Interpellation von Daniel Stadlin
betreffend Cybersicherheit – ist die kantonale Verwaltung genügend geschützt?
(Vorlage Nr. 3308.1 - 16735)

Antwort des Regierungsrats
vom 1. Februar 2022

Sehr geehrte Frau Präsidentin
Sehr geehrte Damen und Herren

Kantonsrat Daniel Stadlin, Zug, hat am 1. Oktober 2021 eine Interpellation betreffend «Cybersicherheit – ist die kantonale Verwaltung genügend geschützt» eingereicht. Der Kantonsrat hat die Interpellation am 28. Oktober 2021 an den Regierungsrat zur Beantwortung überwiesen. Die in der Interpellation gestellten Fragen beantwortet der Regierungsrat wie folgt:

1. Was unternimmt der Regierungsrat aktuell hinsichtlich
a) der Gewährleistung von Cybersicherheit?
b) der Bekämpfung von Cyberattacken?

1a)
Das Risiko von Cyber-Angriffen auf das Informatiknetz des Kantons (an dem auch die Zuger Einwohnergemeinden angeschlossen sind) ist hoch. Primär gilt es, mit geeigneten technischen Massnahmen sicherzustellen, dass Angriffe nicht zum gewünschten Erfolg der Angreifenden führen. Gleichwohl kann es selbst beim Einsatz der besten und aktuellsten Sicherheitsmassnahmen vorkommen, dass ein Angriff gelingt und beispielsweise eine Malware eingeschleust werden kann. Erfahrungsgemäss ist das Einfallstor für Cyber-Angriffe nicht die Technik, sondern die Schwachstelle Mensch. Gelegentlich öffnen Mitarbeitende aus Unachtsamkeit oder Neugier eine entsprechend präparierte Datei, was zu einem Vorfall (Incident) führen kann.

Im Bereich von Cyber-Angriffen hat sich eine eigentliche Industrie entwickelt und entsprechende Angriffe werden mit grosser Professionalität vorgenommen. Als Extrembeispiel ist Ransomware aufzuführen. Diese verschlüsselt Daten. Somit könnten beispielsweise auch Backupdaten verschlüsselt werden, was zu einem Super-GAU für die betroffene Organisation führen würde.

Das Thema Informationssicherheit ist als Grundlage in der «Informatikstrategie Kanton Zug 2018–2022» unter Punkt 2.6 aufgeführt (vgl. Beilage 1). Ziel ist, die Informationssicherheit durch technische und organisatorische Massnahmen angemessen sicherzustellen. Diese richten sich nach den Datenschutzgesetzen und -vorgaben, ISO 27001 und weiteren relevanten Sicherheitsstandards. Eine der sieben strategischen Zielsetzungen der Informatikstrategie beinhaltet das Thema Sicherheit und Verfügbarkeit: «Die Sicherheit, Verfügbarkeit und Integrität der Informatiksysteme sind gewährleistet». Dazu sind verschiedene Massnahmen definiert, die zum Teil bereits umgesetzt werden konnten.

Die Informationssicherheit im Kanton Zug wird durch ein «föderales Modell» geführt. Dieses besteht aus drei Elementen mit unterschiedlichen Aufgaben und Rollen, die durch die zentrale Informatik, die dezentrale Informatik und die IT-Steuerung wahrgenommen werden. In der Informatikverordnung vom 13. November 2018 (ITV; BGS 153.53) werden die Aufgaben, Kompetenzen und Verantwortlichkeiten zur IT-Sicherheit geregelt. Zur Steuerung der Informationssicherheit ist ein übergeordnetes Security Board etabliert. § 8 der ITV verweist auf die

Bestimmungen im kantonalen Datenschutzgesetz und in der Datensicherheitsverordnung. Aufgrund der Legislaturziele 2019–2022 «L104 Stärkung Sicherheit im virtuellen Raum» erfolgte die Überarbeitung und Umbenennung der «Datensicherheitsverordnung» in «Verordnung über Informationssicherheit von Personendaten» (BGS 157.12). Diese ist am 19. Dezember 2020 in Kraft getreten.

