**Landtag von Baden-Württemberg** **Drucksache 17 / 2821**

**17. Wahlperiode** **1.7.2022**

# Antrag

**der Abg. Thomas Blenke und Dr. Matthias Miller u. a. CDU**

**und**

# Stellungnahme

**des Ministeriums des Inneren, für Digitalisierung und Kommunen**

## Kritische Infrastruktur in Baden-Württemberg

Antrag

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. wie sie Kritische Infrastruktur (KRITIS) in Baden-Württemberg definiert;

2. inwieweit die Mobilfunknetze als Kritische Infrastrukturen aufgrund ihrer Bedeutung für die Kommunikation und Datenübertragung eingestuft sind und wie deren Betriebsbereitschaft auch im Katastrophenfall gewährleistet wird;

3. inwieweit die Rechenzentren des Landes einschließlich Universitäten und Hochschulen sowie Universitätskliniken als Kritische Infrastrukturen aufgrund der dort angebotenen Dienste und gespeicherten Daten eingestuft sind und wie deren sicherer Betrieb und Datenübertragung gewährleistet wird;

4. ob und inwieweit es regelmäßige Sicherheitsüberprüfungen (wie z. B. regelmäßige Penetrationstests) gibt;

5. inwieweit der Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben als Kritische Infrastrukturen eingestuft ist und ob die Betriebsbereitschaft des Digitalfunks durch den Schutz der Basisstationen gegen Angriffe von außen sowie Naturkatastrophen auch im Katastrophenfall sichergestellt ist;

6. inwieweit das Kabelfernseh- und Glasfasernetz als Kritische Infrastruktur eingestuft ist und wie die Betriebsfähigkeit der Datenübertragungsnetze bei dem Ausfall oder der Unterbrechung zentraler Kontenpunkte sowie Hauptstränge sichergestellt werden soll;

Eingegangen: 1.7.2022 / Ausgegeben: 8.8.2022

7. wie bei einem Ausfall zentraler Hauptleitungen und Knotenpunkte der Fernwasserversorgungsunternehmen die Wasserversorgung in Baden-Württemberg aufrechtgehalten werden kann;

8. ob die Fernwasserversorgungsunternehmen mit eigenen Notstromaggregaten für den Fall von flächendeckenden Stromausfällen ausgestattet sind;

9. wie sie die Tendenz zur zunehmenden Trinkwasserentnahme aus dem Bodensee einschätzt und ob sie hierdurch eine Gefährdung für die diversifizierte Trinkwasserversorgung in Baden-Württemberg sieht;

10. wie sie die Gefahr von mehrtägigen Stromausfällen und Blackouts einschätzt;

11. welche präventiven Maßnahmen von Seiten der Landesregierung gegen mehrtägige Stromausfälle und Blackouts getroffen werden;

12. welche Maßnahmen im Fall eines Blackouts von Seiten der Landesregierung ergriffen werden sollen, um die Funktionsfähigkeit von Einrichtungen der Kritischen Infrastruktur aufrechtzuerhalten;

13. welche Übungen in den vergangenen fünf Jahren durch die Organisationen des Bevölkerungsschutzes in Baden-Württemberg für das Szenario von mehrtätigen Stromausfällen und Blackouts durchgeführt wurden;

14. wie sich die Anzahl der durchgeführten Cyber-Angriffe auf Einrichtungen der Kritischen Infrastruktur in den vergangenen zehn Jahren entwickelt hat, und ob sich nach dem Kenntnisstand der Landesregierung die Anzahl der geplanten und durchgeführten Cyber-Angriffe seit dem russischen Überfall auf die Ukraine erhöht hat.

29.6.2022

Blenke, Dr. Miller, Gehring, Huber, Hockenberger, Mayr CDU

## Begründung

Kritische Infrastrukturen (KRITIS) sind 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. Angriffe und Cyber-Attacken auf Kritische Infrastrukturen besitzen ein besonders hohes Schadenspotenzial in Bezug auf die Gesellschaft. Flut- und Hochwasserkatastrophen genauso wie die Coronapandemie oder der russische Angriffskrieg auf die Ukraine führen vor Augen, wie bedeutsam Kritische Infrastrukturen für das Funktionieren unserer Gesellschaft sind. Die Gewährleistung des Schutzes Kritischer Infrastrukturen hat für uns oberste Priorität und ist eine Kernaufgabe staatlicher und unternehmerischer Sicherheitsvorsorge. Mit dem vorliegenden Antrag wird die Situation der Kritischen Infrastrukturen in Baden-Württemberg erfragt mit dem Ziel, eine bestmögliche Versorgung der Bevölkerung sicherzustellen.

