Bayerischer Landtag

17. Wahlperiode 11.07.2017 berichtigte **Drucksache*** 17/**17726**

Gesetzentwurf

der Staatsregierung

zur Errichtung des Landesamts für Sicherheit in der Informationstechnik

A) Problem

Digitale Infrastrukturen sind das Nervensystem unserer Informationsgesellschaft geworden. Das Internet verzeichnet mittlerweile über 2 Mrd. Nutzer, übermittelt täglich 144 Mrd. E-Mails und befördert pro Tag ein Datenvolumen von 1 Mrd. Gigabyte. Der volkswirtschaftliche Nutzen und die gesellschaftliche Bedeutung digitaler Infrastrukturen wachsen unaufhörlich. Zuverlässige und sichere IT-Infrastrukturen sind die Grundvoraussetzung für den Fortbestand unserer Standortvorteile sowie eines erfolgreichen und nachhaltigen Wegs in eine vernetzte Zukunft. Auch für die öffentliche Verwaltung ist eine sichere Informations- und Kommunikationstechnik unerlässlich; sie resultiert aus der Verpflichtung der Behörden gegenüber den Bürgern, Kommunen und der Wirtschaft, verantwortungsvoll bei der Verarbeitung von Daten vorzugehen.

Mit wachsender Bedeutung von IT-Infrastrukturen geht gleichlaufend eine höhere Bedrohungslage einher. Waren es früher häufig Jugendliche und junge Erwachsene, die im „Hacken“ von Sicherheitssystemen eine Herausforderung suchten, so können kritische Angriffe heute von praktisch jedermann gestartet werden. Ein großer Teil der gegenwärtigen Cyberattacken ist semiprofessionellen Einzeltätern und Gruppen zuzuschreiben, die ihre Angriffswerkzeuge im Rahmen krimineller Dienstleistungen im Internet („crime as a service“) erworben haben. Damit lassen sich fortgeschrittene Cyberangriffe konzipieren und durchführen. Aber auch professionelle kriminelle Organisationen und ausländische staatliche Institutionen stellen eine Bedrohung dar.

Professionelle Cyberattacken können gerade auf die staatliche IT große Auswirkungen haben. Das Staatsministerium der Finanzen, für Landesentwicklung und Heimat (StMFLH) sichert in seinem Rechenzentrumsverbund BayernServer und dem Bayerischen Behördennetz riesige und hochsensible Mengen an Daten, darunter:

- 5,6 Mio. Steuerfälle jährlich mit einem Steueraufkommen von rund 110 Mrd. Euro;
- Personaldaten von ca. 500.000 Mitarbeitern und Versorgungsempfängern einschließlich derer Gesundheitsdaten;
- Daten zu 10 Mio. Grundstücken und deren Eigentümern;
- 100.000 Förderanträge im Bereich der Landwirtschaft mit einem Fördervolumen von über 1,3 Mrd. Euro;
- Daten der Justiz, der Umweltverwaltung, etc.

Viele dieser Daten sind über das sog. Bayerische Behördennetz erreichbar, das der Freistaat Bayern betreibt. Dabei handelt es sich um eine abgeschlossene Infrastruktureinheit, die der Kommunikation der Behörden und Behördendienste untereinander dient. Mit fortschreitender Digitalisierung kommt dem Behördennetz eine immer größere

** Änderung in der Bezeichnung des Gesetzentwurfs*

Bedeutung zu. Viele Verwaltungsverfahren sind heute abhängig von einem reibungslosen Funktionieren dieser Komponente. Ein Ausfall steht dem Stillstand der Verwaltungsverfahren gleich. Umso wichtiger ist es, das Behördennetz ausreichend vor Gefahren zu schützen.

Aktuell gibt es täglich mehr als 40.000 Angriffsversuche auf diese Infrastruktur. Bislang kam es in Bayern dank professioneller IT-Sicherheit und Datensicherung zu keinen bedeutsamen Datenverlusten und Schäden. Erfolgreiche Angriffe auf das Netz des Deutschen Bundestags im Jahr 2015 zeigen aber, wie groß die Schäden und Auswirkungen für die Verwaltung sein können. Ziele sind dabei nicht nur die Großen, sondern auch Kleine wie die Verwaltungen mittelgroßer Städte.

Die Ereignisse der vergangenen Monate haben gezeigt, dass es Schwachstellen in fast allen Hard- und Softwareprodukten gibt. Absolute Sicherheit ist eine unerreichbare Fiktion. Altbewährte Anti-Virus-Software genügt schon lange nicht mehr, um die Systeme ausreichend zu schützen. Die Netzgrenzen wurden und werden auch in Zukunft überwunden. Der ewige Wettlauf zwischen Angreifern und Verteidigern ist nicht aufzuhalten.

Momentan befindet sich der Bereich der IT-Sicherheit in einem Wandel. Die Angriffe werden immer komplexer und können sich über Monate erstrecken (sog. Advanced Persistent Threats). In dem Wissen, dass es absolute Sicherheit für IT-Systeme nicht geben kann, ändert sich der methodische Ansatz. Neben Prävention setzen IT-Sicherheitsexperten verstärkt auf Detektion und Reaktion. Dabei wird das Verhalten eines entdeckten Angreifers, der erfolgreich in das Netz eingedrungen ist, über einen gewissen Zeitraum beobachtet (Profiling). Um seine Funktionsweise zu verstehen, darf er zunächst (in gewissem Umfang) seiner bestimmten Tätigkeit nachgehen. Erst wenn es zu einem Datenabfluss mit Kritikalität kommt, wird gegen den Angreifer vorgegangen. Aus den gewonnenen Erkenntnissen werden Abwehrsysteme neu konfiguriert und Fachleute lernen die komplexe Gesamtstruktur des Angriffs kennen. Es werden wertvolle Erfahrungen für zukünftige Angriffe gesammelt.

Die notwendigen Abwehr- und Sicherungsmaßnahmen können von den einzelnen Behörden kaum noch geleistet werden. IT-Sicherheit hat sich längst zu einem eigenen Spezialgebiet entwickelt, für das es eigene Fachleute braucht.

B) Lösung

Eine effektive und effiziente Abwehr der Bedrohungen kann von den einzelnen Behörden kaum noch geleistet werden. Die Bündelung von Kompetenzen an einer zentralen Stelle, dem Landesamt für Sicherheit in der Informationstechnik (LSI), schafft hier Abhilfe. Das LSI soll insbesondere dazu beitragen, die IT-Infrastruktur der Staatsverwaltung vor digitalen Bedrohungen zu schützen. Die Verteidigung der IT-Infrastruktur in einer Hand kommt letztlich allen angeschlossenen Behörden zugute.

Aufgabe des LSI wird sein:

- Abwehr von Gefahren für die Sicherheit der Informationstechnik der Staatsverwaltung, insbesondere des Bayerischen Behördennetzes;
- Sammlung, Auswertung und Analyse der neuesten Angriffsmethoden und Schadprogramme, um staatliche IT besser zu schützen und Aufklärungsarbeit für die kommunale IT zu leisten;
- Unterstützung von Behörden bei der Erstellung und Fortschreibung von IT-Sicherheitskonzepten;
- Prüfung und Bewertung der Sicherheit von Hard- und Software sowie IT-Sicherheitskonzepten;
- Überprüfung der Konformität von IT-Systemen der Staatsverwaltung mit den sicherheitstechnischen Anforderungen;
- Entwicklung von Mindeststandards für die IT-Sicherheit, insbesondere die Fortschreibung der bayerischen IT-Sicherheitsrichtlinien;
- Unterstützung, Beratung und Warnung von staatlichen und kommunalen Stellen und öffentlichen Unternehmen über Sicherheitsbedrohungen und -vorkehrungen;
- Unterstützung der Polizeien, Strafverfolgungsbehörden und des Verfassungsschutzes, wenn die Sicherheit der Informationstechnik oder die öffentliche Sicherheit durch Einsatz von Informationstechnik bedroht ist;
- Zusammenarbeit mit Bund und Ländern und Vertretung in Gremien zur IT-Sicherheit wie dem Deutschen CERT-Verbund.

Um diese Aufgaben erfüllen zu können, wird die Behörde mit Fachpersonal aus der IT-Sicherheit sowie modernster Hard- und Software ausgerüstet. Das bestehende Bayern-CERT (Computer Emergency Response Team) am Landesamt für Finanzen wird in das LSI integriert.

Klar abzugrenzen hiervon sind die Aufgaben der Staatsanwaltschaft, der Polizei und des Verfassungsschutzes, insbesondere der bei der Generalstaatsanwaltschaft Bamberg angesiedelten Zentralstelle Cybercrime Bayern, des Kompetenzzentrums Cybercrime am Landeskriminalamt und des Cyber-Allianz-Zentrums am Landesamt für Verfassungsschutz. Das LSI ist kein Ermittlungsorgan, sondern unterstützt diese bei der Strafverfolgung durch eine Datenübermittlung von Amts wegen und im Rahmen von Amtshilfeersuchen. Zur Vermeidung von Reibungsverlusten durch Schnittstellen und zur Erzielung von Synergieeffekten sind regelmäßige Absprachen und ein zielgerichteter Informationsaustauch auf operativer Ebene unabdingbar. Besteht auf Seiten der Staatsanwaltschaft die Möglichkeit zum Informationsaustausch bereits nach § 17 Nr. 3 des Einführungsgesetzes zum Gerichtsverfassungsgesetz, so muss für das LSI eine normative Regelung geschaffen werden.

Die Unterstützung und Beratung von Unternehmen aus der freien Wirtschaft wird aufgrund der fachlichen Überschneidung zur Wirtschaftsspionage weiter im Landesamt für Verfassungsschutz verbleiben.

C) Alternativen

Der Status quo könnte beibehalten werden. IT-Sicherheit wäre dann grundsätzlich alleinige Aufgabe jeder einzelnen Behörde, unterstützt durch einen kleinen Personalkörper beim Landesamt für Finanzen, dem Bayern-CERT. Ob Produkte, die eingesetzt werden, den Sicherheitsstandards genügen, würde weiterhin nur rudimentär geprüft werden. Auf die Einhaltung der IT-Sicherheitsrichtlinien müsste vertraut werden, ohne dass eine explizite Überprüfung stattfindet.

Mangels hinreichender datenschutzrechtlicher Regelungen wäre die Abwehr von Gefahren für die IT-Sicherheit erheblich erschwert. Moderne Abwehrmaßnahmen könnten nicht eingesetzt werden. Die Wahrscheinlichkeit eines erfolgreichen Angriffs auf das bzw. die Infiltration des Behördennetzes wäre signifikant erhöht.

D) Kosten

1. Staat

Die Errichtung des LSI ist mit einem entsprechenden Vollzugsaufwand verbunden. Dessen Umfang und damit die Höhe der Vollzugskosten sind maßgeblich von der zukünftigen Entwicklung der IT-Sicherheitslage abhängig und daher schwer zu beziffern. Entsprechend sind die nachfolgenden Zahlen Schätzwerte auf Basis der aktuellen Sachlage.

1. Die Sachkosten werden von 2017 bis 2020 unter Einbeziehung der voraussichtlichen Baumaßnahmen durchschnittlich 10,5 Mio. Euro p. a. betragen.
2. Die Aufgaben des LSI werden darüber hinaus – im Endausbau, der für das Jahr 2020 geplant ist – bis zu 200 Beschäftigte binden.

