Landtag von Baden-Württemberg **Drucksache 17 / 6613**

17. Wahlperiode **16.4.2024**

Antrag

der Abg. Ruben Rupp und Bernd Gögel u. a. AfD

und

Stellungnahme

des Ministeriums des Inneren, für Digitalisierung und Kommunen

Zur Tätigkeit der Cybersicherheitsagentur Baden-Württemberg

Antrag

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. welche Entwicklungen bei konkreten, herausgehobenen Cyberangriffen seit dem Jahr 2021 festzustellen sind und in welchem Umfang Landesbehörden, Städte und Gemeinden sowie Landkreise bisher davon betroffen waren;

2. welcher finanzielle und personelle Aufwand erforderlich gewesen ist, um seit dem Jahr 2021 die aus schwerwiegenden Cyberangriffen resultierenden Schäden zu beseitigen und störungsfreie EDV-Systeme wiederherzustellen;

3. auf welchem Stand sich die Vernetzung staatlicher Einrichtungen, der Wirtschaft sowie von Wissenschaft und Forschung im Bereich der Cybersicherheit inzwischen befindet und welchen Zeitplan die Landesregierung dabei verfolgt;

4. welche konkreten Beratungsangebote der Cybersicherheitsagentur den Kommunen im Verlauf des Jahres 2023 zur Verfügung gestellt werden konnten und auf welche Resonanz diese Angebote gestoßen sind;

5. mit welchen darüber hinausgehenden Beratungsangeboten die Cybersicherheitsagentur weitere Zielgruppen wie zum Beispiel kleine und mittlere Unternehmen (KMU) erreicht hat;

6. wie der für das zweite Quartal 2023 geplante Roll-out der landesweiten Sensibilisierungskampagne zur Cybersicherheit verlaufen ist;

7. ob und inwieweit die nach dem Haushaltsplan 2023 der Cybersicherheitsagentur zugewiesenen Personalstellen inzwischen vollständig besetzt werden konnten und welchen Fachabteilungen gegebenenfalls nicht besetzte Stellen zuzuordnen sind;

Eingegangen: 16.4.2024 / Ausgegeben: 15.5.2024

8. ob und in welchem Umfang die Cybersicherheitsagentur im Rahmen ihrer Aufgaben externe Dienstleister einsetzt und welcher finanzielle Mehraufwand daraus gegebenenfalls resultiert.

16.4.2024

Rupp, Gögel, Baron, Lindenschmid, Steyer AfD

Begründung

Mit Inkrafttreten des Cybersicherheitsgesetzes wurde in Baden-Württemberg die Cybersicherheitsagentur Baden-Württemberg (CSBW) als zentrale Anlaufstelle für Cybersicherheit gegründet. Der vorliegende Antrag hinterfragt unter Berücksichtigung des Jahresberichts 2022 der Cybersicherheitsagentur die aktuellen Entwicklungen sowie den Stand der verschiedenen Aktivitäten der CSBW, die Cybersicherheit in Baden-Württemberg zu verbessern.

Stellungnahme

Mit Schreiben vom 10. Mai 2024 Nr. IM4-0141-67/5/2 nimmt das Ministerium des Inneren, für Digitalisierung und Kommunen im Einvernehmen mit dem Ministerium für Finanzen zu dem Antrag wie folgt Stellung:

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. welche Entwicklungen bei konkreten, herausgehobenen Cyberangriffen seit dem Jahr 2021 festzustellen sind und in welchem Umfang Landesbehörden, Städte und Gemeinden sowie Landkreise bisher davon betroffen waren;

Zu 1.:

Im Kontext der Darstellung der Tätigkeiten der Cybersicherheitsagentur Baden-Württemberg (CSBW) ist zu Cyberangriffen zunächst anzumerken, dass bei „herausgehobenen Fällen“ i. S. d. Gesetzes für die Cybersicherheit in Baden-Württemberg (CSG) die CSBW umfassende, technisch komplexe und aufwändige Maßnahmen wie forensische Untersuchungen als Grundlage für die Wiederherstellung der betroffenen Systeme ergreift. Dies erfordert in aller Regel entsprechende Einsätze des Mobile Incident Response Teams (MIRT) der CSBW vor Ort. Darüber hinaus erfolgt eine Unterstützung der betroffenen Einrichtung beim Krisenmanagement und bei der Krisenkommunikation.