Stellungnahme

Mit Schreiben vom 26. Juli 2022 Nr. IM6-1441-45/3/38 nimmt das Ministerium des Inneren, für Digitalisierung und Kommunen im Einvernehmen mit dem Staatsministerium, dem Ministerium für Finanzen, dem Ministerium für Kultus, Jugend und Sport, dem Ministerium für Wissenschaft, Forschung und Kunst, dem Ministerium für Umwelt, Klima und Energiewirtschaft, dem Ministerium für Wirtschaft, Arbeit und Tourismus, dem Ministerium für Soziales, Gesundheit und Integration, dem Ministerium der Justiz und für Migration, dem Ministerium für Verkehr, dem Ministerium für Ernährung, Ländlichen Raum und Verbraucherschutz und dem Ministerium für Landesentwicklung und Wohnen zu dem Antrag wie folgt Stellung:

*Der Landtag wolle beschließen,*

*die Landesregierung zu ersuchen*

*zu berichten,*

*1. wie sie Kritische Infrastruktur (KRITIS) in Baden-Württemberg definiert;*

Zu 1.:

Kritische Infrastrukturen (KRITIS) sind 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 Kritischen Infrastrukturen.

Den speziellen Rechtsrahmen für die IT-Sicherheit von bestimmten KRITIS und damit auch die Vorgaben für Meldepflichten von Sicherheitsvorfällen in diesen KRITIS gestaltet der Bund durch das BSI-Gesetz. In der dem BSI-Gesetz nachgelagerten BSI-Kritisverordnung bestimmt der Bund, welche Unternehmen aus den einzelnen Sektoren zu KRITIS im Sinne des BSI-Gesetzes zählen.

*2. inwieweit die Mobilfunknetze als Kritische Infrastrukturen aufgrund ihrer Bedeutung für die Kommunikation und Datenübertragung eingestuft sind und wie deren Betriebsbereitschaft auch im Katastrophenfall gewährleistet wird;*

*6. inwieweit das Kabelfernseh- und Glasfasernetz als Kritische Infrastruktur eingestuft ist und wie die Betriebsfähigkeit der Datenübertragungsnetze bei dem Ausfall oder der Unterbrechung zentraler Kontenpunkte sowie Hauptstränge sichergestellt werden soll;*

Zu 2. und 6.:

Zu den Ziffern 2 und 6 wird wegen des Sachzusammenhangs gemeinsam Stellung genommen.

Betreiber öffentlicher Telekommunikationsnetze oder öffentlich zugänglicher Telekommunikationsdienste bzw. deren Netze sind Kritische Infrastrukturen im Sinne des BSI-Gesetzes, sofern diese den in der BSI-Kritisverordnung genannten Komponenten zuzuordnen sind und die jeweiligen Schwellenwerte erreicht oder überschritten werden, beispielsweise 100 000 Teilnehmeranschlüsse im jeweiligen Zugangsnetz. Allerdings sind diese KRITIS-Betreiber von der Anwendung der Regelungen nach § 8a und § 8b Absätze 4 und 4a BSIG ausgenommen, da sie – wie alle öffentlichen Netzbetreiber und Diensteanbieter – den Regelungen

des Telekommunikationsgesetzes (TKG) und damit den Verpflichtungen der §§ 165 ff. TKG (u. a. technische und organisatorische Schutzmaßnahmen) und darüber hinaus § 185 TKG (Telekommunikationssicherstellungspflicht) unterliegen.

Anbieter von Telekommunikationsdiensten und Betreiber von Telekommunikationsnetzen haben Schutzmaßnahmen zu treffen, die unter anderem die Funktionsfähigkeit der jeweiligen Netze betreffen. Einzelheiten der zu treffenden Schutzmaßnahmen ergeben sich aus dem Telekommunikationsgesetz sowie dem Katalog von Sicherheitsanforderungen der Bundesnetzagentur *(www.bundesnetzagentur.de/sicherheitsanforderungen)*. So haben Verpflichtete zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und Telekommunikationsdiensten führen, soweit sie durch äußere Angriffe und Einwirkungen bedingt sein können, angemessene technische Vorkehrungen und sonstige Maßnahmen zu treffen. Die konkreten Anforderungen richten sich nach dem Gefährdungspotenzial der betroffenen Netzebene.

Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste mit erhöhtem Gefährdungspotenzial haben sich darüber hinaus regelmäßig alle zwei Jahre im Hinblick auf die Einhaltung und Umsetzung der Anforderungen einer Überprüfung durch eine unabhängige Stelle oder Behörde zu unterziehen.

Mit Blick auf die Betriebsbereitschaft im Katastrophenfall ist die Notfallvorsorge nach Teil 10 Abschnitt 2 des Telekommunikationsgesetzes anzuwenden. Diese dient der Sicherung einer Mindestversorgung mit Telekommunikationsdiensten. Danach haben Betreiber öffentlicher Telekommunikationsnetze einschließlich der Mobilfunknetzbetreiber den Betrieb ihres Netzes mindestens in dem Umfang aufrechtzuerhalten, der für die Erbringung von Sprachkommunikationsdiensten, Internetzugangsdiensten, Datenübertragungsdiensten und E-Mail-Diensten erforderlich ist. Außerdem sind die Netzbetreiber verpflichtet, drohende oder eingetretene Netzüberlastungen oder Engpasssituationen zu verhindern bzw. zu beseitigen.

