Landtag von Baden-Württemberg **Drucksache 17 / 6765**

17. Wahlperiode **8.5.2024**

Große Anfrage

der Fraktion GRÜNE

und

Antwort

der Landesregierung

Cybersicherheit in Baden-Württemberg

Große Anfrage

Wir fragen die Landesregierung:

I. Das Cybersicherheitsökosystem Baden-Württemberg

1. Welche Rolle hat die Cybersicherheitsagentur Baden-Württemberg (CSBW) seit deren Gründung im Dezember 2021 im Cybersicherheitsökosystem Baden-Württemberg eingenommen (bitte unter Nennung von Meilensteinen)?

2. Wie sind die Zuständigkeiten in Baden-Württemberg hinsichtlich Cybersicherheit in der Landesverwaltung, Kommunalverwaltung, Wirtschaftsunternehmen und der kritischen Infrastruktur im Speziellen aufgeteilt – insbesondere auch solche, die aus Sicht des Landes zu den KRITIS zählen, jedoch nicht von der BSI-Kritisverordnung des Bundes erfasst werden (bitte aufgeteilt nach Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Medien und Kultur, Wasser, Ernährung, Finanz- und Versicherungswesen, Siedlungsabfallentsorgung, Staat und Verwaltung und unter Nennung der Rolle dieser Akteure bezüglich der Aufgaben Prävention, Detektion und Reaktion)?

3. Wie identifiziert, stärkt und fördert die Landesregierung theoretische und angewandte Cybersicherheitsforschung im Land (unter Nennung der wichtigen Standorte für innovative Cybersicherheitsforschung im Land)?

4. Warum werden mit dem Aufbau des strategischen und des operativen Fachbeirats Cybersicherheit das Entstehen weiterer Gremien gefördert, wobei mit der Gründung der CSBW eine Doppelung von Strukturen und somit eine Bündelung von Expertise erreicht werden sollte (bitte unter Nennung von Gründen, die gegen eine Übernahme von Aufgaben und Zuständigkeiten von Seiten der CSBW stehen)?

Eingegangen: 8.5.2024 / Ausgegeben: 4.7.2024

5. Wie wird die in der Cybersicherheitsstrategie erwähnte Intensivierung der Vernetzung der mit Cybersicherheit betrauten Akteure, Behörden und Gremien mit Hilfe des Aufbaus von erweiterten Kommunikationskanälen durch die CSBW konkret ausgestaltet (bitte unter Nennung der konkret beteiligten Akteure und deren verantwortetem Aufgabenbereich, der spezifischen Kommunikationskanäle und den zeitlichen Abspracheintervallen unter Berücksichtigung erreichter Meilensteine im Konzeptionierungsprozess)?

6. Warum sind fachspezifische Gremienstränge der Polizei und der Nachrichtendienste ausgenommen von der im Cybersicherheitsstrategiedokument erwähnten engen Zusammenarbeit mit der CSBW?

7. Inwieweit werden perspektivisch auch Akteure aus Wirtschaft, Wissenschaft und Zivilgesellschaft abseits von punktuellen Veranstaltungen in die regelmäßigen Vernetzungsaktivitäten des Landes einbezogen beispielsweise im Rahmen eines Fachbeirats Cybersicherheit (unter Angabe, wie diese regelmäßigen Vernetzungsaktivitäten inhaltlich in den Strategieprozess integriert werden sollen)?

8. Inwieweit finden die aktuellen und geplanten Vernetzungsaktivitäten auch unter Einbezug relevanter Landesbehörden, wie beispielsweise der Landesoberbehörde IT Baden-Württemberg (BITBW), statt (bitte unter Nennung von entsprechenden Austauschformaten und deren zeitlichen Struktur [bei Bedarf, regelmäßiger Turnus])?

9. Inwieweit sie ein einheitliches, landesweites Cybersicherheits-Lagebild möglichst in Echtzeit unter Berücksichtigung der vorhandenen relevanten Informationen aller beteiligten Akteure wie beispielsweise BITBW, Polizei und CSBW vorhält?

II. Aktuelle Cybersicherheitsstrategie Baden-Württemberg

1. Inwieweit definiert sie den Prozess für die Erstellung des Cybersicherheitskonzepts sowie der Cybersicherheitsstrategie als ständigen Verbesserungsprozess im Rahmen von Analyse-, Planungs-, Entscheidungs-, Finalisierung- und Umsetzungsphasen (wie bspw. bei der anerkannten PDCA-Methode)?

2. Inwieweit wird dies in der praktischen Arbeit beispielsweise in der Erstellung von Aktionsplänen oder eines Cybersecurity-Reifegradmodells für Baden-Württemberg umgesetzt?

3. Inwieweit ist das Land Baden-Württemberg in der Lage, neue technologische Entwicklungen wie bspw. Post-Quanten-Kryptographie zu erkennen, auf ihr Anwendungspotenzial hin zu überprüfen und zügig in bestehende Infrastruktur zu integrieren (bitte unter Nennung, ob ein spezifisches Konzept/Innovationsmanagement dafür existiert und Erläuterung dessen)?

4. Wie ist der aktuelle Umsetzungsstand der Cybersicherheitsstrategie Baden-Württemberg (bitte unter Nennung der SMART-Zieldimensionen [konkrete Maßnahme der Zielerreichung, Messgröße, Verantwortung, zeitliche Zieldimension, Realisierungswahrscheinlichkeit] der jeweiligen Strategieziele)?

5. Wurden – und wenn ja welche – in der aktuellen Cybersicherheitsstrategie angesprochenen Querschnittsbereiche für die Zusammenarbeit zwischen Innenministerium, Wirtschaftsministerium und dem Wissenschaftsministerium im Kontext Cybersicherheit bereits identifiziert?

III. Cybersicherheit für Wirtschaft, Kritische Infrastruktur (KRITIS) und ähnliche Einrichtungen in Baden-Württemberg

1. Inwieweit wurden für den Fall eines sicherheitsrelevanten Vorfalls bei einem Betreiber von kritischer Infrastruktur bereits klare Strukturen, Melde- und Alarmierungswege in Baden-Württemberg im Sinne eines kontinuierlichen Informationsflusses zwischen den verantwortlichen öffentlichen und privaten Stellen festgelegt und umgesetzt (bitte unter Darlegung der entsprechenden Strukturen, Melde- und Alarmierungswege)?

2. Wie schätzt sie im Kontext der aktuell zunehmenden Digitalisierung in diesem Bereich die Cybersicherheit in baden-württembergischen Krankenhäusern und Arztpraxen ein?

3. Wie wird das Angebot der Cyber-Ersthilfe seit deren Einrichtung nachgefragt (bitte unter Angabe der Anzahl der bearbeiteten Anfragen bzw. Fälle im Vergleich zur Zentralen Ansprechstelle Cybercrime [ZAC] aufgeschlüsselt nach relevanten Personengruppen bzw. Unternehmenskategorien)?

4. Wie weit ist die konkrete Konzeption einer Vermittlungsstelle zwischen kommerziellen IT-Sicherheitsdienstleistern und von Cyberangriffen betroffenen Unternehmen (bitte unter Angabe erreichten und geplanter Meilensteine)?

5. Ist die geplante Vermittlungsstelle aus der vorherigen Frage und die Arbeit der Cyber-Ersthilfe mit dem Cybersicherheitsnetzwerk des BSI abgestimmt (falls nicht, bitte unter Angabe von Gründen)?

6. Inwieweit sind Erkenntnisse aus dem digital@bw Projekt „Cyberwehr BW“ in die Konzeptionierung der Cyber-Ersthilfe beziehungsweise in die geplante Vermittlungsstelle zwischen kommerziellen IT-Sicherheitsdienstleistern und von Cyberangriffen betroffenen Unternehmen eingeflossen oder werden noch einfließen (falls dies der Fall sein sollte, bitte unter Angabe konkreter Aspekte)?

IV. Cybersicherheit für Kommunen und Behörden in Baden-Württemberg

1. Wie ist die Rollen- und Kompetenzverteilung im Bereich Cybersicherheit innerhalb der Landesverwaltung ausgestaltet (bitte unter Nennung der zuständigen Stellen wie Fachabteilungen des Innenministeriums, IT-Leitstellen und Chief Information Security Officer [CISOs] der einzelnen Ressorts und untergeordneten Stellen wie BITBW und CSBW)?

2. Wie hoch ist die kommunale Nachfrage nach Unterstützungsangeboten, wie zum Beispiel Informationsberatungen, IT-Sicherheitsanalysen und Schulungen der CSBW in den letzten zwölf Monaten beziehungsweise seit der Bereitstellung des Angebots, falls der Zeitraum kürzer als zwölf Monate sein sollte?

3. Sieht sie Bedarfe für weitere Unterstützungsangebote an Kommunen im Kontext der Einhaltung von angemessenen Cybersicherheitsstandards, wie zum Beispiel einer Ausweitung der Unterstützungsangebote der CSBW oder einem speziellen Förderprogramm für die Informationssicherheit in Kommunen?

4. Warum werden statt der geplanten punktuellen Schwachstellenscans der CSBW für öffentliche Stellen keine bereits vorhandenen automatisierten Lösungen, die dauerhaft nach Schwachstellen suchen und automatisiert Maßnahmen ergreifen, angewendet?

5. Inwieweit ist eine regelmäßige Teilnahme aller Bediensteten in der öffentlichen Verwaltung vom Land bis zur Kommune an Schulungen zum Thema Cybersicherheit vorgesehen?

6. Wie sieht der normative Vorgangsprozess für eine Kommunalverwaltung im Vergleich zur Landesverwaltung im Fall eines Ransomware-Vorfalls aus (bitte unter der Angabe der zuständigen unterstützenden Akteure während des jeweiligen Prozessschrittes von der Erkennung des Malwarebefall bis zur Beseitigung dieses samt angestrebtem Zeithorizont)?

7. Welche Rollen spielen relevante Akteure im Land wie zum Beispiel die CSBW, die BITBW und die Komm.One im Kontext von Special Operation Center (SOCs) in Baden-Württemberg (bitte unter Angabe, wo sich im Land bereits SOCs etabliert haben)?

8. Wie bewertet sie einen einfach zugänglichen Cybersicherheitsnotfallfonds für akute Cybersicherheitsvorfälle (bitte differenziert nach Zugriff für Landeseinrichtungen, Kommunen und Unternehmen im Land, bei Vorhandensein eines solchen bitte unter Nennung der zugangsberechtigten Akteure, Zugangsvoraussetzungen und der zur Verfügung stehenden Summe)?

9. Besitzen die CSBW, BITBW oder andere relevante Akteure im Land Notfallkompetenzen, die es ohne weitere Abstimmungsprozesse erlauben, unmittelbar Gegenmaßnahmen im Schadensfall zu ergreifen?

10. Wie wird aktuell eine 24-Stunden-Notfallhandlungsfähigkeit bei Notfallverantwortlichen in öffentlichen Stellen sichergestellt (bitte unter Nennung eines exemplarischen Umsetzungskonzepts)?

8.5.2024

Andreas Schwarz, Hildenbrand, Seimer

und Fraktion

Begründung

Die Cybersicherheitsagentur Baden-Württemberg (CSBW) hat im Januar 2024 ihr zweijähriges Jubiläum in ihrer Tätigkeit als formal eigenständige Landesoberbehörde gefeiert. Ziel der CSBW ist es, Doppelstrukturen zu verhindern und die Cybersicherheit in Baden-Württemberg für die Landesverwaltung und andere öffentliche Stellen in den Bereichen der Prävention, Detektion und Reaktion zu fördern. Diese Große Anfrage will den aktuellen Stand des Cybersicherheitskonzepts in Baden-Württemberg in Erfahrung bringen und die aktuelle strategische Ausrichtung des Landes erörtern.

Antwort

Schreiben des Staatsministeriums vom 24. Juni 2024 Nr. STM15SEC-0270-12/2/5:

In der Anlage übersende ich unter Bezugnahme auf § 63 der Geschäftsordnung des Landtags von Baden-Württemberg die von der Landesregierung beschlossene Antwort auf die Große Anfrage.

Hassler

Staatssekretär

Anlage: Schreiben des Ministeriums des Inneren, für Digitalisierung und Kommunen

Mit Schreiben vom 13. Juni 2024 Nr. IM4-0141-67/6/3 beantwortet das Ministerium des Inneren, für Digitalisierung und Kommunen im Einvernehmen mit dem Ministerium für Finanzen, dem Ministerium für Kultus, Jugend und Sport, dem Ministerium für Wissenschaft, Forschung und Kunst, dem Ministerium für Wirtschaft, Arbeit und Tourismus, dem Ministerium für Soziales, Gesundheit und Integration, dem Ministerium der Justiz und für Migration und dem Ministerium für Ernährung, Ländlichen Raum und Verbraucherschutz im Namen der Landesregierung die Große Anfrage wie folgt:

Wir fragen die Landesregierung:

I. Das Cybersicherheitsökosystem Baden-Württemberg

1. Welche Rolle hat die Cybersicherheitsagentur Baden-Württemberg (CSBW) seit deren Gründung im Dezember 2021 im Cybersicherheitsökosystem Baden-Württemberg eingenommen (bitte unter Nennung von Meilensteinen)?