Das Amt für Informatik und Organisation (AIO) des Kantons Zug betreibt ein Information Security Management System (ISMS) und ist ISO 27001 zertifiziert (vgl. Beilage 2).

Ausserdem ist der Kanton Zug aktives Mitglied bei diversen Bundes- und Kantonsgremien, wie beispielsweise der Schweizerischen Informatikkonferenz (SIK) oder der Cyber-Landsgemeinde. Der Kanton Zug engagiert sich stark in der SIK Arbeitsgruppe Informations-/Cybersicherheit, die viermal jährlich tagt. Behandelt werden insbesondere aktuelle Cybervorfälle und deren Gegenmassnahmen.

1b)
Die kantonale IT-Sicherheitsorganisation besteht aus einem IT-Sicherheitsbeauftragten (IT-SIBE) in einer 50%-Stelle, die direkt dem Leiter AIO unterstellt ist. Der IT-SIBE leitet das kantonale Security Board. Er ist für das IT-Riskmanagement, die Definition und Einhaltung von IT-Sicherheitsvorgaben in Projekten und internen Aufträgen, die Ausbildung der User für den korrekten Umgang mit Informationen und für die Umsetzung der Vorgaben aus der Norm ISO 27001 verantwortlich. Er vertritt den Kanton Zug zudem bezüglich IT-Security in der Schweizerischen Informatikkonferenz (SIK), in der Informations-Cybersicherheitsarbeitsgruppe und in anderen Erfahrungsgruppen (www.cscg.ch). Der IT-SIBE wird im AIO durch eine Fachperson unterstützt, welche die operative IT-Sicherheit an den Systemen überwacht.

Heute werden Sicherheitsvorfälle entweder ad-hoc gemeldet oder systematisch gemäss Kontrollplan erkannt. Die Zuständigkeiten sind geregelt. Sollte ein Informationssicherheitsvorfall ein hohes oder gar kritisches Risiko erreichen, kommen die internen Prozesse zur Anwendung, die die Verantwortlichkeiten und das konkrete Vorgehen beinhalten.

Für eine allfällige Bewältigung eines Cyberangriffs kann das AIO auf externe Spezialisten zurückgreifen, insbesondere für forensische Aufgaben. Zudem unterstützt die Melde- und Analysestelle Informationssicherung Melani des Nationalen Zentrums für Cybersicherheit (NCSC) des Bundes den Kanton Zug in Themen der Informationssicherheit.

2. Wie sieht die Zusammenarbeit mit dem Nationalen Zentrum für Cybersicherheit (NCSC) aus?

Der Kanton arbeitet aktiv bei Meetings mit, die vom Nationalen Zentrum für Cybersicherheit (NCSC) organisiert werden. Dazu gehört die bereits zum neunten Mal vom Sicherheitsverbund Schweiz durchgeführte Cyber-Landsgemeinde. An der am 16. September 2021 durchgeführten Cyber-Landsgemeinde tauschte man sich über die Umsetzung der kantonalen Projekte im Rahmen der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022 aus. Zudem wurde über einen konkreten Cyber-Angriff und dessen Bewältigung sowie über Digitale Identität eingehend diskutiert.

3. Gedenkt der Regierungsrat, analoge Strukturen bzw. Positionen wie beim Bund aufzubauen?

Die Bedrohungslage für die IT-Sicherheit in der Schweiz hat sich in den vergangenen Jahren deutlich zugespitzt. Gleichzeitig steigt die Abhängigkeit von IT-basierten Umgebungen für zentrale Geschäftsprozesse.

Die rasch fortschreitende Digitalisierung stellt den Kanton Zug vor Herausforderungen im Spannungsfeld Verfügbarkeit, Benutzerfreundlichkeit und IT-Sicherheit.

Eine IT-Organisation sorgt für einen bestmöglichen Schutz, indem Sicherheitssysteme verwendet werden, die selbst nur minimale Angriffsmöglichkeiten bieten. Gute Sicherheitstechnik reicht heute leider bei Cyberangriffen nicht mehr aus. Cyber-Risiken sind ein permanentes und wesentliches Unternehmensrisiko geworden.

