Bayerischer Landtag

19. Wahlperiode 02.06.2025 Drucksache 19/6508

Schriftliche Anfrage

des Abgeordneten **Florian von Brunn SPD**
vom 11.03.2025

Hacker- und Cyberangriffe in Bayern seit 2019 I

Die Bedrohungslage im Bereich der Cybersicherheit in Bayern hat sich in den letzten Jahren deutlich verschärft. Seit 2019 sieht sich der Freistaat einer zunehmenden Zahl von Cyberangriffen ausgesetzt, die nicht nur staatliche Institutionen, sondern auch Kommunen, Krankenhäuser und kritische Infrastrukturen betreffen. Diese Angriffe reichen von DDoS-Attacken über Ransomware bis hin zu gezielter Cyberspionage und haben das Potenzial, erhebliche finanzielle Schäden zu verursachen, sensible Daten zu kompromittieren und wichtige Dienste lahmzulegen. Angesichts dieser Entwicklung ist es von höchster Bedeutung, einen umfassenden Überblick über die Situation zu gewinnen, um geeignete Schutzmaßnahmen ergreifen zu können.

Die Staatsregierung wird gefragt:

Antwort

des Staatsministeriums des Innern, für Sport und Integration im Einvernehmen mit dem Staatsministerium der Justiz, dem Staatsministerium der Finanzen und für Heimat und dem Staatsministerium für Gesundheit, Pflege und Prävention
vom 29.04.2025

1.a) Wie viele Cyberangriffe auf kritische Infrastrukturen in Bayern wurden seit dem 1. Januar 2019 registriert?

1.b) Welche Schäden (finanziell, operative Ausfälle, Datenverluste) sind durch diese Angriffe entstanden?

1.c) Welche Maßnahmen wurden ergriffen, um die Sicherheit dieser Infrastrukturen zu erhöhen und zukünftige Angriffe zu verhindern?

Die Fragen 1 a bis 1 c werden aufgrund des Sachzusammenhangs zusammen beantwortet.

Cyberangriffe sind von Betreibern kritischer Infrastrukturen nach Art. 8 Abs. 4 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Eine Statistik im Sinne der Fragestellung liegt dem Bayerischen Landesamt für Sicherheit in der Informationstechnik (LSI) daher nicht vor.

2.a) Wie viele Cyberangriffe auf bayerische Behörden (einschließlich Staatsministerien, Bezirksregierungen, Landratsämter, Städte und Gemeinden) wurden seit 1. Januar 2019 verzeichnet?

2.b) Welche Kosten sind durch erfolgreiche Angriffe entstanden, insbesondere in Bezug auf Wiederherstellung, Lösegeldzahlungen und IT-Sicherheitsmaßnahmen?

2.c) Inwieweit haben diese Angriffe zu Datenverlusten oder Einschränkungen im Behördenbetrieb geführt?

Die Fragen 2 a bis 2 c werden aufgrund des Sachzusammenhangs zusammen beantwortet.

Das LSI hat seit 2019 über 16 000 Auffälligkeiten bei bayerischen Behörden registriert. Für den Bereich der Staatsverwaltung sind dem LSI keine Vorfälle bekannt, die zu erheblichen Einschränkungen im Behördenbetrieb geführt haben. Es liegen dem LSI trotz fortlaufender Beobachtung auch keine Erkenntnisse vor, dass im angegebenen Zeitraum im Rahmen eines Cyberangriffs interne Daten abgeflossen sind.

Bezüglich der bayerischen Kommunen liegt dem LSI keine Statistik im Sinne der Fragestellung vor, da für Kommunen keine Pflicht zur Meldung von Cyberangriffen an das LSI besteht.

3.a) Welche Cyberangriffe auf Polizeidienststellen oder andere Sicherheitsbehörden gab es seit 1. Januar 2019 in Bayern?

Seit 2019 kam es zu einer einstelligen Anzahl an sog. DDoS-Angriffen auf die Website www.polizei.bayern.de. Es kam in zwei Fällen zu Phishing-Versuchen per E-Mail an Polizeibeamte. In einem Fall sind über 2000 E-Mails an das Postfach einer Dienststelle versandt worden.

Im Übrigen wird auf die Antwort zu Fragen 2a bis 2c verwiesen.

3.b) Falls ja, welche Art von Daten wurde kompromittiert oder entwendet?

Im Rahmen der unter Frage 3a genannten Sachverhalte wurden keine Daten entwendet oder kompromittiert.

Im Übrigen wird auf die Antwort zu Fragen 2a bis 2c verwiesen.