Zu I. 1.:

Die Cybersicherheitsagentur Baden-Württemberg (CSBW) wurde mit der Verabschiedung des Gesetzes für die Cybersicherheit in Baden-Württemberg (Cybersicherheitsgesetz – CSG) am 4. Februar 2021 gegründet und ist formal seit dem 1. Januar 2022 als eigenständige Landesoberbehörde tätig. Zentrale Aufgabe der CSBW ist es, die Cybersicherheit in Baden-Württemberg zu fördern. Sie ist die zentrale Akteurin im Cybersicherheitsökosystem, deren Aufgaben in § 3 des CSG beschrieben sind. Im Fokus ihrer Arbeit stehen dabei vor allem die Landesverwaltung und andere öffentliche Stellen, also Behörden oder beispielsweise auch Einrichtungen im Verantwortungsbereich der Städte und Gemeinden. Mit der CSBW hat das Land Baden-Württemberg eine zentrale Koordinierungs- und Meldestelle geschaffen, die im ständigen Austausch mit allen relevanten Sicherheitsbehörden sowie weiteren Akteuren steht. Schwerpunktmäßig kommt sie folgenden Aufgaben, die durchaus als Meilensteinerreichung bezeichnet werden können, nach:

Seit dem Jahr 2021 erstellt die CSBW regelmäßige sowie anlassbezogene Lageinformationen zu Angriffen, Schwachstellen oder Sicherheitslücken, die über verschiedene Kanäle mit anderen Akteuren sowie möglicherweise betroffenen Stellen geteilt werden. Zudem baut die CSBW seit dem Jahr 2021 Kontakte zu weiteren Akteuren im Land auf und pflegt diese. So steht sie beispielsweise mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI), den CERTs (Computer Emergency Response Teams) der anderen Länder, den baden-württembergischen Sicherheitsbehörden und Rechenzentren in einem Regelaustausch und beteiligt sich an verschiedenen Gremien wie der Koordinierungsgruppe Informationssicherheit (KG InfoSic), bwInfoSec und dem Arbeitskreis Informationstechnik (AK-IT). Im Übrigen wird auf die Antworten zu den Fragen I. 5. und I. 8. verwiesen.

Zum 1. Juli 2022 startete die CSBW des Weiteren mit der Cyber-Ersthilfe eine rund um die Uhr erreichbare Anlaufstelle für von Cyberangriffen betroffene öffentliche Stellen, für Bürgerinnen und Bürger sowie für Unternehmen in Baden-Württemberg. Hilfesuchende erhalten bei Kontaktaufnahme eine Ersteinschätzung sowie eine Vermittlung zu zielgruppenspezifischen Anlaufstellen. Für betroffene Landeseinrichtungen, kommunale Einrichtungen oder auch Hochschulen können darüber hinaus unmittelbare Unterstützungsleistungen der CSBW über die Cyber-Ersthilfe initiiert werden.

Ebenfalls Mitte des Jahres 2022 übernahm die CSBW die Rolle und die Aufgaben des CERT BWL von der Landesoberbehörde IT Baden-Württemberg (BITBW). Seither fungiert die CSBW als zentrale Anlaufstelle für die Landesverwaltung, für die Kommunen und für die CERTs der Länder und des Bundes.

Seit dem 1. August 2022 ist die CSBW zentrale Kontaktstelle für Kritische Infrastrukturen (KRITIS) für das BSI nach § 8b des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) und gibt die vom BSI erhaltenen relevanten Informationen über Vorfälle im KRITIS-Bereich an die betreffenden Stellen weiter, § 3 Absatz 1 Nr. 5 CSG.

Ende des Jahres 2022 startete die CSBW ihre Sensibilisierungskampagne, die sich mit ihren verschiedenen Angeboten vorwiegend an die Mitarbeitenden der Landes- und Kommunalverwaltung richtet.

Ergänzend informiert die CSBW auf der Webseite *www.cybersicherheit-bw.de* seit Anfang des Jahres 2023 über ihre Arbeit und Angebote. Zudem stehen Informationsmaterialien im Bereich der Prävention auf der Website der CSBW kostenlos zur Verfügung.

Diese Website wurde Mitte des Jahres 2023 um Schulungsangebote ergänzt, welche für die gesamte Landes- und Kommunalverwaltung – von den Führungskräften bis zu den Mitarbeitenden – fertiggestellt und pilotiert wurden. Für die Nutzung der Schulungs- und Sensibiliserungsangebote der CSBW wurde eine Lernplattform geschaffen.

Im Jahr 2023 pilotierte die CSBW ein spezielles Beratungsangebot für Kommunen, das im Jahr 2024 in den Regelbetrieb überging und Checklisten sowie IT-Sicherheitsanalysen für Kommunen beinhaltet.

Bei gemeldeten Verdachtsfällen oder Vorfällen im Bereich der Landesverwaltung oder von Kommunen oder auch Hochschulen untersucht die CSBW die betreffenden Dateien, Mails oder Systeme, veranlasst Maßnahmen mit den betroffenen Stellen oder IT-Dienstleistern. Bei gravierenden Vorfällen unterstützt die CSBW mit forensischer Untersuchung und bei der Krisenkommunikation und -bewältigung. So hat die CSBW im Jahr 2023 214 gemeldete Fälle untersucht und bei acht gravierenden Vorfällen mit dem Einsatz ihres Mobile Incident Response Teams (MIRT) vor Ort unterstützt.

2. Wie sind die Zuständigkeiten in Baden-Württemberg hinsichtlich Cybersicherheit in der Landesverwaltung, Kommunalverwaltung, Wirtschaftsunternehmen und der kritischen Infrastruktur im Speziellen aufgeteilt – insbesondere auch solche, die aus Sicht des Landes zu den KRITIS zählen, jedoch nicht von der BSI-Kritisverordnung des Bundes erfasst werden (bitte aufgeteilt nach Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Medien und Kultur, Wasser, Ernährung, Finanz- und Versicherungswesen, Siedlungsabfallentsorgung, Staat und Verwaltung und unter Nennung der Rolle dieser Akteure bezüglich der Aufgaben Prävention, Detektion und Reaktion)?

Zu I. 2.:

Grundsätzlich ist jede öffentliche Stelle selbst für ihre Cybersicherheit verantwortlich. Dies ergibt sich für die Landesverwaltung aus der sich aus der Landesverfassung ableitenden Ressorthoheit (Artikel 49 Absatz 1 Landesverfassung Baden-Württemberg). Für die Kommunalverwaltungen ist diese Eigenverantwortung in dem verfassungsmäßigen Grundsatz der kommunalen Selbstverwaltung begründet (Artikel 28 Absatz 2 Grundgesetz).

Die CSBW unterstützt nach Maßgabe des CSG alle öffentlichen Stellen der Landesverwaltung und auch der Kommunalverwaltungen mit Maßnahmen in den Bereichen Prävention, Detektion und Reaktion. Denn insbesondere durch die zunehmende, ebenenübergreifende Vernetzung ist es notwendig, alle Beteiligten gleichermaßen auf ein angemessenes Sicherheitsniveau zu bringen. Das gesamte Sicherheitsniveau in einem Verbund wird letztlich von der schwächsten Stelle bestimmt.

Die Sicherstellung der Funktionsfähigkeit und der Schutz der KRITIS – sowohl im Cyberraum als auch im physischen Bereich – obliegt grundsätzlich deren Betreibern. Das BSI ist die zentrale Stelle für die Sicherheit Kritischer Infrastrukturen in Deutschland. Für eine Vielzahl von Wirtschaftsunternehmen und Unternehmen, welche in den in der Fragestellung genannten Sektoren tätig sind, erfolgen aufgrund der am 16. Januar 2023 in Kraft getretenen NIS-2-Richtlinie umfassende Neuregelungen in Bezug auf die Cybersicherheit. Dies betrifft in hohem Maße auch Stellen, die bisher nicht von der BSI-Kritisverordnung erfasst wurden. Die Umsetzung in nationales Recht erfolgt derzeit durch das Gesetzgebungsverfahren des Bundes zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG). Die nähere Ausgestaltung der daraus erwachsenden Anforderungen und Auswirkungen auf die betreffenden Unternehmen und Einrichtungen sind daher noch nicht abschließend darstellbar.

Weiter unterstützt die CSBW Stellen mit wichtiger Bedeutung für das öffentliche Gemeinwesen in Baden-Württemberg – unabhängig von der Rechtsform und unabhängig davon, ob diese von der BSI-Kritisverordnung des Bundes erfasst sind – gemäß § 6 Absatz 7 des CSG im Bereich der Reaktion, also insbesondere bei der Bewältigung von Vorfällen. Hierunter fallen beispielsweise Krankenhäuser oder Betriebe der Daseinsvorsorge, etwa Betriebe der Energieerzeugung oder Wasserversorgung.

Eine weitere tragende Säule in der Cybersicherheitsarchitektur Baden-Württembergs bilden die hochspezialisierten Organisationseinheiten der Polizei Baden-Württemberg. So wurde zur zielgerichteten Bekämpfung der Cyberkriminalität bereits im Jahr 2012 beim Landeskriminalamt Baden-Württemberg (LKA BW) eine eigene Abteilung 5 „Cybercrime und Digitale Spuren“ eingerichtet. Diese bearbeitet unter anderem herausragende Ermittlungsverfahren und bündelt Erkenntnisse ebenso wie landesweite Unterstützungsleistungen für die regionalen Polizeidienststellen. Mit der Umsetzung der Polizeistrukturreform im Jahr 2014 wurden korrespondierend zu der Abteilung „Cybercrime und Digitale Spuren“ des LKA BW in jedem regionalen Polizeipräsidium die spezialisierten „Kriminalinspektionen 5“ mit vergleichbarem Aufgabenspektrum eingerichtet und damit in die Fläche gebracht. In diesen Organisationseinheiten arbeiten speziell aus- und fortgebildete Polizeibeamtinnen und Polizeibeamte eng mit Cyberkriminalistinnen und Cyberkriminalisten und weiteren IT-Expertinnen und -Experten der Polizei zusammen. Neben der im Rahmen der Ermittlungsverfahren bei von Cyberangriffen betroffenen Einrichtungen geleisteten Unterstützung stellen die konkreten Ermittlungserfolge bei der Bekämpfung von Cybercrime ebenfalls eine wichtige Grundlage für ein hohes Cybersicherheitsniveau sowohl für die Landesverwaltung als auch für Kommunalverwaltungen, Wirtschaftsunternehmen und Unternehmen und Einrichtungen der kritischen Infrastruktur dar. So wurden unter Beteiligung der Polizei Baden-Württemberg in enger Kooperation mit nationalen und internationalen Partnern gegen Cyberkriminelle jüngst erfolgreiche Schläge geführt. Durch die in diesem Rahmen erfolgte Zerschlagung von für Cyberangriffe genutzter Infrastruktur wurden weitere Schäden in allen Bereichen verhindert.

Die beim LKA BW angesiedelte Zentrale Ansprechstelle Cybercrime (ZAC) steht Einrichtungen der Landesverwaltung, der Kommunalverwaltung, Wirtschaftsunternehmen und der kritischen Infrastruktur als zentraler und kompetenter Ansprechpartner ebenfalls zur Verfügung. Im Falle eines Cyberangriffs kann die ZAC eine Task Force mit Expertinnen und Experten aus verschiedenen Spezialisierungsbereichen aufrufen. In Fällen, in denen polizeiliche Einrichtungen forensische Untersuchungen im Bereich der Cybersicherheit anstellen und auch die CSBW unterstützend zur Systemwiederherstellung tätig ist, bauen die jeweiligen Untersuchungsergebnisse aufeinander auf und garantieren maximalen Erfolg.

Zu weitergehenden Ausführungen zum Bereich der Cyberkriminalität wird auf die Antwort auf Frage Nr. 4 der Kleinen Anfrage der Abg. Christian Gehring u. a. CDU (Drucksache 17/5254), verwiesen.

Neben der CSBW und der Polizei Baden-Württemberg komplettiert das Landesamt für Verfassungsschutz (LfV) das Fundament der Cybersicherheitsarchitektur

Baden-Württembergs. Die Cyberabwehr im LfV ist durch den gesetzlichen Auftrag nach § 3 Absatz 1 und 2 Landesverfassungsschutzgesetz (LVSG) für die Aufklärung und Abwehr von Cyberangriffen zuständig, die einen mutmaßlich staatlichen bzw. nachrichtendienstlichen Hintergrund aufweisen. Hauptaufgaben der Cyberabwehr sind die frühzeitige Angriffserkennung (Detektion), die technische Analyse zur Angriffsmethodik, die Erkenntnisgewinnung über mögliche Urheber (Attribution) sowie Sensibilisierungsmaßnahmen (Prävention). Diese Zuständigkeit gilt unabhängig davon, ob es sich bei dem möglichen Opfer um eine staatliche Stelle, ein Wirtschaftsunternehmen, eine akademische Einrichtung oder um eine Stelle handelt, die Teil der KRITIS in Baden-Württemberg ist.

Bei mutmaßlich staatlich gelenkten oder nachrichtendienstlich gesteuerten Cyberspionage- oder -sabotageangriffen besteht diese Zuständigkeit bei KRITIS-Betreibern zudem unabhängig davon, ob der jeweilige Betreiber in der derzeit noch gültigen BSI-Kritisverordnung des Bundes gelistet ist oder nicht.

3. Wie identifiziert, stärkt und fördert die Landesregierung theoretische und angewandte Cybersicherheitsforschung im Land (unter Nennung der wichtigen Standorte für innovative Cybersicherheitsforschung im Land)?