Die Fallzahlen entwickelten sich wie folgt:

Im Jahr 2021, also dem Gründungsjahr der CSBW, wurden von ihr parallel zu ihrem Auf- und Ausbau keine herausgehobenen Fälle bearbeitet. Im Jahr 2022 waren es 4 herausgehobene Fälle, davon 2 bei Städten und Gemeinden sowie Landkreisen. Im Jahr 2023 waren 8 herausgehobene Fälle zu verzeichnen, davon 4 bei Städten und Gemeinden sowie Landkreisen. In den Jahren 2021 bis 2023 waren solche Fälle bei den Landesbehörden nicht zu verzeichnen.

Mit dem Übergang der Funktion und Aufgaben des CERT BWL (Computer Emergency Response Team der Landesverwaltung Baden-Württemberg) von der Landesoberbehörde IT Baden-Württemberg (BITBW) zur CSBW zum 1. Juli 2022 wurde die Etablierung der CSBW als zentrale Koordinierungs- und Meldestelle abgeschlossen. Damit ist das Jahr 2023 das erste, für das eine vollständige

Fallerfassung bei der CSBW vorliegt. Neben den im Vorangegangenen erwähnten „herausgehobenen Fällen“ i. S. d. CSG wurden darüber hinaus im Jahr 2023 in Baden-Württemberg insgesamt 224 Fälle von der CSBW aus den in der Frage genannten Zielgruppen erfasst, welche gemeldet wurden. In 214 Fällen hat die CSBW Landesbehörden und Städte, Gemeinden, Landkreise sowie Unternehmen in kommunaler Trägerschaft beispielsweise mit der Untersuchung einzelner maliziöser Dateien oder E-Mails, mit der Untersuchung von Verdachtsfällen kompromittierter Accounts oder mit der Analyse verdächtigen Verhaltens von IT-Systemen beraten und unterstützt.

Im Jahr 2024 war bisher ein herausgehobener Cyberangriff i. S. d. CSG zu verzeichnen, allerdings nicht im Bereich der Landesbehörden, Städte und Gemeinden sowie Landkreise. Im 1. Quartal unterstützte und beriet die CSBW insgesamt in 48 Fällen (Vorjahreszeitraum: 33).

Die CSBW teilt die Einschätzung des Bundesamts für Sicherheit in der Informationstechnik (BSI) und stuft die Cyberbedrohungslage in Deutschland ebenso als unverändert hoch ein. Für Baden-Württemberg bewertet die CSBW dies gleichermaßen. Dabei sind nur die wenigsten Cyberangriffe auch tatsächlich erfolgreich. Die allermeisten Angriffe auf Landes- und Kommunalverwaltungen werden bereits an den Gateways der zentralen IT-Dienstleister Komm.ONE für den Bereich der Kommunen und der BITBW im Bereich der Landesverwaltung automatisch detektiert und blockiert.

2. welcher finanzielle und personelle Aufwand erforderlich gewesen ist, um seit dem Jahr 2021 die aus schwerwiegenden Cyberangriffen resultierenden Schäden zu beseitigen und störungsfreie EDV-Systeme wiederherzustellen;

Zu 2.:

Die CSBW kann in einem herausgehobenen Fall Maßnahmen treffen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind. Dies sind beispielsweise forensische Maßnahmen, um das Ausmaß der Betroffenheit festzustellen und unter anderem die mögliche Verwendbarkeit von vorhandenen Backups zu überprüfen. Auch gehört die wichtige Unterstützung der betroffenen Einrichtung beim Krisenmanagement und bei der Krisenkommunikation dazu. Diese Maßnahmen stellen daher die Grundlage dar, um Systeme wiederaufzubauen oder wiederherstellen zu können. Der finanzielle und personelle Aufwand, der erforderlich gewesen ist, um die aus schwerwiegenden Cyberangriffen resultierenden Schäden zu beseitigen und störungsfreie EDV-Systeme wiederherzustellen, entsteht regelmäßig bei den betreffenden Stellen selbst und kann daher durch die CSBW nicht beziffert werden. Die Personal- und Sachkosten der CSBW, die im Rahmen der dargelegten Unterstützung bei der Bewältigung von Cyberangriffen nach dem CSG anfallen, sind durch die in den jeweiligen Staatshaushaltsplänen etatisierten Personal- und Sachausgaben abgedeckt und werden nicht gesondert ausgewiesen.

3. auf welchem Stand sich die Vernetzung staatlicher Einrichtungen, der Wirtschaft sowie von Wissenschaft und Forschung im Bereich der Cybersicherheit inzwischen befindet und welchen Zeitplan die Landesregierung dabei verfolgt;

Zu 3.:

Seit ihrer Gründung hat die CSBW die Vernetzung staatlicher Einrichtungen, der Wirtschaft sowie von Wissenschaft und Forschung im Bereich der Cybersicherheit vorangetrieben und verstetigt. Um die Cybersicherheit des Landes zu stärken, ist die Zusammenarbeit mit weiteren Akteurinnen und Akteuren unerlässlich. Aus diesem Grund befindet sich die CSBW in regelmäßigem fachlichen Austausch und arbeitet selbst am Aufbau entsprechender Strukturen. Die CSBW tauscht sich beispielsweise stetig aber auch anlassbezogen mit dem Landeskriminalamt Baden-Württemberg, dem Landesamt für Verfassungsschutz Baden-Württemberg, dem Sicherheitszentrum IT in der Finanzverwaltung Baden-Württemberg (SITiF BW), der Komm.ONE und den Rechenzentren des Landes aus. Darüber hinaus ist die CSBW mit allen anderen CERT der Länder und dem BSI in laufendem, meist täglichen Austausch.

Mit dem kommunalen Bereich wird über den operativen Bereich hinaus aktuell auch auf der strategischen Ebene über die Kommunalen Landesverbände eine Vernetzung vorbereitet. Mit Forschungseinrichtungen und Wirtschaftsakteuren steht die CSBW ebenfalls in einem Austausch.

Hinsichtlich der Zusammenarbeit und Vernetzung mit den Hochschulen und bw-InfoSec wird auf die Stellungnahme zur Ziffer 6 des Antrags der Abg. Alexander Salomon und Michael Joukov GRÜNE (Drucksache 17/4075) sowie auf die Stellungnahme zu den Ziffern 9 bis 11 des Antrags der Abg. Dennis Birnstock und Daniel Karrais u. a. FDP/DVP (Drucksache 17/4022) verwiesen.

Auch im Bereich der internationalen Kooperationen und Beziehungen besteht ein stetiger fachlicher Austausch. Die Vernetzungsaktivitäten werden anlass- und bedarfsgerecht ausgebaut und unterliegen keinem festen Zeitplan.

4. welche konkreten Beratungsangebote der Cybersicherheitsagentur den Kommunen im Verlauf des Jahres 2023 zur Verfügung gestellt werden konnten und auf welche Resonanz diese Angebote gestoßen sind;

Zu 4.:

Die CSBW hat seit ihrer Gründung ein vielfältiges Angebot an Schulungen und Präventionsmaßnahmen aufgebaut, das stetig weiterentwickelt wird und sich sehr guter Resonanz erfreut. Diese Angebote richten sich insbesondere an die Mitarbeitenden der Landes- und Kommunalverwaltung als Zielgruppe. Angeboten wird etwa eine Grundlagenschulung zur Cybersicherheit, welche sich an alle Mitarbeiterinnen und Mitarbeiter der Landesverwaltung und Kommunen richtet. Im Jahr 2023 fand die Grundlagenschulung 24-mal mit insgesamt rund 1 400 Teilnehmenden aus den Kommunen statt. Im Jahr 2024 wurde die Grundlagenschulung bereits 28-mal mit insgesamt 1 150 Teilnehmenden aus den Kommunen durchgeführt. Weitere 20 Termine mit voraussichtlich 1 000 Teilnehmenden sind bereits vereinbart.