Eine Versicherungslösung hilft nicht, die Risiken (Wahrscheinlichkeit eines Angriffs, Reputationsschaden etc.) zu vermeiden oder zu lindern. Der Hauptvorteil liegt in der finanziellen Entschädigung. Gewinn- und Ertragsausfälle sind beim Kanton kaum im Fokus. So führen zum Beispiel Betriebsausfälle bei einer Steuerverwaltung oder einem Strassenverkehrsamt höchstens zu einer verzögerten Fakturierung. Aber aufgrund der hohen Kosten zur Wiederherstellung der Daten und IT-Infrastruktur nach einem Ransom-Malwarebefall (Verschlüsselung der Systeme) prüft der Kanton Zug, für die Deckung der Wiederherstellungskosten eine zielgerichtete Cyber-Versicherung abzuschliessen.

Die durch den Sicherheitsverbund Schweiz (SVS) im 2014, 2017 und 2020 durchgeführten Erhebung der Cyberrisiken in den Kantonen haben dem Kanton Zug eine sehr gute Resilienz der Informations- und Kommunikationstechnik (IKT-Resilienz) bestätigt.

Aufgrund der heutigen Cyber-Gefahrenlage führen viele Organisationen in der Wirtschaft und auch der öffentlichen Hand sogenannte Security Operations Center (SOC) ein. Ein SOC ist eine eigene spezialisierte, organisatorische IT-Betriebseinheit, die rund um die Uhr für die Unversehrtheit der IT-Infrastruktur verantwortlich ist. Als wesentliche Komponenten der IT Sicherheit sind die personellen Ressourcen (Mensch), die Software sowie die technische und organisatorische Infrastruktur zu betrachten. Sinnbildlich ist das SOC der Turmwächter einer mittelalterlichen Burg. Dieser erkennt den anrückenden Feind und gibt eine Empfehlung für die Verteidigung ab. Ein SOC kann teilweise oder vollständig an eine bzw. einen Dienstleistenden ausgelagert sein.

Das Security Board hat den IT-SIBE beauftragt aufzuzeigen, wie Angriffe aus dem Internet auf die kantonale und gemeindliche IT und Anomalien oder Sicherheitsverletzungen innerhalb dieser Netzwerke dank dem Einsatz eines Security Operations Center möglichst zeitnah und systematisch erkannt und behoben werden können. Das AIO hat unter der Leitung des IT-SIBE 2021 eine Studie mit Strategieempfehlung in Auftrag gegeben. Die Strategieempfehlung zeigt auf, welche organisatorischen und technischen Massnahmen zu treffen sind und in welcher Reihenfolge diese für eine erfolgreiche SOC Umsetzung einzuleiten sind. Gestützt darauf wird derzeit die schrittweise Einführung eines Security Operation Centers (SOC) im Kanton Zug geprüft. Dabei wird auch die Kooperation mit anderen Kantonen oder den Anschluss an einen Kanton, der bereits ein SOC betreibt, evaluiert.

4. Wie sieht die Abstimmung und Koordination mit den Nachbarkantonen aus?

Auf Stufe der IT-Leiter und der Beauftragten zur IT-Sicherheit finden regelmässige Erfahrungsaustausche statt.

Im Bereich Polizei existieren definierte und abgesprochene Prozesse betreffend Cybercrime / Cybersicherheit auch in Zusammenarbeit mit den Nachbarkantonen und dem Bund.

5. Was unternimmt der Kanton im Bereich der systemrelevanten Infrastrukturen wie Energie, Wasser, Sicherheit oder Rettung?

Einleitend ist festzuhalten, dass grundsätzlich jede Organisation für ihre Cybersicherheit und die diesbezügliche Schulung der Mitarbeitenden selber verantwortlich ist. Die kantonalen und kommunalen Führungsorgane und die Partnerorganisationen (Polizei, Feuerwehr, Gesundheitswesen, Technische Betriebe und Zivilschutz), welche direkt beim Kanton oder einer Gemeinde eingebunden sind, halten sich dabei grundsätzlich an die verbindlichen Sicherheitsvorgaben des IT-Security-Boards des AIO, der Zuger Polizei und, bei Systemen des Bundes, an die entsprechenden Sicherheitsvorgaben der Fachstellen des Bundes. Die Infrastruktur-Werke für Wasser, Strom, Gas usw. sorgen selbstständig für ihre Cybersicherheit. Dabei stehen den Werken die Cyberfachstellen von Bund und Kantonen beratend zur Verfügung.