3.c) Welche zusätzlichen Maßnahmen wurden ergriffen, um die IT-Sicherheit der Polizei und anderer Sicherheitsbehörden zu verbessern?

Die Bayerische Polizei hat seit 2012 ein Informationssicherheitsmanagement nach den Standards des BSI (BSI Standard 200-1) aufgebaut und etabliert. Neben dem strategischen Informationssicherheitsmanagement sind etwa 30 operative Informationssicherheitsbeauftragte innerhalb der Bayerischen Polizei mit der Umsetzung der Anforderungen des BSI IT-Grundschutzes (BSI Standard 200-2) und somit der Gewährleistung der Informationssicherheit nach dem aktuellen Stand der Technik betraut. Der Informationssicherheitsprozess gewährleistet dabei eine kontinuierliche Betrachtung und Bewertung der aktuellen Cybersicherheitslage und der sich daraus ableitenden erforderlichen Maßnahmen. In der Vergangenheit wurden dabei diverse technologische und organisatorische Maßnahmen zum Schutz der Bayerischen Polizei ergriffen. Das Netz der Bayerischen Polizei ist aufgrund der infrastrukturellen Eingliederung in das Behördennetz durch aktive Schutzmaßnahmen der Außengrenzen durch das LSI überwacht und abgesichert. Zusätzlich wurden und werden innerhalb der Netze der Bayerischen Polizei diverse weitere Schutzmaßnahmen ergriffen. Darüber hinaus wurde das Landeskriminalamt mit dem Aufbau eines Security-Operations-Centers als weitere proaktive Sicherheitsinstanz innerhalb der eigenen Netze beauftragt, um der steigenden Bedrohung von Cyberangriffen auch künftig effektiv entgegenzuwirken.

Hinsichtlich der vom Landesamt für Verfassungsschutz (BayLfV) ergriffenen internen Maßnahmen kann eine Auskunft nach Abwägung des Informationsrechts des Abgeordneten mit dem Staatswohl nicht erfolgen. Ein öffentliches Bekanntwerden der internen Maßnahmen des BayLfV, die teilweise auch Dritte betreffen, würde dessen künftige Aufgabenerfüllung erheblich beeinträchtigen und hätte daher erhebliche nachteilige Auswirkungen auf die Sicherheit der Länder und des Bundes. Auch eine VS-Einstufung und Hinterlegung der angefragten Informationen in der VS-Registratur des Landtags würde ihrer erheblichen Relevanz in Hinblick auf die Bedeutung der Aufgabenerfüllung des BayLfV und die Sicherung des Staatswohls nicht ausreichend Rechnung tragen. Im Hinblick auf den Verfassungsgrundsatz der wehrhaften Demokratie hält die Staatsregierung die Informationen der angefragten Art für derart sensibel, dass selbst ein geringfügiges Risiko des Bekanntwerdens unter keinen Umständen hingenommen werden kann.

4.a) Welche Angriffe auf Krankenhäuser, Pflegeeinrichtungen und soziale Organisationen (z. B. Wohlfahrtsverbände) wurden seit 1. Januar 2019 registriert?

Für die Plankrankenhäuser und Pflegeeinrichtungen liegen dem Staatsministerium für Gesundheit, Pflege und Prävention (StMGP) – über die in der allgemeinen Presseberichterstattung bekannt gewordenen Fälle (etwa Klinikum Fürth, Bezirkskliniken Mittelfranken) – keine Erkenntnisse zu Hacker- oder Cyberangriffen vor. Die Plankrankenhäuser sind diesbezüglich nicht gegenüber dem StMGP auskunftspflichtig. Auch bestehen für Betreiber von Pflegeeinrichtungen aus ordnungsrechtlicher Sicht keine Meldeverpflichtungen hinsichtlich Cyberangriffen.

4.b) Welche konkreten Auswirkungen hatten diese Angriffe auf die Versorgungssicherheit und den Betrieb der betroffenen Einrichtungen?

Dem StMGP liegen keine Hinweise darüber vor, dass die Versorgungssicherheit oder der Betrieb von Plankrankenhäusern oder Pflegeeinrichtungen aufgrund von Cyberattacken gefährdet waren.

4.c) Welche finanziellen Belastungen und strukturellen Folgen ergaben sich für die betroffenen Institutionen (bitte mit Angabe der Unterstützungsangebote, die der Freistaat bereitstellt)?

