kantonschwyz

Beschluss Nr. 323/2021
Schwyz, 18. Mai 2021 / pf

Interpellation I 26/20: Sind unsere Spitäler genügend gegen Cyberrisiken gewappnet und ist die Aufsicht über die Krankenhäuser diesbezüglich adäquat?
Beantwortung

1. Wortlaut der Interpellation

Am 1. Dezember 2020 haben die Kantonsräte Roland Lutz, Roman Bürgi und Thomas Hänggi folgende Interpellation 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, als auch 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, 2014 letztmals revidiert und in Kraft seit 1.1.2015) verpflichtet den Regierungsrat die Spitalversorgung sicherzustellen. Er 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).

Absicht der Interpellation
Da die IT-technische Entwicklung rasant fortschreitet ist eine mögliche Unterdeckung der zielführenden Massnahmen im Sinne einer zeitgemässen und wirkungsvollen Aufsicht ein hohes Risiko. Ziel unserer Interpellation ist die Beschaffung von Auskünften als Grundlagen für Vorschläge für angezeigte Verbesserungsmöglichkeiten.

Fragen an den Regierungsrat
1. Erlangt der Regierungsrat periodisch Kenntnis über den Stand der Bemühungen zur Minimierung von Cyberrisiken und somit der Qualität der Cybersicherheit?
2. Welches Gewicht hat bei der Beurteilung der Bewilligungsvergabe die Qualität der „Cybersicherheit" der Spitäler?
3. Gibt es spezifische (Minimal-)Vorgaben für die Spitäler im Themenkomplex „Cybersicherheit" ...
a. zur periodischen Prüfung, Beurteilung und allenfalls Rapportierung an die Aufsicht?
b. Audits durch interne / externe Prüfinstanzen oder dergleichen?
c. für (Minimal-)Erfordernisse als Grundlage für die Bewilligungsvergabe?

4. Sind seitens Aufsicht betriebsorganisatorische Prozesse etabliert, die der laufenden Anpassung der Beurteilungskriterien aufgrund der steigenden Risiken und der Komplexität Rechnung tragen, namentlich in den Bereichen...
a. Beschaffungsmanagement der Spitäler?
b. Asset Life Cycle Management der Spitäler?
c. Security Operations & Incident Response der Spitäler?
d. Datenschutz & Risiko Management der Spitäler?

Für die wohlwollende Beantwortung danken wir im Voraus.»

2. Antwort des Regierungsrates

2.1 Ausgangslage

Cybersicherheit in den Spitälern ist ein höchst aktuelles Thema und von grosser Bedeutung. Nach Aussage von Fachstellen haben Cyberangriffe auf Spitäler in letzter Zeit zugenommen. Auch das Nationale Zentrum für Cybersicherheit schätzt die Lage als ernst ein und befürchtet, dass die Angriffsfläche bei den Spitälern nach wie vor hoch ist. Es hat seine diesbezügliche Besorgnis im September 2020 gegenüber der Schweizerischen Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren (GDK) zum Ausdruck gebracht. Bund und Kantone haben im Bereich Cybersicherheit ein übereinstimmendes Interesse an einer koordinierten Bearbeitung der Thematik, beispielsweise mittels gesamtschweizerisch verbindlicher Vorgaben hinsichtlich einzuhaltender Minimalstandards im Bereich der Informations- und Kommunikationstechnologie (IKT). Der Vorstand der GDK hat darum im Januar 2021 beschlossen, dass das Thema Cybersicherheit im Rahmen des Dialogs Nationale Gesundheitspolitik – einer ständigen Plattform von Bund und Kantonen – behandelt und eine Empfehlung zum Thema Cybersicherheit in den Spitälern erarbeitet werden soll.

In diesem Zusammenhang führte die GDK im März 2021 eine Umfrage zum Thema Cybersicherheit in den Spitälern bei allen Kantonen durch. Die Ergebnisse dieser Umfrage zeigten, dass aktuell kein Kanton den Spitälern im Rahmen der Spitalplanung Vorgaben im Bereich Cybersicherheit macht. Zudem erhalten nur wenige Kantone (5) periodisch Kenntnis über den Stand der Bemühungen zur Minimierung von Cybersicherheit in den Spitälern. Cybersicherheit wird im Rahmen der Erteilung einer Betriebsbewilligung nur in einem Kanton berücksichtigt.

Im Zusammenhang mit der Einführung und Umsetzung des elektronischen Patientendossiers (EPD) sind die Stammgemeinschaften verpflichtet, bei den angeschlossenen Gesundheitseinrichtungen – also u. a. den Spitälern – Datenschutz- und Datensicherheitsvorgaben durchzusetzen. Damit dürfte das Datensicherheitsniveau der Gesundheitseinrichtungen angehoben werden.

