Landtag von Baden-Württemberg **Drucksache 17 / 10063**

17. Wahlperiode **16.12.2025**

Antrag

der Abg. Peter Seimer und Andrea Schwarz u. a. GRÜNE

und

Stellungnahme

des Ministeriums des Inneren, für Digitalisierung und Kommunen

Digitale Resilienz in Baden-Württemberg

Antrag

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. welche digitalen Kommunikationswege die Landesregierung in Krisensituationen anbietet, um Bürgerinnen/Bürger über Notfalltreffpunkte, Verhaltensanweisungen etc. aufzuklären und zu informieren (bitte unter Angabe, wie darüber auch vor Krisenereignissen zur persönlichen Krisenvorbereitung aufgeklärt wird);

2. wie die Landesregierung eine resiliente Kommunikationsinfrastruktur für diese Zwecke sicherstellt (unter Angabe einer Bewertung von [Teil-]Ausfällen von Mobilfunknetz, Breitbandnetz, Satellitenkommunikation, DAB+, UKW etc.);

3. wie sie eine Notwendigkeit des Erhalts von DVB-T2 und Simulcast (gleichzeitiger Betrieb von UKW und DAB+) im Speziellen den Erhalt von UKW vonseiten des öffentlich-rechtlichen Rundfunks im Hinblick auf Resilienz in Krisensituationen bewertet;

4. ob die Landesregierung aktuell Maßnahmen plant, um die digitale Vernetzung des Bevölkerungsschutzes zu verbessern (wenn ja, welche);

5. ob der Landesregierung Projekte zu digitalen Schnittstellen zwischen den Führungs- und Lagezentren der Polizei und den Integrierten Leitstellen für Feuerwehr und Rettungsdienst bekannt sind und wie sie diese bewertet und ggf. voranbringt;

6. wie die Integrierten Leitstellen gegen Angriffe auf deren digitale Infrastruktur geschützt sind und welche präventiven Vorgaben hierzu bestehen;

Eingegangen: 16.12.2025 / Ausgegeben: 24.2.2026

7. inwiefern insbesondere Vorgaben zum betrieblichen Kontinuitätsmanagement (BCM) nach einem digitalen (bspw. durch Ransomware, Datendiebstahl, Datenlöschung) oder physischen Angriff (bspw. durch Feuer, Einsturz, notwendige Evakuierung) für die Integrierten Leitstellen bestehen bzw. umgesetzt sind;

8. ob es zur Wahrung der digitalen Resilienz im Krisenfall Ausfalloptionen für bspw. das Vorhalten von wichtigen Daten – wie es kritische Patientendaten sind – oder notwendiger Rechenleistung, welche physisch nicht in Baden-Württemberg und nicht in einem angrenzenden Bundesland angesiedelt sind, gibt;

9. ob aktuell im Fall eines Cybersicherheitsvorfalls, welcher die Verfügbarkeit, Integrität oder Vertraulichkeit von kritischen IT-Systeme beeinträchtigt, physische Faktoren wie bspw. das Runterfahren eines industriellen Hochofens mitbedacht werden;

10. inwieweit der Landesregierung – in Anbetracht der Tatsache, dass die praktische Sicherstellung der Funktionsfähigkeit und der Schutz der KRITIS grundsätzlich deren Betreibern obliegt – praktische Kenntnisse über die digitale Arbeitsfähigkeit von KRITIS in Baden-Württemberg im Krisenfall hinsichtlich einer stabilen Stromversorgung vorliegen;

11. inwieweit der Landesregierung – in Anbetracht der Tatsache, dass die Sicherstellung der Funktionsfähigkeit und der Schutz der KRITIS grundsätzlich deren Betreibern obliegt – praktische Kenntnisse über die digitale Arbeitsfähigkeit von KRITIS im besonderen Fall eines Cybersicherheitsvorfalls, welcher die Verfügbarkeit, Integrität oder Vertraulichkeit von kritischen IT-Systemen beeinträchtigt, vorliegen;

12. ob die Landesregierung einen Bedarf sieht, notwendige – die bundes- und EU-weiten Entwicklungen und Vorgaben begleitende – Maßnahmen zu prüfen, um die Sicherheit bei KRITIS in Baden-Württemberg zu erhöhen (evtl. wissenschaftliche Analysen, Umsetzungshilfen);

13. ob in der Vergangenheit bereits wissenschaftliche Analysen zum Thema Cybersicherheit in der öffentlichen Verwaltung in Baden-Württemberg angefertigt wurden (bspw. zu gegenseitigen Abhängigkeiten zwischen Behörden oder ob Ausfälle übergeordneter Behörden auch darunterliegende Behörden betreffen würden);

14. ob sie die öffentliche Verwaltung (kommunal wie landesseitig) oder Teile derer in Baden-Württemberg als KRITIS einstuft und welche Vorgaben sie für diese macht (bitte im Falle von vorhandenen Vorgaben im Speziellen auch auf Managementthemen wie Informationssicherheitsmanagement und Kontinuitätsmanagement sowie auf Informationen bzgl. deren Finanzierung eingehen);

15. welche Erkenntnisse und Maßnahmen sie aus dem Sicherheitsvorfall in der Verwaltung des Landkreises Anhalt-Bitterfeld bspw. auch für andere Verwaltungseinheiten wie Regierungspräsidien oder Oberstaatsanwaltschaften abgeleitet hat.

16.12.2025

Seimer, Andrea Schwarz, Dr. Geugjes, Häffner,
Hildenbrand, Lede Abal, Sperling, Tuncer GRÜNE

Begründung

Digitale Resilienz wird immer wichtiger. Insbesondere in Krisensituationen ist die digitale Kommunikations- und Arbeitsfähigkeit der Betreiber kritischer Infrastruktur aus den Sektoren Energie, Informationstechnik und Telekommunikation, Gesundheit, Wasser und zeitlich einem Krisenfall jeweils versetzt nachfolgend aus den Sektoren Ernährung, Siedlungsabfallentsorgung, Transport und Verkehr, Medien und Kultur, Finanz- und Versicherungswesen unentbehrlich, um Notfällen mit größeren Ausmaßen begegnen zu können. Ebenso spielt die digitale Notfallkommunikation in den Gemeinden eine entscheidende Rolle in Krisen- und Katastrophenlagen. Der Antrag soll beleuchten, wie das Land die Kommunen dabei unterstützt, digitale Kommunikationswege im Krisenfall aufrecht zu erhalten und inwieweit KRITIS-Einrichtungen in Baden-Württemberg auf kritische Cybersicherheitsvorfälle vorbereitet sind.

Stellungnahme*)

Mit Schreiben vom 19. Februar 2026 Nr. IM6-1441-46/20/41 nimmt das Ministerium des Inneren, für Digitalisierung und Kommunen im Einvernehmen mit dem Staatsministerium, dem Ministerium für Kultus, Jugend und Sport, dem Ministerium für Wissenschaft, Forschung und Kunst, dem Ministerium für Umwelt, Klima und Energiewirtschaft, dem Ministerium für Soziales, Gesundheit und Integration, dem Ministerium der Justiz und für Migration, dem Ministerium für Verkehr sowie dem Ministerium für Ernährung, Ländlichen Raum und Verbraucherschutz zu dem Antrag wie folgt Stellung:

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. *welche digitalen Kommunikationswege die Landesregierung in Krisensituationen anbietet, um Bürgerinnen/Bürger über Notfalltreffpunkte, Verhaltensanweisungen etc. aufzuklären und zu informieren (bitte unter Angabe, wie darüber auch vor Krisenereignissen zur persönlichen Krisenvorbereitung aufgeklärt wird);*

Zu 1.:

Die Landesregierung stellt den Menschen in Baden-Württemberg in Krisensituationen verschiedene digitale Kommunikationswege zur Verfügung, um zeitnah und verlässlich über Notfalltreffpunkte, Verhaltensanweisungen sowie weitere erforderliche Maßnahmen zu informieren. Ziel ist es, sowohl im Vorfeld über Vorsorge und richtiges Verhalten aufzuklären als auch im eingetretenen Krisenfall verlässliche und aktuelle Informationen bereitzustellen. Eine zentrale Informationsplattform ist der Internetauftritt der Landesregierung (abrufbar unter: *www.baden-wuerttemberg.de*).

Falls die regulären Internetauftritte des Landes, etwa aufgrund technischer Störungen, Überlastung oder eines Cyberangriffs in Folge einer Krisensituation nicht oder nur eingeschränkt erreichbar sind, steht allen Ministerien als Rückfallebene der „Sonderinformationsdienst der Landesregierung“ (abrufbar unter: *www.infodienst-bw.de*) zur Verfügung. Über die auch als „Kriseninternet“ bezeichnete Plattform können den Menschen in Baden-Württemberg und

*) Der Überschreitung der Drei-Wochen-Frist wurde zugestimmt.

den Medien in einer Krisensituation relevante Informationen zentral bereitgestellt werden. Die über das Kriseninternet bereitgestellten Seiten sind „responsiv“: Das Layout der dargestellten Informationen wird automatisch daran angepasst, welche Art von Endgerät (PC/Laptop, Smartphone) beziehungsweise welches Bildschirmformat zur Darstellung verwendet wird. Darüber hinaus sind die generierten Seiten weitestgehend barrierefrei gestaltet. Um sehr viele gleichzeitige Anfragen bearbeiten zu können, nutzt der Sonderinformationsdienst der Landesregierung entsprechend leistungsfähige und weitgehend ausfallsichere Server.

