Landtag von Baden-Württemberg **Drucksache 17 / 8665**

17. Wahlperiode **8.4.2025**

Antrag

der Abg. Sascha Binder und Jonas Hoffmann u. a. SPD

und

Stellungnahme

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

Cybersicherheit und Investitionsbedarfe in Baden-Württemberg

Antrag

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. wie sie die aktuelle Cybersicherheitslage in Baden-Württemberg bewertet, insbesondere vor dem Hintergrund der Gefahren hybrider Kriegsführung und Desinformation und im Hinblick auf relevante Produktions- und Versorgungsprozesse, kritische Infrastrukturen wie die Sicherheitsbehörden und das Gesundheits- und Pflegewesen sowie die Wirtschaft;

2. wie sie die personelle und finanzielle Ausstattung der Cybersicherheitsagentur Baden-Württemberg (CSBW) bewertet und ob Erweiterungen geplant sind, auch mit Blick auf eine resiliente Gestaltung der CSBW;

3. welche Maßnahmen bereits durchgeführt werden und welche die Landesregierung plant, um die Resilienz von Unternehmen und insbesondere kleinen und mittleren Unternehmen (KMU) sowie staatlichen Einrichtungen auf kommunaler Ebene in Baden-Württemberg gegenüber Cyberangriffen zu stärken, insbesondere mit Blick auf die Ermöglichung des Einsatzes des Computer Emergency Response Teams (CERT) in der Cybersicherheitsagentur;

4. inwiefern sie Investitionen in Forschung und Entwicklung im Bereich Cybersicherheit fördert oder zu fördern plant, insbesondere an Hochschulen und Forschungseinrichtungen im Land;

5. welche Möglichkeiten der Aus- und Weiterbildung von Fachkräften im Bereich Cybersicherheit in Baden-Württemberg bestehen und welche Maßnahmen die Landesregierung plant, um diese zu verbessern;

6. wie die Landesregierung die Zusammenarbeit zwischen Behörden, Wirtschaft und Forschung im Bereich Cybersicherheit in Baden-Württemberg bewertet und welche Verbesserungsmöglichkeiten sie sieht;

Eingegangen: 8.4.2025 / Ausgegeben: 9.5.2025

7. welche Maßnahmen die Landesregierung plant, um das Bewusstsein für Cybersicherheit in der Bevölkerung, in Unternehmen und den Behörden sowie der öffentlichen Verwaltung, insbesondere den Kommunen, zu stärken;

8. welchen Umsetzungsstand die Richtlinie (EU) 2022/2555 des europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) und die Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Cyberresilienz-Verordnung) sowie die Cybersicherheitsstrategie Baden-Württemberg – Perspektive 2026 haben und wie sie die weitere Umsetzung zur Anpassung der Cybersicherheitsstruktur in Baden-Württemberg an diese Anforderungen plant;

9. welche Investitionen in die technische Infrastruktur zur Abwehr von Cyberangriffen notwendig sind;

10. welche Meldepflichten für Cybersicherheitsvorfälle, insbesondere für KMU, bestehen und inwiefern die Landesregierung eine Ausweitung plant oder für sinnvoll erachtet;

11. ob es einen landesweiten Cybersicherheitsnotfallplan gibt und falls nein, wie sie die Notwendigkeit bewertet, einen landesweiten Cybersicherheitsnotfallplan zu entwickeln, um im Krisenfall koordiniert reagieren zu können;

12. welche Möglichkeiten sie sieht, um die grenzüberschreitende Zusammenarbeit im Bereich Cybersicherheit, insbesondere mit den Nachbarländern und auf EU-Ebene, zu intensivieren;

13. wie die Landesregierung die flächendeckende Wartung der Cybersicherheitsinfrastruktur sicherstellt.

8.4.2025

Binder, Hoffmann, Ranger, Dr. Weirauch, Weber SPD

Begründung

Mit Blick auf die Digitalisierung der Wirtschaft, unserer Sicherheitsbehörden, der kritischen Infrastruktur sowie des Alltags der Menschen stellt sich die Frage, inwieweit das Land Baden-Württemberg auf die damit zusammenhängenden Risiken durch Cyberangriffe vorbereitet ist, welche Maßnahmen die Landesregierung insbesondere zur Umsetzung der Richtlinie (EU) 2022/2555 des europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) ergriffen hat und welche Investitionsbedarfe künftig bestehen. Der Antrag dient der Klärung dieser Fragen.

Stellungnahme

Mit Schreiben vom 2. Mai 2025 Nr. IM4-0141.5-655/3/2 nimmt das Ministerium des Inneren, für Digitalisierung und Kommunen im Einvernehmen mit dem Ministerium für Finanzen, dem Ministerium für Wissenschaft, Forschung und Kunst, dem Ministerium für Wirtschaft, Arbeit und Tourismus und dem Ministerium für Soziales, Gesundheit und Integration zu dem Antrag wie folgt Stellung:

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. wie sie die aktuelle Cybersicherheitslage in Baden-Württemberg bewertet, insbesondere vor dem Hintergrund der Gefahren hybrider Kriegsführung und Desinformation und im Hinblick auf relevante Produktions- und Versorgungsprozesse, kritische Infrastrukturen wie die Sicherheitsbehörden und das Gesundheits- und Pflegewesen sowie die Wirtschaft;

Zu 1.:

Die abstrakte Bedrohungslage im Cyberraum für Einrichtungen der Kritischen Infrastruktur (KRITIS), staatliche Stellen, Forschungseinrichtungen und Unternehmen in Baden-Württemberg ist anhaltend hoch und wird durch die zunehmende Gefahr hybrider Kriegsführung und Desinformation zusätzlich belastet.

Die staatlichen Stellen im Land, davon umfasst sind auch die Sicherheitsbehörden, müssen verstärkt mit Angriffen auf ihre IT-Infrastrukturen rechnen, was zu einer erhöhten Anforderung an umzusetzende Cybersicherheitsmaßnahmen führt. Die abstrakte Bedrohungslage kann sowohl mögliche Handlungen krimineller Organisationen als auch potenziell staatlich motivierte Angriffe umfassen, die versuchen, Lücken in Sicherheitsarchitekturen auszunutzen. Regelmäßig dürfte es sich dabei um Attacken handeln, die großräumig, breit gestreut und automatisiert durchgeführt werden.