Insgesamt geht die Schätzung im Zeitraum bis zum Jahr 2020, in dem das LSI seine geplante Personalkörpergröße von 200 Beschäftigten erreicht haben soll, von Kosten in Höhe von ca. 60 Mio. Euro aus. Darin enthalten sind u. a.:

– Personalkosten (einschl. Aus- und Fortbildung von IT-Spezialisten),
– Planungs- und Entwicklungskosten,
– Gebäudekosten (Pacht, Baukosten einschl. Bewirtschaftung),
– Arbeitsplatzausstattung, Geschäftsbedarfe und Ausrüstung,
– Hard- und Software,
– Kosten für Spezialprodukte (Kryptoanalyse, Forensik etc.),
– Beratungsdienstleistungen in Spezialgebieten.

Soweit Kosten für die Entwicklung oder zentrale Beschaffung von IT-Sicherheitsprodukten entstehen, können diese durch Einsparungen bei anderen Stellen kompensiert werden, die entsprechende Produkte nicht mehr einzeln beschaffen müssen. Zusätzliches Einsparungspotenzial ergibt sich aus der Nutzung von Synergien und Mengenrabatten.

Das Gesetz enthält neue Informationspflichten für die Verwaltung, die den Informationsaustausch zu Sicherheitslücken und Sicherheitsvorkehrungen über das LSI kanalisieren. Schon heute informiert das Bayern-CERT, welches in das LSI integriert wird, die Behörden zeitnah zu aktuellen IT-Sicherheitsfragen. Dies wird nunmehr durch die Informationspflicht in Art. 11 Abs. 2 konkretisiert. Gegenüber den bisher bestehenden Strukturen, bei denen das LSI auf freiwillige bzw. zufällige Informationen angewiesen ist, schafft die Meldepflicht eine bessere Datenbasis und ermöglicht die zentrale Auswertung, Aufbereitung und Verteilung der IT-Sicherheitsinformationen an die übrigen Behörden.

Würde das LSI nicht wie vorgesehen als zentrale Stelle tätig, müssten im Zweifel alle Behörden parallel derartige Strukturen und die erforderlichen technischen Fähigkeiten und Fertigkeiten aufbauen, um auf dem für den Betrieb und Schutz ihrer internen Informationstechnik erforderlichen Wissensstand zu bleiben. Insofern wurde die kostengünstigste Regelungsalternative gewählt, die im höchstmöglichen Maß Synergieeffekte nutzt.

Die Integration des Bayern-CERT in das LSI wurde in obiger Kostenschätzung berücksichtigt.

Des Weiteren ergeben sich nicht bezifferbare Synergieeffekte u. a. aus der Prüfung von Hard- und Softwareprodukten, die nicht mehr durch verschiedene Stellen dezentral durchgeführt werden müssen, oder der Forensik von Schadsoftware.

Die Erhöhung der Sicherheit der staatlichen IT-Infrastruktur führt insgesamt zu Einsparungen bei der Behebung von Sicherheitsvorfällen. Durch die erhöhte Sicherheit werden weniger Systeme mit Schadprogrammen befallen, was den Aufwand zur Wiederherstellung und Bereinigung der Systeme mindert. Mangels übergreifender Statistiken und individuell geprägten Einzelaufwänden ist die Höhe der Einsparungen nicht bezifferbar.

Bei der Umsetzung der Maßnahmen ist dem Grundsatz der Wirtschaftlichkeit und Sparsamkeit Rechnung zu tragen (Art. 7 Bayerische Haushaltsordnung – BayHO).

2. Kommunen

Alle, auch nicht an das Behördennetz angeschlossene Kommunen können sich Beratung und Unterstützung durch das LSI einholen. Für die Leistungen werden unter Umständen Entgelte erhoben. Da die Leistungen auf freiwilliger Basis abgerufen werden, können sie nicht beziffert werden.

Es besteht eine Meldepflicht für Sicherheitsvorfälle oder andere relevante Ereignisse, wobei die Kommunen im Gegenzug sofort Meldungen über Gefahren erhalten. Die Erfüllung der Meldepflicht ist mit nur marginalen Aufwänden verbunden.

Das LSI kann technische Anforderungen vorgeben, an die sich die Kommunen halten müssen, soweit sie an das Behördennetz angeschlossen sind. Dies dient letztlich einem einheitlichen Sicherheitsniveau. Die Erfüllung der technischen Anforderungen des LSI wird in der Regel keine zusätzlichen Kosten auslösen. Die an das Behördennetz angeschlossenen Kommunen müssen bereits jetzt informationssicherheitstechnische Vorgaben erfüllen, um einen Zugang zum Behördennetz zu erhalten.

Ist eine Kommune an das Bayerische Behördennetz angeschlossen, so profitiert sie generell von einem hohen Schutzniveau und einem Eingreif- und Reaktionsteam, das im Falle von Sicherheitsvorfällen der Kommune schnelle Hilfe bieten kann. Folglich werden sich Einsparungen bei der Wiederherstellung und Bereinigung der IT-Systeme ergeben, da das LSI die Kommunen bei den IT-Sicherheitsvorfällen unterstützt. Mangels Statistiken über die Anzahl erfolgreicher Angriffe auf kommunaler Ebene ist eine Schätzung der Einsparungen nicht möglich.

Einsparungen ergeben sich des Weiteren durch die Unterstützung aller Kommunen bei der Erstellung ihrer IT-Sicherheitskonzepte, zu der sie gemäß Art. 11 Abs. 1 Satz 2 (Art. 8 Abs. 1 Satz 2 Bayerisches E-Government-Gesetz – BayEGovG in der Fassung vom 30.12.2015) i. V. m. Art. 19 Abs. 2 Satz 2 Nr. 3 BayEGovG ab 01.01.2019 verpflichtet sind.

Eine Ausgleichspflicht nach dem Konnexitätsprinzip ergibt sich aus den Regelungen grundsätzlich nicht. Bereits nach Art. 8 Abs. 1 BayEGovG a. F. ist die Sicherheit der informationstechnischen Systeme der Behörden im Rahmen der Verhältnismäßigkeit sicherzustellen.

Folglich ist für Kommunen, die nicht an das Behördennetz angeschlossen sind, keine Konnexität gegeben. Für sie sind die Leistungen des LSI freiwillig und die technischen Anforderungen nicht bindend.

Bei kommunalen Behörden, die an das Behördennetz angeschlossen sind, ist eine Ausgleichspflicht nach dem Konnexitätsprinzip ebenfalls nicht gegeben. Die Anbindung an das Behördennetz erfolgt freiwillig und ist nicht verpflichtend. Anschlussbedingungen für die Teilnahme am Behördennetz sind bereits jetzt zu erfüllen.

Einen Sonderfall stellen die Landratsämter mit ihrer Doppelfunktion als staatliche und kommunale Stelle dar. Müssen sie für die Erreichung der technischen Anforderungen des LSI Investitionen tätigen, so ist unter Umständen das Konnexitätsprinzip (Art. 83 Abs. 3 und 6 der Verfassung, Art. 53 Abs. 2 Landkreisordnung – LKrO) berührt. Es ist allerdings im Einzelfall zu prüfen, ob es sich um Anforderungen an die Erfüllung bestehender Aufgaben oder reine Verfahrens- und Organisationsregelungen handelt. Nur im ersteren Fall wäre Konnexität gegeben, wobei den Kosten Einsparungen entgegenzuhalten wären, da ein Eigeninteresse an einer hinreichenden IT-Sicherheit besteht.

3. Wirtschaft und Bürger

Kosten für die Wirtschaft können wie bislang bei Beantragung eines Sicherheitszertifikats entstehen. Da das Sicherheitszertifikat freiwillig ist, können es die Unternehmen von einer Wirtschaftlichkeitsbetrachtung abhängig machen, ob sie ihr Produkt einem Zertifizierungsverfahren mit der damit ggf. einhergehenden Kostenfolge unterziehen.

Auf Ersuchen werden Betreiber kritischer Infrastrukturen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen – insbesondere öffentliche Unternehmen – im Bereich der IT-Sicherheit unterstützt. In diesem Fall werden die Kosten in Form von Entgelten in Rechnung gestellt. Der Leistungsabruf ist freiwilliger Natur und richtet sich individuell nach Art und Umfang, weshalb eine Kostenschätzung nicht möglich ist.

Im Bereich der elektronischen Rechnungen wird der Begriff des öffentlichen Auftraggebers in Art. 5 Abs. 2 BayEGovG geändert. Dies ist der Novelle des Gesetzes gegen Wettbewerbsbeschränkung geschuldet, die auf den Richtlinien 2014/25/EU und 2014/55/EU beruht. Aus diesem Grund ist eine Ausgleichspflicht nach dem Konnexitätsprinzip nicht gegeben.

Auswirkungen auf die Einzelpreise und das Preisniveau, insbesondere auf das Verbraucherpreisniveau, sind von diesem Gesetz nicht zu erwarten.

Durch das Gesetz werden keine Informationspflichten eingeführt oder abgeschafft.

Bayerischer Landtag
17. Wahlperiode

Drucksache 17/**17726**
11.07.2017

Gesetzentwurf

zur Errichtung des Landesamts für Sicherheit in der Informationstechnik

§ 1
Änderung des Bayerischen E-Government-Gesetzes

Das Bayerische E-Government-Gesetz (BayEGovG) vom 22. Dezember 2015 (GVBl. S. 458, BayRS 206-1-F) wird wie folgt geändert:

1. Dem Art. 1 wird folgende Überschrift vorangestellt:

   „Teil 1
   Elektronische Verwaltung".

2. In Art. 1 Abs. 1 und 2 Satz 1 und 2 werden jeweils die Wörter „Dieses Gesetz" durch die Wörter „Dieser Teil" ersetzt.

3. In Art. 3 Abs. 2 wird die Angabe „Art. 9 Abs. 2" durch die Angabe „Art. 8 Abs. 2" ersetzt.

4. Art. 5 Abs. 2 Satz 1 wird wie folgt gefasst:

   „[1]Auftraggeber im Sinn von § 98 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) stellen den Empfang und die Verarbeitung elektronischer Rechnungen sicher, soweit für sie gemäß § 159 GWB eine Vergabekammer des Freistaates Bayern zuständig ist."

5. Art. 8 wird aufgehoben.

6. Der bisherige Art. 9 wird Art. 8.

7. Der bisherige Art. 9a wird aufgehoben.

8. Nach Art. 8 wird folgender Teil 2 eingefügt:

   „Teil 2
   Sicherheit in der Informationstechnik

   Kapitel 1
   Allgemeine Vorschriften

   Art. 9
   Landesamt für
   Sicherheit in der Informationstechnik

   [1]Es besteht ein Landesamt für Sicherheit in der Informationstechnik (Landesamt). [2]Es ist dem Staatsministerium der Finanzen, für Landesentwicklung und Heimat unmittelbar nachgeordnet.

