Bayerischer Landtag

18. Wahlperiode 28.01.2021 Drucksache 18/12316

Schriftliche Anfrage

der Abgeordneten **Martin Hagen, Albert Duin FDP**
vom 15.12.2020

Cybersicherheit in den Kommunen

Ich frage die Staatsregierung:

1.1 Wie bewertet die Staatsregierung den aktuellen Stand der Cybersicherheit in den Kommunen? ... 3

1.2 In welchen Bereichen haben die Kommunen nach Ansicht der Staatsregierung Verbesserungsbedarf? ... 3
1.3 Welche der Kommunen betreiben nach Kenntnis der Staatsregierung ein Information Security Management System (ISMS) nach einem offiziellen Standard? ... 3

2.1 Welche Kommunen haben einen Informationssicherheitsbeauftragten benannt (bitte aufschlüsseln nach Beschäftigungsart: Vollzeit, Nebenfunktion oder extern)? ... 3
2.2 Welche Stellen in Bayern prüfen und evaluieren die Cybersicherheit in den Kommunen? ... 3
2.3 In welchen Intervallen findet eine Prüfung statt? ... 3

3.1 Wie viele erfolgreiche Angriffe auf die IKT-Infrastruktur der bayerischen Kommunen wurden nach Kenntnis der Staatsregierung seit 2015 verzeichnet (bitte nach Jahr und Angriffsart aufschlüsseln; Erfolg bezeichnet hierbei mindestens die Verschlüsselung/Einsatzunfähigkeit eines IKT-Systems oder den Abfluss von Daten)? ... 3
3.2 Welche Schäden haben diese Angriffe jeweils verursacht? ... 3
3.3 Bei welchem Prozentsatz dieser Angriffe konnte ein Täter ermittelt werden? ... 3

4.1 Wie viele meldepflichtige Datenschutzvorfälle nach der Datenschutz-Grundverordnung (DSGVO) gab es im Zusammenhang mit Angriffen auf die IKT-Infrastruktur der Kommunen bisher (bitte nach Jahr aufschlüsseln)? ... 4
4.2 Wie sehen die Kommunikations- und Informationswege im Falle eines Cyberangriffs auf eine Kommune aus? ... 4
4.3 In wie vielen Fällen wurde das LSI hinzugezogen? ... 4

5.1 In wie vielen Fällen wurde nach Kenntnis der Staatsregierung durch die Kommunen ein externer Dienstleister hinzugezogen (bitte aufschlüsseln nach Dienstleister)? ... 4
5.2 Wie bewertet die Staatsregierung die Gefahrenlage hinsichtlich gezielter Angriffe auf die IKT-Infrastruktur der Kommunen aktuell? ... 4
5.3 Welche Unterstützungsangebote und Fördermöglichkeiten bietet der Freistaat für die Kommunen zur Stärkung der Cyber- und Informationssicherheit an? ... 4

6.1 Welche Haushaltmittel stehen hierfür zur Verfügung (seit 2015, bitte nach Jahr aufschlüsseln)? ... 5

6.2 Wie hoch war der tatsächliche Mittelabfluss (seit 2015, bitte nach Jahr aufschlüsseln)? ... 5

Hinweis des Landtagsamts: Zitate werden weder inhaltlich noch formal überprüft. Die korrekte Zitierweise liegt in der Verantwortung der Fragestellerin bzw. des Fragestellers sowie der Staatsregierung.

6.3 Können die Kommunen Erstattungen vom Land für die Kosten von Cyber- und Informationssicherheitsmaßnahmen erhalten? 5

7.1 Welche Art von Beratung steht den Kommunen durch das LSI zur Verfügung? 5

7.3 Entspricht das Zertifikat dem Level der Basis-Absicherung bzw. ISO 27001? 6

7.2 Welche Kommunen haben das Zertifikat „Kommunale IT-Sicherheit“ des LSI erhalten? 6

8.1 Entspricht das Zertifikat dem Level der BSI-Standardabsicherung (BSI = Bundesamt für Sicherheit in der Informationstechnik)? 6

8.2 Wenn das Niveau unter der BSI-Standardabsicherung liegt, wieso gelten für die Kommunen niedrigere Anforderungen als für andere Verwaltungsbereiche? 6