Zu I. 3.:

Die Cybersicherheitsforschung ist für die Landesregierung ein wichtiges Thema, welches in der Cybersicherheitsstrategie Baden-Württemberg verankert ist und an den verschiedenen Hochschulen im Land thematisch breit bearbeitet wird. Beispielhaft wird an dieser Stelle das Institut für Informationssicherheit und Verlässlichkeit (KASTEL) am Karlsruher Institut für Technologie (KIT) genannt, welches aus dem Kompetenzzentrum für Angewandte Sicherheitstechnologie hervorgegangen ist und seither Teil der KASTEL Security Research Labs *(https://kastel-labs.de/)* ist. Das Institut repräsentiert die Forschung und Lehre im Bereich der Informationssicherheit und Verlässlichkeit am KIT und deckt mit verschiedenen Forschungsgruppen eine große Bandbreite unterschiedlicher Themen ab. KASTEL steht darüber hinaus nicht nur für exzellente Forschung, sondern bildet auch wissenschaftlichen Nachwuchs für Wissenschaft und Wirtschaft auf höchstem Niveau aus. Des Weiteren bieten beispielsweise das KIT, die Universität Stuttgart und die Hochschule Aalen spezialisierte Studiengänge und Weiterbildungsprogramme im Bereich IT-Sicherheit bzw. Cybersicherheit an.

Auch an außeruniversitären Forschungseinrichtungen wird mit finanzieller Förderung durch das Land im Wege der institutionellen Förderung sowie der Projektförderung Cybersicherheitsforschung betrieben. Der Fokus liegt hierbei auf der wirtschaftsnahen Forschung sowie dem Technologietransfer in die Wirtschaft mit dem Ziel, sowohl die Cybersicherheit der Wirtschaft insgesamt zu stärken als auch die Innovations- und Wertschöpfungschancen von Cybersicherheitstechnologien zu nutzen. Schwerpunkte im Bereich der Cybersicherheitsforschung haben u. a. das Forschungszentrum Informatik (FZI) in Karlsruhe mit seinem Kompetenzzentrum für IT-Sicherheit als Anlaufstelle speziell für kleine und mittlere Unternehmen (KMU), Hahn-Schickard in Villingen-Schwenningen, das IMS Chips – Institut für Mikroelektronik in Stuttgart, das Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung in Karlsruhe sowie das Institut für KI-Sicherheit des Deutschen Zentrums für Luft- und Raumfahrt in Ulm etabliert.

Innovative Cybersicherheitstechnologien und -lösungen werden bzw. wurden von diesen Instituten beispielsweise im Rahmen der vom Ministerium für Wirtschaft, Arbeit und Tourismus geförderten Projekte InnoSecBW (Unterstützung von KMU bei der Entwicklung innovativer, cybersicherer Produkte und Services), NeMoH und DoRIe (Entwicklung von lernfähigen, sicheren und energieefizienten KI-Chips), CyberProtect (Entwicklung und Anwendung innovativer Sicherheitstechnologien speziell in Produktionsprozessen), Kompetenzzentrum für KI-Engineering Karlsruhe (Security von KI-Anwendungen in den Domänen Produktion und Mobilität) und KI-Allianz BW – Datenplattform (Cybersicherheitsaspekte beim Aufbau von Datenräumen) erforscht.

Darüber hinaus werden Cybersicherheitsforschung und Innovationen im Bereich Cybersicherheit auch im Rahmen des Programms Invest BW gefördert. Darin sind sowohl Unternehmen als auch Verbünde von Forschungseinrichtungen und Hochschulen mit Unternehmen förderberechtigt. Vorhaben der angewandten Cybersicherheitsforschung konnten bei den verschiedenen themenoffenen Förderaufrufen seit dem Jahr 2021 oder beim missionsorientierten Förderaufruf zu Digitalisierung und Künstliche Intelligenz von 2022 eingereicht werden. Letzterer bezog sich neben Künstlicher Intelligenz auf verschiedene Innovationen im Bereich Software und Hardware, etwa digitale Identitäten oder Technologien und Modelle für das sichere Teilen von Daten. Auch bei der aktuellen Fortführung von Invest BW sind Vorhaben mit Bezug zu Cybersicherheitsforschung antragsberechtigt, sofern sie in Verbundvorhaben zu Innovationen in Unternehmen beitragen.

Auf Grundlage der beiden Förderaufrufe „KI und Cybersicherheit“ (April 2022) und „Sicherheit mit und für KI“ (März 2023) werden zudem Unternehmen bei der Entwicklung von Sicherheitsinnovationen gefördert, bei denen Künstliche Intelligenz entweder zur Verbesserung der Sicherheit in den drei Bereichen Security (Schutz von digitalen Systemen vor absichtlichen Angriffen), Safety (Betriebssicherheit) und Privacy (Schutz von personenbezogenen Daten und die Gewährleistung der informationellen Selbstbestimmung) eingesetzt wird („Sicherheit mit KI“) oder die dazu beitragen, die Sicherheitseigenschaften von bestehenden KI-Systemen zu verbessern („Sicherheit für KI“).

Im Rahmen des Strategiedialog Automobilwirtschaft BW (SDA) wurde im Jahr 2023 eine Mission zum Thema Automotive Cybersecurity durchgeführt. Das digitale Fahrzeug, mithin das „Software-Defined Vehicle“, macht Cybersecurity zu einem zentralen Erfolgsfaktor für die Automobilwirtschaft. Auf Basis eines im Jahr 2022 veröffentlichten Themenpapiers des Clusters Elektromobilität Süd-West wurden die verschiedenen relevanten Aspekte des Themas Cybersecurity umfassend über den gesamten Lebenszyklus eines Fahrzeugs von der Entwicklung über die Produktion bis zum Betrieb mit den beteiligten Akteuren wie etwa dem FZI oder dem KASTEL diskutiert. In einem Workshop diskutierten Teilnehmende aus Forschung, Industrie und Kfz-Gewerbe u. a. Fragen zur Konsistenz des Rechtsrahmens auf internationaler, europäischer und nationaler Ebene sowie zur notwendigen Sensibilisierung aller Akteure.

4. Warum werden mit dem Aufbau des strategischen und des operativen Fachbeirats Cybersicherheit das Entstehen weiterer Gremien gefördert, wobei mit der Gründung der CSBW eine Doppelung von Strukturen und somit eine Bündelung von Expertise erreicht werden sollte (bitte unter Nennung von Gründen, die gegen eine Übernahme von Aufgaben und Zuständigkeiten von Seiten der CSBW stehen)?

Zu I. 4.:

Der Aufbau und operative Betrieb der CSBW hat gezeigt, dass die in der Cybersicherheitsstrategie definierten Ziele durch die vorhandenen Gremien und Strukturen im Land, etwa dem AK-IT und der KG InfoSic ebenso wie durch die regelmäßigen und institutionalisierten Austausche mit dem BSI, den CERTs der Länder und den weiteren Partnern der CSBW auch aus dem Bereich der Wirtschaft erreicht werden können. Dies gilt auch für Themen, welche die Zusammenhänge der Cybersicherheit mit übergeordenten Themen der Digitalisierung betreffen. Auch für die Erreichung eines Lagebildes hat sich gezeigt, dass die bereits bestehenden Strukturen und insbesondere auch der Austausch mit dem BSI und den weiteren Ländern effektiv genutzt werden kann. Die Etablierung eines weiteren Gremiums in Form eines Fachbeirats bleibt daher bis auf Weiteres ausgesetzt.

5. Wie wird die in der Cybersicherheitsstrategie erwähnte Intensivierung der Vernetzung der mit Cybersicherheit betrauten Akteure, Behörden und Gremien mit Hilfe des Aufbaus von erweiterten Kommunikationskanälen durch die CSBW konkret ausgestaltet (bitte unter Nennung der konkret beteiligten Akteure und deren verantwortetem Aufgabenbereich, der spezifischen Kommunikationskanäle und den zeitlichen Abspracheintervallen unter Berücksichtigung erreichter Meilensteine im Konzeptionierungsprozess)?

Zu I. 5.:

Seit ihrer Gründung hat die CSBW die Vernetzung staatlicher Einrichtungen, der Wirtschaft sowie von Wissenschaft und Forschung im Bereich der Cybersicherheit vorangetrieben und verstetigt. Um die Cybersicherheit des Landes zu stärken, ist die Zusammenarbeit mit weiteren Partnern unerlässlich. Aus diesem Grund befindet sich die CSBW in regelmäßigem fachlichen Austausch und arbeitet selbst am Aufbau entsprechender Strukturen mit. Die CSBW tauscht sich etwa stetig, aber auch anlassbezogen mit dem LKA BW, dem LfV, dem Sicherheitszentrum IT in der Finanzverwaltung Baden-Württemberg (SITiF BW), der Komm.ONE und den Rechenzentren der Landesverwaltung aus. Darüber hinaus ist die CSBW mit allen anderen CERTs der Länder und dem BSI in laufendem, meist täglichem Austausch. Mit dem kommunalen Bereich wird über den operativen Bereich hinaus auch auf der strategischen Ebene über die Kommunalen Landesverbände eine noch intensivere Vernetzung vorbereitet. Mit Forschungseinrichtungen und Wirtschaftsakteuren steht die CSBW ebenfalls in einem Austausch.

Die Vernetzungsvorhaben wurden direkt nach Gründung der CSBW aufgenommen, sukzessive verstetigt und weiter ausgebaut. Sie unterliegen keinem festen Ausbauprozess und werden anlassbezogen und bedarfsgerecht weiterentwickelt. Für die Vernetzung mit den relevanten Landesbehörden wird außerdem auf die Antwort zur Frage I. 8. verwiesen. Die wesentlichen Vernetzungsaktivitäten der CSBW lassen sich im Sinne der Fragestellung auszugsweise wie folgt aufschlüsseln:

Akteure	Aufgabenbereiche	Kommunikations-kanäle	Intervalle
CSBW Lagezentrum, LKA BW, LfV, BITBW, SITiF BW, Komm.ONE	Warn- und Informationsdienst, Lageeinschätzung; Austausch zu veröffentlichten Schwachstellen	Gängige technische Formate, persönliche Treffen	Regelmäßig und anlassbezogen; oft täglich
Verwaltungs-CERT-Verbund (VCV)	CERTs der Länder und des Bundes; BSI; wichtiges Lagebildinstrument	Technisches Format/ Persönliche Arbeitstreffen	täglich und anlassbezogen; Austauschtreffen persönlich i. d. R. halbjährlich
Landes-CISO und Sicherheitsbeauftragte der Ressorts, BITBW, des LZfD, des Landtags, des Rechnungshofs, des LFDI und der CSBW (KG InfoSic)	Alle Themen der IT-Sicherheit und Informationssicherheit der Landesverwaltung und der Beteiligten	Gremiensitzungen per Videokonferenz und in Präsenz	Anlassbezogen und regelmäßig 6-wöchig
bwInfoSec und CSBW	Informationssicherheitsbeauftragte (ISBs) der Hochschulen + Kernteam Hochschulen und Universitäten zur Lage und zur Abstimmung von Maßnahmen	Videokonferenzen	Monatlich; mit dem Kernteam einer Hochschule wöchentlich
Hessen-CERT H3C und CSBW	Aktuelle CERT-Themen, Threat Intelligence und Darknet-Monitoring	Videokonferenzen; vereinzelt auch Präsenz	wöchentlich
Austausche der CSBW mit Einrichtungen der Cybersicherheit aus USA, Israel, Spanien	Cal OES, INCD, Agència de ciberseguretat de Catalunya	Videokonferenzen & vor Ort beim Cybersicherheitsforum International	anlassbezogen

Hinsichtlich der Vernetzung der CSBW mit Hochschuleinrichtungen ist anzuführen, dass die Hochschulen an den Warn- und Informationsdienst der CSBW angebunden sind und regelmäßig über aktuelle Gefahrenlagen und mögliche Handlungsoptionen informiert werden. Hierzu zählen auch Mitteilungen zu Präventionsmaßnahmen und zur Detektion verdächtiger Aktivitäten. Das CERT BWL der CSBW ist in Krisenfällen eine der ersten Anlaufstellen für Hochschulen. Somit kooperieren Hochschulen und CSBW sowohl im reaktiven als auch im präventiven Bereich. Die Unterstützung des CERT BWL wurde im letzten Jahr von verschiedenen Hochschulen in Anspruch genommen. Um die Kooperation zwischen den Hochschulen des Landes weiter zu intensivieren und zu verstetigen, wurde eine Arbeitsgruppe aus der Föderation bwInfoSec und der CSBW etabliert.

Weitere Einzelheiten zu der konkreten Ausgestaltung der Vernetzung und der daraus resultierenden regelmäßigen und einzelfallbezogenen Austausche insbesondere mit internationalen Partnern unterliegen regelmäßig Geheimhaltungsvereinbarungen mit den Partnern.

6. Warum sind fachspezifische Gremienstränge der Polizei und der Nachrichtendienste ausgenommen von der im Cybersicherheitsstrategiedokument erwähnten engen Zusammenarbeit mit der CSBW?

Zu I. 6.:

Die in der Fragestellung zitierte Passage trägt dem Umstand Rechnung, dass das LKA BW und das LfV grundsätzlich andere Aufgaben und Zuständigkeiten haben und mithin die Themen der Cybersicherheit aus unterschiedlichen Blickwinkeln heraus betrachten. So ist etwa das LKA BW als Strafverfolgungsbehörde unmittelbar zuständig für die Strafverfolgung bei Cyberangriffen. Das LfV ist hingegen die zuständige Behörde für die Abwehr von Cyberspionage und -sabotage mit (mutmaßlich) staatlich gelenktem beziehungsweise nachrichtendienstlichem Hintergrund. Bei der Zusammenarbeit der Sicherheitsbehörden sind diverse verfassungsrechtliche und einfachgesetzliche Vorgaben zu beachten.