   Art. 10
   Aufgaben

   (1) Das Landesamt hat

   1. Gefahren für die Sicherheit der Informationstechnik an den Schnittstellen zwischen Behördennetz und anderen Netzen abzuwehren,
   2. die staatlichen und die sonstigen an das Behördennetz angeschlossenen Stellen bei der Abwehr von Gefahren für die Sicherheit in der Informationstechnik zu unterstützen,
   3. sicherheitstechnische Mindeststandards an die Informationstechnik für die staatlichen und die sonstigen an das Behördennetz angeschlossenen Stellen zu entwickeln,
   4. die Einhaltung der Mindeststandards nach Nr. 3 zu prüfen,
   5. alle für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik erforderlichen Informationen zu sammeln und auszuwerten und die staatlichen und die sonstigen an das Behördennetz angeschlossenen Stellen unverzüglich über die sie betreffenden Informationen zu unterrichten,
   6. die zuständigen Aufsichtsbehörden über Informationen, die es als Kontaktstelle im Rahmen des Verfahrens zu § 8b des BSI-Gesetzes erhalten hat, zu unterrichten.

   (2) Auf Ersuchen kann das Landesamt staatliche und kommunale Stellen, öffentliche Unternehmen, Betreiber kritischer Infrastrukturen und weitere Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen beraten und unterstützen.

   (3) Auf Ersuchen kann das Landesamt die Polizei, die Strafverfolgungsbehörden und das Landesamt für Verfassungsschutz bei der Wahrnehmung ihrer gesetzlichen Aufgaben technisch unterstützen, insbesondere bei der Durchführung von technischen Untersuchungen oder der Datenverarbeitung.

   (4) Für die Kommunikationstechnik des Landtags, der Gerichte, des Obersten Rechnungshofs und des Landesbeauftragten für den Datenschutz ist das Landesamt nur zuständig, soweit sie an das Behördennetz angeschlossen sind oder Dienste im Sinn des Art. 8 Abs. 2 und 3 nutzen.

Art. 11
Behördenübergreifende Pflichten

(1) [1]Die Sicherheit der informationstechnischen Systeme der Behörden, die in den Anwendungsbereich des Teils 1 fallen, ist im Rahmen der Verhältnismäßigkeit sicherzustellen. [2]Die Behörden treffen zu diesem Zweck angemessene technische und organisatorische Maßnahmen im Sinn des Art. 7 des Bayerischen Datenschutzgesetzes (BayDSG) und erstellen die hierzu erforderlichen Informationssicherheitskonzepte.

(2) Werden staatlichen oder sonstigen an das Behördennetz angeschlossenen Stellen Informationen bekannt, die zur Abwehr von Gefahren für die Sicherheit in der Informationstechnik von Bedeutung sind, unterrichten diese das Landesamt und ihre jeweilige oberste Dienstbehörde unverzüglich hierüber, soweit andere Vorschriften oder Vereinbarungen mit Dritten nicht entgegenstehen.

(3) Die staatlichen und die sonstigen an das Behördennetz angeschlossenen Stellen unterstützen das Landesamt bei Maßnahmen nach Art. 10 Abs. 1 Nr. 1, 2, 4 und 5, soweit keine Vorschriften entgegenstehen.

Kapitel 2
Befugnisse

Art. 12
Abwehr von Gefahren für die Informationstechnik

(1) [1]Das Landesamt kann zur Erfüllung seiner Aufgaben gegenüber staatlichen und an das Behördennetz angeschlossenen Stellen die nötigen Anordnungen treffen oder Maßnahmen ergreifen, um Gefahren für die Informationstechnik etwa durch Schadprogramme oder programmtechnische Sicherheitslücken, unbefugte Datennutzung oder unbefugte Datenverarbeitung durch Dritte zu erkennen und abzuwehren. [2]Das umfasst insbesondere auch die dazu nötige Datennutzung und -verarbeitung. [3]Die Sätze 1 und 2 gelten nicht für die vom Behördennetz getrennte Informationstechnik des Landesamts für Verfassungsschutz.

(2) Das Landesamt kann hierzu, soweit dies erforderlich ist,

1. Protokolldaten, die beim Betrieb von Informationstechnik des Landes oder der an das Behördennetz angeschlossene Stellen anfallen, erheben und automatisiert auswerten,
2. die an den Schnittstellen zwischen dem Behördennetz und anderen Netzen anfallenden Daten erheben und automatisiert auswerten.

Art. 13
Untersuchung der Sicherheit
in der Informationstechnik

(1) [1]Das Landesamt kann zur Erfüllung seiner Aufgaben nach Art. 10 Abs. 1 Nr. 1 und 4 die Sicherheit der Informationstechnik staatlicher und an das Behördennetz angeschlossener Stellen untersuchen und bewerten. [2]Über das Ergebnis erstellt das Landesamt einen Bericht, der der untersuchten Stelle zur Verfügung gestellt wird.

(2) Das Landesamt kann auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte und Systeme untersuchen.

Art. 14
Mindeststandards

[1]Das Landesamt erarbeitet Mindeststandards für die Sicherheit der Informationstechnik. [2]Das zuständige Staatsministerium kann im Einvernehmen mit den weiteren Staatsministerien und der Staatskanzlei diese Mindeststandards ganz oder teilweise als allgemeine Verwaltungsvorschriften erlassen. [3]Für Landratsämter und die an das Behördennetz angeschlossenen nicht staatlichen Stellen gelten die Mindeststandards für die Teilnahme am Behördennetz.

Art. 15
Warnungen

(1) Das Landesamt kann Warnungen zu Gefahren für die Sicherheit in der Informationstechnik, insbesondere zu Sicherheitslücken, Schadprogrammen oder unbefugten Datenzugriffen aussprechen und Sicherheitsmaßnahmen empfehlen.

(2) [1]Stellen sich die von der Behörde an die Öffentlichkeit gegebenen Informationen im Nachhinein als falsch oder die zu Grunde liegenden Umstände als unrichtig wiedergegeben heraus, so ist dies unverzüglich öffentlich bekannt zu machen, sofern der betroffene Wirtschaftsbeteiligte dies beantragt oder dies zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist. [2]Diese Bekanntmachung soll in derselben Weise erfolgen, in der die Information der Öffentlichkeit ergangen ist.

Kapitel 3
Datenschutz

Art. 16
Datenspeicherung und -auswertung

(1) [1]Sofern nicht die nachfolgenden Absätze eine weitere Verwendung gestatten, muss eine automatisierte Auswertung der Daten durch das Landesamt unverzüglich erfolgen und müssen die Daten nach erfolgtem Abgleich sofort und spurlos gelöscht werden. [2]Daten, die weder dem Fernmeldegeheimnis unterliegen noch Personenbezug aufweisen, sind von den Verwendungsbeschränkungen dieser Vorschrift ausgenommen.

(2) [1]Protokolldaten nach Art. 12 Abs. 2 dürfen über den für die automatisierte Auswertung erforderlichen Zeitraum hinaus, längstens jedoch für drei Monate, gespeichert werden, soweit tatsäch-

liche Anhaltspunkte bestehen, dass die Daten erforderlich sein können

1. für den Fall der Bestätigung eines Verdachts nach Abs. 4 Satz 1 Nr. 2 zur Abwehr von Gefahren für die Informationstechnik oder
2. zur Verhütung, Unterbindung oder Verfolgung damit zusammenhängender Straftaten.

[2]Die Daten sind im Gebiet der Europäischen Union zu speichern. [3]Durch organisatorische und technische Maßnahmen nach dem Stand der Technik ist sicherzustellen, dass eine Auswertung der nach diesem Absatz gespeicherten Daten nur automatisiert erfolgt. [4]Die Daten sind zu pseudonymisieren, soweit dies automatisiert möglich ist. [5]Soweit hierzu die Wiederherstellung des Personenbezugs pseudonymisierter Daten erforderlich ist, muss diese durch die Behördenleitung angeordnet werden. [6]Die Entscheidung ist zu dokumentieren. [7]Eine nicht automatisierte Auswertung oder eine personenbezogene Verwendung ist nur nach Maßgabe der nachfolgenden Absätze zulässig.

(3) [1]Für die Datenverarbeitung von Inhaltsdaten gilt Abs. 2 mit der Maßgabe, dass eine Speicherung für höchstens zwei Monate zulässig ist, die Speicherung und Auswertung von der Behördenleitung und einem weiteren Bediensteten des Landesamts mit der Befähigung zum Richteramt angeordnet sind und dies zum Schutz der technischen Systeme unerlässlich ist. [2]Die Anordnung gilt längstens für zwei Monate; sie kann verlängert werden.

(4) [1]Eine über die Abs. 2 und 3 hinausgehende Verarbeitung und Nutzung der Protokoll- und Inhaltsdaten ist nur zulässig,

1. wenn bestimmte Tatsachen den Verdacht begründen, dass die Daten Gefahren für die Informationstechnik, etwa durch Schadprogramme oder programmtechnische Sicherheitslücken, unbefugte Datennutzung oder unbefugte Datenverarbeitung, enthalten oder Hinweise auf solche Gefahren geben können und soweit die Datenverarbeitung erforderlich ist, um den Verdacht zu bestätigen oder zu widerlegen,
2. wenn sich der Verdacht nach Nr. 1 bestätigt und soweit dies zur Abwehr von Gefahren für die Informationstechnik erforderlich ist oder
3. wenn bei einer Verarbeitung oder Nutzung der Daten ein nach Art. 17 Abs. 2 zu übermittelndes Datum festgestellt wird.

[2]Werden Daten, welche die richterliche Unabhängigkeit berühren, nach diesem Absatz verarbeitet, ist der jeweils zuständigen obersten Dienstbehörde unverzüglich zu berichten. [3]Berührt die Datenverarbeitung die Aufgabenwahrnehmung anderer unabhängiger Stellen oder ein Berufs- oder besonderes Amtsgeheimnis, ist die betroffene Stelle unverzüglich zu unterrichten. [4]Die jeweiligen Stellen nach den Sätzen 2 und 3 können vom Landesamt Auskunft über die Verarbeitung von Daten nach diesem Absatz verlangen.

(5) [1]Soweit möglich, ist bei der Datenverarbeitung technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. [2]Werden Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt, dürfen diese nicht verwendet werden und sind unverzüglich zu löschen; die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. [3]Dies gilt auch in Zweifelsfällen.

Art. 17
Datenübermittlung

(1) Das Landesamt übermittelt Daten nach Art. 16 Abs. 2 bis 4 an die für den Betrieb der Informations- und Kommunikationstechnik verantwortlichen Stellen, wenn und soweit dies zur Abwehr oder Beseitigung von Gefahren für die Vertraulichkeit, Verfügbarkeit und Integrität der Daten in der Informations- und Kommunikationsinfrastruktur des Landes erforderlich ist.

(2) [1]Das Landesamt soll Daten nach Art. 16 Abs. 2 bis 4 unverzüglich übermitteln

1. an die Sicherheitsbehörden und Polizei zur Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person sowie zur Verhütung und Unterbindung von in Nr. 2 genannten Straftaten und
2. an die Strafverfolgungsbehörden zur Verfolgung einer Straftat,
   a) soweit die Tatsachen, aus denen sich eine Gefahr für die Informationstechnik oder der diesbezügliche Verdacht ergibt, den Verdacht einer Straftat begründen oder
   b) soweit bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 der Strafprozessordnung bezeichnete Straftat begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht oder durch eine Straftat vorbereitet hat.