8.3 Inwieweit beteiligt sich das Staatsministerium für Digitales an der Fortschreibung der Bayerischen Cybersicherheitsstrategie? 6

Antwort

des Staatsministeriums der Finanzen und für Heimat unter Einbindung des Staatsministeriums des Innern, für Sport und Integration und des Staatsministeriums für Digitales
vom 18.01.2021

1.1 Wie bewertet die Staatsregierung den aktuellen Stand der Cybersicherheit in den Kommunen?
1.2 In welchen Bereichen haben die Kommunen nach Ansicht der Staatsregierung Verbesserungsbedarf?
1.3 Welche der Kommunen betreiben nach Kenntnis der Staatsregierung ein Information Security Management System (ISMS) nach einem offiziellen Standard?
2.1 Welche Kommunen haben einen Informationssicherheitsbeauftragten benannt (bitte aufschlüsseln nach Beschäftigungsart: Vollzeit, Nebenfunktion oder extern)?
2.2 Welche Stellen in Bayern prüfen und evaluieren die Cybersicherheit in den Kommunen?
2.3 In welchen Intervallen findet eine Prüfung statt?

Kommunale Behörden haben aufgrund Art. 11 Bayerisches E-Government-Gesetz (BayEGovG) geeignete technische und organisatorische Maßnahmen zum Schutz ihrer IT-Systeme zu treffen und die hierzu erforderlichen Informationssicherheitskonzepte zu erstellen. Sie entscheiden im Rahmen der durch das Selbstverwaltungsrecht garantierten Organisationshoheit eigenverantwortlich, auf welche Art und Weise sie dieser gesetzlichen Aufgabe nachkommen. Die Erfahrungen des Landesamts für Sicherheit in der Informationstechnik (LSI) zeigen diesbezüglich ein hohes Beratungsinteresse der Kommunen, das die Vielfalt der kommunalen Gegebenheiten wie Größe, Personal, Finanzmittel, Fachverfahren, Unterstützung durch Landratsämter usw. widerspiegelt. Alle Kreisverwaltungsbehörden haben aufgrund der Anschlussbedingungen an das Bayerische Behördennetz einen Informationssicherheitsbeauftragten benannt und dem LSI mitgeteilt.

Das LSI bietet den bayerischen Kommunen an, mit dem Siegel „Kommunale IT-Sicherheit“ auf Basis einer Selbstauskunft eine Mindestabsicherung in der Informationssicherheit nachzuweisen. Das Siegel „Kommunale IT-Sicherheit“ ist in der Regel zwei Jahre gültig und bietet gerade auch kleineren bayerischen Städten, Märkten und Gemeinden die Möglichkeit, eine individuelle Einschätzung des LSI zur Informationssicherheit und fachliche Unterstützung zu erhalten. So wird erreicht, dass mit dem jeweiligen Informationssicherheitskonzept die wichtigsten Aspekte adressiert werden und somit die gesetzeskonforme Einführung eines Informationssicherheitskonzeptes belegt ist. Im Übrigen besteht keine Meldepflicht bzw. Prüfung der Kommunen im Sinne der Fragestellung durch das LSI oder andere staatliche Behörden.

Die mit der Fragestellung erbetene Einschätzung zur IT-Sicherheit der Kommunen ist ohnedies nicht valide zu treffen, weil sich Angriffsszenarien, Sicherheitslücken und Bedrohungen ebenso wie der der Stand der Digitalisierung in der einzelnen Kommune nahezu täglich ändern.

3.1 Wie viele erfolgreiche Angriffe auf die IKT-Infrastruktur der bayerischen Kommunen wurden nach Kenntnis der Staatsregierung seit 2015 verzeichnet (bitte nach Jahr und Angriffsart aufschlüsseln; Erfolg bezeichnet hierbei mindestens die Verschlüsselung/Einsatzunfähigkeit eines IKT-Systems oder den Abfluss von Daten)?
3.2 Welche Schäden haben diese Angriffe jeweils verursacht?
3.3 Bei welchem Prozentsatz dieser Angriffe konnte ein Täter ermittelt werden?

