Auszug aus dem Protokoll des Regierungsrates des Kantons Zürich

KR-Nr. 73/2020

Sitzung vom 29. April 2020

426. Anfrage (Cybersicherheit an Spitälern im Kanton Zürich)

Kantonsrätin Bettina Balmer-Schiltknecht, Zürich, und Kantonsrat Benjamin Walder, Wetzikon, haben am 24. Februar 2020 folgende Anfrage eingereicht:

Bereits im Zusammenhang mit den Jahresberichten 2016 des Kantonsspitals Winterthur und des Universitätsspitals Zürich hat sich die Aufsichtskommission für Bildung und Gesundheit mit der Cybersicherheit an den kantonalen Spitälern befasst und dies im Kantonsrat Zürich öffentlich thematisiert. Die Problematik von Cyberattacken darf gerade angesichts der zunehmenden Digitalisierung im Gesundheitswesen nicht unterschätzt werden. Um der wachsenden Bedrohungslage gerecht zu werden, müssen Spitäler immer grössere finanzielle und personelle Ressourcen dafür aufwenden. Ungeachtet dessen kommt es immer wieder zu Cyberattaken auf Spitäler – auch im Kanton Zürich. Am 28.1.2020 thematisierte die NZZ einen Cyberangriff auf das Spital Wetzikon im letzten Oktober und berichtete ausführlich über das Einfallstor und den entstandenen wirtschaftlichen Schaden.

Wir bitten den Regierungsrat deshalb um die Beantwortung der folgenden Fragen:

1. Wie viele Cyberattacken auf Spitäler im Kanton Zürich gab es in den letzten Jahren und waren sensitive Patientendaten oder die Grundversorgung betroffen? Wie kritisch schätzt der Regierungsrat die Bedrohungslage insgesamt für Spitäler ein?
2. Wie viele Ressourcen setzen das USZ und KSW heute ein, um die IT-Sicherheit zu gewährleisten und sich gegen Cyberangriffe zu schützen? Sind das KSW und USZ der Meinung, dass die heute eingesetzten Ressourcen ausreichen, um eine optimale IT-Sicherheit zu gewährleisten? Mit welchem Aufwand rechnen sie in Zukunft?
3. Welche Vorkehrungen empfiehlt der Regierungsrat den Spitälern, um gegen Cyberattacken gerüstet zu sein und warum gibt es heute keine Minimalstandards?
4. Sieht der Regierungsrates Bedarf für Minimalstandards und wenn ja, in welchen Bereichen und Umfang würde der Regierungsrat diese festlegen? Wer wäre in der Pflicht, diese zu definieren, umzusetzen und zu kontrollieren?
5. Falls es aus Sicht des Regierungsrates keine Minimalstandards für IT-Sicherheit an den Spitälern im Kanton Zürich braucht, warum nicht?

6. Einzelne Spitäler im Kanton Zürich haben ihre Kompetenzen für die IT-Sicherheit in privatwirtschaftlich organisierten Firmen gebündelt und ausgegliedert. Wie beurteilt der Regierungsrat dieses Vorgehen in Bezug auf das Kosten-Nutzen-Verhältnis und auf die angesprochenen Sicherheitsstandards? Wer steht im Falle eines Cyberangriffs in der Verantwortung und käme für den entstanden Schaden auf?
7. Wie steht der Regierungsrat gegenüber einer möglichen Meldepflicht von Spitälern bei Cyberattacken?

Auf Antrag der Gesundheitsdirektion

beschliesst der Regierungsrat:

I. Die Anfrage Bettina Balmer-Schiltknecht, Zürich, und Benjamin Walder, Wetzikon, wird wie folgt beantwortet:

Zu Frage 1:

Die Spitalinformatik stellt mit ihrer digital vernetzten medizinischen Infrastruktur und der digitalen Datenbearbeitung, insbesondere von besonders sensiblen Patientendaten, ein begehrtes Ziel von Cyberattacken dar. Das macht Spitäler anfällig für unrechtmässige Datenentwendungen beispielsweise zu Erpressungs- oder Betrugszwecken. Die Anzahl Angriffe kann nicht genannt werden, denn es gibt sie täglich. Viele davon bleiben unentdeckt, weil sie von den ICT-Sicherheitseinrichtungen abgefangen werden. Wie eine Umfrage bei den Listenspitälern vom März 2020 ergeben hat, sind sich die Spitalleitungen ausnahmslos des Risikos bewusst. Sie beurteilen das Risiko eines Cyberangriffs im Allgemeinen als hoch bis sehr hoch.