Aus dem Bereich des Landesamts für Verfassungsschutz (LfV) ist bekannt, dass fremde Nachrichtendienste im Bereich der Cyberangriffe seit vielen Jahren sehr aktiv sind. Hervorzuheben sind in diesem Zusammenhang die Nachrichtendienste der Russischen Föderation, der Volksrepublik China, der Islamischen Republik Iran sowie Nordkorea. Durchgeführt werden solche Cyberangriffe überwiegend von sogenannten APT-Gruppierungen („Advanced Persistent Threat“; übersetzt: fortgeschrittene, andauernde Bedrohung), die von den jeweiligen Staaten gesteuert oder zumindest maßgeblich beeinflusst werden. APT-Angriffe erfordern einen hohen personellen und finanziellen Ressourceneinsatz, zeichnen sich durch ausgeprägte technisch-methodische Fähigkeiten aus und sind in ihrem Entstehen nur schwer zu entdecken.

Nach einer Studie des Branchenverbandes Bitkom e. V. betrug die Schadenssumme für die deutsche Wirtschaft im Jahr 2024 durch digitale und analoge Angriffe 267 Milliarden Euro, davon alleine 179 Milliarden Euro durch Cybercrime. Dies entspricht einer Steigerung beim Gesamtschaden um rund 29 Prozent und bei Schäden durch Cybercrime um rund 21 Prozent gegenüber dem Vorjahr.

In einer ebenfalls vom Branchenverband Bitkom e. V. durchgeführten Studie „Wirtschaftsschutz 2024“ berichtet eine deutliche Mehrheit der befragten Unternehmen von einer Zunahme von Cyberangriffen auf das eigene Unternehmen. Auch kleine und mittlere Unternehmen (KMU) werden immer häufiger Ziel von Cyberattacken. Dabei handelt es sich oftmals nicht um zielgerichtete Attacken auf einzelne Unternehmen, sondern um großflächige und automatisiert durchgeführte Angriffe. Trotz der zunehmenden Betroffenheit sind gerade KMU oftmals nicht adäquat gegen Cyberangriffe geschützt, weil es ihnen an qualifiziertem Personal und Fachkenntnis fehlt, um das eigene Expositionsrisiko einzuschätzen und eine adäquate Cybersicherheitsarchitektur aufzubauen. Auf die Stellungnahme zu Ziffer 3 wird hingewiesen.

Auch die Cybersicherheitslage im Gesundheitswesen beurteilt sich, analog der allgemeinen Lageentwicklung im Cyberraum, zunehmend angespannt. Angesichts der fortschreitenden Digitalisierung steigen die Risiken von Cyberangriffen, die die Verfügbarkeit und Sicherheit von IT-Systemen gefährden können. Der Bundesgesetzgeber hat die Erforderlichkeit der Erhöhung der Cybersicherheit in der Gesundheitsversorgung erkannt. Das bedeutet, dass Einrichtungen des Gesundheitswesens organisatorische und technische Maßnahmen ergreifen müssen, um die Resilienz ihrer Informationssysteme zu verbessern und entsprechende Risiken zu reduzieren. Gesetzliche Vorgaben wie § 391 Sozialgesetzbuch Fünftes Buch (SGB V) und § 8a des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) erfordern von Krankenhäusern, dass sie Maßnahmen zur IT-Sicherheit treffen, um die Funktionsfähigkeit und den Schutz von Patientendaten zu gewährleisten. Der Branchenspezifische Sicherheitsstandard (B3S Krankenhaus) hilft dabei, relevante Risiken zu identifizieren und zu minimieren. Ein weiteres Beispiel sind die neuen IT-Sicherheitsvorgaben für die vertragsärztliche Versorgung durch das Digitalgesetz 2024. Diese sollen die IT-Sicherheit stärken und das Risiko von Datenverlust und Betriebsunterbrechungen verringern.

Der Fachtag des Landeskompetenzzentrums Pflege & Digitalisierung BW verdeutlichte die Notwendigkeit, Datensicherheit auch in der Pflege zu gewährleisten, ohne die Benutzerfreundlichkeit zu beeinträchtigen. Dabei wurde auch auf die Bedeutung von Security-Awareness hingewiesen, um Vorfälle zu verhindern und deren Auswirkungen zu minimieren.

Bezüglich der konkreten Cybersicherheitslage kritischer Infrastrukturen wird darauf hingewiesen, dass nach § 8b Absatz 1 des BSI-Gesetzes das Bundesamt für Sicherheit in der Informationstechnik (BSI) die zentrale Meldestelle für diese Stellen ist. Auch hat das BSI die Aufgabe, die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik in diesem Zusammenhang wesentlichen Informationen zu sammeln und auszuwerten. Eine Auswertung ist dem Bericht „Die Lage der IT-Sicherheit in Deutschland 2024“ des BSI zu entnehmen.

2. wie sie die personelle und finanzielle Ausstattung der Cybersicherheitsagentur Baden-Württemberg (CSBW) bewertet und ob Erweiterungen geplant sind, auch mit Blick auf eine resiliente Gestaltung der CSBW;

Zu 2.:

Der Cybersicherheitsagentur Baden-Württemberg (CSBW) stehen im aktuellen Doppelhaushalt für das Jahr 2025 8 466 600 Euro zur Verfügung. Davon entfallen 6 289 500 Euro auf Personalmittel und 2 177 100 Euro auf Sachmittel. Von den der CSBW zustehenden 88,5 Stellen sind 73 Stellen besetzt, für sechs weitere Stellen laufen aktuell Stellenbesetzungsverfahren. Die aktuelle Lage am Arbeitsmarkt und die daraus resultierende Bewerbersituation ist allgemein für alle Behörden, so auch für die CSBW, eine große Herausforderung. Mit dem bestehenden Personalbestand können die gesetzlich definierten Aufgaben, in deren Fokus Einrichtungen des Landes und Kommunen stehen, erfüllt werden. Die Erforderlichkeit einer Erweiterung des Aufgabenspektrums wird entlang aktueller Lageentwicklungen stetig geprüft. Eine solche Erweiterung wäre jedoch nur mit der weiteren Ausstattung von finanziellen Ressourcen möglich. Die Entscheidung hierüber obliegt dabei dem Haushaltsgesetzgeber.

