Mecklenburg-Vorpommern
Ministerium für Soziales,
Gesundheit und Sport

Die Staatssekretärin

An die
Präsidentin des Landtages
Mecklenburg-Vorpommern
Lennéstraße 1
Schloss

19053 Schwerin

Kleine Anfrage des Abgeordneten Thomas de Jesus Fernandes, Fraktion der AfD
Titel: Folgen des Cyberangriffes auf den Klinikverbund AMEOS für Mecklenburg-Vorpommern
Drs.-Nr.: 08/5258

Als Anlage übersende ich die Antwort der Landesregierung auf die vorbezeichnete Kleine Anfrage.

Mit freundlichen Grüßen
In Vertretung

Hartmut Renken

Anlage

Hausanschrift:
Ministerium für Soziales, Gesundheit und Sport Mecklenburg-Vorpommern
Werderstraße 124 · 19055 Schwerin

Postanschrift:
Ministerium für Soziales, Gesundheit und Sport Mecklenburg-Vorpommern
19048 Schwerin

Telefon: 0385/588-19077
Telefax: 0385/588-19709
E-Mail: poststelle@sm.mv-regierung.de
Internet: www.mv-regierung.de/sm

LANDTAG MECKLENBURG-VORPOMMERN
8. Wahlperiode

Drucksache 8/5258

(Termin zur Beantwortung
gemäß § 64 Absatz 1 GO LT:
16.09.2025)

KLEINE ANFRAGE

des Abgeordneten Thomas de Jesus Fernandes, Fraktion der AfD

Folgen des Cyberangriffes auf den Klinikverbund AMEOS für Mecklenburg-Vorpommern

und

ANTWORT

der Landesregierung

Der Klinikverbund AMEOS hat am 7. Juli 2025 nach eigenen Angaben einen Cyberangriff auf seine IT-Systeme festgestellt und vorsorglich sämtliche digitalen Netzwerke an zahlreichen Standorten abgeschaltet. Medienberichten zufolge kam es bundesweit zu erheblichen Einschränkungen in der Patientenversorgung. Rettungsdienste konnten betroffene Einrichtungen nur eingeschränkt anfahren, und digitale Diagnostik war teilweise nicht verfügbar. AMEOS betreibt auch mehrere Kliniken in Mecklenburg-Vorpommern, darunter in Ueckermünde, Anklam und Pasewalk. Vor dem Hintergrund der zunehmenden Cyberbedrohungen im Gesundheitswesen ergeben sich dringende Fragen zur Versorgungssicherheit, zum Datenschutz sowie zu den Aufsichtspflichten des Landes.

1. Wann wurde die Landesregierung erstmals über den Cyberangriff auf den Klinikverbund AMEOS informiert?
   Welche Informationen liegen ihr zur Art des Angriffes (z. B. Ransomware, Phishing) sowie zum Schadensausmaß an den AMEOS-Einrichtungen in Mecklenburg-Vorpommern vor?

Polizeilich wurde der Sachverhalt am 10.07.2025 aus Presseinformationen vom 09.07.2025 im Landeskriminalamt Mecklenburg-Vorpommern (LKA M-V) bekannt. Die Information wurde zur weiteren Verwendung an die Kriminalpolizeiinspektion (KPI) Anklam gegeben. Eine Kontaktaufnahme seitens der AMEOS-Kliniken in Mecklenburg-Vorpommern zur Polizei Mecklenburg-Vorpommern fand seinerzeit nicht statt, auch nicht zur Landeskrankenhausplanungsbehörde.

Die Minister für Soziales, Gesundheit und Sport hat namens der Landesregierung die Kleine Anfrage mit Schreiben vom 17. September 2025 beantwortet.

Eine Anzeige zum Nachteil des AMEOS-Klinikums wurde bei der Kriminalpolizeiinspektion Anklam durch eine Vertreterin des Klinikums im September 2025 erstattet. Der tatsächliche Ereignisort des Angriffes befindet sich in Sachsen-Anhalt, da sich das angegriffene Rechenzentrum dort befindet. Zu dem Komplex (der Ransomware-Gruppe) werden in einem anderen LKA zentrale Ermittlungen (ZE) geführt.

2. Welche AMEOS-Einrichtungen in Mecklenburg-Vorpommern waren nach Kenntnis der Landesregierung technisch betroffen?
Welche kritischen Systeme (z. B. Krankenhausinformationssysteme, Labor-IT, digitale Patientenakten) wurden an diesen Standorten abgeschaltet oder beeinträchtigt?

