Landtag von Baden-Württemberg **Drucksache 17 / 4048**

17. Wahlperiode **27.1.2023**

Geänderte Fassung

Antrag

der Fraktion der FDP/DVP

und

Stellungnahme

des Ministeriums des Inneren, für Digitalisierung und Kommunen

Cybersicherheit in Baden-Württemberg

Antrag

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. wie viele Sicherheitslücken in der IT-Infrastruktur in der Landesverwaltung inklusive aller nachgeordneten Bereiche sowie Unternehmen von besonderem öffentlichem Interesse, Unternehmen mit Landesbeteiligung, Kommunen und Unternehmen in kommunaler Trägerschaft, Wirtschaftsunternehmen mit Sitz in Baden-Württemberg, staatlichen Schulen, Hochschulen und Universitäten in Baden-Württemberg sowie bei Bürgerinnen und Bürgern mit Wohnsitz in Baden-Württemberg in den vergangenen 24 Monaten offengelegt wurden (bitte differenziert nach Art der Sicherheitslücken);

2. welche Maßnahmen nach Offenlegung der jeweiligen Sicherheitslücken ihrer Kenntnis nach ergriffen wurden und mit welchem Erfolg (bitte differenziert nach Art der Sicherheitslücken);

3. wie viele Cyberangriffe auf die IT-Infrastruktur in der Landesverwaltung inklusive aller nachgeordneten Bereiche sowie Unternehmen von besonderem öffentlichem Interesse, Unternehmen mit Landesbeteiligung, Kommunen und Unternehmen in kommunaler Trägerschaft, Wirtschaftsunternehmen mit Sitz in Baden-Württemberg, staatlichen Schulen, Hochschulen und Universitäten in Baden-Württemberg sowie bei Bürgerinnen und Bürgern mit Wohnsitz in Baden-Württemberg seit Drucksache 17/483 erfolgt sind (bitte differenziert nach Art der Angriffe);

Eingegangen: 27.1.2023 / Ausgegeben: 16.3.2023

4. wie viele Verdachtsfälle auf Cyberangriffe seit dem 1. Juli 2022 bei der Cyber-Ersthilfe BW eingegangen sind (bitte differenziert nach Meldungen aus der Landesverwaltung inklusive aller nachgeordneten Bereiche sowie Unternehmen von besonderem öffentlichem Interesse, Unternehmen mit Landesbeteiligung, Kommunen und Unternehmen in kommunaler Trägerschaft, Wirtschaftsunternehmen mit Sitz in Baden-Württemberg, staatlichen Schulen, Hochschulen und Universitäten in Baden-Württemberg sowie von Bürgerinnen und Bürgern mit Wohnsitz in Baden-Württemberg);

5. welche diesem Verdachtsfälle sich als Cyberangriff bestätigt haben und welche Maßnahmen diesbezüglich ergriffen wurden (bitte differenziert nach Art des jeweiligen Cyberangriffs);

6. zu welchen Ergebnis sie mittlerweile bei der von ihr laut Drucksache 17/3255 in enger Abstimmung mit einzelnen IHKen durchgeführten Prüfung, welche weiteren konkreten Leistungen, Angebote und Informationen die Cybersicherheitsagentur Baden-Württemberg – unter Einbeziehung von Multiplikatoren – Unternehmen im Rahmen der haushaltsrechtlichen Ermächtigungsgrundlage zur Verfügung stellen kann, gekommen ist;

7. welche Maßnahmen sie noch in dieser Legislaturperiode vorsieht bzw. umsetzen wird, um Datensicherheit, Datenschutz und Verbraucherschutz sicherzustellen;

8. wie hoch die durch Cyberkriminalität verursachten Kosten in den vergangenen fünf Jahren waren (bitte differenziert nach Jahren sowie nach den Kosten für die Landesverwaltung inklusive aller nachgeordneten Bereiche sowie Unternehmen von besonderem öffentlichem Interesse, Unternehmen mit Landesbeteiligung, Kommunen und Unternehmen in kommunaler Trägerschaft, Wirtschaftsunternehmen mit Sitz in Baden-Württemberg, staatliche Schulen, Hochschulen und Universitäten in Baden-Württemberg sowie Bürgerinnen und Bürger mit Wohnsitz in Baden-Württemberg);

9. mit welcher Entwicklung sie bei der Cyberkriminalität in Baden-Württemberg in den kommenden fünf Jahren rechnet;

10. wie sie die von der Europäischen Union Ende 2022 verabschiedeten Rechtsvorschriften (Richtlinie NIS2) zur Stärkung der Cybersicherheitsmaßnahmen mit Blick auf Baden-Württemberg bewertet, die die Reaktionsfähigkeit des öffentlichen und privaten Sektors verbessern und die dahin geltenden Regeln für die Sicherheit von Netzwerken und Informationssystemen (NIS) ersetzen sollen;

11. welche Maßnahmen sie umsetzt, um die Verfügbarkeit von IT-Anwendungen von Landesbehörden auch nach physischen Ausfällen (aufgrund eines Cyberangriffs oder technischen Versagens) zu gewährleisten;

12. welche Lehren sie aus den massiven Störungen der Polizeiarbeit und anderer Sicherheitsbehörden nach einem Brand in einer Liegenschaft des Landeskriminalamts zieht;

13. nach welchen Maßstäben und Kriterien die IT-Sicherheit von Landesbehörden hinsichtlich Risiken und Resilienz bewertet werden;

14. in welcher Kontinuität sie in den vergangenen fünf Jahren Bestandsaufnahmen zur Bedrohungslage durch Cyberangriffe der IT-Sicherheit der Landesverwaltung inklusive aller nachgeordneter Bereiche mit welchem Ergebnis durchgeführt hat;

15. inwiefern sie die bisher ergriffenen technischen, organisatorischen und prozessualen Schutzmaßnahmen bezüglich der IT-Sicherheit der Landesverwaltung inklusive aller nachgeordneter Bereiche angesichts der aktuellen Bedrohungslage durch Cyberangriffe für ausreichend erachtet.

27.1.2023

Dr. Rülke, Karrais

und Fraktion

Begründung

Neben Risiken wie steigenden Lebenshaltungskosten, Naturkatastrophen, Konflikten, geoökonomischen Spannungen sowie dem Klimawandel zählt Cyberkriminalität zu den zehn größten Herausforderungen der kommenden Jahre. Laut dem Global Risk Report 2023 des Weltwirtschaftsforums steht Cyberkriminalität sowohl kurz- wie auch mittelfristig in der Liste der Top-10-Risiken auf Platz acht. Schätzungen zufolge wird sie bis 2025 wirtschaftliche Verluste in Höhe von 10,5 Billionen US-Dollar jährlich verursachen. Um die Cybersicherheit zu erhöhen, fordert das Weltwirtschaftsforum deshalb international verbindliche Regeln.

