Bayerischer
Landtag

19. Wahlperiode 10.12.2025 Drucksache 19/8802

Schriftliche Anfrage

des Abgeordneten **Florian von Brunn SPD**
vom 17.09.2025

Cyberabwehr in Bayern: Blindflug im Dunkelfeld?

Die fortschreitende Digitalisierung durchdringt nahezu alle Bereiche des öffentlichen Lebens und der Wirtschaft in Bayern. Sie ist zweifellos ein Motor für Effizienz und Innovation, birgt jedoch auch eine stetig wachsende Bedrohung durch Cyberangriffe, deren Komplexität und Häufigkeit in den letzten Jahren signifikant zugenommen hat. Die Antworten der Staatsregierung auf die Schriftlichen Anfragen „Hacker- und Cyberangriffe in Bayern seit 2019 I und II“ haben zwar erste Einblicke in die Lage gegeben, aber zugleich erhebliche Wissens- und Datensicherheitslücken offengelegt. Die Staatsregierung räumt ein, dass sie über Cyberangriffe auf Kommunen, Krankenhäuser und einen Großteil der bayerischen Unternehmen keine belastbaren Statistiken hat, da hierfür keine Meldepflichten existieren.

Ein effektives Krisen- und Risikomanagement setzt jedoch eine genaue Kenntnis der Bedrohungslage voraus. Der Vergleich zwischen den offiziell erfassten Schäden und den Schätzungen von Industrieverbänden verdeutlicht einen fundamentalen Mangel an staatlicher Lagekenntnis, da polizeiliche Zahlen nur das sog. „Hellfeld“ abbilden, während ein Großteil der Angriffe im Dunkelfeld verbleibt. Diese fehlende Datengrundlage ist eine strukturelle Schwachstelle, da sie die Fähigkeit der Staatsregierung beeinträchtigt, übergeordnete Trends zu erkennen und rechtzeitig wirksame Abwehrmaßnahmen zu entwickeln. Zudem ist die Strafverfolgung der Justiz aufgrund mangelnder statistischer Erfassung nicht in der Lage, die Erfolge der polizeilichen Ermittlungen nachzuverfolgen.

Ohne ein umfassendes Lagebild droht der Freistaat im Umgang mit dieser zentralen Sicherheitsherausforderung im „Blindflug“ zu agieren. Die Notwendigkeit einer klaren und transparenten Datengrundlage ist daher von überragender Bedeutung, um die Resilienz des Freistaates Bayern, seiner kritischen Infrastrukturen und seiner Wirtschaft nachhaltig zu stärken und das Vertrauen der Bürgerinnen und Bürger in die Fähigkeiten des Staates zu sichern.

Die Staatsregierung wird gefragt:

1.a) Wie erklärt die Staatsregierung die massive Diskrepanz zwischen den in ihrer Antwort genannten polizeilichen Schadenssummen für bayerische Unternehmen (z. B. 2023: ca. 74 Mio. Euro) und den aktuellen Jahresschadensschätzungen des Digitalverbands Bitkom für die deutsche Wirtschaft, die bei über 267 Mrd. Euro liegen? 4

Antwort

des Staatsministeriums des Innern, für Sport und Integration in Abstimmung mit dem Staatsministerium der Justiz, dem Staatsministerium der Finanzen und für Heimat sowie dem Staatsministerium für Gesundheit, Pflege und Prävention, soweit die dortigen Geschäftsbereiche betroffen sind
vom 04.11.2025

1.a) Wie erklärt die Staatsregierung die massive Diskrepanz zwischen den in ihrer Antwort genannten polizeilichen Schadenssummen für bayerische Unternehmen (z. B. 2023: ca. 74 Mio. Euro) und den aktuellen Jahresschadensschätzungen des Digitalverbands Bitkom für die deutsche Wirtschaft, die bei über 267 Mrd. Euro liegen?