Bei keinem der Angriffe auf die Zürcher Spitäler war die Grundversorgung in Gefahr. Patientendaten sind immer «sensitive» Daten (sogenannt besondere Personendaten gemäss Gesetz über die Information und den Datenschutz [IDG, LS 170.4]). Insofern geht es bei Cyberangriffen auf Spitäler immer um besonders heikle Daten. Das macht die Angriffe auf Spitäler letztlich auch so attraktiv für Cyberkriminelle. Der Regierungsrat schätzt die Lage als kritisch ein und erachtet Vorgaben zuhanden der Spitäler als notwendig (vgl. Beantwortung der Fragen 3–5).

Zu Frage 2:

Das Universitätsspital Zürich betreibt ein auf dem international anerkannten Standard ISO 27001 beruhendes Information Security Management System und verfügt über einen von der IT unabhängigen Chief Information Security Officer (CISO). Die IT-Einheiten beschäftigen rund 170 Mitarbeitende und stellen innerhalb des Betriebs die Informationssicherheit operativ sicher. Eine zentrale Rolle spielt dabei das aus vier

Personen bestehende Netzwerk-Security-Management-Team, das fallweise weitere Spezialistinnen und Spezialisten innerhalb der einzelnen Bereiche beiziehen kann. Da die technologische Abhängigkeit und mit dieser auch die Verletzbarkeit der Spitäler künftig weiter zunehmen wird und gleichzeitig die Anzahl und die Qualität der Cyberangriffe steigt, wird im Rahmen der stetigen Optimierung der Informationssicherheit auch der personelle Aufwand zunehmen.

Das Kantonsspital Winterthur beschäftigt insgesamt rund 60 Personen für IT-Belange. Es betreibt ein spezielles Security Operation Center mit wechselnder Besetzung von bis zu fünf Personen und setzt zudem ebenfalls einen von der IT unabhängigen CISO ein. Die zunehmende Exposition der Spitäler und die steigende Anzahl von Cyberattacken machen jedoch einen Ausbau der personellen Mittel nötig. Entsprechend zeichnet sich ab, dass sich gewisse Profile zu Vollzeitstellen entwickeln, was gegenwärtig auch konkret in Planung ist.

Zu Fragen 3–5:

Spitäler sind gemäss § 7 IDG verpflichtet, die Informationssicherheit durch angemessene organisatorische und technische Massnahmen sicherzustellen. Die zu treffenden Massnahmen haben sich insbesondere nach dem jeweiligen Stand der Technik zu richten.

Zur Sicherstellung der Informationssicherheit gibt es bereits verschiedene international anerkannte Standards, wie z. B. ISO 27001, NIST, COBIT, BSI 100-2, sowie den Minimalstandard zur Verbesserung der IKT-Resilienz des Bundes. Der Regierungsrat hält es für sinnvoll, dass sich die Spitäler an den vorhandenen Standards orientieren. Der Aufbau von zusätzlichen Standards brächte keinen Gewinn für die Datensicherheit.

Die Gesundheitsdirektion prüft derzeit, ob die Spitallisten um einen Anhang zur Informationssicherheit oder – alternativ dazu – die gesundheitspolizeilichen Bewilligungen der Spitäler um entsprechende Auflagen ergänzt werden sollen.

Zu Frage 6:

Die (gänzliche oder teilweise) Ausgliederung von Aufgaben der Informationssicherheit ist in gewissen Spitälern bereits heute Tatsache. Dagegen ist aus Sicht des Regierungsrates nichts einzuwenden, solange die gesetzlichen Anforderungen an den Datenschutz und die Informationssicherheit eingehalten werden. In der Verantwortung gegenüber der Patientin oder dem Patienten oder – wenn es um die Einhaltung von Sicherheitsstandards geht – gegenüber dem Kanton als Aufsichtsinstanz und Leistungsauftraggeber stehen immer die Spitalleitungsorgane. Über das Kosten-Nutzen-Verhältnis einer Ausgliederung äussert sich der Regierungsrat nicht. Dies zu beurteilen, ist Sache der Spitalleitungsorgane.

Zu Frage 7:

Eine Meldepflicht würde die Informationssicherheit nicht verbessern, denn einerseits sind die Sicherheitsverantwortlichen der Spitäler unter einander vernetzt und tauschen Meldungen über Sicherheitsgefährdungen laufend aus und anderseits setzt die Melde- und Analysestelle Informationssicherheit des Bundes nach entsprechenden Meldungen von anderen Nutzerinnen und Nutzern Warnmeldungen an die angeschlossenen Betriebe ab; dadurch ist sichergestellt, dass die Sicherheitsverantwortlichen der Spitäler zeitnah alarmiert werden.

II. Mitteilung an die Mitglieder des Kantonsrates und des Regierungsrates sowie an die Gesundheitsdirektion.

Vor dem Regierungsrat
Die Staatsschreiberin:
Kathrin Arioli