Eine Reihe von Sicherheitsvorfällen in jüngster Vergangenheit hat gezeigt, dass die vorhandenen Schutzmechanismen bezüglich der Cybersicherheit in Baden-Württemberg unzureichend sind. Allein der Wirtschaft im Land gehen Jahr für Jahr Millionensummen verloren, weil sie ihr Wissen und ihre Innovationen nicht ausreichend schützt. Immer häufiger sind auch kleine und mittlere Unternehmen mit hoher technologischer Kompetenz betroffen. Die „SiFo-Studie 2009/10 – Know-how-Schutz in Baden-Württemberg“ zeigt beispielsweise, dass Urheberrechtsverletzungen, Spionage und ungewollter Informationsabfluss besonders forschungsintensive Unternehmen bedrohen.

Der Antrag soll unter anderem in Erfahrung bringen, welche Maßnahmen die Landesregierung vorsieht, um die Cybersicherheit in Baden-Württemberg zu erhöhen.

Stellungnahme

Mit Schreiben vom 23. Februar 2023 Nr. IM7-0141-48/2/2 nimmt das Ministerium des Inneren, für Digitalisierung und Kommunen im Einvernehmen mit dem Ministerium für Ernährung, Ländlichen Raum und Verbraucherschutz zu dem Antrag wie folgt Stellung:

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. *wie viele Sicherheitslücken in der IT-Infrastruktur in der Landesverwaltung inklusive aller nachgeordneten Bereiche sowie Unternehmen von besonderem öffentlichem Interesse, Unternehmen mit Landesbeteiligung, Kommunen und Unternehmen in kommunaler Trägerschaft, Wirtschaftsunternehmen mit Sitz in Baden-Württemberg, staatlichen Schulen, Hochschulen und Universitäten in Baden-Württemberg sowie bei Bürgerinnen und Bürgern mit Wohnsitz in Baden-Württemberg in den vergangenen 24 Monaten offengelegt wurden (bitte differenziert nach Art der Sicherheitslücken);*

2. *welche Maßnahmen nach Offenlegung der jeweiligen Sicherheitslücken ihrer Kenntnis nach ergriffen wurden und mit welchem Erfolg (bitte differenziert nach Art der Sicherheitslücken);*

Zu 1. und 2.:

Die Ziffern 1 und 2 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Schwachstellen in der IT-Infrastruktur und deren Komponenten wie Computer, Server, Netzwerkgeräte, Betriebssysteme, Softwarebibliotheken und Anwendungen ergeben sich jeden Tag. Bis zum jeweiligen Beheben der Schwachstellen und bis zum Umsetzen entsprechender Gegenmaßnahmen ergeben sich Sicherheitslücken in den betroffenen Systemen. Dies stellt alle Betreiber von IT-Infrastrukturen gleichermaßen vor besondere Herausforderungen. Zugleich steigt die Anzahl erkannter Sicherheitslücken weltweit stetig. Dazu hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem letzten Bericht zur Lage der IT-Sicherheit in Deutschland 2022 ausgeführt: „Im Jahr 2021 wurden zehn Prozent mehr Schwachstellen in Software-Produkten bekannt als im Vorjahr. Mehr als die Hälfte von ihnen wiesen hohe oder kritische Scores nach dem Common Vulnerability Scoring System (CVSS) auf. Als kritisch wurden 13 Prozent der Schwachstellen bewertet.“ Alleine im Softwarebereich sind im betreffenden Berichtsjahr demnach 20.174 Schwachstellen neu bekannt geworden. Informationen zur Quantifizierung und zur Qualifizierung der Sicherheitslücken in der IT Infrastruktur der Landesverwaltung berühren in besonderem Maße die Sicherheitsinteressen der Landesverwaltung und können daher nicht bereitgestellt werden. Über die Art und Zahl von Sicherheitslücken der in der jeweiligen Eigenverantwortung betriebenen IT-Infrastrukturen von Unternehmen, Kommunen, Schulen, Hochschulen und Universitäten in Baden-Württemberg sowie in den von Bürgerinnen und Bürgern genutzten IT-Geräten liegen zudem keine Erkenntnisse vor.

Um Maßnahmen gegen Sicherheitslücken überhaupt erst ergreifen zu können, kommt dem schnellen Erlangen der Kenntnis über eine Schwachstelle besondere Bedeutung zu. Die Cybersicherheitsagentur Baden-Württemberg (CSBW) nimmt für die Landesverwaltung und für weitere öffentliche Stellen dabei eine Schlüsselrolle ein. So sammeln die hierfür eingesetzten Expertinnen und Experten der CSBW u. a. durch ein permanentes Monitoring einschlägiger öffentlicher Quellen, aber auch von Quellen im Darknet die relevanten Informationen über Schwachstellen. Auch steht die CSBW in stetigem Austausch u. a. mit der Polizei Baden-Württemberg und dem für die Bearbeitung und Prävention von Cyberangriffen mit mutmaßlich nachrichtendienstlichem Hintergrund zuständigen Lan-

desamt für Verfassungsschutz Baden-Württemberg (LfV), mit dem BSI, mit den Computer Emergency Response Teams (CERTs) des Bundes und der Länder und weiteren Institutionen wie dem Nationalen Cyber-Abwehrzentrum.

Hieraus erlangt die CSBW zusätzlich aktuellste Erkenntnisse über neue Schwachstellen. Auch erlangt sie aus dieser Vernetzung und Zusammenarbeit strukturiert aufgearbeitete, anonymisierte Informationen aus erfolgten Cyberattacken – sogenannte „Indicators of Compromise (IOCs)“. All diese Informationen analysieren und bewerten die Sicherheitsexpertinnen und -experten der CSBW und geben sie in Form von Warnmeldungen und ergänzt um Handlungsempfehlungen schnellstmöglich weiter. Auf diesem Wege erreichen die Warnmeldungen der CSBW aktuell rund 800 Empfängerinnen und Empfänger, dies sind u. a. Sicherheitsbeauftragte und Sicherheitsverantwortliche in den Rechenzentren, Ressorts und weiteren Einrichtungen. Diese Leistung der CSBW ist skalierbar und soll hinsichtlich des Empfängerkreises sukzessive weiter ausgebaut werden.