Die Unterschiede zwischen den in der Polizeilichen Kriminalstatistik (PKS) dokumentierten Schäden in bayerischen Unternehmen durch Cyberangriffe und den vom Digitalverband Bitkom e. V. in seiner Studie „Wirtschaftsschutz 2024“ für die gesamte deutsche Wirtschaft abgegebenen Jahresschadensschätzungen in Höhe von 266,6 Mrd. Euro (davon 178,6 Mrd. Euro durch Cyberattacken) ergeben sich aus den folgenden Umständen und Rahmenbedingungen:

Bei den in der Bitkom-Studie aufgeführten Schadenssummen handelt es sich um eine geschätzte Extrapolation auf Grundlage von Umfrageergebnissen bei 1 003 Unternehmen in Deutschland mit mindestens zehn Beschäftigten und einem Jahresumsatz von 1 Mio. Euro oder mehr. Die nach bundeseinheitlichen Richtlinien geführte PKS für Bayern enthält systemimmanent ausschließlich die der Polizei bekannt gewordenen Straftaten, einschließlich der strafbewehrten Versuche (sog. Hellfeld) mit Tatort in Bayern. Eine Hochrechnung, um ein bestehendes Dunkelfeld (nicht angezeigte Taten) auszugleichen, findet nicht statt.

Die gegenüber der Polizei angesetzten Schadenssummen sind dabei meist erste grobe Schätzungen der geschädigten Unternehmen und beziehen sich häufig nur auf die gestellten Lösegeldforderungen, wohingegen die Schadensschätzungen des Branchenverbandes Bitkom e. V. weitere kostenintensive Positionen wie beispielsweise Produktionsausfälle, Betriebsunterbrechungen, Kosten für IT-Forensik und Datenwiederherstellung sowie Reputationsverlust (z. B. durch Kurseinbrüche) umfassen.

1.b) Was unternimmt die Staatsregierung konkret, um das von ihr im „Bericht zur Cybersicherheit“ anerkannte „erhebliche Dunkelfeld“ zu verkleinern und die Bereitschaft von Unternehmen und Privatpersonen zur Anzeigenerstattung zu erhöhen?

Mit der Bayerischen Cybersicherheitsstrategie 2.0 hat die Staatsregierung die wesentlichen Bestandteile und Herausforderungen moderner Cybersicherheitspolitik zielsicher identifiziert und den strategischen Handlungsrahmen für die Behörden und Einrichtungen mit Cybersicherheitsaufgaben geschaffen, um diese strukturiert zu bewältigen.

Zu den im Handlungsfeld „Schutz der Wirtschaft und Wissenschaft“ festgelegten Zielen zählt – neben der Stärkung der Resilienz von Wirtschaft und Forschung in Bayern gegen Cyberkriminalität, Cyberspionage und -sabotage – auch die weitere Verbesserung des Anzeigeverhaltens (Dunkelfeldaufhellung) im Deliktsfeld Cybercrime.

Um die Bereitschaft zur Anzeigenerstattung weiter zu erhöhen, erfolgen u. a. zielgruppenspezifische Informationsangebote und öffentlichkeitswirksame Veranstaltungen, um potenzielle Angriffsopfer noch intensiver über die Möglichkeiten, Fähigkeiten und Zuständigkeiten der Strafverfolgungsbehörden im Bereich Cybercrime aufzuklären.

Damit einhergehend werden, insbesondere durch strukturelle Maßnahmen, die notwendigen fachlichen Kompetenzen bei den Behörden und Einrichtungen mit Cybersicherheitsaufgaben mit hinreichenden Kapazitäten auf- und sukzessive weiter ausgebaut.

Beim Landeskriminalamt (BLKA) wurde die „Zentrale Ansprechstelle Cybercrime“ (ZAC) etabliert. Diese steht allen (Wirtschafts-)Organisationen als kompetenter Ansprechpartner zur Verfügung. Das Beratungsspektrum umfasst hier sowohl Präventionsangebote als auch Unterstützung im Falle eines erfolgten Cyberangriffs.

Die Rahmenkonzeption „Polizeiliche Cybercrime-Präventionsberatung“ richtet die jeweiligen Präventionsmaßnahmen auch auf die verantwortlichen Entscheidungsträger in diesen Organisationen aus. Hierzu kooperiert die ZAC mit Multiplikatoren (Verbände, Kammern u. a.), nutzt deren Reichweite und adressiert in mehreren Vortragsmodulen (online und in Präsenz) aktuelle Kriminalitätsphänomene. Regionale Maßnahmen werden zudem durch die örtlich zuständigen Polizeipräsidien umgesetzt.

Daneben gewährleisten „Quick-Reaction-Teams“ (QRT) seit 2021 die Rund-um-die-Uhr-Verfügbarkeit qualifizierter polizeilicher Kräfte. Diese unterstützen geschädigte (Wirtschafts-)Organisationen bei der Bewältigung andauernder oder kürzlich erfolgter Cyberangriffe und verbessern den Austausch von Informationen zu diesen Angriffen.