Im Übrigen behandeln die polizeilichen Gremienstränge fachspezifische Themen der Polizei und dienen unter anderem dem Zweck, die polizeiliche Zusammenarbeit zu stärken und polizeiliche Standards zu etablieren. Die CSBW ist keine Polizeidienststelle. Eine Beteiligung der CSBW an Gremiensträngen der Polizei wäre daher schon aus formalen Gründen nicht möglich.

Die Cyberabwehr und der Behörden- und Wirtschaftsschutz im LfV sind intensiv in fachspezifische Gremienstrukturen des Verfassungsschutzverbundes eingebunden, welcher ausschließlich das Bundesamt für Verfassungsschutz (BfV) und die Verfassungsschutzbehörden der Länder umfasst. Soweit die gewonnenen Erkenntnisse und Hintergründe nicht besonders eingestuft sind und keinen Weitergabevorbehalten (z. B. Third Party Rule) unterliegen, werden diese mit den weiteren Sicherheitsbehörden geteilt.

All dies führt zu dem im Strategiedokument beschriebenen Umgang mit den fachspezifischen Gremiensträngen. Gleichwohl findet unter diesen Rahmenbedingungen – regelmäßig und institutionalisiert – eine enge Zusammenarbeit der CSBW mit Polizei und Verfassungsschutz statt, und zwar sowohl zur Lagebilderzeugung als auch bei der konkreten Bewältigung akuter Fälle.

7. Inwieweit werden perspektivisch auch Akteure aus Wirtschaft, Wissenschaft und Zivilgesellschaft abseits von punktuellen Veranstaltungen in die regelmäßigen Vernetzungsaktivitäten des Landes einbezogen beispielsweise im Rahmen eines Fachbeirats Cybersicherheit (unter Angabe, wie diese regelmäßigen Vernetzungsaktivitäten inhaltlich in den Strategieprozess integriert werden sollen)?

Zu I. 7.:

Im Bereich der Wirtschaft besteht ein fachlicher Austausch vor allem mit Verbänden, den Industrie- und Handelskammern sowie den Handwerkskammern, u. a. im Rahmen der Initiative Wirtschaft 4.0 und der Allianz Industrie 4.0 Baden-Württemberg. Dieser wird durch den derzeit von dem Ministerium des Inneren, für Digitalisierung und Kommunen und der CSBW in Zusammenarbeit mit dem Ministerium für Wirtschaft, Arbeit und Tourismus vorbereiteten Rollout eines niederschwelligen Beratungskonzepts für KMU weiter vertieft und verstetigt.

Mit dem Cybersicherheitsforum findet zudem einmal jährlich ein Vernetzungstreffen von Expertinnen und Experten statt, welches auch Akteure von Wirtschaft, Wissenschaft und Zivilgesellschaft umfasst.

Das Ministerium des Inneren, für Digitalisierung und Kommunen, das Ministerium für Wirtschaft, Arbeit und Tourismus, das LfV und das LKA BW sind außerdem Mitglied im Sicherheitsforum Baden-Württemberg, einem unabhängigen Gremium aus Unternehmen, Wissenschaft und Verwaltung, das es sich zur Aufgabe gemacht hat, die heimische Wirtschaft und Forschung beim Schutz ihres Wissens und ihrer Innovationen zu unterstützen.

Zu Vernetzungsaktivitäten mit Akteuren aus dem Bereich der Wissenschaft wird auf die Antwort zur Frage I. 5. verweisen. Die Universitäten und Hochschulen des Landes Baden-Württemberg haben sich zur Föderation bwInfoSec zusammengeschlossen. Hierüber stehen sie in engem Austausch und sind in Kooperationen im Bereich der Cybersicherheit beispielsweise mit der CSBW oder dem Wissenschaftsnetzwerk BelWü sowie mit multilateralen Kooperationsprojekten wie dem CampusNetz – hier arbeiten mehrere Universitäten unter Leitung des KIT zusammen. Ferner vernetzt bwInfoSec die beteiligten Institutionen hochschulartübergreifend in verschiedenen Arbeitsgruppen.

Zudem unterhält das LfV im Rahmen seiner Präventionsstrategie zahlreiche Formate, um gefährdete Stellen in Baden-Württemberg umfassend vor nachrichtendienstlich gesteuerten Cyberangriffen zu warnen. Dies betrifft Akteure aus der Wirtschaft, Wissenschaft und Forschung, staatliche Stellen und Betreiber von KRITIS. Im Übrigen wird auf die Antwort zur Frage I. 4. verwiesen.

Die Landesregierung beobachtet die Bedarfe der in der Fragestellung genannten Akteure sehr genau und bewertet sie fortwährend. Sollte sich herausstellen, dass ein Bedarf besteht, der über die bereits bestehenden, umfassenden Vernetzungsaktivitäten hinausgeht, wird dies im Rahmen der perspektivischen Planungen Berücksichtigung finden.

8. Inwieweit finden die aktuellen und geplanten Vernetzungsaktivitäten auch unter Einbezug relevanter Landesbehörden, wie beispielsweise der Landesoberbehörde IT Baden-Württemberg (BITBW), statt (bitte unter Nennung von entsprechenden Austauschformaten und deren zeitlichen Struktur [bei Bedarf, regelmäßiger Turnus])?

Zu I. 8.:

Die CSBW richtet als Regeltermin einmal wöchentlich eine dem behördenübergreifenden Lageaustausch mehrerer Landes- und Sicherheitsbehörden dienende Besprechung aus. Teilnehmende sind die BITBW, die Komm.ONE, die SITiF BW, das LfV und das LKA BW. Das LKA BW ist mit der ZAC vertreten. Er-

gänzend erfolgt zwischen der ZAC und der CSBW auch fallorientiert ein lageangepasster Informationsaustausch. Darüber hinaus besteht seit dem Jahr 2020 ein Kooperationsvertrag zwischen dem Ministerium des Inneren, für Digitalisierung und Kommunen und der Energie Baden-Württemberg AG (EnBW) zur Bekämpfung der Cyberkriminalität und für den Schutz kritischer Infrastrukturen, welche vom LKA BW und der CSBW operativ ausgestaltet wird. Im Übrigen wird auf die Antwort zur Frage I. 5. verwiesen.

9. Inwieweit sie ein einheitliches, landesweites Cybersicherheits-Lagebild möglichst in Echtzeit unter Berücksichtigung der vorhandenen relevanten Informationen aller beteiligten Akteure wie beispielsweise BITBW, Polizei und CSBW vorhält?

Zu I. 9.:

Die CSBW erstellt verschiedene Lagebilder und Berichte. So werden als wichtiger Teil des Lagebildes etwa Warnhinweise und Handlungsempfehlungen zu Schwachstellen und Sicherheitslücken oder zu erfolgten oder versuchten Cyberangriffen unmittelbar nach Bekanntwerden geteilt. Außerdem werden wöchentliche Lageberichte zur Cybersicherheitslage im Land und anlassbezogene Führungsinformationen zu Cybersicherheitsvorfällen verfasst. In die Berichte und Lagebilder fließen Erkenntnisse anderer Stellen ein. Im Jahr 2023 hat die CSBW 98 Führungsinformationen (inkl. Nachträgen), 52 Wochenberichte sowie 56 Warn- und Handlungsempfehlungen (inkl. Nachträgen) erstellt und zielgruppenspezifisch verteilt. Im ersten Quartal 2024 hat die CSBW 7 Führungsinformationen (inkl. Nachträgen), 13 Wochenberichte sowie 12 Warn- und Handlungsempfehlungen (inkl. Nachträgen) erstellt und zielgruppenspezifisch verteilt. In ihrem Jahresbericht 2023 liefert die CSBW eine allgemeine Lageeinschätzung zur Situation in Baden-Württemberg sowie ein Lagebild bezogen auf das Fallaufkommen bei der CSBW.

Der Informationsaustausch zwischen Polizei, Verfassungsschutz und CSBW erfolgt auf Arbeitsebene fallorientiert und lageangepasst. Dabei werden bei neu aufkommenden Modi Operandi oder aktuell ausgenutzten Schwachstellen niederschwellig und schnell entsprechende Informationen an die CSBW weitergeleitet, die in die Lagebilderstellung der CSBW einfließen.

II. Aktuelle Cybersicherheitsstrategie Baden-Württemberg

1. Inwieweit definiert sie den Prozess für die Erstellung des Cybersicherheitskonzepts sowie der Cybersicherheitsstrategie als ständigen Verbesserungsprozess im Rahmen von Analyse-, Planungs-, Entscheidungs-, Finalisierung- und Umsetzungsphasen (wie bspw. bei der anerkannten PDCA-Methode)?

2. Inwieweit wird dies in der praktischen Arbeit beispielsweise in der Erstellung von Aktionsplänen oder eines Cybersecurity-Reifegradmodells für Baden-Württemberg umgesetzt?

Zu II. 1. und II. 2.:

Die Fragen II. 1 und II. 2 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Aufgrund wachsender Gefährdungen und immer neuer Anforderungen müssen die Maßnahmen der Informations- und Cybersicherheit kontinuierlich überprüft und angepasst werden. Für die Landesverwaltung ist in der Verwaltungsvorschrift des Innenministeriums zur Informationssicherheit (VwV Informationssicherheit) festgelegt, dass die Standards des BSI anzuwenden sind. Dabei ist die Informationssicherheit als kontinuierlicher Prozess zu gestalten. Wesentliches Element dabei ist, dass die in diesem Rahmen getroffenen organisatorischen Maßnahmen und Regelungen ebenso wie die dokumentiert umgesetzten technischen Maß-

nahmen einer Plan-Do-Check-Act-Methode (PDCA) unterliegen. Dieser Prozess sieht die Überprüfung der Umsetzung und der Wirksamkeit von Sicherheitsmaßnahmen und gegebenenfalls die Vornahme erforderlicher Anpassungen vor. Durch den Prozess soll gewährleistet werden, dass das Sicherheitsniveau der jeweiligen Anforderungen des IT-Grundschutzes jederzeit bedarfsgerecht angepasst und fortgeschrieben werden kann. Das Ministerium des Inneren, für Digitalisierung und Kommunen wird zusammen mit der CSBW darüber hinaus für die Landesverwaltung eine Methodik zur Messung des erreichten Reifegrads auf Basis des zwischen Bund und Ländern im IT-Planungsrat abgestimmten und praktizierten Modells entwickeln.

Die Cybersicherheitsstrategie Perspektive 2026 wird zu gegebener Zeit unter besonderer Berücksichtigung der Entwicklungen im Cyberraum als auch der Entwicklungen auf Ebene der Europäischen Union, des Bundes und der Länder in Bezug auf die ebenenübergreifende Zusammenarbeit fortgeschrieben.

3. Inwieweit ist das Land Baden-Württemberg in der Lage, neue technologische Entwicklungen wie bspw. Post-Quanten-Kryptographie zu erkennen, auf ihr Anwendungspotenzial hin zu überprüfen und zügig in bestehende Infrastruktur zu integrieren (bitte unter Nennung, ob ein spezifisches Konzept/Innovationsmanagement dafür existiert und Erläuterung dessen)?

Zu II. 3.:

Im Rahmen des vom Ministerium für Wissenschaft, Forschung und Kunst und dem Ministerium für Wirtschaft, Arbeit und Tourismus gemeinsam geförderten Innovationscampus QuantumBW wurde neben der Quantensensorik das Quantencomputing sowie Quantennetzwerke als zentrale Bereiche identifiziert, in denen Baden-Württemberg bereits heute stark ist. Diese Bereiche wurden bzw. werden mit Technologie-Roadmaps und strategischen Zielesetzungen unterlegt. Im Advisory Board von QuantumBW werden die Roadmaps kontinuierlich überprüft und ggf. nachjustiert. Darüber hinaus werden nationale und internationale Entwicklungen beobachtet und es findet eine Evaluierung der daraus resultierenden Implikationen für QuantumBW statt.

Die CSBW ist zu neuen technologischen Entwicklungen u. a. mit dem BSI im Austausch. Zudem besteht zwischen dem Land und der Agentur für Innovation in der Cybersicherheit ein Austausch. Diese versteht sich als „treibende Kraft einer offenen Innovations- und Wagniskultur und für ein lebendiges Ökosystem zur Förderung von Cybersicherheitstechnologien“ und beschreibt ihren Auftrag mit dem „Vorantreiben von Forschung sowie bahnbrechender Innovationen im Bereich der Cybersicherheit und diesbezüglicher Schlüsseltechnologien im Bereich der inneren und äußeren Sicherheit“.

Im Bereich der BITBW werden neue technologische Entwicklungen sowohl von der BITBW selbst identifiziert, aber auch von den Kunden an die BITBW herangetragen. Daraus resultierende Projekte zur Weiterentwicklung der IT-Landschaft werden durch das Architekturmanagement der BITBW hinsichtlich technologischer Standardisierung, Zukunftsfähigkeit und Servicepotenzial geprüft und anschließend durch das sogenannte „Project Advisory Board“ bewertet und freigegeben. Hierzu werden auch Konzepte wie etwa die technische Richtlinie des BSI zum Thema Post-Quanten-Kryptografie herangezogen.

4. Wie ist der aktuelle Umsetzungsstand der Cybersicherheitsstrategie Baden-Württemberg (bitte unter Nennung der SMART-Zieldimensionen [konkrete Maßnahme der Zielerreichung, Messgröße, Verantwortung, zeitliche Zieldimension, Realisierungswahrscheinlichkeit] der jeweiligen Strategieziele)?