Des Weiteren haben die Betreiber öffentlicher Mobilfunknetze Verbindungen im Mobilfunk für interpersonelle Kommunikation für Telekommunikationsbevorrechtigte (unter anderem Behörden, Gerichte, Hilfs- und Rettungsdienste, Katastrophenschutzorganisationen, Gesundheitswesen) vorrangig herzustellen.

Nach Auskunft der Vodafone West GmbH, einem der größten Netzbetreiber in Baden-Württemberg, sind die entsprechenden Netze als Kritische Infrastruktur im Sinne des BSI-Gesetzes eingestuft. Insofern sind die Netze auch beim Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeldet. Dementsprechend gebe es Sicherheitskonzepte, die mit der Bundesnetzagentur und dem BSI abgestimmt seien.

Mit Blick auf den Rundfunk als Kritische Infrastruktur sei zunächst darauf hingewiesen, dass der Südwestrundfunk (SWR) die entsprechenden Datenübertragungsnetze (Glasfaser- bzw. Kabelnetz) nicht selbst betreibt. Insofern wird auf die obigen Ausführungen verwiesen.

Darüber hinaus existieren seitens des SWR Planungen und Mechanismen, um die Sendesicherheit im Krisenfall hinsichtlich der selbst verantworteten terrestrischen Verbreitung zu gewährleisten. Hierzu wird auf nachfolgende Stellungnahme des SWR verwiesen:

„Nur ein sehr geringer Prozentsatz der Bevölkerung in Baden-Württemberg nutzt terrestrisches Fernsehen; über 97 % der Bevölkerung empfangen Fernsehen via Satellit, Kabel oder Internet. Die Versorgung über Fernsehen ist deshalb aus Sicht des SWR auch deshalb weniger relevant, da davon auszugehen ist, dass bei Stromausfall kaum ein Bürger seinen Fernseher nutzen kann. Deshalb richtet der SWR sein Augenmerk am stärksten auf die Hörfunkversorgung (Radio), der mit Abstand sicherste Kommunikationsweg im Verantwortungsbereich des SWR. Dieser würde z. B. bei großflächigen Stromausfällen weiter die Erreichbarkeit der Bürger erlauben. Die Menschen können beispielsweise im Auto oder mit kleinen

batteriebetriebenen Radios die UKW-Programme empfangen. Um eine möglichst hohe Sendesicherheit zu gewährleisten, ist unsere Infrastruktur an den Hauptstandorten hochredundant aufgebaut und somit gut abgesichert. Im Falle eines langfristigen großflächigen Netzausfalls kann die UKW-Versorgung mit SWR-Programmen über ein Programmzuführungskonzept (Ballempfangs-Konzept) mit entsprechender Notversorgung für das Programm SWR3 für ca. 3 bis 4 Tage (begrenzt durch die Treibstoffbevorratung für die Notstromaggregate) gewährleistet werden. Konkret können in Baden-Württemberg in diesem Fall ca. 74 % der Bevölkerung ein Radioprogramm des SWR empfangen."

*3. inwieweit die Rechenzentren des Landes einschließlich Universitäten und Hochschulen sowie Universitätskliniken als Kritische Infrastrukturen aufgrund der dort angebotenen Dienste und gespeicherten Daten eingestuft sind und wie deren sicherer Betrieb und Datenübertragung gewährleistet wird;*

Zu 3.:

Die Landesoberbehörde IT Baden-Württemberg (BITBW) zählt zu den Kritischen Infrastrukturen im Sektor Staat und Verwaltung gemäß der in der Stellungnahme zu 1. dargestellten Definition. Der Sektor Staat und Verwaltung unterliegt jedoch nicht der Regulierung durch das BSI-Gesetz. Gemäß § 16 Absatz 1 des E-Government-Gesetzes Baden-Württemberg (EGovG BW) ist die BITBW verpflichtet, die erforderlichen Maßnahmen nach dem Stand der Technik zur Sicherung der elektronischen Kommunikation und der Verwendung elektronischer Dokumente umzusetzen.

Die BITBW ist für den überwiegenden Teil der polizeilichen IT-Infrastruktur zentrale Dienstleisterin. Lediglich bestimmte und für den Dienstbetrieb der Polizei essentielle IT-Anwendungen werden durch diese eigenständig betrieben (z. B. Anwendungen für die Führungs- und Echtzeitkommunikation). Für den IT-Betrieb der Polizei werden zwei Rechenzentrums-Standorte genutzt: Das Rechenzentrum der BITBW und das gemeinsam genutzte Rechenzentrum der Polizei (RZP). Das RZP ist wie die BITBW Teil der Kritischen Infrastruktur. Zur Gewährleistung eines (ausfall-)sicheren Betriebs sind für einzelne zentrale technische Infrastrukturkomponenten Redundanzen vorhanden. Zur Gewährleistung der Sicherheit sind bauliche, technische und organisatorische Maßnahmen umgesetzt.