Der Kantonale Führungsstab (KFS) und die Gemeindeführungsstäbe (GFS) koordinieren aufgrund von vorbereiteten Einsatz-Checklisten mögliche Ereignisse (Hochwasser, Pandemie, Schweiz-Dunkel etc.). In Zusammenarbeit mit dem Bund und anderen Kantonen sind umfangreiche Sicherheitsverbundübungen durchgeführt worden. Diese umfassten unter anderem die Problemlösung der aus einem Cyberangriff entstandenen Probleme, jedoch nicht die eigentliche Bewirtschaftung der Cybersicherheit.

6. Erlangt der Regierungsrat periodisch Kenntnis über den Stand der Bemühungen zur Minimierung von Cyberrisiken und somit der Qualität der Cybersicherheit in der kantonalen Verwaltung und in den kantonalen Schulen?

Die Nutzung kantonaler Informatikmittel setzt voraus, dass die Merkblätter zur Informationssicherheit eingehalten werden. Sie gelten umfassend und verpflichtend. Die Einsatzrichtlinie definiert den Umgang von klassifizierten Informationen.

Aufbauend auf den Merkblättern existiert ein E-Learning. Dieses muss gemäss Regierungsratsbeschluss vom 10. Dezember 2013 von allen Mitarbeitenden der kantonalen Verwaltung, der Gerichte, verwaltungsnahen Betrieben sowie von Organisationen, die über einen Leistungsauftrag verfügen, innert drei Monate nach Eintritt und danach alle zwei Jahre absolviert werden.

Sämtliche Mitarbeitenden, temporär Angestellten und weitere Personen, welche für das AIO tätig sind, haben die IT-Sicherheitsbestimmungen (AIO) zu unterschreiben. Externe Personen, die Zugriff auf kantonale Daten und IT-Systeme benötigen, müssen zusätzlich vorgängig eine Geheimhaltungserklärung unterschreiben.

Im September 2020 hat das Security Board eine einjährige Sensibilisierungskampagne lanciert, mit dem Ziel, gefälschte oder mit Malware verseuchte E-Mails besser zu erkennen. Dabei wurden die Mitarbeitenden der kantonalen Verwaltung, der Gerichte und der kantonalen Schulen sowie der Einwohnergemeinden und verwaltungsnahen Betriebe, mit sechs fingierten «E-Mail-

Angriffen» konfrontiert. Die Mitarbeitenden wurden vorher über diese Aktion informiert. Sie haben den Hinweis erhalten, dass sie innerhalb eines Jahres sechs unterschiedliche E-Mails erhalten werden. Aus der Sensibilisierungskampagne resultieren folgende Erkenntnisse, welche dem Regierungsrat als Bericht zur Verfügung gestellt wurde:

- Der Effekt einer erhöhten Achtsamkeit gegenüber gefährlichen E-Mails konnte erzielt werden, allerdings nicht im erhofften Umfang.
- Im Vergleich zu anderen Organisationen im öffentlichen Sektor ist die Sensibilität noch nicht auf einem akzeptablen Niveau.
- Die Resultate der einzelnen Direktion, Gerichte, Einwohnergemeinden und Dritten variieren erheblich.
- Die Kampagne wird mit neuen Szenarien fortgeführt, um die Aufmerksamkeit gegenüber gefährlichen E-Mails und generell gegen Angriffe von aussen zu steigern.
- Das Security Board prüft weitere Massnahmen zur Sensibilisierung der Mitarbeitenden auf die Cyber Kriminalität.

7. Gibt es spezifische Vorgaben im Themenkomplex «Cybersicherheit» betreffend:
a) periodischer Prüfung, Beurteilung und Rapportierung?
b) Audits durch externe Prüfinstanzen?

