

**KANTONSRATSPROTOKOLL**

Sitzung vom 4. Dezember 2023  
Kantonsratspräsidentin Schmutz Judith

**A 6 Anfrage Estermann Rahel und Mit. über die Cybersicherheit der öffentlichen Verwaltung und der Infrastruktur im Kanton Luzern / Justiz- und Sicherheitsdepartement i. V. mit Finanzdepartement**

Rahel Estermann ist mit der Antwort des Regierungsrates teilweise zufrieden und verlangt Diskussion.

Rahel Estermann: Mir ist bewusst, dass es nicht einfach ist, in der Öffentlichkeit zu solchen Fragen Stellung zu nehmen. Es ist ein Balanceakt, und es wäre naiv, zu viel über das eigene Sicherheitsdispositiv zu erzählen. Die ausführlichen Antworten hinterlassen bei mir den Eindruck, dass die Regierung und die Verwaltung das Thema ernst nehmen. Trotzdem bin ich mit der Beantwortung einiger Aspekte nur teilweise zufrieden. Einer davon ist die Sicherheitskultur. In der Geschichte der Technologien zeigt sich etwas sehr Interessantes: Transparenz führt zu mehr Sicherheit. Dies erscheint zwar paradox, ist aber tatsächlich so. Dass Zugfahren und Fliegen heute so sicher sind, hat mit den umfangreichen Sicherheitsmanagementsystemen zu tun, bei denen Vorfälle transparent und sehr eingehend untersucht werden. In der Schweiz beispielsweise untersucht die Schweizerische Sicherheitsuntersuchungsstelle (Sust) jeden Vorfall im Zusammenhang mit Zügen, Flugzeugen oder Schiffen und publiziert einen detaillierten Bericht mit Erkenntnissen. Auf der Webseite der Sust werden relativ ausführliche Informationen über Ereignisse aufgeschaltet, ein aktuelles Beispiel ist der Zugunfall im Gotthard-Basistunnel. Dank diesem Verfahren können aus solchen Vorfällen Lehren gezogen werden. Es etabliert sich eine Sicherheitskultur und zwingt alle Organisationen zu einem Sicherheitsmanagement. Genau in diese Richtung müssen wir im Bereich Cybersicherheit gehen. Mit dem Cyberkoordinator auf kantonaler Ebene und dem nationalen Zentrum für Cybersicherheit (NCSC) sind entsprechende Plattformen vorhanden. Es ist aber auch eine echte Zielsetzung aller Staatsebenen nötig, um diese gemeinsame Aufgabe anzugehen. Es müssen möglichst viele Informationen ausgetauscht werden, so weit wie möglich auch mit der Öffentlichkeit. Es braucht den Willen, Vorfälle schonungslos zu analysieren und daraus zu lernen. Zudem brauchen wir eine Sicherheitskultur, also das Verständnis, dass es nur gemeinsam möglich ist, die Sicherheit im digitalen Raum zu verbessern. Die Einstellung, dass jeder Akteur nur für sich selbst schaut, macht die Welt schlussendlich unsicherer. Es muss uns ein Anliegen sein, dass die digitalen Systeme sicher sind, funktionieren und keine Attacks geschehen. Am Schluss müssen unsere Institutionen funktionieren. Zudem sind bei einer Attacke unsere Daten und damit unsere Privatsphäre betroffen. Auf kantonaler und kommunaler Ebene werden sehr viele schützenswerte Daten zumindest temporär gespeichert: Steuern, individuelle

Prämienverbilligung, Geschwindigkeitsbussen oder welche Volksinitiative unterschrieben wurde. In diesem Zusammenhang erscheint auch der Verweis auf die Gemeindeautonomie sehr fragwürdig. Am Schluss geht es auf Kosten der Bürgerinnen und Bürger, wenn der Kanton und die Gemeinden nicht zusammenarbeiten und sie nur halb fertige Lösungen produzieren. Einzelne Gemeinden sind mit der Cybersicherheit sehr gefordert, wenn nicht sogar überfordert, was auch auf die Ressourcen zurückzuführen ist. Sie sind nicht in der Lage, sich genügend auszurüsten und vorzubereiten. Natürlich liegt die Verantwortung bei den Gemeinden, trotzdem ist es wenig sinnvoll, wenn alle 80 Gemeinden diese Aufgabe selbst übernehmen. Weshalb gibt es keine gemeinsame Initiative des Kantons zusammen mit dem Verband Luzerner Gemeinden (VLG), um dieses Thema vertiefter anzugehen? Sie alle haben sicher vom Fall «Xplain» gehört, einem Softwarehersteller auf Bundesebene, der gehackt wurde. Ich habe die Erwartung, dass der Kanton und die Gemeinden bei der eigenen Beschaffung in Zukunft genau hinsehen.