Generell ist in allen Bereichen der CSBW eine hohe und stetig steigende Arbeitslast zu verzeichnen, die auch in absehbarer Zeit nicht abnehmen wird. Durch die fortschreitende Digitalisierung ebenso wie durch neue Vorgaben im Bereich der Cybersicherheit beispielsweise durch die Umsetzung der NIS-2-Richtlinie (Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union) kommen weitere Aufgaben auf die CSBW zu. Auch zeichnet sich ab, dass mit den aktuell diskutierten Fragestellungen rund um Sicherheit und Verteidigung und den daraus erwachsenden Herausforderungen gerade auch im Bereich der Cybersicherheit zusätzliche Unterstützungsleistungen zu erbringen sind, um Staat, Wirtschaft und Gesellschaft noch resilienter aufzustellen. Um die CSBW in einem sich sehr dynamisch entwickelnden Umfeld entsprechend zukunftsfähig aufzustellen und damit die Resilienz der Adressaten durch die Leistungen der CSBW

dauerhaft weiter zu stärken, sind die erforderlichen finanziellen und personellen Ressourcen der CSBW im Rahmen künftiger Haushaltsberatungen zu diskutieren. Hierbei gilt es zu berücksichtigen, dass weitere Investitionen in die Prävention Risiken im Bereich der Cybersicherheit verringern und damit unkalkulierbare Aufwände und Kosten durch verhinderte Cyberangriffe und Sicherheitsvorfälle vermieden werden. Über diese Bedarfe ist im Rahmen des Planaufstellungsverfahrens vom Haushaltsgesetzgeber, vorrangig durch Mittelumschichtungen, zu entscheiden.

3. welche Maßnahmen bereits durchgeführt werden und welche die Landesregierung plant, um die Resilienz von Unternehmen und insbesondere kleinen und mittleren Unternehmen (KMU) sowie staatlichen Einrichtungen auf kommunaler Ebene in Baden-Württemberg gegenüber Cyberangriffen zu stärken, insbesondere mit Blick auf die Ermöglichung des Einsatzes des Computer Emergency Response Teams (CERT) in der Cybersicherheitsagentur;

Zu 3.:

Die CSBW unterstützt im Rahmen der vorhandenen Ressourcen mit konkreten Angeboten in den Bereichen Prävention, Detektion und Reaktion. Für öffentliche Einrichtungen, Unternehmen (insbesondere kleine und mittlere Unternehmen [KMU]) und Bürgerinnen und Bürger gibt es niederschwellige Beratungsangebote, wie die Cyber-Ersthilfe bei Cybersicherheitsvorfällen oder -verdachtsfällen. Unternehmen können zudem über die Webseite der CSBW auf kostenlose Präventionsmaterialien zugreifen und bei Bedarf Warnmeldungen des Warn- und Informationsdienstes der CSBW abonnieren.

Weiter analysiert das Computer Emergency Response Team (CERT BWL) der CSBW kontinuierlich Sicherheitslücken und Angriffsmuster, bewertet die Cybersicherheitslage und gibt konkrete, präventive Handlungsempfehlungen.

Im Bereich der Detektion und Reaktion unterstützt die CSBW öffentliche Stellen und kommunale Einrichtungen mit gezielten Warnmeldungen, Lageberichten und einer operativen Unterstützung bei Cyberangriffen. Ein Mobile Incident Response Team (MIRT) unterstützt, falls notwendig, vor Ort bei der forensischen Analyse und gibt Hilfestellungen für die Wiederherstellung der Systeme nach einem Angriff. Institutionen, auch Unternehmen, werden von der CSBW direkt gewarnt, sobald sie aus ihrem Cyber-Monitoring Hinweise auf erfolgte oder erfolgende Angriffe erhält.

Zentraler Bestandteil der Präventionsarbeit der CSBW ist zudem die Schulung und Sensibilisierung von Mitarbeitenden. Dazu bietet die CSBW u. a. eine Lernplattform, Web-Based-Trainings, Fachfortbildungen sowie Leitfäden und Sensibilisierungsmaterialien an. Außerdem können öffentliche Stellen auf speziell angepasste Vorlagen für ein Informationssicherheits-Management-System (ISMS) zugreifen, die ihnen helfen, ihre Sicherheitsmaßnahmen effektiv umzusetzen. Zusätzlich bietet die CSBW mit dem ‚Stufenplan Mindestsicherheitsniveau' für Kommunen einen strukturierten Einstieg in die Umsetzung der Standards des BSI (BSI-Grundschutz), beginnend mit einer Checkliste zur Einschätzung des aktuellen Sicherheitsniveaus und gefolgt von individuellen Handlungsempfehlungen zur Verbesserung der IT-Sicherheit.

Für Unternehmen aus allen Branchen existiert in Baden-Württemberg ein starkes Cybersicherheits-Ökosystem, das Informationen, Beratung sowie professionelle Unterstützung auf dem Gebiet der Cybersicherheit bietet. Dazu zählen zahlreiche spezialisierte Cybersicherheitsunternehmen, Kammern und Verbände mit Beratungs- und Informationsangeboten, Forschungseinrichtungen, die Sicherheitsbehörden mit ihren Präventionsangeboten sowie verschiedene regionale Netzwerke, in denen sich Anbieter- und Anwenderunternehmen gemeinsam mit weiteren Akteuren engagieren.

Auch wenn das Thema Cybersicherheit zuallererst in der Verantwortung jedes einzelnen Unternehmens liegt, unterstützt die Landesregierung die baden-württembergische Wirtschaft im Rahmen der zur Verfügung stehenden Ressourcen dabei, sich vor Cyberangriffen zu schützen. Ein besonderer Fokus liegt dabei auf Maßnahmen zur Erhöhung des Cybersicherheitsniveaus von KMU.

Für KMU stellt der vom Ministerium des Inneren, für Digitalisierung und Kommunen, der CSBW, dem Landeskriminalamt Baden-Württemberg (LKA) und der Hochschule Aalen entwickelte „CyberSicherheitsCheck für KMU“ eine wichtige Maßnahme dar, um die Resilienz im Bereich der Cybersicherheit zu stärken. Dieser einstündige Vor-Ort-Check bietet eine gezielte Beratung für die Geschäftsleitung, um über wesentliche Themen der Cybersicherheit, wie etwa die Absicherung von Netzübergängen und die Erstellung von Notfallplänen, zu sensibilisieren. Mithilfe von Beratungsmaterialien und einem speziellen Beratungstool werden dringende Handlungsbedarfe ermittelt, der aktuelle Sicherheitsstatus überprüft und konkrete Handlungsempfehlungen zur Verbesserung der Cybersicherheit gegeben. Die Beratung wird von qualifizierten Multiplikatoren der Industrie- und Handelskammern und künftig auch der Handwerkskammern, durchgeführt. Ziel ist es, die Widerstandsfähigkeit der Unternehmen gegen Cyberbedrohungen nachhaltig zu erhöhen. Eine Erweiterung auf weitere Multiplikatorengruppen ist im Rahmen der vorhandenen Ressourcen geplant.