Zur Warnung der Bevölkerung setzt Baden-Württemberg bereits seit vielen Jahren auf den bewährten Warnmix aus verschiedenen Warnkanälen. Insbesondere können die für die Gefahrenabwehr zuständigen Behörden zur amtlichen Warnung der Bevölkerung vor Gefahrensituationen seit Oktober 2016 landesweit das im gesamten Bundesgebiet verfügbare satellitengestützte Modulare Warnsystem (MoWaS) nutzen. Derzeit sind an MoWaS die Warn-Apps NINA, KATWARN und BIWAPP, einige regionale Warn-Apps, Cell Broadcast, Fernseh- und Hörfunkveranstalter, Zeitungsredaktionen und Onlinedienste, digitale Stadtinformationstafeln sowie einige Verkehrsunternehmen angeschlossen. Alle Warnmeldungen über MoWaS werden auch auf der vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) betriebenen Internetseite *„warnung.bund.de“* veröffentlicht. In Zukunft sollen auch Sirenen an MoWaS angeschlossen werden. Alle angeschlossenen Warnmittel können über MoWaS zeitgleich und mit einer Eingabe ausgelöst werden. Jährlich, in der Regel am zweiten Donnerstag im September, findet der Bundesweite Warntag statt. Der Warntag ist ein gemeinsamer Aktionstag von Bund, Ländern und Kommunen. Der Warntag dient der Erprobung der Warnsysteme. Gleichzeitig dient der Warntag dazu, die Menschen im Land für das Thema „Warnung“ und die vorhandenen Warnkanäle zu sensibilisieren. Grundsätzlich obliegt die Warnung der Bevölkerung als Teil der nötigenfalls zu treffenden Maßnahmen zur Gefahrenabwehr bei einer Schadenlage den Gemeinden in ihrer Eigenschaft als Ortspolizeibehörde.

Das Staatsministerium kommt seiner Informationspflicht im Rahmen der allgemeinen Öffentlichkeitsarbeit nach und klärt Bürgerinnen und Bürger auf den offiziellen Informationskanälen auf.

Das Ministerium des Inneren, für Digitalisierung und Kommunen nutzt seine offiziellen Kanäle in sozialen Medien, beispielsweise Instagram, zur schnellen Verbreitung von Warnhinweisen, Kurzmeldungen und Verweisen auf weiterführende Informationen auf seiner Internetseite (abrufbar unter: *im.baden-wuerttemberg.de*). Dadurch werden eine möglichst große Reichweite und eine zeitnahe Information der Bevölkerung sichergestellt.

Auch außerhalb konkreter Krisenereignisse werden diese Kanäle genutzt, um über Maßnahmen der persönlichen Krisenvorbereitung zu informieren. Hierzu zählen insbesondere allgemeine Hinweise zum richtigen Verhalten in unterschiedlichen Krisenszenarien, Informationen zur individuellen Vorsorge sowie Hinweise auf bestehende Warn- und Informationsangebote.

Weiterführende Erläuterungen zu Notfalltreffpunkten können einer eigens hierfür eingerichteten Internetseite (abrufbar unter: *www.notfalltreffpunkt-bw.de*) entnommen werden. Die Gemeinden sollten durch eine entsprechende Beschilderung sowie Hinweise in den Gemeindemitteilungen dafür sorgen, dass die Lage der jeweiligen Notfalltreffpunkte den Bürgerinnen und Bürgern bekannt ist.

Die Polizei BW nutzt soziale Medien zur schnellen und unmittelbaren Kommunikation mit der Öffentlichkeit zu Zwecken der einsatzbegleitenden Öffentlichkeitsarbeit, polizeilichen Berichterstattung, für Fahndungen, Prävention, Imagepflege und Nachwuchswerbung. Aktuell werden hierbei über 50 Kanäle sowohl dezentral durch einzelne Polizeidienststellen und Einrichtungen für den Polizeivollzugsdienst als auch zentral durch das Landespolizeipräsidium, auf Instagram, X, Facebook, WhatsApp, Mastodon und YouTube genutzt. Die konkrete Plattformauswahl richtet sich hierbei grundsätzlich nach einer Betrachtung von rechtlichen, gesellschaftlichen sowie ressourcentechnischen Aspekten vor dem Hintergrund

des polizeilichen Ziels, einen möglichst großen Teil der Bevölkerung und der Medien mit relevanten Informationen zu versorgen. Diese Plattformen kommen auch zur Kommunikation in Krisensituationen zum Einsatz, um die Öffentlichkeit zu Zwecken der polizeilichen Aufgaben in Form von Gefahrenabwehr und Strafverfolgung zu erreichen. Dies umfasst auch die Veröffentlichung von Informationen und Verhaltenshinweisen zum Schutz der Bevölkerung.

Darüber hinaus können auf der zentralen Internetpräsenz der Polizei BW (abrufbar unter: *www.polizei-bw.de*) aktuelle Beiträge und Warnhinweise veröffentlicht werden. Bei Bedarf nutzt die Polizei BW zur Warnung und Information der Menschen im Land auch MoWaS.

Das Ministerium für Umwelt, Klima und Energiewirtschaft nutzt zur Information der Bevölkerung in Krisensituationen ebenfalls verschiedene digitale Kommunikationswege. Zum einen erfolgt die Information über soziale Medien, den offiziellen Internetauftritt des Ministeriums für Umwelt, Klima und Energiewirtschaft sowie – je nach Anlass – über themenspezifische Internetseiten, wie beispielsweise das Hochwasserportal Baden-Württemberg.

Die Hochwasservorhersagezentrale des Landes Baden-Württemberg hat zudem die Möglichkeit, bei Hochwassergefahr die Bevölkerung über MoWaS zu informieren und zu warnen. Ein Bestandteil der Warnung sind Verhaltenshinweise für Bürgerinnen und Bürger während und nach dem Hochwasserfall, welche auf *www.hochwasserbw.de* bereitgestellt werden.

Im Bereich des radiologischen Notfallschutzes und der nuklearspezifischen Gefahrenabwehr (NGA) des Ministeriums für Umwelt, Klima und Energiewirtschaft wird die Information der Bevölkerung in aller Regel über die für den Katastrophenschutz zuständigen Behörden (Innenministerium, Regierungspräsidien und Polizeipräsidien/bei NGA) und den Bund sichergestellt. Zur Vorabinformation für Unfälle im Bereich auch grenznaher (Schweizer) Kernkraftwerke wurden bisher Infobroschüren für die Bevölkerung in Papierform in der Umgebung der Kernkraftwerke verteilt. Diese sind auch digital auf den Internetauftritten der Regierungspräsidien abrufbar.

Das Ministerium für Soziales, Gesundheit und Integration stellt den Bürgerinnen und Bürgern Informationen auf seinem Internetauftritt und über die sozialen Medien (Instagram, Facebook, LinkedIn, Mastodon, X, zum Teil YouTube) zur Verfügung. Zudem haben die Bürgerinnen und Bürger die Möglichkeit, Anfragen an das Ministerium zu richten.

Auch das Ministerium für Verkehr informiert Bürgerinnen und Bürger in Krisensituationen über verschiedene digitale Kommunikationswege. Zur Aufklärung vor Krisenereignissen sowie zur begleitenden Information in Krisensituationen nutzt das Ministerium für Verkehr bei Bedarf seine regulären digitalen Kanäle. Dazu zählen insbesondere die Internetseite des Ministeriums sowie die Auftritte in sozialen Medien und auch die bwegt-App für unter anderem die Fahrtauskunft mit einer Nachrichten-Funktion. Diese digitalen Angebote werden durch die klassische Medienarbeit ergänzt. Über diese Kanäle werden unter anderem Hinweise zu Auswirkungen auf den Verkehr, zu Verhaltensanweisungen sowie zu allgemeinen Aspekten der persönlichen Krisenvorbereitung kommuniziert. Der letzte größere Kommunikationsbedarf dieser Art hat während der Coronapandemie stattgefunden. Im Verkehrsbereich hat sich dabei gezeigt, dass neben digitalen Instrumenten und klassischer Medienarbeit zumindest im Krisenfall die Durchsagen an Bahnsteigen oder Bahnhöfen oder Aushänge in Fahrzeugen weiterhin eine hohe Relevanz besitzen.

