Bayerischer Landtag

19. Wahlperiode 10.07.2025 **Drucksache** 19/**7476**

Beschluss

des Bayerischen Landtags

Der Landtag hat in seiner heutigen öffentlichen Sitzung beraten und beschlossen:

Nichtlegislatives Vorhaben der Europäischen Union

Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Europäischer Aktionsplan für die Cybersicherheit von Krankenhäusern und Gesundheitsdienstleistern
COM(2025) 10 final
BR-Drs. 77/25

Drs. 19/**5947**, 19/**7425**

Dem Vorhaben wird zugestimmt.

Der Landtag begrüßt die Bemühungen der EU-Kommission, die Cybersicherheit im Bereich des Gesundheitswesens zu stärken. Der Schwerpunkt des Aktionsplans liegt auf der Prävention von Cybersicherheitsvorfällen, der Erkennung von Bedrohungen und Maßnahmen für eine bessere Reaktion auf Sicherheitsvorfälle.

Krankenhäuser sind ein wesentlicher Bestandteil der Gesundheitsversorgung, in denen insbesondere auch lebensbedrohliche Krankheiten und Verletzungen behandelt werden. Ein Ausfall aufgrund erfolgreicher Cyberattacken könnte daher zu schwerwiegenden Folgen für die Patientinnen und Patienten führen. Für die Krankenhäuser besonders bedeutend ist, dass der Aktionsplan vorsieht, ein Europäisches Unterstützungszentrum für Cybersicherheit für Krankenhäuser und Gesundheitsdienstleister einzurichten.

Das Unterstützungszentrum soll schrittweise einen umfassenden Dienstleistungskatalog aufstellen, der den Bedürfnissen von Krankenhäusern und Gesundheitsdienstleistern entspricht und die ganze Palette der verfügbaren Dienste für Abwehrbereitschaft, Prävention, Erkennung und Reaktion enthält. Nach den bisherigen Ausführungen im Aktionsplan dürfte der angedachte Aufbau eines Unterstützungszentrums auch keine Belastung für die Krankenhäuser bedeuten, da sie vielmehr von ihm profitieren sollen. Das Zentrum müsste dabei natürlich die bereits bestehenden nationalen Pflichten, notwendige Maßnahmen zur Cybersicherheit umzusetzen (§ 391 Abs. 1 Sozialgesetzbuch Fünftes Buch (SGB V), § 80a Abs. 1 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG), mitberücksichtigen und seine Beratungen hieran orientieren.

Im Bereich der vertragsärztlichen Versorgung wurden im Jahr 2023 allein in bayerischen Praxen 95 Mio. Behandlungsfälle (Behandlung Regelversorgung) sowie 141 Millionen Arzt-Patientenkontakte (ohne laborähnliche und pathologische Fachgruppen) gezählt. Jede dieser Interaktionen bedeutet eine digitale Datenübermittlung, sei es durch die Abgleichung der Versichertendaten über die elektronische Versichertenkarte oder die Übermittlung von Abrechnungsdaten der Behandlungen an die Kassenärztliche Vereinigung Bayerns (KVB). Dabei handelt es sich um sehr sensible Daten, da diese Diagnosen und medizinische Informationen über einzelne Patienten enthalten. Der Bund gibt den Sicherheitsstandard der verwendeten informationstechnischen Systeme vor. Dabei ergibt sich sowohl im Hinblick auf den Grad der Digitalisierung sowie dem Bewusstsein für die Sicherheit der IT-Systeme ein heterogenes Bild bei den niedergelassenen Praxen. Aufgrund der immer noch vorherrschenden Einzelpraxis mit einem Arzt als selbstständigem Unternehmer obliegt es diesem, entsprechende Maßnahmen der Cybersicherheit zu implementieren.

Weitergehend verfügen die Krankenkassen über einen Datenbestand, der – weil es sich um Gesundheitsdaten handelt – besonders schutzwürdig ist.
Sollte es möglichen Angreifern nicht darum gehen, Daten zu stehlen, sondern schlicht Systeme zum Erliegen zu bringen, dürfte die „kriminelle Anziehungskraft“ einer Krankenkasse dagegen weniger groß sein. Von den erwähnten Unterstützungsleistungen dürften aber auch die Krankenkassen profitieren. Derartige Gefahrenpotenziale bestehen gleichermaßen auch für weitere Körperschaften wie dem Medizinischen Dienst oder den Kassenärztlichen Vereinigungen.

Aus dem Bereich des Apothekenwesens ist auszuführen, dass nach Auskunft der Bayerischen Landesapothekerkammer das Anliegen, die Cybersicherheit von Krankenhäusern und Gesundheitsdienstleistern zu stärken und hierfür Ressourcen zu bündeln, zu unterstützen ist. Gesundheitsdaten sind sensible Daten. Aufgrund der zunehmenden Digitalisierung im Gesundheitswesen (E-Rezept, elektronische Patientenakte – hier nur beispielhaft genannt) steigt die Gefahr möglicher Cyberangriffe in diesem Sektor erheblich an, mit der entsprechend in dem Aktionsplan skizzierten gesundheitlichen oder lebensbedrohlichen und evtl. auch wirtschaftlichen Gefährdung für die betroffenen Patientinnen und Patienten, einem Vertrauensverlust in die Digitalisierung, zugleich aber auch einer wirtschaftlichen Gefährdung des jeweiligen Unternehmens bzw. der jeweiligen Gesundheitseinrichtung.