Die Fachadministratorinnen und Fachadministratoren in den Rechenzentren erhalten über die Informationen der CSBW hinaus auch direkt von den einzelnen Lösungsanbietern entsprechende Mitteilungen zu Schwachstellen in deren Produkte. Alle eingehenden Informationen werden von den Administratorinnen und Administratoren im Rahmen der jeweiligen Schwachstellenmanagement-Mechanismen geprüft. Von den Herstellern zur Verfügung gestellte Updates und Patches werden im Rahmen eines Regelprozesses behandelt, dies wird teilweise auch von organisatorischen Maßnahmen, wie z. B. der Information und Sensibilisierung der Mitarbeitenden, flankiert. In der Landesverwaltung werden außerdem regelmäßig und auch anlassbezogen Schwachstellenanalysen und Penetrationstests auf einzelne IT-Systeme durchgeführt. So wurden jüngst vom Ministerium des Inneren, für Digitalisierung und Kommunen und der CSBW im Benehmen mit den Ressorts 400 Websysteme untersucht. Vereinzelt gefundene Lücken wurden umgehend geschlossen. Eine entsprechend verstetigte Dienstleistung der CSBW für Schwachstellenscans von Webservices öffentlicher Stellen im Land befindet sich in Arbeit.

3. wie viele Cyberangriffe auf die IT-Infrastruktur in der Landesverwaltung inklusive alle nachgeordneten Bereiche sowie Unternehmen von besonderem öffentlichem Interesse, Unternehmen mit Landesbeteiligung, Kommunen und Unternehmen in kommunaler Trägerschaft, Wirtschaftsunternehmen mit Sitz in Baden-Württemberg, staatlichen Schulen, Hochschulen und Universitäten in Baden-Württemberg sowie bei Bürgerinnen und Bürgern mit Wohnsitz in Baden-Württemberg seit Drucksache 17/483 erfolgt sind (bitte differenziert nach Art der Angriffe);

Zu 3.:

Bezüglich der Begriffsdefinition „Angriff“ wird auf die Stellungnahme zu Ziffer 1 bis 3 des Antrags der Abgeordneten Daniel Karrais u. a. FDP/DVP (Drucksache 17/483) verwiesen. Dabei ist nochmals herauszustellen, dass solche Angriffe massenhaft täglich und rund um die Uhr, sowohl auf Institutionen der Landesverwaltung als auch auf andere Einrichtungen, stattfinden. Bei der Beantwortung wird daher vorangestellt, dass mit „Angriffen“ nur solche gemeint sind, die als „Sicherheitsvorfall“ einzustufen und zu behandeln waren. Daneben besteht eine Meldeverpflichtung gegenüber der CSBW nach § 4 Absatz 3 des Cybersicherheitsgesetzes Baden-Württemberg nur für öffentliche Stellen des Landes oder unmittelbar an das Landesverwaltungsnetz angeschlossene Stellen. Über diese Stellen hinaus nimmt die CSBW auch freiwillige Meldungen weiterer Stellen entgegen. Nachfolgend aufgeführte Vorfälle beziehen sich daher auf Angriffe, in deren Folge Beeinträchtigungen in diesen Bereichen entstanden sind und die der CSBW gemeldet wurden und/oder bei deren Bewältigung die CSBW unmittelbar beteiligt war.

Insgesamt wurden im angefragten Zeitraum 39 Vorfälle registriert. Diese teilen sich wie folgt auf:

5 Vorfälle in der Landesverwaltung, davon

2 x Phishing,

2 x Überlastungsangriffe (Distributed-Denial-of-Service (DDoS)-Angriffe),

1 x unbefugter Zugriff auf Web-Server.

34 Vorfälle bei anderen Stellen (u. a. Kommunen und Hochschulen), die aus Meldungen an die CSBW und/oder der Beteiligung der CSBW berichtet werden können, davon

6 x unberechtigte Benutzung von Zugangsdaten/Accounts,

2 x Überlastungsangriffe (DDoS),

16 x Phishing und Postfachmissbrauch für Spam-Versand,

4 x Ransomware,

4 x sonstige Schadsoftware,

1 x Kompromittierung eines Web-Servers durch SQL-Injection,

1 x Schadsoftware auf IT-System, die Port-Scan ausführte.

Darüber hinaus wurden der CSBW rd. 30 weitere Verdachtsfälle sogenannter „sicherheitsrelevanter Ereignisse“ gemeldet, die die CSBW analysiert oder bei deren Bewertung die CSBW unterstützt hat, bei denen jedoch keine Beeinträchtigung der angegriffenen Systeme festzustellen war.

Neben diesen Vorkommnissen wurden bei der CSBW im Rahmen der Lageerhebung 28 Ransomware-Vorfälle bei Unternehmen in Baden-Württemberg erfasst.

Von der Cyberabwehr des LfV wurden im angefragten Zeitraum seit 1. Juli 2021 eine niedrige, dreistellige Zahl von Cyberangriffen mit mutmaßlich nachrichtendienstlichem Hintergrund auf Ziele in Baden-Württemberg festgestellt. Nach sorgfältiger Abwägung zwischen dem verfassungsrechtlich zu gewährleistenden Informationsinteresse des Landtags und dem öffentlichen Interesse an der Geheimhaltung der genauen Fallzahlen und deren Hintergründe können weitergehende Einzelheiten im Rahmen dieser Beantwortung nicht dargestellt werden. Aus ihrem Bekanntwerden könnten fremde Nachrichtendienste Rückschlüsse auf die Analysefähigkeiten des LfV ziehen und ihre Vorgehensweise hieran gezielt anpassen. Dadurch könnte die Funktionsfähigkeit des LfV beeinträchtigt werden, was sich wiederum schädlich auf die Interessen des Landes Baden-Württemberg auswirken kann.

Fremde Staaten greifen bei diesen Cyberangriffen auf unterschiedliche Tätergruppierungen zurück, welche als APT-Gruppen (Advanced Persistent Threat) bezeichnet werden. Die Besonderheit bei APT-Angriffen ist die Vorgehensweise der Cyberakteure. Sie versuchen bei ihren Angriffen möglichst lange unentdeckt zu bleiben und sich langfristig im attackierten System einzunisten. Insofern bleiben vermutlich erfolgreiche nachrichtendienstlich gesteuerte Cyberangriffe in nicht abschätzbarer Quantität unentdeckt. Unter Zugrundelegung dieser Prämissen ist davon auszugehen, dass die tatsächliche Anzahl der Cyberangriffe mit nachrichtendienstlichem Hintergrund wohl eher deutlich höher ist als die Anzahl erkannter Fälle. Zudem liegen der Cyberabwehr immer wieder technische Indikatoren vor, die auf weitere Betroffene hindeuten. Alleine sind diese Parameter allerdings nicht ausreichend, um konkret vermutete Opfer eindeutig zu identifizieren. Das LfV geht hier zusammenfassend von einem doppelten Dunkelfeld aus.

