Bayerischer Landtag

18. Wahlperiode 07.12.2021 Drucksache 18/18056

Schriftliche Anfrage

der Abgeordneten **Benjamin Adjei, Johannes Becher BÜNDNIS 90/DIE GRÜNEN**
vom 30.08.2021

IT-Sicherheit in bayerischen Kommunen II – Management und Zertifizierung

Anfang Juli hat ein Cyber-Angriff auf die Kommunalverwaltung von Anhalt-Bitterfeld zum Ausrufen des ersten Cyber-Katastrophenfalls in Deutschland geführt. Solche Angriffe sind leider keine Seltenheit mehr. Immer mehr Kommunalverwaltungen und Einrichtungen in kommunaler und staatlicher Hand werden in den letzten Jahren Ziel und Opfer von gezielten Cyber-Attacken. Der Schaden dabei ist jedes Mal immens. Im Fall von Anhalt-Bitterfeld war die Verwaltung über zwei Wochen nicht in der Lage, ihre für manche Menschen dringend notwendigen Dienste wie Ausbezahlung von Sozial- und Unterhaltsleistungen zu leisten (https://www.dw.com/de/katastrophenfall-cyberattacke-legt-landkreis-lahm/a-58227033).

Wir fragen die Staatsregierung:

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.

Antwort

des Staatsministeriums der Finanzen und für Heimat im Einvernehmen mit dem Staatsministerium des Innern, für Sport und Integration
vom 29.09.2021

1.1 Welche Angebote stellt das Landesamt für Sicherheit in der Informationstechnik (LSI) für bayerische Kommunen bereit?
1.2 Wie gut werden diese Angebote von den Kommunen angenommen?
1.3 Plant die Staatsregierung den Umfang dieser Angebote (quantitativ oder qualitativ) auszuweiten?

Gegenüber den bayerischen Kommunen wird das LSI sowohl in der Rolle eines Kommunal-CERT[1] als auch in (herstellerunabhängiger) beratender Funktion tätig. Das LSI bietet insoweit Beratungen insbesondere zu sicherer IT-Infrastruktur, Organisation der IT-Sicherheit, Sicherheitsrichtlinien, Informationssicherheitsmanagementsysteme, Audits und Zertifizierungen, Awareness-Kampagnen, Penetrationstests, Notfallmanagement sowie zur aktuellen Bedrohungslage (z. B. mittels speziell für Kommunen angepasster Warnmeldungen). Auf einige Schwerpunkte in der Arbeit des LSI wird im Folgenden näher eingegangen:

Das LSI bietet kleineren und mittleren Kommunen an, mit dem Siegel „Kommunale IT-Sicherheit“ auf Basis einer Selbstauskunft ihre Mindestabsicherung in der Informationssicherheit nachzuweisen. Außerdem wird eine Handreichung zum IT-Notfallmanagement angeboten. Mit den „LSI-Infos“, werden zielgruppenspezifische Informationen an die Kommunen herausgegeben, die einen relativ kurzen Überblick zu diversen Fragestellungen der IT-Sicherheit bieten. Darüber hinaus werden seit Dezember 2020 allen kommunalen Verwaltungen Sensibilisierungskurse zur kostenlosen Nutzung in einem Webportal angeboten. Zu diesem Portal haben sich bis Anfang September 2021 schon 457 Gemeinden, 59 Landratsämter und 4 Bezirksverwaltungen angemeldet.

Mit Sicherheitskonferenzen und Thementagen bietet das LSI in den einzelnen Regierungsbezirken eine kommunale Informations- und Austauschplattform. In einem -Corona-bedingt -rein digital durchgeführten Durchgang im ersten Halbjahr 2021 konnten hierbei zuletzt mit acht Veranstaltungen 650 kommunale Ansprechpartner erreicht werden. Im Rahmen der Bayerischen Verwaltungsschule beteiligt sich das LSI außerdem an der Ausbildung von kommunalen Informationssicherheitsbeauftragten.

Bei der Bewältigung von konkreten IT-Sicherheitsvorfällen werden die bayerischen Kommunen vom LSI unbürokratisch und fachkundig unterstützt. Das LSI bietet den Kommunen ferner an, über konkrete, im Internet detektierbare Sicherheitslücken in den von ihnen eingesetzten Systemen gewarnt zu werden. Davon machen aktuell 320 Kommunen direkt Gebrauch. Die Detektion findet in enger Zusammenarbeit mit dem CERT-Bund am BSI statt. Etwaige Hinweise auf Sicherheitslücken werden vom LSI unmittelbar in aufbereiteter Form an die Kommunen weitergegeben.

Die Beratung der Kommunen ist weiterhin eine Schwerpunktaufgabe des LSI.

2.1 Wie viele Kommunen haben bisher noch keine Leistungen des LSI in Anspruch genommen?
2.2 Wie will die Staatsregierung diese Kommunen zu einer Inanspruchnahme der Leistungen des LSI motivieren?
2.3 Wie bewertet die Staatsregierung die Inanspruchnahme der Angebote durch die Kommunen?