[2]Näheres regeln Verwaltungsvorschriften, die das Staatsministerium der Finanzen, für Landesentwicklung und Heimat im Einvernehmen mit dem Staatsministerium des Innern, für Bau und Verkehr und dem Staatsministerium der Justiz festlegt."

9. Nach Art. 17 wird folgende Überschrift eingefügt:

„Teil 3
Schlussbestimmungen".

10. Nach der Überschrift des Teils 3 wird folgender Art. 18 eingefügt:

„Art. 18
Einschränkung von Grundrechten

Die Art. 12, 16 und 17 schränken das Fernmeldegeheimnis (Art. 10 des Grundgesetzes, Art. 112 der Verfassung) ein."

11. Der bisherige Art. 10 wird Art. 19 und wird wie folgt geändert:

a) In der Überschrift wird das Wort „Schlussvorschriften" durch die Wörter „Experimentierklausel, Inkrafttreten" ersetzt.

b) In Abs. 2 Satz 2 Nr. 3 werden die Wörter „Art. 8 Abs. 1 Satz 2 am 1. Januar 2018" durch die Wörter „Art. 11 Abs. 1 Satz 2 am 1. Januar 2019" ersetzt.

c) Abs. 3 wird aufgehoben.

§ 2
Änderung des Bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen

In Art. 122 Abs. 5 des Bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen (BayEUG) in der Fassung der Bekanntmachung vom 31. Mai 2000 (GVBl. S. 414, 632, BayRS 2230-1-1-K), das zuletzt durch § 3 des Gesetzes vom … Juli 2017 (GVBl. S. …) geändert worden ist, werden die Wörter „Art. 9 Abs. 2 und 3 sowie Art. 10 Abs. 1" durch die Wörter „Art. 8 Abs. 2 und 3 sowie Art. 19 Abs. 1" ersetzt.

§ 3
Änderung der Bayerischen Barrierefreie Informationstechnik-Verordnung

In § 3 Abs. 1 Satzteil vor Nr. 1 der Bayerischen Barrierefreie Informationstechnik-Verordnung (BayBITV) vom 8. November 2016 (GVBl. S. 314, BayRS 206-1-1-F) wird die Angabe „Art. 9 Abs. 3" durch die Angabe „Art. 8 Abs. 3" ersetzt.

§ 4
Inkrafttreten

Dieses Gesetz tritt am ……..… in Kraft.

Begründung:

A. Allgemeines

I. Ausgangslage

Das Bayerische E-Government-Gesetz ist zum 30.12.2015 in Kraft getreten und regelt im Wesentlichen die Vorgaben zur elektronischen Verwaltung. Die Bedrohungslage für die elektronische Verwaltung hat sich in jüngster Zeit stark erhöht. Daher hat die Staatsregierung beschlossen, eine zentrale Behörde zur Abwehr von Gefahren für die Sicherheit der Informationstechnik der Staatsverwaltung zu schaffen. Neben redaktionellen Änderungen sollen die Aufgaben des neu zu gründenden Landesamts für Sicherheit in der Informationstechnik (LSI) in das Bayerische E-Government-Gesetz aufgenommen werden.

Ein Landesamt für Sicherheit in der Informationstechnik kann dem Erhalt der Leistungsfähigkeit und der Effizienz der Verwaltung dienen. Darüber hinaus leistet es einen wesentlichen Beitrag zur Verwaltungsmodernisierung. Die Sicherung der behördlichen Netze vor Angriffen ist wesentlich für das Funktionieren eines Staates. Angriffe auf die Infrastruktur können Teile der Verwaltung de facto zusammenbrechen lassen und damit dessen Handlungsfähigkeit erheblich schwächen. Das unberechtigte Abziehen von staatlichen oder kommunalen Informationen stellt neben der Verletzung des Rechts auf informationelle Selbstbestimmung einer Person auch ein Risiko für die administrative Grundordnung des Staates dar.

Verlässliche IT-Sicherheit erfordert einen umfassenden Ansatz, der technische und organisatorische Umsetzungsmaßnahmen, finanzielle Investitionen und rechtliche Regelungen verbindet.

II. Gegenstand des Gesetzentwurfs

Das Gesetz über das Landesamt für Sicherheit in der Informationstechnik regelt die Errichtung des Landesamts für Sicherheit in der Informationstechnik sowie dessen Befugnisse. Es übernimmt folgende Aufgaben:

– Abwehr von Gefahren für die Sicherheit der Informationstechnik der Staatsverwaltung, insbesondere des Bayerischen Behördennetzes;
– Zentrale Sammlung, Analyse und Auswertung zu Sicherheitslücken und Schadprogrammen;
– Zurverfügungstellung der gewonnenen Erkenntnisse für andere Stellen;
– Prüfung und Bewertung der Sicherheit von Hard- und Software und IT-Sicherheitskonzepten der Staatsverwaltung;
– Überprüfung der Konformität von IT-Systemen der Staatsverwaltung mit den sicherheitstechnischen Anforderungen;
– Aufstellung von Mindeststandards an die IT-Sicherheit und Fortschreibung der bayerischen IT-Sicherheitsrichtlinien;

– Beratung und Warnung von staatlichen und kommunalen Stellen und öffentlichen Unternehmen vor Schadprogrammen und Schutzvorkehrungen;
– Unterstützung der Polizeien, Strafvermittlungsbehörden und des Verfassungsschutzes, wenn die Sicherheit der Informationstechnik oder die öffentliche Sicherheit durch den Einsatz von Informationstechnik bedroht ist.

Für die aufgelisteten Aufgaben sind Rechtsgrundlagen erforderlich. Insbesondere der Schutz des Bayerischen Behördennetzes bedarf einer umfangreichen Analyse des Datenverkehrs an den Übergängen zum Internet. Anders kann eine hinreichende Sicherheit des Netzes nicht erreicht werden. Dabei müssen Verkehrs-, Bestands- und Inhaltsdaten automatisiert nach Angriffen durchsucht werden. Allerdings unterliegt eine entsprechende Regelung wegen der mit ihr verbundenen Grundrechtseingriffe strengen Anforderungen. Sie ist auf das absolut Notwendige zu beschränken. Hinsichtlich der Datensicherheit muss ein hoher Standard normenklar und verbindlich vorgegeben werden. Eine umfangreiche datenschutzrechtliche Vorschrift, die die Vorgaben des Bundesverfassungsgerichts und des Bundesgerichtshofs erfüllt, ist hierfür unerlässlich.

Das LSI soll als zentrale Meldestelle alle sicherheitsrelevanten Vorfälle bei den Behörden sammeln und auswerten. Im Gegenzug werden die Behörden unverzüglich über neue Bedrohungen gewarnt. Die Behörden werden verpflichtet, IT-Sicherheitsvorfälle zu melden um schnelle Reaktionszeiten zu gewährleisten. Darüber hinaus ist es die zentrale Kontaktstelle des Freistaates Bayern im Bereich der Kritischen Infrastrukturen. Das LSI nimmt die Meldungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) entgegen und gibt sie gegebenenfalls entsprechend aufbereitet an die zuständigen Aufsichtsbehörden weiter.

Neben den staatlichen Behörden kann das LSI auch Warnungen vor Sicherheitslücken, Schadprogrammen oder erfolgten Hacking-Attacken an kommunale Stellen oder öffentliche Unternehmen ausgeben. Dabei hat es jedoch die Interessen der betroffenen Hersteller zu wahren. Falls die Informationen auch Bürgern oder privaten Unternehmen dienlich sein können, so ist darüber hinaus eine Veröffentlichung denkbar.

Vor dem Einsatz von Hard- und Software in Behörden sollte diese auf Sicherheitslücken, Angreifbarkeit etc. geprüft werden. Diese Aufgabe übernimmt zukünftig das LSI, da staatliche Behörden diese Aufgabe mangels Ressourcen und/oder Kompetenzen nicht im erforderlichen Umfang wahrnehmen können.

Die IT-Sicherheitsrichtlinien werden zukünftig durch das LSI fortgeschrieben. Der IT-Beauftragte kann sie im Benehmen mit dem Rat der Ressort-CIOs zu allgemeinen Verwaltungsvorschriften erklären.

B. Zu den einzelnen Vorschriften

Zu § 1

Änderung des Bayerischen E-Government-Gesetzes

Zu Nrn. 1 und 2:

Im Zuge der Einführung von Vorschriften, die allein das LSI betreffen, wird das BayEGovG in drei Teile gegliedert. Der erste Teil regelt die elektronische Verwaltung, der zweite die Sicherheit in der Informationstechnik und der dritte die Schlussbestimmungen. Entsprechend wird der Anwendungsbereich von Art. 1 BayEGovG angepasst.

Zu Nr. 3:

Redaktionelle Änderung.

Zu Nr. 4:

Die Vorschrift wird an die neue Fassung des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) angepasst. Mit einher geht eine Erweiterung des Begriffs des öffentlichen Auftraggebers, der auf der Richtlinie 2014/25/EU beruht. Diese ist wiederum vom Anwendungsbereich der Richtlinie 2014/55/EU über die elektronische Rechnungsstellung bei öffentlichen Aufträgen umfasst.

Zu Nr. 5:

Die Regelung des Art. 8 Abs. 1 BayEGovG a. F. wird aus rechtssystematischen Gründen in den Teil zur Sicherheit in der Informationstechnik – dort Art. 11 Abs. 1 BayEGovG – verschoben.

Das Bayern-CERT wird Teil des LSI. Entsprechend werden die Aufgaben im zweiten Teil des BayEGovG neu geregelt und Art. 8 Abs. 2 BayEGovG a. F. kann entfallen.

Zu Nr. 7:

Art. 9a BayEGovG diente lediglich der Änderung von Rechtsvorschriften anderer Gesetze und kann nunmehr entfallen.

Zu Nr. 8:

Im Anschluss an Art. 8 BayEGovG werden die Art. 9 bis 17 eingefügt, die die Sicherheit in der Informationstechnik regeln.

Die Begriffsbestimmungen dieses Teils wurden in Anlehnung an die Begrifflichkeiten des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik gewählt.

Zu Art. 9
Landesamt für Sicherheit in der Informationstechnik

Die Vorschrift regelt die Errichtung des Landesamts für Sicherheit in der Informationstechnik. Dienstsitz ist Nürnberg. Außenstellen werden in Würzburg und Neustadt a. d. Saale bestehen.

Zu Art. 10
Aufgaben

Art. 10 regelt die Aufgaben des LSI.

Zu Abs. 1

Zu Nr. 1

Aufgabe des LSI ist die Abwehr von Gefahren für die Sicherheit in der Informationstechnik an den Schnittstellen zwischen Behördennetz und anderen Netzen. Schwerpunkt des LSI wird der Schutz des Bayerischen Behördennetzes sein, das täglich Tausenden von Angriffen ausgesetzt ist. Zentrale Bedeutung hat hier die Überwachung des zentralen Internetübergangs, dem größten Einfallstor für Angriffe aus dem Internet. Erforderlich ist sowohl präventives als auch repressives Vorgehen. Dem LSI stehen hierzu die Befugnisse des zweiten Abschnitts zur Verfügung.

