Landtag von Baden-Württemberg **Drucksache 17 / 2225**
17. Wahlperiode **24.3.2022**

Kleine Anfrage

des Abg. Dr. Reinhard Löffler CDU

und

Antwort

des Ministeriums des Inneren, für Digitalisierung und Kommunen

Cybersicherheit auf kommunaler Ebene

Kleine Anfrage

Ich frage die Landesregierung:

1. Wie bewertet sie die aktuelle Cybersicherheit in den Kommunen des Landes?

2. In welchen Bereichen sieht sie Verbesserungsbedarf?

3. Welche Kommunen arbeiten mit einem Information Security Management System (ISMS) nach offiziellem Standard des Landes?

4. Welche Kommunen haben einen Informationssicherheitsbeauftragten benannt (bitte aufschlüsseln nach Beschäftigungsart: Vollzeit, Nebenfunktion oder extern)?

5. Welche Stellen evaluieren die Cybersicherheit in baden-württembergischen Kommunen?

6. Nach welchen Standards wird bei der Evaluierung nach Frage 5 vorgegangen und in welchen Intervallen finden diese Prüfungen statt?

7. Wie viele erfolgreiche Angriffe auf die IKT-Infrastruktur der Kommunen des Landes wurden nach Kenntnis der Landesregierung seit 2018 verzeichnet (bitte nach Jahr und Angriffsart aufschlüsseln; „erfolgreich“ bezeichnet hierbei mindestens die Einsatzunfähigkeit eines IKT-Systems oder den Abfluss von Daten)?

8. Welche Schäden wurden bei diesen Angriffen verursacht unter Angabe, in wie vielen Fällen Täter ermittelt werden konnten?

9. Können die Kommunen Erstattungen vom Land für die Kosten von Cyber- und Informationssicherheitsmaßnahmen erhalten?

Eingegangen: 24.3.2022 / Ausgegeben: 25.4.2022

10. Welche Unterstützungsangebote und Fördermöglichkeiten bietet das Land für die Kommunen für Cybersicherheit?

24.3.2022

Dr. Löffler CDU

Begründung

Seit Beginn des russischen Angriffskriegs gegen die Ukraine im Februar rückt das Thema Cybersicherheit zwingend in den Fokus. Bereits in den vergangenen Jahren wurde eine stetig wachsende Zahl von Cyberangriffen auf Infrastruktur und Kommunen des Landes verzeichnet. Da im Hinblick auf den aktuellen Konflikt mit einer Zunahme solcher Attacken zu rechnen ist, soll mit dieser Kleinen Anfrage geklärt werden, wie es um die Cybersicherheit baden-württembergischer Kommunen bestellt ist und wo im Zweifelsfall Verbesserungsbedarf besteht.

Antwort

Mit Schreiben vom 19. April 2022 Nr. IM7-0141-27/9 beantwortet das Ministerium des Inneren, für Digitalisierung und Kommunen im Einvernehmen mit dem Ministerium für Finanzen die Kleine Anfrage wie folgt:

1. Wie bewertet sie die aktuelle Cybersicherheit in den Kommunen des Landes?

2. In welchen Bereichen sieht sie Verbesserungsbedarf?

Zu 1. und 2.:

Die Bedrohungslage durch Cyberangriffe hat sich auch für die Kommunen deutlich verschärft. Angesichts der Komplexität der kommunalen IT-Infrastrukturen, des hohen Grads der Vernetzung und der Abhängigkeit der Verwaltung von IT-gestützten Verfahren sehen sich Kommunen vor der zunehmenden Herausforderung, den stetig wachsenden Anforderungen an ihre Cyber- und Informationssicherheit gerecht zu werden. Insoweit ist eine weitere Professionalisierung anzustreben.

Bei den Kommunen in Baden-Württemberg besteht ein heterogenes Niveau der Cyber- und Informationssicherheit. Manche Kommunen sind inhaltlich bereits weiter fortgeschritten und weisen gute Schutzvorkehrungen auf, andere jedoch weit weniger – und auch innerhalb einer Kommune kann es erhebliche Unterschiede geben. So sind beispielsweise die Landratsämter als Teil der sogenannten „EU-Zahlstelle“, welcher einen vom Land verantworteten, BSI-zertifizierten IT-Sicherheitsverbund darstellt, seit vielen Jahren mit den Anforderungen der BSI-Standards vertraut.

