Regierungsrat des Kantons Schwyz

Beschluss Nr. 894/2021
Schwyz, 14. Dezember 2021 / ju

Motion M 5/21: Nachweis über adäquate Kontrolle der Cyberrisiken in Spitälern als Voraussetzung für die Betriebsbewilligung
Beantwortung

1. Wortlaut der Motion

Am 25. Juni 2021 haben die Kantonsräte Roland Lutz, Roman Bürgi und Thomas Haas folgende Motion eingereicht:

«In den letzten Jahren häuften sich Vorfälle im Bereich Cybersicherheit in der Schweiz. Die Folgen waren Betriebsunterbrüche, Datenverlust und finanzielle Schäden. Angriffsziele sind IT-Systeme und - im Fall von Spitälern - medizinische Apparate und Systeme. Der jüngste erfolgreiche Cyberangriff auf die Hirslanden-Gruppe zeigt die Verletzlichkeit des Gesundheitswesens in aller Deutlichkeit. Ein erfolgreicher Cyberangriff auf ein Krankenhaus kann im schlimmsten Fall Menschenleben kosten.

Gefahren bergen zudem der Einsatz von langjährig betriebenen und damit potentiell verwundbaren Systemen wie auch die Zunahme von Verbindungen ins Internet und die vermehrte Nutzung von Homeoffice.

Spitäler und das Gesundheitswesen insgesamt zählen zu den kritischen Infrastrukturen. Gerade kleinere Spitäler stehen unter finanziellem Druck; die Cybersicherheit wird deswegen möglicherweise nicht prioritär behandelt.

Aufsichtspflicht gemäss Spitalgesetz:
Das kantonale Spitalgesetz (SpitG) verpflichtet den Kanton, die Spitalversorgung sicherzustellen. Der Regierungsrat übt hierzu die Oberaufsicht über die Spitalversorgung aus. § 4 fordert u.a. die Sicherstellung der Betreuung der Patienten und der betrieblichen Voraussetzungen. Darauf basiert auch die Bewilligung für den Betrieb.

Zur Bewilligungsvergabe gehört u.E. auch die Beurteilung der Effektivität der Cybersicherheit (Massnahmen, um Risiken abwehren und Schäden zu verhindern).

Forderung:
Wir fordern den Regierungsrat dazu auf, eine genügende Rechtsgrundlage zu erarbeiten, damit die Spitäler periodisch einen Nachweis zu erbringen haben, dass sie die mit Cybersecurity im Zusammenhang stehenden Risiken quantitativ und qualitativ adäquat im Griff haben.

Hierzu soll jeweils ein aktuelles positiv ausfallendes Testat einer qualifizierten Prüfstelle eingefordert werden.

Für die wohlwollende Bearbeitung danken wir im Voraus.»

2. Antwort des Regierungsrates

2.1 Ausgangslage

Cybersicherheit im Gesundheitswesen und in den Spitälern ist ein Thema, welches in letzter Zeit zunehmend stärkere Wahrnehmung erfährt. Dies ist der Bedeutung dieses Themas für die Sicherstellung einer guten, sicheren und verlässlichen Gesundheitsversorgung auch durchaus angemessen.

Wie das Nationale Zentrum für Cybersicherheit (NCSC) in seinem Halbjahresbericht vom 11. Mai 2021, welcher sich im Fokus dem Gesundheitswesen widmet, schreibt, sind Spitäler und andere Gesundheitsdienstleister den gleichen Cyberrisiken ausgesetzt wie alle Unternehmen, die einen Internetanschluss haben und mit Computern arbeiten. Jedoch weisen die Bedrohungen von Cyber-Angriffen im Gesundheitswesen durchaus Besonderheiten aus. Zum einen sind bei einem Datenabfluss meistens besonders schützenswerte Personendaten betroffen, und zum anderen können Funktionsausfälle von IT-Systemen oder auch eine temporäre Nichtverfügbarkeit von Daten die Gesundheit oder sogar das Leben von Menschen gefährden.

Das NCSC schätzt die Lage als ernst ein und befürchtet, dass die Angriffsfläche bei den Spitälern hoch ist. Es hat seine diesbezügliche Besorgnis bereits im September 2020 auch gegenüber der Schweizerischen Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren (GDK) zum Ausdruck gebracht und um Unterstützung bei der Sensibilisierung der Spitäler in diesem wichtigen Thema ersucht.

2.2 Handlungsfelder auf Ebene Bund und Kantone

Das Thema Cybersicherheit wird sowohl auf Ebene Bund als auch auf Ebene Kantone ernst genommen, und es werden Schritte zur Sensibilisierung der Gesundheitseinrichtungen vor Cyber-Attacken sowie deren Vorbeugung und Unterbindung unternommen.