Eva Forster: Ein bestmöglicher Schutz gegen Cyberangriffe ist auch der FDP-Fraktion ein sehr grosses Anliegen. Es ist keine Frage, dass es zu Angriffen kommen wird. Die Frage lautet nur, wann und wie gross der Schaden sein wird. Die aufgezeigten Massnahmen und die aktuelle Organisation zeigen das Bewusstsein der Regierung auf. Es ist uns aber wichtig, dass die Cybersicherheit bei der täglichen Arbeit, bei Informatikprojekten und auch bei der Anpassung von Prozessen sehr aktiv mit einbezogen wird. Wir erwarten von der Regierung, der Verwaltung, den Gemeinden, aber auch von jedem Einzelnen ein aktives statt reaktives Handeln. Treffen wird es uns in jedem Fall, es fragt sich nur wann und wie stark.

Andrea Pfäffli: Die SP-Fraktion kann Verständnis dafür aufbringen, dass aufgrund der Datensensibilität keine konkreteren Informationen zur Beurteilung der aktuellen Situation genannt werden können. In ihrer Antwort schreibt die Regierung, dass sie einer klaren Strategie folgt und bereits diverse Massnahmen zur Stärkung der Cybersicherheit der öffentlichen Verwaltung und der Infrastruktur des Kantons Luzern ergriffen hat. Dies ist wichtig und richtig. Die besten Strategien nützen aber nichts, wenn sie nicht wirksam umgesetzt werden. Diesbezüglich kommt der kürzlich geschaffenen Stelle des kantonalen Cyberkoordinators eine ganz zentrale Rolle zu. Sie hat viel und gewichtige Arbeit vor sich. Die Frage lautet nicht, ob der Kanton und seine ausgelagerten Einheiten von Cyberangriffen betroffen sind, sondern vielmehr wann. Ich zweifle stark daran, dass die Gemeindeautonomie, wie sie von der Regierung in ihrer Antwort hervorgehoben wird, bei dieser Thematik wirklich zielführend ist. Im Gegenteil, zum Erreichen der Ziele ist mehr gemeinsame Sensibilisierungsarbeit notwendig und auch unterstützende und qualitative Standardlösungen für die Gemeinden, insbesondere auch deshalb, weil bei den Gemeinden sehr unterschiedliche Voraussetzungen zur Gewährleistung der Datensicherheit herrschen. Es ist zentral, dass der Kanton im Interesse aller sein Wissen bündelt und zur Verfügung stellt, genügend Ressourcen bereithält und eine koordinative Funktion wahrnimmt. Ich möchte insbesondere betonen, dass wir in dieser Angelegenheit über den Schutz von sensiblen und auch besonders schützenswerten Personendaten unserer Bürgerinnen und Bürger diskutieren. Deshalb müssen dieses Thema und die Suche nach möglichen Lösungen im Interesse von uns allen sein.

Melissa Frey-Ruckli: Für einen modernen und sicheren Kanton Luzern ist es von entscheidender Bedeutung, dass die Cybersicherheit der öffentlichen Verwaltung und von kritischen Infrastrukturen auf höchstem Niveau gewährleistet ist. Die Umsetzung der Nationalen Cyberstrategie (NCS II) ist ein wichtiger Schritt in die richtige Richtung, um diese Sicherheit zu gewährleisten. Dennoch lässt sich feststellen, dass Verbesserungspotenzial vorhanden ist, da vieles auf Eigenverantwortung und auf föderalistischen Prinzipien beruht.

Die sehr knappen Ressourcen in gewissen Gemeinden stellen eine grosse Herausforderung dar. Es ist wichtig, dass die schützenswerten Personendaten auch dort gut geschützt bleiben. Die Mitte-Fraktion ist der Meinung, dass besonders dort die Überprüfung gestärkt und gegebenenfalls auch koordiniert werden sollte, damit alle Verwaltungen einen Mindeststandard für IT-Dienstleistungen gewährleisten. Die Bedrohungslage im Bereich der Cybersicherheit entwickelt sich ständig weiter. Deshalb ist es wichtig, dass die Sicherheitsmassnahmen regelmässig überprüft und bei Bedarf angepasst werden. Ein flexibles und agiles Sicherheitskonzept ist unerlässlich, um der sich wandelnden Bedrohung entgegenzutreten. In den letzten Jahren wurde im Kanton Luzern insgesamt eine gute Cyberstrategie entwickelt, aber es bedarf kontinuierlicher Anstrengungen, um die Cybersicherheit auf diesem Niveau zu behalten und stetig zu aktualisieren. So können wir eine erhöhte Widerstandsfähigkeit gegen diese Bedrohungen gewährleisten. Die Mitte-Fraktion will eine gute und agile Cybersicherheit für den Kanton und die Luzerner Bevölkerung. Wir werden den schnellen technischen Wandel in dieser Thematik aufmerksam weiterverfolgen.

