Bayerischer Landtag

19. Wahlperiode 27.07.2026 Drucksache 19/12533

Schriftliche Anfrage

der Abgeordneten **Roland Magerl, Andreas Winhart, Matthias Vogler, Elena Roon, Franz Schmid AfD**
vom 22.05.2026

Cyberangriffe auf Arztpraxen und ambulante Versorgungseinrichtungen in Bayern

Die Staatsregierung wird gefragt:

Antwort

des Staatsministeriums für Gesundheit, Pflege und Prävention im Einvernehmen mit dem Staatsministerium des Innern, für Sport und Integration und dem Staatsministerium der Finanzen und für Heimat
vom 24.06.2026

1.1 Welche Erkenntnisse liegen der Staatsregierung über die aktuelle Bedrohungslage durch Cyberangriffe auf Arztpraxen und ambulante Versorgungseinrichtungen in Bayern vor?

Die allgemeine Bedrohungslage ist schon seit vielen Jahren und auch weiterhin sehr hoch. Mangels valider, expliziter Rechercheparameter ist eine automatisierte Auswertung im Sinne der Fragestellung weder auf Basis der Polizeilichen Kriminalstatistik noch auf Grundlage anderer polizeilicher Datenquellen möglich, da eine Erfassung von Arztpraxen, Medizinischen Versorgungszentren und sonstigen ambulanten Gesundheitseinrichtungen nicht einheitlich nach Katalog, Listenwert oder Ähnlichem erfolgt. Insofern müsste eine umfangreiche manuelle (Einzel-)Auswertung von Akten und Datenbeständen erfolgen. Dies würde zu einem erheblichen zeitlichen und personellen Aufwand führen. Auch unter Berücksichtigung der Bedeutung des sich aus Art. 13 Abs. 2, 16a Abs. 1 und 2 Satz 1 Bayerische Verfassung (BV) ergebenden parlamentarischen Fragerechts der Abgeordneten des Landtags kann daher eine Auswertung von Einzelakten u. Ä. nicht erfolgen. Zur allgemeinen Bedrohungslage wird auf den öffentlichen Bericht des Staatsministeriums des Innern, für Sport und Integration (StMI) und des Staatsministeriums der Finanzen und für Heimat (StMFH) zur Cybersicherheit in Bayern 2025 verwiesen (siehe www.stmi.bayern.de[1]).

1.2 Wie viele Cyberangriffe auf Arztpraxen, Medizinische Versorgungszentren und sonstige ambulante Gesundheitseinrichtungen in Bayern sind der Staatsregierung seit 2019 bekannt geworden (bitte nach Jahren aufschlüsseln)?

Seit dem 01.01.2019 gingen beim Landesamt für Datenschutzaufsicht (BayLDA) 11 964 Meldungen nach Art. 33 Datenschutz-Grundverordnung (DSGVO; Verletzung der Sicherheit) ein, die eindeutig dem Bereich der Cyberangriffe zugeordnet werden können. Davon waren jedoch nur ein kleiner Anteil Angriffe auf Arztpraxen, Medizinische Versorgungszentren und andere ambulante Gesundheitseinrichtungen. Eine genaue Aufschlüsselung der Daten und Zahlen nach der Art der Einrichtung ist nicht möglich (s. hierzu Antwort zu Frage 1.1).

1.3 Welche Erkenntnisse liegen der Staatsregierung darüber vor, welche Arten von Schadsoftware oder Angriffsmethoden hierbei überwiegend eingesetzt wurden?

Historisch und branchenüblich dominieren im ambulanten Sektor drei Vektoren, die auch zu Datenschutzverletzungen und Meldungen nach Art. 33 DSGVO führen: Ransomware, Phishing und kompromittierte E-Mail-Konten.

---

1 https://www.stmi.bayern.de/media/05_innere_sicherheit/Cybersicherheit/StMI_Cybersicherheitsbericht_2025_A5_Okt__3_.pdf

Zu den allgemein vorherrschenden Phänomenen wird auf den öffentlichen Bericht des StMI und des StMFH zur Cybersicherheit in Bayern 2025 verwiesen.