Zu Nr. 2

Das LSI kann staatliche und an das Behördennetz angeschlossene Stellen bei der Abwehr von Gefahren für die Sicherheit in der Informationstechnik unterstützen. Die Vorschrift ist aufgrund der schnelllebigen Entwicklung der Informationstechnologie bewusst weit gefasst, um eine Amtshilfe durch das LSI in möglichst vielen und auch zukünftig neuen Bereichen zuzulassen.

Die Aufgabe beschränkt sich bewusst auf die reine Unterstützungsleistung. Die Verantwortlichkeit der Behörden für die Sicherheit ihrer IT soll nicht auf das LSI übergeben.

Als Unterstützung kann das LSI bspw. einzelne Hard- und Softwarekomponenten (etwa Betriebssysteme, Textverarbeitungsprogramme oder Netzwerkkomponenten) auf Sicherheitsrisiken überprüfen. Damit entlastet es die IT-Stellen der einzelnen Behörden, die bereits geprüfte Produkte nicht erneut auf Einsatztauglichkeit in ihrem Bereich untersuchen müssen. Auch entfallen unnötige Mehrfachprüfungen, da Standardprodukte an einer zentralen Stelle geprüft werden.

Im Fall eines Angriffs kann ein Eingreif- und Reaktionsteam – eventuell sogar durch Vor-Ort-Service – bei der Abwehr mit seiner Fachexpertise behilflich sein.

Eine weitere Unterstützung kann in der Erteilung von Sicherheitszertifikaten liegen. Mit Genehmigung des originären Ausstellers des Sicherheitszertifikats, dass das LSI nach Vorliegen der Voraussetzungen hierzu befugt, kann es ein Zertifikat (bspw. Zertifizierung nach BSI-Grundschutz oder ISIS 12) verleihen. Möglich ist es auch, eigene, sog. LSI-Zertifikate, zu verleihen, die die Einhaltung von Sicherheitsrichtlinien oder bestimmten Standards bestätigen. Auch die Aufstellung eines eigenen LSI-Anforderungskatalogs ist denkbar.

Darüber hinaus kann das LSI als zentrale Stelle für IT-Sicherheit in der Verwaltung Verfahren und Geräte entwickeln, bereitstellen und betreiben, die staatlichen und an das Behördennetz angeschlossenen Einrichtungen zur Verfügung gestellt werden. In erster Linie wird es sich dabei um Krypto- und Sicherheitsmanagementsysteme handeln, die behördenübergreifend zum Einsatz kommen. Solche Systeme verschlüsseln u. a. die staatliche Kommunikation für Angreifer. Das LSI kann Schlüssel vergeben und Public Key Infrastructures (PKI) zur Verteilung der Schlüssel betreiben. Auch sorgt das LSI dafür, dass die eingesetzten Anwendungen immer dem aktuellen Stand der Technik entsprechen. Werden diese Verfahren als Basisdienste nach Art. 8 Abs. 2 BayEGovG oder zentrale Dienste nach Art. 8 Abs. 3 BayEGovG bereitgestellt, können Sie sogar von allen staatlichen und kommunalen Behörden genutzt werden.

Zu Nr. 3

Das LSI muss ein für die staatliche informationstechnische Verwaltungsinfrastruktur angemessenes Sicherheitsniveau durchsetzen können. Hierfür kann es Mindeststandards entwickeln, die gemäß Art. 14 Abs. 1 Satz 2 BayEGovG als Verwaltungsvorschriften festgelegt werden können. Unter die Mindeststandards fallen auch die bereits gültigen IT-Sicherheitsrichtlinien der Staatsregierung.

Zu Nr. 4

Das LSI prüft, ob die eingesetzten informationstechnischen Systeme, Komponenten, Prozesse und IT-Sicherheitskonzepte der Staatsverwaltung und der an das Behördennetz angeschlossenen Stellen die sicherheitstechnischen Mindeststandards erfüllen. Hierfür hat es gemäß Art. 13 Abs. 1 BayEGovG ein Prüfungsrecht.

Zu Nr. 5

Das LSI sammelt zentral Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen. Dabei beschäftigt es sich nicht nur mit aktuellen Ereignissen, auch Informationen über Zukunftstechnologien in der Branche werden untersucht und verprobt. Die Erkenntnisse stellt es den staatlichen und den an das Behördennetz angeschlossenen Stellen zur Verfügung. In Betracht kommen staatliche und kommunale Stellen, aber auch nationale oder internationale Einrichtungen wie das BSI, das European Cybercrime Center oder die Europäische Agentur für Netz- und Informationssicherheit können über neue Erkenntnisse informiert werden.

Schnelle Reaktionszeiten sind bei der Abwehr von Schadsoftware unabdingbar. Über aktuelle Bedrohungen hat es daher unverzüglich die betroffenen staatlichen und sonstige an das Behördennetz angeschlossenen Stellen zu unterrichten. Damit soll sichergestellt werden, dass diese rechtzeitigen Abwehrmaßnahmen gegen neue oder bevorstehende Bedrohungen ergreifen können.

Als Annex zur Informationspflicht von Behörden kann das LSI darüber hinaus seine Erkenntnisse veröffentlichen. Dies ist sinnvoll, wenn die Informationen auch für Bürger, private Unternehmen oder sonstige Organisationen von Wichtigkeit oder Interesse sein können. Hierbei sollten die Informationen unter Berücksichtigung des Empfängerkreises durch klare und verständliche Handlungsempfehlungen über aktuelle Risiken und Bedrohungen und mögliche Abwehrmaßnahmen bestechen und über einfache Kanäle (bspw. soziale Medien) verteilt werden. Derartige Hinweise bedürfen keiner besonderen gesetzlichen Ermächtigung; Warnungen hingegen richten sich nach Art. 15.

Zu Nr. 6

Das LSI übernimmt die Aufgabe als zentrale Kontaktstelle gemäß § 8b Abs. 2 Nr. 4 Buchst. c Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG). Die vom BSI erhaltenen Informationen gibt es an die Aufsichtsbehörden weiter. Ziel ist es, die Meldungen zu kanalisieren und dadurch die Gesamtsicherheitslage besser zu überblicken. Auch können die Informationen für andere Aufsichtsbehörden, die zunächst nicht direkt betroffen zu sein scheinen, von Nutzen sein. Je nach Komplexität der Meldung bereitet das LSI die Informationen des BSI für die Aufsichtsbehörde derart auf, dass auch technische Laien die Kritikalität der Informationen beurteilen können. In Einzelfällen kann eine unverzügliche Weitergabe notwendig sein.

Zu Abs. 2

Große Bedeutung kommt der Beratung und Warnung von staatlichen und kommunalen Stellen, öffentlichen Unternehmen, Betreibern kritischer Infrastrukturen und weiteren Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen zu. Auf Ersuchen können diese bei Fragen der IT-Sicherheit eingehend vom LSI unterstützt und beraten werden.

Ziel der Regelung ist insbesondere die Unterstützung von öffentlichen Unternehmen kleinerer und mittlerer Größe, die nicht die Schwellenwerte der BSI-KritisV erreichen und bislang nur unzureichend im Bereich der IT-Sicherheit vom Staat unterstützt werden. Ausfälle von Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen wie z. B. Betriebe des öffentlichen Personennahverkehrs oder lokale Energie- oder Wasserversorgungsunternehmen können regional große Schäden anrichten und müssen deshalb erforderlichenfalls mit staatlicher Unterstützung abgewehrt werden. Die Kosten werden in einer gesonderten Gebührenverordnung festgelegt.

Eine weitere Unterstützungsleistung kann die Erstellung und Fortschreibung von Informationssicherheitskonzepten sein, die staatliche Behörden und Kommunen gemäß Art. 11 Abs. 1 BayEGovG erstellen müssen. Bei dieser anspruchsvollen Aufgabe können sie im Rahmen von Art. 10 Abs. 1 Nr. 2 und Abs. 2 BayEGovG Unterstützung durch das LSI erhalten.

Auch bei anderen IT-Sicherheitskonzepten, wie sie bspw. bei einer Zertifizierung nach ISIS 12 oder ISO 27001 benötigt werden, kann das LSI andere Behörden etwa durch das Erstellen von Vorlagen oder die Übernahme der Projektleitung unterstützen.

Zu Abs. 3

Das LSI kann auf Ersuchen die Polizeien, Strafverfolgungsbehörden und das Landesamt für Verfassungsschutz mit technischer Expertise – bspw. im Bereich Forensik, Kyptoanalyse oder BigData – unterstützen. In diesen Fällen wird es lediglich als Hilfsorgan tätig.

Zu Abs. 4

Zur Achtung der Gewaltenteilung ist das LSI nicht für die Kommunikationstechnik von Judikative, Legislative, des Obersten Rechnungshofs und des Landesbeauftragten für den Datenschutz zuständig. Allerdings steht die Gewaltenteilung im Interessenwiderstreit mit der Notwendigkeit der Absicherung des Behördennetzes. Aus diesem Grund ist das LSI wiederum zuständig, soweit diese Stellen am Behördennetz angeschlossen sind oder elektronische Verwaltungsinfrastrukturen bzw. zentrale Dienste im Sinne des Art. 8 BayEGovG nutzen. Dies ist gerechtfertigt, da der Anschluss an das Bayerische Behördennetz auf freiwilliger Basis erfolgt. Wer das erhöhte Sicherheitsniveau des Behördennetzes in Anspruch nehmen möchte, muss sich – zum Schutze aller – dem dort geltenden Sicherheitsdekret unterwerfen.

Soweit die Kommunikationstechnik von Judikative, Legislative, dem Obersten Rechnungshof und dem Landesbeauftragten für den Datenschutz ausschließlich in eigener Zuständigkeit betrieben wird, bleibt diese dem Zugriff des LSI verwehrt.

Zu Art. 11

Behördenübergreifende Pflichten

Zu Abs. 1

Der ehemalige Art. 8 Abs. 1 BayEGovG, der die Behördenpflichten zur Wahrung der IT-Sicherheit regelt, wird aus gesetzessystematischen Gründen in den Teil zur Sicherheit in der Informationstechnik verschoben.

Zu Abs. 2

Staatliche und sonstige an das Behördennetz angeschlossene Stellen sind nach Abs. 2 verpflichtet, Sicherheitslücken, Schadprogramme und erfolgte oder versuchte Angriffe unverzüglich an das Landesamt und die für sie zuständige oberste Dienstbehörde zu melden, soweit andere Vorschriften oder Vereinbarungen mit Dritten dem nicht entgegenstehen. Nur wenn das LSI über eine Bedrohung in Kenntnis gesetzt ist, kann es die anderen Behörden warnen. Vorschriften, die eine Weitergabe verhindern, können solche des Geheimschutzes oder über personenbezogene Daten sein, wobei die übermittelten Informationen in der Regel rein technischer Natur sind und keinen Personenbezug aufweisen. Auch privatrechtli-

che Verträge mit Herstellern können eine Unterrichtung verhindern. In solchen Fällen sollten die Behörden die Informationsweitergabe nicht unterlassen, sondern derart beschränken, dass Vertragsverletzungen vermieden werden. Unvollständige Informationen können zur IT-Sicherheit mehr beitragen als keine Informationen.

Die Meldeprozesse zwischen dem LSI und den Behörden können in allgemeinen Verwaltungsvorschriften bestimmt werden, für die es keine gesonderte Ermächtigung bedarf.

