Bayerischer Landtag

19. Wahlperiode 02.06.2025 Drucksache 19/6511

Schriftliche Anfrage

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

Hacker- und Cyberangriffe in Bayern seit 2019 II

Die Staatsregierung wird gefragt:

Antwort

des Staatsministeriums des Innern, für Sport und Integration in Abstimmung mit dem Staatsministerium der Finanzen und für Heimat
vom 29.04.2025

Vorbemerkung:
Soweit parlamentarische Anfragen Umstände betreffen, die aus Gründen des Staatswohls geheimhaltungsbedürftig sind, ist zu prüfen, ob und auf welche Weise die Geheimhaltungsbedürftigkeit mit dem parlamentarischen Informationsanspruch in Einklang gebracht werden kann (vgl. Entscheidungen des Bundesverfassungsgerichts [BVerfGE] 124, 161 [189]). Die Staatsregierung ist nach sorgfältiger Abwägung des Informationsrechts des Abgeordneten mit dem Staatswohl, das durch Bekanntwerden geheimhaltungsbedürftiger Informationen gefährdet werden könnte, zu der Auffassung gelangt, dass aufgrund der Schutzbedürftigkeit der erbetenen Informationen eine Beantwortung der Fragen 5 a, 5 b, 6 a und 6 b und 7 a teilweise nicht erfolgen kann.

Eine öffentliche Bekanntgabe detaillierter Informationen zu einzelnen Aufklärungserkenntnissen des Landesamts für Verfassungsschutz (BayLfV) im Bereich der Spionageabwehr über die Aktivitäten von ausländischen Nachrichtendiensten und damit einhergehend die Kenntnisnahme durch Unbefugte hätte erhebliche nachteilige Auswirkungen auf die Sicherheit des Landes. Entsprechendes gilt für die internen Vorgänge des BayLfV. Die preisgegebenen Informationen könnten insbesondere von ausländischen Nachrichtendiensten genutzt werden, um ihre Methoden und die eigene Erkenntnislage anzupassen. Die künftige Aufgabenerfüllung des BayLfV wäre somit erheblich beeinträchtigt. Hierdurch könnten signifikante Lücken mit Folgewirkungen für die Sicherheitslage im Freistaat Bayern und der Bundesrepublik Deutschland entstehen.

Auch eine VS-Einstufung und Hinterlegung der angefragten Informationen in der VS-Registratur des Landtags würde ihrer erheblichen Relevanz im Hinblick auf die Bedeutung der Aufgabenerfüllung des BayLfV und die Sicherung des Staatswohls nicht ausreichend Rechnung tragen. Die angefragten Informationen würden gerade angesichts ihres spezifischen Detailierungsgrades in einem so bedeutenden Maße Aufschluss über das mögliche Potenzial der Aktivitäten ausländischer Nachrichtendienste geben, dass eine Weitergabe der besonders geheimhaltungsbedürftigen Informationen auch gegenüber einem eng begrenzten Kreis von Empfängern nicht vertreten werden kann. Je größer der Kreis an Geheimnisträgern ist, umso höher ist die Wahrscheinlichkeit, dass Geheimnisse, sei es absichtlich oder versehentlich, weitergegeben oder ausgespäht werden (vgl. BVerfGE 70, 324 [364]).

1.a) Welche Ransomware-Angriffe auf bayerische Behörden, Kommunen und öffentliche Einrichtungen wurden seit dem 1. Januar 2019 registriert?

1.b) Welche finanziellen Schäden sind durch diese Angriffe entstanden?

1.c) Welche anderen Schäden und Einschränkungen wurden durch diese Ransomware-Angriffe verursacht?

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

Dem Landesamt für Sicherheit in der Informationstechnik (LSI) ist kein erfolgreicher Ransomware-Angriff auf staatliche Behörden im angegebenen Zeitraum bekannt. Bisherige Angriffsversuche verschiedener Ransomware-Gruppierungen, wie zum Beispiel GootKit, Lockbit, Lockbit 2.0 und INC, waren nicht erfolgreich. Durch die Möglichkeit, Angriffsversuche frühzeitig durch das Sicherheitsmonitoring des LSI zu erkennen, konnten potenzielle Kompromittierungen bereits zu einem frühen Zeitpunkt abgewehrt werden.

Dem LSI liegt keine Statistik im Sinne der Fragestellung zu erfolgreichen Ransomware-Angriffen auf bayerische Kommunen vor, da für Kommunen keine Pflicht zur Meldung von Cyberangriffen an das LSI besteht.