Eine weitere wichtige Maßnahme zur Verkleinerung des Dunkelfelds ist die effektive Strafverfolgung im Bereich der Cyberkriminalität. Um Cyberkriminalität effektiv zu verfolgen, besteht bei der Generalstaatsanwaltschaft Bamberg die Zentralstelle Cybercrime Bayern (ZCB), die für komplexe und schwerwiegende Cybercrimefälle zuständig ist. Mit derzeit 30 juristisch, technisch und ermittlungstaktisch speziell geschulten Staatsanwältinnen und Staatsanwälten sowie vier IT-Forensikern ist die ZCB eine der größten und erfahrensten Spezialstaatsanwaltschaften in Deutschland. Um die effektive Verfolgung jeder Art von Cyberkriminalität in Bayern sicherzustellen, gibt es zudem für Fälle, in denen die ZCB nicht zuständig ist, bei allen 22 Staatsanwaltschaften und den drei Generalstaatsanwaltschaften in Bayern IT-Sonderdezernate und IT-Ansprechpartner.

Ein wichtiger Schwerpunktbereich der ZCB ist die Bekämpfung von Cyberangriffen auf Unternehmen und Einrichtungen, wofür die Taskforce „Cyberangriffe auf Unternehmen und Einrichtungen“ besteht. Um die Anzeigebereitschaft in Unternehmen zu erhöhen, steht dort eine Oberstaatsanwältin speziell für Unternehmen als Ansprechpartnerin zur Verfügung. Zudem werden die für Unternehmen wichtigen Informationen in der vom Staatsministerium der Justiz herausgegebenen Broschüre „Cybercrime – Hilfe für betroffene Unternehmen“ bereitgestellt.

Im Rahmen des gemeinsam vom Staatsministerium des Innern, für Sport und Integration und vom Staatsministerium der Justiz mit der IHK für München und Oberbayern bereits zum zweiten Mal veranstalteten Cybersecurity Day am 29.01.2025 wurden Unternehmen unter dem Motto „Gelebte Cybersicherheit im Unternehmen – Strategie, Technik und Mensch“ über aktuelle Cyberbedrohungen informiert. Konkret wurde dort bei einem Workshop der Zentralen Ansprechstelle Cybercrime (ZAC) beim Landeskriminalamt und der Zentralstelle Cybercrime Bayern (ZCB) bei der Generalstaatsanwaltschaft Bamberg erläutert, warum Polizei und Staatsanwaltschaft ein unverzichtbarer Partner der Unternehmen bei der Bekämpfung von Cyberangriffen sind.

Um die Bereitschaft von Privatpersonen zur Anzeigeerstattung zu erhöhen, wird auch die Öffentlichkeit regelmäßig über die Gefahren im Cyberbereich informiert und auf aktuelle Phänomene hingewiesen, beispielsweise in Pressekonferenzen, wie z. B. zum Thema Phishing oder Cyberlagebericht Bayern und Pressemitteilungen.

1.c) Welche Maßnahmen sind vorgesehen, um die Erfassungsmethoden in der polizeilichen Kriminalstatistik und den Justizstatistiken zu verbessern, da das Staatsministerium der Justiz bestätigt, dass die Strafverfolgung nicht nach dem Phänomenbereich „Cyberkriminalität“ erfasst wird?

In der PKS wird der Phänomenbereich Cybercrime über die PKS-Sonderkennung (Tatmittel Internet und/oder IT-Geräte) und über den PKS-Summenschlüssel 899000 Cybercrime (vor 2021 wurde dieser Summenschlüssel mit Computerkriminalität bezeichnet) abgebildet. Dieser Summenschlüssel bildet begrifflich Straftaten ab, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne).