In die digitale Kommunikation sind über einen regelmäßigen Austausch auch die Verkehrsverbünde sowie die Eisenbahnverkehrsunternehmen eingebunden. Diese informieren ihrerseits über eigene Internetauftritte, Apps und soziale Medien und tragen so zur Verbreitung verkehrsbezogener Informationen und Hinweise bei.

Um Bürgerinnen und Bürger über Möglichkeiten zur persönlichen Krisenvorbereitung zu informieren, wurde der Internetauftritt des Ministeriums für Ernährung, Ländlichen Raum und Verbraucherschutz um das Thema „Ernährungsnotfallvorsorge“ ergänzt, um klare und praxisnahe Empfehlungen bereitzustellen. Hier finden Interessierte praktische Hinweise zur privaten und staatlichen Vorsorge. Darüber hinaus gibt es Antworten auf Fragen rund um das Thema Notfallvorsorge und konkrete Tipps, wie man zum Beispiel im Ernstfall auch ohne Strom kochen und sich gut versorgen kann. Damit unterstützt das Ministerium die Bürgerinnen und Bürger dabei, sich eigenverantwortlich auf mögliche Krisensituationen vorzubereiten, und trägt zugleich zur Stärkung der gesamtgesellschaftlichen Resilienz in Baden-Württemberg bei.

Darüber hinaus werden bei konkreten Vorfällen zum Beispiel im Bereich der Trinkwasserversorgung entsprechende Meldungen in MoWaS eingespeist.

2. wie die Landesregierung eine resiliente Kommunikationsinfrastruktur für diese Zwecke sicherstellt (unter Angabe einer Bewertung von [Teil-]Ausfällen von Mobilfunknetz, Breitbandnetz, Satellitenkommunikation, DAB+, UKW etc.);

Zu 2.:

Zur Sicherstellung der in Ziffer 1 dargestellten (digitalen) Kommunikationswege der Landesregierung in Krisensituationen ist Folgendes festzustellen:

Die Resilienz der Kommunikationsinfrastruktur ist durch mehrere Rückfallebenen beziehungsweise Ausweichmöglichkeiten sichergestellt. Das bedeutet, Führungs- und Warnkommunikation wird nicht auf einzelne öffentliche Netze (Mobilfunk/ Internet) gestützt, sondern auf einen mehrschichtigen Kommunikationsmix aus eigenständigen Systemen der Behörden und Organisationen mit Sicherheitsaufgaben (BOS), Rückfallebenen und voneinander unabhängigen Warnkanälen. Dies gilt auch für die Kommunikation in und mit den Notfalltreffpunkten. Grundsätzlich kann auf die gesamte Bandbreite der Kommunikationsmöglichkeiten zugegriffen werden, die der staatlichen Gefahrenabwehr zur Verfügung stehen. Zu nennen sind hierbei Digitalfunk BOS, Mobilfunk und Satellitenkommunikation. Zur Warnung und Information der Öffentlichkeit, wie unter Ziffer 1 dargestellt, steht MoWaS, aber auch unabhängig hiervon beispielsweise Radio und Fernsehen, die Internetauftritte des Landes einschließlich der Auftritte in den sozialen Medien ober auch der Sonderinformationsdienst der Landesregierung (siehe Stellungnahme zu Ziffer 1) zur Verfügung.

MoWas ist als hochverfügbares, gehärtetes System zur Warnung der Bevölkerung konzipiert. Die Übertragung der Warnmeldung innerhalb von MoWaS erfolgt redundant via Satelliten und kabelgebunden. Die technische Basis macht das System unempfindlich gegen Stromausfälle und Ausfälle der terrestrischen Übertragungswege. Wie in der Stellungnahme zu Ziffer 1 dargestellt, können alle an MoWaS angeschlossenen Warnmittel zeitgleich und mit einer Eingabe ausgelöst werden. So ist sichergestellt, dass bei Ausfall einzelner Warnkanäle die Warnmeldungen über die weiteren Warnkanäle ausgeliefert werden.

Der Digitalfunk BOS ist ein flächendeckendes, hochverfügbares und sicheres Kommunikationsnetz. Er wurde im Auftrag von Bund und Ländern seit 2007 durch die gemeinsame Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) aufgebaut und wird durch die anstaltseigene Betreibergesellschaft betrieben und überwacht. Auf Grundlage eines Verwaltungsratsbeschlusses der BDBOS wird der Betrieb des Digitalfunks BOS bei lokalen und regionalen Stromausfällen sowie darüberhinausgehenden Szenarien bis hin zu einem Blackout – ohne Einschränkungen in der Netzkapazität oder der Flächenversorgung – für mindestens 72 Stunden sichergestellt. In Baden-Württemberg wurden die Maßnahmen zur Netzhärtung im Rahmen des Projekts „Modernisierung Digitalfunk 2030“ beim Präsidium Technik, Logistik, Service der Polizei weitgehend umgesetzt. Die letzte Ausbaustufe zur Optimierung dieser Infrastruktur soll bis 2027 abgeschlossen werden. Die Fahrzeugfunkversorgung bei einem landesweiten Stromausfall ist seit Ende 2023 gewährleistet.

Ergänzend zum Digitalfunk BOS wird die Kommunikation zwischen dem Ministerium des Inneren, für Digitalisierung und Kommunen als oberster Katastrophenschutzbehörde, den Regierungspräsidien als höheren Katastrophenschutzbehörden und den Stadt- und Landkreisen als untere Katastrophenschutzbehörden mittels von der öffentlichen Stromversorgung unabhängigen Satellitenkommunikationssystemen (Telefonie, Datenfunk, Push-To-Talk Gruppenkommunikation/Projekt „SaFe“) sichergestellt. Diese Kommunikationsmedien werden in regelmäßigen, kurzen Abständen mit den unteren Katastrophenschutzbehörden und der obersten Katastrophenschutzbehörde beübt, um die Einsatzbereitschaft zu gewährleisten.

Die Verpflichtung zur Aufrechterhaltung der (öffentlichen) Telekommunikationsdienste liegt grundsätzlich in der Verantwortung der Telekommunikationsunternehmen. Die Pflichten zur Aufrechterhaltung des Betriebs, zur Vorsorgeplanung und zur Umsetzung geeigneter Sicherheitsmaßnahmen ergeben sich für Telekommunikationsnetzbetreiber insbesondere aus dem Telekommunikationsgesetz sowie aus den Vorgaben des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz – BSIG).

Die analoge (UKW) und digitale Hörfunkverbreitung (DAB+) bildet nach Überzeugung der Landesregierung einen zentralen Teil der Kommunikationsinfrastruktur in Baden-Württemberg. Die Marktdurchdringung von DAB+ und entsprechender Empfangsgeräte nimmt dabei stetig zu und gewinnt immer mehr an Bedeutung. Die Landesanstalt für Kommunikation hat in den vergangenen Jahren erfolgreich erhebliche Anstrengungen zum weiteren Ausbau des DAB+-Netzes in Baden-Württemberg unternommen. Gleichzeitig stellt UKW auch weiterhin einen wichtigen Verbreitungsweg von Hörfunkangeboten sowohl für den öffentlich-rechtlichen Rundfunk als auch den privaten Rundfunk dar. Gerade mit Blick auf den privaten Rundfunk bildet die analoge Verbreitung eine wichtige Refinanzierungsquelle für digitale Innovationen und Verbreitung in DAB+. Die Landesregierung hat daher zur Schaffung von Planungssicherheit für die Anbieter mit der Novelle des Landesmediengesetzes im Jahr 2022 eine Verlängerungsmöglichkeit aller bestehenden UKW- und DAB-Zuweisungen im Hörfunk bis Ende 2032 gegeben. Die Landesregierung beobachtet fortwährend die weiteren Entwicklungen zu den Verbreitungswegen im Bereich des Hörfunks und steht mit den Beteiligten in engem Austausch.

3. wie sie eine Notwendigkeit des Erhalts von DVB-T2 und Simulcast (gleichzeitiger Betrieb von UKW und DAB+) im Speziellen den Erhalt von UKW vonseiten des öffentlich-rechtlichen Rundfunks im Hinblick auf Resilienz in Krisensituationen bewertet;

Zu 3.:

Aus Sicht der Landesregierung leistet die digitale Antennenfernsehverbreitung über DVB-T2 einen Beitrag für ein breites und attraktives Portfolio der Verbreitungswege für Rundfunk sowie den Grundversorgungsauftrag im Bereich des öffentlich-rechtlichen Rundfunks. Im Übrigen wird auf die Stellungnahme zu Ziffer 2 verwiesen.