2.1 Welche Erkenntnisse liegen der Staatsregierung über erfolgreiche Angriffe mit Datenverlust, Verschlüsselung oder Betriebsunterbrechungen in bayerischen Arztpraxen vor?

2.2 Welche Erkenntnisse liegen der Staatsregierung darüber vor, ob im Zusammenhang mit Cyberangriffen Patientendaten abgeflossen oder dauerhaft verloren gegangen sind?

Aufgrund des Sachzusammenhangs werden die Fragen 2.1 und 2.2 gemeinsam beantwortet.

Nach dem Wiederherstellen von Daten auf Grundlage von Backups, welche mittlerweile auch bei vielen kleineren Arztpraxen vorhanden sind, können die Praxen regelmäßig schnell wieder arbeiten.

Schwerwiegender ist in solchen Fällen oftmals die Erlangung von Daten und die Drohung, diese Daten zu veröffentlichen.

Für betroffene Organisationen besteht im Falle des Abfließens personenbezogener Daten an Unberechtigte in der Regel eine Meldepflicht an die zuständige Datenschutzaufsichtsbehörde innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls (Art. 33 DSGVO). Für den nichtöffentlichen Bereich in Bayern ist das BayLDA die zuständige Datenschutzaufsichtsbehörde, für den öffentlichen Bereich der Landesbeauftragte für den Datenschutz (BayLfD).

In sensiblen Bereichen wie Einrichtungen der kritischen Infrastruktur (KRITIS) bzw. Objekten i. S. der NIS-2-Richtlinie (Network and Information Security) ergeben sich weiterhin regelmäßig Meldeverpflichtungen an das Bundesamt für Sicherheit in der Informationstechnik (BSI).

2.3 Welche Erkenntnisse liegen der Staatsregierung darüber vor, welche Auswirkungen Cyberangriffe auf die medizinische Versorgung und den Praxisbetrieb in Bayern hatten?

In aller Regel sind Arztpraxen durch Cyberangriffe zumindest temporär nicht oder nur eingeschränkt arbeitsfähig. Diese Auswirkungen sind in aller Regel von eher kurzer Dauer. Gerade die Sensibilisierung der Verantwortlichen hat dazu beigetragen, dass Verantwortliche mittlerweile im Hinblick auf technische und organisatorische Maßnahmen gut aufgestellt sind.

3.1 Welche Maßnahmen hat die Staatsregierung seit 2019 ergriffen, um die IT- und Cybersicherheit von Arztpraxen und ambulanten Versorgungseinrichtungen in Bayern zu stärken?

3.2 Welche Beratungs-, Informations- oder Unterstützungsangebote bestehen derzeit für Arztpraxen im Bereich Cybersicherheit und Datenschutz?

3.3 Welche Rolle spielen hierbei das Landeskriminalamt, das Landesamt für Sicherheit in der Informationstechnik sowie sonstige staatliche Stellen?

Aufgrund des Sachzusammenhangs werden die Fragen 3.1 bis 3.3 gemeinsam beantwortet.

Für alle Unternehmen in Bayern steht die Zentrale Ansprechstelle Cybercrime (ZAC) des Landeskriminalamts (BLKA) als kompetenter Ansprechpartner zur Verfügung. Die ZAC bietet u. a. Vorträge, Informationsbroschüren, Informationsvideos und interaktive Fallbeispiele zu Präventionszwecken in diesem Bereich an.

Der BayLfD und das BayLDA stellen eine Checkliste mit Best-Practice-Maßnahmen zur Sicherstellung der Verfügbarkeit bezüglich Cyberattacken in medizinischen Einrichtungen zur Verfügung (siehe www.lda.bayern.de[2]). Auf der Website des BayLDA sind zum Datenschutz bei Ärzten weitere Informationen abrufbar (siehe Website des BayLDA: www.lda.bayern.de[3]; bspw. der Flyer: DSGVO einfach umgesetzt in Arztpraxen, s. Link: www.lda.bayern.de[4]).