Aus Sicht des Landes ist wichtig, dass aktuelle Sicherheitskonzepte und eine Umsetzungsdokumentation der vorgegebenen technischen und organisatorischen Maßnahmen auf Grundlage der einschlägigen BSI-Standards vorliegen und den sich daraus ergebenden Schritten nachgekommen wird. Weiterhin sollten die Kommunen prüfen, im Zuge einer Standardisierung und Konsolidierung, möglichst viele Dienste zentral beim kommunalen Rechenzentrum, der Komm.ONE, zu betreiben, zumal der Rechenzentrumsbetrieb der Komm.ONE nach ISO27001 auf Basis IT-Grundschutz zertifiziert ist.

3. Welche Kommunen arbeiten mit einem Information Security Management System (ISMS) nach offiziellem Standard des Landes?

4. Welche Kommunen haben einen Informationssicherheitsbeauftragten benannt?

Zu 3. und 4.:

Eine Erhebung darüber, welche Kommunen über ein Informationssicherheitsmanagementsystem verfügen, liegen dem Innenministerium und den angefragten kommunalen Landesverbänden nicht vor.

Die Benennung eines Informationssicherheitsbeauftragten ist bei allen Landkreisen erfolgt. Im Zuge der Klärung künftiger Anforderungen aus der jüngst vom Bundesinnenministerium nach § 5 Onlinezugangsgesetzes (OZG) erlassenen IT-Sicherheitsverordnung Portalverbund (ITSiV-PV) wird zu den offenen Fragen eine entsprechende Abfrage bei den Kommunen erfolgen.

5. Welche Stellen evaluieren die Cybersicherheit in baden-württembergischen Kommunen?

6. Nach welchen Standards wird bei der Evaluierung nach Frage 5 vorgegangen und in welchen Intervallen finden diese Prüfungen statt?

Zu 5. und 6.:

Die Absicherung der Informationstechnik in den Kommunen ist Bestandteil der kommunalen Selbstverwaltung. Entscheidet sich eine Kommune für die Evaluierung ihrer Cybersicherheit, steht die Cybersicherheitsagentur Baden-Württemberg (CSBW) den Kommunen perspektivisch beratend zur Seite.

Eine wesentliche Rolle für die Ausgestaltung der Cyber- und Informationssicherheit in den Kommunen spielt der zentrale IT-Dienstleister Komm.ONE. Dort werden eine Vielzahl von IT-Lösungen und Fachanwendungen für die Kommunen betrieben. Zwischen dem Innenministerium, der BITBW, der CSBW und Komm.ONE wird eine regelmäßige und gute Zusammenarbeit gepflegt, etwa zur Abstimmung gemeinsamer Maßnahmen im Bereich der technischen IT-Sicherheit oder zur Sicherheit ebenenübergreifender Verfahren und Prozesse (z. B. EU-Zahlstelle, Wahlen, Fachverfahren). Durch verschiedene Vorgaben seitens des Landes (vgl. nur § 16 des E-Government-Gesetzes Baden-Württemberg) sowie des Bundes (vgl. die gemäß § 5 des Onlinezugangsgesetzes erlassene IT-Sicherheitsverordnung Portalverbund) werden aktuell gemeinsame Vorgehensweisen und Standards zukunftsweisend verbindlich festgelegt.

7. Wie viele erfolgreiche Angriffe auf die IKT-Infrastruktur der Kommunen des Landes wurden nach Kenntnis der Landesregierung seit 2018 verzeichnet (bitte nach Jahr und Angriffsart aufschlüsseln; „erfolgreich“ bezeichnet hierbei mindestens die Einsatzunfähigkeit eines IKT-Systems oder den Abfluss von Daten)?

8. Welche Schäden wurden bei diesen Angriffen verursacht unter Angabe, in wie vielen Fällen Täter ermittelt werden konnten?

