Bayerischer Landtag

18. Wahlperiode 16.07.2022 Drucksache 18/22327

Schriftliche Anfrage

des Abgeordneten **Dr. Helmut Kaltenhauser FDP**
vom 03.03.2022

IT-Sicherheit von Ministerpräsident Dr. Markus Söder (2/2)

Die Staatsregierung wird gefragt:

Antwort

der Staatskanzlei
vom 14.04.2022

Vorbemerkung
Die parlamentarische Kontrolle von Regierung und Verwaltung verwirklicht den Grundsatz der Gewaltenteilung. Die Gewaltenteilung stellt aber nicht nur den Grund, sondern auch die Grenze der parlamentarischen Kontrolle dar. Parlamentarische Kontrolle ist politische Kontrolle, nicht administrative Überkontrolle (Entscheidungen des Bundesverfassungsgerichts – BVerfGE 67, 100, 140).

Die vorliegenden Fragen betreffen insbesondere die innere Organisation der Verwaltung und die persönlichen Gestaltungsräume handelnder Personen. Das ist Kernbereich exekutiver Eigenverantwortung, der dem parlamentarischen Fragerecht nicht unterfällt. Die erbetenen Auskünfte sind darüber hinaus teilweise geheimhaltungsbedürftig, weil sie sicherheitsrelevante Angaben berühren, die nach einer Veröffentlichung negative Auswirkungen auf die Kommunikationsfähigkeit der Staatsregierung zur Folge haben, dadurch die innere Sicherheit gefährden und somit zu erheblichen Nachteilen für den Freistaat Bayern führen könnten.

Das Offenlegen der angefragten Informationen (Einzelheiten zur genutzten Hard- und Software, organisatorische Maßnahmen und methodische Ansätze) birgt die Gefahr, dass sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf Vorgehensweisen und Fähigkeiten der Gefahrenabwehr ziehen können. Dies würde das Gefährdungspotenzial gezielter Angriffe auf die gesamte Behördennetzinfrastruktur signifikant erhöhen und damit die Handlungsfähigkeit der Staatsverwaltung zumindest nachhaltig beeinträchtigen.

Eine Beantwortung der Schriftlichen Anfrage unter Absehen von der Drucklegung bzw. Einstufung als Verschlusssache (VS-Einstufung) und Weiterleitung der angefragten Informationen an die VS-Registratur des Landtags kommt angesichts ihrer erheblichen Bedeutung für die Funktionsfähigkeit der Staatsregierung und aus den zuvor benannten Gründen nicht in Betracht, weil insoweit auch ein nur geringfügiges Risiko des Bekanntwerdens unter keinen Umständen hingenommen werden kann.

1. Sicherheitsmaßnahmen allgemein

1.1 Welche IT-Sicherheitsmaßnahmen wurden bzw. werden ergriffen, um die IT-Sicherheit in der Staatskanzlei zu gewährleisten?

1.2 Welche IT-Sicherheitsmaßnahmen wurden bzw. werden ergriffen, um die IT-Sicherheit der digitalen Endgeräte, die Ministerpräsident Dr. Markus Söder dienstlich nutzt, zu sichern?

1.3 Welche IT-Sicherheitsmaßnahmen wurden bzw. werden ergriffen, um die IT-Sicherheit der digitalen Endgeräte, die Ministerpräsident Dr. Markus Söder privat nutzt, zu sichern?

2. Nutzung digitaler Endgeräte

2.1 In welchen Fällen nutzt Ministerpräsident Dr. Markus Söder private digitale Endgeräte grundsätzlich für dienstliche Zwecke?

2.2 In welchen konkreten Fällen kam dies seit seinem Amtsantritt vor?

2.3 Welche besonderen IT-Sicherheitsregeln gelten für diese Fälle?

3. Sicherstellung der IT-Sicherheit

3.1 Welche Stellen innerhalb der Staatsregierung kümmern sich um die IT-Sicherheit der Staatskanzlei (bitte hierbei auch personelle Ausstattung angeben)?

3.2 Welche Stellen innerhalb der Staatsregierung kümmern sich um die IT-Sicherheit von Ministerpräsident Dr. Markus Söder (bitte hierbei auch personelle Ausstattung angeben)?

3.3 Welche Stellen außerhalb der Staatsregierung kümmern sich um die IT-Sicherheit der Staatskanzlei und von Ministerpräsidenten Dr. Markus Söder?