Für Führungskräfte der Kommunen und der Landesverwaltung bietet die CSBW außerdem ein Schulungsangebot mit dem Titel „Cybersicherheit als Führungsaufgabe“ an. Diese ist nach der Grundlagenschulung die am zweithäufigsten angefragte Schulung der CSBW. Sie wurde im Jahr 2023 an insgesamt neun Terminen in der Kommunalverwaltung durchgeführt. Damit wurden insgesamt ca. 380 Personen erreicht. Für 2024 sind bereits 7 Schulungen mit Kommunen terminiert, 5 haben bereits stattgefunden. Daran nahmen 120 Personen teil.

Zudem wurde eine fünftägige Online-Schulung zum „BSI-IT-Grundschutz-Praktiker“ angeboten, wodurch 83 Personen zu BSI-IT-Grundschutz-Praktikern und -Praktikerinnen zertifiziert werden konnten, davon 32 aus Kommunen. Im Jahr 2024 wurden bereits zwei fünftägige BSI-IT-Grundschutz-Praktiker-Schulungen durchgeführt, zwei weitere sind geplant. Von den insgesamt 60 teilnehmenden Personen kamen 35 aus Kommunen.

Zusammengefasst konnte die CSBW im Jahr 2023 mit den verschiedenen Schulungen und Vorträgen bereits rund 1 700 Personen aus dem kommunalen Bereich sensibilisieren und schulen. Diese Zahlen hat die CSBW 2024 bereits im 1. Quartal nahezu erreicht.

Über die Schulungsangebote hinaus können Kommunen über die Lernplattform der CSBW kostenlos auf weitere Schulungs- und Sensibilisierungselemente wie Web-Based-Trainings, Erklärvideos, Factsheets und ein Serious Game (Lernspiel) zugreifen. Zudem entstand in Zusammenarbeit mit den Kommunalen Landesverbänden, Vertreterinnen und Vertretern aus Kommunen sowie der Komm.ONE der „Stufenplan Mindestsicherheitsniveau“. Damit wird das Ziel verfolgt, das Sicherheitsniveau weiter zu steigern und die Städte, Gemeinden und Landkreise beim Einstieg in den IT-Grundschutz des BSI zu unterstützen. Kommunen können mit einer Checkliste ihr Sicherheitsniveau erfassen und über die CSBW ausführliche IT-Sicherheitsanalysen durchführen lassen. Das Angebot wurde im Jahr 2023 mit

rund 50 Kommunen pilotiert, wovon 9 Kommunen eine IT-Sicherheitsanalyse durchführen ließen. Für das Jahr 2024 sind bereits 14 IT-Sicherheitsanalysen bei Kommunen abgeschlossen, im Gange oder terminiert.

Doch auch wenn Kommunen verdächtiges Verhalten in ihren Systemen feststellen, steht die CSBW mit Rat und Tat zur Seite. Über die Cyber-Ersthilfe BW können sich betroffene Kommunen rund um die Uhr an die CSBW wenden. Wie zu Ziffer 1 erläutert, wurden im Jahr 2023 durch die CSBW rund 50 Verdachtsfälle im kommunalen Umfeld untersucht und gegebenenfalls erforderliche Maßnahmen eingeleitet, von der Vorfallsteuerung über die Unterstützung bei der Krisenkommunikation bis hin zu einem Einsatz des MIRT und IT-forensischen Untersuchungen.