Sibylle Boos-Braun: Das Thema Cybersicherheit ist wichtig, auch bei den Gemeinden. Deshalb haben die Gemeinden gemeinsame Veranstaltungen mit dem Kanton durchgeführt und sogar mit der entsprechenden Stelle auf Bundesebene, um die Verwaltungen auf kommunaler Ebene zu sensibilisieren. Wir müssen uns aber bewusst sein, dass die Gemeinden über sehr unterschiedliche Infrastrukturen und unterschiedliche Anbieter verfügen; entsprechend arbeiten sie auch unterschiedlich. Die Gemeinden sind sich des Risikos bewusst und schränken es nach Möglichkeit ein. Eine 100-prozentige Sicherheit gibt es bei diesem Thema aber nicht.

Für den Regierungsrat spricht Justiz- und Sicherheitsdirektorin Ylfete Fanaj.

Ylfete Fanaj: Wir sind der Postulantin dankbar für diese Fragen. So erhielten wir die Möglichkeit, wenigstens gewisse Antworten zu geben. Wir nehmen das Thema ernst und befassen uns damit. Im Kanton Luzern setzen wir die NCS um. Diese legt fest, dass der Schutz vor Cyberbedrohungen eine gemeinschaftliche Aufgabe von Gesellschaft, Wirtschaft und Staat ist und es klar definierte Zuständigkeiten gibt. Sie beruht auf föderalistischen Prinzipien, sie ist dezentral und in gemeinsamer Verantwortung. Natürlich haben auch die Gemeinden eine Verantwortung. Der kantonale Cyberkoordinator hat bei den Gemeinden eine Umfrage durchgeführt und sie um eine Selbsteinschätzung gebeten. Dabei hat es sich gezeigt, dass die meisten Gemeinden gut bis sehr gut aufgestellt sind. Es gibt aber auch Gemeinden, die über einen ungenügenden Sicherheitsstandard verfügen. Einzelne Gemeinden haben sich nicht an der Umfrage beteiligt. Es gibt auch IT-Dienstleister, die ungenügend aufgestellt sind. Diesen Handlungsbedarf haben wir erkannt und mit den entsprechenden Gemeinden Kontakt aufgenommen. Schlussendlich können wir nur beratend und im Sinn einer Empfehlung agieren. Schlussendlich sind die Gemeinden selbst für die Cybersicherheit zuständig. Aus dieser Datenerhebung hat sich beim Cyberkrisenmanagement Handlungsbedarf ergeben, das heisst es stellt sich die Frage, was bei einem Vorfall zu tun wäre. In diesem Bereich müssen wir mehr tun und die Gemeinden unterstützen. Wir haben auch festgestellt, dass es für den Fall, wenn etwas passiert, fehlende Absprachen mit den IT-Dienstleistern gibt. Zudem fehlen Sensibilisierungsmassnahmen. Um diesen Themen gerecht zu werden, haben wir verschiedene Massnahmen ergriffen, die wir nun umsetzen. Eine davon ist, dass wir Sensibilisierungsanlässe durchführen. Sie waren ja im September ebenfalls persönlich zu einem solchen Anlass eingeladen, an welchem 90 Personen aus Gemeinden sowie IT-Dienstleister teilnahmen. Es ging um Themen wie Prävention, das richtige Vorgehen bei Cybervorfällen und die Krisenorganisation. Diesen Anlass haben wir gemeinsam mit dem VLG

durchgeführt. Zudem stellen wir den Gemeinden ein kostenloses E-Learning-Angebot über Cyber- und Informationssicherheit zur Verfügung. Über das NCSC erhalten die Gemeinden auch relevante Sicherheitsinformationen. Wenn es zu Sicherheitsvorfällen kommt, schauen wir uns diese konkreter an und klären ab, was genau passiert ist und was wir daraus lernen können. Das haben wir auch im Fall von Xplain getan. Wir widmen uns dem Thema Cybersicherheit auch in Zukunft, und ich danke Ihnen für Ihre kritische Begleitung dabei.