Zudem besteht die Möglichkeit, PKS-Fälle, die Bezüge zum Bereich Cybercrime aufweisen, mit einem der folgenden PKS-Phänomenwerte zu versehen, welche entsprechende Auswertungen ermöglichen:

– NFC-Manipulation (Nahfeldkommunikation, abgekürzt NFC)
– NFC-Manipulation mit Persönlicher Identifikationsnummer (PIN)
– NFC-Manipulation ohne PIN
– Angriff auf das Onlinebanking
– Ransomware
– Digitaler Identitätsdiebstahl/Accountübernahme
– (D)Dos-Attacke
– Eindringen in Datennetze/Datenveränderung/Datendiebstahl bei nichtnatürlichen Personen

Die bundeseinheitlich zwischen allen Ländern abgestimmten Justizgeschäftsstatistiken der Gerichte und Staatsanwaltschaften sind reine Verfahrensstatistiken, bei denen grundsätzlich keine Tatmodalitäten und Angaben zu Beteiligten erhoben werden. Erfasst wird nach Sachgebieten zusammengefasst nur das tatschwerste Delikt. Die Justizgeschäftsstatistiken dienen in erster Linie dazu, die Arbeitsbelastung der Gerichte und Staatsanwaltschaften nachvollziehen zu können, und nicht dazu, Kriminalitätsentwicklungen aufzuzeigen. Darüber hinaus würde für eine Erfassung personenbezogener Daten von Beteiligten die notwendige Rechtsgrundlage fehlen.

Vor diesem Hintergrund hat die letzte Bundesregierung an dem Entwurf eines Gesetzes über die Statistiken der Strafrechtspflege des Bundes (Strafrechtspflegestatistikgesetz – StrafStatG) gearbeitet, der die Grundlage für evidenzbasierte Entscheidungen auf dem Gebiet der Kriminalpolitik bilden sollte. Dieser Entwurf ist mit Ablauf der Legislaturperiode der Diskontinuität anheimgefallen und wurde von der aktuellen Bundesregierung nicht wieder aufgegriffen.

Auch bei der bayerischen Strafverfolgungsstatistik handelt es sich um eine statistische Datenerhebung nach bundeseinheitlichen Vorgaben. Um etwaige Erkenntnislücken zu schließen, bedürfte es ebenfalls einer bundeseinheitlichen Lösung.

2.a) Warum besteht für bayerische Kommunen nach wie vor keine Pflicht zur Meldung von Cyberangriffen an das Landesamt für Sicherheit in der Informationstechnik (LSI) oder eine andere zentrale Landesbehörde, obwohl die Staatsregierung selbst festhält, dass Kommunalverwaltungen ein Ziel von Cyberangriffen sind?

2.b) Welche konkreten Gefahren sieht die Staatsregierung in der fehlenden Datengrundlage über erfolgreiche Angriffe auf Kommunen, insbesondere im Hinblick auf die Fähigkeit, übergeordnete Trends zu erkennen, rechtzeitig zu warnen und wirksame Abwehrmaßnahmen zu entwickeln?

2.c) Wie gedenkt die Staatsregierung zu gewährleisten, dass die freiwilligen und kostenlosen Unterstützungsangebote des LSI tatsächlich bei den bedürftigsten Kommunen ankommen und nicht nur von jenen genutzt werden, die bereits über eine hohe IT-Sicherheitskompetenz verfügen?

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

Für alle an das Behördennetz angeschlossenen Stellen bestehen aufgrund von Art. 43 Abs. 3 und Art. 49b Abs. 1 Bayerisches Digitalgesetz (BayDiG) Meldepflichten gegenüber dem Landesamt für Sicherheit in der Informationstechnik (LSI). Im Übrigen pflegt das LSI eine gute und vertrauensvolle Zusammenarbeit mit den Kommunen. Aufgrund von freiwilligen Meldungen, Analysen im Bayerischen Behördennetz, eigenen Recherchen sowie dem Austausch mit anderen Ländern und dem Bund geht das LSI von einem ausreichenden Überblick über die aktuelle IT-Sicherheitslage aus.

Im Fokus steht für das LSI die kompetente Unterstützung der bayerischen Kommunen, insbesondere im Angriffsfall, nicht das Erstellen von Statistiken. Die Unterstützung der Kommunen erfolgt gemäß Art. 42 Abs. 2 BayDiG jeweils auf Ersuchen. Die Angebote zur Beratung und allen weiteren konkreten Unterstützungen stehen allen bayerischen Kommunen jedoch uneingeschränkt zur Verfügung.

Alle Kommunen werden regelmäßig zu den Angeboten des LSI informiert. 2024 haben über 98 Prozent der bayerischen Kommunen kostenlose Angebote des LSI genutzt. Eine einseitige Nutzung der Angebote durch Kommunen mit „hoher IT-Sicherheitskompetenz“ ist nicht ersichtlich.

