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

17. Wahlperiode Eingang: 8.5.2024

Große Anfrage

der Fraktion GRÜNE

Cybersicherheit in Baden-Württemberg

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)?

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 vom Malwarebefall bis zur Beseitigung dieser samt angestrebten 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 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)?

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.