Das Landeszentrum für Datenverarbeitung (LZfD) als steuerliches Rechenzentrum kann im Sektor Staat und Verwaltung als Kritische Infrastruktur angesehen werden. Es unterliegt jedoch wie die BITBW nicht den Regelungen des BSI-Gesetzes, jedoch den Verpflichtungen aus § 16 Absatz 1 EGovG BW.

Das BSI-Gesetz fordert in § 8a Absatz 1 von Betreibern Kritischer Infrastrukturen angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Diese Grundsätze werden auch für die Sicherung der Systeme, Komponenten und Prozesse des LZfD angewandt.

Die landeseigenen Universitätsklinika (UK) in Freiburg, Heidelberg, Tübingen und Ulm zählen zur Kritischen Infrastruktur und unterliegen den Nachweispflichten nach § 8a BSIG. Ein Informationssicherheits-Managementsystem (ISMS) ist erfolgreich nach den Vorgaben des BSI etabliert und wird regelmäßig im 2 Jahres-Zyklus auditiert. Die Ergebnisse werden an das BSI berichtet.

Die Gewährleistung der Sicherheit von Betrieb und Datenübertragung erfolgt durch eine Vielzahl technischer und organisatorischer Maßnahmen, die im Rahmen eines ISMS gesteuert werden. Grundlagen sind dafür der Branchenstandard B3S, die ISO 27001 sowie die Empfehlungen des BSI. Dazu zählt u. a. auch die redundante und hochverfügbare Architektur der Rechenzentren am jeweiligen UK-Standort.

Um den geforderten Stand der Technik zeitnah erreichen und nachhalten zu können, werden auf Basis von Risiko- und Gap-Analysen mithilfe des Nachtragshaushalts (Fördermaßnahme „Kooperationsverbund Hochschulmedizin BW“) und des Krankenhauszukunftsgesetzes sich ergänzende Verbundvorhaben der vier Universitätsklinika umgesetzt.

Die Rechenzentren an den Universitäten und Hochschulen des Landes werden in Eigenverantwortung der jeweiligen Einrichtung betrieben und sind nicht als KRITIS eingestuft. Einem sicheren Betrieb und einer zuverlässigen Datenübertragung wird dennoch ein sehr hoher Stellenwert beigemessen. Dem Einsatz zeitgemäßer Technik und technischer Verfahren sowie beständigen Updates der verwendeten Softwarepakete kommt eine große Bedeutung zu. Hierfür haben die Universitäten und Hochschulen des Landes ein gemeinsames Rahmenkonzept zur Informationssicherheit entwickelt. Für die Umsetzung des Rahmenkonzepts wurden vom Land in den vergangenen Haushalten insgesamt 58 Stellen bereitgestellt.

*4. ob und inwieweit es regelmäßige Sicherheitsüberprüfungen (wie z. B. regelmäßige Penetrationstests) gibt;*

Zu 4.:

Sicherheitsüberprüfungen wie Schwachstellenscans werden für verschiedene Systeme der Landesverwaltung immer wieder durchgeführt, diese betreffen auch regelmäßig grundlegende Infrastrukturkomponenten der BITBW, vertiefend oder bei kritischen Anwendungen kommen zusätzlich auch Penetrationstests zum Einsatz.

Im Bereich des Finanzressorts wurde angewiesen, dass neue oder aktualisierte Anwendungssysteme mit Schnittstellen zu Komponenten außerhalb der Landesverwaltung vor Produktivsetzung immer einer Schwachstellenuntersuchung und einem Penetrationstest unterzogen werden sollen.

Im Rahmen des gemeinsamen Informationssicherheitskonzepts aller Universitäten und Hochschulen des Landes werden u. a. externe Penetrationstests und zukünftig auch Schwachstellenscans durchgeführt.

An allen Universitätsklinika des Landes erfolgt eine offizielle BSI-Prüfung des Stands der Technik alle zwei Jahre. Dabei wird jeweils ein internes und ein externes Audit durch ein durch die Deutsche Akkreditierungsstelle GmbH akkreditiertes Unternehmen durchgeführt. Zusätzlich erfolgen an allen Standorten ein permanentes Schwachstellen- und Risikomanagement und jährliche interne und externe Penetrationstests.