Zum Angebot für Unternehmen im Land zählen auch die Aktivitäten des vom Ministerium für Wirtschaft, Arbeit und Tourismus geförderten Netzwerks aus insgesamt 17 regionalen, nationalen und europäischen Digital-Hubs in Baden-Württemberg. Diese bieten vielfältige Informationsveranstaltungen, Workshops, Erstberatung und Match-Making-Formate zum Thema Cybersicherheit für Unternehmen an. Mit Förderung des Ministeriums für Wirtschaft, Arbeit und Tourismus wurde darüber hinaus von der Allianz Industrie 4.0 Baden-Württemberg ein „Leitfaden zur Etablierung eines Cyber-Bündnisses“ entwickelt. Dieser gibt Unternehmen konkrete Handreichungen, wie der Zusammenschluss mehrerer Unternehmen zu einem rechtssicheren Cyber-Bündnis gelingen kann. Ziel solcher Bündnisse ist es, dass sich die beteiligten Unternehmen im Falle eines Cyberangriffs gegenseitig bei der Bewältigung des Vorfalls, beispielsweise mit zusätzlichen personellen Ressourcen, unterstützen. Zudem organisierte das Ministerium für Wirtschaft, Arbeit und Tourismus Informationsveranstaltungen zu aktuellen cybersicherheitsrelevanten Themen, wie beispielsweise der NIS-2-Richtlinie oder der Cyberresilienz-Verordnung.

KMU, die in Maßnahmen zur Verbesserung der Cybersicherheit investieren, können hierfür die Digitalisierungsprämie Plus in Anspruch nehmen, die ausdrücklich auch für die Implementierung von Cybersicherheitskonzepten und Einzelmaßnahmen beantragt werden kann. Seit Programmstart im Jahr 2020 wurden durch die Digitalisierungsprämie Plus in 4 187 Projekten Investitionen von über 26 Millionen Euro in Cybersicherheit ausgelöst.

Im Rahmen seines gesetzlichen Auftrags bearbeitet das LfV Cyberangriffe mit nachrichtendienstlichem beziehungsweise staatlichem Hintergrund. Zu den Hauptaufgaben der Cyberabwehr zählen in diesem Zusammenhang die frühzeitige Angriffserkennung, die technische Analyse der Angriffsmethodik, die Gewinnung von Erkenntnissen über mögliche Urheber sowie die Prävention und die Sensibilisierung. Die Cyberabwehr des LfV stellt eine kontinuierliche Bearbeitung sämtlicher Verdachtsfälle gemeinsam mit ihren Partnern im Verfassungsschutzverbund sicher. Hierzu stehen dem LfV eine Vielzahl gesetzlich definierter nachrichtendienstlicher Mittel zur Verfügung.

Ein weiterer Tätigkeitsschwerpunkt der Cyberabwehr des LfV liegt in der Präventionsarbeit, deren Zweck es ist, potenzielle Ziele nachrichtendienstlicher Cyberangriffe in Baden-Württemberg zu sensibilisieren und auf diese Weise die Resilienz der IT-Systeme gegen entsprechende Angriffe zu erhöhen. Die Cyberabwehr sowie der Behörden- und Wirtschaftsschutz des LfV stellen ein umfassendes Angebot an Präventionsmaßnahmen bereit und tragen so zu einem effektiven Schutz vor Spionage und Sabotage im Cyberraum bei. Dieses Präventionsangebot richtet sich

auch an Unternehmen sowie staatlichen Einrichtungen. Da KMU, unabhängig von der jeweiligen Branche, im Vergleich zu Großkonzernen häufig über vergleichsweise kleine IT-Sicherheitsabteilungen verfügen, stehen sie im besonderen Fokus der Präventionsarbeit.

Die Präventionsarbeit gliedert sich in anlassbezogene und allgemeine Beratungsformate. Liegt der konkrete Verdacht eines nachrichtendienstlich gesteuerten Cyberangriffs vor oder besteht die Gefahr, dass eine bislang unbekannte Schwachstelle in einer Software von staatlich gesteuerten oder beeinflussten Akteuren ausgenutzt werden könnte, verfasst die Cyberabwehr anlassbezogene Warnmeldungen und sensibilisiert potenziell gefährdete Stellen im Land passgenau und individuell. Im Zuge der anlassunabhängigen Beratung bietet die Cyberabwehr des LfV spezielle Vorträge bei Multiplikatoren, wie etwa Unternehmensverbänden, zum Vorgehen ausländischer Nachrichtendienste an, erstellt Handreichungen mit Hinweisen und Handlungsempfehlungen und veröffentlicht Sicherheitshinweise für IT-Fachkräfte auf der Homepage des LfV. Diese Sicherheitshinweise beschäftigen sich jeweils mit einem aktuellen Thema aus dem Bereich der Cybersicherheit und richten sich dabei auch an IT-Sicherheitsverantwortliche in Unternehmen sowie staatlichen Einrichtungen auf kommunaler Ebene. Die gesamte Präventionsarbeit der Spionage- und Cyberabwehr des LfV erfolgt dabei in enger Zusammenarbeit mit dem Behörden- und Wirtschaftsschutz des LfV, mit anderen Behörden im Verfassungsschutzverbund und mit den Sicherheitsbehörden des Landes, insbesondere dem LKA und der CSBW.

Bezüglich weiterer Maßnahmen und Angebote für staatliche Einrichtungen auf kommunaler Ebene zur Stärkung gegenüber Cyberangriffen wird ergänzend auf die Antworten zu IV. 2 der Großen Anfrage der Fraktion GRÜNE „Cybersicherheit in Baden-Württemberg“ (Drucksache 17/6765) verwiesen.