Bei der Polizei Baden-Württemberg erfolgt die statistische Erfassung von Straftaten anhand der Polizeilichen Kriminalstatistik (PKS). Bei der PKS handelt es sich um eine sogenannte reine Ausgangsstatistik, in der strafrechtlich relevante Sachverhalte nach der polizeilichen Sachbearbeitung vor Abgabe an die Strafverfolgungsbehörden erfasst werden. Die PKS ist als Jahresstatistik konzipiert. Die Fallerfassung erfolgt nach den bundeseinheitlichen „Richtlinien für die Führung der Polizeilichen Kriminalstatistik“. „Cyberangriff“ ist kein Erfassungsparameter der PKS. Überdies werden in der PKS Merkmale zu Opfern ausschließlich zu natürlichen Personen erfasst. Dies geschieht gemäß den bundeseinheitlichen PKS-Richtlinien lediglich zu sogenannten Opferdelikten. Zu diesen zählen vor allem Straftaten gegen die höchstpersönlichen Rechtsgüter, wie Leben, körperliche Un-

versehrtheit, Freiheit und sexuelle Selbstbestimmung. Diebstahlsdelikte oder Sachbeschädigungen fallen nicht darunter. Juristische Personen, wie zum Beispiel Unternehmen, Kommunen oder Bildungseinrichtungen sind keine Opfer im Sinne der bundeseinheitlichen „Richtlinien für die Führung der Polizeilichen Kriminalstatistik“, weshalb auf Grundlage der PKS keine Aussagen im Sinne der Fragestellung getroffen werden können.

4. wie viele Verdachtsfälle auf Cyberangriffe seit dem 1. Juli 2022 bei der Cyber-Ersthilfe BW eingegangen sind (bitte differenziert nach Meldungen aus der Landesverwaltung inklusive aller nachgeordneten Bereiche sowie Unternehmen von besonderem öffentlichem Interesse, Unternehmen mit Landesbeteiligung, Kommunen und Unternehmen in kommunaler Trägerschaft, Wirtschaftsunternehmen mit Sitz in Baden-Württemberg, staatlichen Schulen, Hochschulen und Universitäten in Baden-Württemberg sowie von Bürgerinnen und Bürgern mit Wohnsitz in Baden-Württemberg);

5. welche dieser Verdachtsfälle sich als Cyberangriff bestätigt haben und welche Maßnahmen diesbezüglich ergriffen wurden (bitte differenziert nach Art des jeweiligen Cyberangriffs);

Zu 4. und 5.:

Die Ziffern 4 und 5 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Seit dem 1. Juli 2022 sind bei der Cyber-Ersthilfe BW 17 Verdachtsfälle auf Cyberangriffe eingegangen. Diese lassen sich nach folgenden Zielgruppen differenzieren:

– Kommunen oder Unternehmen in kommunaler Trägerschaft: 4 Verdachtsfälle,
– Wirtschaftsunternehmen mit Sitz in Baden-Württemberg: 3 Verdachtsfälle,
– Bürgerinnen und Bürgern mit Wohnsitz in Baden-Württemberg: 10 Verdachtsfälle.

Aus den Bereichen der Landesverwaltung, der Unternehmen von besonderem öffentlichem Interesse, der Unternehmen mit Landesbeteiligung, der staatlichen Schulen und der Hochschulen sind keine Verdachtsfälle bei der Cyber-Ersthilfe BW eingegangen. Für diese Bereiche und deren Institutionen sind unter Beteiligung der jeweiligen Rechenzentren gesonderte Meldewege zur CSBW eingerichtet.

Von den insgesamt 17 Verdachtsfällen haben sich 14 als Cyberangriff bestätigt. Die ergriffenen Maßnahmen durch die Cyber-Ersthilfe BW umfassen jeweils eine erste Einordnung des Vorfalls und davon ausgehend zunächst die Aussprache von Handlungsempfehlungen sowie die Empfehlung einer Anzeige bei der Polizei und die Übersendung von zielgruppenspezifischen Anlaufstellen für die weitere Analyse und Unterstützung. Die weiteren Maßnahmen sowie Hilfestellungen orientieren sich jeweils am individuellen Fall und sind daher nicht kategorisierbar.

Die vorliegenden 14 Cyberangriffe lassen sich wie folgt differenzieren:

– 9 x unberechtigte Verwendung von Zugangsdaten/Accounts,
– 1 x Phishing,
– 3 x Ransomware,
– 1 x sonstige Schadsoftware.

6. zu welchem Ergebnis sie mittlerweile bei der von ihr laut Drucksache 17/3255 in enger Abstimmung mit einzelnen IHKen durchgeführten Prüfung, welche weiteren konkreten Leistungen, Angebote und Informationen die Cybersicherheitsagentur Baden-Württemberg – unter Einbeziehung von Multiplikatoren – Unternehmen im Rahmen der haushaltsrechtlichen Ermächtigungsgrundlage zur Verfügung stellen kann, gekommen ist;

Zu 6.:

Derzeit wird – als ein Bestandteil der Prüfung – ein Konzept der bedarfsorientierten Erstberatung für kleinere und mittlere Unternehmen (KMU) zur Cybersicherheit abgestimmt. Ziel dabei ist es, niederschwellige Angebote zu schaffen. Kleine und mittlere Unternehmen sowie Selbständige soll damit einerseits die notwendige Sensibilität für die Bedeutung der Cybersicherheit vermittelt werden, andererseits sollen aber schon im Beratungsgespräch erste Erkenntnisse über vorhandene Sicherheitslücken gewonnen und Empfehlungen zu konkreten Maßnahmen gegeben werden können. Anfang Februar 2023 erfolgte eine Vorstellung des Konzeptes und der erarbeiteten Beratungsmaterialien bei Vertreterinnen und Vertretern aller IHKen. Auch wurde das gemeinsame weitere Vorgehen abgestimmt. So soll ab März 2023 ein Pilotprojekt mit ausgewählten Unternehmen und verschiedenen IHKen starten, in welchem die Beratungsansätze erprobt und weiterentwickelt werden. Das Projekt wird von einer Hochschule wissenschaftlich begleitet. Nach erfolgreicher Evaluierung der Ergebnisse des Pilotprojekts, unter Einbindung des Ministeriums für Wirtschaft, Arbeit und Tourismus und weiterer Kooperationspartner und Multiplikatoren, sollen die Beratungsangebote landesweit ausgerollt werden.