Nach Auskunft des fachlich zuständigen Staatsministeriums des Innern, für Sport und Integration (StMI) ist weder in der Polizeilichen Kriminalstatistik (PKS) noch im polizeilichen Vorgangssystem IGVP eine automatisierte Recherche nach „bayerischen Kommunen“ möglich. Aus diesem Grund kann eine valide Aussage im Sinne der Fragestellung

nicht getroffen werden. Eine manuelle Auswertung wäre mit unverhältnismäßig großem Aufwand verbunden.

4.1 Wie viele meldepflichtige Datenschutzvorfälle nach der Datenschutz-Grundverordnung (DSGVO) gab es im Zusammenhang mit Angriffen auf die IKT-Infrastruktur der Kommunen bisher (bitte nach Jahr aufschlüsseln)?

Die in Art. 33 DSGVO vorgesehene Meldung von Verletzungen des Schutzes personenbezogener Daten erfolgt vom Verantwortlichen, d. h. in diesem Fall der Kommune, unmittelbar an die (unabhängige) Aufsichtsbehörde – im Fall von Kommunen an den Landesbeauftragten für den Datenschutz gemäß Art. 15 Bayerisches Datenschutzgesetz. Die Staatsregierung hat daher keine Kenntnis über die erbetenen Zahlen.

4.2 Wie sehen die Kommunikations- und Informationswege im Falle eines Cyberangriffs auf eine Kommune aus?

Wenn dem LSI Angriffe auf oder Gefährdungen für eine oder mehrere Kommunen bekannt werden, werden diese informiert und zu möglichen Abwehrmaßnahmen beraten. Zudem ergreift das LSI gemeinsam mit dem BayernServer eigene Abwehrmaßnahmen, soweit der Angriff über das Bayerische Behördennetz läuft.

Kommunen sind im Allgemeinen nicht verpflichtet, IT-Sicherheitsvorfälle an das LSI zu melden. Soweit eine Kommune an das Behördennetz angebunden ist, besteht hingegen eine Meldepflicht. Bei der Vorfallsbearbeitung werden bei Bedarf das Landratsamt oder auch Dienstleister der Kommune mit eingebunden. Im Zuge der Vorfallbearbeitung wird die Kommune auch über erweiterte Meldepflichten (BayLfD) bzw. die Möglichkeit einer Strafanzeige informiert.

4.3 In wie vielen Fällen wurde das LSI hinzugezogen?

Das LSI wurde seit der Gründung bei circa 500 Vorfällen in Kommunen hinzugezogen. Dabei wurden die Vorfälle jeweils analysiert und, soweit erforderlich, in Abstimmung mit der jeweiligen Kommune Gegenmaßnahmen eingeleitet bzw. empfohlen.

5.1 In wie vielen Fällen wurde nach Kenntnis der Staatsregierung durch die Kommunen ein externer Dienstleister hinzugezogen (bitte aufschlüsseln nach Dienstleister)?

Dazu liegen der Staatsregierung keine Informationen vor.

5.2 Wie bewertet die Staatsregierung die Gefahrenlage hinsichtlich gezielter Angriffe auf die IKT-Infrastruktur der Kommunen aktuell?

Generell kann die Bedrohungslage für Kommunen als hoch eingestuft werden. Auch kleine Kommunen sind ohne funktionierende IT nicht arbeitsfähig. Mit baukastenartiger Schadsoftware und öffentlich verfügbaren Datenbanken von angreifbaren Systemen können Angreifer gerade auch kleine Kommunen ins Visier nehmen.

5.3 Welche Unterstützungsangebote und Fördermöglichkeiten bietet der Freistaat für die Kommunen zur Stärkung der Cyber- und Informationssicherheit an?

Das LSI bietet den Kommunen Unterstützung in Form von Beratung (per E-Mail, Telefon, Videokonferenz oder vor Ort), dem Siegel „Kommunale IT-Sicherheit“, der Handreichung zum Notfallmanagement, einer Online-Sensibilisierungsplattform (Awareness-Kurs), eines Warn- und Informationsdienstes, Unterstützung bei Vorfällen, Handreichungen zu Fachthemen (LSI-Infos) sowie Informationsveranstaltungen.

Ein Anschluss an das bayerische Behördennetz erhöht die kommunale IT-Sicherheit deutlich und wird vom Staatsministerium der Finanzen und für Heimat (StMFH) unterstützt (siehe Antwort auf Frage 6.3).