4. inwiefern sie Investitionen in Forschung und Entwicklung im Bereich Cybersicherheit fördert oder zu fördern plant, insbesondere an Hochschulen und Forschungseinrichtungen im Land;

Zu 4.:

Den Hochschulen fließen jährlich Mittel in Höhe von 6,8 Millionen Euro für die eigene Cybersicherheit der Hochschulen in Form von Stellen für Informationssicherheitsbeauftragte und Sachmittel zu. Weitere Förderaktivitäten des Ministeriums für Wissenschaft, Forschung und Kunst mit speziellem Fokus auf Forschung und Entwicklung im Bereich Cybersicherheit sind aktuell nicht geplant. Im Übrigen wird auf die Antworten zu I. 3 der Großen Anfrage der Fraktion GRÜNE „Cybersicherheit in Baden-Württemberg“ (Drucksache 17/6765) verwiesen.

5. welche Möglichkeiten der Aus- und Weiterbildung von Fachkräften im Bereich Cybersicherheit in Baden-Württemberg bestehen und welche Maßnahmen die Landesregierung plant, um diese zu verbessern;

Zu 5.:

Der Ausbildungsberuf Fachinformatiker/-in, insbesondere mit der Fachrichtung Digitale Vernetzung, bereitet angehende Fachkräfte u. a. auf die Arbeit im Bereich IT-Sicherheit vor. Auszubildende dieser Fachrichtung lernen den Umgang mit Netzwerkinfrastruktur und Schnittstellen zwischen Netzwerkkomponenten und cyber-physischen Systemen. Der Ausbildungsberuf Fachinformatiker/-in gehört zu den Top-10-Berufen in der Rangliste der Ausbildungsberufe nach Neuabschlüssen (2024 in Baden-Württemberg auf Rang 5, in Deutschland auf Rang 4). Im Jahr 2020 traten neue Ausbildungsordnungen für die dualen IT-Berufsausbildungen in Kraft, die den Fokus vermehrt auf die Themen IT-Sicherheit und Datenschutz legen.

Neben verschiedenen einschlägigen Studienangeboten an Universitäten und Hochschulen für angewandte Wissenschaften bringen die Hochschulen des Landes ihre Expertise im Bereich der Cybersicherheit auch in die wissenschaftliche Weiterbildung ein. So gibt es mehrere Kontaktstudien sowie Microcredentials zur Cybersicherheit (z. B. „Cyber Security“ der Duale Hochschule Baden-Württem-

berg (DHBW), verschiedene Module zur Cybersicherheit der Hochschule Albstadt-Sigmaringen, das Weiterbildungsangebot „Infrastruktur & Sicherheit“ der Universität Ulm oder „Informationssicherheit für Unternehmen“ der Hochschule Aalen), die alle auf der Plattform *Südwissen.de* veröffentlicht sind. Die an der Universität Freiburg neu eingerichtete Geschäftsstelle „Südwissen“ führt die Maßnahmen der Weiterbildungsoffensive aus den Jahren 2021 bis 2024/2025 ab dem Jahr 2025 fort. Diese umfasst u. a. die Plattform „Südwissen.de“ sowie ein Netz von vier Weiterbildungskoordinatoren mit Sitz in den vier Regierungsbezirken des Landes, welche das Zusammenspiel zwischen Wirtschaft und Gesellschaft sowie den Hochschulen unterstützen.

6. wie die Landesregierung die Zusammenarbeit zwischen Behörden, Wirtschaft und Forschung im Bereich Cybersicherheit in Baden-Württemberg bewertet und welche Verbesserungsmöglichkeiten sie sieht;

Zu 6.:

Die Zusammenarbeit von Behörden, Wirtschaft und Forschung ist ein wichtiger Baustein der Cybersicherheitsökonomie in Baden-Württemberg. Wirtschaftsnahe Forschung und Technologietransfer tragen sowohl zur Verbesserung der Cybersicherheit in der Wirtschaft insgesamt bei als auch zur besseren Nutzung des wirtschaftlichen Potenzials, welches Cybersicherheit im Hinblick auf Wettbewerbsvorteile und neue Wertschöpfungspotenziale bietet. Konkret fördert und stärkt das Ministerium für Wirtschaft, Arbeit und Tourismus die wirtschaftsnahe Cybersicherheitsforschung und den Technologietransfer im Wege der institutionellen Förderung sowie der Projektförderung, u. a. im Rahmen des Programms Invest BW.

Schwerpunkte im Bereich der Cybersicherheitsforschung haben u. a. das FZI Forschungszentrum Informatik in Karlsruhe mit seinem Kompetenzzentrum für IT-Sicherheit als Anlaufstelle für KMU, Hahn-Schickard in Villingen-Schwenningen, das IMS Chips – Institut für Mikroelektronik in Stuttgart, das Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung in Karlsruhe, das Fraunhofer-Institut für Arbeitswirtschaft und Organisation in Stuttgart sowie das Institut für KI-Sicherheit des Deutschen Zentrums für Luft- und Raumfahrt in Ulm etabliert.

Gerade in einem dynamischen technologischen Feld wie der Cybersicherheit ist die enge Verzahnung von Wirtschaft und Forschung ausschlaggebend, um es Unternehmen zu ermöglichen, sich nach aktuellem Stand der Technik zu schützen. Weiter wird kontinuierlich geprüft, wie die Zusammenarbeit von wirtschaftsnahen Forschungseinrichtungen und Unternehmen verbessert und weiterentwickelt werden kann.

Darüber hinaus spielt die CSBW eine zentrale Rolle in der Zusammenarbeit zwischen Forschungseinrichtungen und Behörden, indem sie als zentrale Koordinierungs- und Meldestelle fungiert und die Vernetzung aller relevanten Akteure sicherstellt. Zwischen den Hochschulen und der CSBW sind gut funktionierende Melde- und Informationswege etabliert, die eine schnelle und effiziente Kommunikation ermöglichen. Zudem bietet die CSBW sowohl präventive Beratung als auch Unterstützung bei der Reaktion auf Cyberangriffe für Hochschulen. Besonders wertvoll ist hierbei der Einsatz des MIRT im Ernstfall, um gezielt auf Sicherheitsvorfälle zu reagieren.

7. welche Maßnahmen die Landesregierung plant, um das Bewusstsein für Cybersicherheit in der Bevölkerung, in Unternehmen und den Behörden sowie der öffentlichen Verwaltung, insbesondere den Kommunen, zu stärken;

Zu 7.:

Um das Bewusstsein für Cybersicherheit in der Bevölkerung, in Unternehmen und Behörden weiter zu steigern, wird die Cybersicherheit bei allen Projekten der Digitalisierung berücksichtigt. Auch bei nicht speziell auf Cybersicherheit bezogenen Maßnahmen, wie etwa dem Kongress „Virtuelle Welten – Chancen im Metaverse erleben“, des Ministeriums für Wirtschaft, Arbeit und Tourismus am 8. Mai 2025. Dort werden u. a. Angebote zum Thema Cybersicherheit vorgestellt, um Unternehmen für Gefahren im Cyberraum zu sensibilisieren.