2.a) Welche DDoS-Attacken auf staatliche Webseiten bayerischer Behörden und Institutionen gab es seit 1. Januar 2019?

2.b) Welche Behörden waren am häufigsten betroffen?

2.c) Wie lange dauerten die Ausfälle im Durchschnitt?

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

DDoS-Angriffsversuche auf staatliche Webseiten bayerischer Behörden finden laufend statt. Zur Abwehr wird vom Vertragspartner, der die Internetanbindung des Behördennetzes betreibt, providerseitig ein DDoS-Abwehrsystem eingesetzt, das Angriffsversuche automatisiert erkennt und frühzeitig blockiert. Daher werden nicht alle Angriffsversuche vom LSI erfasst, sodass keine Statistik im Sinne der Fragestellung vorliegt.

DDoS-Angriffe eines größeren Ausmaßes werden seitens des LSI zur Anzeige gebracht. Seit 2019 wurden 29 Fällen angezeigt, schwerpunktmäßig in den Jahren 2019 (9 Fälle) und 2020 (12 Fälle).

Ziele der Angreifer sind in der Regel Webseiten mit großer Außenwirkung, etwa der Internetauftritt der Polizei. Ausfallzeiten wurden nicht statistisch erfasst. Angriffstechniken ändern sich dynamisch, sodass die Abwehrmaßnahmen laufend angepasst werden müssen.

Im Übrigen wird auf die Antwort der Staatsregierung vom 29. April 2025 zu Frage 3a der Schriftlichen Anfrage des Abgeordneten Florian von Brunn (SPD) betreffend Hacker- und Cyberangriffe in Bayern seit 2019 I verwiesen.

3.a) Wie viele Fälle von Datendiebstahl oder -verlust bei bayerischen Behörden und öffentlichen Einrichtungen wurden seit 1. Januar 2019 gemeldet?

3.b) Welche Arten von Daten waren betroffen?

3.c) Wie viele Bürgerinnen und Bürger wurden durch diese Vorfälle geschädigt?

Die Fragen 3a bis 3c werden aufgrund des Sachzusammenhangs zusammen beantwortet.

Eine Meldepflicht für Datenschutzverletzungen besteht nach Art. 33 der Datenschutz-Grundverordnung nur gegenüber den Datenschutzaufsichtsbehörden. Der Landesbeauftragte für den Datenschutz, der für Meldungen bayerischer öffentlicher Stellen zuständig ist, ist aufgrund europa- und verfassungsrechtlicher Vorgaben nicht Teil der Staatsregierung. Daher liegen der Staatsregierung insoweit keine Angaben zu gemeldeten Datenschutzverletzungen bei bayerischen öffentlichen Stellen vor.

Hinsichtlich der Kommunen führt das LSI keine Statistik im Sinne der Fragestellung, da gegenüber dem LSI keine Pflicht zur Meldung von Datenverlusten besteht.

Allgemein wird mitgeteilt, dass das Lagezentrum des LSI seit 2019 rund 1600 IT-Sicherheitsvorfälle unterschiedlichster Schwere im kommunalen Umfeld bearbeitet hat. In diesen Fällen hat das LSI die betreffenden Kommunen im unterschiedlichen Grad bei Aufklärung bzw. Bewältigung der Vorfälle unterstützt. Eine händische Auswertung würde zu keiner aussagekräftigen Zahlenangabe führen und entsprechend unverhältnismäßigen Aufwand verursachen.

Im Übrigen wird auf die Antwort der Staatsregierung vom 29. April 2025 zu Fragenkomplex 2 der Schriftlichen Anfrage des Abgeordneten Florian von Brunn (SPD) betreffend Hacker- und Cyberangriffe in Bayern seit 2019 I verwiesen.

4.a) Wie viele Phishing-Angriffe auf Mitarbeiter bayerischer Behörden und öffentlicher Einrichtungen wurden seit 1. Januar 2019 verzeichnet?

4.b) Welche finanziellen Schäden sind durch erfolgreiche Phishing-Angriffe entstanden?

Die Fragen 4a und 4b werden aufgrund des Sachzusammenhangs zusammen beantwortet.

Phishing-Mails werden neben anderem unerwünschtem Mailverkehr bereits weitgehend an der Netzgrenze des Behördennetzes erkannt und blockiert. Die Erhebung konkreter Kennzahlen für Gründe von Nichtzustellung erfolgt nicht. Alleine 2024 wurden von 500 Mio. Zustellversuchen (E-Mails) 390 Mio. blockiert, diese beinhalten unter anderem auch Phishing-Mails.