5. mit welchen darüber hinausgehenden Beratungsangeboten die Cybersicherheitsagentur weitere Zielgruppen wie zum Beispiel kleine und mittlere Unternehmen (KMU) erreicht hat;

Zu 5.:

Auf der Website *www.cybersicherheit-bw.de* stehen alle verfügbaren Angebote und die öffentlich zugänglichen Informationen der CSBW zum Abruf bereit. So kann das Informationsniveau zu Cybersicherheitsthemen auch bei weiteren Akteurinnen und Akteuren im Land verbessert werden. Factsheets, Erklärvideos sowie der Leitfaden zur Cybersicherheit und ein Prüfdokument für IT-Sicherheitsarchitekturen stehen dort auch kleinen und mittleren Unternehmen (KMU) zur Verfügung. Die bereits im Rahmen der Stellungnahme zu Ziffer 4 genannte Cyber-Ersthilfe BW mit ihrem 24/7-Beratungsangebot richtet sich auch an KMU. Die CSBW wird darüber hinaus auch häufiger für diverse Veranstaltungen angefragt und stellt, insbesondere. bei Berufsverbänden, ihre Angebote vor und sensibilisiert für das Thema Cybersicherheit.

6. wie der für das zweite Quartal 2023 geplante Roll-out der landesweiten Sensibilisierungskampagne zur Cybersicherheit verlaufen ist;

Zu 6.:

Die im Jahr 2022 gestartete landesweite Sensibilisierungskampagne der CSBW für die Landes- und Kommunalverwaltung wurde im Jahr 2023 ausgerollt und wird fortlaufend um weitere Produkte und Angebote ergänzt. Auf die Stellungnahme zu Ziffer 4 wird verwiesen. Außerdem erreichte die CSBW-Sommeraktion 2023 mit gezielten Informationen und Empfehlungen zu Cybersicherheitsrisiken auf Reisen beispielsweise tausende Personen in der Landes- und Kommunalverwaltung. Das neueste Kampagnenprodukt ist die Broschüre „Leitfaden zur Cybersicherheit“. Der Leitfaden spricht grundlegende Themen der Cybersicherheit an und liefert konkrete Empfehlungen, wie man sich vor den vielfältigen Gefahren im Cyberraum schützen kann. Der Leitfaden wurde in digitaler Form an die Landes- und Kommunalverwaltung versendet und kann auf der CSBW-Website heruntergeladen werden. Die Printversion wird bei Veranstaltungen und Schulungen ausgegeben.

7. ob und inwieweit die nach dem Haushaltsplan 2023 der Cybersicherheitsagentur zugewiesenen Personalstellen inzwischen vollständig besetzt werden konnten und welchen Fachabteilungen gegebenenfalls nicht besetzte Stellen zuzuordnen sind;

Zu 7.:

Der Cybersicherheitsagentur sind im Staatshaushaltsplan 2024 88,5 Stellen zugeordnet. Rund 80 Prozent der Stellen konnten mittlerweile besetzt werden. In allen Abteilungen sind noch vereinzelte Stellen unbesetzt, die Ausschreibungen hierzu laufen aktuell oder befinden sich in Vorbereitung.

8. ob und in welchem Umfang die Cybersicherheitsagentur im Rahmen ihrer Aufgaben externe Dienstleister einsetzt und welcher finanzielle Mehraufwand daraus gegebenenfalls resultiert.

Zu 8.:

Die CSBW arbeitet in unterschiedlichem Umfang mit externen Dienstleistern zusammen. Dies betrifft beispielsweise eine Unterstützung für den Fall, dass im Bereich der sehr zeitkritisch vorzunehmenden Forensik-Analysen mehrere größere Fälle gleichzeitig zu bewältigen sind und Ressourcenengpässe dringlichst vermieden werden müssen. Hierbei entstehen keine finanziellen Mehraufwände über die in den Staatshaushaltsplänen jeweils etatisierten Mittel hinaus.

Strobl

Minister des Inneren,
für Digitalisierung und Kommunen