*5. inwieweit der Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben als Kritische Infrastrukturen eingestuft ist und ob die Betriebsbereitschaft des Digitalfunks durch den Schutz der Basisstationen gegen Angriffe von außen sowie Naturkatastrophen auch im Katastrophenfall sichergestellt ist;*

Zu 5.:

Der Digitalfunk BOS ist aufgrund seiner Bedeutung für die Kommunikation der Einsatz- und Rettungskräfte in Deutschland ein Kernelement der Deutschen Sicherheitsarchitektur und als Kritische Infrastruktur im Sinne der Definition in der Stellungnahme zu 1. zu betrachten. Er unterliegt im Sektor Staat und Verwaltung jedoch nicht den Regelungen des BSI-Gesetzes.

Entsprechend stellt die Bundesanstalt für den Digitalfunk BOS (BDBOS) als Betreiberin des Digitalfunks BOS nach § 2 Absatz 1 Satz 1 des BDBOS-Gesetzes hierauf ausgerichtete Dienstleistungen zur Verfügung. Die Verantwortlichkeit für den Schutz und die Sicherheit der Basisstationen liegt primär in der Zuständigkeit der Länder. Ihre Ausgestaltung orientiert sich dabei an bundeseinheitlichen Planungsvorgaben. Zur Gewährleistung der Sicherheit von Basisstationen werden

bauliche, technische und organisatorische Maßnahmen getroffen. Beispielsweise unterliegen die Basisstationen in Baden-Württemberg einem Alarm- und Zutrittsmanagement. Die Autorisierte Stelle für den Digitalfunk Baden-Württemberg (ASDBW) beim Präsidium Technik, Logistik, Service der Polizei überwacht in Echtzeit und rund um die Uhr den Zugang zu allen Basisstationen, deren Funktionsfähigkeit und die dazugehörigen Leitungswege. Die ASDBW wird beim Störungs- und Fehlermanagement der Infrastruktur durch den Zentralen Betrieb der BDBOS unterstützt.

Generell zeichnet sich der Digitalfunk BOS in Baden-Württemberg bislang durch seine hohe Verfügbarkeit und seine im Vergleich zu den Analogfunknetzen deutlich bessere Flächenabdeckung im Land aus. Um diesen sicheren Netzbetrieb auch weiterhin zu gewährleisten, werden kontinuierlich hohe Investitionen in die Betriebsinfrastruktur getätigt. Für Modernisierung, Weiterentwicklung und Betrieb des Digitalfunknetzes bis mindestens 2030 wurden über 500 Millionen Euro bereitgestellt. In diesem Rahmen wird die Resilienz des Digitalfunks durch verschiedene Maßnahmen weiter gesteigert. Beispielsweise gewährleisten zukünftig (teilweise brennstoffzellenbetriebene) Netzersatzanlagen die Funktionsfähigkeit der einzelnen Funkstandorte (Basisstationen) für das Szenario eines längerfristigen oder eines großflächigen Stromausfalls für einen Zeitraum von mindestens 72 Stunden.

Die derzeit laufende Netzmodernisierung mit neuer Übertragungstechnik führt dazu, dass in den kommenden Jahren neue, zukunftsfähige und leistungsfähigere Basisstationen mit höheren Kapazitäten eingesetzt werden. Diese werden neben aktuellen Funkstandards künftig auch 5G-Technik unterstützen. So wird gewährleistet, dass im Einsatz- oder Krisenfall auch bei einer schnellen und starken Zunahme von Einsatzkräften die Kommunikationsfähigkeit verlässlich gegeben ist. Daneben kann ein Ausfall einzelner Verbindungswege zukünftig dynamisch und selbstständig durch das Zugangsnetz kompensiert werden. Bei diesen Maßnahmen wird auch neuen Herausforderungen in Folge klimatischer Veränderungen begegnet. Durch eine umfassende Erneuerung der im Zugangsnetz eingesetzten Richtfunktechnik wird beispielsweise auch vermehrt auftretenden Starkregenereignissen durch Anwendung modernster Modulationsverfahren Rechnung getragen.

*7. wie bei einem Ausfall zentraler Hauptleitungen und Knotenpunkte der Fernwasserversorgungsunternehmen die Wasserversorgung in Baden-Württemberg aufrechtgehalten werden kann;*

Zu 7.:

Ausfallszenarien und entsprechende Maßnahmen, um die Wasserversorgung, ggf. mit einer reduzierten Wassermenge, aufrechtzuerhalten, sind in den Notfallmaßnahmenplänen der Fernwasserversorger festgehalten. Für Wasserversorgungsunternehmen sind solche Pläne, die die örtlichen Gegebenheiten der Wasserversorgung berücksichtigen, verpflichtend. Beispielsweise können die Fernwasserversorger durch vernetzte Anlagen und Steuerungen ausgefallene Leitungen und Speicherbehälter über Bypässe in begrenztem Rahmen umfahren.