Zu II. 4.:

Viele der in der Cybersicherheitsstrategie benannten Ziele wurden bereits realisiert oder befinden sich aktuell in Umsetzung. So kommt dem von der CSBW geschaffenen Lagezentrum besondere Bedeutung zu. Die Expertinnen und Experten der CSBW erstellen und verteilen anlassbezogen und regelmäßig aktuellste Lagebilder. Dazu sammeln sie Daten zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen aus Informationsquellen von Staat, Wirtschaft und Wissenschaft, werten diese aus und verfassen Warnmeldungen und Handlungsempfehlungen. Auch die in der Cybersicherheitsstrategie beschriebenen Vernetzungsaktivitäten sind weit gediehen. Die von der CSBW organisierte institutionalisierte und anlassbezogene Zusammenarbeit in Baden-Württemberg mit der Polizei, dem Verfassungsschutz, der BITBW, dem LZfD, dem SITiF BW, der Komm.ONE und den Hochschuleinrichtungen ebenso wie die Zusammenarbeit mit dem BSI und den CERTs des Bundes und der Länder und internationalen Partnern stellen eine wichtige Grundlage der Arbeit der CSBW dar.

Eine Aufschlüsselung des aktuellen Umsetzungsstands der Cybersicherheitsstrategie befindet sich in Anlage 1. Aus der tabellarischen Übersicht ergibt sich, dass bereits viele Ziele realisiert sind bzw. sich in der Umsetzung befinden. Die Landesregierung ist bestrebt, verbleibende Maßnahmen zeitnah umzusetzen.

5. Wurden – und wenn ja welche – in der aktuellen Cybersicherheitsstrategie angesprochenen Querschnittsbereiche für die Zusammenarbeit zwischen Innenministerium, Wirtschaftsministerium und dem Wissenschaftsministerium im Kontext Cybersicherheit bereits identifiziert?

Zu II. 5.:

Auch wenn das Thema Cybersicherheit zuallererst in der Verantwortung jedes einzelnen Unternehmens liegt, unterstützt die Landesregierung Unternehmen dabei, sich vor Schäden infolge gravierender Cyberangriffe zu schützen. Daher wurden in der aktuellen Cybersicherheitsstrategie des Landes „Angebote für breite Zielgruppen wie etwa Sensibilisierungsthemen und Informationsangebote“ als wichtiger Querschnittsbereich für die Zusammenarbeit zwischen den Ministerien identifiziert.

Beispielhaft kann hier auf die Umsetzung des von dem Ministerium des Inneren, für Digitalisierung und Kommunen und der CSBW geschaffenen Beratungskonzepts für KMU verwiesen werden, das in Zusammenarbeit mit dem Ministerium für Wirtschaft, Arbeit und Tourismus und über Multiplikatoren wie die Industrie- und Handelskammern, die Handwerkskammern und das Digital-Hub-Netzwerk für Unternehmen in ganz Baden-Württemberg zur Verfügung gestellt werden soll. In Folge des derzeit vorbereiteten Rollouts dieses Beratungskonzepts soll auch die Projektierung einer Konzeption zum Aufbau eines Dienstleisternetzwerkes für den Bereich der Prävention gemeinsam zwischen dem Ministerium des Inneren, für Digitalisierung und Kommunen und dem Ministerium für Wirtschaft, Arbeit und Tourismus unter Einbindung der CSBW und des BSI geprüft werden. Mit dem Beratungskonzept wird das bereits bestehende Unterstützungsangebot für KMU bei der Cybersicherheit zielgerichtet und bedarfsorientiert ergänzt, zu dem u. a. die Investitionsförderung für KMU im Rahmen der „Digitalisierungsprämie Plus“ sowie der „Leitfaden zur Etablierung von Cyber-Bündnissen“ zählen, welcher von der Allianz Industrie 4.0 Baden-Württemberg mit finanzieller Förderung durch das Ministerium für Wirtschaft, Arbeit und Tourismus erarbeitet wurde.

Darüber hinaus kooperieren beide Ministerien beispielsweise bei der alle zwei Jahre stattfindenden Verleihung des Sicherheitspreises, bei dem unter anderem

herausragende Cybersicherheitskonzepte ausgezeichnet werden, sowie bei der Ausrichtung des 6. Cybersicherheitsforums im Oktober 2024 unter dem Oberthema „Cybersicherheit und KI“, welches vom Ministerium des Inneren, für Digitalisierung und Kommunen organisiert und durch das Ministerium für Wirtschaft, Arbeit und Tourismus mit einem eigenen Fachpanel zum Thema Cybersicherheit in der Wirtschaft ergänzt wird. Im Mai 2024 organisierte das Ministerium für Wirtschaft, Arbeit und Tourismus unter Beteiligung des Ministeriums des Inneren, für Digitalisierung und Kommunen die Veranstaltung „Cybersicherheit duldet keinen Aufschub – Was bedeutet NIS 2 für Ihr Unternehmen?“, die Unternehmen über die Vorgaben der neuen europäischen NIS 2 – Richtlinie aufklärte und über allgemeine Strategien zur Verringerung von Cyberrisiken informierte.

Darüber hinaus ist geplant, die im Bereich der Prävention auch von der CSBW erstellten Lageinformationen, Warnmeldungen und Materialien zur Mitarbeitersensibilisierung auch Unternehmen zugänglich zu machen. Auch hierzu sollen die umfassenden Kontakte des Ministeriums für Wirtschaft, Arbeit und Tourismus gemeinsam genutzt werden.

Hinsichtlich der angesprochenen Zusammenarbeit zwischen dem Ministerium des Inneren, für Digitalisierung und Kommunen und dem Ministerium für Wissenschaft, Forschung und Kunst stellen insbesondere die in den Antworten zu den Fragen I. 5. und I. 7. dargelegten Vernetzungsaktivitäten mit Akteuren aus dem Bereich der Wissenschaft ein wichtiges Ergebnis der vorgenommenen Identifizierung entsprechender Querschnittsbereiche zwischen dem Ministerium des Inneren, für Digitalisierung und Kommunen und dem Ministerium für Wissenschaft, Forschung und Kunst dar. Die daraus resultierende operative Ausgestaltung erfolgt in der Zusammenarbeit zwischen der CSBW und den zur Föderation bwInfoSec zusammengeschlossenen Universitäten und Hochschulen.

Ein Querschnittsbereich wird außerdem in der Aus- und Weiterbildung von Cybersicherheits-Fachkräften gesehen. Die CSBW und das LKA BW engagieren sich im Rahmen einer Ausbildungskooperation mit der EnBW bei der Bereitstellung von jährlich zwei berufsbegleitenden Studienplätzen an der DHBW Heilbronn. Ende 2022 konnten erstmals zwei Studierende ihre Rotationsphase bei der CSBW beginnen, im Jahr 2023 betreute die CSBW einen Studierenden.

III. Cybersicherheit für Wirtschaft, Kritische Infrastruktur (KRITIS) und ähnliche Einrichtungen in Baden-Württemberg

1. Inwieweit wurden für den Fall eines sicherheitsrelevanten Vorfalls bei einem Betreiber von kritischer Infrastruktur bereits klare Strukturen, Melde- und Alarmierungswege in Baden-Württemberg im Sinne eines kontinuierlichen Informationsflusses zwischen den verantwortlichen öffentlichen und privaten Stellen festgelegt und umgesetzt (bitte unter Darlegung der entsprechenden Strukturen, Melde- und Alarmierungswege)?

Zu III. 1.:

Nach dem BSI-Gesetz liegt die Zuständigkeit für die Betreiber von KRITIS, auch in Bezug auf wesentliche Maßnahmen der IT-Sicherheit, wie etwa der Meldung sicherheitsrelevanter Vorfälle, beim BSI. Die CSBW ist gegenüber dem BSI als zentrale Kontaktstelle nach § 8b BSI-Gesetz benannt. In dieser Funktion erhält die CSBW die relevanten Informationen und gibt diese unmittelbar an die jeweils fachlich zuständigen und einzubindenden Stellen in der Landesverwaltung weiter. Damit sind eindeutige Strukturen, Prozesse und Melde- und Alarmierungswege geschaffen. Eine Information erfolgt immer dann, wenn es sich um eine akute (noch anhaltende) Störung handelt, in deren Folge Ausfälle einer kritischen Dienstleistung auf lokaler, regionaler oder nationaler Ebene eingetreten sind oder eintreten können oder Auswirkungen für die öffentlichen Sicherheit bestehen oder erwartet werden können.

Zur Aufnahme des festgelegten Informationsaustausches zwischen dem BSI und der CSBW mussten diverse Rahmenbedingungen sichergestellt werden. Hierunter fällt beispielsweise der Grad der Verschlüsselung der Kommunikationsverbindung sowie eine BSI-Zertifizierung für die zur Koppelung der Netze verwendeten Komponenten. Baden-Württemberg erfüllt mit der CSBW sämtliche Rahmenbedingungen. Das bestätigt auch der entsprechende Bericht des Bundesministeriums des Innern und für Heimat (Stand Dezember 2023), der Baden-Württemberg als eines der ersten Länder benennt, das die einschlägigen Rahmenbedingungen erfüllte.

2. Wie schätzt sie im Kontext der aktuell zunehmenden Digitalisierung in diesem Bereich die Cybersicherheit in baden-württembergischen Krankenhäusern und Arztpraxen ein?

Zu III. 2.:

Gemäß § 28 Absatz 2 Landeskrankenhausgesetz Baden-Württemberg (LKHG BW) sind Krankenhäuser dazu verpflichtet, durch geeignete Vorkehrungen, insbesondere durch die Erstellung und Fortschreibung von Alarm- und Einsatzplänen, sicherzustellen, dass auch bei einem Massenanfall von Verletzten oder Erkrankten eine ordnungsgemäße Versorgung der Patientinnen und Patienten gewährleistet werden kann. Kommt es zu einem Cyberangriff, der zum EDV-Ausfall eines Krankenhauses führt, ist dieses gezwungen, auf den analogen Betrieb umzustellen, was mit einer enormen Leistungsminderung einhergeht. Angesichts dieser Bedrohungssituation ist Cybersicherheit eine notwendige und unumgängliche Bedingung für die Digitalisierung.

Auch die Erkenntnisse und Erfahrungen der CSBW zeigen, dass Krankenhäuser immer wieder von Cyberangriffen betroffen sind. Solche Angriffe können erhebliche Auswirkungen auf den Krankenhausbetrieb haben. Daher unterstützt die CSBW im Einzelfall auch diese Stellen, insbesondere bei der forensischen Analyse als Grundlage für eine schnelle Wiederherstellung der Systeme nach einem Cyberangriff.

3. Wie wird das Angebot der Cyber-Ersthilfe seit deren Einrichtung nachgefragt (bitte unter Angabe der Anzahl der bearbeiteten Anfragen bzw. Fälle im Vergleich zur Zentralen Ansprechstelle Cybercrime [ZAC] aufgeschlüsselt nach relevanten Personengruppen bzw. Unternehmenskategorien)?

Zu III. 3.:

Ein direkter Vergleich ist nicht möglich, da beide Angebote unterschiedliche Zielrichtungen verfolgen. Die ZAC des LKA BW nimmt Strafanzeigen aus dem Phänomenbereich Cybercrime entgegen, veranlasst die Einleitung polizeilicher Ermittlungsverfahren und steht den Behörden und Unternehmen sowie sonstigen relevanten Institutionen beratend zur Verfügung. Dabei gewährleistet sie eine durchgehende Erreichbarkeit.

Die ebenfalls rund um die Uhr erreichbare Cyber-Ersthilfe der CSBW hat dagegen die Aufgabe, Betroffenen niederschwellig eine erste Einordnung der geschilderten Ereignisse, Verdachtsfälle oder Vorfälle zu geben und Hilfestellung zu weiteren Schritten zu leisten. Bei Verdacht von Straftaten legt sie den Betroffen auch immer nahe, die Polizei zu verständigen.

Die Eingangsstatistik der ZAC des LKA BW bewegt sich auf einem gleichbleibend hohen Niveau. Obwohl die ZAC insbesondere Behörden und Unternehmen als Ansprechstelle zur Verfügung steht, wenden sich auch immer wieder Bürgerinnen und Bürger an die ZAC. Die Statistik weist folgende Kontaktierungsdaten auf:

Jahr	Kontaktierungen gesamt	Unternehmen	Behörden	Sonstige Institutionen[1]	Bürgerinnen oder Bürger
		ZAC-Zielgruppe			
2019	1.638	802	86	89	661
2020	1.806	641	43	100	1.022
2021	1.867	642	68	118	1.039
2022	1.395	618	61	105	611
2023	1.498	604	46	79	769

[1] Unter sonstige Institutionen fallen beispielsweise Schulen oder Krankenhäuser.

Die Eingangsstatistik der Cyber-Ersthilfe weist die nachfolgenden Kontaktierungsdaten auf. Diesbezüglich ist zu beachten, dass das Jahr 2023 das erste Jahr ist, für das eine vollständige Fallerfassung bei der CSBW vorliegt. Die endgültigen Zahlen für das Jahr 2024 liegen noch nicht vor. Im Rahmen des aktuell geplanten Rollouts der in den nachfolgenden Antworten dargelegten Umsetzung eines Beratungskonzeptes für KMU zusammen mit Multiplikatoren wie den Industrie- und Handelskammern und Handwerkskammern und im Zuge des Ausbaus der Kontakte zu Kommunen, kommunalen Unternehmen und auch Einrichtungen der Hochschulen werden die Angebote der CSBW und insbesondere auch die Cyber-Ersthilfe gezielt beworben, was eine stetige Steigerung der Inanspruchnahme der Cyber-Ersthilfe erwarten lässt.