Die AMEOS Gruppe ist am 07.07.2025 Opfer eines Cyberangriffs geworden. Nach Auskunft des Klinikverbundes AMEOS waren in Mecklenburg-Vorpommern alle Standorte betroffen; das AMEOS Klinikum Ueckermünde und das AMEOS Hanse Klinikum Anklam inklusive des Außenstandortes AMEOS Klinikum Pasewalk. Es wurden unmittelbar diverse Maßnahmen ergriffen. Dazu zählen Trennung aller externen und internen Netzwerkverbindungen, Herunterfahren aller Systeme, Einschaltung der IT-Dienstleister und Forensik-Dienstleister. Die Polizei / Landeskriminalämter wurden nach Auskunft von AMEOS informiert.

Nach derzeitigem Kenntnisstand des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI) war die Verfügbarkeit der digitalen Patientenakten an allen Standorten in Mecklenburg-Vorpommern beeinträchtigt. Auch die Nichtverfügbarkeit kann datenschutzrechtlich als „Datenpanne“ im Sinne des Artikel 33, 34 Datenschutz-Grundverordnung (DSGVO) zu werten sein.

3. Welche konkreten Auswirkungen hatte nach Kenntnis der Landesregierung der Vorfall auf die Patientenversorgung in Mecklenburg-Vorpommern, insbesondere hinsichtlich der Einschränkung von Notaufnahmen, OP-Planungen, Labordiagnostik oder anderen essenziellen Dienstleistungen?
Mussten Rettungsdienste Umleitungen zu anderen Kliniken vornehmen?

Der Vorfall hatte keine direkte Auswirkung auf die Patientenversorgung. Die Notaufnahmen waren nach Auskunft von AMEOS vollumfänglich aufnahmebereit und essentielle Dienstleistungen standen jederzeit zur Verfügung. Die Einschränkungen der Computertomografie-Untersuchungen über Nacht im AMEOS Klinikum Ueckermünde führten zu keiner Einschränkung in der Patientenversorgung. Die ständige Kommunikation und Abstimmung mit dem Rettungsdienst waren zu jeder Zeit gewährleistet. Es sind auch im Rettungsdienst keine Beeinträchtigungen durch den Cyberangriffs aufgetreten. Insbesondere mussten keine Umleitungen zu anderen Kliniken gefahren werden.

4. Welche Meldungen im Zusammenhang mit dem Cyberangriff sind bei der Krankenhausaufsicht, dem Landesdatenschutzbeauftragten, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) oder dem CERT-MV eingegangen?
Welche Maßnahmen wurden daraufhin von diesen Stellen ergriffen?

Entdeckt wurde der Cyberangriff nach Auskunft der AMEOS AG durch die AMEOS Sicherheitssoftware, die verdächtige Aktivitäten feststellte und unterbunden hat. Nachdem Erkenntnisse über einen möglichen Datenabfluss vorlagen, ist fristgerecht eine Meldung gemäß Artikel 33 DSGVO (vorsorglich) vorgenommen worden. Die AMEOS Gruppe ist ein privatwirtschaftliches Unternehmen und obliegt damit nicht dem Geltungsbereich des Computer Emergency Response Team Mecklenburg-Vorpommern (CERT M-V). Es konnte zu dem Zeitpunkt nicht ermittelt werden, ob und gegebenenfalls welche Standorte der AMEOS Gruppe betroffen waren. Deshalb sei die Meldung (vorsorglich) für alle Einrichtungen der AMEOS Gruppe erfolgt. Nach interner Abstimmung zwischen den Datenschutzbehörden der Länder hat die Datenschutzbehörde des Bundeslandes Bremen die Federführung des Verfahrens übernommen.

Auf Nachfrage des LfDI teilte AMEOS mit, dass eine Meldung nur in den Bundesländern erfolgt sein soll, in denen es tatsächlich zu einem Datenabfluss gekommen ist. Der LfDI hat als die für die Standorte in Mecklenburg-Vorpommern zuständige Datenschutz-Aufsichtsbehörde ein Verfahren eingeleitet. Dieses ist noch nicht abgeschlossen. Da Standorte in mehreren Bundesländern betroffen sind, werden die Maßnahmen deutschlandweit abgestimmt, um ein harmonisiertes Vorgehen zu gewährleisten.

Die Landeskrankenhausplanungsbehörde hat von der Cyberattacke Kenntnis über den Newsletter des Nationalen IT-Lagezentrums des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erlangt. Demnach ist der Sachverhalt auch beim BSI bekannt gewesen.