4. ob die Landesregierung aktuell Maßnahmen plant, um die digitale Vernetzung des Bevölkerungsschutzes zu verbessern (wenn ja, welche);

Zu 4.:

Die Landesregierung verfolgt aktuell Maßnahmen, um die digitale Vernetzung im Bevölkerungsschutz weiter zu verbessern. Schwerpunkt ist der fortlaufende Ausbau einer einheitlichen, verwaltungsebenenübergreifenden digitalen Lage- und Informationsplattform sowie die Erweiterung des Nutzer- und Partnerkreises. Insbesondere wird hierzu die Elektronische Lagedarstellung Bevölkerungsschutz (ELD-BS) fortlaufend weiterentwickelt, unter anderem mit dem Update ELD-BS 4.0 und zusätzlichen Funktionen und Modulen für Lagebewertung, Planungs-

unterstützung und behördenübergreifenden Datenaustausch. Ferner wird derzeit die Einbindung weiterer Nutzergruppen vorbereitet beziehungsweise umgesetzt. Flankierend werden zielgruppenbezogene Online-Fortbildungen zur Nutzung neuer Funktionalitäten (ELD-BS 4.0) vorgesehen, um den Rollout und die durchgängige Nutzung im Bevölkerungsschutz und Krisenmanagement zu unterstützen.

Bei den Einrichtungen des Bevölkerungsschutzes ist insbesondere eine eigenständige und hochverfügbare Sprachkommunikation für den einsatzrelevanten Informationsaustausch von großer Bedeutung. Das Land unterstützt die Gemeindefeuerwehren daher bei der Nutzung des Digitalfunks BOS als einheitliches, übergreifendes Kommunikationssystem. Dies erfolgt unter anderem durch die Gewährung von Zuwendungen nach der Verwaltungsvorschrift des Innenministeriums über Zuwendungen für das Feuerwehrwesen (ZFeuVwV), die Bereitstellung einer vernetzten Infrastruktur zur Übertragung von Update-Daten für die Digitalfunkgeräte und die Veröffentlichung von Handlungsleitfäden zum Digitalfunk BOS. Darüber hinaus hat das Land die Feuerwehraufsicht mit satellitengestützten Kommunikationssystemen ausgestattet sowie eine Plattform für eine erweiterte Nutzung des Systems geschaffen (Projekt „SaFe“). Das Land vernetzt die Gemeindefeuerwehren beziehungsweise die Gemeinden als Träger der Feuerwehren darüber hinaus in den Fällen, in denen unmittelbar das Land Zuständigkeiten hat. Dies ist beispielsweise bei der Erfassung der Daten für die Feuerwehr-Jahresstatistik der Fall aber auch bei der Anmeldung zu Lehrgängen an der Landesfeuerwehrschule.

Jede Gemeinde hat darüber hinaus nach § 3 des Feuerwehrgesetzes als weisungsfreie Pflichtaufgabe im Rahmen der kommunalen Selbstverwaltung auf eigene Kosten eine leistungsfähige Feuerwehr aufzustellen, auszurüsten und zu unterhalten. Die Umsetzung von Projekten zur digitalen Vernetzung innerhalb von Gemeindefeuerwehren, zwischen Gemeindefeuerwehren oder mit der Integrierten Leitstelle und anderen externen Stellen ist damit eine kommunale Aufgabe, soweit dies vor Ort als erforderlich angesehen wird. Die Landkreise unterstützen entsprechend den Regelungen des § 4 des Feuerwehrgesetzes außerdem die Gemeinden in unterschiedlichster Form. Unter anderem sind sie für den Aufbau und Betrieb von unabhängigen Kommunikationsnetzen zur Alarmierung der Einsatzkräfte zuständig. Darüber hinaus gibt es teilweise auch weitere Projekte, beispielsweise für ergänzende Benachrichtigungssysteme für Einsatzkräfte oder die Bereitstellung von Verwaltungs- oder Ausbildungssoftware.

5. ob der Landesregierung Projekte zu digitalen Schnittstellen zwischen den Führungs- und Lagezentren der Polizei und den Integrierten Leitstellen für Feuerwehr und Rettungsdienst bekannt sind und wie sie diese bewertet und ggf. voranbringt;

Zu 5.:

Für die Sicherstellung der unabhängigen, gesicherten Kommunikation zwischen den Führungs- und Lagezentren der Polizei und den Integrierten Leitstellen für Feuerwehr und Rettungsdienst (ILS) bestehen gemeinsame Einsatzpläne für die Nutzung des Digitalfunks BOS.

Die Führungs- und Lagezentren der Polizei und die ILS arbeiten mit unterschiedlichen Einsatzleit- (ELS) und Kommunikationsmanagementsystemen (KMS). Während die Polizei Baden-Württemberg über eine einheitliche Anwendung verfügt, sind bei den ILS ELS und KMS jeweils verschiedener Hersteller im Einsatz.

Ein bidirektionaler und medienbruchfreier Austausch von relevanten Einsatzinformationen zwischen dem ELS der Polizei sowie den Anwendungen der beteiligten BOS, wie zum Beispiel Feuerwehr und Rettungsdienst, kann die gegenseitigen Alarmierungs- und Verständigungsvorgänge beschleunigen sowie die Fehlerquote bei der Datenübermittlung zumindest reduzieren oder ausschließen.

Aus diesem Grund werden im Präsidium Technik, Logistik, Service der Polizei derzeit die technische Umsetzbarkeit einer interoperablen Leitstellenkommunikation betrachtet sowie organisatorische, technische und rechtliche Herausforderungen identifiziert.

6. wie die Integrierten Leitstellen gegen Angriffe auf deren digitale Infrastruktur geschützt sind und welche präventiven Vorgaben hierzu bestehen;

Zu 6.:

Die Trägerschaft für die ILS wird für den Feuerwehrteil der Leitstellen durch die Stadt- und Landkreise und für den rettungsdienstlichen Teil der Leitstellen durch die Landesverbände des Deutschen Roten Kreuzes wahrgenommen. Die Stadt- und Landkreise üben die Trägerschaft im Rahmen der kommunalen Selbstverwaltung als weisungsfreie Pflichtaufgabe aus. Damit legen sie die Standards für die Sicherheitsarchitektur ihrer ILS im Rahmen der gesetzlichen Vorgaben und dem Stand der Technik selbst fest. Nach ZFeuVwV ist eine Voraussetzung bei der Förderung von Maßnahmen zur Beschaffung von Technik für Alarmierungseinrichtungen und die Einrichtung von ILS, dass für die betroffenen informationstechnischen Systeme die Sicherheitsgrundsätze, die Sicherheitsstrategie sowie die Pflichten und Berichtswege entsprechend der Verwaltungsvorschrift Informationssicherheit des Landes in der jeweils geltenden Fassung sinngemäß umgesetzt werden. Dies ist im Verwendungsnachweis zu bestätigen.

Ein elementarer Bestandteil der Arbeit der Cybersicherheitsagentur Baden-Württemberg (CSBW) liegt nach § 3 des Cybersicherheitsgesetzes (CSG) in der Prävention. Dieses präventive Angebot steht auch den Stadt- und Landkreisen für ihre Aufgaben als Träger der ILS zur Verfügung. Das Präventionsangebot der CSBW umfasst dabei ein breites Schulungs- und Sensibilisierungsangebot zu Themen der Cybersicherheit, umfassende Informationsmaterialien inklusive Erklärvideos, Vorlagen zur Erstellung von Sicherheitsrichtlinien und -konzepten oder auch eine individuelle Beratung zu allen Themen der Cybersicherheit.

Darüber hinaus kann die CSBW auch im Falle eines bereits erfolgten Cyberangriffs für die Stadt- und Landkreise für ihre Aufgaben als Träger der ILS tätig werden, indem sie zum Beispiel bei der Vorfallbehandlung unterstützt. Von der Analyse des Sicherheitsvorfalls über die technische Unterstützung und Beratung bei der Behandlung des Sicherheitsvorfalls (auch vor Ort durch Entsenden eines Mobile Incident Response Teams) bis hin zur Bereitstellung eines Notfall-Equipments und die Unterstützung bei der Krisenkommunikation steht die CSBW an der Seite der betroffenen Stelle.

7. inwiefern insbesondere Vorgaben zum betrieblichen Kontinuitätsmanagement (BCM) nach einem digitalen (bspw. durch Ransomware, Datendiebstahl, Datenlöschung) oder physischen Angriff (bspw. durch Feuer, Einsturz, notwendige Evakuierung) für die Integrierten Leitstellen bestehen bzw. umgesetzt sind;

Zu 7.:

Maßnahmen des BCM liegen ebenfalls in der Zuständigkeit der Träger der ILS. Auf die Ausführungen zur Trägerschaft der ILS in Ziffer 6 wird verwiesen.

Insofern eine ILS in der Trägerschaft einer Kommune liegt, ergibt sich für diese aus § 3 Absatz 10 der Cybersicherheitsverordnung (CSVO) die Empfehlung, die Maßnahmen nach § 3 Absätze 3 bis 5 und 8 umzusetzen. Die dort aufgeführten Maßnahmen, wie die Aufrechterhaltung des Betriebs durch ein Backup-Management und die Wiederherstellung nach einem Notfall- sowie ein Krisenmanagement, sind explizite Maßnahmen eines BCM.