	2023	2024
Landesverwaltung in Baden-Württemberg inkl. aller nachgeordneten Bereiche sowie Unternehmen von besonderem öffentlichem Interesse	7	1
Kommunen in Baden-Württemberg (inkl. Unterer Landesbehörden)	20	2
Wirtschaftsunternehmen mit Sitz in Baden-Württemberg davon Unterrichtungen bei Dark- und Clearnet-Funden	55 (41)	28 (24)
Schulen in öffentlicher Trägerschaft, Hochschulen und Universitäten in Baden-Württemberg (inkl. IHK und HWK)	6	3
Bürgerinnen und Bürger mit Wohnsitz in Baden-Württemberg	49	12
Sonstige/Sonderfälle (Polizeidienststellen, Krankenhäuser, eingetragene Vereine)	2	2

4. Wie weit ist die konkrete Konzeption einer Vermittlungsstelle zwischen kommerziellen IT-Sicherheitsdienstleistern und von Cyberangriffen betroffenen Unternehmen (bitte unter Angabe erreichten und geplanter Meilensteine)?

5. Ist die geplante Vermittlungsstelle aus der vorherigen Frage und die Arbeit der Cyber-Ersthilfe mit dem Cybersicherheitsnetzwerk des BSI abgestimmt (falls nicht, bitte unter Angabe von Gründen)?

6. Inwieweit sind Erkenntnisse aus dem digital@bw Projekt „Cyberwehr BW" in die Konzeptionierung der Cyber-Ersthilfe beziehungsweise in die geplante Vermittlungsstelle zwischen kommerziellen IT-Sicherheitsdienstleistern und von Cyberangriffen betroffenen Unternehmen eingeflossen oder werden noch einfließen (falls dies der Fall sein sollte, bitte unter Angabe konkreter Aspekte)?

Zu III. 4. bis 6.:

Die Fragen zu III. 4 bis 6 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die Cyber-Ersthilfe ist mit verschiedenen Akteuren und Mitgliedern des Cybersicherheitsnetzwerks des BSI vernetzt. In Abhängigkeit des jeweiligen Arbeitsschwerpunktes und Bedarfes der Cyber-Ersthilfe wird ein gezielter Austausch innerhalb des Cybersicherheitsnetzwerks des BSI gesucht. Mitarbeitende der Cyber-Ersthilfe haben mehrere Schulungen bzw. Qualifizierungen zum Digitalen Ersthelfer, Vorfall-Praktiker und Vorfall-Experten absolviert. An Veranstaltungen des Cybersicherheitsnetzwerks des BSI wird regelmäßig seitens der Cyber-Ersthilfe teilgenommen. Im Rahmen der kontinuierlichen Prüfung und Evaluation des Dienstleistungsangebots der Cyber-Ersthilfe werden auch Erkenntnisse und Entwicklungen aus dem Cybersicherheitsnetzwerk des BSI aufgenommen und innerhalb der eigenen (Informations-)Produkte eingearbeitet. Bei der Erbringung der Cyber-Ersthilfe wird seit Dienstleistungsbeginn auf die vom BSI geführten Listen der qualifizierten IT-Sicherheitsdienstleister, das Melde- und Informationsportal des BSI, sowie die Kontaktstelle des Cybersicherheitsnetzwerks des BSI, verwiesen.

Das Ministerium des Inneren, für Digitalisierung und Kommunen und die CSBW haben sich bei der Schaffung von Angeboten für die Wirtschaft im Bereich der Cybersicherheit zunächst auf die Ausgestaltung des Beratungskonzeptes für KMU fokussiert. Dieses Vorgehen entspricht in hohem Maße auch den Ergebnissen einer entsprechenden Bedarfserhebung bei der Zielgruppe KMU, die im Rahmen eines wissenschaftlich begleitenden Projektes erfolgte. Das nun im Ergebnis vorliegende Beratungskonzept, welches über Multiplikatoren wie den Industrie- und Handelskammern und Handwerkskammern umgesetzt werden soll, zeichnet sich auch nach einer umfassenden Pilotierungsphase als Erfolgsmodell ab. Sobald die Vorbereitungen für einen flächendeckenden Rollout abgeschlossen sind – dazu gehört beispielsweise die Schulung der künftigen Beraterinnen und Berater – können die Ressourcen im Ministerium des Inneren, für Digitalisierung und Kommunen und bei der CSBW dazu eingesetzt werden, in Zusammenarbeit mit dem Ministerium für Wirtschaft, Arbeit und Tourismus eine Konzeption für eine Vermittlungsstelle zu erarbeiten. Dies soll unter Einbeziehung der aus der Umsetzung des Beratungskonzeptes für KMU gewonnenen Erkenntnisse und in Mitwirkung der an der Umsetzung beteiligten Partner erfolgen. Die Erkenntnisse des Cyberwehr-Projektes werden in diese Konzeption ebenfalls einfließen. Es zeichnet sich jetzt jedoch schon ab, dass es nicht nur einer Vermittlung für die Fälle der Reaktion und Detektion, also zur Vorfallsbehandlung bedarf. Vielmehr sollte die Prävention im Fokus eines solchen Netzwerkes stehen. Bis zum Abschluss eines noch formal zu projektierenden Vorhabens greifen das Ministerium des Inneren, für Digitalisierung und Kommunen und die CSBW auf die vom BSI geschaffenen Strukturen zurück und verweisen auf die mittlerweile vom BSI geschaffene Auswahl an qualifizierten Sicherheitsdienstleistenden.

Die Cyberwehr wurde im Zeitraum 2018 bis 2022 im Rahmen der Digitalisierungsstrategie digital@bw als Forschungsprojekt angelegt und zeitlich begrenzt gefördert. Das Forschungsprojekt hat wertvolle Grundlagenarbeit geleistet. Die

im Rahmen des Forschungsprojektes erzielten Ergebnisse und gewonnenen Erfahrungen wurden beim Aufbau der CSBW und bei der Konzeption und Umsetzung der Cyber-Ersthilfe genutzt. Seit dem 1. Juli 2022 besteht die Cyber-Ersthilfe und damit eine zentrale Meldestelle für Cybersicherheitsvorfälle und Verdachtsfälle, die neben der Landesverwaltung und den KMU im Land auch den Kommunen zur Verfügung steht. Von einem Cybervorfall Betroffene erhalten Unterstützung bei einer ersten Einordnung des Vorfalls oder Verdachtsfalls, und es werden weitere spezifische Anlaufstellen zur weiteren Fallbehandlung empfohlen.

IV. Cybersicherheit für Kommunen und Behörden in Baden-Württemberg

1. Wie ist die Rollen- und Kompetenzverteilung im Bereich Cybersicherheit innerhalb der Landesverwaltung ausgestaltet (bitte unter Nennung der zuständigen Stellen wie Fachabteilungen des Innenministeriums, IT-Leitstellen und Chief Information Security Officer [CISOs] der einzelnen Ressorts und untergeordneten Stellen wie BITBW und CSBW)?

Zu IV. 1.:

Die Säulen der Cybersicherheitsarchitektur in Baden-Württemberg bilden die CSBW, das LfV und das LKA BW. Hinsichtlich der Ausgestaltung der Zusammenarbeit wird auf die Antwort zur Frage I. 8. verwiesen.

Die Rollen- und Kompetenzverteilung innerhalb der Landesverwaltung und das Zusammenwirken der Rollen und Bedarfsträger ist unter anderem in Nr. 5 der VwV Informationssicherheit geregelt. Für die Sicherstellung der Informationssicherheit der zentralen informationstechnischen Infrastruktur für die Landesverwaltung ist nach Maßgabe des Gesetzes zur Errichtung der Landesoberbehörde IT Baden-Württemberg (BITBWG) die BITBW verantwortlich. Das CERT BWL ging mit Erlass des CSG von der BITBW auf die CSBW über. Die CSBW, die BITBW und die Informationssicherheitsbeauftragten der Ressorts (Ressort-CISOs) stimmen sich in einem vom Ministerium des Inneren, für Digitalisierung und Kommunen eingerichteten und koordinierten Gremium, der KG InfoSic, unter Beteiligung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI), des Rechnungshofes, des Landeszentrums für Datenverarbeitung (LZfD) und des Informationssicherheitsbeauftragten des Landtages regelmäßig zu Maßnahmen der IT- und Informationssicherheit ab, die entweder unmittelbar in den Rechenzentren umgesetzt werden oder unter Beteiligung der IT-Leitstellen im AK-IT abgestimmt werden. Für die IT-Infrastruktur der BITBW bündelt die dortige Stabsstelle Informations- und Cybersicherheit alle Themen der Informations- und Cybersicherheit und hält ein Berichtswesen vor.

Die Dienst- und Fachaufsicht über die CSBW führt das Ministerium des Inneren, für Digitalisierung und Kommunen (Abteilung 4). Zur Abstimmung finden regelmäßige ebenso wie anlassbezogene Fachaustausche zwischen Abteilung 4 des Ministeriums des Inneren, für Digitalisierung und Kommunen und der CSBW-Führung statt.

Im Fokus der Aufgaben des Cybercrime-Zentrums der Justiz, der Abteilung 5 „Cybercrime und Digitale Spuren“ des LKA BW und der in den regionalen Polizeipräsidien eingerichteten „Kriminalinspektionen 5“ steht die Bekämpfung von Straftaten und damit der Kampf gegen Cybercrime.

Das LfV, mit den Arbeitsbereichen Spionage- und Cyberabwehr, bietet langjährige Expertise sowie fachliche und methodische Kompetenz in der Aufklärung und Abwehr von nachrichtendienstlich und staatlich gesteuerten Spionage- und Cyberangriffen. Durch den Behörden- und Wirtschaftsschutz sowie der Cyberabwehr leistet das LfV seinen Beitrag zum Schutz vor Know-how-Verlust und zur Cybersicherheit bei baden-württembergischen Behörden und Unternehmen. Mit den Strukturen zur Informationssicherheit des Innenressorts findet ein stetiger und

vertrauensvoller Austausch statt. Die Dienst- und Fachaufsicht über das LfV führt das Ministerium des Inneren, für Digitalisierung und Kommunen (Abteilung 6).

2. Wie hoch ist die kommunale Nachfrage nach Unterstützungsangeboten, wie zum Beispiel Informationsberatungen, IT-Sicherheitsanalysen und Schulungen der CSBW in den letzten zwölf Monaten beziehungsweise seit der Bereitstellung des Angebots, falls der Zeitraum kürzer als zwölf Monate sein sollte?

Zu IV. 2.:

Die CSBW bietet zahlreiche Unterstützungsangebote für Kommunen, die sich guter Resonanz erfreuen. Die Nachfrage nach den konkreten Angeboten in den letzten 12 Monaten bzw. seit Bereitstellung der Angebote stellt sich wie folgt dar:

Die Schulungsangebote richten sich insbesondere an die Mitarbeitenden der Landes- und Kommunalverwaltung als Zielgruppe. Hierbei handelt es sich zum Beispiel um eine Grundlagenschulung zur Cybersicherheit. Im Jahr 2023 fand die Grundlagenschulung 24-mal mit insgesamt rund 1 500 Teilnehmenden aus den Kommunen und der Landesverwaltung statt. Im Jahr 2024 wurde die Grundlagenschulung allein im Bereich der Kommunen bereits 29-mal mit insgesamt 1 170 Teilnehmenden durchgeführt, weitere 26 Termine mit voraussichtlich 1 300 Teilnehmenden sind bereits vereinbart. Für Führungskräfte der Kommunen bietet die CSBW außerdem ein Schulungsangebot mit dem Titel „Cybersicherheit als Führungsaufgabe“ an. Diese ist nach der Grundlagenschulung die am zweithäufigsten angefragte Schulung der CSBW. Sie wurde im Jahr 2023 an insgesamt neun Terminen in der Kommunalverwaltung durchgeführt. Damit wurden insgesamt ca. 380 Personen erreicht. Für das Jahr 2024 sind bereits siebenmal Schulungen mit Kommunen terminiert, sechs haben bereits stattgefunden. Die Aufbauschulung „Präventionsmaßnahmen im eigenen Verantwortungsbereich“ wurde im Jahr 2024 bereits dreimal mit insgesamt 150 Teilnehmenden durchgeführt und es sind zwei neue Termine vereinbart.

Das zu den Schulungen eingeholte Feedback der CSBW ergibt, dass die Zufriedenheit mit den Schulungen durchweg sehr hoch ist – der Zufriedenheitsindex liegt bei 90 Prozent.

Unter Federführung des Ministeriums des Inneren, für Digitalisierung und Kommunen und der CSBW entstand in enger Zusammenarbeit mit den Kommunalen Landesverbänden, Vertreterinnen und Vertretern aus Kommunen sowie der Komm.ONE der „Stufenplan Mindestsicherheitsniveau“. Damit wird das Ziel verfolgt, das Sicherheitsniveau weiter zu steigern und die Städte, Gemeinden und Landkreise beim Einstieg in den IT-Grundschutz des BSI zu unterstützen. Kommunen können mit einer Checkliste ihr Sicherheitsniveau erfassen und über die CSBW ausführliche IT-Sicherheitsanalysen durchführen lassen. Das Angebot wurde im Jahr 2023 mit rund 50 Kommunen pilotiert, wovon 9 Kommunen eine IT-Sicherheitsanalyse durchführen ließen. Für das Jahr 2024 sind bereits 14 IT-Sicherheitsanalysen bei Kommunen abgeschlossen, in Umsetzung oder terminiert.