Zu Abs. 3

Staatliche und an das Behördennetz angeschlossene Stellen sind verpflichtet, das Landesamt bei Maßnahmen nach Art. 10 Nr. 1, 2, 4 und 5 zu unterstützen. Dies gilt selbstverständlich nur vorbehaltlich datenschutzrechtlicher Vorschriften.

Klarstellend wird angemerkt, dass die Unterstützungsleistung der Rechenzentren insbesondere in der Übermittlung bereits erhobener Daten liegt. Sie ist erforderlich, wenn das LSI die Systeme, die die Daten erzeugen, nicht selbst betreibt. So wird bspw. der zentrale Internetübergang in das Behördennetz beim IT-Dienstleistungszentrum des Landesamts für Digitalisierung, Breitband und Vermessung betrieben. Dabei handelt es sich um ein komplexes Konglomerat verschiedenster Abwehr- und Kontrollmechanismen (Firewalls, VPNs, Proxy-Server, Anti-Viren-Systeme etc.). Schon Störungen im Promillebereich hätten erhebliche Auswirkungen auf das reibungslose Funktionieren des Behördennetzes. Die Fehlersuche würde sich aufgrund der Abstimmungsschwierigkeiten zweier Betreiber um ein Vielfaches erschweren. Die 140.000 Beschäftigten, die den Internetübergang nutzen, wären an ihrer Arbeit gehindert. Auch müssten jedes Mal die Auftraggeber als Verantwortliche im Rahmen von Auftragsdatenverarbeitungsverhältnissen der Übermittlung zustimmen.

Zu Art. 12

Abwehr von Gefahren für die Informationstechnik

Zu Abs. 1

Art. 12 stellt die zentrale Befugnisnorm für das LSI dar, um die Abwehr von Gefahren für die Sicherheit der Informationstechnik des Behördennetzes nach Art. 10 Abs. 1 Nr. 1 effektiv und effizient mit technischen Mitteln zu gestalten.

Effektive Gefahrenabwehr kann nur durch ein einheitlich hohes Schutzniveau gewährleistet werden. Das beste IT-Sicherheitskonzept einer Behörde ist nutzlos, wenn der Angreifer durch nicht ausreichend gesicherte Kanäle einer anderen Behörde in das gesamte Netz eindringen kann. Dies gilt es zu verhindern.

Daher darf das LSI zur Gefahrenabwehr gegenüber staatlichen und an das Behördennetz angeschlossenen Stellen die nötigen Anordnungen treffen oder Maßnahmen ergreifen. Nur so kann ein homogenes Qualitätsniveau der IT-Sicherheit gewährleistet werden. Die Gefahren können durch einen Audit nach Art. 13 Abs. 1 BayEGovG entdeckt oder durch sonstigen Kenntnisgewinn festgestellt worden sein.

Bei den zu ergreifenden Maßnahmen ist der Verhältnismäßigkeitsgrundsatz zu beachten, insbesondere ist stets das mildeste Mittel zur Erreichung des Zwecks zu wählen.

Die datenschutzrechtliche Generalklausel des Satz 2 dient dem legitimen Datenzugriff zur Gefahrenabwehr. Muss das LSI auf Systeme zugreifen um bspw. Schadprogramme zu entfernen, so könnte es hierbei auf personenbezogene Daten stoßen. Eine Einwilligung ist in diesen Fällen nicht immer (rechtzeitig) wirksam einzuholen, wenn Gefahr im Verzug vorliegt und/oder der Systeminhaber keine Einwilligungserklärung für die betroffenen Daten geben kann. Wie sich aus Satz 1 ergibt, beschränkt sich die Datennutzung bzw. -verarbeitung auf das Notwendige.

Zu Abs. 2

Abs. 2 konkretisiert die Generalbefugnis. Nach Art. 12 Abs. 2 Nr. 1 BayEGovG kann das LSI Protokolldaten, die beim Betrieb von Informationstechnik des Landes anfallen, erheben und automatisiert auswerten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Informationstechnik des Landes, von Angriffen auf die Informationstechnik des Landes, zur Abwehr von unbefugter Datennutzung oder -verarbeitung oder sonstigen Gefahren erforderlich ist.

Die Erforderlichkeit stellt dabei eine Relevanzgrenze dar. Informationen – bspw. Zugriffe auf Verzeichnisdienste oder Zugriffsprotokolldaten der Polizei – die für eine effiziente Abwehr von Schadprogrammen oder anderen Angriffen nicht von Bedeutung sind, dürfen nicht erhoben und ausgewertet werden. Für den unwahrscheinlichen Fall, dass ein Zugriff durch das LSI auf solche sensiblen Systeme unabdingbar wird, sind die Mitarbeiter einer Sicherheitsüberprüfung zu unterziehen, die Zugriffe zu protokollieren und der Bericht bzw. die Akte als Verschlusssache zu deklarieren.

Bei Protokolldaten handelt es sich um sog. Logfiles von Servern, Firewalls, WebProxys etc. Diese Logfiles protokollieren sog. Events, also Ereignisse über Anfragen von anderen Systemen, Softwareänderungen, Fehlermeldungen etc. Sie enthalten keine Inhaltsdaten.

Setzt man Protokolldaten verschiedener Systeme in Korrelation und wertet diese aus, so können Unregelmäßigkeiten und damit potenzielle Bedrohungen erkannt werden. Protokolldateien, die für die Abwehr von Gefahren interessant sind, können unter anderem sein:

– Protokolldateien von Firewall-Systemen einschließlich Erhebungszeitpunkt, IP-Adresse und Port so-

wie vollständigem Domänennamen von ein- und ausgehenden Verbindungen sowie die durch die Firewall durchgeführte Aktion;

- Protokolldateien 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;
- Protokolldateien 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;
- Protokolldateien von Datenbankservern einschließlich Erhebungszeitpunkt, Anmeldename, IP-Adresse und vollständigem Domänennamen von Verbindungen und die Identifikationsnummer der ausgegebenen Meldung und deren Klartext;
- Protokolldateien von Web- und Proxyservern einschließlich Erhebungszeitpunkt, IP-Adresse und vollständigem Domänennamen von ein- und ausgehenden Verbindungen sowie dem einheitlichen Ressourcenzeiger (Uniform Resource Locator URL) und Kopfdaten und
- Protokolldateien der Betriebssoftware von Computersystemen einschließlich Erhebungszeitpunkt, IP-Adresse und vollständigem Domänennamen des betroffenen Computersystems, Namen des Programms oder Systemdiensts sowie dessen Typ, die Identifikationsnummer der ausgegebenen Meldung und deren Klartext.

Nach Nr. 2 kann das LSI die an den Schnittstellen zwischen dem Behördennetz und öffentlichen Netzen anfallenden Daten erheben und automatisiert auswerten. Die Vorschrift erlaubt eine sofortige Analyse des in das Behördennetz eindringenden Datenverkehrs. Damit sollen Schadprogramme bereits am Übergang vom Internet zum Behördennetz erkannt und abgewehrt werden. Davon umfasst ist auch der Zugriff auf (technische) Telekommunikationsinhalte. Nur so können gefährliche Dateianhänge oder Links zu Internetseiten, die ihrerseits Schadsoftware einzuschleusen versuchen, analysiert und abgewehrt werden. Die automatisierte Auswertung gestattet nicht die Speicherung der Inhalte über den für die technische Abwicklung des Kommunikations- und Erkennungsvorgangs ohnehin notwendigen Umfang hinaus.

Einzelheiten zur Datenverarbeitung und -übermittlung regeln Art. 16 und 17 BayEGovG.

Zu Art. 13

Untersuchungen der Sicherheit in der Informationstechnik

Zu Abs. 1

Das LSI kann die Sicherheit der Informationstechnik staatlicher und an das Behördennetz angeschlossener Stellen untersuchen und bewerten, mithin hat es ein Recht zur Prüfung einzelner Systemkomponenten bis hin zur Auditierung der gesamten IT-Infrastruktur. Damit wird sichergestellt, dass alle Stellen des Behördennetzes das erforderliche Sicherheitsniveau erfüllen. Zwingend zu beachten ist dabei, dass die Aufgabenerfüllung von unabhängigen Stellen wie dem Landtag, dem Obersten Rechnungshof oder dem Landesbeauftragten für den Datenschutz nicht behindert wird.

Über das Ergebnis der Prüfung erstellt das LSI einen Bericht, den es der untersuchten Stelle zur Verfügung stellt.

Art. 11 Abs. 3 BayEGovG stellt sicher, dass das LSI bei der Auditierung hinreichende Unterstützung erfährt. Das LSI muss für eine Beurteilung der IT-Sicherheit Zugang zu den Systemen haben. Dieser kann u. U. nur eingeschränkt gewährt werden, wenn bspw. Vorschriften des Geheimschutzes dem entgegenstehen. Vorab ist zu prüfen, ob eine Sicherheitsüberprüfung der auditierenden LSI-Beschäftigten Abhilfe schaffen kann.

Werden bei der Auditierung Gefahren für die Informationstechnik des Landes entdeckt, kann das LSI nach Art. 12 Abs. 1 BayEGovG die nötigen Anordnungen treffen oder entsprechende Maßnahmen zur Abwehr der Gefahren ergreifen.

Zu Abs. 2

Abs. 2 dient dazu, Rechtssicherheit für umfassende Untersuchungen von IT-Produkten (z. B. mittels Reverse - Engineering) und IT-Systemen durch das LSI zur Erfüllung seiner Aufgaben nach Art. 11 Abs. 1 Nr. 4 und 8 herzustellen. Die gesetzliche Befugnis führt dazu, dass die Beschaffung von Daten und Informationen über den Aufbau und die Funktionsweise der Untersuchungsgegenstände durch das LSI nicht als „unbefugt“ im Sinne von § 202a Strafgesetzbuch (StGB) bzw. § 17 ff. des Gesetzes gegen den unlauteren Wettbewerb (UWG) anzusehen ist.

Auf dem Markt bereitgestellte bzw. zur Bereitstellung auf dem Markt vorgesehene Untersuchungsgegenstände sind solche, die für einen Erwerb durch das LSI verfügbar sind. Die Formulierung „auf dem Markt bereitgestellte Produkte“ ist angelehnt an eine entsprechende Formulierung im Produktsicherheitsgesetz. Durch die Formulierung „zur Bereitstellung auf dem Markt vorgesehene“ Untersuchungsgegenstände wird klargestellt, dass die Untersuchungsbefugnis auch solche Produkte und Systeme erfasst, die zwar vom Hersteller bereits angekündigt wurden, aber noch nicht allgemein am Markt verfügbar sind. Untersu-

chungsrechte bei Herstellern, Anbietern und sonstigen Einrichtungen werden durch Abs. 2 nicht begründet.

Sollten Dritte mit der Untersuchung beauftragt werden, hat das LSI bei der Auswahl der Dritten die schutzwürdigen Interessen des Herstellers zu berücksichtigen. Hierzu gehört auch, dass es den beauftragten Dritten zur Wahrung einer entsprechenden Vertraulichkeit verpflichtet. Die Beauftragung eines direkten Konkurrenten des Herstellers ist in diesem Zusammenhang ausgeschlossen.

