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

17. Wahlperiode Eingang: 27.01.2023

Antrag

des Abg. Daniel Karrais u. a. FDP/DVP

Cybersicherheit in Baden-Württemberg

Der Landtag wolle beschließen,
die Landesregierung zu ersuchen

zu berichten,

1. wie viele Sicherheitslücken in der IT-Infrastruktur in der Landesverwaltung inkl. 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) 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 inkl. 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 seit Drucksache 17/483 erfolgt sind (bitte differenziert nach Art der Angriffe);

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 inkl. 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);

5. welche dieser 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 inkl. 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 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 inkl. 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 inkl. aller nachgeordneter Bereiche angesichts der aktuellen Bedrohungslage durch Cyberangriffe für ausreichend erachtet.

27.01.2023

Karrais, Goll, Weinmann, Dr. Rülke, Haußmann, Dr. Kern, Bonath, Brauer, Haag, Heitlinger, Hoher, Dr. Jung, Reith, Prof. Dr. Schweickert, Trauschel, FDP/DVP

B e g r ü n d u n g

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 8. 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.