Interpellation von Luzian Franzini, Tabea Zimmermann Gibson und Rita Hofer betreffend Datensicherheit und Datenschutz beim Zuger Impfzentrum und allgemein beim Kanton Zug
(Vorlage Nr. 3221.1 - 16563)

Antwort des Regierungsrats
vom 9. November 2021

Sehr geehrte Frau Präsidentin
Sehr geehrte Damen und Herren

Der Kantonsrat Luzian Franzini sowie die Kantonsrätinnen Tabea Zimmermann Gibson und Rita Hofer haben am 5. April 2021 eine Interpellation betreffend Datensicherheit und Datenschutz beim Zuger Impfzentrum und allgemein beim Kanton Zug (Vorlage Nr. 3221.1 – 16563) eingereicht. Der Kantonsrat überwies die Interpellation am 6. Mai 2021 an den Regierungsrat.

Der Regierungsrat nimmt wie folgt Stellung.

A. Vorbemerkung

Einleitend ist anzumerken, dass der Kanton Zug selbst kein Corona-Impfzentrum betreibt. Das Impfzentrum in Baar wird von den beiden Akutspitälern im Kanton Zug, des Zuger Kantonsspitals und der Hirslanden AndreasKlinik, im Auftrag des Kantons Zug betrieben. Der Kanton Zug ist nicht in die operativen Tätigkeiten des Impfzentrums involviert.

Der Kanton Zug und das Zuger Impfzentrum nutzen seit Beginn der Corona-Impfaktion die Software OneDoc für die Registrierungen, Anmeldungen und Terminvergaben der Corona-Impfungen. Diese Softwarelösung wurde den Kantonen vom Bund zur Verfügung gestellt und zur Nutzung empfohlen. Die grosse Mehrheit der Kantone nutzt diese Software. Der Kanton Zug hat aus Zeit- und Effizienzgründen auf die Ausarbeitung einer eigenen Softwarelösung verzichtet.

B. Beantwortung der Fragen

Frage 1: Weshalb wurde der Amazon-Mailservice für eine bezüglich des Datenschutzes heikle Funktion verwendet, die vom Bund so nicht vorgesehen war, bzw. weshalb wurde dessen Informationssicherheit nicht von der Datenschutzstelle geprüft und eine datenschutztechnische Folgeabschätzung durchgeführt?

Die Möglichkeit, allen geimpften Personen automatisch einen Impfnachweis per E-Mail zuzustellen, wurde von Softwareanbieter OneDoc ermöglicht. Das Zuger Impfzentrum hat diese Möglichkeit umgehend genutzt, um dem Bedürfnis der geimpften Zugerinnen und Zugern nach der elektronischen Zustellung des Impfnachweises schnell und unkompliziert nachzukommen. Da der Versand durch die vom Bund explizit empfohlene Software ermöglich wurde, konnte davon ausgegangen werden, dass die datenschutztechnischen Folgeabschätzungen von den zuständigen Bundesstellen vorgenommen wurden.

Sobald der Kanton Zug Kenntnis davon erhalten hatte, dass beim automatischen Versand der Impfnachweise datenschutztechnische Fragen zu klären sind, wurde das Impfzentrum umgehend angewiesen, den Versand der E-Mails zu stoppen. Dies wurde vom Impfzentrum sofort umgesetzt.

Frage 2: Kann der Regierungsrat bestätigen, dass zumindest die Übertragung der unverschlüsselten Patientendaten über ausländische Server verschlüsselt war?

Die versandten E-Mails wurden stets via HTTPS-Verschlüsselung verschickt. Die Daten in den jeweiligen E-Mails umfassten zudem lediglich die persönlichen Angaben der geimpften Person (Vorname, Name, Adresse, Geburtsdatum, Krankenkassennummer) sowie das Datum der Impfung und der verabreichte Impfstoff. Weitere Gesundheitsdaten, etwa über allfällige Vorerkrankungen, wurden zu keinem Zeitpunkt übermittelt.

Frage 3: Wie lassen sich aus Sicht des Regierungsrats solche Sicherheitslücken künftig verhindern? Wer stellt den Schutz der Daten sicher?

Ein ähnlicher Fall lässt sich kaum vermeiden. Der Kanton muss sich bei Anwendungen, die vom Bund zur Verfügung gestellt werden, darauf verlassen können, dass Datenschutzfragen durch die zuständigen Bundesbehörden geklärt wurden.

Bei Anwendungen, welche durch den Kanton selbst entwickelt oder in Auftrag gegeben werden, bestehen umfassende Vorgaben und Prozesse, um Sicherheitslücken zur verhindern. Gemäss § 5d des Datenschutzgesetzes (DSG) vom 28. September 2000 (BGS 157.1) und § 3 der Verordnung über die Informationssicherheit von Personendaten (VIP) vom 16. Januar 2007 (BGS 157.12) ist das Organ, das Personendaten bearbeitet, für die datenschutzkonforme Datenbearbeitung verantwortlich.

Sicherheitslücken lassen sich primär mit institutionalisierten und standardisierten Datenschutzprozessen verhindern. Die entsprechenden gesetzlichen Vorgaben und Prozesse bestehen im Kanton Zug. Damit Sicherheitslücken künftig verhindert werden können, ist die Einhaltung der bestehenden Prozesse durchzusetzen und dadurch sicherzustellen, dass die Prozesse auch wirksam sind.

Neben institutionalisierten und standardisierten Datenschutzprozessen stellt auch die Sensibilisierung der verantwortlichen Organe für Datenschutz und Informationssicherheit durch Schulungen der Mitarbeitenden aller Führungsstufen eine weitere wichtige Massnahme zur Verhinderung von Sicherheitslücken dar.