Zu Art. 14

Mindeststandards

Art. 14 BayEGovG weist dem LSI die Befugnis zu, allgemeine technische Mindeststandards für die IT-Sicherheit zu entwickeln. Auch hier ist es Ziel, ein einheitlich hohes Niveau der IT-Sicherheit bei den Behörden zu schaffen. Das Staatsministerium der Finanzen, für Landesentwicklung und Heimat als zuständiges Staatsministerium kann im Einvernehmen mit den weiteren Staatsministerien und der Staatskanzlei diese Mindeststandards ganz oder teilweise als verbindliche allgemeine Verwaltungsvorschriften für alle staatlichen Stellen erlassen. Im Falle der IT-Sicherheitsrichtlinien geschieht dies bereits heute durch den IT-Beauftragten der Staatsregierung im Einvernehmen mit den Ressort-CIOs. Dieses Verfahren ist auch auf andere Mindeststandards übertragbar.

Nur durch derartige Vorgaben kann sichergestellt werden, dass Sicherheitslücken auf Seiten einer Behörde nicht die Gesamtsicherheit des Behördennetzes und damit aller anderen Behörden gefährden. Für Kommunen und unabhängige Stellen, die nicht an das Behördennetz angeschlossen sind, haben die Mindeststandards lediglich empfehlenden Charakter.

Nicht staatliche Stellen können durch Verwaltungsvorschriften des Landes nicht zur Einhaltung von Mindeststandards verpflichtet werden. Daher regelt Satz 3, dass für Landratsämter und die an das Behördennetz angeschlossenen, nicht staatlichen Stellen die Mindeststandards für die Teilnahme am Behördennetz gelten. Damit wird sichergestellt, dass die bislang gültigen Anschlussbedingungen für Teilnehmer am Bayerischen Behördennetz verpflichtend sind. Die Landratsämter werden aufgrund ihrer Doppelfunktion ausdrücklich erwähnt. Das Konnexitätsprinzip wird durch die Regelung nicht berührt, da der Anschluss am Behördennetz auf freiwilliger Basis erfolgt.

Zu Art. 15

Warnungen

Die Vorschrift regelt, dass das LSI aufgrund von gewonnenen Erkenntnissen über Sicherheitslücken, Schadprogramme oder unbefugte Datenverarbeitung Warnungen aussprechen und Sicherheitsmaßnahmen empfehlen darf. Um einen schnellen Informationsfluss zu gewährleisten, wird nach Abschluss der Errichtungsphase mittelfristig ein 24-Stunden/7-Tage-Betrieb angestrebt.

Mit Warnungen zu Hard- oder Softwareprodukten kann ein nicht unerheblicher Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb einhergehen. Schlimmstenfalls ist das betroffene Unternehmen in seiner Existenz gefährdet. Aus diesem Grund sind Informationen, die sich im Nachhinein als falsch oder unrichtig wiedergegeben herausstellen, unverzüglich zu berichtigen. Die Berichtigung erfolgt auf Antrag des Betroffenen oder, wenn erhebliche Belange des Gemeinwohls gefährdet sind, von Amts wegen.

Zu Art. 16

Datenspeicherung und -auswertung

Zu Abs. 1

Grundsätzlich richtet sich die Löschung nach Art. 12 BayDSG. Personenbezogene Daten sind zu löschen, wenn ihre Speicherung unzulässig ist oder ihre Kenntnis für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

Besonderheiten gilt es bei der Auswertung von automatisierten Daten nach Art. 12 i. V. m. Art. 16 Abs. 1 BayEGovG zu beachten. Die Norm stellt klar, dass Daten, die Personenbezug aufweisen oder dem Fernmeldegeheimnis unterliegen, bei der automatisierten Auswertung nach Art. 12 Abs. 2 BayEGovG grundsätzlich nicht über die Dauer der automatisierten Auswertung hinaus gespeichert werden dürfen und sofort und spurlos zu löschen sind. Damit werden die Anforderungen des Bundesverfassungsgerichts aus dem Urteil zur automatisierten Erfassung von Kfz-Kennzeichen erfüllt (BVerfG in BVerfGE 120, 378 ff.).

In diesem Zusammenhang ist ein besonderes Augenmerk auf Daten zu legen, die dem Steuer- oder dem Sozialgeheimnis unterfallen. Bei der hierunter fallenden Kommunikation ist der Kreis der zugriffsbefugten Personen einzuschränken. Zudem muss durch Dokumentation nachvollziehbar sein, wer zu welchem Zeitpunkt welche Daten geprüft, ausgewertet oder sonst verarbeitet hat. Darüber hinaus muss den prüfenden Personen verdeutlicht werden, dass ein Verstoß gegen das Steuer- bzw. Sozialgeheimnis strafbewehrt ist und Disziplinarmaßnahmen nach sich zieht.

Im Übrigen gelten für die Löschung und Auswertung personenbezogener Daten die Vorschriften des Bayerischen Datenschutzgesetzes.

Zu Abs. 2

Abs. 2 regelt den Umgang mit Protokolldaten. Diese können für einen erforderlichen Zeitraum, längstens jedoch 3 Monate, gespeichert werden. Voraussetzung ist, dass tatsächliche Anhaltspunkte dafür bestehen, dass die Daten für den Fall der Bestätigung eines

Verdachts nach Abs. 4 Satz 1 Nr. 2 zur Abwehr von Gefahren für die Informationstechnik erforderlich sein können. Dabei handelt es sich um das sog. Quick-Freezing-Verfahren, bei dem die Speicherung nicht anlasslos, sondern nur im Einzelfall und erst zu dem Zeitpunkt stattfindet, zu dem ein tatsächlicher Anhaltspunkt gegeben ist (vgl. BVerfG in BVerfGE 1 BvR 256/08 = NJW 2010, 833, Rn. 208).

Tatsächliche Anhaltspunkte liegen vor, wenn es möglich ist, dass die Protokolldaten zur Gefahrenabwehr erforderlich sein könnten. Der Begriff orientiert sich am Anfangsverdacht gemäß § 152 Abs. 2 Strafprozessordnung (StPO).

Die Speicherhöchstdauer von 3 Monaten ist verhältnismäßig, insbesondere verfolgt sie einen legitimen Gemeinwohlzweck, ist geeignet, erforderlich und angemessen (vgl. BVerfG in BVerfGE 100, 313, 359 = NJW 2000, 55). Art. 10 Abs. 1 Grundgesetz verbietet nicht jede vorsorgliche Erhebung und Speicherung von Daten überhaupt, sondern schützt vor einer unverhältnismäßigen Gestaltung solcher Datensammlungen und hierbei insbesondere vor entgrenzenden Zwecksetzungen. Strikt verboten ist lediglich die Speicherung von personenbezogenen Daten auf Vorrat zu unbestimmten und noch nicht bestimmbaren Zwecken (vgl. BVerfG 1 BvR 256/08 in NJW 2010, 833, Rn. 206).

Die staatliche IT-Infrastruktur ist zu schützen. Zum einen können dort sensible Informationen wie Steuer- oder Gesundheitsdaten von Bürgern und Unternehmen abgegriffen werden. Zum anderen ist die IT für eine funktionierende Staatsverwaltung und damit für die Sicherheit des Staates von elementarer Bedeutung. Bereits heute würden bei einem Ausfall die überwiegende Anzahl von Verwaltungsverfahren nicht mehr bearbeitet werden können.

Das Prüfen der Protokolldaten ist geeignet, Angriffe zu erkennen und abzuwehren. Dies erfordert nicht, dass das Regelungsziel in jedem Einzelfall tatsächlich erreicht wird, sondern verlangt lediglich, dass die Zweckerreichung gefördert wird (vgl. BVerfGE 1 BvR 256/08 in NJW 2010, 833, Rn. 207 m.w.N.). Des Weiteren ist es das mildeste, weil zugleich das einzige Mittel, um gefährlichen Datenverkehr von außen an einem Eindringen in die Systeme zu verhindern. Weniger einschneidende Mittel, die ebenso weitreichende Aufklärungsmaßnahmen ermöglichen, sind nicht ersichtlich.

Die Maßnahme ist auch verhältnismäßig im engeren Sinne, das heißt angemessen. Regelmäßig können Schadprogramme erst mit zeitlichem Verzug von Tagen oder Wochen aufgespürt werden. Im Anschluss muss dem LSI genug Zeit zur Verfügung stehen, die Daten zu analysieren. Nach bisheriger Erfahrung werden ca. 80 Prozent der Angriffe innerhalb der ersten 3 Monate entdeckt. Unter Berücksichtigung des hohen Schutzbedarfs der staatlichen IT-Infrastruktur wird deshalb die maximale Speicherdauer der zur Erkennung von Schadprogrammen relevante Protokolldaten auf 3 Monate festgelegt. Darüber hinaus wird das Recht auf informationelle Selbstbestimmung durch die Sicherstellung einer automatisierten Erkennung nach Satz 4 sowie einer Pseudonymisierung der Daten nach Satz 5 geschützt.

Nach Nr. 2 ist eine Speicherung von Protokolldaten auch möglich, wenn die Daten zur Verhütung, Unterbindung oder Verfolgung damit zusammenhängender Straftaten erforderlich sein können. Die Regelung erlaubt die Speicherung von Daten, die bspw. bei einem versuchten Cyberangriff auf die IT-Infrastruktur angefallen sind. Nur so wird dem Freistaat Bayern als Geschädigtem die Möglichkeit gegeben, strafrechtliche Ermittlungen einleiten zu lassen. Zudem können die Sicherheitsbehörden diese Daten nutzen, um künftige Straftaten zu verhindern oder laufende Straftaten zu unterbinden.

Nach Satz 2 müssen die Daten im Gebiet der Europäischen Union gespeichert werden. Damit werden Vorgaben des Europäischen Gerichtshofs (EuGH) (vgl. EuGH C-293/12 Rn. 66 ff.; EuGH C-203/15 und C-698/15, Rn. 122) erfüllt.

Satz 3 regelt die Anforderungen an die Datensicherheit. Demnach müssen die organisatorischen und technischen Maßnahmen zur Sicherstellung einer automatisierten Auswertung zu jeder Zeit dem Stand der Technik entsprechen. Die einfachgesetzliche Rechtsfigur des Stands der Technik erfüllt die Vorgaben des Bundesverfassungsgerichts (vgl. BVerfG in NJW 2010, 833 ff., Rn. 224).

Zu Abs. 3

Abs. 3 regelt den Umgang von Inhaltsdaten, die einer restriktiveren Regelung bedürfen. Dabei darf der Gesetzgeber bei der Entscheidung, wie weit solche Daten zu löschen oder zu speichern sind, einen Interessenausgleich vornehmen und die Belange staatlicher Aufgabenwahrnehmung berücksichtigen (vgl. BVerfGE 1 BvR 256/08 in NJW 2010, 833, Rn. 217). Eine Speicherung solcher Daten für 2 Monate ist zulässig und angemessen, da sie nur bei gesteigertem Risiko oder bei Vorliegen einer konkreten Gefahrenlage erfolgt (vgl. BVerfGE 120, 378).