Im Rahmen des 7. CyberSicherheitsForums (CSF) am 27. November 2025 stehen die Themen der Cybersicherheit komplett im Fokus. Fachleute aus Wissenschaft, Verwaltung und Wirtschaft stellen aktuelle Entwicklungen dar, tauschen sich zur Lage aus und informieren über zukünftige Potenziale der Cybersicherheit. Als öffentlich zugängliche Veranstaltung hat sich das CSF in den letzten sieben Jahren zu einem Fixpunkt im Cybersicherheitskalender, auch weit über die Grenzen Baden-Württembergs hinaus entwickelt. Als hybride Veranstaltung konzipiert, werden ca. 1 000 Teilnehmende vor Ort und digital erwartet.

Die CSBW bietet zudem vielfältige Angebote zur Sensibilisierung und Bewusstseinsbildung für Themen der Cybersicherheit. Auf das unter Ziffer 3 dargestellte Angebot für die genannten Zielgruppen wird verwiesen. Insbesondere die Sensibilisierungsprodukte der CSBW wie etwa Erklärvideos, Factsheets und anlassbezogene Aktionen, beispielsweise zur Urlaubszeit, stehen auch der Bevölkerung und KMU zur Verfügung. Das gleiche gilt für die öffentlich über die Startseite der Website *cybersicherheit-bw.de* zugänglichen Warnmeldungen der CSBW.

Die Landeskriminalprävention beim LKA arbeitet derzeit an der Entwicklung von Konzepten und einem Umsetzungsplan für Präventions- und Fortbildungsangebote zu den Themen „Cybercrime“ und „Künstliche Intelligenz“ (KI). Diese Angebote richten sich sowohl an interne als auch externe Zielgruppen. Der Abschluss des Projekts sowie die Fertigstellung des Umsetzungsplans sind für den Sommer 2025 vorgesehen.

Das Angebot der beim LKA BW rund um die Uhr erreichbaren Zentralen Ansprechstelle Cybercrime (ZAC) als polizeiliche Ansprechstelle im Falle eines Cyberangriffs besteht fortlaufend. Die ZAC unterstützt bei konkreten IT-Sicherheitsvorfällen beratend, kann zeitnah polizeiliche Erstmaßnahmen veranlassen und stimmt sich anlassbezogen eng mit der CSBW ab. Die ZAC bietet darüber hinaus Präventionsveranstaltungen für institutionelle Bedarfsträger (z. B. Unternehmensverbände, Behörden) an. Dies umfasst unter anderem auch themenspezifische Vorträge zur Cybersicherheitslage und zum Handlungsfeld Awareness, insbesondere bezogen auf Fragen der Cybersecurity und Incident Response-Planung. Zudem findet im Rahmen der gesetzlichen Vorgaben ein institutionalisierter Austausch mit der Cyberabwehr des LfV statt.

Im Übrigen wird auf die Stellungnahme zu Ziffer 3 verwiesen.

8. welchen Umsetzungsstand die Richtlinie (EU) 2022/2555 des europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) und die Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Cyberresilienz-Verordnung) sowie die Cybersicherheitsstrategie Baden-Württemberg – Perspektive 2026 haben und wie sie die weitere Umsetzung zur Anpassung der Cybersicherheitsstruktur in Baden-Württemberg an diese Anforderungen plant;

Zu 8.:

In der letzten Legislaturperiode des Bundestages wurde die Umsetzung NIS-2-Richltinie im Bund nicht vollzogen. Der Gesetzentwurf der damaligen Bundesregierung sah neben den Regelungen für die Bundesverwaltung eine bundeseinheitliche Umsetzung für die wirtschaftsbezogenen Regelungen der NIS-2-Richtlinie vor.

In Baden-Württemberg erfolgt die Umsetzung der NIS-2-Richtlinie für die Landesverwaltung bzw. die öffentlichen Stellen im Land – unabhängig von den auf Bundesebene eingetretenen Verzögerungen – durch das Cybersicherheitsgesetz Baden-Württemberg und die Cybersicherheitsverordnung.

Die Cyberresilienz-Verordnung (Verordnung [EU] 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen), auch bekannt als Cyber Resilience Act (CRA), ist am 10. Dezember 2024 in Kraft getreten. Diese ist

direkt in allen EU-Mitgliedsstaaten anwendbar, sodass eine nationale Umsetzung nicht erforderlich ist. Der CRA richtet sich an Hersteller, Importeure und Händler von Produkten mit digitalen Elementen, wie z. B. Smart Home-Geräten oder Betriebssystemen. Diese müssen künftig u. a. sicherstellen, dass ihre Produkte den festgelegten Cybersicherheitsanforderungen entsprechen. Die Umsetzungszeit für den vorgenannten Adressatenkreis für Maßnahmen des CRA beträgt 36 Monate nach dem Inkrafttreten.

Mit der Cybersicherheitsstrategie und der damit einhergehenden Überarbeitung der Cybersicherheitsarchitektur sowie der Errichtung der CSBW im Jahr 2021 hat das Land frühzeitig die wesentlichen Maßnahmen ergriffen und sich damit bereits vor Inkrafttreten der NIS-2-Richtlinie zukunftsorientiert aufgestellt. Die wesentlichen Anforderungen der NIS-2-Richtlinie wurden somit bereits initiiert oder sind bereits umgesetzt. Vor diesem Hintergrund sind nur unwesentliche Anpassungen der bestehenden Cybersicherheitsarchitektur erforderlich. Diese werden in Form einer Cybersicherheitsverordnung umgesetzt.

Die Cybersicherheitsstrategie Baden-Württemberg – Perspektive 2026 – unterliegt einer kontinuierlichen Überprüfung und wird bei Bedarf fortgeschrieben. Im Übrigen und hinsichtlich des Umsetzungsstands der Cybersicherheitsstrategie Baden-Württemberg – Perspektive 2026 – wird auf die Antworten zu II. der Großen Anfrage der Fraktion GRÜNE „Cybersicherheit in Baden-Württemberg“ (Drucksache. 17/6765) verwiesen.