8. ob es zur Wahrung der digitalen Resilienz im Krisenfall Ausfalloptionen für bspw. das Vorhalten von wichtigen Daten – wie es kritische Patientendaten sind – oder notwendiger Rechenleistung, welche physisch nicht in Baden-Württemberg und nicht in einem angrenzenden Bundesland angesiedelt sind, gibt;

Zu 8.:

Mit der Produktivnahme der ersten Leistungen im ressortübergreifenden Projekt MEDI:CUS (Medizindaten-Infrastruktur: cloudbasiert, universell, sicher) wird ab Ende 2026 ein weiterer Meilenstein auf dem Weg zur Krisenresilienz des Gesundheitswesens erreicht werden. So wird es für teilnehmende Einrichtungen zunächst der klinischen Versorgung unter anderem möglich, Backups für den Krisenfall neben den lokalen Möglichkeiten auch georedundant abzulegen. Mit dem weiteren Ausbau von MEDI:CUS ab 2027 werden daneben immer mehr Services angeboten, die durch die cloudbasierte orts- und anbieterunabhängige Architektur hinsichtlich Ausfallsicherheit deutlich einfacher zu schützen sein werden, als in den heutigen überwiegend lokal aufgestellten Strukturen.

Um für einen Krisenfall, wie etwa im Falle eines digitalen Ausfalls, auch weiterhin die Patientensicherheit (insbesondere die Versorgung) aufrechterhalten zu können, sind die Krankenhäuser in eigener Zuständigkeit unter anderem nach § 28 Absatz 2 des Landeskrankenhausgesetzes Baden-Württemberg verpflichtet, geeignete Vorkehrungen zu treffen. Dies soll insbesondere durch Erstellung und Fortschreibung von Krankenhaus Alarm- und Einsatzplänen (KAEP) sichergestellt werden. Ein funktionierender KAEP ist deshalb ein zentrales Instrument, um schnell, koordiniert und effektiv handeln zu können. Auf Betreiben des Ministeriums für Soziales, Gesundheit und Integration wurde ein Rahmenplan erstellt, mit welchem die Krankenhausträger bei der Erstellung, Weiterentwicklung und Anwendung eines strukturierten KAEP unterstützt werden. Der Rahmenplan bietet eine praxisnahe Orientierung und berücksichtigt die aktuellen gesetzlichen Anforderungen, fachlichen Standards sowie die Erfahrungen aus vergangenen Einsatzlagen. Ziel ist es, dass das jeweilige Krankenhaus sich gezielt auf diese besonderen Anforderungen, wie etwa eines digitalen Ausfalls, vorbereiten kann.

Bei den Zentren für Psychiatrie sind teilweise Ersatzprozesse mit Daten von Patientinnen und Patienten in den einzelnen Häusern verfügbar. Die Sicherung der Daten erfolgt in unterschiedlichen Ländern der Bunderepublik Deutschland.

Für die Universitätsklinika des Landes gilt: Zur Wahrung der digitalen Resilienz bestehen für kritische Daten und Rechenleistung Notfall- und Wiederherstellungsprozesse gemäß KRITIS- und BSI-Vorgaben. Intern stellen mehrere Rechenzentren (mindestens zwei) eine Hochverfügbarkeit sicher. Zusätzlich gibt es Konzepte, um kritische Patientendaten im Krisen- oder IT-Notfall analog auf Papier bereitzustellen. Für alle an der kritischen Versorgung beteiligten Bereiche existieren dezentrale Notfallpläne wie gegebenenfalls lokal oder durch Papier der Betrieb aufrechterhalten werden kann. Details zur IT-Sicherheits-Architektur unterliegen der Vertraulichkeit. Perspektivisch könnten versorgungsrelevante Kerndatensätze auch durch MEDI:CUS als Multicloud vorgehalten werden.

Ein Beispiel für ein von der Landesverwaltung vorgehaltenes und genutztes System ist der in Ziffer 1 beschriebene Sonderinformationsdienst der Landesregierung. Das System wird hoch skalierbar und unabhängig von den übrigen Systemen des Landes betrieben.

Für den Bereich der pädagogischen IT-Verfahren gilt: Schulische Verwaltungs-IT (zum Beispiel Stundenplanprogramm, digitales Tagebuch) wird durch den Schulträger verantwortet. Die Landesregierung hat keine Kenntnis darüber, wie resilient kommunale IT-Strukturen im Einzelfall sind.

Landesseitig bereitgestellte pädagogische IT-Verfahren der digitalen Bildungsplattform verfügen über eine Ausfallredundanz inklusive örtlicher Trennung der redundanten Rechenzentren.

Im Ressortbereich des Ministeriums für Umwelt, Klima und Energiewirtschaft wird überwiegend die Infrastruktur der BITBW genutzt. In Ausnahmefällen, zum Beispiel in der Zusammenarbeit mit anderen Ländern, nutzt die Landesanstalt für Umwelt Baden-Württemberg in geringem Maße Cloud-Lösungen externer Dienstleister für bestimmte Fachdaten oder Internetauftritte. Die jeweiligen Rechenzentren liegen teilweise außerhalb Baden-Württembergs oder angrenzender Länder der Bundesrepublik.

Sofern Datenhaltungen und Rechenzentrumsdienste, welche physisch nicht in Baden-Württemberg und nicht in einem angrenzenden Land der Bundesrepublik angesiedelt sind, Daten aus dem Geschäftsbereich der baden-württembergischen Justiz betreffen, sind entweder über vertraglich festgelegte IT-Verbünde mit Justizverwaltungen aus anderen Ländern oder über standardisierte Verträge mit externen IT-Dienstleistern Ausfalloptionen entsprechend dem Schutzbedarf der Daten festgelegt, die mit dem Betriebs-Standard in Baden-Württemberg vergleichbar sind.

9. ob aktuell im Fall eines Cybersicherheitsvorfalls, welcher die Verfügbarkeit, Integrität oder Vertraulichkeit von kritischen IT-Systeme beeinträchtigt, physische Faktoren wie bspw. das Runterfahren eines industriellen Hochofens mitbedacht werden;

Zu 9.:

Die Sicherstellung der Funktionsfähigkeit von Kritischen Infrastrukturen (KRITIS) ist in erster Linie Aufgabe der jeweiligen Betreiber. Ihnen obliegt es, erforderliche Maßnahmen zu treffen, um die von ihnen erbrachten kritischen Dienstleistungen auch im Fall einer Störung – hierzu zählen auch Störungen aufgrund von Cybersicherheitsvorfällen – aufrechterhalten beziehungsweise wiederherstellen zu können. Dies umfasst sowohl präventive Maßnahmen als auch die Vorplanung und Vorbereitung reaktiver Maßnahmen, um trotz aller Vorkehrungen mögliche Ausfälle zumindest in Teilen kompensieren und deren Auswirkungen abmildern zu können.

Als zentrales Element beim Schutz von KRITIS ist der sogenannte „All-Gefahren-Ansatz“ etabliert: Im Rahmen des Risiko- und Krisenmanagements zum Schutz KRITIS sollen möglichst alle denkbaren Gefahren und Szenarien, die die Funktionsfähigkeit von KRITIS teilweise oder ganz stören können, berücksichtigt werden – Naturgefahren, Gefahren durch technisches Versagen ebenso wie versehentliche und absichtliche menschliche Handlungen einschließlich der hieraus resultierenden Szenarien. Diese Betrachtungen umfassen damit auch die Betrachtung möglicher physischer Auswirkungen von Cybersicherheitsvorfällen.

Gerade bei kritischen IT-Systemen wie industriellen Steuerungssystemen oder auch bei Systemen der Gebäudetechnik werden physische Faktoren bei einer Vorfallbehandlung grundsätzlich mitbetrachtet. So beinhaltete auch die 2023 durchgeführte neunte Länder- und Ressortübergreifende Krisenmanagementübung LÜKEX 23 mit dem Thema „Cyberangriff auf das Regierungshandeln“ – an der sich Baden-Württemberg in der höchsten Beteiligungsform (vollübend) beteiligte – ein Szenario, in dem manipulierte Speicherprogrammierbare Steuerungen (SPS) als Ursache von Störungen in Rechenzentren beziehungsweise Dienstgebäuden behandelt wurden. Bei SPS handelt es sich um insbesondere in der Industrie aber auch in der Gebäudetechnik vielfach verbaute Geräte, die zur Steuerung oder Regelung einer Maschine oder Anlage eingesetzt und auf digitaler Basis programmiert werden. Beispiele hierfür sind SPS in Fertigungsanlagen, Kühlsystemen, Schließanlagen, Beleuchtungsanlagen, Wasserpumpen oder Alarmierungssystemen.

Sowohl das Ministerium für Wissenschaft, Forschung und Kunst als auch sein Geschäftsbereich setzen den BSI-IT-Grundschutz um. Innerhalb dieses Rahmenwerks werden Gefahren durch physische Faktoren und Cybergefahren im Zuge der Resilienzplanung fortlaufend geprüft. Durch technische, organisatorische, in-

frastrukturelle und personelle Gegenmaßnahmen wird ein angemessenes Sicherheitsniveau erreicht.