7. welche Maßnahmen sie noch in dieser Legislaturperiode vorsieht bzw. umsetzen wird, um Datensicherheit, Datenschutz und Verbraucherschutz sicherzustellen;

Zu 7.:

Mit der Verabschiedung des Cybersicherheitsgesetzes Baden-Württemberg, der Errichtung der CSBW und dem Beschluss der Cybersicherheitsstrategie wurden die wesentlichen Grundsteine für eine bedarfsgerechte und zukunftsfähige Datensicherheit gelegt. Nun gilt es, die auf verschiedenen Ebenen bestehenden Maßnahmen fortzuführen oder zu ergänzen und neue Maßnahmen in die Wege zu leiten. Dazu wird unter anderem die CSBW ihr Leistungsportfolio sowohl im präventiven als auch im reaktiven Bereich weiter ausbauen. Neben der weiteren Unterstützung der Rechenzentren und Einrichtungen in der Landesverwaltung und der konzipierten Multiplikatoren-Beratungsleistungen für KMU gilt es insbesondere, zielgruppengerechte Angebote und Unterstützungsleistungen für Kommunen zu gestalten. So ist unter anderem in Vorbereitung, in der Landesverwaltung etablierte Schulungsangebote zur Informationssicherheit auf Kommunen auszuweiten. Dazu und zu weiteren Maßnahmen stehen das Ministerium des Inneren, für Digitalisierung und Kommunen und die CSBW in engem Austausch mit den Kommunalen Landesverbänden Baden-Württemberg und dem kommunalen IT-Dienstleister Komm.ONE AöR. Ziel dabei ist unter anderem auch, in einem Stufenmodell praktikable und handhabbare Maßnahmen für ein gemeinsames Mindestsicherheitsniveau zu entwickeln. In den Ressorts und den weiteren Stellen in der Landesverwaltung werden die Anstrengungen fortgesetzt, die umfangreichen Standards des BSI zu etablieren. Dazu werden beispielsweise weitere Sicherheitsuntersuchungen von Fachanwendungen vorgenommen und BSI-konforme Sicherheitskonzepte erstellt. In verschiedenen Bereichen sind außerdem Anwendungen einer BSI-Zulassung oder einer BSI-Zertifizierung zuzuführen. Das betrifft unter anderem die zur Verschlüsselung des Datenverkehrs im Landesverwaltungsnetz an über 1.000 Zugangsknoten eingesetzte Lösung ebenso wie die Kommunikationsinfrastruktur zum Zusammenschluss des Landesnetzes mit den Netzen des Bundes.

Das LfV bietet hinsichtlich staatlich gesteuerter bzw. nachrichtendienstlich gelenkter Cyberangriffe bereits ein breit gefächertes Präventionsangebot für öffentliche und nichtöffentliche Stellen im Land an. Dabei handelt es sich um eine dauerhafte Aufgabe des LfV, die vielmehr einen stetigen Prozess darstellt. Diese informierende und beratende Tätigkeit insbesondere durch den Behörden- und Wirtschaftsschutz des LfV zielt explizit auf die Erhöhung der Sensibilität bei allen Bedarfsträgern in Bezug auf Datensicherheit ab. Soweit Fragen der Datensicherheit den Schutz vor einschlägigen Cyberangriffen betreffen, werden von der Cyberabwehr anlassbezogen wie anlassunabhängig vielfältige Präventionsangebote, z. B. Vorträge, Informationsveranstaltungen, Warnhinweise und Handlungsempfehlungen, unterbreitet. Das LfV berät und sensibilisiert im Rahmen seiner Zuständigkeit dabei umfassend im Sinne eines ganzheitlichen Informationsschutzes der sowohl personelle und organisatorische wie auch materielle Aspekte der Sicherheit umfasst.

Um angemessenen Verbraucherschutz sicherzustellen liegt ein Schwerpunkt des Ministeriums für Ernährung, Ländlichen Raum und Verbraucherschutz in der Verbraucherbildung und Verbraucherinformation für verschiedene Zielgruppen. Denn eine entscheidende Rolle bei der Nutzung des Internets kommt den Verbraucherinnen und Verbrauchern selbst zu. Ziel ist es, aufzuklären, Alltagskompetenzen zu vermitteln und Bewusstsein u. a. für einen sicheren Umgang mit dem digitalen Alltag zu schaffen. Die Verbraucherbildung soll im Bereich des Ministeriums für Ernährung, Ländlichen Raum und Verbraucherschutz weiter ausgebaut werden. Partner der Verbraucherbildung sind die Schulen, die Erwachsenbildungsträger, die Seniorenorganisationen, die Landesanstalt für Kommunikation, das Landesmedienzentrum und vor allem die Verbraucherzentrale Baden-Württemberg e. V. Über die Förderung des Ministeriums für Ernährung, Ländlichen Raum und Verbraucherschutz erstellt die Verbraucherzentrale Baden-Württemberg e. V. kontinuierlich Bildungsmaterialien für die schulische Verbraucherbildung, stellt diese Lehrkräften und Schulen kostenlos zur Verfügung und ist in die Fortbildung der Lehrkräfte eingebunden.

Mit den vom Ministerium für Ernährung, Ländlichen Raum und Verbraucherschutz geförderten regionalen Kursangeboten „Verbraucherbildung für Erwachsene und Familien“ der Volkshochschulen und Familienbildungsstätten erreichen Verbraucherthemen zur digitalen Welt und zur Cybersicherheit breite Bevölkerungsgruppen. Im Jahr 2023 bieten die Erwachsenenbildungsträger zusätzlich überregionale digitale Vortragsangebote zu Themen mit dem bisherigen Arbeitstitel „Fit für die digitale Zukunft“ an. Auch das vom Ministerium für Ernährung, Ländlichen Raum und Verbraucherschutz in Kooperation mit der Landesanstalt für Kommunikation geförderte Projekt „Smart Surfer – Fit im digitalen Alltag“ unterstützt bereits Verbraucherinnen und Verbraucher 50+ mit verständlichen und an ihre Bedürfnisse angepasste Informationen und Tipps zu den wichtigsten Themen der Internetnutzung sowie auch zur Cybersicherheit. Die Smart Surfer-Lernhilfen und Kursangebote, beispielsweise bei den Volkshochschulen und der Verbraucherzentrale Baden-Württemberg e. V., vermitteln verständlich und praxisnah Kompetenzen für die digitale Welt.