9. welche Investitionen in die technische Infrastruktur zur Abwehr von Cyberangriffen notwendig sind;

Zu 9.:

Die sich schnell wandelnde Bedrohungslage – etwa durch geopolitische Spannungen, neue Angriffstechniken oder Sicherheitslücken – macht eine regelmäßige Überprüfung und Anpassung der technischen Infrastruktur unumgänglich. Dabei wird gezielt an der Modernisierung, Standardisierung und Zentralisierung der Landes-IT im Rahmen der zur Verfügung stehenden Mitteln gearbeitet. Die Abwehrfähigkeit gegen Cyberangriffe erfordert jedoch kontinuierliche und vorausschauende Investitionen in die technische Infrastruktur. Über die im aktuellen Landeshaushalt bereits vorgesehenen und abgedeckten Maßnahmen hinaus, wird ein fortlaufender und zum Teil deutlich zunehmender Investitionsbedarf, insbesondere in Anbetracht aktueller Bedrohungslagen und technologischer Entwicklungen, erwartet.

Über die Bereitstellung entsprechender Ressourcen entscheidet der Haushaltsgesetzgeber. Der erhöhte Investitionsbedarf ergibt sich insbesondere durch die Zunahme KI-basierter Angriffe, welche den Einsatz von ebenfalls KI-basierten Abwehrmechanismen erfordern. Angesichts der zunehmenden Bedrohungslage gewinnen zudem Redundanzmechanismen und Maßnahmen zur Erhöhung der Ausfallsicherheit weiter an Bedeutung. Der gezielte Ausbau redundanter Strukturen ist dabei essenziell, um die Funktionsfähigkeit kritischer Prozesse auch im Falle von Störungen oder Angriffen verlässlich sicherzustellen. Auch der zunehmende Wechsel hin zu skalierbaren Cloud-Lösungen macht gezielte Investitionen in moderne Infrastruktur, sichere Migrationsprozesse und leistungsfähige Sicherheitstechnologien erforderlich. Im Zuge dessen gewinnt außerdem die Umsetzung von Zero-Trust-Prinzipien an Bedeutung, um den Zugriff auf Systeme und Daten konsequent abzusichern. Es bestehen darüber hinaus weitere Investitionsbedarfe für die Ausführung von Anwendungen in abgeschlossenen Systemen (Containerisierung). Neben den erforderlichen Investitionen in die technische Infrastruktur bedarf es weiterer Ressourcen für den Betrieb der Sicherheitsinfrastruktur. Über diese Bedarfe ist im Rahmen des Planaufstellungsverfahrens vom Haushaltsgesetzgeber, vorrangig durch Mittelumschichtungen, zu entscheiden.

Die Abwehr von möglichen Cyberangriffen und der Aufbau einer resilienten Infrastruktur ist eine Daueraufgabe. Die beschriebenen Handlungsfelder werden weiter konkretisiert und sollen in kommende Haushaltsberatungen einfließen.

10. welche Meldepflichten für Cybersicherheitsvorfälle, insbesondere für KMU, bestehen und inwiefern die Landesregierung eine Ausweitung plant oder für sinnvoll erachtet;

Zu 10.:

Die Meldepflichten für Cybersicherheitsvorfälle aus dem Bereich der Wirtschaft, etwa für KRITIS oder Unternehmen im besonderen öffentlichen Interesse, richten sich nach dem BSI-Gesetz. Die NIS-2-Richtlinie sieht eine Ausweitung auf eine Vielzahl weiterer Einrichtungen in insgesamt 18 Sektoren vor. Bezüglich des Standes der Umsetzung der NIS-2-Richtlinie wird auf die Antwort zu Ziffer 8 verwiesen. Darüber hinaus regelt das Cybersicherheitsgesetz die Meldepflicht von Cybersicherheitsvorfällen für öffentliche Stellen des Landes. Zudem ist im Falle einer Verletzung des Schutzes personenbezogener Daten nach Artikel 33 der Datenschutz-Grundverordnung eine Meldung an den Landesbeauftragten für den Datenschutz und die Informationsfreiheit erforderlich. Derzeit ist keine Ausweitung der bestehenden Meldepflichten über die jüngst durch die NIS-2-Richtlinie vorgenommene Erweiterung geplant. Auch im Bereich der Cybersicherheit gilt es, die Balance zwischen den bürokratischen Anforderungen einer Meldepflicht, die durch gesetzliche Vorgaben entstehen, und dem tatsächlichen Nutzen für die Cybersicherheit zu wahren.

11. ob es einen landesweiten Cybersicherheitsnotfallplan gibt und falls nein, wie sie die Notwendigkeit bewertet, einen landesweiten Cybersicherheitsnotfallplan zu entwickeln, um im Krisenfall koordiniert reagieren zu können;

Zu 11.:

Um auf einen krisenrelevanten Cybersicherheitsnotfall koordiniert und schnell reagieren zu können, wurden entsprechende Organisations- und Handlungsvorgaben sowie mehrstufige Prozesse im Sinne einer Notfallplanung definiert. Bei Bedarf werden die in der Landesverwaltung bewährten Strukturen der besonderen Aufbauorganisation im Krisenmanagement eingesetzt. Je nach Lage können die etablierten Stabsstrukturen gemäß der Verwaltungsvorschrift Stabsarbeit bis hin zum Interministeriellen Verwaltungsstab aufgerufen werden.

Bei einer entsprechenden Lage wird der Verwaltungsstab des Ministeriums des Inneren, für Digitalisierung und Kommunen beziehungsweise der Interministerielle Verwaltungsstab um den speziellen Verwaltungsstabsbereich „IT-Sicherheit/ Cyberangriff“ erweitert.

Zeichnet sich eine entsprechende Lage ab, beispielsweise aufgrund von Meldungen des Lagezentrums der CSBW, das mit allen relevanten Akteuren im Land und im Bund vernetzt ist, erfolgt im Ministerium des Inneren, für Digitalisierung und Kommunen anhand definierter Prozesse eine Bewertung des Vorfalls sowie gegebenenfalls die Verständigung und Einbindung weiterer Personen beziehungsweise Funktionen und Einrichtungen.