In Bezug auf die Plankrankenhäuser oder Pflegeeinrichtungen liegen dem StMGP keine Erkenntnisse im Sinne der Fragestellung vor. Eine diesbezügliche Auskunftspflicht gegenüber dem StMGP besteht nicht.

5.a) Wie viele Unternehmen in Bayern wurden seit 1. Januar 2019 Opfer von Cyberangriffen?

Bei der Bayerischen Polizei wurden folgende Fallzahlen verzeichnet, bei denen juristische Personen als Geschädigte im Vorgangserfassungssystem erfasst wurden und die im Bereich Cybercrime liegen. Dabei ist es möglich, dass Unternehmen mehrfach erfasst sind.

2019	10 321
2020	11 882
2021	11 480
2022	11 461
2023	11 612
2024	8 657

Als Datenquelle für die vorliegende Erhebung diente der Datenbestand des polizeilichen Vorgangsverwaltungssystems IGVP-FE. Die enthaltenen Rohdaten sind durch laufende Ermittlungen und Qualitätssicherungsmaßnahmen teils dynamischen Änderungen unterworfen und geben stets den aktuellen Erfassungsstand zum Zeitpunkt der Abfrage wieder.

5.b) Welche Branchen waren besonders betroffen?

Die betroffenen Branchen der bei Frage 5 a aufgeführten Fälle können mangels expliziter, valider Rechercheparameter, die eine automatisierte Auswertung im Sinne der Fragestellung zulassen würden, weder auf Basis der Polizeilichen Kriminalstatistik (PKS) noch auf Basis von IGVP-FE erhoben werden. Für eine Beantwortung müsste insofern eine umfangreiche manuelle (Einzel-)Auswertung von Akten und Datenbeständen bei den Präsidien der Landespolizei und dem Landeskriminalamt erfolgen. Dies würde zu einem erheblichen zeitlichen und personellen Aufwand führen. Auch unter Berücksichtigung der Bedeutung des sich aus Art. 13 Abs. 2, Art. 16a Abs. 1 und 2 Satz 1 Bayerische Verfassung (BV) ergebenden parlamentarischen Fragerechts der Abgeordneten des Landtags kann daher eine Auswertung von Einzelakten und Ähnlichem nicht erfolgen.

5.c) Welche finanziellen Schäden wurden durch Cyberkriminalität für bayerische Unternehmen verursacht?

Die zugehörigen Schadenszahlen für die in Frage 5 a aufgelisteten Fälle betrugen:

2019	36.404.755,46 Euro
2020	55.076.998,39 Euro
2021	102.046.856,00 Euro
2022	64.202.451,60 Euro
2023	74.237.581,36 Euro
2024	60.957.578,41 Euro

Ergänzend wird darauf hingewiesen, dass die dargestellten Schadenshöhen entsprechend den Ausführungen bei Frage 5 a auf dem Datenbestand des polizeilichen Vorgangsverwaltungssystems IGVP-FE basieren. Die in der PKS ausgewiesenen Schadenshöhen im Bereich Cybercrime fallen hingegen deutlich geringer aus, da in den bundeseinheitlichen PKS-Richtlinien zur Erfassung von Cybercrime ausschließlich Schäden aus den Deliktsfeldern „Computerbetrug“ mit Tatort im Inland Berücksichtigung finden. Im Rahmen der hier vorliegenden IGVP-FE-Recherche wurden darüber hinaus Schäden berücksichtigt, bei denen der Erfolgsort statistisch nicht ausgewiesen ist bzw. im Ausland liegt und das geschädigte Unternehmen einen Sitz in Bayern hat.

6. Welche Programme oder Initiativen zur Unterstützung der IT-Sicherheit in Unternehmen bietet die Staatsregierung an?

Es wird auf den Bericht zur Cybersicherheit in Bayern 2024, S. 14 ff., auf das aktuelle Landeslagebild Cybercrime des Landeskriminalamtes, Ziffer 6 „Prävention“, den 14. Tätigkeitsbericht des Landesamts für Datenschutzaufsicht (BayLDA) 2024, S. 78, die Cybersicherheitsstrategie 2.0 sowie auf den Verfassungsschutzbericht Bayern 2024, S. 315 ff., verwiesen, die alle öffentlich über das Internet verfügbar sind.

7.a) Welche Datenschutzverletzungen wurden durch Cyberangriffe in Bayern seit 1. Januar 2019 gemeldet?

Beim BayLDA, das für den Datenschutz im nichtöffentlichen Bereich zuständig ist, sind seit 1. Januar 2019 11 964 Meldungen nach Art. 33 Datenschutz-Grundverordnung

(Verletzung der Sicherheit) eingegangen, die eindeutig in den Bereich Cyberangriffe zugeordnet werden können.