Neben der Unterstützung des LSI erhalten bayerische Kommunen, die ein hinreichendes ISMS nach Beschlusslage des IT-Planungsrats einführen, seit 2015 eine staatliche Förderung. Das Förderprogramm zur Implementierung eines Informationssicherheits-Managementsystems (ISMS) bei den kommunalen Gebietskörperschaften trägt nach Auskunft des fachlich zuständigen StMI dazu bei, das IT-Sicherheitsniveau bei den bayerischen Kommunen rasch und nachhaltig zu erhöhen. Insgesamt konnten seit dessen Einführung in 2015 die Förderanträge von 335 Kommunen, kommunalen Zusammenschlüssen und öffentlich-rechtlich organisierten Unternehmen genehmigt werden.

6.1 Welche Haushaltmittel stehen hierfür zur Verfügung (seit 2015, bitte nach Jahr aufschlüsseln)?

6.2 Wie hoch war der tatsächliche Mittelabfluss (seit 2015, bitte nach Jahr aufschlüsseln)?

	2015	2016	2017	2018	2019	2020
HH-Ansatz abzgl. Sperre (Tsd. Euro)	270	1.085	1.000	3.400	2.700	2.700
Gebundene Mittel (Euro)	100.548,48	523.100,72	1.645.713,00	1.071.203,94	351.705,06	512.684,80

Nach der geltenden ISMS-Förderrichtlinie kann nach Auskunft des StMI die Auszahlung erst nach vollständiger Implementierung des ISMS beantragt werden, die spätestens 24 Monate nach Erlass des Förderbescheids beendet sein muss. Die tatsächliche Auszahlung der veranschlagten Mittel erfolgt daher regelmäßig erst 18–24 Monate nach Bewilligung der Fördermittel.

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

Das Bayerische Behördennetz ist das Rückgrat für die sichere Kommunikation der staatlichen Verwaltung und der Kommunen. Die angeschlossenen Kommunen profitieren zudem von den zentralen Sicherheitsmaßnahmen des LSI. Zu diesem Zweck können alle Landratsämter Haushaltsmittel i. H. v. bis zu 70.000 Euro zum Auf- bzw. Ausbau von Kommunalen Behördennetzen beantragen; bislang (Stand: Dezember 2020) wurden über 1,5 Mio. Euro an 30 Landratsämter zugewiesen. Mit den zugewiesenen Mitteln wird regelmäßig auch eine signifikante Verbesserung der IT-Sicherheit erreicht.

7.1 Welche Art von Beratung steht den Kommunen durch das LSI zur Verfügung?

Das LSI berät die Kommunen in Bezug auf den Schutz der IT-Infrastruktur, der Organisation der IT-Sicherheit, Sicherheitsrichtlinien, Informationssicherheitsmanagementsysteme, Audits und Zertifizierung, Awareness-Kampagnen, Penetrationstests, Notfallmanagement, zur aktuellen Bedrohungslage und allen weiteren Themen der kommunalen Informationssicherheit. Dieses Angebot wurde von den Kommunen alleine im Jahr 2020 über 600-mal genutzt.

Folgende Kommunen haben das Siegel „Kommunale IT-Sicherheit“ bisher erhalten: Adelsdorf, Altenmarkt a. d. Alz, Alzenau, Aschau a. Inn, Bad Aibling, Beilngries, Berngau, Bessenbach, Bibertal, Bobingen, Burghaslach, Chieming, Dettelbach, Ebensfeld, Engelsberg, Eschlkam, Flintsbach a. Inn, Fraunberg, Freyung, Fridolfing, Grabenstätt, Grassau, Große Kreisstadt Erding, Gunzenhausen, Haar, Haarbach, Hebertshausen, Hemau, Herzogenaurach, Hilpoltstein, Hohenau, Inzell, Kirchanschöring, Klingenberg a. Main, Kolitzheim, Landsberg am Lech, Landratsamt (LRA) Garmisch-Partenkirchen, LRA Landsberg am Lech, LRA Neu-Ulm, LRA Starnberg, Maisach, Markt Igensdorf, Markt Maroldsweisach, Markt Postbauer-Heng, Marktbreit, Moorenweis, Mühlhausen, Murnau a. Staffelsee, Neufahrn b. Freising, Neunburg vorm Wald, Neunkirchen a.