7a)
Oberstes Ziel ist es, Angriffe aus dem Internet auf die kantonale und gemeindliche IT und Anomalien oder Sicherheitsverletzungen innerhalb dieser Netzwerke möglichst zeitnah und systematisch zu erkennen und abzuwehren. Durch gezielte sorgfältige Analyse der einzelnen Komponenten der IT Sicherheit können Risiken minimiert, Schwachstellen identifiziert und die wirksame Funktion der IT Sicherheitsinfrastruktur gewährleistet werden.

7b)
Ein wesentlicher Teil der ISO 27001 Zertifizierung besteht in der kontinuierlichen Prüfung durch unabhängige Instanzen. Dies beinhaltet einerseits jährliche Überwachungsaudits durch die ISO-Zertifizierungsstelle und andererseits auch durch externe spezialisierte Unternehmen, die die Einhaltung während dem Jahr prüfen. Zur Vermeidung von Vorfällen werden Verwundbarkeitsscans gegen die IT-Infrastruktur und gezielte IT-Audits und Penetrationstests über Anwendungen durch externe Partnerinnen bzw. Partner durchgeführt.

8. Sind seitens Regierungsrat Prozesse etabliert, die der laufenden Anpassung der Beurteilungskriterien aufgrund der steigenden Risiken und der Komplexität Rechnung tragen, namentlich in den Bereichen:
a) Beschaffungsmanagement?
b) Datenschutz und ICT-Risiko Management?

8a)
Das Kompetenzzentrum IT-Beschaffungen (BKZ IT) des AIO stellt Muster von zentralen Dokumenten für IT-Beschaffungen im Kanton Zug zur Verfügung. Neben Musterverträgen stehen auch Musterpflichtenhefte zur Verfügung.

8b)
Die Organe sind verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden. Im Vorfeld einer geplanten Datenbearbeitung sind die Risiken für die Grundrechte der betroffenen Personen entsprechend zu identifizieren, zu bewerten und mit geeigneten Massnahmen zu reduzieren. Dazu gehört die

Erstellung einer Datenschutz-Folgenabschätzung und Erstellung eines Informationssicherheits- und Datenschutzkonzepts (ISDS-Konzept). Diese Massnahmen sind in die bestehenden und kantonal vorgegebenen Projektabläufe des AIO (nach HERMES) eingebunden.

Es bestehen damit datenschutzseitige Vorgaben und Prozessabläufe. Die Datenschutzstelle hat mit dem Inkrafttreten des revidierten DSG per 1. September 2020 dazu entsprechende Vorlagen und Informationen erarbeitet und bereitgestellt. Die Vorlagen und Informationen sollen die verantwortlichen Organe dabei unterstützen, ihren gesetzlichen Pflichten mit Blick auf die Bearbeitung von Personendaten nachzukommen. Die datenschutzseitigen Vorgaben und Prozesse sind im Rahmen der DSG-Revision in die bestehenden und kantonal vorgegebenen Projektabläufe des AIO eingebunden worden. Sie gelten aber unabhängig von einem (nach HERMES geführten kantonalen) IT-Projekt bei allen Datenbearbeitungen durch (kantonale und gemeindliche) Organe.

Daneben betreibt das AIO ein Cloud Competence Center (kurz CCC). Dieses dient innerhalb der kantonalen Verwaltung als Anlaufstelle, wenn ein Amt oder eine Direktion die Einführung oder auch die Migration einer Fachanwendungen in die Cloud beabsichtigt. Als Single Point of Contact (SPoC) bietet das CCC standardisierte Beratungsleistungen im Bereich der Prozesseinhaltung der vom Amt oder von der Direktion zu liefernden Leistungen. Das CCC stellt eine Projektumgebung zur Verfügung, um die erforderlichen Dokumente zentral zu sammeln und um die Planung und Koordination der nächsten Prozessschritte zu unterstützen.

Antrag

Kenntnisnahme.

Zug, 1. Februar 2022

Mit vorzüglicher Hochachtung
Regierungsrat des Kantons Zug

Der Landammann: Martin Pfister

Die stv. Landschreiberin: Renée Spillmann Siegwart

Beilagen:
1. Informatikstrategie Kanton Zug 2018–2022
2. Zertifikat ISO 27001 AIO

90/mb