3.a) Welche Maßnahmen werden unternommen, um eine verpflichtende Meldepflicht für Cyberangriffe auf Plankrankenhäuser und Pflegeeinrichtungen einzuführen, da das Staatsministerium für Gesundheit, Pflege und Prävention (StMGP) seine Kenntnisse derzeit auf „allgemeine Presseberichterstattung“ beschränkt und eine solche Pflicht für Betreiber nicht existiert?

Für die Krankenhäuser, die der kritischen Infrastruktur zuzurechnen sind, besteht eine Meldepflicht gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (§ 8b Abs. 4 BSI-Gesetz – BSIG). Es wäre Sache des Bundesgesetzgebers, entsprechende Meldepflichten auch auf weitere Krankenhäuser auszudehnen und dies im Rahmen der einschlägigen Gesetze zu regeln.

Soweit das Heimrecht bezüglich der stationären Pflegeeinrichtungen und besonderen Wohnformen der Eingliederungshilfe betroffen ist, existiert bereits eine verpflichtende Meldepflicht der Betreiber für Cyberangriffe auf Pflegeeinrichtungen. Gemäß Art. 4 Abs. 6 Satz 1 Gesetz zur Regelung der Pflege-, Betreuungs- und Wohnqualität im Alter und bei Behinderung (Pflege- und Wohnqualitätsgesetz – PfleWoqG) haben stationäre (Pflege-)Einrichtungen der zuständigen Behörde besondere Ereignisse und die daraus eingeleiteten Maßnahmen unverzüglich anzuzeigen. Gemäß Art. 4 Abs. 6 Satz 2 Nr. 4 PfleWoqG liegen besondere Ereignisse im Sinn von Satz 1 vor, wenn eine erhebliche Beeinträchtigung für Bewohnerinnen und Bewohner oder des ordnungsgemäßen Betriebs der stationären Einrichtung oder besonderen Wohnform der Eingliederungshilfe zu befürchten oder eingetreten ist. Unter diese Norm lassen sich bereits nach derzeitiger Rechtslage Cyberangriffe subsumieren. Sofern durch einen solchen Angriff z. B. die EDV oder IT-Infrastruktur einer in Art. 4 Abs. 6 Satz 1 PfleWoqG genannten Einrichtung ganz oder teilweise in ihrer Funktion beeinträchtigt ist, kann zumindest auch ein ordnungsgemäßer Betrieb der Einrichtung nicht mehr gewährleistet werden. Je nach Art des Angriffs und der betroffenen Systeme ist auch eine erhebliche Bewohnerwohlgefährdung nicht auszuschließen. Über ein solches Ereignis wären die zuständigen Behörden, in Bayern die Fachstellen für Pflege und Behinderteneinrichtungen – Qualitätsentwicklung und Aufsicht (FQA), bei der zuständigen Kreisverwaltungsbehörde unverzüglich zu informieren. Gemäß Art. 23 Abs. 2 Nr. 2 PfleWoqG kann eine vorsätzliche oder fahrlässige Verletzung dieser Meldepflicht (nicht, nicht richtige oder nicht rechtzeitige Erstattung der Meldung) mit Geldbuße bis zu 10.000 Euro belegt werden.

3.b) Wie stellt die Staatsregierung sicher, dass es in bayerischen Krankenhäusern durch Cyberattacken zu keiner Gefährdung der Versorgungssicherheit kommt, obwohl eine Studie zeigt, dass ein Drittel der Vorfälle in deutschen Krankenhäusern zu geringen oder erheblichen Auswirkungen auf die Patientenversorgung führte?

Für die notwendigen Investitionen zum Schutz vor Cyberattacken können die bayerischen Plankrankenhäuser auf die pauschalen Fördermittel aus dem Krankenhausförderetat zurückgreifen. Diese betragen aktuell rd. 318 Mio. Euro jährlich und können von den Trägern eigenverantwortlich – etwa auch für die IT-Sicherheit – eingesetzt werden. Darüber hinaus stehen den Plankrankenhäusern insgesamt rd. 590 Mio. Euro aus dem Krankenhauszukunftsfonds des Bundes zur Verfügung. Die notwendige Ko-Finanzierung in Höhe von rd. 180 Mio. Euro wurde hierbei vom Freistaat Bayern übernommen. Die Mittel sind insbesondere für Investitionen in die IT-Sicherheit vorgesehen. So müssen für jedes Projekt mindestens 15 Prozent der Kosten hierfür aufgewendet werden. Diese Quote wird mit rd. 117 Mio. Euro, die ausschließlich für die IT-Sicherheit verwendet werden, deutlich überschritten.