Für kritische IT-Systeme im Bereich des Ministeriums für Umwelt, Klima und Energiewirtschaft, wie zum Beispiel die Hochwasservorhersage oder die Kernreaktorfernüberwachung, wurden verschiedene Maßnahmen getroffen, die die Sicherheit und Stabilität der Systeme gewährleisten.

In einigen Zentren für Psychiatrie werden im Rahmen des BCM bei einem Cybersicherheitsvorfall, der die Verfügbarkeit, Integrität oder Vertraulichkeit kritischer IT-Systeme beeinträchtigt, auch physische Faktoren bedacht und berücksichtigt, zum Beispiel bei der Gebäudeleittechnik mit elektronischer Schließung.

Aus Sicht des Ministeriums der Justiz und für Migration sind physische Faktoren integrierte Bestandteile der Cybersicherheit und demzufolge der Bearbeitung von Cybersicherheitsvorfällen. Insoweit und sofern dies zur Schadensbegrenzung notwendig ist, kommt auch das Herunterfahren von IT-Systemen in Betracht.

Soweit Cybersicherheitsvorfälle die Sicherheit kritischer IT-Systeme im Ressortbereich des Ministeriums für Verkehr beeinträchtigen könnten, werden physische Faktoren im Zuge der Sicherheitskonzeption berücksichtigt.

Im Ministerium für Ernährung, Ländlichen Raum und Verbraucherschutz wurde ein ganzheitliches BCM etabliert, im Rahmen dessen für verschiedene Szenarien Notfallpläne entwickelt wurden und noch entwickelt werden, welche alle relevanten Aspekte, wie zum Beispiel IT, Strom- und Wasserversorgung, für zumindest einen Notbetrieb berücksichtigen, soweit dies bei Erstellung abschätzbar ist.

10. inwieweit der Landesregierung – in Anbetracht der Tatsache, dass die praktische Sicherstellung der Funktionsfähigkeit und der Schutz der KRITIS grundsätzlich deren Betreibern obliegt – praktische Kenntnisse über die digitale Arbeitsfähigkeit von KRITIS in Baden-Württemberg im Krisenfall hinsichtlich einer stabilen Stromversorgung vorliegen;

Zu 10.:

Die Nationale Strategie zum Schutz Kritischer Infrastrukturen definiert KRITIS als Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Im Sinne dieser Definition zählen in Baden-Württemberg Organisationen und Einrichtungen aus den Sektoren Energie, Ernährung, Finanz- und Versicherungswesen, Gesundheit, Informationstechnik und Telekommunikation, Siedlungsabfallentsorgung, Medien und Kultur, Staat und Verwaltung, Transport und Verkehr sowie Wasser zu den KRITIS.

Vor dem Hintergrund, dass die Sicherstellung der Funktionsfähigkeit von Kritischer Infrastruktur Aufgabe der jeweiligen Betreiber ist, obliegt es diesen, die erforderlichen Maßnahmen zu treffen, um die von ihnen erbrachten kritischen Dienstleistungen – beispielsweise auch im Falle eines Ausfalls der öffentlichen Stromversorgung – aufrecht erhalten zu können. Der Landesregierung liegen praktische Kenntnisse zur digitalen Arbeitsfähigkeit der KRITIS im Krisenfall nur in dem Umfang vor, in dem diese im Rahmen der Zusammenarbeit und des Informationsaustauschs mit den zuständigen Fachressorts, Aufsichts- und Sicherheitsbehörden sowie den jeweiligen Betreibern erhoben und lagebezogen aktualisiert werden. Insbesondere bezüglich des KRITIS-Sektors „Staat und Verwaltung“ wird auf die Stellungnahmen im Rahmen des Antrags der Abgeordneten Sascha Binder und Klaus Ranger und anderer SPD „Notstromversorgung der kritischen Infrastruktur in Baden-Württemberg“ (Drucksache 17/8664), dort gemeinsame Stellungnahme zu den Ziffern 1, 2, 4 und 8 sowie Stellungnahme zu Ziffer 11, verwiesen.

Im Bereich der Feuerwehren fördert das Land die Beschaffung von Netzersatzanlagen für Feuerwehrhäuser. Die Gemeinden und Städte werden durch die För-

derung darin unterstützt, die Funktionsfähigkeit ihrer Feuerwehrhäuser auch bei Ausfällen der Stromversorgung gewährleisten zu können. Im Rahmen der Erstausstattung von Rettungswachen fördert das Land ebenfalls die Notstromversorgung der baulichen Anlagen.

Krankenhäuser sind für den Krisenfall hinsichtlich einer stabilen Stromversorgung verpflichtet, einen aktuellen und wirksamen KAEP vorzuhalten. In der Investitionsförderung der Krankenhausfinanzierung werden die sogenannten Ersatznetz- oder Notstromanlagen als förderfähig eingestuft, soweit sie für den stationären Bereich erforderlich und angemessen sind. Die Staatshaushaltspläne des Landes Baden-Württemberg weisen für die jährlich aufzustellenden Jahreskrankenhausbauprogramme ein hohes jährliches Investitionsvolumen in Höhe von aktuell 248 Millionen Euro aus.

Die Rechenzentren der Universitätsklinika sind über Netzersatzanlagen (Notstrom) auch bei einem Stromausfall versorgt und können weiterhin interne IT-Dienste erbringen.

Die Notstromversorgung ist in den Zentren für Psychiatrie ebenfalls grundsätzlich gewährleistet.

Soweit Arzneimittel- und Medizinprodukthersteller sowie Apotheken eine KRITIS-Anlage betreiben, kommen nach Angaben der für die Arzneimittel- und Medizinprodukteüberwachung zuständigen Regierungspräsidien hinsichtlich einer stabilen Stromversorgung unter anderem Anlagen zur unterbrechungsfreien Stromversorgung zum Einsatz, um im Bedarfsfall zum Beispiel ein strukturiertes Herunterfahren von IT-Anlagen insbesondere zur Vermeidung von Datenverlust zu ermöglichen. Einzelne Betriebsstätten verfügen zudem über Notstromversorgung, um im Bedarfsfall für den gesetzlichen Versorgungsauftrag relevante Anlagen über einen begrenzten Zeitraum weiterbetreiben zu können.

Bezüglich KRITIS hat das Ministerium für Ernährung, Ländlichen Raum und Verbraucherschutz Zuständigkeiten im Bereich der Versorgung der Bevölkerung mit Trinkwasser. Für die Aufrechterhaltung der Wasserversorgung haben Wasserversorgungsunternehmen und Kommunen in den letzten Jahren deutlich in die Beschaffung von Notstromaggregaten investiert, sodass im Fall eines Stromausfalls die Wasserversorgung noch nicht flächendeckend, aber für wenige Tage relativ gut abgesichert wäre. Daten zu allen etwa 1 300 Wasserversorgern liegen der Landesregierung nicht vor. Beim derzeit laufenden Projekt Masterplan Wasserversorgung wird als Nebenaspekt mit einem Fragebogen zur Organisation der Wasserversorgung ebenfalls abgefragt, ob Notstromaggregate vorhanden sind – auch um die Betreiber für das Thema zu sensibilisieren. Eine erste Auswertung der mittels Selbstauskunft erhobenen Daten zeigt, dass von circa 440 Betreibern rund 55 % angegeben haben, ein Notstromaggregat sei vorhanden oder ein Handbetrieb möglich.

11. inwieweit der Landesregierung – in Anbetracht der Tatsache, dass die Sicherstellung der Funktionsfähigkeit und der Schutz der KRITIS grundsätzlich deren Betreibern obliegt – praktische Kenntnisse über die digitale Arbeitsfähigkeit von KRITIS im besonderen Fall eines Cybersicherheitsvorfalls, welcher die Verfügbarkeit, Integrität oder Vertraulichkeit von kritischen IT-Systemen beeinträchtigt, vorliegen;

Zu 11.:

Der Landesregierung liegen praktische Kenntnisse zur digitalen Arbeitsfähigkeit der KRITIS im Krisenfall in dem Umfang vor, in dem diese im Rahmen der Zusammenarbeit und des Informationsaustauschs mit den zuständigen Fachressorts, Aufsichts- und Sicherheitsbehörden sowie den jeweiligen Betreibern erhoben und lagebezogen aktualisiert werden.

Den speziellen bundesrechtlichen Rechtsrahmen für die IT-Sicherheit von bestimmten KRITIS und damit auch die Vorgaben für Meldepflichten von Sicher-

heitsvorfällen in diesen KRITIS gestaltet der Bund durch das BSI-Gesetz (BSIG). In der nachgelagerten BSI-Kritisverordnung (BSI-KritisV) bestimmt der Bund, welche Anlagen (aus Bundessicht) zu den KRITIS im Sinne des BSIG zählen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist gemäß BSIG die zuständige Aufsicht- und Meldebehörde für entsprechende KRITIS-Betreiber und überwacht unter anderem die Meldepflichten bei Cybersicherheitsvorfällen.