*8. ob die Fernwasserversorgungsunternehmen mit eigenen Notstromaggregaten für den Fall von flächendeckenden Stromausfällen ausgestattet sind;*

Zu 8.:

Alle Fernwasserversorger verfügen über Notstromaggregate, auch mobile, um an bestimmten Scheitelbehältern auch Wasser geländeunabhängig befördern zu können. Die Notstromversorgung ermöglicht kurzfristig die Aufrechterhaltung der Wasserversorgung in einem – bzgl. der Wassermenge – begrenzten Umfang.

*9. wie sie die Tendenz zur zunehmenden Trinkwasserentnahme aus dem Bodensee einschätzt und ob sie hierdurch eine Gefährdung für die diversifizierte Trinkwasserversorgung in Baden-Württemberg sieht;*

Zu 9.:

Gegenwärtig sieht die Landesregierung keine steigende Tendenz bei der Trinkwasserentnahme aus dem Bodensee. Die genehmigten Wasserentnahmerechte werden gegenwärtig nicht voll ausgeschöpft.

Die Wasserversorgung in Baden-Württemberg stützt sich auf drei Säulen, die Fernwasserversorgung, Gruppenwasserversorgungen sowie ortsnahe Wasserversorgungen. Die größte Bedeutung genießt dabei die ortsnahe Wasserversorgung, wie es im Leitbild zur Wasserversorgung Baden-Württemberg festgehalten ist.

*10. wie sie die Gefahr von mehrtägigen Stromausfällen und Blackouts einschätzt;*

*11. welche präventiven Maßnahmen von Seiten der Landesregierung gegen mehrtägige Stromausfälle und Blackouts getroffen werden;*

Zu 10. und 11.:

Zu Ziffern 10 und 11 wird aufgrund des Sachzusammenhangs gemeinsam Stellung genommen.

Für die Sicherheit und die Zuverlässigkeit der Stromversorgungsnetze sind nach dem Energiewirtschaftsgesetz die Netzbetreiber zuständig. Diese treffen die nötigen Vorkehrungen um mehrtägige Stromausfälle und Blackouts zu vermeiden.

Aufschluss über die Netzqualität in Deutschland gibt der „System Average Interruption Duration Index“ (SAIDI), der die durchschnittliche Unterbrechungsdauer der Stromversorgung pro Endkunde wiedergibt. Der Wert für 2020 lag mit 10,7 Minuten erneut auf dem niedrigsten Stand seit Beginn der Veröffentlichung im Jahr 2006 (Baden-Württemberg bei 12,3 Minuten). Auch im europäischen Vergleich hatte Deutschland in der Vergangenheit einen der niedrigsten SAIDI-Werte.

Die Landesregierung sieht derzeit keine Anzeichen für mehrtägige Stromausfälle oder gar Blackouts im Land.

Zur Aufrechterhaltung ihrer eigenen Handlungsfähigkeit im Falle eines Stromausfalls treffen die Behörden des Landes vorbereitend die jeweils erforderlichen organisatorischen und technischen Maßnahmen. In den Blick genommen werden dabei Themen wie beispielsweise die Identifikation kritischer Geschäftsprozesse, Vorbereitungen zur Stabsarbeit im Ereignisfall, Notstromversorgung oder Redundanzkommunikation für den Fall eines Ausfalls von öffentlichen Kommunikationsnetzen.

*12. welche Maßnahmen im Fall eines Blackouts von Seiten der Landesregierung ergriffen werden sollen, um die Funktionsfähigkeit von Einrichtungen der Kritischen Infrastruktur aufrechtzuerhalten;*

Zu 12.:

Die Sicherstellung der Funktionsfähigkeit von Kritischen Infrastrukturen ist Aufgabe der jeweiligen Betreiber. Ihnen obliegt es daher in eigener Zuständigkeit, erforderliche Maßnahmen zu treffen, um die von ihnen erbrachten kritischen Dienstleistungen auch im Falle eines Blackouts aufrecht erhalten zu können.

Gleichzeitig erfordert der Schutz Kritischer Infrastrukturen ein koordiniertes Zusammenwirken von KRITIS-Betreibern und staatlichen Stellen. Die im Innenministerium angesiedelte Koordinierungsstelle Kritische Infrastrukturen bündelt

Aktivitäten zum Schutz Kritischer Infrastrukturen unter Wahrung der fachlichen Ressortzuständigkeit.

Für die Notfallplanung und das Krisenmanagement bei einem großflächigen Stromausfall liegt mit dem vom Innenministerium Baden-Württemberg zusammen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe im Jahr 2010 herausgegebenen Krisenhandbuch „Stromausfall“ eine bis heute aktuelle Planungsgrundlage für die bei einem Stromausfall besonders betroffenen öffentlichen und privaten Akteure, wie zum Beispiel KRITIS-Betreiber, vor. Diese wurde im Jahr 2014 durch eine speziell für Gemeindeverwaltungen konzipierte praxisorientierte Handreichung ergänzt.