Aufgrund der Sensibilität der Daten ist die Maßnahme durch die Behördenleitung und einen Bediensteten mit der Befähigung zum Richteramt anzuordnen. Das Vier-Augen-Prinzip und die Einschätzung eines Juristen sollen die Wahrung der Verhältnismäßigkeit sicherstellen. Allerdings ist die Anordnung zeitlich beschränkt (vgl. EuGH C-293/12, Rn. 59). Sie gilt längstens 2 Monate, kann aber erforderlichenfalls verlängert werden. Klarstellend wird angemerkt, dass sich ein Ablauf der Anordnung nicht auf die Speicherfrist auswirkt, d. h. die Daten sind unabhängig von ihrer Speicheranordnung max. 2 Monate speicherbar.

Darüber hinaus ist eine Speicherung nur zulässig, wenn dies zum Schutz der technischen Systeme unerlässlich ist. Im Gegensatz zur Erforderlichkeit aus

Art. 12 Abs. 1 BayEGovG ist die Hürde bei der Unerlässlichkeit nochmals erhöht.

Im Übrigen wird auf die Ausführung zu Abs. 2 verwiesen.

Zu Abs. 4

Liegt ein hinreichender Verdacht vor, so können weitere, auch nicht automatisierte Maßnahmen folgen. Dazu dürfen die Daten über die Abs. 2 und 3 hinaus verarbeitet und genutzt werden. Eine Legaldefinition der Begriffe findet sich in Art. 4 Abs. 6 und 7 BayDSG. Notwendige Untersuchungen der Daten sind zulässig, um einen Verdacht, dass die Daten eine Gefahr für die Informationstechnik etwa durch ein Schadprogramm, durch programmtechnische Sicherheitslücken, unbefugte Datennutzung oder -verarbeitung enthalten, zu bestätigen.

Hat sich der Verdacht, dass die Daten Gefahren für die Informationstechnik enthalten, bestätigt, so ist eine weitere Verarbeitung der Daten, etwa zur Abwehr des Schadprogramms, zur Abwehr von Gefahren, die von dem aufgefundenen Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme zulässig, soweit dies erforderlich ist. Beispielweise kann die Funktionsweise einer Schadsoftware untersucht oder ihre Signatur in Datenbanken von Anti-Viren-Software aufgenommen werden.

Ein hinreichender Verdacht liegt vor, wenn 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 lässt als das Szenario, dass dies nicht der Fall ist. Der Begriff orientiert sich am hinreichenden Tatverdacht nach § 170 Abs. 1 StPO.

Auch ist eine über die Abs. 2 und 3 hinausgehende Verarbeitung und Nutzung der Daten zulässig, wenn bei der Verarbeitung oder Nutzung der Daten zu übermittelnde Daten (Art. 17 Abs. 2 BayEGovG) festgestellt werden. Nr. 3 regelt damit auch den sog. Zufallsfund. Werden bei der Analyse der Daten Hinweise auf eine Gefahr für Leib, Leben oder Freiheit einer Person oder Daten bekannt, die zur Verhütung und Unterbindung von Straftaten oder zur Verfolgung einer von Art. 17 Abs. 2 Nr. 2 BayEGovG umfassten Straftaten benötigt werden können, so dürfen diese u. a. gespeichert werden. Dies gilt auch, wenn sich letztlich der Verdacht, dass die Daten eine Gefahr für die Informationstechnik darstellen, nicht bestätigt. Damit wird verhindert, dass Daten gelöscht werden müssten und eine Übermittlung an die Sicherheitsbehörden, Polizei bzw. Strafverfolgungsbehörden nach Art. 17 Abs. 2 BayEGovG dann nicht mehr möglich wäre.

Während Abs. 2 und Abs. 3 lediglich eine automatisierte Auswertung und nicht personenbezogene Verwendung von Daten zulassen, kann sich Abs. 4 auch auf die inhaltliche Prüfung von Dokumenten, bspw. nach Schadcode, beziehen. Zur Gewährleistung der richterlichen Unabhängigkeit ist daher, wenn Daten verarbeitet werden, welche die richterliche Unabhängigkeit berühren, nach Satz 3 der jeweils zuständigen obersten Dienstbehörde zu berichten. Die obersten Dienstbehörden können die Berichte den jeweiligen Kontrollgremien weiterleiten. Darüber hinaus sind nach Satz 3 unabhängige Stellen wie der Landesbeauftragte für den Datenschutz und die auch anderweitig hervorgehobenen geschützten Träger von Berufs- oder besonderen Amtsgeheimnissen (vgl. Wilde u.a., Kommentar und Handbuch zum BayDSG, Art. 22 BayDSG, Rn. 7 ff.) zu unterrichten, soweit deren Datenverarbeitung berührt ist.

Zu Abs. 5

Die Vorschrift stellt besondere Anforderungen an den Datenschutz, auch um die Verhältnismäßigkeit der Norm zu wahren.

Daten, die den Kernbereich privater Lebensgestaltung betreffen, dürfen, soweit möglich, nicht erhoben werden. Aus Art. 1 Abs. 1 Grundgesetz ergibt sich, dass ein Kernbereich privater Lebensgestaltung als absolut unantastbar geschützt ist (vgl. BVerfG in BVerfGE 119, 1 ff.). Selbst sehr schwerwiegende Interessen der Allgemeinheit können einen Eingriff in ihn nicht rechtfertigen; eine Abwägung findet nicht statt (vgl. BVerfG in BVerfGE 34, 238 ff.). Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen, und zwar ohne Angst, dass staatliche Stellen dies überwachen. Vom Schutz umfasst sind auch Gefühlsäußerungen, Äußerungen des unbewussten Erlebens sowie Ausdrucksformen der Sexualität (vgl. BVerfG in BVerfGE 109, 279 ff.).

Werden Erkenntnisse aus dem Kernbereich privater Lebensgestaltung dennoch erlangt, dürfen diese nicht verwendet werden und sind sofort und spurlos zu löschen (vgl. BVerfG in BVerfGE 120, 378 ff.). Die Tatsache ihrer Erlangung und ihre Löschung sind zu dokumentieren.

Zu Art. 17

Datenübermittlung

Zu Abs. 1

Abs. 1 regelt die Übermittlung der nach Art. 12 i. V. m. Art. 16 BayEGovG erlangten Daten. Die Vorschrift stellt sicher, dass eine Datenübermittlung an Rechenzentren und andere Betreiber von IT-Technik, wenn und soweit dies zur Abwehr oder Beseitigung von Gefahren erforderlich ist, möglich ist.

Zu Abs. 2

Ein Angriff auf die staatliche IT stellt zumeist auch eine Straftat (z. B. nach §§ 202a ff., 303a f. StGB) dar. Mit Abs. 2 wird dem LSI die datenschutzrechtliche Befugnis zur Datenübermittlung an Sicherheitsbehörden, Polizei und Strafverfolgungsbehörden einge-

räumt. Als datenschutzrechtliche Zweckänderungs- und Weiterverarbeitungserlaubnis unterliegt die Regelung in besonderer Weise dem Grundsatz der Verhältnismäßigkeit, dem dadurch Rechnung getragen wird, dass nicht in sämtlichen Fällen Daten übermittelt werden dürfen bzw. sollen. Für den präventiven Bereich beschränkt sich die Übermittlungsbefugnis auf die Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person sowie auf die Fälle der Verhütung und Unterbindung von in Art. 17 Abs. 2 Nr. 2 BayEGovG genannten Straftaten. Für den Bereich der Strafverfolgung wiederum soll eine Übermittlung erfolgen, soweit die Tatsachen, aus denen sich die Gefahr für die Informationstechnik oder der diesbezügliche Verdacht ergibt, selbst den Verdacht einer Straftat begründen. Sog. Zufallsfunde sollen nur übermittelt werden, wenn die Voraussetzungen der Nr. 2 Buchst. b vorliegen.

Die Vorschrift stellt die Übermittlung in ein intendiertes Ermessen des LSI. Sie lässt damit Spielraum für konkretisierende Absprachen zwischen dem LSI und den empfangenden Stellen, durch die vermieden werden kann, dass eine generelle Regelübermittlung bei ca. 40.000 versuchten Angriffen pro Tag die Kapazitäten aller beteiligten Stellen unnötig belasten würde. Es sollen nur Angriffe mit einem gewissen Grad an Erheblichkeit gemeldet und folglich nur diese Daten übermittelt werden.

Satz 2 gibt vor, dass das Staatsministerium der Finanzen, für Landesentwicklung und Heimat im Einvernehmen mit dem Staatsministerium des Innern, für Bau und Verkehr und dem Staatsministerium der Justiz Verwaltungsvorschriften zum konkreten Verfahren der Zusammenarbeit zwischen LSI und den Sicherheitsbehörden, der Polizei und den Strafverfolgungsbehörden festlegt. Geregelt werden meldepflichtige Ereignisse, Schwellenwerte bzw. Meldekategorien, klare Handlungsabläufe und Meldewege für Störungsfälle. Des Weiteren werden Ansprechpartner für alle beteiligten Stellen benannt. Insoweit wird die „soll"-Regelung konkretisiert.

Die Datenübermittlung an das Landesamt für Verfassungsschutz (LfV) richtet sich nach Art. 24 Bayerisches Verfassungsschutzgesetz (BayVSG); mithin ist sie vorliegend nicht regelungsbedürftig. Demnach haben Behörden wie das LSI dem Verfassungsschutz die ihnen bei Erfüllung ihrer Aufgaben bekanntgewordenen Informationen einschließlich personenbezogener Daten auch ohne vorheriges Ersuchen des LfV zu übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Informationen für die Erfüllung der Aufgaben des LfV nach Art. 3 BayVSG erforderlich sein könnten.

Zu Nr. 10

Zu Art. 18

Einschränkung von Grundrechten

Das Fernmeldegeheimnis könnte verletzt werden, wenn durch das LSI Daten eines Telekommunikationsvorgangs zwischen einem Bürger und einer staatlichen oder kommunalen Behörde ausgewertet werden.

Nach Art. 19 Abs. 1 Satz 2 i. V. m. Art. 10 Grundgesetz dürfen Beschränkungen des Fernmeldegeheimnisses nur auf Grund eines Gesetzes angeordnet werden, das wiederum das Grundrecht unter Angabe des Artikels nennen muss.

Zu Nr. 11

Zu Art. 19

Schlussvorschriften

Art. 19 regelt das Inkrafttreten des Gesetzes.

Die Experimentierklausel des Art. 10 Abs. 1 BayEGovG endet nicht zum 30.12.2019, sondern bleibt auf unbestimmte Zeit wirksam.

Die Einführung der Pflicht für Behörden, angemessene technische und organisatorische Maßnahmen im Sinn des Art. 7 BayDSG zu treffen und die hierzu erforderlichen Informationssicherheitskonzepte zu erstellen, wird um ein Jahr verschoben. Das Inkrafttreten der Regelung zum 1. Januar 2018 stellt einen Großteil der Kommunen, insbesondere die über 1.500 bayerischen Gemeinden mit weniger als 5.000 Einwohnern, vor Umsetzungsprobleme. Die für die Implementierung erforderlichen IT-Berater können aufgrund der aktuellen Marktlage so kurzfristig nicht beauftragt werden.

Zu §§ 2 und 3
Änderung des Bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen und der Bayerischen Barrierefreie Informationstechnik-Verordnung

Aufgrund der Änderung der Nummerierung von Art. 9 BayEGovG a.F. zu Art. 8 BayEGovG sind Art. 122 Abs. 5 BayEUG und § 3 Abs. 1 BayBITV entsprechend anzupassen.