8. wie hoch die durch Cyberkriminalität verursachten Kosten in den vergangenen fünf Jahren waren (bitte differenziert nach Jahren sowie nach den Kosten für die Landesverwaltung inklusive aller nachgeordneten Bereiche sowie Unternehmen von besonderem öffentlichem Interesse, Unternehmen mit Landesbeteiligung, Kommunen und Unternehmen in kommunaler Trägerschaft, Wirtschaftsunternehmen mit Sitz in Baden-Württemberg, staatliche Schulen, Hochschulen und Universitäten in Baden-Württemberg sowie Bürgerinnen und Bürger mit Wohnsitz in Baden-Württemberg);

9. mit welcher Entwicklung sie bei der Cyberkriminalität in Baden-Württemberg in den kommenden fünf Jahren rechnet;

Zu 8. und 9.:

Die Ziffern 8 und 9 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Ein Schaden im Sinne der PKS ist grundsätzlich der Geldwert (Verkehrswert) eines rechtswidrig erlangten Gutes. Bei Vermögensdelikten wie dem Computerbetrug ist unter Schaden die Wertminderung des Vermögens zu verstehen. Kosten im Sinne von Folgeschäden, die beispielsweise durch Produktionsausfall und Wiederherstellung der IT-Systeme entstehen, werden gemäß den PKS-Richtlinien nicht erfasst, weshalb hierzu im Sinne der Fragestellung keine belastbaren Aussagen getroffen werden können. Bis zum 31. Dezember 2020 wurde in der PKS im Deliktsbereich Cyberkriminalität zwischen der Computerkriminalität und der Internetkriminalität unterschieden. Mit Beginn des Jahres 2021 wurde die bundeseinheitliche statistische Zählweise der Cyberkriminalität umfassend umgestellt, Straftatbestände inhaltlich neu zugeordnet und die Kriminalitätsform sprachlich angepasst. Fortan weist die PKS die klassischen Delikte der Computerkriminalität und des Computerbetruges als Cyberkriminalität aus. Delikte der Softwarepiraterie fallen nicht mehr darunter.

Im Detail umfasst der Deliktsbereich der Cyberkriminalität seit Beginn des Jahres 2021 die folgenden Straftatbestände: Fälschung beweiserheblicher Daten gem. § 269 Strafgesetzbuch (StGB), Täuschung im Rechtsverkehr bei Datenverarbeitung gem. § 270 StGB, Datenveränderung gem. § 303a StGB, Computersabotage gem. § 303b StGB, Ausspähen von Daten gem. § 202a StGB, Abfangen von Daten gem. § 202B StGB, Vorbereiten des Ausspähens und Abfangens von Daten gem. § 202c StGB, Datenhehlerei gem. § 202d StGB und Computerbetrug gem. § 263a StGB.

Die Fallzahlen der Computerkriminalität/Cyberkriminalität sowie der hierzu erfasste Schaden entwickelten sich in den Jahren 2017 bis 2021 in Baden-Württemberg wie folgt:

Anzahl der Fälle von Computerkriminalität/ Cybercrime in Baden-Württemberg	**2017**	**2018**	**2019**	**2020**	**2021**
Computerkriminalität/Cybercrime	7.056	7.512	9.847	10.248	10.744
Schaden Computerkriminalität/Cybercrime in Mio. Euro	7,1	6,7	9,2	8,4	7,8

Seit fünf Jahren nehmen die Fallzahlen im Bereich der Computerkriminalität/ Cybercrime kontinuierlich zu. Im Jahr 2021 steigen die Fallzahlen im Bereich Cybercrime im Vergleich zum Vorjahr um 4,8 Prozent auf 10.744 (10.248) an. Die Schadensumme sinkt um 7,1 Prozent auf 7,8 (8,4) Millionen Euro. Der größte Anteil entfällt mit 8.152 Fällen im Jahr 2021 auf Delikte des Computerbetrugs. Eine besonders deutliche Steigerung ist bei den Delikten der Datenveränderung und Computersabotage mit 63 Prozent auf insgesamt 326 Fälle festzustellen. Auch die Fälle des Ausspähens und Abfangens von Daten steigen im Jahr 2021 um rund 25 Prozent auf 1.046 Fälle im Vergleich zum Vorjahr.

Die Datenbasis der PKS für das Jahr 2022 steht bislang noch nicht für valide Aussagen zur Kriminalitätslage zur Verfügung. Für das Jahr 2022 können Trendaussagen getroffen werden. Für das Jahr 2022 zeichnet sich für den Deliktsbereich der Cyberkriminalität sowohl bei den Fallzahlen auch bei der Schadenssumme ein Anstieg ab.

Als Wirtschaftsstandort mit zahlreichen großen und mittelständischen Unternehmen wird Baden-Württemberg auch in Zukunft ein attraktives Ziel für Cyberkriminelle darstellen. Vor dem Hintergrund der stetigen technischen Weiterentwicklungen ist auch mit neuen Kriminalitätsphänomenen zu rechnen. Die Möglichkeit eines weiteren Anstiegs der Fallzahlen in den kommenden Jahren, der auch auf eine erhöhte Anzeigebereitschaft zurückzuführen sein kann, ist daher grundsätzlich einzukalkulieren.

10. wie sie die von der Europäischen Union Ende 2022 verabschiedeten Rechtsvorschriften (Richtlinie NIS2) zur Stärkung der Cybersicherheitsmaßnahmen mit Blick auf Baden-Württemberg bewertet, die die Reaktionsfähigkeit des öffentlichen und privaten Sektors verbessern und die dahin geltenden Regeln für die Sicherheit von Netzwerken und Informationssystemen (NIS) ersetzen sollen;

Zu 10.:

Durch die Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2-Richtlinie) werden eine Vielzahl von Einrichtungen im öffentlichen und privaten Sektor erfasst, die von der bisherigen Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie) nicht erfasst wurden. Die vom Anwendungsbereich erfassten Einrichtungen haben viele Pflichten zu erfüllen, etwa in Bezug auf die Umsetzung von Präventionsmaßnahmen im Bereich der Cybersicherheit. Die vorgegebenen Maßnahmen tragen wesentlich dazu bei, die Cybersicherheit im öffentlichen und privaten Sektor zu stärken. Alleine schon deshalb ist die Verabschiedung der noch in nationales Recht umzusetzenden NIS2-Richtlinie zu begrüßen. Von den unionsweit einheitlichen Meldepflichten bei Sicherheitsvorfällen wird zudem ein verbesserter Informationsaustausch erwartet, um frühzeitig reagieren und rechtzeitig Abwehrmaßnahmen treffen zu können. Auch dies ist ausdrücklich zu begrüßen.

