

Bericht und Antrag der Kommission Gesundheit, Arbeit und soziale Sicherheit betreffend der Petition über die Cybersicherheit am Luzerner Kantonsspital und an anderen Spitälern

1 Ausgangslage

Am 29. Januar 2025 hat Bernhard Isenegger die Petition über die Cybersicherheit am Luzerner Kantonsspital und an anderen Spitälern bei der Staatskanzlei eingereicht. Sie richtet sich an den Kantonsrat. Die Geschäftsleitung des Kantonsrates hat die Petition gemäss § 81 der Geschäftsordnung des Kantonsrates zur Prüfung und Berichterstattung der Kommission Gesundheit, Arbeit und soziale Sicherheit (GASK) zugewiesen.

Die Petition nimmt Bezug auf einen vom Nationalen Testinstitut für Cybersicherheit (NTC) durchgeführten Test von Klinikinformationssystemen und den dazu veröffentlichten Bericht. Der Petitionär fordert die sofortige Kündigung von sogenannten «Stillhaltevereinbarungen» der Spitäler der LUKS-Gruppe gegenüber Herstellern von Klinikinformationssystemen.

2 Rechtliche Grundlagen

Als Petitionen werden gemäss § 83 Abs. 1 des Kantonsratsgesetzes Eingaben von Behörden und Privatpersonen behandelt, welche bestimmte Begehren oder Beanstandungen enthalten und keine besondere Rechtsform aufweisen. Entsprechend § 82 Abs. 2 und 3 der Geschäftsordnung des Kantonsrates erstattet die zuständige Kommission dem Kantonsrat schriftlich Bericht und stellt Antrag, wie eine Petition zu erledigen ist. Der Kantonsrat erledigt eine Petition, indem er sie mit oder ohne Stellungnahme zur Kenntnis nimmt.

3 Feststellungen und Folgerungen

Die GASK hat zur Petition Stellungnahmen des NTC, des Datenschutzbeauftragten des Kantons Luzern und des LUKS eingeholt. Zudem wurden die zuständigen Leitungspersonen des LUKS für die Bereiche Informatik sowie Recht, Compliance und Datenschutz an der Kommissionssitzung vom 7. April 2025 angehört.

Gemäss dem kantonalen Datenschutzbeauftragten besteht für das LUKS eine Melde- und Informationspflicht bei einem Sicherheitsvorfall (Kantonales Datenschutzgesetz, § 7). Das LUKS muss dem oder der Beauftragten für den Datenschutz unverzüglich unbefugte Datenbearbeitungen melden, wenn diese voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen führen. Weiter muss das LUKS die betroffenen Personen informieren, wenn es zu deren Schutz erforderlich ist oder wenn der oder die Beauftragte für den Datenschutz es verlangt, und soweit erforderlich andere Organe und Dritte. Die Information kann eingeschränkt oder aufgeschoben oder es kann darauf verzichtet werden, wenn überwiegende öffentliche Interessen dies erfordern oder wenn die Information

einen unverhältnismässigen Aufwand verursacht. «Stillhaltevereinbarungen» in den Verträgen zwischen dem LUKS und dem Softwarehersteller Epic, welche der Melde- und Informationspflicht entgegenstehen, wären ein klarer Gesetzesverstoss. Der Datenschutzbeauftragte geht davon aus, dass das LUKS die vertraglichen Vereinbarungen mit Epic auf Konformität mit kantonalem Recht und Bundesrecht überprüft und Anpassungen in den Verträgen verlangt hat, sollte dies notwendig gewesen sein.

Gemäss Stellungnahme des LUKS besteht keine «Stillhaltevereinbarung» mit dem Hersteller des betriebenen Klinikinformationssystems. Zudem führt das LUKS selbst regelmässige Tests der Software durch. Dabei geht es etwa um Prävention, Schutz, Erkennung, Abwehr von Vorfällen respektive um die Wiederherstellung der Systeme im Ereignisfall. Das LUKS arbeitet zudem seit Jahren auch mit den Cybersecurity-Stellen des Bundes zusammen.

Die Kommission erachtet die Forderung der Petition aufgrund der obenstehenden Erkenntnisse als erfüllt und sieht bezüglich allfälliger «Stillhaltevereinbarungen» keinen Handlungsbedarf.

4 Antrag an den Kantonsrat

Die GASK beantragt, die Petition im Sinne der vorgenannten Feststellungen und Folgerungen zur Kenntnis zu nehmen.

07.04.2025

Kommission Gesundheit, Arbeit und soziale Sicherheit (GASK)
Die Präsidentin

Pia Engler