3.c) Welche konkreten, messbaren Ergebnisse und Fortschritte kann die Staatsregierung hinsichtlich der Verwendung der 590 Mio. Euro aus dem Krankenhauszukunftsfonds vorlegen, insbesondere in Bezug auf die dort vorgeschriebenen 15 Prozent für IT-Sicherheitsmaßnahmen?

In Bayern wurden über 1 200 Förderanträge vom Landesamt für Pflege verbeschieden. Die Maßnahmen befinden sich zum Teil noch in der Umsetzung oder sind erst kürzlich abgeschlossen worden. Da auch bei den meisten abgeschlossenen Projekten das Verwendungsnachweisverfahren noch andauert, können aktuell noch keine abschließenden Aussagen getroffen werden.

4.a) Wie erklärt die Staatsregierung den in ihrem „Bericht zur Cybersicherheit“ angeführten Rückgang der Ransomware-Fälle in Bayern, während globale Studien und Berichte von einem deutlichen Anstieg der Angriffe berichten?

Ransomware ist nach wie vor eine prägende Bedrohung im Cyberraum. Die Unterschiede in den Fallzahlen liegen einerseits darin begründet, dass hier von einem Dunkelfeld im Bereich der Cyberkriminalität auszugehen ist. Diese Fälle werden polizeilich nicht bekannt. Anderseits ist der Rückgang der Ransomware-Fälle in Bayern auch auf Ermittlungserfolge und behördliche Takedown-Aktionen gegen Ransomware-Gruppierungen, z. B. die Gruppierung Lockbit, zurückzuführen. Eine ähnliche Entwicklung spiegelt sich auch im Bundeslagebild Cybercrime 2024 wider.

4.b) Welche Vorgehensweise empfiehlt die Bayerische Polizei, insbesondere die Quick-Reaction-Teams (QRT), den Opfern, wenn sie zur Zahlung eines Lösegeldes aufgefordert werden?

Die betroffenen Unternehmen entscheiden in Erpressungslagen im Einzelfall immer selbst, ob sie in Verhandlungen eintreten oder zahlungsbereit sind. Diesbezüglich wird auf die ausschließliche Entscheidungshoheit der Unternehmensverantwortlichen im Hinblick auf die betriebliche und wirtschaftliche Krisenbewältigung hingewiesen.

Die taktische Betreuung der QRT (ggf. unterstützt durch weitere Spezialisten) fördert die Definition realistischer strategischer, taktischer und operativer Ziele für eine mögliche Verhandlungsführung. Des Weiteren werden den Unternehmen Informationen aus benachbarten Verfahren oder bezüglich der Tätergruppierung und deren bisherigem Verhalten bereitgestellt.

Grundsätzlich wird seitens der Polizei dazu geraten, wenn möglich, nicht zu bezahlen, um das dem Modus Operandi zugrunde liegende Geschäftsmodell nicht weiter zu fördern und kriminelle Vereinigungen nicht zu unterstützen. Zudem kann eine kooperative Haltung gegenüber den Angreifern nicht garantieren, dass dadurch Schäden oder Folgeangriffe abgewendet werden.

Details zu Technik und Taktik der Verhandlungsführung können aus einsatztaktischen Gründen nicht näher beauskunftet werden.

4.c) Welche konkreten Maßnahmen werden ergriffen, um die Finanzierung des Cyberterrorismus durch Lösegeldzahlungen zu unterbinden?

In geeigneten Fällen können Transaktionen in Absprache mit der zuständigen Staatsanwaltschaft unter Einbeziehung kooperativer Kryptowährungsbörsen angehalten und sichergestellt werden. Auch über Netzwerke zur Vermögensabschöpfung bei bestimmten Kryptowährungen kann das Abgreifen der Lösegeldzahlungen gelingen.

5.a) Welche durchschnittliche Höhe hatten die Lösegeldforderungen in den bayerischen Fällen, die von den Sicherheitsbehörden begleitet wurden?

In der polizeilichen Erfassung von Ransomware-Fällen wird nicht eindeutig zwischen Lösegeldzahlungen und dem allgemeinen „Schaden“ unterschieden. Für Bayern wurden im Jahr 2024 Gesamtschäden bei Ransomware-Vorfällen dokumentiert, die von

einigen Tausend bis zu mehreren Mio. Euro reichten. Die durchschnittlich erfasste Schadenshöhe betrug rund 500.000 Euro.