Aktuell macht der Regierungsrat den Standort- und Listenspitälern keine expliziten Vorgaben im Bereich der Cybersicherheit/Cyberrisiken. Der Regierungsrat ist sich der Wichtigkeit der Cybersicherheit im Gesundheitswesen und der damit einhergehenden Herausforderungen insbesondere für die Spitäler jedoch durchaus bewusst. Das zuständige Departement des Innern wird darum gestützt auf die Ergebnisse des Nationalen Dialogs Gesundheitspolitik die Einführung von geeigneten Vorgaben im Bereich Cybersicherheit im Rahmen der Spitalplanung bei der Neuzuteilung der Leistungsaufträge prüfen.

Eine durch das Amt für Gesundheit und Soziales durchgeführte Umfrage bei den Schwyzer Spitälern Einsiedeln, Lachen und Schwyz hat zudem ergeben, dass die Spitäler der Cybersicherheit bereits grosses Gewicht und eine hohe Priorität beimessen. Entsprechende Massnahmen und Konzepte sind bereits etabliert und werden laufend überprüft. So wurden beispielsweise im Spital Einsiedeln und in der Seeklinik Brunnen, die beide zur AMEOS Gruppe gehören, Stabsstellen zum IT-Security- und IT-Risk-Management etabliert, IT-Security-Richtlinien entwickelt oder moderne IT-Lösungen und Technologien zur Absicherung der Infrastruktur eingeführt.

2.2 Beantwortung der Fragen

2.2.1 Erlangt der Regierungsrat periodisch Kenntnis über den Stand der Bemühungen zur Minimierung von Cyberrisiken und somit der Qualität der Cybersicherheit?

Der Regierungsrat erhält aktuell keine periodische und institutionalisierte Kenntnis darüber, welche konkreten Anstrengungen die Spitäler unternehmen, um Cyberrisiken zu minimieren. Themen wie u. a. Cybersicherheit werden jedoch je nach Bedarf an periodisch stattfindenden Austauschgesprächen zwischen den Spitälern und dem Departement des Innern respektive dem Amt für Gesundheit und Soziales thematisiert und besprochen.

2.2.2 Welches Gewicht hat bei der Beurteilung der Bewilligungsvergabe die Qualität der „Cybersicherheit" der Spitäler?

Bis anhin wurden im Rahmen der Erteilung der Betriebsbewilligung keine expliziten Vorgaben im Bereich Cybersicherheit gemacht. Nicht zuletzt auch darum, weil aktuell ein national einheitlicher Standard dafür fehlt. Im Zuge der Spitalplanung 2024 wird geprüft, ob neu explizite Vorgaben bezüglich Cybersicherheit bei der Bewilligungsvergabe und der Erteilung der Leistungsaufträge gemacht werden sollen. Möglicherweise kann dabei bei den Datenschutz- und Datensicherheitsvorgaben, welche im Rahmen der Einführung und Umsetzung des EPD umgesetzt werden müssen, angeknüpft werden. Der Regierungsrat erachtet es hierbei als zentral, dass keine doppelten Hürden für die Spitäler aufgestellt werden.

2.2.3 Gibt es spezifische (Minimal-)Vorgaben für die Spitäler im Themenkomplex „Cybersicherheit" ...

a. zur periodischen Prüfung, Beurteilung und allenfalls Rapportierung an die Aufsicht?
b. Audits durch interne / externe Prüfinstanzen oder dergleichen?
c. für (Minimal-)Erfordernisse als Grundlage für die Bewilligungsvergabe?

Alle Spitäler im Kanton Schwyz sind privatrechtlich organisiert und haben unterschiedliche Trägerschaften. Durch diese Eigenständigkeit verfügen die Schwyzer Spitäler über eine grosse unternehmerische Freiheit und handeln operativ selbstständig. In diesem Sinne wurden den Spitälern

bisher keine expliziten Vorgaben im Bereich der Cybersicherheit gemacht. Allfällige Minimalvorgaben werden im Zuge der Spitalplanung 2024 geprüft (siehe Ziffer 2.2.2).

2.2.4 Sind seitens Aufsicht betriebsorganisatorische Prozesse etabliert, die der laufenden Anpassung der Beurteilungskriterien aufgrund der steigenden Risiken und der Komplexität Rechnung tragen, namentlich in den Bereichen...

a. Beschaffungsmanagement der Spitäler?
b. Asset Life Cycle Management der Spitäler?
c. Security Operations & Incident Response der Spitäler?
d. Datenschutz & Risiko Management der Spitäler?

Siehe Ziffer 2.2.2, die Umfrage bei den Spitälern hat zudem gezeigt, dass die Schwyzer Spitäler bereits entsprechende betriebsorganisatorische Prozesse etabliert haben.

Beschluss des Regierungsrates

1. Die Vorsteherin des Departements des Innern wird beauftragt, die Antwort im Kantonsrat zu vertreten.

2. Zustellung: Mitglieder des Kantonsrates.

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

Im Namen des Regierungsrates:

Dr. Mathias E. Brun
Staatsschreiber