2.2.1 Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018–2022 (NCS)

Mit der NCS verpflichtet sich der Bund, die darin beschriebenen Massnahmen in Zusammenarbeit mit den Kantonen, der Wirtschaft und der Gesellschaft umzusetzen. Unter anderen wird eine Massnahme zur Evaluierung und Einführung von Minimalstandards aufgeführt. Ziel der Massnahme ist es, in enger Zusammenarbeit zwischen Behörden, Privatwirtschaft und Verbänden

überprüfbare Minimalstandards in der Informations- und Kommunikationstechnologie (IKT) zu evaluieren und einzuführen.

2.2.2 Strategie eHealth Schweiz 2.0 2018–2022

Die Strategie eHealth Schweiz wurde von Bund und Kantonen gemeinsam erarbeitet. Ein Ziel ist die Verstärkung der Cyber- und Datensicherheit im Gesundheitssystem, im Rahmen dessen Bund und Kantone konkrete Massnahmen ausarbeiten.

Bund und Kantone haben also im Bereich Cybersicherheit ein übereinstimmendes Interesse an einer koordinierten und abgestimmten Bearbeitung der Thematik, insbesondere was gesamtschweizerisch verbindliche Vorgaben hinsichtlich Minimalstandards in der IKT betrifft. Der Vorstand der GDK hat deshalb im Januar 2021 beschlossen, das Thema Cybersicherheit im Kontext des Dialogs Nationale Gesundheitspolitik (einer ständigen Plattform zum Austausch zwischen Bund und Kantonen) zu behandeln und eine Empfehlung zuhanden der Spitäler zu erarbeiten.

2.2.3 Kantonale Handlungsmöglichkeiten

Die Kantone haben im Bereich der Spitalplanung Möglichkeiten, für zugelassene Leistungserbringer verbindliche Vorgaben hinsichtlich Minimalstandards im Bereich Cybersicherheit zu erlassen.

2.3 Stand in den Kantonen und im Kanton Schwyz

Im März 2021 führte die GDK eine Umfrage bei allen Kantonen zum Thema Cybersicherheit durch. Die Ergebnisse zeigten, dass aktuell kein Kanton im Rahmen der Spitalplanung Vorgaben im Bereich Cybersicherheit macht. Nur fünf Kantone erhalten periodisch Kenntnis über den Stand der Bemühungen zur Minimierung der Cyberrisiken in den Spitälern. Und im Rahmen der Erteilung einer Betriebsbewilligung wird das Thema Cybersicherheit nur in einem Kanton berücksichtigt.

Auch im Kanton Schwyz macht der Regierungsrat den Standort- und Listenspitälern keine expliziten Vorgaben im Bereich Cybersicherheit; auch nicht im Rahmen der Erteilung von Betriebsbewilligungen. Dies unter anderem, weil aktuell ein national einheitlicher Standard hierfür fehlt. Im Zuge der Spitalplanung 2024 wird geprüft, ob neu solche sinnvollen Vorgaben bei der Bewilligungsvergabe und/oder der Erteilung der Leistungsverträge gemacht werden sollen.

Eine durch das Amt für Gesundheit und Soziales (AGS) im März 2021 durchgeführte Umfrage bei den Schwyzer Spitälern Einsiedeln, Lachen und Schwyz hat ergeben, dass diese Spitäler der Cybersicherheit bereits grosses Gewicht und hohe Priorität beimessen. Entsprechende Massnahmen und Konzepte (z. B. Etablierung von Stabsstellen im Bereich IT-Security- und IT-Risk-Management, Erstellung und Durchsetzung von IT-Security-Richtlinien, Abstützen auf moderne IT-Lösungen und Technologien) sind bereits etabliert und werden laufend überprüft.

Um die Spitäler für die zunehmenden Cyber-Risiken zu sensibilisieren, hat das AGS im Juni 2021 auf Empfehlung der GDK einen Brief an die Leitungen der Spitäler im Kanton gesendet, in welchem auf das Thema und die wachsende Bedrohung aufmerksam gemacht wurde. Ebenfalls wurden konkrete, unkompliziert umsetzbare Handlungsmöglichkeiten seitens der Spitäler aufgezeigt, welche einen relevanten Beitrag zum Schutz vor Cyberangriffen leisten. So zum Beispiel, dass vom NCSC kostenlos technische Hilfsmittel bezogen werden können, welche Angriffsversuche blockieren, sowie dass das NCSC den Informationsaustausch in diesem Bereich im Gesundheitssektor unterstützt. Auch wurden die Spitäler aufgefordert, die Hilfsmittel des NCSC einzusetzen und sich am Informationsaustausch zu diesem Thema über MELANI (Melde- und Analysestelle Informationssicherheit des Bundes) zu beteiligen.