Die CSBW stellt über ihre jüngst gestartete Lernplattform Schulungs- und Sensibilisierungselemente wie Web-Based-Trainings, Erklärvideos, Factsheets und ein Serious Game zur Verfügung.

Die Lernplattform der CSBW hat aktuell 505 Nutzende – im kommunalen Kontext ist eine steigende Nachfrage zu verzeichnen. Einige Kommunen nutzen die Schulungs- und Sensibilisierungselemente der CBSW bereits als Schulungsmaßnahme für deren gesamte Belegschaft. Die im Rahmen der Sensibiliserungskampagne der CSBW gestarteten Aktionen wie die „Sommeraktion“ zu Cybersicherheitsthemen rund ums Reisen, Arbeiten von unterwegs und von Zuhause usw. erreichte weit mehr als 12 000 Personen der Landes- und Kommunalverwaltung. Weitere vergleichbare Aktionen wurden und werden fortlaufend umgesetzt.

Die CSBW hat Landkreise, Städte und Gemeinden sowie Unternehmen in kommunaler Trägerschaft in den letzten 12 Monaten in 46 Fällen beraten und unter-

stützt. 4 Fälle erforderten einen Einsatz des Mobile Incident Response Teams (MIRT) der CSBW zur Unterstützung vor Ort, einschließlich Unterstützung beim Krisenmanagement und der Krisenkommunikation.

Außerdem ist die Einführung von regelmäßigen Webinaren zu verschiedenen IT-Sicherheitsthemen geplant. Hierbei sollen auch Kommunen die Möglichkeit erhalten, innovative Konzepte („Best Practices“) einem breiten kommunalen Publikum vorzustellen. Mit solchen Webinaren soll es den kommunalen Informations- bzw. IT-Sicherheitsverantwortlichen ermöglicht werden, sich weiterzubilden und dabei von den Erfahrungen und dem Wissen sowohl von Personen aus anderen Kommunen als auch der CSBW-Expertinnen und -Experten zu profitieren.

3. Sieht sie Bedarfe für weitere Unterstützungsangebote an Kommunen im Kontext der Einhaltung von angemessenen Cybersicherheitsstandards, wie zum Beispiel einer Ausweitung der Unterstützungsangebote der CSBW oder einem speziellen Förderprogramm für die Informationssicherheit in Kommunen?

Zu IV. 3.:

Das Ministerium des Inneren, für Digitalisierung und Kommunen und die CSBW stehen in engem Austausch sowohl mit den Kommunalen Landesverbänden als auch mit Komm.ONE und einzelnen Kommunen. Hieraus und aufgrund der umfassenden Erkenntnisse, die die CSBW durch ihre verschiedenen Beratungsangebote für Kommunen gewonnen hat, wurde über die bereits angebotenen Unterstützungsleistungen des Landes für Kommunen hinaus insbesondere im Bereich Notfallmanagement sowie bei der Dokumentation von Informationssicherheitskonzepten und -richtlinien zusätzlicher Unterstützungsbedarf identifiziert. Sowohl bei den durchgeführten IT-Sicherheitsanalysen als auch in den zahlreichen individuellen Beratungen und Rückmeldungen hat sich gezeigt, dass Kommunen häufig Schwierigkeiten bei der Erstellung und Pflege von IT-Sicherheitsdokumentationen und der Planung und Übung von Notfallszenarien haben. Ebenso wird ein Bedarf gesehen, Musterdokumente für verschiedene IT-Sicherheitskonzepte und -richtlinien zu entwickeln und zur Verfügung zu stellen. Diese sollen den Kommunen dabei helfen, ihre Informationssicherheit systematisch und nach den neuesten Standards zu gestalten. Diese Maßnahmen sollen nicht nur die IT-Sicherheit erhöhen, sondern auch die Gemeinden, Städte und Landkreise in die Lage versetzen, eigenständig nachhaltige Sicherheitsstrategien zu entwickeln.

Eine Ausweitung der aktuellen Unterstützungsangebote wäre ebenso wie das Angebot eines Förderprogramms, welches Kommunen bei der Umsetzung von Mindeststandards unterstützt und Kommunen in dieser Hinsicht finanziell entlastet, möglich. Dies übersteigt allerdings die vorhandenen finanziellen und personellen Ressourcen und müsste daher im Rahmen des Haushaltsgesetzgebungsverfahrens vom Haushaltsgesetzgeber zusätzlich implementiert werden.

4. Warum werden statt der geplanten punktuellen Schwachstellenscans der CSBW für öffentliche Stellen keine bereits vorhandenen automatisierten Lösungen, die dauerhaft nach Schwachstellen suchen und automatisiert Maßnahmen ergreifen, angewendet?

Zu IV. 4.:

Die von Seiten der CSBW eingesetzten Lösungen sind grundsätzlich sowohl für punktuelle Schwachstellenscans als auch für dauerhafte, automatisierte Scans nutzbar und können bei Bedarf entsprechend eingesetzt werden. Häufig hängt die Entscheidung darüber, welche Methodik zum Einsatz kommt, von der Zielrichtung und der „Tiefe“ der vorzunehmenden Untersuchungen sowie von der konkreten Ausgestaltung der Infrastruktur ab. So verhindern Sicherheitsmaßnahmen etwa durch Firewall-Konfigurationen in vielen Fällen bewusst, dass automatisiert nach Schwachstellen gesucht werden kann. Eine Entscheidung, wie im jeweiligen Fall vorgegangen wird, wird jeweils im Einzelfall bei Vorbereitung der Unterstützungsleistung getroffen.

5. Inwieweit ist eine regelmäßige Teilnahme aller Bediensteten in der öffentlichen Verwaltung vom Land bis zur Kommune an Schulungen zum Thema Cybersicherheit vorgesehen?

Zu IV. 5.:

Nach Nummer 3.1 der VwV Informationssicherheit haben alle Dienststellen und Einrichtungen der Landesverwaltung die Informationssicherheit gemäß IT-Grundschutz umzusetzen. Dies bedeutet in Bezug auf Schulungen, dass alle Mitarbeitenden entsprechend ihren Aufgaben und Verantwortlichkeiten zu Informationssicherheitsthemen geschult werden sollen. Die Umsetzung durch entsprechende Schulungs- und Sensibilisierungsangebote für die Mitarbeitenden erfolgt in der Landesverwaltung einerseits dezentral und in Eigenverantwortung durch die jeweiligen Ressorts, Dienststellen und Einrichtungen. Dies umfasst beispielsweise Basisinformationen zur Informationssicherheit für neu eingestellte Mitarbeitende, aber auch gezielte fachbezogene Schulungs- und Sensibilisierungsformate für alle Mitarbeitenden. Anlassbezogen erfolgen Schulungen und Sensibilisierungsmaßnahmen bei Auftreten von akuten und klassifizierbaren Phishing-Wellen oder Betrugsversuchen und dergleichen sowohl zentral über die CSBW als auch dezentral in den Ressorts, Einrichtungen und Dienststellen. Ergänzend gestaltet die CSBW regelmäßig Schulungsangebote und Sensibilisierungsformate für die Landesverwaltung und für Kommunen. Auf die Antwort zur Frage IV. 2. wird verwiesen. Die dort dargelegten Angebote stehen gleichermaßen Kommunen wie Einrichtungen des Landes zur Verfügung.

6. Wie sieht der normative Vorgangsprozess für eine Kommunalverwaltung im Vergleich zur Landesverwaltung im Fall eines Ransomware-Vorfalls aus (bitte unter der Angabe der zuständigen unterstützenden Akteure während des jeweiligen Prozessschrittes von der Erkennung vom Malwarebefall bis zur Beseitigung dieser samt angestrebten Zeithorizont)?

Zu IV. 6.:

Im Falle eines Ransomware-Vorfalls sowohl im Bereich der Landesverwaltung als auch bei einer Kommunalverwaltung erfolgt eine Meldung sowohl an die CSBW als auch an die verantwortlichen IT-Betreiber wie die Komm.ONE oder die BITBW. Weitere erforderliche Stellen wie die ZAC des LKA BW werden eingebunden. In enger Zusammenarbeit zwischen den beteiligten Akteuren und der betroffenen Einrichtung erfolgt die weitere Behandlung des Vorfalls. Diese umfasst neben den nachfolgend dargestellten Phasen auch Unterstützungsleistungen im Bereich der Krisenbewältigung und der Krisenkommunikation.

Abstrakt kann ein Ransomware-Vorfall in die folgenden Phasen eingeteilt werden:

Phase	**Unterstützende Akteure**	
	Kommunalverwaltung	**Landesverwaltung**
1. Auftreten: Der Vorfall wird erkannt	Betroffene Stelle, ggf. Komm.ONE	Betroffene Stelle, ggf. BITBW, LZfD
2. Meldung	Komm.ONE oder CSBW/ Cyber-Ersthilfe, ZAC	CSBW, ZAC
3. Identifizierung: Betroffene System werden identifiziert	Betroffene Stelle, CSBW, ggf. Komm.ONE, ggf. externe Dienstleister, ZAC	Betroffene Stelle, CSBW, ggf. BITBW, LZfD, ggf. externe Dienstleister, ZAC
4. Eindämmung: Eine weitere Ausbreitung wird nach Möglichkeit verhindert	CSBW, ggf. Komm.ONE, ggf. externe Dienstleister	CSBW, ggf. BITBW, LZfD ggf. externe Dienstleister
5. Entfernung: Ausgrenzung des Angreifers	CSBW, ggf. Komm.ONE, ggf. externe Dienstleister	CSBW, ggf. BITBW, LZfD ggf. externe Dienstleister
6. Neu-Aufbau: Neuer Aufbau des betroffenen Netzes	Betroffene Stelle, CSBW beratend, ggf. Komm.ONE, ggf. externer Dienstleister	Betroffene Stelle, CSBW beratend, ggf. BITBW, LZfD ggf. externer Dienstleister
7. Überprüfung: Konzeptionelle und technische Überprüfung des neu aufgebauten Netzes auf Einhaltung von Standards	Betroffene Stelle, CSBW beratend, ggf. Komm.ONE, ggf. externer Dienstleister	Betroffene Stelle, CSBW beratend, ggf. BITBW, LZfD ggf. externer Dienstleister

7. Welche Rollen spielen relevante Akteure im Land wie zum Beispiel die CSBW, die BITBW und die Komm.One im Kontext von Special Operation Center (SOCs) in Baden-Württemberg (bitte unter Angabe, wo sich im Land bereits SOCs etabliert haben)?

Zu IV. 7.:

Ein Security Operations Center (SOC) hat im Kontext der Cyber- und IT-Sicherheit eine Vielzahl von Aufgaben. Diese reichen von präventiven Maßnahmen wie dem Erkennen und Schließen von Sicherheitslücken bis hin zur technischen Überwachung von komplexen IT-Infrastrukturen, um Anomalien und Bedrohungen identifizieren und darauf reagieren zu können. Gerade der technischen Überwachung der Systemlandschaften kommt daher besondere Bedeutung zu. So gilt es zunächst, die millionenhaft von den verschiedenen technischen Systemen erzeugten Protokolldaten zusammenzuführen und automatisiert zu analysieren und zu bewerten. Dies betrifft beispielsweise die Protokolldaten der sogenannten „Ak-

tiven Komponenten“, also Router und Switches, die Protokolldaten der Firewalls, der Virenscanner, der Gateways, der Spam-Filter, der Verzeichnisdienste ebenso wie Protokolldaten von Servern, Storage und Mailsystemen. Dazu werden in den Rechenzentren bei BITBW, beim Rechenzentrum der Steuerverwaltung LZfD und Komm.ONE sogenannte „Security Information and Event Management-Systeme“ aufgebaut oder eingesetzt. Die dazu initiierten Projekte werden konsequent fortgesetzt. Flankiert werden können diese Maßnahmen durch den zusätzlichen Einsatz von Intrusion Detection Systemen (IDS), Intrusion Prevention Systems (IPS) oder ähnlichen Tools. Die unmittelbare Überwachung und Auswertung dieser auf diese Weise zusammengetragenen Datensätze erfolgt dezentral in den Rechenzentren der BITBW, des LZfD und der Komm.ONE, wo entsprechende SOC-Strukturen aufgebaut und etabliert wurden, die stetig lageangepasst weiterentwickelt werden.

Lässt die Analyse der Daten Anomalien erkennen, werden diese in einem ersten Schritt von den SOC-Teams unter Hinzuziehung des jeweiligen Fachbereichs der Rechenzentren bewertet. Dazu wird im Bedarfsfall auch die CSBW hinzugezogen, um relevante länderübergreifende Lageinformationen in die Analyse einzubringen und um Maßnahmen zur Vorbeugung oder Eindämmung von Vorfällen auch rechenzentrums- oder gar länderübergreifend koordinieren zu können. Zentrale SOC-Dienstleistungen im präventiven Bereich erbringt die CSBW für alle Rechenzentren der Landesverwaltung. So unterstützt die CSBW beispielsweise das jeweilige Schwachstellenmanagement der Rechenzentren durch schnellen und unmittelbaren fachlichen Austausch zu bekanntwerdenden Schwachstellen in Systemen. Darüber hinaus sammelt die CSBW aus ihrer Tätigkeit im Bereich „Threat Intelligence“, also aus der Überwachung einschlägiger Quellen unter anderem im Internet und im Darknet und aus ihren bundesweiten und internationalen Kontakten, wichtige Informationen über aktuelle Bedrohungen und Angriffsmethoden und sogenannte „Indicators of Compromise (IoC)“ und gibt diese in Echtzeit an die SOCs der Rechenzentren weiter, um vor Ort Betroffenheiten prüfen und vorbeugende Maßnahmen ergreifen zu können.