Die Länder haben keine unmittelbare Zuständigkeit für die IT-Sicherheitsaufsicht dieser KRITIS-Betreiber, sondern überwachen fachliche Anforderungen, wenn Sektor-Unternehmen in Landeszuständigkeit liegen. Davon unbenommen ist die CSBW in Baden-Württemberg die zentrale Kontaktstelle nach § 8b BSIG und erhält in diesem Rahmen BSI-Informationen über betroffene KRITIS-Unternehmen im Land beziehungsweise gibt relevante Informationen des BSI an diese weiter.

Die digitale Arbeitsfähigkeit der vier Universitätsklinika wird auch im Falle eines Cybersicherheitsvorfalls durch ein mehrstufiges Sicherheits- und Notfallkonzept gewährleistet. Dazu gehören definierte Incident- und Security-Incident-Prozesse, mehrere Rechenzentren zur Hochverfügbarkeit, analoge Fallback-Lösungen für kritische Patientendaten sowie dezentrale Notfallpläne in allen versorgungsrelevanten Bereichen. Ergänzend werden gesetzliche KRITIS- und BSI-Vorgaben umgesetzt, einschließlich Angriffserkennung, BCM und regelmäßiger Tests.

Soweit Arzneimittel- und Medizinprodukteherstellersowie Apotheken eine KRITIS-Anlage betreiben, beschränken sich die verfügbaren Informationen überwiegend auf Vorsorgemaßnahmen zur Datensicherungen und Backup-Konzepte für Warenwirtschaftssysteme.

Die Justiz verfügt über einen Prozess zur Bearbeitung von Cybersicherheitsvorfällen, der sich bezüglich der Schnittstellen mit der CSBW und der BITBW bewährt hat und die Vorgaben des CSG und der Cybersicherheitsverordnung umsetzt.

Für das Ministerium für Ernährung, Ländlichen Raum und Verbraucherschutz wird für ein solches Szenario aktuell ein Notfallplan entwickelt, welcher zumindest einen Notbetrieb sicherstellen soll. Darüber hinaus erfolgt bereits seit 2016 eine regelmäßige Prüfung und Zertifizierung der Informationssicherheit nach BSI-Grundschutz und damit verbunden eine stetige Weiterentwicklung der Resilienz im Bereich der Cybersicherheit, um eventuelle Angriffe frühzeitig abwehren zu können.

Im Bereich der Trinkwasserversorgung sind die großen Wasserversorgungsunternehmen in Baden-Württemberg ebenfalls bereits BSI-zertifiziert beziehungsweise streben dies an.

Auf die Stellungnahme der Landesregierung zum Antrag der Abgeordneten Georg Heitlinger und Daniel Karrais und anderer FDP/DVP „Cybersicherheit im Ernährungssektor in Baden-Württemberg“ (Drucksache 17/7934) wird verwiesen.

Darüber hinaus wird auf die nachfolgenden Ausführungen zum KRITIS-Dachgesetz und zum NIS2-Umsetzungsgesetz in Ziffer 12 verwiesen.

12. ob die Landesregierung einen Bedarf sieht, notwendige – die bundes- und EU-weiten Entwicklungen und Vorgaben begleitende – Maßnahmen zu prüfen, um die Sicherheit bei KRITIS in Baden-Württemberg zu erhöhen (evtl. wissenschaftliche Analysen, Umsetzungshilfen);

Zu 12.:

Mit dem KRITIS-Dachgesetz, das am 29. Januar 2026 vom Deutschen Bundestag beschlossen wurde, werden erstmals sektorenübergreifende Regelungen zum physischen Schutz von KRITIS geschaffen. Mit dem KRITIS-Dachgesetz wird die Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen (sogenannte CER-Richtlinie) in nationales Recht umgesetzt.

Das KRITIS-Dachgesetz ergänzt das Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2-Umsetzungsgesetz). Das NIS2-Umsetzungsgesetz ist die nationale Umsetzung der NIS-2-Richtlinie und novelliert das BISG. Das NIS2-Umsetzungsgesetz erhöht die Anforderungen an die Cybersicherheit der Bundesverwaltung sowie bestimmter (KRITIS-)Unternehmen.

Wie in der Stellungnahme zu Ziffer 11 dargestellt, liegt die Zuständigkeit für bestimmte KRITIS-Unternehmen gemäß BSIG und BSI-KritisV beim BSI. Eine Unterstützung dieser KRITIS-Betreiber durch die CSBW würde hier zu einer rechtlichen Vermischung der Zuständigkeiten führen. Darüber hinaus würde durch ein Vorhalten entsprechender Unterstützungsleistungen bei der CSBW auch für KRITIS-Unternehmen in Baden-Württemberg ein zusätzlicher Ressourcenbedarf entstehen, der in kommenden Haushalten Niederschlag finden müsste.

Im Zuständigkeitsbereich des Ministeriums für Ernährung, Ländlichen Raum und Verbraucherschutz werden die Wasserversorgungsunternehmen und Kommunen bereits anhand von Handreichungen für Maßnahmen zur Erhöhung der Sicherheit der Wasserversorgung sensibilisiert, unter anderem im Fall einer Unterbrechung der Stromversorgung oder im Bereich der IT-Sicherheit. Ausfallszenarien und entsprechende Maßnahmen, um die Wasserversorgung, gegebenenfalls mit einer reduzierten Wassermenge, aufrechterhalten zu können, sollen ferner in den verpflichtenden, mit den Trinkwasserüberwachungsbehörden abzustimmenden Notfallmaßnahmenplänen der Wasserversorger festgehalten sein.

Für den Ernährungsbereich wird auf die Stellungnahme der Landesregierung zum Antrag der Abgeordneten Georg Heitlinger und Daniel Karrais und anderer FDP/DVP „Cybersicherheit im Ernährungssektor in Baden-Württemberg“ (Drucksache 17/7934), Ziffer 7, verwiesen.

13. ob in der Vergangenheit bereits wissenschaftliche Analysen zum Thema Cybersicherheit in der öffentlichen Verwaltung in Baden-Württemberg angefertigt wurden (bspw. zu gegenseitigen Abhängigkeiten zwischen Behörden oder ob Ausfälle übergeordneter Behörden auch darunterliegende Behörden betreffen würden);

Zu 13.:

Bezüglich der Cybersicherheitsforschung im Land wird auf die Antwort der Landesregierung auf die Große Anfrage der Fraktion GRÜNE „Cybersicherheit in Baden-Württemberg“ (Drucksache 17/6765), Frage 3, verwiesen.

Grundsätzlich beobachten die Cybersicherheitsexperten im Ministerium des Inneren, für Digitalisierung und Kommunen mit Interesse entsprechende Projekte und Initiativen zum Thema Cybersicherheit. So zum Beispiel das vom Ferdinand-Steinbeis-Institut in Kooperation mit Schwarz Digits initiierte offene Projekt „Europas innere und äußere Sicherheit im Spannungsfeld digitaler Souveränität“. Ziel dieses Projekts ist es, Fähigkeiten zu identifizieren, die entscheidend für Resilienz und Sicherheit einer digitalen Souveränität Europas sind, um damit neue Perspektiven für praktisch umsetzbare, digitalsouveräne Lösungen zu eröffnen.

Ein weiteres wissenschaftliches Vorhaben, das von der CSBW aufmerksam verfolgt wird, ist das vom Brandenburgischen Institut für Gesellschaft und Sicherheit in Kooperation mit dem Hasso-Plattner-Institut für Digital Engineering initiierte Projekt „Resilienz Digitaler Kommunen in Krisenzeiten (REDIKOM)“. Ziel dieses Projekts ist es, die Resilienz kommunaler Verwaltungen gegenüber schwerwiegenden IT-Sicherheitsvorfällen zu steigern und eine größtmögliche Handlungsfähigkeit im Schadensfall zu erhalten. Zu diesem Zweck sollen Maßnahmen zur Abwehr von Cyberangriffen und zur schnellstmöglichen Wiederaufnahme des Verwaltungsbetriebs konzipiert, über forensische Analyse vergangene IT-Sicherheitsvorfälle in deutschen Kommunen systematisch ausgewertet und aus den gewonnenen Erkenntnissen ein Leitfaden mit Handlungsempfehlungen für den Umgang mit dem Krisenfall generiert werden.

Die Justiz fertigt einzelfallbezogen wissenschaftliche Analysen bezüglich Cybersicherheit an oder beauftragt, sofern dies angezeigt erscheint.