Im Übrigen wird auf die Antwort der Staatsregierung vom 29. April 2025 zu Frage 3a der Schriftlichen Anfrage des Abgeordneten Florian von Brunn (SPD) betreffend Hacker- und Cyberangriffe in Bayern seit 2019 I verwiesen.

4.c) Welche Schulungs- und Sensibilisierungsmaßnahmen wurden durchgeführt, um Mitarbeitende besser vor Phishing-Angriffen zu schützen?

Das LSI bietet allen Mitarbeitern staatlicher und kommunaler Behörden kostenfreie Onlineschulungen zu IT-Sicherheit an, die auch für Phishing-Angriffe sensibilisieren.

Staatlichen und kommunalen Behörden bietet das LSI daneben Phishing-Simulationen an, um Mitarbeiter für Phishing zu sensibilisieren.

5.a) Wie viele Fälle von vermuteter Cyberspionage gegen bayerische Behörden und Unternehmen wurden seit 1. Januar 2019 registriert?

Zu den Spionageaktivitäten von Regierungen anderer Länder sowie zur Cyberspionage wird allgemein auf den Verfassungsschutzbericht Bayern 2024, S. 300 ff. und S. 327 ff., verwiesen.

Im Übrigen wird auf die Vorbemerkung verwiesen.

5.b) Welche Sektoren oder Behörden waren besonders von Spionageversuchen betroffen?

Auf die Vorbemerkung wird verwiesen.

5.c) Welche Maßnahmen wurden ergriffen, um die Abwehr von und die Resilienz gegen Ransomware-, DDoS-Angriffe und Cyberspionage zu verbessern?

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.

6.a) Wie viele Advanced-Persistent-Threats-Angriffe (APT-Angriffe) wurden seit dem 1. Januar 2019 auf bayerische Behörden, Kommunen, Unternehmen und kritische Infrastrukturen registriert (bitte mit Nennung der Angriffsgruppen, z. B. staatliche Akteure oder organisierte Kriminalität)?

6.b) Welche Schäden sind durch APT-Angriffe entstanden (finanziell, Datenverlust, Betriebsunterbrechungen)?

Die Fragen 6 a und 6 b werden aufgrund des Sachzusammenhangs zusammen beantwortet.

Seitens des LSI werden grundsätzlich keine Attribuierungen vorgenommen. Inwieweit Informationen über Angreifer vorliegen, hängt vom jeweiligen Einzelfall ab. Eine Statistik im Sinne der Fragestellungen liegt dem LSI daher nicht vor.

Allgemein wird zu den Spionageaktivitäten von Regierungen anderer Länder auf den Verfassungsschutzbericht Bayern 2024, S. 300 ff., sowie auf den Bericht zur Cybersicherheit in Bayern 2024, S. 9 f., verwiesen, die öffentlich über das Internet verfügbar sind.

Im Übrigen wird auf die Vorbemerkung verwiesen.

6.c) Welche spezifischen Maßnahmen wurden in Bayern ergriffen, um die Erkennung, Abwehr und Schadensbegrenzung bei APT-Angriffen zu verbessern (z. B. Einsatz von KI, Schulungen, externe Experten)?

Durch das umfassende Sicherheitsmonitoring des LSI sowie den Betrieb zentraler Sicherheitsinstanzen werden im Behördennetz potenzielle Angriffe frühzeitig erkannt und abgewehrt. Hierbei hilft auch die stetige Anreicherung von Indikatoren zur Angriffserkennung mittels eigener Analysen und dem intensiven Austausch mit Partnern. Die Abwehrmechanismen des LSI werden in enger Zusammenarbeit mit den staatlichen Rechenzentren kontinuierlich weiterentwickelt. Die hochautomatisierten Maßnahmen zum Schutz des Behördennetzes verhindern unter anderem präventiv rund 1,2 Mrd. potenziell schadhafte Internetaufrufe pro Monat. Für die Reaktion auf Sicherheitsvorkommnisse unterhält der Freistaat Bayern ein Computer Emergency Response Team (CERT) im LSI, das durch eine Rufbereitschaft rund um die Uhr erreichbar ist.

Im Übrigen wird auf den Verfassungsschutzbericht Bayern 2024, S. 315 ff., sowie auf den Bericht zur Cybersicherheit in Bayern 2024, S. 9 f. und 14 ff., verwiesen, die öffentlich über das Internet verfügbar sind.

7.a) Wie haben sich die personellen und finanziellen Ressourcen für die Cybersicherheit in Bayern seit 1. Januar 2019 entwickelt?