Zuletzt wurden diese Prozesse und Strukturen bis hin zur Arbeit im Interministeriellen Verwaltungsstab im Jahr 2023 im Rahmen der Bund-, Länder- und Ressortübergreifenden Krisenmanagementübung „LÜKEX 23“ unter Einbindung aller relevanten Akteure intensiv beübt. Übungs-Szenario der LÜKEX 23 war hierbei ein Cyberangriff auf das Regierungshandeln. Baden-Württemberg hat sich an der Übung breit beteiligt. Das Staatsministerium, alle elf Fachministerien, die CSBW, die IT-Dienstleisterin des Landes BITBW sowie die Regierungspräsidien Freiburg, Tübingen und Stuttgart haben – in unterschiedlicher Intensität – teilgenommen. Die Vorbereitung, Übungssteuerung und Durchführung erfolgte maßgeblich im Ministerium des Inneren, für Digitalisierung und Kommunen.

12. welche Möglichkeiten sie sieht, um die grenzüberschreitende Zusammenarbeit im Bereich Cybersicherheit, insbesondere mit den Nachbarländern und auf EU-Ebene, zu intensivieren;

Zu 12.:

Insbesondere durch die Umsetzung der NIS-2-Richtlinie wird die grenzüberschreitende Zusammenarbeit im Bereich der Cybersicherheit in erheblichem Maße gefördert. So legt die NIS-2-Richtlinie etwa fest, dass nationale Behörden der Mitgliedsstaaten sowie die Europäische Kommission eng zusammenarbeiten, um die Cybersicherheitslage der EU zu stärken. Ein zentraler Aspekt dieser Zusammenarbeit ist der regelmäßige Informationsaustausch, beispielsweise zu Sicherheitsvorfällen sowie die Koordination von Reaktionsmaßnahmen, um grenzüberschreitende Sicherheitsvorfälle effizient zu bewältigen. Ziel ist es, die kollektive Sicherheitslage der EU zu verbessern und sicherzustellen, dass sowohl Unternehmen als auch öffentliche Stellen in der Lage sind, schneller und gezielter auf Cyberrisiken zu reagieren, auch wenn diese über die Landes-/Bundesgrenzen hinweg auftreten.

Die CSBW wurde gegenüber der Europäischen Kommission als zuständige Behörde nach Artikel 8 der NIS-2-Richtlinie benannt. Als solche ist sie die zentrale Ansprechstelle im Land und übernimmt auch die Aufgaben eines Computer-Notfallteams. Darüber hinaus kann die CSBW an Peer Reviews teilnehmen, die nach Artikel 19 der NIS-2-Richtlinie durchgeführt werden, um die Sicherheitsstandards der Mitgliedsstaaten kontinuierlich zu überprüfen und zu verbessern.

Weiter besteht u. a. mit den Partnerregionen der Vier Motoren für Europa (Auvergne-Rhône-Alpes, Katalonien, Lombardei sowie Baden-Württemberg) ein Austausch zu verschiedenen Themen der Cybersicherheit, um die Herausforderungen einer zunehmend digitalisierten Welt gemeinsam zu bewältigen. Darüber wird mit dem „National Cyber Security Centre“ (NCSC) aus Finnland aktuell der Austausch auf technischer und strategischer Ebene im gemeinsamen Vorgehen mit der CSBW vertieft. Dazu gehört z. B. die geplante Einbindung des NCSC in das diesjährige CSF in Stuttgart und ein Besuch der finnischen Kolleginnen und Kollegen bei der CSBW.

Die Teilnahme an Kongressen dient der Förderung der grenzüberschreitenden Zusammenarbeit und dem Austausch von Wissen sowie Erfahrungen, um internationale Netzwerke zu stärken und gemeinsame Lösungen für globale Herausforderungen zu entwickeln. So war die CSBW im vergangenen Jahr u. a. an einem Panel auf dem „Cybersecurity Congress“ in Barcelona beteiligt. Gegenstand der Diskussionen mit den italienischen und spanischen Fachleuten waren zum Beispiel erfolgreiche Strategien zur langfristigen Sensibilisierung der Bevölkerung sowie zur Gewinnung von IT-Fachkräften. Darüber hinaus finden weitere Fach- und Lageaustausche mit internationalen Partnern statt, mit denen das Land bereits Kooperationsvereinbarungen im Bereich der Cybersicherheit unterhält.

Im Übrigen wird auf die Antworten zu 9 der Kleinen Anfrage der Abgeordneten Christian Gehring u. a., CDU (Kampf gegen Cyberkriminalität in Baden-Württemberg, Drucksache 17/5254) verwiesen.

13. wie die Landesregierung die flächendeckende Wartung der Cybersicherheitsinfrastruktur sicherstellt.

Zu 13.:

Die flächendeckende Wartung der Cybersicherheitsinfrastruktur ist eine kontinuierliche Aufgabe, die eine regelmäßige Pflege und Anpassung aller sicherheitsrelevanten Systeme erfordert. Angesichts der sich ständig weiterentwickelnden Bedrohungen muss die Infrastruktur fortlaufend an neue Risiken angepasst werden. Dafür sind regelmäßige Investitionen im Rahmen der bestehenden Haushaltsermächtigungen notwendig, um die Integrität und Funktionsfähigkeit dauerhaft zu sichern.

Ziel ist es, Angriffsflächen zu minimieren und die Resilienz gegen neue Bedrohungen nachhaltig zu sichern. So werden etwa Sicherheitslücken schnellstmöglich durch ein risikobasiertes Patchmanagement geschlossen, wobei etwa der CVSS-Score (Common Vulnerability Scoring System – ein standardisiertes Bewertungssystem zur Bewertung der Schwere von Sicherheitslücken anhand von Faktoren wie etwa Ausnutzbarkeit oder Auswirkungen) zur Priorisierung herangezogen wird. Daneben werden regelmäßig Schwachstellenanalysen und Penetrationstests sowie darauf abgestimmte Updateprozesse eingesetzt, um Systeme kontinuierlich zu härten. Ein weiterer wesentlicher Bestandteil ist die Schulung der Mitarbeiterinnen und Mitarbeiter, um auf Bedrohungen wie Phishing-Angriffe vorbereitet zu sein.

Die Überwachung und Wartung der Cybersicherheitsinfrastruktur erfolgt dabei rund um die Uhr durch interne Strukturen in den Dienststellen sowie bei den zentralen IT-Dienstleistern des Landes, der BITBW und dem LZfD. Auch bestehen Wartungsverträge mit spezialisierten externen IT-Dienstleistern oder Herstellern, die eine kontinuierliche Wartung und Pflege sicherstellen.

Strobl

Minister des Inneren,
für Digitalisierung und Kommunen