Die von den Behörden des Landes bei einer längeren Abschaltung des Stromnetzes zu ergreifenden Maßnahmen richten sich nach den Erfordernissen der jeweiligen Lage. Im Ereignisfall werden die entsprechenden Mechanismen der operativen Gefahrenabwehr angewendet.

*13. welche Übungen in den vergangenen fünf Jahren durch die Organisationen des Bevölkerungsschutzes in Baden-Württemberg für das Szenario von mehrtätigen Stromausfällen und Blackouts durchgeführt wurden;*

Zu 13.:

Im Übungswesen der Katastrophenschutzbehörden auf örtlicher Ebene ist das Thema „Stromausfall“ als eines der grundlegenden Szenarien auf der Agenda. Beispielhaft können die Übungen „Sturmschäden und Stromausfall“ des Landratsamts Sigmaringen im Jahr 2017, die Stabsübungen „Stromausfall“ des Landratsamts Schwarzwald-Baar-Kreis und des Landratsamts Alb-Donau-Kreis unter Mitwirkung u. a. der Energiedienste bzw. der Bundeswehr im Jahr 2018, die Stabsübung „Stromausfall“ der Stadt Karlsruhe und die Übung des Landratsamts Main-Tauber-Kreis zur zivil-militärischen Zusammenarbeit und mit benachbarten bayerischen Landkreisen mit dem Thema „Hochwasser, Stromausfall“ im Jahr 2019 genannt werden. Die für März 2020 geplante Übung „langanhaltender Stromausfall“ der Stadt Baden-Baden musste coronabedingt verschoben werden.

Ende 2017 haben Energieversorger aus Baden-Württemberg gemeinsam mit Innenministerium und Umweltministerium das Thema eines großflächigen Stromausfalls beübt. Die weiteren Ministerien des Landes wurden im Rahmen des Interministeriellen Verwaltungsstabs in die Übung einbezogen.

*14. wie sich die Anzahl der durchgeführten Cyber-Angriffe auf Einrichtungen der Kritischen Infrastruktur in den vergangenen zehn Jahren entwickelt hat, und ob sich nach dem Kenntnisstand der Landesregierung die Anzahl der geplanten und durchgeführten Cyber-Angriffe seit dem russischen Überfall auf die Ukraine erhöht hat.*

Zu 14.:

Wie in der Stellungnahme zu 1. dargestellt, hat der Bund mit dem BSI-Gesetz und der BSI-Kritisverordnung den Rechtsrahmen für die IT-Sicherheit bestimmter KRITIS gestaltet. Gemäß § 8b Absatz 1 BSIG ist das BSI zentrale Meldestelle für Betreiber Kritischer Infrastrukturen im Sinne des BSI-Gesetzes in Angelegenheiten der Sicherheit in der Informationstechnik. Die Betreiber Kritischer Infrastrukturen nach dem BSI-Gesetz haben die in diesem Gesetz beschriebenen IT-Störungen unverzüglich an das BSI zu melden.

Ebenso hat das BSI zur Wahrnehmung dieser Aufgabe die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik wesentlichen Informationen zu sammeln und auszuwerten, insbesondere Informationen zu Sicherheitslücken, zu Schadprogrammen, zu erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und zu der dabei beobachteten Vorgehensweise.

Ein Austausch des BSI mit den Ländern zu gemeldeten Cyberangriffen und daraus resultierenden IT-Störungen findet bisher nur dann statt, wenn sich aus Sicht des BSI hiervon direkte Mehrwerte für die Bewältigung des Vorfalls ergeben, die Länder die entsprechenden Informationen für ihr Aufsichtshandeln benötigen oder es sich um Vorfälle mit großem medialen Interesse handeln könnte. Aus diesem Grund verfügt die Landesregierung nicht über valide Angaben zur Entwicklung der Anzahl der durchgeführten Cyberangriffe auf KRITIS-Einrichtungen im Sinne des BSI-Gesetzes in den vergangenen zehn Jahren oder über die Anzahl der geplanten und durchgeführten Cyberangriffe auf entsprechende KRITIS-Betreiber seit dem russischen Überfall auf die Ukraine.

Über die nach dem BSI-Gesetz und der BSI-Kritisverordnung bestehenden Meldepflichten hinaus ergeben sich jedoch zum Beispiel auch aus der Ausübung der Aufsicht über die betreffenden KRITIS-Unternehmen und aus polizeilicher und verfassungsschutzrechtlicher Ermittlungs- bzw. Aufklärungstätigkeit weitere Melde- und Informationswege. Hieraus liegen derzeit folgende Erkenntnisse über Cyberangriffe vor:

Das Landesamt für Verfassungsschutz Baden-Württemberg (LfV) hat in den vergangenen zehn Jahren mehrere Fallkomplexe im Zusammenhang mit nachrichtendienstlich gesteuerten Cyberangriffen auf Einrichtungen von Kritischen Infrastrukturen in Baden-Württemberg bearbeitet. Insgesamt ist im angefragten Zeitraum eine Steigerung von Cyberangriffen auf Einrichtungen der Kritischen Infrastruktur (KRITIS) oder deren Dienstleister festzustellen gewesen. Für die Jahre 2012 bis 2016 liegen der Cyberabwehr des LfV keine Erkenntnisse zu Cyberangriffen auf KRITIS-Einrichtungen vor, in den Jahren 2017 bis 2021 wurde pro Jahr je eine einstellige Zahl von Fallkomplexen bearbeitet. Im Jahr 2022 hat die Cyberabwehr zum Bearbeitungszeitpunkt keine Erkenntnisse über einen erfolgreich durchgeführten staatlich bzw. nachrichtendienstlich gesteuerten Cyberangriff auf KRITIS-Einrichtungen.

Die statistische Erfassung von Straftaten erfolgt bei der Polizei Baden-Württemberg anhand der Polizeilichen Kriminalstatistik (PKS). Bei der PKS handelt es sich um eine sogenannte reine Ausgangsstatistik, in der strafrechtlich relevante Sachverhalte nach der polizeilichen Sachbearbeitung vor Abgabe an die Strafverfolgungsbehörden erfasst werden. Die PKS ist als Jahresstatistik konzipiert. Die Fallerfassung erfolgt nach den bundeseinheitlichen „Richtlinien für die Führung der Polizeilichen Kriminalstatistik“. Eine gesonderte Erfassung von Cyberangriffen auf Kritische Infrastrukturen ist in der PKS nicht vorgesehen. Hinzu kommt, dass, wie eingangs dargestellt, für bestimmte Betreiber Kritischer Infrastrukturen lediglich gegenüber dem BSI eine Verpflichtung zur Meldung von IT-Sicherheitsvorfällen besteht. Vor diesem Hintergrund sind belastbare Aussagen im Sinne der Fragestellung nicht möglich. Nach Einschätzung des Landeskriminalamts Baden-Württemberg zeichnet sich seit Beginn des russischen Angriffskriegs bislang allerdings kein Anstieg der Anzahl von Cyberangriffen auf Unternehmen und öffentliche Institutionen – unabhängig von deren Einstufung als Kritische Infrastruktur – ab.

Angesichts des Ukrainekriegs ist jedoch mit gezielten russischen Cyberaktivitäten/Cyberangriffen gegen westliche Staaten zu rechnen. Dabei sind auch gezielte Cybersabotageangriffe und Cyberspionageaktivitäten, insbesondere gegen Sicherheitsbehörden, Kritische Infrastrukturen sowie rüstungsnahe Wirtschaftsunternehmen, einzukalkulieren. Auch Cyberangriffe auf einen Drittstaat können zu einer mittelbaren Betroffenheit Deutschlands führen, etwa durch Beeinträchtigungen von Lieferketten oder der Verfügbarkeit von Waren, Diensten oder Rohstoffen.

Im Kontext des Angriffskriegs Russlands auf die Ukraine erfolgte bereits ein DDoS-Angriff (Überlastungsangriff auf die IT-Infrastruktur) auf die Internetseite der Polizei Baden-Württemberg, der von der pro-russischen Gruppierung Killnet beansprucht wird. Infolge des Angriffs war die Webseite kurzzeitig nicht oder nur erschwert zu erreichen. Dieser Angriff hatte allerdings zu keinem Zeitpunkt Auswirkungen auf kritische Leistungen oder die Funktionsfähigkeit der Polizei Baden-Württemberg insgesamt. Derzeit liegen dem LfV keine Erkenntnisse vor,

dass es sich hierbei um einen staatlich bzw. nachrichtendienstlich gesteuerten Angriff handelt.

Die Polizei Baden-Württemberg geht vor diesem Hintergrund von einer erhöhten Bedrohung der Cyber-Sicherheitslage aus. Sie ist eng in das bundesweite Monitoring eingebunden und beobachtet die Lage fortlaufend.

In den vergangenen zehn Jahren verzeichnete die Justiz im Dezember 2019 und im Jahr 2020 einige versuchte, aber erfolglose Cyber-Angriffe, vor allem in möglichem Zusammenhang mit der Schadsoftware Emotet. Schädliche Auswirkungen in Form von Datenabfluss, Integritätsverletzungen oder Infektionen mit Schadsoftware wurden hierbei nicht festgestellt. Seit dem 24. Februar 2022 wurden keine Cyber-Angriffe auf die baden-württembergische Justiz beobachtet.

Die Universitätsklinika beobachten über den Zeitraum der vergangenen zehn Jahre eine massiv steigende Anzahl an Cyberangriffen und Angriffsvektoren. Ob und in welchem Umfang die Ukraine-Krise zu einem zusätzlichen Anstieg geführt hat, lässt sich derzeit nicht belastbar beantworten.

Strobl

Minister des Inneren,
für Digitalisierung und Kommunen