Brand, Neuötting, Neuried, Neu-Ulm, Nördlingen, Nußdorf, Palling, Pappenheim, Pettendorf, Petting, Pfarrkirchen, Pilsach, Pocking, Reit im Winkl, Rohr, Ruderting, Ruhpolding, Schleching, Schnaitsee, Schwangau, Schwebheim, Seeon-Seebruck, Sengenthal, Sennfeld, Siegsdorf, Solnhofen, Soyen, Stadt Kelheim, Stadt Traunstein, Surberg, Tacherting, Tittmoning, Traunreut, Trostberg, Übersee, Üchtelhausen, Unterwössen, Utting am Ammersee, Valley, Veitshöchheim, Verwaltungsgemeinschaft Bergen (Bergen, Vachendorf), Verwaltungsgemeinschaft Burgbernheim, Verwaltungsgemeinschaft Eichstätt, Verwaltungsgemeinschaft Geisenfeld, Verwaltungsgemeinschaft Ichenhausen, Verwaltungsgemeinschaft Marquartstein, Verwaltungsgemeinschaft Mitterteich (Stadt Mitterteich), Verwaltungsgemeinschaft Neumarkt i. d. Opf., Verwaltungsgemeinschaft Obing, Verwaltungsgemeinschaft Offingen (Gundremmingen, Markt Offingen, Rettenbach), Verwaltungsgemeinschaft Rotthalmünster (Malching, Markt Rotthalmünster), Verwaltungsgemeinschaft Stadtprozelten (Altenbuch, Stadt Stadtprozelten), Verwaltungsgemeinschaft Unterneukirchen, Verwaltungsgemeinschaft Volkach (Nordheim a. Main, Sommerach, Stadt Volkach), Verwaltungsgemeinschaft Waging am See (Taching a. See, Markt Waging a. See, Wonnneberg), Verwaltungsgemeinschaft Wiesentheid, Verwaltungsgemeinschaft Zolling (Attenkirchen, Haag a. d. Amper, Wolfersdorf, Zolling), Vierkirchen, Vohburg a. d. Donau, Waldbüttelbrunn, Wallgau, Wegscheid, Weiden und Wunsiedel.

7.3 Entspricht das Zertifikat dem Level der Basis-Absicherung bzw. ISO 27001?
7.2 Welche Kommunen haben das Zertifikat „Kommunale IT-Sicherheit“ des LSI erhalten?
8.1 Entspricht das Zertifikat dem Level der BSI-Standardabsicherung (BSI = Bundesamt für Sicherheit in der Informationstechnik)?
8.2 Wenn das Niveau unter der BSI-Standardabsicherung liegt, wieso gelten für die Kommunen niedrigere Anforderungen als für andere Verwaltungsbereiche?

Das Siegel ist unabhängig von einem ISMS-Standard. Bei der Entwicklung des Siegels „Kommunale IT-Sicherheit“ wurden die bei bayerischen Kommunen verbreiteten ISMS-Standards in Bezug auf den Umfang der jeweils behandelten Informationssicherheitsaspekte verglichen. Das Siegel berücksichtigt die grundlegenden Fragen der Informationssicherheit, die in der Schnittmenge der betrachteten Standards abgedeckt sind. Das Siegel beruht auf einer Selbstauskunft und bestätigt der Kommune darauf beruhend die Konformität nach Art. 11 Abs. 1 Satz 2 BayEGovG. Das Siegel wird regelmäßig, unter Berücksichtigung der Sicherheitslage und Angemessenheit, fortentwickelt. Es ist daher nicht mit dem BSI IT-Grundschutz oder ISO 270001 gleichzusetzen. Die Grundlage für die Anforderungen an die Kommunen in Bayern ergibt sich aus Art. 11 BayEGovG. Gefordert sind angemessene technische und organisatorische Maßnahmen sowie ein Informationssicherheitskonzept.

8.3 Inwieweit beteiligt sich das Staatsministerium für Digitales an der Fortschreibung der Bayerischen Cybersicherheitsstrategie?

Das Staatsministerium für Digitales beteiligt sich über die einschlägigen Gremien und Steuerungskreise und setzt auch eigene Akzente, wie bspw. mit der Initiative „Online – aber sicher“!