Bei den Cyberangriffen handelt es sich um Ransomware, (Cloud-)Hacking, Malware, Phishing und Zugriff auf Daten in Netzwerken. Die Abgrenzung im Einzelfall ist fließend.

7.b) Welche Kategorien von personenbezogenen Daten waren betroffen (bitte mit Angabe der Konsequenzen die sich für die Betroffenen ergaben)?

Die Kategorie personenbezogener Daten, die entwendet werden, hängt insbesondere von der Zielsetzung der Cyberangriffe ab. Beispielsweise soll bei Ransomware durch eine drohende Veröffentlichung zu einer Lösegeldzahlung bewogen werden. Entsprechend werden dort meist alle verfügbaren Daten in sehr großem Umfang entwendet. Bei Angriffen beispielsweise auf Mailsysteme, die für Betrugsversuche (z. B. gefälschte Rechnungen) verwendet werden, stehen oft die Daten der Beschäftigten im Fokus. Bei Gesundheitseinrichtungen sind in der Regel auch sensitive Gesundheitsdaten betroffen.

7.c) Welche Maßnahmen wurden seitens des Freistaates ergriffen, um den Datenschutz im öffentlichen und privaten Sektor zu verbessern?

Es wird auf den 14. Tätigkeitsbericht des BayLDA 2024, S. 78, den Bericht zur Cybersicherheit in Bayern 2024, S. 14 ff., auf das aktuelle Landeslagebild Cybercrime des Landeskriminalamtes, Ziffer 6 „Prävention“, die Cybersicherheitsstrategie 2.0 sowie auf den Verfassungsschutzbericht Bayern 2024, S. 315 ff., verwiesen, die alle öffentlich über das Internet verfügbar sind.

8.a) Welche Erkenntnisse über Tätergruppen oder Organisationen gibt es, die hinter Cyberangriffen in Bayern stehen?

Die jeweiligen Tätergruppen weisen fallspezifische und unterschiedliche Strukturen auf. Die Taten werden immer seltener von Einzeltätern begangen. Gerade qualitativ hochwertige Angriffe (APT) können Tätergruppen zugeordnet werden, deren Organisationsgrad von losen Strukturen („crime as a service“) bis zur komplexen Organisierten Kriminalität im klassischen Sinn reicht. Der Großteil von Angriffen auf Behörden, öffentliche Einrichtungen sowie Firmen wird von Ransomwaregruppierungen ausgeführt. Die bekanntesten Gruppierungen aus dem Bereich Ransomware, die eine verstärkte Bedrohung für bayerische Organisationen darstellen, sind die Gruppierungen LockBit und Phobos/8Base.

Ergänzend wird hierzu auch auf die Antwort der Staatsregierung vom 29. April 2025 zu Fragen 1 a bis 1 c der Schriftlichen Anfrage des Abgeordneten Florian von Brunn (SPD) betreffend Hacker- und Cyberangriffe in Bayern seit 2019 II verwiesen.

Im Übrigen wird auf den Bericht zur Cybersicherheit in Bayern 2024, S. 7 ff., das aktuelle Landeslagebild Cybercrime des Landeskriminalamtes sowie auf den Verfassungsschutzbericht Bayern 2024, S. 300 ff., verwiesen, die alle öffentlich über das Internet verfügbar sind.

8.b) Wie viele Cyberkriminelle wurden in Bayern seit 2019 identifiziert, gefasst oder strafrechtlich verfolgt?

Seitens der Bayerischen Polizei kann die Anzahl Tatverdächtiger wie folgt nach Jahren anhand der zurückliegenden PKS-Zahlen aufgeschlüsselt werden (Deliktsschlüssel 897000):

2019:	4273
2020:	4872
2021:	3723
2022:	3974
2023:	4098
2024:	4140

Dem Staatsministerium der Justiz liegen zu der Fragestellung keine statistischen Zahlen vor. Die nach bundeseinheitlichen Kriterien geführten Justizgeschäftsstatistiken der Staatsanwaltschaften und Strafgerichte geben Auskunft über die Anzahl der Fälle, in denen strafrechtliche Ermittlungsverfahren durchgeführt und Strafverfahren von den Gerichten abgeschlossen wurden. In diesen Statistiken sind bestimmte Arten von Ermittlungsverfahren und Strafverfahren nach Sachgebieten gesondert ausgewiesen. Hintergründe von Tat oder Tätern sowie bestimmte Tatmittel werden jedoch nicht erfasst. Ob eine Tat zum Verbrechensphänomen „Cyberkriminalität“ gehört, wird daher nicht gesondert ausgewiesen.