Zu 7. und 8.:

Die statistische Erfassung von Straftaten erfolgt bei der Polizei Baden-Württemberg anhand der Polizeilichen Kriminalstatistik (PKS). Bei der PKS handelt es sich um eine sogenannte Ausgangsstatistik, in der strafrechtlich relevante Sachverhalte nach der polizeilichen Sachbearbeitung vor Abgabe an die Strafverfolgungsbehörden erfasst werden. Die Fallerfassung erfolgt nach den bundeseinheitlichen „Richtlinien für die Führung der Polizeilichen Kriminalstatistik“. Eine eigenständige Erfassung von Cyberangriffen auf kommunale Informations- und Kommunikationstechnik erfolgt im Zusammenhang mit der PKS nicht. Vor diesem Hintergrund können keine belastbaren Aussagen im Sinne der Fragestellungen getroffen werden.

Im Übrigen wird auf die Antworten zu den Ziffern 1 bis 3 des Antrags der FDP/DVP-Fraktion (Drucksache 17/483) verwiesen.

9. Können die Kommunen Erstattungen vom Land für die Kosten von Cyber- und Informationssicherheitsmaßnahmen erhalten?

10. Welche Unterstützungsangebote und Fördermöglichkeiten bietet das Land für die Kommunen für Cybersicherheit?

Zu 9. und 10.:

Das Innenministerium verfolgt – vorbehaltlich der zur Verfügung stehenden Haushaltsmittel – verschiedene Vorhaben und Maßnahmen, um die Cyber- und Informationssicherheit ebenenübergreifend auf einem gemeinsamen Mindestsicherheitsniveau zu gewährleisten. Hierunter fallen sowohl konkrete operative Unterstützungsangebote im Einzelfall als auch konzeptionelle und strategische Maßnahmen, mit denen eine zukunftsfähige und leistungsstarke staatliche Cybersicherheitsarchitektur langfristig sichergestellt ist.

So ist geplant, dass die CSBW noch in diesem Jahr eine übergreifende Plattform für den Warn- und Informationsdienst in Betrieb nimmt. Hierüber werden tagesaktuell Warnmeldungen zu Themen der Cybersicherheit, Schwachstellenwarnungen sowie technische Handlungsempfehlungen bereitgestellt. Unmittelbar nach Inbetriebnahme wird der Dienst auch für die Kommunen freigeschaltet werden.

Daneben ist geplant, Cyber- und Informationssicherheitsexperten der Städte, Landkreise und Gemeinden mittels einer technischen Austauschplattform im Alltag zu vernetzen, um den übergreifenden Fachaustausch zu ermöglichen. Sofern auf Seiten der Kommunen relevante Sicherheitslücken erkannt werden, steht die CSBW für Fragen und konkrete Hilfestellungen zur Verfügung.

Im Laufe des Jahres 2022 startet die CSBW eine landesweite Sensibilisierungskampagne zur Cybersicherheit, welche auch die Städte, Landkreise und Gemeinden als Zielgruppe erfasst. Dazu plant die CSBW u. a. im Bereich Prävention den Kommunen diverse E-Learning-Angebote und Schulungsvideos auf einer eigenen Lernplattform frei zur Verfügung zu stellen, ebenso wie Materialien, Checklisten und Unterlagen. Der Schulungs-Hub als ein Teil der zukünftigen CSBW-Webseite wird zu bestehenden Schulungsangeboten im Land auch die Gemeinden, Städte und Landkreise informieren und diese Angebote vermitteln. Das in der Landesverwaltung zentral und sehr erfolgreich umgesetzt Schulungsangebot „BSI-zertifizierte/-r IT-Grundschutzpraktiker/-in“, das sich an künftige Informationssicherheitsbeauftragte adressiert, soll den Kommunen ebenfalls zugänglich gemacht werden.

Um den Herausforderungen der Cybersicherheit sowohl auf kommunaler als auch auf Landesebene zukunftsorientiert zu begegnen, hat die Landesregierung im Dezember 2021 zudem eine Cybersicherheitsstrategie beschlossen. Durch die Festlegung konkreter Ziele und Maßnahmen wird ein gemeinsamer verbindlicher Rahmen für die Cybersicherheit in Baden-Württemberg geschaffen.

Bei der Umsetzung der Anforderungen der o. a. IT-Sicherheitsverordnung Portalverbund zu § 5 des Onlinezugangsgesetzes wird das Innenministerium intensiv mit den Kommunen zusammenarbeiten, um die sich aus der Regelung ergebenden Anforderungen zur Absicherung der mit dem Portalverbund verbundenen IT-Komponenten effektiv und effizient umzusetzen.

Strobl

Minister des Inneren,
für Digitalisierung und Kommunen