5. Liegen der Landesregierung Hinweise auf einen Abfluss oder eine Kompromittierung personenbezogener Daten, insbesondere sensibler Gesundheitsdaten, aus AMEOS-Einrichtungen in Mecklenburg-Vorpommern, vor?
Welche Schritte zur Information und Unterstützung potenziell Betroffener wurden geprüft oder eingeleitet?

Der Klinikverbund AMEOS hat mitgeteilt, dass die Täter durch den Angriff von einigen Standorten der AMEOS Gruppe teilweise personenbezogene Daten unrechtmäßig erlangt haben. Es können Patienten- oder Mitarbeitendendaten wie beispielsweise

- Kontaktdaten (zum Beispiel Vor- und Nachname, Anschrift, E-Mail, Telefonnummer)
- verwaltungsbezogene Daten (zum Beispiel Patientennummer, Personalnummer)
- gesundheitsbezogene Informationen

betroffen sein.

Die Mitarbeitenden wurden per Rundschreiben informiert. Auch Informationen für die Patientinnen und Patienten hängen in alles AMEOS Einrichtungen aus. Zudem befindet sich ein Hinweis auf der jeweiligen Internetseite. Es werden Kontaktformulare für Auskunftsersuchen zur Verfügung gestellt. Zudem können auch formlose Anfragen gestellt werden.

Da bereits die Nichtverfügbarkeit der digitalen Patientendaten eine Benachrichtigungspflicht nach Artikel 34 DSGVO auslösen kann, hat sich der LfDI dafür eingesetzt, dass eine Benachrichtigung zunächst aller Patientinnen und Patienten erfolgt. Zum jetzigen Zeitpunkt ist eine Benachrichtigung durch öffentliche Bekanntmachung, wie sie auch erfolgt ist, zulässig. Kritsch bewerten die Datenschutz-Aufsichtsbehörden den Prozess von AMEOS hinsichtlich der Benachrichtigung im Falle einer konkreten Betroffenheit. Kurzzeitig sollten Patientinnen und Patienten über ein Formular ihre Betroffenheit abfragen und dabei eine Kopie ihres Personalausweises übermitteln. Die Datenschutz-Aufsichtsbehörden haben hier sofort interveniert. Zum einen darf die Erteilung der Information nicht pauschal von der Übersendung der Ausweiskopie abhängig gemacht werden. Zum anderen ist das Formular sicher sinnvoll, darf aber andere Wege der Informationserlangung nicht ausschließen. Schließlich soll eine Benachrichtigung durch AMEOS in konkreten Einzelfall jedenfalls dann erfolgen, wenn tatsächlich Daten abgeflossen sind.

6. Unterliegen die AMEOS-Kliniken in Mecklenburg-Vorpommern den Vorgaben der KRITIS-Verordnung bzw. des IT-Sicherheitsgesetzes 2.0?
Welche Nachweise oder regelmäßigen Prüfungen zur IT-Sicherheit fordert das Land von privaten Klinikträgern im Rahmen seiner Aufsichtspflichten?

Es gibt keinen hundertprozentigen Schutz vor Cyberangriffen. Entscheidend ist, wie gut die Krankenhäuser bei einem solchen Angriff geschützt sind und wie schnell sie reagieren können, um die Risiken und den Schaden möglichst gering zu halten. Dazu müssen technische und organisatorische Maßnahmen getroffen werden, um etwa Zugriffe auf personenbezogene Daten bei einem Angriff auf die IT-Infrastruktur zu erschweren. Backups an unterschiedlichen Aufbewahrungsorten sind elementar, um die Behandlung der Patientinnen und Patienten sicherzustellen, wenn beispielsweise Datenbanken durch Angreifer verschlüsselt werden. Und nicht zuletzt müssen in Notfallplänen Prozesse festgelegt werden, wie im Ernstfall schnell und effizient reagiert werden kann. All diese Dinge sind aufwendig und erfordern finanzielle und personelle Ressourcen. Die Erfahrung zeigt aber, dass folgenschwere Datenpannen mit weitaus mehr Aufwand und Kosten verbunden sind, als präventive Maßnahmen. Eine Übersicht, wie gut die Krankenhäuser im Land hier aufgestellt sind, soll die Auswertung einer durch den LfDI ab September 2025 geplanten umfangreichen Prüfaktion bringen.

Zu den „KRITIS-relevanten Krankenhäusern“ gemäß der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) zählen Kliniken mit einer Anzahl von mehr als 30.000 vollstationären Behandlungsfällen pro Jahr. Welche Kliniken in Mecklenburg-Vorpommern dazu gehören, wird nicht vom Land erfasst, sondern vom BSI.