All diese Pflichten gehen allerdings mit einem hohen Aufwand für die betroffenen Einrichtungen einher. Nach der EU-Folgenabschätzung für die NIS2-Richtlinie sollten Unternehmen die bereits unter die NIS-Richtlinie fielen, eine Steigerung der Cybersicherheitsbudgets von bis zu 12 Prozent einplanen, für Einrichtungen, die nicht von der NIS-Richtlinie erfasst wurden, wird eine Erhöhung der Cybersicherheitsbudgets von 22 Prozent erwartet.

Mit der CSBW und der am 21. Dezember 2021 vom Ministerrat beschlossenen Cybersicherheitsstrategie wurden in Baden-Württemberg bereits elementare Grundlagen geschaffen, um den aus der NIS2-Richtline folgenden Anforderungen gerecht werden zu können, gleichwohl wird ein großer zusätzlicher Aufgabenzuwachs für die CSBW erwartet, welcher auch zusätzliche Haushaltsmittel erfordern wird.

11. welche Maßnahmen sie umsetzt, um die Verfügbarkeit von IT-Anwendungen von Landesbehörden auch nach physischen Ausfällen (aufgrund eines Cyberangriffs oder technischen Versagens) zu gewährleisten;

Zu 11.:

Zur Gewährleistung der Verfügbarkeit von Anwendungen auch nach physischen Ausfällen gibt es unterschiedliche Mechanismen. Diese reichen im Bereich der klassischen IT-Anwendungen vom einfachen Backup von Systemen bis hin zur Schaffung von Hochverfügbarkeiten von Hard- und Softwarekomponenten. Diese Mechanismen unterscheiden sich einerseits in den zu tolerierenden Ausfallzeiten, aber eben auch in den für die jeweilige Realisierung anfallenden Kosten. Nicht zuletzt auch unter Beachtung des Grundsatzes der Wirtschaftlichkeit und Sparsamkeit wird bei der Auswahl entsprechender Mechanismen geprüft, welche Verfügbarkeitsanforderungen für die jeweiligen Verfahren und Komponenten bestehen. Nicht jedes Verfahren muss in einem hochverfügbaren Server-Cluster mit gespiegelten und doppelt redundanten Mechanismen betrieben werden. Auf besonders wichtige Verfahren und insbesondere auf zentrale Infrastrukturkomponenten trifft dies jedoch zu, daher sind diese so abzusichern, dass Ausfälle kompensiert werden können. An entsprechenden Maßstäben orientiert sich die Landesoberbehörde IT Baden-Württemberg (BITBW) als zentrale Dienstleisterin der Landesverwaltung bei der Auswahl der zu treffenden Notfallmaßnahmen. Im Rahmen der Erfüllung der Vorgaben der Verwaltungsvorschrift des Ministeriums des Inneren, für Digitalisierung und Kommunen zur Informationssicherheit (VwV Informationssicherheit) richten die BITBW und die Ressorts ihre Maßnahmen zur

Notfallvorsorge und Notfallbewältigung an den einschlägigen Standards des BSI aus. So wurden im Rahmen der Notfallvorsorge unter anderem geschäftskritische Verfahren identifiziert, um zielgerichtet die weiteren Maßnahmen ableiten zu können. Im Bereich der BITBW wurden die Alarmierungswege und die Zusammensetzung der Notfallorganisation zur Bewältigung von Notfällen neu definiert. Für Kernsysteme der BITBW liegen Notfallpläne vor, um den Wiederanlauf zu steuern. Dazu werden mögliche Notfallszenarien definiert und das Wiederanlaufen je nach Szenario durchgeplant. Notfallpläne werden im Rahmen von Notfallübungen getestet und kontinuierlich verbessert. Alle Personen, die in die jeweiligen Prozesse eingebunden sind, werden entsprechend regelmäßig geschult.

Das Rechenzentrum der BITBW und das Ausfall-Rechenzentrum des Landeszentrums für Datenverarbeitung (LZfD) verfügen über USV-Anlagen (Unterbrechungsfreie Stromversorgung), die Lastspitzen ausgleichen und bei einem Stromausfall das Rechenzentrum und dessen wesentliche Komponenten zunächst unterbrechungsfrei mit Strom versorgen. Zusätzlich verfügen die Rechenzentren über Netzersatzanlagen, die anschließend die Stromversorgung übernehmen. Auch sind Vorkehrungen realisiert, die den Anschluss externer, mobiler Stromversorgungen wie sie beispielsweise das Technische Hilfswerk bereithält, ermöglichen. Somit wirkt sich auch ein länger andauernder Stromausfall nicht unmittelbar auf die Infrastruktur der Rechenzentren aus.

12. welche Lehren sie aus den massiven Störungen der Polizeiarbeit und anderer Sicherheitsbehörden nach einem Brand in einer Liegenschaft des Landeskriminalamts zieht;

Zu 12.:

Die Sicherheit der Bürgerinnen und Bürger war trotz des Ausfalls von Teilen der IT-Infrastruktur zu keiner Zeit bedroht. Die Erreichbarkeit über den Polizeinotruf war durchweg gegeben. Die Störungen zeigen allerdings, dass die IT-Verfahren der baden-württembergischen Sicherheitsbehörden stabil, hochverfügbar und georedundant sein müssen. Derzeit werden mit Hochdruck verschiedene Lösungsalternativen für eine trag- und zukunftsfähige Lösung hinsichtlich des Rechenzentrums der Polizei geprüft. In Zusammenarbeit mit dem Landesbetrieb Vermögen und Bau Baden-Württemberg, Amt Stuttgart, werden darüber hinaus Verträge mit Fachfirmen abgeschlossen, welche eine Erreichbarkeit rund um die Uhr, auch für die Themen der Gebäudeinfrastruktur und Gebäudetechnik, gewährleisten.