Die Fragenkomplexe 1 bis 3 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die IT-Systeme der Staatskanzlei sind in das bayerische Behördennetz und die hier zum Einsatz kommende IT-Sicherheitsinfrastruktur integriert, die auf den Empfehlungen und Vorgaben des Landesamts für Sicherheit in der Informationstechnik (LSI) beruhen. Das IT-Dienstleistungszentrum des Freistaates Bayern (IT-DLZ) betreibt diese Sicherheitsinfrastruktur. Neben dem o. a. LSI und dem IT-DLZ obliegt die Umsetzung innerhalb der Staatskanzlei dem Referat für Informations- und Kommunikationstechnik (IuK-Referat) und dem Beauftragten für IT-Sicherheit.

Zum Aufdecken möglicher Sicherheitsrisiken und zur Abwehr etwaiger Schadsoftware werden die Systeme fortlaufend und regelmäßig überwacht und geprüft.

Unter Verweis auf die o. a. Vorbemerkung können zur Nutzung digitaler Endgeräte keine detaillierten Angaben gemacht werden.

Hinsichtlich weiterer Details wird auf die o. a. Vorbemerkung verwiesen.

4. Kommunikationsmittel von Ministerpräsident Dr. Markus Söder

4.1 Welche Anwendungen nutzt Ministerpräsident Dr. Markus Söder für die dienstliche Kommunikation?

4.2 Welche Apps nutzt Ministerpräsident Dr. Markus Söder für die dienstliche Kommunikation?

4.3 Bei welchen Gelegenheiten nutzt er diese Apps jeweils?

Jeweils situationsabhängig kommen unterschiedliche Kommunikationsmittel zum Einsatz. Hinsichtlich der Details wird auf die o. a. Vorbemerkung verwiesen.

5. Umgang mit digitalen Daten von Ministerpräsident Dr. Markus Söder

5.1 Wie wird grundsätzlich mit den digitalen Daten, die seitens Ministerpräsident Dr. Markus Söder durch die Nutzung seiner digitalen Endgeräte entstehen, umgegangen?

5.2 Nach welchem Zeitraum findet in der Regel eine Löschung dieser Daten statt?

5.3 Werden diese Daten in einer Cloud oder auf einer externen Festplatte gespeichert?

Unter Berücksichtigung der einschlägigen geltenden normativen Vorgaben wird in der Staatskanzlei mit den Daten nach Recht und Gesetz verfahren.

Hinsichtlich der Details wird auf die o. a. Vorbemerkung verwiesen.

6. Hackerangriffe

6.1 In wie vielen Fällen kam es seit dem Amtsantritt von Ministerpräsident Dr. Markus Söder bei den von ihm genutzten Endgeräten nachweislich zu einem Angriff von Hackern (bitte hierbei jeweils Datum nennen als auch auf technischen Weg des Informationsabflusses eingehen)?

6.2 Auf welchen Bereich des digitalen Endgeräts zielten diese Hackerangriffe jeweils ab?

6.3 Wer konnte bisher als Täter ermittelt werden?

7. Spyware Pegasus

7.1 Wurden innerhalb der Staatsregierung seit Dr. Markus Söders Amtsantritt als Ministerpräsident Ausspähversuche mit der Spyware Pegasus oder ähnlichen Programmen festgestellt?

7.2 Wenn ja, an welchen Tagen war dies der Fall (bitte hierbei auch die Dauer bis der Hack behoben wurde, angeben)?

7.3 Wer konnte bisher als Täter ermittelt werden?

8. Kritische Schwachstelle Log4Shell in Java-Bibliothek Log4j

8.1 Konnte auf digitalen Endgeräten der Staatskanzlei die kritische Schwachstelle (Log4Shell) in der weit verbreiteten Java-Bibliothek Log4j identifiziert werden?

8.2 Konnte auf digitalen Endgeräten von Ministerpräsident Dr. Markus Söder die kritische Schwachstelle (Log4Shell) in der weit verbreiteten Java-Bibliothek Log4j identifiziert werden?

8.3 Falls ja, wie wurde auf die in 8.1 und 8.2 erfragten Sachverhalte jeweils reagiert?

Die Fragenkomplexe 6 bis 8 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Zu den Fragenkomplexen 6 bis 8 sind bislang keine Vorfälle bekannt geworden.

Hinweise des Landtagsamts

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

Zur Vereinfachung der Lesbarkeit können Internetadressen verkürzt dargestellt sein. Die vollständige Internetadresse ist als Hyperlink hinterlegt und in der digitalen Version des Dokuments direkt aufrufbar. Zusätzlich ist diese als Fußnote vollständig dargestellt.

Drucksachen, Plenarprotokolle sowie die Tagesordnungen der Vollversammlung und der Ausschüsse sind im Internet unter www.bayern.landtag.de/parlament/dokumente abrufbar.

Die aktuelle Sitzungsübersicht steht unter www.bayern.landtag.de/aktuelles/sitzungen zur Verfügung.