8. Wie bewertet sie einen einfach zugänglichen Cybersicherheitsnotfallfond für akute Cybersicherheitsvorfälle (bitte differenziert nach Zugriff für Landeseinrichtungen, Kommunen und Unternehmen im Land, bei Vorhandensein eines solchen bitte unter Nennung der zugangsberechtigten Akteure, Zugangsvoraussetzungen und der zur Verfügung stehenden Summe)?

Zu IV. 8.:

Cybersicherheitsnotfallfonds können wichtige finanzielle Absicherungen im Falle von Cyberangriffen auf öffentliche und private Stellen darstellen. Gleichwohl ist anzumerken, dass die Inanspruchnahme von Notfallfonds regelmäßig an die Erfüllung von Bedingungen zu knüpfen sein wird. So sehen etwa die Überlegungen zum Cybersicherheitsnotfallfonds der Europäischen Union vor, dass von Cyberangriffen betroffene Stellen dann berechtigt sind, auf den Fonds zuzugreifen, wenn alle vorgeschriebenen Cybersicherheitsmaßnahmen ordungsgemäß umgesetzt wurden. Die Erfahrungen der Expertinnen und Experten der CSBW zeigen hingegen immer wieder, dass Angriffe regelmäßig dann erfolgreich sind, wenn vorgeschriebene Maßnahmen nicht umgesetzt wurden.

Bei bedingungslosen Cybersicherheitsnotfallfonds besteht hingegen die Gefahr, dass sich öffentliche und private Stellen in einem falschen Gefühl der Sicherheit wähnen und möglicherweise auf bedeutsame präventive Absicherungsmaßnahmen verzichten. Dabei verfolgt ein Notfallfonds regelmäßig lediglich die Unterstützung mit finanziellen Mitteln, kann jedoch eine Wiederherstellung von Daten, etwa aufgrund fehlendem Backup-Management, nicht herbeiführen.

Nach alledem sieht die Landesregierung vielmehr die bereits gegenwärtige Unterstützung der genannten Stellen zur Umsetzung des Standes der Technik bei der Absicherung der IT als auch Prozesse für Cybernotfälle (Business Continuity Management) als geboten an.

9. Besitzen die CSBW, BITBW oder andere relevante Akteure im Land Notfallkompetenzen, die es ohne weitere Abstimmungsprozesse erlauben, unmittelbar Gegenmaßnahmen im Schadensfall zu ergreifen?

Zu IV. 9.:

Die kompetenzrechtlichen Ermächtigungen der CSBW ergeben sich insbesondere aus § 5 und § 6 CSG, die es der CSBW erlauben, die erforderlichen Anordnungen und Maßnahmen zum Schutz von öffentlichen Stellen und des Landesverwaltungsnetzes zu treffen, und bei herausgehobenen Fällen auf Ersuchen der betroffenen Stelle die Maßnahmen zu treffen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind. Ein Beispiel für eine sich daraus ableitende Maßnahme könnte die Herbeiführung einer Netztrennung einer von einem Cyberangriff betroffenen Organisationseinheit sein. Allerdings können im Rahmen der Umsetzung einer solchen Maßnahme im Einzelfall auch weitere Abstimmungen notwendig werden, wenn beispielsweise durch eine durchzuführende Netzabtrennung Dritte betroffen sind. Solche Abstimmungen kann die CSBW im Rahmen der Vorfallsunterstützung schnell und zielführend vornehmen.

Die gesetzlichen Grundlagen für die Umsetzung entsprechender Gegenmaßnahmen im Bereich der BITBW und des von ihr verantworteten Landesverwaltungsnetzes leiten sich insbesondere aus der im BITBWG normierten Verantwortung der BITBW ab. Die BITBW als zentrale IT-Dienstleisterin des Landes betreibt ein Notfallmanagement und hält Notfall- und Sofortmaßnahmenpläne vor. Im Rahmen dieses Notfallmanagements wurden geschäftskritische Verfahren identifiziert und bewertet, um zielgerichtet die weiteren Maßnahmen ableiten zu können. Im Falle eines Notfalls werden diese Maßnahmenpläne aktiviert. Bei einem unmittelbar bevorstehenden erheblichen Schadensereignis kann die BITBW selbständig und ohne frühzeitige vorherige Abstimmung mit der betroffenen Einrichtung Maßnahmen ergreifen. Dies ist beispielsweise die Abschaltung eines kompromitierten IT-Verfahrens sowie die Entscheidung darüber, ob Netztrennungen vorgenommen werden müssen. Bei erheblichen, aber nicht unmittelbar bevorstehenden Schadensereignissen finden unter Einbeziehung des Beauftragten der Landesregierung für Informationstechnologie (Chief Information Officer – CIO) und des Ministeriums des Inneren, für Digitalisierung und Kommunen entsprechende Abstimmungen mit der betroffenen Einrichtung statt.

10. Wie wird aktuell eine 24-Stunden-Notfallhandlungsfähigkeit bei Notfallverantwortlichen in öffentlichen Stellen sichergestellt (bitte unter Nennung eines exemplarischen Umsetzungskonzepts)?

Zu IV. 10.:

Die 24-Stunden-Erreichbarkeit der CSBW ist über die Cyber-Ersthilfe sichergestellt. Innerhalb der CSBW sind entsprechende Notfallprozesse vorgesehen, die sowohl die entsprechende Verständigung und Alarmierung eigenen Personals als auch die Verständigung und Alarmierung dafür eingerichteter Notfallkontakte in öffentlichen Stellen und Rechenzentren wie der BITBW und der Komm.ONE beinhalten. Bei der BITBW ist eine Notfall-Rufbereitschaft mit einem regelmäßig wechselnden Notfallmanager der Dienststelle implementiert. Dieser kann bei akutem Handlungsbedarf einen Notfall ausrufen, die Lage mit Hilfe einer besonderen Aufbau- und Ablauforganisation bewältigen und entsprechend notwendiges Personal in den Dienst berufen.

Die Komm.ONE hat im März 2024 für das dortige Cyber Security Incident Response Team (CSIRT) eine Dauerrufbereitschaft eingerichtet. Darüber sind jederzeit Expertinnen und Experten erreichbar, die bei sicherheitskritischen Situationen unterstützen können. Des Weiteren hat die Komm.ONE in vielen technischen Bereichen zusätzliche Dauerrufbereitschaften. Somit sind auch technische Reaktionen rasch möglich.

Sollte es durch einen IT-Notfall zu relevanten Einschränkungen der Handlungs- und Entscheidungsfähigkeit von Landesregierung oder Landesverwaltung kommen oder der IT-Notfall aus anderen Gründen krisenhafte Auswirkungen haben, greifen parallel zum IT-Notfallmanagement die Meldewege- und Reaktionswege des Krisenmanagements der Landesverwaltung. Hierzu zählt insbesondere die situationsgerechte Aktivierung der Verwaltungsstäbe beziehungsweise bei ressortübergreifenden Lagen des Interministeriellen Verwaltungsstabes. Erst im vergangenen Jahr übte die Landesverwaltung im Rahmen der bund-, länder- und ressortübergreifenden Krisenmanagement-Übung LÜKEX 23 erfolgreich die Bewältigung eines Cyberangriffs auf die Landesverwaltung.

Neben der rund um die Uhr gewährleisteten Erreichbarkeit der Polizei ist auch das LfV durch einen allgemeinen Bereitschaftsdienst zu jedem Zeitpunkt erreichbar und handlungsfähig. Soweit es im Rahmen von Lageverschärfungen erforderlich ist, richtet die Cyberabwehr des LfV temporär einen eigenen Bereitschaftsdienst ein.

Strobl

Minister des Inneren,
für Digitalisierung und Kommunen

Anlage 1_17_6765 zur Antwort auf die Frage II. 4.

Nr.	Strategieziel (konkrete Maßnahmen)	Messgröße	Verantwortung (nach Ressorts)	Zeitliche Dimension	Realisierungswahrscheinlichkeit
1.	Vernetzung mit jährlich über 500 Teilnehmenden (u. a. Cybersicherheitsforum)	500	IM	fortlaufend	realisiert
2.	Ermöglichung einer Information Security Management System (ISMS)-Dokumentation in zentralem Tool	1	IM	fortlaufendes Angebot	realisiert
3.	Mindestens 6 Untersuchungen (Schwachstellen-Scans) durch CSBW anbieten	6	IM	fortlaufendes Angebot	realisiert
4.	CSBW baut Plattform zum Austausch von Indicators of Compromise	1	IM	begonnen	hoch
5.	Erstellung von Notfallkonzepten für alle zentralen, landesweiten Systeme und Fachverfahren	1	IM	begonnen	hoch
6.	Erlass Cybersicherheitsverordnung	1	IM (im Einvernehmen mit IT-Rat)	begonnen, voraussichtlicher Abschluss 2024/2025	hoch
7.	Prüfung, inwieweit Security by Design und Einsatz von Produkten mit Sicherheitsgütesiegeln stärker im Rahmen der Beschaffung und der IT-Vorhaben berücksichtigt werden können (u. a. VwV IT-Standards, Überarbeitung		WM	begonnen, voraussichtlicher Abschluss der VwV Beschaffung 2024/2025	hoch

	VwV Beschaffung)				
8.	Neue Beschäftigte für CSBW		IM	bis 2026	realisiert
9.	Neue Beschäftigte für LfV		IM	bis 2026	abhängig von der Entscheidung des Haushaltsgesetz-gebers
10.	Neue Beschäftigte für Polizei		IM	bis 2026	abhängig von der Entscheidung des Haushaltsgesetz-gebers
11.	Neue Beschäftigte für Justiz		JuM	bis 2026	realisiert
12.	Lagebilder durch CSBW	50	IM	fortlaufen-des Ange-bot	realisiert
13.	Bedarfsorientierte Beratungen im Bereich der Ab-wehr von Spiona-ge und Sabotage		IM	fortlaufen-des Ange-bot	realisiert
14.	Bedarfsorientierte Hilfestellung für Selbständige und KMU (u. a. Cyber-Ersthilfe)		IM	fortlaufen-des Ange-bot	hoch
15.	zumindest 15 IT-Dienstleister pro Jahr neu in das Netzwerk		IM	s. Antwort auf die Frage III. 4. – 6.	
16.	Unterstützung bei der Erstellung von Notfallvorsorge-konzepten und Notfallbehand-lungsplänen		IM	begonnen	hoch
17.	Cybersicherheit in Konzeptionen und Maßnahmen im Bereich der Aus- und Fortbildung der Lehrkräfte durch das Zentrum für Schulqualität und Lehrerbildung Baden-Württemberg (ZSL) weiterent-wickeln und Ange-bote intensivieren (u. a. Angebot PC		KM	begonnen	hoch

	und Internet – Sicherheitsstrategien und -lösungen für mich – fächer- und schulartübergreifend für alle Lehrkräfte; "Networking Academy Programs" – für berufliche Schulen und Lehrkräfte)				
18.	Verbesserung über www.fortbildung-bw.de		WM	fortlaufend	hoch
19.	Angebot von Fortbildungen für mindestens 15.000 Bedienstete (u. a. Lernplattform der CSBW)	15.000	IM	fortlaufendes Angebot	hoch
20.	Konkrete Sensibilisierungsmaßnahmen (u. a. führt das MLR laufend Sensibilisierungsmaßnahmen zu Informationssicherheit, Datenschutz und Notfallmanagement durch. Im zweijährigen Turnus findet eine Pflichtschulung aller Mitarbeitenden statt)		IM, MLR	fortlaufendes Angebot	hoch
21.	Angebot von berufsbegleitenden Studienplätzen	4	IM	fortlaufendes Angebot	realisiert
22.	Jährlich 60 Fachkräfte vertieft fortbilden	60	IM	fortlaufendes Angebot	realisiert
23.	Stärkung bereits sichtbarer Standorte		MWK	begonnen	hoch
24.	Förderung der anwendungsorientierten, wirtschaftsnahen Forschung und Entwicklung sowie des wechselseitigen Wis-		MWK, WM	fortlaufend	realisiert

	sens- und Technologietransfers zwischen Wissenschaft und Wirtschaft stärken (s. Antwort auf die Frage I. 3.)				
25.	Förderung von mindestens einem Start-up-BW-Accelerator mit Cybersicherheit (Das WM fördert seit dem Jahr 2023 den CyberLab High Potential IT Accelerator in Karlsruhe als IT-Accelerator zur Unterstützung von IT-Start-ups mit Fokus KI, IT-Security und Smart Production.)		WM	fortlaufend	realisiert
26.	Anzahl der Kooperationsvereinbarungen erhöhen		IM	fortlaufend	realisiert
27.	bestehende Kooperationen überprüfen/ggf. anpassen		IM	fortlaufend	realisiert
28.	Austausch von jährlich mindestens 50 Lagebildern innerhalb der Kooperationen	50	IM	fortlaufend	realisiert
29.	jährlich mindestens drei Hospitationen von Beschäftigten bei Kooperationspartnern	3	IM	noch nicht begonnen	mittel
30.	jährlich mindestens drei Hospitationen von Kooperationspartnern bei Landesverwaltung	3	IM	noch nicht begonnen	mittel