Die Gewährleistung der Cybersicherheit ist eine Querschnittsaufgabe in allen Ressorts und wird jeweils in der Breite der Organisation wahrgenommen. Es ist daher nicht immer möglich, aufgewendete personelle und finanzielle Ressourcen eindeutig der Cybersicherheit zuzuordnen. Die Beantwortung fokussiert sich deshalb auf die Entwicklung der Ressourcen bei den bayerischen Behörden und Einrichtungen mit operativen Cybersicherheitsaufgaben.

Seit Gründung Ende 2017 wurde der Personalaufbau im LSI kontinuierlich vorangetrieben, derzeit beschäftigt das LSI rund 160 Personen. Personell soll das LSI auf insgesamt 200 Personen anwachsen.

Bei der Bayerischen Polizei wurden flächendeckend „Cybercrime“-Kommissariate bei grundsätzlich jeder Kriminalpolizeiinspektion eingerichtet. Neben dem Kriminalfachdezernat 12 in München (seit 1. April 2014) besteht mit dem Kriminalfachdezernat 5 (seit 1. Juni 2021) nun auch eine eigens eingerichtete Schwerpunktdienststelle zur kriminalpolizeilichen Bekämpfung von Cybercrime im Ballungsraum Nürnberg.

Daneben wurde die Sonderlaufbahn der IT-Kriminalisten geschaffen. Hierbei werden studierte Informatiker in einer einjährigen polizeifachlichen Unterweisung zu Polizeivollzugsbeamten ausgebildet und unterstützen die Dienststellen in der Bekämpfung der Cyberkriminalität. Mittlerweile werden 200 IT-Kriminalisten bei der Bayerischen Polizei eingesetzt.

Darüber hinaus beschäftigt die Bayerische Polizei mittlerweile ca. weitere 400 Spezialisten in diesem Bereich. Dabei handelt es sich um ca. 300 speziell aus- und fortgebildete Ermittler bei den Kommissariaten und Dezernaten für Cybercrime und ca. 100 IT-Forensiker, die durch Sicherung und Aufbereitung digitaler Spuren die Ermittlungen unterstützen.

Seit 1. Juli 2021 sind bei allen Polizeipräsidien und dem Landeskriminalamt Cybercrime Quick-Reaction-Teams (QRT) eingerichtet, die über eine Rund-um-die-Uhr-Erreich-

barkeit verfügen und bei schwerwiegenden Cybervorfällen eine schnelle Reaktionsfähigkeit gewährleisten.

Bei der Zentralstelle Cybercrime Bayern (ZCB) bei der Generalstaatsanwaltschaft Bamberg ermitteln bayernweit mittlerweile 25 juristisch, technisch und ermittlungstaktisch geschulte Spezialstaatsanwälte und vier IT-Forensiker in besonders komplexen und schwerwiegenden Fällen im Bereich Cyberkriminalität.

Das BayLDA ist zu einer Datenschutzaufsichtsbehörde für alle nichtöffentlichen Stellen in Bayern mit einer Personalstärke von 38 Planstellen aufgewachsen.

Hinsichtlich des Personaleinsatzes im BayLfV wird auf die Vorbemerkung verwiesen.

7.b) Welche spezialisierten Einheiten oder Behörden sind für die Abwehr von Cyberangriffen in Bayern zuständig?

Die wesentlichen Akteure zur Abwehr sowie der Eindämmung von Cyberangriffen in Bayern sind

– das Landesamt für Sicherheit in der Informationstechnik (LSI),
– das Cyber-Allianz-Zentrum Bayern (CAZ) beim BayLfV,
– die Zentrale Ansprechstelle Cybercrime (ZAC) beim Landeskriminalamt sowie
– die Quick-Reaction-Teams (QRT) der Bayerischen Polizei.

7.c) Welche Pläne gibt es, um die Fähigkeiten zur Cyberabwehr in Bayern weiter auszubauen?

Die Fortentwicklung der operativen Fähigkeiten der bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben erfolgt nach Maßgabe der Bayerischen Cybersicherheitsstrategie 2.0. Unter dem Leitgedanken „Resilienz von Staat, Wirtschaft und Gesellschaft gegen Cyberangriffe bedarfsgerecht stärken“ bilden die darin aufgeführten strategischen Ziele die Leitplanken für das staatliche Handeln im Bereich Cybersicherheit.

Die Umsetzung der daraus abgeleiteten Maßnahmen erfolgt durch das jeweils zuständige Ressort im Rahmen der zur Verfügung stehenden Stellen und Mittel bzw. bleibt künftigen Haushaltsverhandlungen vorbehalten.

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.