Frage 4: Welche Änderungen in den Prozessabläufen werden angestrebt, damit solche Fehler bezüglich des Datenschutzes und der Datensicherheit nicht mehr gemacht werden?

Eine Änderung von Prozessabläufen ist nicht erforderlich.

Frage 5: Wie sensibilisiert der Kanton Zug seine Mitarbeitenden in der Verwaltung und an den Schulen bezüglich des Datenschutzes und der Datensicherheit?

Die Merkblätter der Datenschutzstelle zur Datensicherheit wurden letztmals im Herbst 2020 aktualisiert. Sie enthalten verbindliche Sicherheitsvorgaben zum sicheren Umgang mit Daten, Passwörtern, E-Mail, Internet, mobilen Geräten und Datenträgern. Sämtliche Mitarbeitenden wurden im letzten Herbst über die angepassten Merkblätter informiert. Die Datenschutzstelle sensibilisiert die Mitarbeitende des Kantons darüber hinaus u.a. durch Schulungen. Namentlich ist sie an der vom Personalamt organisierten Einführungsveranstaltung für neue Mitarbeitende mit einem Kurzreferat vertreten. Für die gemeindlichen Schulen hat die Datenschutzstelle einen Datenschutz-Leitfaden herausgegeben (2. überarbeitete Auflage, 2017).

Aufbauend auf den Merkblättern existiert ein E-Learning-Tool zur Datensicherheit. Dieses muss gemäss Regierungsratsbeschluss vom 10. Dezember 2013 von allen Mitarbeitenden der kantonalen Verwaltung, der Gerichte, der öffentlich-rechtlichen Anstalten des Kantons sowie privater Dritter mit Leistungsvereinbarung mit dem Kanton innert drei Monate nach Stellenantritt und danach alle zwei Jahre mit einem erfolgreichen Test absolviert werden.

Frage 6: Werden in der Verwaltung Tests bezüglich der Datensicherheit durchgeführt (z.B. eigene Phishing Mails, falsche Links, Anfragen zu vertraulichen Informationen)? Falls ja, was sind die Ergebnisse?

Ein Phishing Awareness-Service ist etabliert. Alle IT-User (Verwaltungsangestellte der Gemeinden und des Kantons inklusive Gerichte und kantonale Schulen) erhalten zufällig zugestellte Phishing-E-Mails. Klickt ein User in einem zugestellten E-Mail auf einen Link, gibt er Daten ein oder versucht er ein Makro zu starten, wird er auf eine Seite weitergeleitet, welche ihn an die Unzulässigkeit seines Verhaltens erinnert und ihn über die Gefahren seines Verhaltens aufgeklärt. Die Ergebnisse werden periodisch, anonym und nach Organisationseinheiten ausgewertet und können für weitere zielgerichtete Awareness-Massnahmen genutzt werden. Die Resultate zeigen, dass das Phishing Awareness Training wirkt. Da zwischen den verschiedenen Organisationseinheiten aber noch Unterschiede bestehen, hat das Security Board des AIO entschieden, diese Sensibilisierungsmassnahmen weiterzuführen.

Frage 7: Welche Massnahmen können aus der Sicht des Regierungsrats bei sensiblen Daten zu höherer Datensicherheit und höherem Datenschutz beitragen?

Mit der Informatikverordnung (ITV) vom 13. November 2018 (BGS 153.53) sind im Bereich der Informationssicherheit funktionierende Strukturen und Prozesse etabliert worden (z. B. ISO-27001-Zertifizierung). Auf der Intranetseite des AIO stehen Mitarbeitenden des Kantons und der Einwohnergemeinden Informationen zur Informationssicherheit zur Verfügung (z. B. IT Sicherheitsauflagen bei Projekten). Ebenfalls aufgeschaltet sind die einzuhaltenden IT Nutzungsregeln (z. B. Skype-Nutzungsregeln).

Wie in den vorherigen Antworten ausgeführt, sind die fortlaufende Institutionalisierung, Standardisierung und Sensibilisierung für die Fragen des Datenschutzes entscheidend.

Frage 8: Der Kanton Zug ist ein Vorreiter im Blockchain-Bereich und sieht sich auch als Herz des Swiss Crypto-Valleys. Teilt der Regierungsrat die Ansicht der Interpellierenden, dass der Kanton Zug bezüglich des Datenschutzes und der Datensicherheit ebenfalls in der obersten Liga spielen sollte, wenn er in diesem Bereich als politischer Partner ernst genommen werden will?

Ja, der Regierungsrat teilt diese Ansicht. Der Kanton Zug unternimmt viel, um diesem Anspruch gerecht zu werden. Der Regierungsrat verweist dabei auf die geplante Cybersecurity-Offensive im Rahmen des Programms Zug+. Der Regierungsrat beantragt dem Kantonsrat die Beteiligung an den Aufbaukosten des Nationalen Testinstituts für Cybersicherheit NTC im Kanton Zug (7,55 Millionen Franken) sowie einer zentralen Informations- und Anlaufstelle für kleine und mittlere Unternehmen im Kontext der Cybersicherheit (ITSec4KMU) in der Höhe von rund 1,4 Millionen Franken. Mit diesen Investitionen soll der Kanton Zug einen spürbaren Beitrag im wichtigen Bereich der Cybersicherheit leisten.

C. Antrag

Kenntnisnahme.

Zug, 9. November 2021

Mit vorzüglicher Hochachtung
Regierungsrat des Kantons Zug

Der Landammann: Martin Pfister

Die stv. Landschreiberin: Renée Spillmann Siegwart

90/mb