5.b) Wie hat sich dieser Betrag seit 2019 entwickelt?

Die durchschnittlich erfasste Schadenshöhe bei Ransomware-Fällen ist seit 2019 deutlich gestiegen. 2019 lag sie noch bei rund 100.000 Euro pro Vorfall.

5.c) Wie viele der seit 2019 registrierten „über 16 000 Auffälligkeiten“ bei bayerischen Behörden haben tatsächlich zu einer erfolgreichen Kompromittierung von Systemen oder Daten geführt?

Im angefragten Zeitraum war das LSI im kommunalen Umfeld bei 24 Vorfällen beratend beteiligt, die als schwerwiegend einzustufen sind.

Im Übrigen wird auf die Antwort des Staatsministeriums des Innern, für Sport und Integration vom 29.04.2025 zu den Fragenkomplexen 2 und 3 der Schriftlichen Anfrage des Abgeordneten Florian von Brunn (SPD) vom 11.03.2025 betreffend „Hacker- und Cyberangriffe in Bayern seit 2019 I“ (Drs. 19/6508 vom 02.06.2025) verwiesen.

6.a) Welche konkreten Sicherheitslücken oder Angriffsmethoden waren am häufigsten für die erfolgreichen Angriffsversuche auf das bayerische Behördennetz verantwortlich?

6.b) Wie stellt die Staatsregierung die kontinuierliche und lückenlose Aktualisierung der Abwehrmaßnahmen sicher?

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

Mit dem LSI hat Bayern vor über sieben Jahren eine eigenständige Fachbehörde für IT-Sicherheit geschaffen. Im Cyber Defence Center des LSI kümmern sich IT-Sicherheitsexpertinnen und -experten in einem hochautomatisierten Umfeld um die Aktualisierung der Sicherheitssysteme, die Überwachung des bayerischen Behördennetzes, die Analyse von Bedrohungen und die schnelle Reaktion bei Auffälligkeiten. Durch das permanente technische Monitoring und die enge Zusammenarbeit mit anderen Cybersicherheitsbehörden wird gewährleistet, dass die Schutzmaßnahmen hochaktuell sind.

Die vom LSI am häufigsten beobachteten Angriffsversuche sind E-Mails mit schadhaftem Inhalt.

6.c) Wie gedenkt die Staatsregierung die Datenlücke in der Justizstatistik zu schließen?

Auf die Antwort zu Frage 1 c wird verwiesen.

7.a) Wie beurteilt die Staatsregierung die Aufklärungsquote bei Cyberkriminalität, die deutlich unter der Gesamtaufklärungsquote der Polizeilichen Kriminalstatistik liegt?

Ein Großteil der Straftaten im Bereich der Cyberkriminalität wird aus dem Ausland begangen oder der Tatort ist unbekannt. Der hohe Anteil an Auslandstaten stellt die Polizei im Bereich Cybercrime vor große Herausforderungen. Im Vergleich zu Inlandstaten zeichnet sich die Bearbeitung von Auslandstaten durch höheren Ermittlungsaufwand und eine niedrigere Aufklärungsquote aus. Um das Bedrohungspotenzial von Straftaten mit ausländischem oder ungeklärtem Tatort besser in der PKS abbilden zu können, werden entsprechende Straftaten, die ihre Wirkung (Erfolgsort) im Inland entfalten, erstmalig für das Berichtsjahr 2024 in der PKS erfasst. Die statistische Erfassung und Darstellung von Auslandstaten erfolgt dabei getrennt von den Inlandstaten. Demnach liegt die Aufklärungsquote für Auslandsstraftaten insgesamt bei 5,8 Prozent und für Auslandstaten im Deliktsbereich Cybercrime im engeren Sinne bei 2,1 Prozent. Tätergruppen, welche frequent aus dem Ausland agieren, können nur mit erheblichem Aufwand sowie unter enger polizeilicher und/oder justizieller Kooperation identifiziert werden. Allerdings ist nicht mit allen Staaten eine entsprechende polizeiliche bzw. justizielle Kooperation umsetzbar.

7.b) Welche konkreten Maßnahmen und Ressourcen werden zusätzlich bereitgestellt, um die Aufklärungsquote bei Cyberkriminalität signifikant zu verbessern?