Hinsichtlich der in dem Aktionsplan geplanten Maßnahmen müssten aufgrund der unterschiedlichen Ausgestaltung der Gesundheitssysteme in den EU-Mitgliedstaaten sowie der unterschiedlichen „Größe“ und Funktion der betroffenen Einrichtungen (Krankenhäuser, Gesundheitsdienstleister; somit vom Kleinstunternehmen bis zum Großunternehmen alles umfasst) die Leitlinien sehr differenziert ausgearbeitet werden, um tatsächlich alle Besonderheiten und Einzelfälle sowohl bei den Gesundheitsdienstleistern als auch in den EU-Mitgliedstaaten zu berücksichtigen. Zudem stellt sich auch die Frage der „Verbindlichkeit“ dieser Leitlinien bzw. welche Verpflichtungen resultieren ggf. daraus konkret für die betroffenen Gesundheitsdienstleister. Eine Überregulierung sollte vermieden werden; vielmehr muss der Praxisbezug beziehungsweise die Praktikabilität gewahrt werden; dies dürfte nur möglich sein, wenn die Maßnahmen und Hilfsangebote vonseiten der EU intensiv mit den nationalen Gesundheitsministerien, Berufsvertretungen sowie Fachgesellschaften und Patientenvertreterinnen und -vertretern abgestimmt werden.

Insbesondere für Kleinst- und Kleinunternehmen (konkret die Vor-Ort-Apotheken) besteht mit der Ausweitung der Maßnahmen zudem das Risiko eines erheblichen administrativen und monetären Aufwandes, sodass es hier gezielter Unterstützung und Lösungen bedarf.

Betreffend die Heilberufe-Kammern – konkret die Psychotherapeutenkammer Bayern (PTK) sowie die Bayerische Landesärztekammer (BLÄK) – wird darauf hingewiesen, dass eher die Gesamtheit der Telematikinfrastruktur für den Aktionsplan relevant wäre. In diesem Zusammenhang möchte die PTK noch besonders auf Privatpraxen hinweisen und anmerken, dass hier möglicherweise ein Bedarf an Unterstützung im Bereich der Telematikinfrastruktur bestehen könnte. Die Bedrohung durch Cyberangriffe im Gesundheitssektor unter Zugrundelegung der geopolitischen Lage wird vonseiten der

BLÄK als hoch angesehen. Aus diesem Grund wird die Intention zur Schaffung eines gesamteuropäischen Zentrums zur Unterstützung der Cybersicherheit für Krankenhäuser und Gesundheitsdienstleister begrüßt, um diesen Leitlinien und Handlungsanweisungen zur Verfügung zu stellen. Zudem wird bei niedergelassenen Ärztinnen und Ärzten das Potenzial gesehen, von entsprechenden Leitlinien zu profitieren und die dort verarbeiteten Gesundheitsdaten vor Cyberangriffen effektiv schützen zu können. Insbesondere Einzel- bzw. kleinere Praxen verfügen, anders als beispielsweise größere Medizinische Versorgungszentren oder Krankenhäuser, oftmals nicht über die finanziellen Mittel, um einen umfassenden Schutz vor Cyberangriffen sicherzustellen bzw. diesen aufrechtzuerhalten. Gerade diese Gruppe könnte von maßgeschneiderten Leitlinien und Handlungsanweisungen profitieren. Auch die elektronische Patientenakte, das E-Rezept, Portale zur Bereitstellung von Bildmaterial (z. B. MRT-Befunde) und die Gesundheits-ID als digitale Identität im Gesundheitswesen werden als potenzielle Ziele für Cyberangriffe angesehen. Für diese Bereiche wären Handreichungen ebenfalls wünschenswert.

Auch können Medizinprodukte, welche in die Infrastruktur von Krankenhäusern und Gesundheitsdienstleistern integriert werden, potenziellen Cyberrisiken ausgesetzt sein. Die grundlegenden Anforderungen an die Sicherheit und Cybersicherheit von Medizinprodukten und In-vitro-Diagnostika sind dabei bereits in der Medizinprodukteverordnung und In-vitro-Diagnostika-Richtlinien geregelt und werden von Herstellern im Zuge des Risikomanagements betrachtet und umgesetzt.

Der Beschluss des Bayerischen Landtags wird unmittelbar an die Europäische Kommission, das Europäische Parlament, den Ausschuss der Regionen und den Deutschen Bundestag übermittelt.

Die Präsidentin

Ilse Aigner