14. ob sie die öffentliche Verwaltung (kommunal wie landesseitig) oder Teile derer in Baden-Württemberg als KRITIS einstuft und welche Vorgaben sie für diese macht (bitte im Falle von vorhandenen Vorgaben im Speziellen auch auf Managementthemen wie Informationssicherheitsmanagement und Kontinuitätsmanagement sowie auf Informationen bzgl. deren Finanzierung eingehen);

Zu 14.:

Für die Einstufung von bestimmten Stellen und Anlagen als KRITIS im Sinne des BSIG ist die BSI-KritisV maßgeblich – auf die Ausführungen zu BSIG und BSI-KritisV in Ziffer 11 wird verwiesen. Maßstab hierfür sind insbesondere die in der BSI-KritisV benannten Sektoren sowie die jeweils festgelegten Schwellenwerte. Demnach zählen Landes- oder Kommunalverwaltungen grundsätzlich nicht zu den KRITIS im Sinne des BSIG. Anders verhält es sich jedoch bei kommunalen Anlagen und Einrichtungen, sofern diese die relevanten Schwellenwerte der BSI-KritisV erreichen oder überschreiten. Soweit einzelne Bereiche in den Kommunen als KRITIS eingestuft sind, liegt die Zuständigkeit für entsprechende Vorgaben beim Bund.

Unabhängig von einer Einstufung als KRITIS unterliegt die Landesverwaltung spezifischen Anforderungen an die Informationssicherheit sowie an die Notfallvorsorge und -behandlung. Diese ergeben sich aus dem CSG, der CSVO und der Verwaltungsvorschrift Informationssicherheit. Die CSVO setzt dabei auf Landesebene die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) um und enthält unter anderem Vorgaben zur Notfallvorsorge und -behandlung. Aufgrund des Beschlusses 2023/39 des IT-Planungsrates vom 3. November 2023 (42. Sitzung), sind die Kommunalverwaltungen von der Umsetzung dieser Vorgaben aus der NIS-2-Richtlinie ausgenommen.

Die Landesverwaltung setzt aufgrund der vorgenannten Vorschriften die Standards des BSI (BSI-Standards) um. Dazu gehört es, Informationssicherheitsmanagementsysteme (ISMS) aufzubauen und zu betreiben. Auch gehört dazu die Ausgestaltung eines Notfallmanagements beziehungsweise eines BCM, das kontinuierlich weiter auszubauen ist.

Die BITBW hat bereits nach dem entsprechenden BSI-Standard zum Notfallmanagement/BCM alle wesentlichen Informationen zur Notfallbewältigung im Notfallhandbuch der BITBW hinterlegt und die benötigten organisatorischen Regelungen geschaffen. Diese umfassen unter anderem den Aufbau und die Besetzung des Notfallstabs, Regelungen zur Notfallarbeit wie Erreichbarkeiten und Bereitschaftszeiten sowie die Festlegung von Alarmierungswegen und Sofortmaßnahmen in Notfällen. Für die wesentlichen zentralen IT-Systeme des Landesverwaltungsnetzes existieren Notfallpläne. Diese umfassen neben IT-Systemen auch wichtige Gebäude- und Personalressourcen. Überdies hat das Ministerium des Inneren, für Digitalisierung und Kommunen sichergestellt, dass die bewährten Organisationsformen, Abläufe und Infrastruktureinrichtungen (Lagezentrum) des landesweiten, ressortübergreifenden Krisenmanagements auch im Falle eines einschlägigen IT-Notfalls greifen. Zeichnet sich eine entsprechende Lage ab, werden die Prozesse des ressortübergreifenden Krisenmanagements unter Einbindung der Sonderrollen des Landes-CIO, des Landes-CISO, der CSBW und der BITBW aktiviert und die jeweiligen Stäbe, wie der Verwaltungsstab des Innenministeriums und der Interministerielle Verwaltungsstab, aufgerufen.

15. welche Erkenntnisse und Maßnahmen sie aus dem Sicherheitsvorfall in der Verwaltung des Landkreises Anhalt-Bitterfeld bspw. auch für andere Verwaltungseinheiten wie Regierungspräsidien oder Oberstaatsanwaltschaften abgeleitet hat.

Zu 15.:

Der Cyberangriff auf die Landkreisverwaltung Anhalt-Bitterfeld hatte erhebliche Konsequenzen über einen langen Zeitraum und zeigt, welche Auswirkungen eine unzureichend geschützte IT-Infrastruktur haben kann. Es kam zum Ausfall von Geldzahlungen und zur Veröffentlichung personenbezogener Daten.

Unabhängig von dem konkreten Sicherheitsvorfall in der Verwaltung des Landkreises Anhalt-Bitterfeld hat die Landesregierung mit der Cybersicherheitsstrategie und der geschaffenen Cybersicherheitsarchitektur, in deren Mittelpunkt die CSBW steht, bereits frühzeitig wichtige und mustergültige Voraussetzungen geschaffen, um mit einer Vielzahl an präventiven und reaktiven Angeboten Risiken durch Cyberangriffe begegnen zu können. So stellt das Lagezentrum der CSBW über den Warn- und Informationsdienst kontinuierlich und umgehend Informationen und Handlungsempfehlungen zu Schwachstellen und Sicherheitslücken bereit. Mit dem Cybermonitoring informiert die CSBW insbesondere auch Verwaltungseinheiten der Landesverwaltung über beispielsweise im Darknet gefundene Hinweise zu gegenwärtigen oder bereits erfolgten Angriffen. Überdies bietet sie vielfältige Beratungsangebote sowie Schulungen für alle Mitarbeitenden sowie speziell für IT-Fachpersonal an und informiert regelmäßig über aktuelle Themen, Herausforderungen und Lösungen im Bereich der Cybersicherheit. Im Falle eines Angriffs unterstützt die CSBW im Rahmen ihrer Zuständigkeit betroffene Einrichtungen mit ihrem Mobile Incident Response Team vor Ort. Mit ihrer 7x24 Stunden erreichbaren Cyber-Ersthilfe bietet sie zudem eine Erstberatung für Betroffene eines Cyberangriffs an. Alle zuvor aufgeführten Leistungen der CSBW stehen auch den Regierungspräsidien und den Oberstaatsanwaltschaften zur Verfügung.

Im Übrigen wird zu Erkenntnissen und Maßnahmen aus dem Sicherheitsvorfall in der Verwaltung des Landkreises Anhalt-Bitterfeld auf das in der Stellungnahme zu Ziffer 13 angeführte Projekt REDIKOM verwiesen.

Der Sicherheitsvorfall im Landkreis Anhalt-Bitterfeld hat die Relevanz einer resilienten Cybersicherheitsarchitektur unter besonderer Berücksichtigung des „Faktors Mensch“ verdeutlicht. Vor diesem Hintergrund hat das Ministerium für Wissenschaft, Forschung und Kunst seine Präventionsmaßnahmen intensiviert und verfolgt eine hybride Sensibilisierungsstrategie, die das sicherheitsbewusste Verhalten der Beschäftigten im digitalen Raum ganzheitlich adressiert. Durch die synergetische Verknüpfung digitaler und analoger Formate werden über eine zentrale Lernplattform kontinuierlich Online-Awareness-Trainings durchgeführt, welche künftig durch simulierte Phishing-Tests ergänzt werden, um die Wachsamkeit gegenüber Social-Engineering-Angriffen im Arbeitsalltag nachhaltig zu verstetigen. Diese digitalen Angebote werden durch gezielte Präsenzveranstaltungen flankiert, die insbesondere der vertieften Vermittlung von Kenntnissen über spezifische Gefährdungslagen sowie der Stärkung der allgemeinen Sicherheitskultur dienen, um die organisatorische Widerstandsfähigkeit dauerhaft zu erhöhen.

Seit dem Angriff auf die Kreisverwaltung Anhalt-Bitterfeld wurden im Ressortbereich des Ministeriums für Umwelt, Klima und Energiewirtschaft die technischen, organisatorischen sowie personellen Informationssicherheitsmaßnahmen noch weiter verstärkt. Führungskräfte und Beschäftigte müssen regelmäßig an Pflichtschulungen teilnehmen. Auch sind Phishing-Tests in Planung. Außerdem wird das Thema im Krisenmanagement als ein relevantes Szenario betrachtet.

Die Justiz erachtet die Sensibilisierung der Anwendenden als effektivste Maßnahme, da die Infektion über E-Mails nach wie vor das größte und gefährlichste Einfallstor darstellt.

Im Ministerium für Verkehr als eigene Verwaltungseinheit flossen die Erkenntnisse aus dem Sicherheitsvorfall im Landkreis Anhalt-Bitterfeld in den kontinuierlichen Verbesserungsprozess der Informationssicherheit ein.

Unabhängig vom konkreten genannten Vorfall ist die Informationssicherheit im Ministerium für Ernährung, Ländlichen Raum und Verbraucherschutz bereits seit vielen Jahren sehr hoch priorisiert und wird im Rahmen der regelmäßigen Zertifizierung stetig weiterentwickelt – auf die Stellungnahme zu Ziffer 13 wird verwiesen.

Strobl

Minister des Inneren,
für Digitalisierung und Kommunen