Angesichts der Schnelllebigkeit des Phänomens Cyberkriminalität bedarf es insbesondere der ständigen Fortentwicklung technischer Fähigkeiten und Tools. Regelmäßige Marktschau und Beschaffungsprozesse erforderlicher Hard- und Softwareprodukte dienen dazu, die Cybercrime-Fachdienststellen der Bayerischen Polizei weiterhin dem Stand der Technik entsprechend zu befähigen, die Aufklärungsquote zu verbessern. Die personelle, strukturelle und technische Ausstattung der Cybercrime-Fachdienststellen wird darüber hinaus fortwährend geprüft und bedarfsgerecht angepasst.

7.c) Wie begründet die Staatsregierung juristisch ihre Position, dass selbst eine Einstufung als Verschlusssache und die Hinterlegung in der VS-Registratur des Landtags nicht ausreicht, um dem parlamentarischen Informationsrecht zu genügen?

8.a) Welche juristischen und operativen Kriterien legt die Staatsregierung bei der Abwägung zwischen dem Informationsrecht eines Abgeordneten und dem Staatswohl an?

Die Fragen 7 c und 8 a werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

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]).

Dabei ist im jeweiligen Einzelfall eine Abwägung zwischen dem parlamentarischen Informationsanspruch und den Belangen, die einer Weitergabe der angefragten In-

formationen entgegenstehen, zu treffen. Da diese Abwägung im jeweiligen Einzelfall anhand dessen konkreter Umstände zu treffen ist, ist eine allgemeine Benennung von Kriterien ohne Rücksicht auf den jeweiligen Sachbereich nicht möglich.

Ebenfalls ist zu prüfen, ob eine VS-Einstufung und Hinterlegung der angefragten Informationen in der VS-Registratur des Landtags den widerstreitenden Rechtspositionen zum Ausgleich verhelfen können.

Sachleitend ist hier insbesondere die Erwägung, ob eine Preisgabe gegenüber einem im Vergleich zu einer öffentlichen Beantwortung erheblich verringerten Kreis von Personen unter Berücksichtigung des Geheimhaltungsbedürfnisses aus Staatswohlgründen im jeweiligen Einzelfall möglich ist.

Einzustellen in die Abwägung ist dabei auch die Erwägung, dass je größer der Kreis an Geheimnisträgern ist, desto höher die Wahrscheinlichkeit ist, dass Geheimnisse, sei es absichtlich oder versehentlich, weitergegeben oder ausgespäht werden (vgl. BVerfGE 70, 324 [364]). Entsprechend ist zu prüfen, ob die geheimhaltungsbedürftige Information derart sensibel ist, dass selbst ein geringfügiges Risiko des Bekanntwerdens unter keinen Umständen hingenommen werden kann (vgl. BVerfGE 146, 1).

8.b) Was ist die konkrete, aufgeschlüsselte jährliche finanzielle und personelle Entwicklung für Cybersicherheit in allen bayerischen Ressorts seit 2019, über die in den Antworten genannten operativen Behörden hinaus?

Die Gewährleistung der Cybersicherheit ist eine Querschnittsaufgabe in allen Ressorts und wird jeweils in der Breite der Organisation wahrgenommen. Es ist daher nicht möglich, aufgewendete personelle und finanzielle Ressourcen eindeutig der Cybersicherheit zuzuordnen. IT-Sicherheit zählt im Allgemeinen zum Aufgabenbereich der Informationstechnik. Konkrete mit der IT-Sicherheit verbundene Stellen sind nur bei Kap. 06 20 ausgewiesen.

8.c) Welche spezifischen Pläne gibt es, um die Kapazitäten des LSI über die aktuell angestrebten 200 Personen hinaus weiter auszubauen, da der „Bericht zur Cybersicherheit“ eine weitere „zunehmende Komplexität und Frequenz von Cyberangriffen“ erwartet?

In Hinblick auf die Entwicklung der Cybersicherheitslage wird derzeit von einer bedarfsgerechten Ausstattung des LSI ausgegangen. Neben dem fragegegenständlichen Personalaufbau sind im Übrigen auch die technische Entwicklung der Abwehrmaßnahmen sowie Maßnahmen der Standardisierung und Konsolidierung zu nennen, wie sie im Verhältnis zu den Kommunen insbesondere im Rahmen der Zukunftskommission #Digitales Bayern 5.0 angestrebt werden.

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.