Das Landesamt für Sicherheit in der Informationstechnik (LSI) und das BLKA kooperieren eng miteinander. Gemeinsam gestalten sie regelmäßig Präventionsveranstaltungen, insbesondere im Jahr 2025 die vom LSI organisierten Thementage „Informationssicherheit in Kliniken“. Ziel dieser Präventionsmaßnahmen ist es, die Resilienz der bayerischen Gesundheitsinfrastruktur zu erhöhen.

4.1 Welche Erkenntnisse liegen der Staatsregierung darüber vor, wie gut Arztpraxen in Bayern gegen Cyberangriffe geschützt sind?

4.2 Welche Erkenntnisse liegen der Staatsregierung darüber vor, in welchem Umfang regelmäßige Datensicherungen, Offline-Backups oder Notfallpläne in Arztpraxen eingesetzt werden?

Aufgrund des Sachzusammenhangs werden Fragen 4.1 und 4.2 gemeinsam beantwortet.

Der Staatsregierung liegen hierzu keine Erkenntnisse vor.

Dies liegt insbesondere daran, dass Arztpraxen der Privatwirtschaft zuzuordnen sind. Über das deutsche KRITIS-Dachgesetz wird der Betreiber kritischer Infrastrukturen selbst verpflichtet, sich umfassend gegen Cyberangriffe, Sabotage und physische Bedrohungen abzusichern. Bei Cyberangriffen auf Arztpraxen ist die Praxisinhaberin oder der Praxisinhaber mithin selbst verantwortlich.

Ergänzend wird auf die Tätigkeitsberichte bzw. die Studien CyberPraxMed und SiRiPrax des BSI hingewiesen.

---

2 https://www.lda.bayern.de/media/checkliste/baylda_checkliste_medizin.pdf

3 https://www.lda.bayern.de/de/thema_aerzte.html

4 https://www.lda.bayern.de/media/veroeffentlichungen/DS-GVO_in_Arztpraxen.pdf

4.3 Welche Erkenntnisse liegen der Staatsregierung darüber vor, ob insbesondere kleine und mittelständische Praxen aufgrund begrenzter IT-Ressourcen besonders gefährdet sind?

Es wird auf die Antwort zu Frage 1.1 verwiesen.

5.1 Welche Erkenntnisse liegen der Staatsregierung über den Einsatz künstlicher Intelligenz (KI) bei Cyberangriffen auf Einrichtungen des Gesundheitswesens vor?

5.2 Wie bewertet die Staatsregierung die Entwicklung der Bedrohungslage durch KI-gestützte Cyberangriffe im Gesundheitswesen?

Aufgrund des Sachzusammenhangs werden die Fragen 5.1 und 5.2 gemeinsam beantwortet.

Konkrete Erkenntnisse zum Einsatz künstlicher Intelligenz (KI) bei Cyberangriffen speziell im Gesundheitswesen liegen nicht vor.

Insgesamt ist bei langfristiger Betrachtung eine Verlagerung von Straftaten in den digitalen Raum zu beobachten. Bedingt durch den Einsatz von KI ist zukünftig mit einer weiteren Verschärfung der Cyber-Gefährdungslage zu rechnen. Dies gilt unabhängig von der Branche.

5.3 Welche Maßnahmen werden ergriffen, um Arztpraxen und andere Einrichtungen des Gesundheitswesens gegen KI-gestützte Angriffe besser zu schützen?

6.1 Plant die Staatsregierung weitere Maßnahmen zur Verbesserung der Cybersicherheit im ambulanten Gesundheitswesen?

6.2 Falls ja, welche konkreten Maßnahmen sind geplant und in welchem Zeitraum sollen diese umgesetzt werden?

6.3 Welche Erkenntnisse liegen der Staatsregierung darüber vor, ob bestehende gesetzliche Vorgaben und Sicherheitsstandards ausreichend sind, um Arztpraxen wirksam vor Cyberangriffen zu schützen?

Aufgrund des Sachzusammenhangs werden die Fragen 5.3 bis 6.3 gemeinsam beantwortet.

Hierzu wird auf die Antwort zu den Fragen 4.1 und 4.2 verwiesen.

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.