegen klar, dass die Betroffenen durch eine Benachrichtigung in die Lage versetzt werden müssen, ihre Rechte auf Auskunft, Berichtigung, Sperrung und Löschung gegenüber der verantwortlichen Stelle geltend machen zu können. Auch eine Schadensersatzforderung wegen rechtswidriger Datenverwendung können sie nur begründen, wenn sie von den Vorgängen Kenntnis erlangen.

Die Benachrichtigung hat auch zum frühestmöglichen Zeitpunkt zu erfolgen, in der Regel binnen weniger Tage. Sie kann nur dann unterbleiben, wenn die betroffene Person nicht identifiziert ist und die Identifizierung nicht oder nur mit unverhältnismäßigem Aufwand möglich wäre. Dies wird bei dem Absender eines Schadprogramms regelmäßig der Fall sein, da der Absender bereits technisch, etwa aufgrund von gefälschten Adressen, nicht ermittelbar ist.

Zu Satz 2

Satz 2 statuiert eine Ausnahme dieser unverzüglichen Benachrichtigungspflicht. Im Falle eines laufenden Straf- oder Disziplinarverfahrens oder bei Gefährdung der Tätigkeit der Verfassungsschutzbehörden kann auf eine Benachrichtigung verzichtet werden, wenn diese den Ermittlungszweck bzw. die Tätigkeit gefährden würde.

Zu Satz 3 und 4

Werden die Daten aufgrund der Befugnisse nach § 13 Abs. 2 für ein Strafverfahren oder für Zwecke der Verfassungsschutzbehörden weiterverwendet, erfolgt die Benachrichtigung durch die insoweit zuständigen Behörden nach Maßgabe der für diese geltenden Vorschriften der Strafprozessordnung, der Polizeigesetze oder der Verfassungsschutzgesetze. Soweit keine Regelung zur Benachrichtigung existiert, gelten die Vorschriften der Strafprozessordnung.

Zu § 18 (Meldepflichten)

§ 18 statuiert eine Meldepflicht, insbesondere bei Sicherheitslücken und Sicherheitsvorfällen, an das Zentrum für Informationssicherheit, soweit andere Vorschriften nicht entgegenstehen. Die Vorschriften können bspw. solche des Geheimschutzes sein. Auch privatrechtliche Verträge mit Dritten sind umfasst. Dies lässt die Meldepflicht jedoch nicht entfallen, sondern beschränkt sie auf ein Maß, dass Vertragsverletzungen vermieden werden. Das Zentrum für Informationssicherheit kann andere Behörden nur vor Bedrohungen warnen, wenn es in Kenntnis gesetzt wurde. Unvollständige Informationen tragen dabei mehr zur Informationssicherheit bei als keine Informationen. Die Inhalte der Meldepflicht und die Meldeprozesse sind in der Informationssicherheitsleitlinie zu konkretisieren.

Durch Satz 2 wird sichergestellt, dass die Stellen mit besonderer Rechtsstellung in ihrer Unabhängigkeit geschützt werden.

Zu § 19 (Dokumentationspflichten)

§ 19 bezieht sich auf Anordnungen zur nicht automatisierten oder direkt personenbezogenen Verarbeitung der nach §§ 7 ff. gewonnenen Daten. Diese Ausnahmefälle sind für eine nachträgliche Rechtmäßigkeitskontrolle und aus Gründen der Transparenz zu dokumentieren und nach § 14 Abs. 4 in die jährliche Aufstellung an die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten bzw. an die IT-Kontrollkommission der hessischen Justiz aufzunehmen.

Die Dokumentation darf für andere Zwecke als der nachträglichen Überprüfung der Rechtmäßigkeit der Verarbeitung nicht verwendet werden und ist zu löschen, wenn sie nicht mehr erforderlich ist, spätestens jedoch zum Ablauf des Kalenderjahres, das dem Jahr der Dokumentation folgt.

Zu § 20 (Einschränkung von Grundrechten)

Da §§ 7 bis 11, 13 und 16 Einschränkungen des Fernmeldegeheimnisses und des Rechts auf informationelle Selbstbestimmung vornehmen, ist diese Vorschrift gemäß Art. 19 Abs. 1 Satz 2 GG aufzunehmen.

Zu § 21 (Inkrafttreten, Außerkrafttreten)

Die Vorschrift regelt das Inkrafttreten und das Außerkrafttreten des Gesetzes.

Wiesbaden, 13. März 2023

Der Hessische Ministerpräsident
Boris Rhein

Der Hessische Minister
des Innern und für Sport
Peter Beuth