13. nach welchen Maßstäben und Kriterien die IT-Sicherheit von Landesbehörden hinsichtlich Risiken und Resilienz bewertet werden;

Zu 13.:

Die Beurteilung und Bewertung der IT-Sicherheit der Landesbehörden ist ein stetiger Prozess. Zu den Kernaufgaben der Sicherheitsbeauftragten der Landesbehörden gehört es, aktuelle Situationen und Lageentwicklungen permanent zu bewerten und zu beurteilen, Risiken zu erkennen und entsprechende Maßnahmen vorzuschlagen oder zur Umsetzung zu bringen. Dabei finden anlassbezogen auf den Standards des BSI basierende, standardisierte Methoden zur Erstellung von Risikoanalysen Anwendung. Bei der Erstellung solcher Risikoanalysen werden die für das jeweilige System individuell festzulegenden Gefährdungen und Schadenspotenziale, aber auch mögliche Maßnahmen zur Minimierung der Risiken oder zum Ausschluss von Risiken betrachtet und dargelegt. Die dabei anzuwendenden Maßstäbe und Kriterien variieren von System zu System und können nicht verallgemeinert werden. Ein Beispiel für ein solches Kriterium ist die Festlegung der sogenannten „Maximalen tolerierbaren Ausfallzeit“ eines Systems, einer Anwendung oder eines Prozesses. Die Umsetzung gewählter Maßnahmen dient dabei nicht nur der akuten Risikobehandlung, sondern auch der Erhöhung der Resilienz der betrachteten Zielobjekte.

14. in welcher Kontinuität sie in den vergangenen fünf Jahren Bestandsaufnahmen zur Bedrohungslage durch Cyberangriffe der IT-Sicherheit der Landesverwaltung inklusive aller nachgeordneter Bereiche mit welchem Ergebnis durchgeführt hat;

Zu 14.:

Die strategische und operative Auswertung der Cybersicherheit im Allgemeinen und der Kriminalitätslage ist eine Daueraufgabe für die Sicherheitsbehörden im Land und dabei nicht alleine auf die IT-Sicherheit der Landesverwaltung ausgerichtet.

Die Sicherheitsbehörden sind in nationalen und internationalen Kooperationen, Partnerschaften und Netzwerkstrukturen eingebunden, innerhalb derer Informationen zu aktuellen Bedrohungslagen ausgetauscht werden. Ein Beispiel hierfür ist der enge Kontakt zwischen dem LfV, dem Landeskriminalamt Baden-Württemberg und der CSBW sowie der Austausch im Verbund der Zentralen Ansprechstellen Cybercrime (ZAC) im gesamten Bundesgebiet.

Darüber hinaus werden Lagebilder und Sicherheitsmeldungen anderer Behörden, unter anderem des Bundeskriminalamts, des BSI und des Nationalen Cyber-Abwehrzentrums ausgewertet und analysiert.

In der Landesverwaltung findet darüber hinaus ein regelmäßiger fachlicher Austausch der „Koordinierungsgruppe Informationssicherheit“ (KG InfoSIC) unter Federführung des Ministeriums des Inneren, für Digitalisierung und Kommunen statt. Die Informationssicherheitsbeauftragten der Ressorts und die Expertinnen und Experten der CSBW, der BITBW, des LZfD, des Sicherheitszentrums IT in der Finanzverwaltung (SITiF) sowie der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit und der Sicherheitsbeauftragten des Rechnungshofes und des Landtages erörtern die Bedrohungslage gemeinsam und koordinieren die auch auf Basis der Standards des BSI umzusetzenden Maßnahmen regelmäßig in einem formalen Sitzungsformat. In den vergangenen 5 Jahren haben 24 protokollierte Regel-Sitzungen und viele anlassbezogene ad-hoc-Austausche je nach Lageentwicklung stattgefunden, ab dem 4. Quartal 2022 wurde der Sitzungsrhythmus auf vier Wochen verkürzt. Darüber hinaus fanden in den vergangenen 5 Jahren eine Vielzahl an auf verschiedene fachliche Unterarbeitsgruppen aufgeteilte Abstimmungsrunden statt. Im Rahmen der Sitzungen und Austausche findet ein kontinuierlicher Abgleich der Entwicklung der Maßnahmen der IT- und Informationssicherheit in der Landesverwaltung mit dem sich stetig verändernden Bedarf statt, um angemessen reagieren zu können. Das Ministerium des Inneren, für Digitalisierung und Kommunen stellt den weiteren Ressorts, Dienststellen und Einrichtungen eine Softwarelösung zur Verfügung, in denen die IT Dienstleister ebenso wie die Ressorts, Einrichtungen und Dienststellen ihre Sicherheitsmaßnahmen auf Basis der Standards des BSI dokumentieren, Sicherheitskonzepte erstellen und aktualisieren.

15. inwiefern sie die bisher ergriffenen technischen, organisatorischen und prozessualen Schutzmaßnahmen bezüglich der IT-Sicherheit der Landesverwaltung inklusive aller nachgeordneter Bereiche angesichts der aktuellen Bedrohungslage durch Cyberangriffe für ausreichend erachtet.

Zu 15.:

Die Bedrohungslage im Cyberraum ist nach den Feststellungen des BSI und nach den Erkenntnissen der Sicherheitsbehörden im Land so hoch wie nie. Insgesamt spitzt sich die bereits zuvor angespannte Lage durch den völkerrechtswidrigen Angriffskrieg Russlands gegen die Ukraine weiter zu. Mit der aktuellen Sicherheitsarchitektur im Land, aber auch mit den bereits umgesetzten und initiierten, ebenso wie mit den weiter geplanten Maßnahmen ist das Land gut aufgestellt. Gleichwohl ist zu erwähnen, dass in der weiteren Konsolidierung und Aktualisierung von in vielen Jahren gewachsenen Systemen, Strukturen, Prozessen und

Anwendungen noch Potenzial steckt, dessen Aufarbeitung weitere Ressourcen in Anspruch nehmen wird.

Mit der aktuell erfolgenden Digitalisierung einer Vielzahl weiterer Verwaltungsprozesse stellen sich gerade auch in den Bereichen der Cybersicherheit weitere Aufgaben. Einer stetigen Verbesserung der Resilienz bei Cyberangriffen kommt daher weiterhin entsprechende Bedeutung für alle Stellen der Landesverwaltung zu. Angesichts der Komplexität der IT-Infrastrukturen, des hohen Grades der Vernetzung und der Abhängigkeit der Verwaltung von IT-gestützten Verfahren sieht sich die Landesverwaltung nebst nachgeordneter Bereiche vor der zunehmenden Herausforderung, den stetig wachsenden Anforderungen an ihre Cybersicherheit weiterhin gerecht zu werden. Alleine im technischen Bereich bedeutet dies ein unablässiges Schritthalten.

Strobl

Minister des Inneren,
für Digitalisierung und Kommunen