Die Listen unterliegen einer Sicherheitseinstufung. Aktuell unterliegen die Krankenhäuser nur einer Rechtsaufsicht. Wie die Informationssicherheit sichergestellt wird, ist dabei Sache des Krankenhauses und wird vom Land nicht vorgegeben.

7. Welche kurzfristigen Unterstützungsmaßnahmen (z. B. technische oder personelle Hilfe) und langfristigen Präventionsstrategien (z. B. Förderung von IT-Sicherheit über das Krankenhauszukunftsgesetz, Aufbau eines landesweiten Melde- und Frühwarnsystems für Cyberangriffe) plant oder ergreift die Landesregierung, um die Cyber-Resilienz der stationären Versorgung in Mecklenburg-Vorpommern zu stärken?

Die Zentrale Ansprechstelle Cybercrime (ZAC M-V) beim LKA M-V nahm am 21.07.2025 (Veranstaltung war schon vor dem Vorfall geplant) an der Fachveranstaltung "Cybersicherheit im Krankenhaus" der Krankenhausgesellschaft M-V und des LfDI teil. Dabei gab die ZAC M-V Handlungsempfehlungen, insbesondere in Bezug auf Erfahrungen in bisherigen Ermittlungen im Zusammenhang mit Cyber-Angriffen auf Kliniken in Mecklenburg-Vorpommern. Weiterhin wurden die Krankenhäuser bei konkreten Ereignissen mit Hinweisen (zum Beispiel Listen mit Indicators of Compromise (IoC)) zur eigenen Überprüfung der IT versorgt. Die Vernetzung der ZAC M-V mit den Kliniken des Landes wird aktuell intensiviert.

Die Gewährleistung der IT-Sicherheit in Krankenhäusern ist gemäß § 391 SGB V Pflicht der Krankenhausträger. Demnach sind Krankenhäuser verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und den Schutzbedarf der verarbeiteten Patienteninformationen maßgeblich sind und verpflichtende Maßnahmen zur Steigerung der Security-Awareness von Mitarbeiterinnen und Mitarbeitern zu gewährleisten.

Weiterführende Vorgaben gelten für „KRITIS-relevante Krankenhäuser“. Gemäß Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) zählen dazu Kliniken mit einer Anzahl von mehr als 30.000 vollstationären Behandlungsfällen pro Jahr. Diese müssen besondere Sicherheitsvorkehrungen treffen, um ihre Funktionsfähigkeit sicherzustellen. Diese Maßnahmen umfassen technische und organisatorische Vorkehrungen, um die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der IT-Systeme zu gewährleisten.

Die Bestimmungen für die Krankenhäuser für die Vorbereitung auf Krisensituationen richten sich zudem nach dem Landeskrankenhausgesetz Mecklenburg-Vorpommern (LKHG M-V). Nach aktueller Rechtslage sind die Krankenhäuser gemäß § 29 Absatz 2 LKHG M-V verpflichtet, zur Mitwirkung im Brand- und Katastrophenschutz Alarm- und Einsatzpläne aufzustellen, mit den zuständigen Stellen abzustimmen und an Übungen teilzunehmen.

Das für Gesundheit zuständige Ministerium entwickelt derzeit im Rahmen der Neufassung des LKHG M-V konkrete Vorgaben zur Steigerung der Resilienz von Krankenhäusern.

Das Land beteiligt sich mittels Kofinanzierung außerdem an der Förderung der Krankenhäuser über den Krankenhauszukunftsfonds (KHZF). Für Mecklenburg-Vorpommern stehen aus diesem Sonderprogramm aus den Bundesmitteln rund 58,6 Millionen Euro zur Verfügung. Hinzu kommen die 25,1 Millionen Euro Landesanteil. Damit konnten 90 Anträge bewilligt und den 37 Krankenhäusern hier im Land zusätzliche Investitionsmittel in Höhe von rund 83,7 Millionen Euro zur Verfügung gestellt werden.