Das breite Informationsangebot des LSI wird von vielen Kommunen in Bayern genutzt. Beispielsweise erreichen die Warnmeldungen zu aktuellen kritischen Bedrohungen des LSI alle bayerischen Kommunen – Bezirke, Landkreis und Gemeinden. Aufgrund der organisatorischen Heterogenität der bayerischen Kommunen im Bereich des IT-Betriebs und der Informationssicherheit ist der Beratungsbedarf bezüglich Umfang und Häufigkeit sehr unterschiedlich. Das LSI ist für alle Kommunen ansprechbar.

Das LSI will durch das konsequente Weiterentwickeln praxisnaher Beratungsangebote, regelmäßige Informationsveranstaltungen sowie zusätzlicher, techniknaher

1 Computer Emergency Response Team

Bereitstellung von Schadcodeinformationen die Kommunen in ganzer Breite bei der Steigerung ihres IT-Sicherheitslevels unterstützen. Die finanzielle Unterstützung des StMFH zum Ausbau kommunaler Behördennetze oder das Förderverfahren des StMI zur Implementierung zertifizierbarer ISMS, bei dem sich die Förderung erhöht, wenn die Kommune das Siegel „Kommunale IT-Sicherheit“ erworben hat, sind zudem Beispiele für Maßnahmen, die das attraktive Beratungsangebot des LSI flankieren.

Durch den Warn- und Informationsdienst und durch Einladungen zu Informationsveranstaltungen werden alle Kommunen durch das LSI erreicht. Dass nicht alle Kommunen weitergehende Informationsangebote des LSI nutzen, ist in dem unterschiedlichen kommunalen Vorgehen im IT-Bereich begründet und aufgrund der kommunalen Selbstverwaltung zu respektieren.

3.1 Wie viele Kommunen in Bayern haben das Siegel „Kommunale IT-Sicherheit“ des LSI bisher noch nicht erhalten?
3.2 Aus welchen Gründen haben nicht alle Kommunen das Siegel „Kommunale IT-Sicherheit“ erhalten?
3.3 Welche konkreten Schritte unternimmt die Staatsregierung, um zu erreichen, dass alle Kommunen das Siegel „Kommunale IT-Sicherheit“ des LSI erhalten?

Im Rahmen der kommunalen Selbstverwaltung entscheiden die Kommunen selbstständig über die Ausgestaltung ihrer IT-Sicherheitskonzepte. Das Siegel „Kommunale IT-Sicherheit“ richtet sich an kleine und mittlere Städte, Märkte und Gemeinden und soll diesen dabei helfen, einfachen Zugang zu dem Thema IT-Sicherheit zu erhalten. Diese Kommunen werden durch das LSI auf unterschiedlichen Wegen motiviert, das Siegel zu erwerben. Bislang wurden an diese Zielgruppe 191 Siegel erteilt. Insbesondere größere Kommunen nutzen weiterführende Angebote des LSI zur Verbesserung ihrer IT-Sicherheit oder arbeiten mit Beratungsunternehmen zusammen (vgl. Frage 4.3) und sehen deshalb von einer rein formalen Bestätigung durch das Siegel ab.

Um das Interesse am Siegel weiter zu erhöhen, wurden u. a. kommunale Dienstleister zum Siegel informiert. Der Bayerische Kommunale Prüfungsverband berücksichtigt bei seinen Prüfungen, ob eine Kommune das Siegel erhalten hat. In Cyberversicherungen für Kommunen kann durch das Siegel ein Beitragsbonus entstehen.

4.1 Wie viele Kommunen haben sich weitergehend im Bereich IT-Sicherheit zertifizieren lassen (z. B. ISIS12, ISO 27001, BSI-Grundschutz)?
4.2 Aus welchen Gründen haben sich Kommunen nicht weitergehend zertifizieren lassen?

Es besteht für die Kommunen keine Meldepflicht bezüglich Zertifizierungen im Bereich IT-Sicherheit.

4.3 Welche konkreten Schritte unternimmt die Staatsregierung, um zu erreichen, dass sich alle Kommunen auch weitergehend zertifizieren lassen?

Das Siegel „Kommunale IT-Sicherheit“ ist als Einstieg in das Thema IT-Sicherheit zu sehen und dokumentiert, dass eine Kommune ein Basissicherheitsniveau erreicht hat. Das LSI empfiehlt Kommunen aber grundsätzlich, nach dem Siegel weiterzugehen und eine Zertifizierung nach einem gängigen ISMS-Standard anzustreben. Die Zertifizierung nach ISIS 12, ISO 270001 sowie BSI IT-Grundschutz wird im Rahmen der „Richtlinie zur Förderung der Informationssicherheit durch Implementierung eines Informationssicherheitsmanagementsystems bei kommunalen Gebietskörperschaften“ vom Freistaat finanziell gefördert.