Die ebenfalls nach bundeseinheitlichen Kriterien geführte Strafverfolgungsstatistik liefert Angaben zu der Zahl der Abgeurteilten und Verurteilten. Die Zahl der Abgeurteilten setzt sich zusammen aus der Zahl der Verurteilten und den Personen, gegen die das Verfahren nach Eröffnung des Hauptverfahrens endgültig und rechtskräftig endete (z. B. Freispruch, Einstellung des Strafverfahrens). In der Strafverfolgungsstatistik wird aber nur nach Straftatbeständen unterschieden, nicht nach einzelnen Verbrechensphänomenen („Cyberkriminalität“) oder Tatmitteln.

Mangels statistischer Daten kann die Frage daher in der zur Verfügung stehenden Zeit mit vertretbarem Aufwand nicht beantwortet werden. Die Frage könnte nur beantwortet werden, wenn die Verfahrensakten händisch durchgesehen würden. Dies würde ganz erhebliche Arbeitskraft binden und eine – verfassungsrechtlich gebotene – effektive Strafverfolgung durch die Staatsanwaltschaft gefährden.

8.c) Welche konkreten Maßnahmen werden ergriffen, um Kommunen, Behörden, Krankenhäuser und Unternehmen in Bayern bei der Cyberabwehr zu unterstützen?

Aufgabe des LSI ist die Abwehr von Gefahren für die Sicherheit in der Informationstechnik des Behördennetzes und der daran angeschlossenen Stellen. Daneben stellt das LSI umfangreiche Angebote zur Verbesserung der IT-Sicherheit bereit, die auf die Bedürfnisse von Kommunen und Betreibern kritischer Infrastruktur zugeschnitten sind. Hierzu zählen beispielsweise Handlungsempfehlungen, Orientierungshilfen, Musterunterlagen, Vorgehensmodelle, Sensibilisierungskurse, Phishing-Simulationen, das Siegel „Kommunale IT-Sicherheit“, ein Warn- und Informationsdienst (WID), eine Malware Information Sharing Platform (MISP), Arbeitshilfen z. B. zu IT-Notfallmanagement, Table-Top-Übungen, IT-Resilienz und Risikomanagement, regelmäßige Informationsveranstaltungen, Individualberatungen und die Möglichkeit, sich rund um

die Uhr bei IT-Sicherheitsvorfällen an das LSI zu wenden. Darüber hinaus unterstützt das LSI bei Cyberangriffen bei der Koordinierung von Sofortmaßnahmen und forensischen Untersuchungen im Rahmen der Vorfallsbearbeitung. Alle Beratungsangebote des LSI sind für Kommunen und Betreiber kritischer Infrastrukturen kostenfrei. Durch die enge Vernetzung des LSI mit anderen Behörden mit Cybersicherheitsaufgaben auf internationaler, Bundes- und Landesebene, aber auch im Bereich der Forschung, bündelt und erweitert das LSI seine hohe Fachkompetenz, um im Rahmen seines gesetzlichen Auftrages bestmöglich zu unterstützen.

Im Gesundheitsbereich können die bayerischen Plankrankenhäuser für Investitionen im Bereich der Cybersicherheit auf die pauschalen Fördermittel aus dem Krankenhausförderetat zurückgreifen. Diese betragen aktuell rund 318 Mio. Euro und können von den Trägern eigenverantwortlich – etwa auch für IT-Sicherheit- und Digitalisierungsprojekte – eingesetzt werden.

Darüber hinaus stehen den Plankrankenhäusern insgesamt rd. 590 Mio. Euro aus dem Krankenhauszukunftsfonds des Bundes zur Verfügung. Die notwendige Kofinanzierung in Höhe von rd. 180 Mio. Euro wurde hierbei vom Freistaat Bayern unternommen. Die Mittel aus dem Krankenhauszukunftsfonds sind insbesondere für Investitionen in die IT-Sicherheit vorgesehen. So müssen für jedes Projekt mindestens 15 Prozent der Kosten für Maßnahmen in die IT-Sicherheit aufgewendet werden. Diese Quote wird mit rd. 117 Mio. Euro, die ausschließlich für die IT-Sicherheit verwendet werden, deutlich überschritten.

Im Übrigen wird auf die Antwort zu Frage 6 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.