Ziel ist, durch gezielte Projekte das Digitalisierungsniveau anzuheben und die technische Ausstattung der Krankenhäuser deutlich zu verbessern. Der Aspekt der IT-Sicherheit wird durch den KHZF auf zwei Wege adressiert. Zum einen sind nach § 14a Absatz 3 Satz 5 KHG mindestens 15 Prozent der für die Förderung eines jeweiligen Vorhabens beantragten Mittel für Maßnahmen zur Verbesserung der Informationssicherheit zu verwenden. Ziel dessen ist es, dass alle geförderten Maßnahmen bereits zu Beginn den Anforderungen und Standards der IT- und Cybersicherheit entsprechen. Zum anderen wird durch Fördertatbestand 10 explizit der Tatbestand der IT-Sicherheit gefördert (§ 19 Absatz 1 Satz 1 Nummer 10 KHSFV), für den 18 Krankenhäuser Fördermittelbescheide erhalten haben und insgesamt 12.152.103,14 Euro (Landesanteil 3.645.630,94 Euro) zur Verfügung stehen. Geplant ist, dass die Projekte bis zum 31.12.2025 abgeschlossen sein werden.

Des Weiteren führt der LfDI zunehmend Kontrollen von Einrichtungen im Gesundheitswesen durch. Darüber hinaus steht der LfDI diesen Stellen auch beratend zur Seite. Dem LfDI stehen aber auch verwaltungsrechtliche Mittel sowie Sanktionen zur Verfügung, um die Beseitigung festgestellter und datenschutzrelevanter Lücken bei der Cybersicherheit anzuordnen. Festzuhalten bleibt hier aber auch, dass die Maßnahmen stets verhältnismäßig sein müssen und die Behandlung nicht gefährden dürfen.

Die Herstellung der Cybersicherheit liegt im Verantwortungsbereich der Krankenhausträger. Darüber hinaus verfolgt die Landesregierung einen ganzheitlichen Ansatz zur Erhöhung der Cyber-Resilienz. Durch geplante gesetzliche Vorgaben im neuen LKHG M-V und gezielte Investitionen im Rahmen des Krankenhauszukunftsfonds wird sowohl die organisatorische Vorbereitung als auch die technische IT-Sicherheit systematisch gestärkt. Zusätzlich steht der LfDI beratend zur Seite. Ziel ist es, Krankenhäuser umfassend auf digitale Gefahrenlagen vorzubereiten und ihre Handlungsfähigkeit im Krisenfall sicherzustellen.

8. Gab es im Zusammenhang mit dem Cyberangriff Hinweise darauf, dass Daten betroffen waren, die im Rahmen des Gesundheitsdatennutzungsgesetzes erhoben und gespeichert wurden?
Wenn ja, welche konkreten Datensätze und wie viele Personen aus Mecklenburg-Vorpommern könnten davon betroffen sein?

Aufgrund des Gesundheitsdatennutzungsgesetzes werden keine Daten neu erhoben. Es können ausschließlich bereits vorhandene im Rahmen der Patientenversorgung rechtmäßig erhobene Daten auf Anfrage abgefordert werden. Da bei AMEOS gerade keine Forschung mit Patientendaten betrieben wird, sind aktuell keine für die Forschung nach § 37 Absatz 1 Nummer 1 LKHG anonymisierten Patientendaten vorhanden.

Auch wird aktuell keine Forschung mit Klardaten gemäß § 31 Absatz 1 Nummer 3 LKHG betrieben. Ein Datenfluss aus einem Datenverarbeitungssystem im Sinne des § 37 Absatz 1 Nummer 3 LKHG war daher nicht möglich.

Die Aufbereitung mit Pseudonymisierung zu Forschungszwecken erfolgt nicht bei den Krankenhäusern, sondern durch eine Treuhandstelle. Die Treuhandstellen waren nicht vom Cyberangriff betroffen. Auch hier ist kein Datenabfluss erfolgt. Insofern sind bei dem Cyberangriff keine Daten abgeflossen, die aufgrund des Gesundheitsdatennutzungsgesetzes gespeichert wurden.

9. Welche konkreten organisatorischen und technischen Verantwortlichkeiten bestehen für die Sicherstellung der IT-Sicherheit und Überwachung sensibler Patientendaten in den AMEOS-Kliniken in Mecklenburg-Vorpommern?
Welche Rolle spielen dabei das Land, die Klinikträger sowie externe Stellen (z. B. das BSI)?

Für alle Krankenhäuser gilt unter anderem die DSGVO, wonach technische Maßnahmen ergriffen werden müssen, die unter anderem vor dem Zugriff unbefugter Dritter schützen. Patientendaten genießen einen hohen Schutzbedarf, an dem die Geeignetheit der ergriffenen Maßnahmen zu messen ist. Ob vorliegend hinreichend geeignete Maßnahmen ergriffen worden sind, um einen Angriff zu verhindern beziehungsweise die Auswirkungen eines Angriffs gering zu halten, prüft der LfDI derzeit gemeinsam mit den anderen Datenschutz-Aufsichtsbehörden.