Nach Mitteilung des StMI bietet dieses den Kommunen seit 2015 Unterstützung in Form eines Förderprogramms zur Einführung eines hinreichenden Informationssicherheitsmanagementsystems (ISMS) nach Beschlusslage des IT-Planungsrats. Mit dem Ziel, das IT-Sicherheitsniveau bei den bayerischen Kommunen rasch und nachhaltig zu erhöhen, wurde das Förderprogramm im April 2021 evaluiert und durch ein Stufenkonzept erweitert. Durch diese Neuausrichtung werden die den Kommunen für eine höherwertigere Zertifizierung entstehenden Aufwände in leistbare Schritte aufgeteilt

und so Anreize geschaffen, in Bezug auf IT-Sicherheit nicht auf der Stelle zu treten. Das StMI macht auf obiges Förderprogramm u. a. in den vom LSI regelmäßig für die bayerischen Kommunen ausgerichteten Online-Veranstaltungen „Aktuelle Themen der kommunalen IT-Sicherheit“ aufmerksam.

5.1 Welche konkreten Maßnahmen unternimmt die Staatsregierung, um das Personal der bayerischen Kommunen für das Thema IT-Sicherheit zu sensibilisieren?
5.2 Welche Strukturen existieren auf kommunaler Ebene in Bayern, um Mitarbeiterinnen/Mitarbeiter zu motivieren, Sicherheitsvorfälle und sicherheitsrelevante Fehler frühzeitig zu melden?
5.3 Wie unterstützt die Staatsregierung die Kommunen dabei entsprechende Strukturen zu etablieren?

Das LSI bietet allen kommunalen Verwaltungen Sensibilisierungskurse in einem Webportal zur kostenlosen Nutzung an. Dieser Awareness-Kurs soll die Beschäftigten in die Lage versetzen, Cyberangriffe zu erkennen, zu melden und eventuell sogar zu verhindern.

Des Weiteren berät das LSI die Kommunen individuell zu Maßnahmen, die über den Online-Kurs hinausgehen. Mittels Informationsveranstaltungen und den Warnmeldungen unterstützt das LSI die Verantwortlichen in den Kommunen bei der Sensibilisierung der Beschäftigten. Außerdem enthält die Handreichung zu IT-Notfallmanagement des LSI hierzu unterstützende Dokumente (z. B. eine Notfallkarte). Weitere Maßnahmen sind u. a. Live-Hacking-Shows, die im Rahmen von LSI-Regionalkonferenzen durchgeführt wurden oder bei der anstehenden Messe KOMMUNALE2021 geplant sind.

Die Entscheidung über Umsetzung und Strukturen in ihrem Bereich treffen die Kommunen im Rahmen ihrer Selbstverwaltung eigenverantwortlich.

6.1 Wie viele bayerische Kommunen haben eine/einen IT-Sicherheitsbeauftragte/Sicherheitsbeauftragten bzw. ein Informationssicherheits-Management-Team?
6.2 Plant die Staatsregierung, IT-Sicherheitsbeauftragte auf kommunaler Ebene verpflichtend einzuführen?
6.3 Wie viele bayerische Kommunen haben eine verbriefte Informationssicherheitsleitlinie (ISLL)?

Organisatorische Regelungen und klare Zuständigkeitsverteilung sind essenziell für ein notwendiges IT-Sicherheitsniveau. Deshalb sind die Bestellung von IT-Sicherheitsbeauftragten ebenso wie die Erstellung einer IT-Sicherheitsleitlinie ständiger Beratungsgegenstand des LSI. Die konkrete organisatorische Ausgestaltung obliegt den Kommunen grundsätzlich selbst.

Alle bayerischen Kreisverwaltungsbehörden haben einen IT-Sicherheitsbeauftragten oder eine IT-Sicherheitsbeauftrage bestellt. Die Kontaktdaten liegen dem LSI auf Grund des direkten Zugangs der Kreisverwaltungsbehörden zum Behördennetz vor.

7.1 Wie viele der bayerischen Kommunen haben ein Informationssicherheits-Managementsystem (ISMS)?

Zu den angefragten Informationen werden keine statistischen Daten erhoben. Im Zusammenhang mit dem im Antwortbeitrag zu Frage 4.3 aufgeführten Förderprogramm haben nach Mitteilung des StMI bislang 335 Kommunen, kommunale Zusammenschlüsse und öffentlich-rechtlich organisierte Unternehmen die Einführung eines ISMS nachgewiesen.

7.2 Wie unterstützt die Staatsregierung die bayerischen Kommunen beim Aufbau eines ISMS?

Es wird auf die Antwort zu den Fragen 4.2 und 4.3 verwiesen.

7.3 In welchen Zeitabständen wird das ISMS in bayerischen Kommunen im Schnitt evaluiert und gegebenenfalls auf den neuesten Stand gebracht?

Die einschlägigen ISMS-Standards nach Maßgabe der Beschlusslage des IT-Planungsrates (ISIS12, ISO27001 und BSI-Grundschutz) sehen eine Rezertifizierung nach spätestens 2 Jahren vor.