2.4 Bestehende gesetzliche Grundlagen

Das Spitalgesetz vom 19. November 2014 (SpitG, SRSZ 574.110) gilt für Leistungen, die stationär in Spitälern erbracht werden (§ 2 Abs. 1 SpitG). Das Gesetz regelt unter anderem insbesondere das Leistungs-, Finanz- und Qualitätscontrolling in den Spitälern mit Leistungsvereinbarung (§ 2 Abs. 2 Bst. e SpitG), wobei diese Aufzählung nicht abschliessend ist. Der Betrieb eines Spitals bedarf der Bewilligung des Regierungsrates. Für die Erteilung einer Bewilligung wird unter anderem vorausgesetzt, dass das Spital die baulichen und betrieblichen Voraussetzungen erfüllt und die Einrichtungen dem Verwendungszweck entsprechen (§ 4 Abs. 1 und 2 Bst. b SpitG). Der Regierungsrat kann die Bewilligung entziehen, mit Auflagen oder Bedingungen versehen, wenn eine oder mehrere Voraussetzungen entfallen (§ 4 Abs. 3 SpitG). Der Regierungsrat bzw. das Departement schliesst mit den Spitälern Leistungsvereinbarungen ab. In den Leistungsvereinbarungen werden insbesondere die Einzelheiten der Leistungsaufträge, die Qualitätssicherung, die Bereitstellung von Daten und Teilzahlungen geregelt (§ 6 Abs. 1 und 2 SpitG).

Es besteht somit eine hinreichende gesetzliche Grundlage, um den Spitälern Vorgaben zur Cybersicherheit machen zu können. Eine solche muss nicht erst geschaffen werden.

2.5 Haltung des Regierungsrates

Aufgrund von zurzeit noch nicht bestehenden national einheitlichen Standards bezüglich Vorgaben an die Spitäler im Bereich Cybersicherheit und der jedoch bereits laufenden Arbeiten auf Ebene Bund und Kantone hierzu, ist es sinnvoll, dass der Kanton Schwyz mit solchen Vorgaben noch zuwartet, bis sinnvolle Standards bezüglich Vorgaben erarbeitet wurden, national einheitlich empfohlen werden und zur Anwendung gelangen.

Die gesetzlichen Grundlagen für solche Vorgaben bestehen bereits aktuell im kantonalen Spitalgesetz, weshalb keine neuen gesetzlichen Grundlagen geschaffen werden müssen.

Das AGS misst der Sensibilisierung der Spitäler für das Thema grosse Bedeutung zu und hat dies auch mit dem Versand des Sensibilisierungsschreibens im Sommer 2021 zum Ausdruck gebracht. Die Schwyzer Spitäler Einsiedeln, Lachen und Schwyz haben, gemäss der vom AGS Anfang 2021 durchgeführten Umfrage, auch bereits sinnvolle und zielgerichtete Massnahmen zu ihrem Schutz ergriffen. Die Problematik der Cyberrisiken im Gesundheitswesen ist dem AGS ausgesprochen bewusst, und ebenso wird klar zur Kenntnis genommen, dass es aufgrund der Verantwortung, welche die Kantone für die Gesundheitsversorgung tragen, ebenfalls in ihrem Interesse liegt, dass sich Spitäler möglichst gut vor Cyberangriffen schützen. Deshalb wird das AGS auch im Zuge der laufenden Spitalplanung 2024 prüfen, ob Vorgaben im Zusammenhang mit Cybersicherheit der Spitäler bei der Bewilligungsvergabe oder der Erteilung von Leistungsaufträgen gemacht werden sollen.

Was die Einforderung eines Testats seitens des Kantons zur Bestätigung, dass die Leistungserbringer die mit Cybersicherheit im Zusammenhang stehenden Risiken quantitativ und qualitativ adäquat handhaben, betrifft, so ist dies erst zum Zeitpunkt in Betracht zu ziehen, wenn nationale Standards und Vorgaben bestehen. Zudem ist zu empfehlen, dass die Spitäler sich für jene Qualitätssicherungsinstrumente entscheiden können, die für ihren jeweiligen Betrieb am geeignetsten sind.

Der Regierungsrat beantragt, die vorliegende Motion als nicht erheblich zu erklären.

Beschluss des Regierungsrates

1. Dem Kantonsrat wird beantragt, die Motion M 5/21 nicht erheblich zu erklären.

2. Zustellung: Mitglieder des Kantonsrates.

3. Zustellung elektronisch: Mitglieder des Regierungsrates; Staatsschreiber; Sekretariat des Kantonsrates; Departement des Innern; Sicherheitsdepartement; Finanzdepartement; Amt für Gesundheit und Soziales; Amt für Informatik.

Im Namen des Regierungsrates:

Petra Steimen-Rickenbacher
Landammann

Regierungsrat Kanton Schwyz

Dr. Mathias E. Brun
Staatsschreiber