Interpellation von Philip C. Brunner, Gregor Bruhin, Alex Haslimann und Hans Jörg Villiger
betreffend IT-Sicherheit und Schutz sensibler Registerdaten beim Amt für Informatik und Organisation (AIO) – Lehren aus dem Vorfall in Liechtenstein
(Vorlage Nr. 4167.1 - 18708)

Antwort des Regierungsrats
vom 8. September 2026

Sehr geehrter Herr Präsident
Sehr geehrte Damen und Herren

Philip C. Brunner, Gregor Bruhin, Alex Haslimann und Hans Jörg Villiger haben am 11. August 2026 eine Interpellation eingereicht, in welcher sie sich nach der IT-Sicherheit und dem Schutz sensibler Registerdaten beim AIO erkundigen. Der Kantonsrat hat den Vorstoss am 27. August 2026 zur Beantwortung an den Regierungsrat überwiesen. Die in der Interpellation gestellten Fragen beantwortet der Regierungsrat wie folgt:

1. Fragen zu den Zugriffskonzepten und der Authentifizierung

1.1. Welcher Authentifizierungsstandard, zum Beispiel Zwei- oder Mehrfaktor-Authentifi-zierung mit Hardware-Token, FIDO2/Passkeys oder ZUG-Login, kommt bei extern zugänglichen Portalen und Registern des Kantons Zug zum Einsatz?

1.2. Wie ist das Rollen- und Berechtigungskonzept für neu erstellte oder neu registrierte Benutzerkonten bei kantonalen Online-Diensten ausgestaltet?

1.3. Sind Massenabfragen von Grund auf technisch ausgeschlossen?

Für extern zugängliche Portale und Register des Kantons Zug werden Mehrfaktor-Authentisierung sowie zusätzliche, risikobasierte Zugriffsrichtlinien eingesetzt. Je nach Anwendung kommen unterschiedliche Identitäts- und Anmeldelösungen zum Einsatz, insbesondere AGOV (Behörden-Login der Schweiz) oder ZugLogin. Beide Systeme beinhalten eine Überprüfung der Identität der Nutzenden. Bei AGOV erfolgt diese mittels amtlichen Ausweises und, je nach erforderlichem Vertrauensniveau, zusätzlichen Verifikationsverfahren. Beim ZugLogin wird die Identität entweder persönlich bei einer Registrierungsstelle oder durch den Abgleich mit amtlichen Einwohner- und Steuerdaten geprüft. Der Kanton Zug überprüft und entwickelt seine Authentisierungs- und Identitätslösungen laufend entsprechend den technischen Möglichkeiten und aktuellen Sicherheitsanforderungen weiter.

Der Zugriff auf kantonale Online-Dienste erfolgt nach einem klar geregelten Rollen- und Berechtigungskonzept. Schützenswerte Daten sind nur für berechtigte Personen zugänglich. Die vergebenen Berechtigungen werden regelmässig überprüft. Für Bürgerkonten ist eine Identitätsprüfung erforderlich. Je nach Anwendung werden zusätzliche Angaben erhoben und verifiziert.

Ein vollständiger technischer Ausschluss von missbräuchlichen Zugriffen oder Massenabfragen kann nicht garantiert werden. Durch den Einsatz von Mehrfaktor-Authentisierung, Identitätsprüfungen, rollenbasierten Berechtigungen sowie einer umfassenden Protokollierung und Überwachung wird dieses Risiko jedoch erheblich reduziert. Der Kanton Zug verfügt insbesondere zum Schutz vor Massenabfragen über ein hohes Sicherheitsniveau und wirksame Kontrollmechanismen. Darüber hinaus werden die bestehenden Schutzmassnahmen kontinuierlich weiterentwickelt, insbesondere durch den Ausbau der automatischen Erkennung ungewöhnlicher Registrierungs- und Zugriffsmuster sowie die verstärkte Überwachung von Anomalien bei Registrierungen und Anmeldungen, um potenzielle Missbrauchsversuche frühzeitig zu erkennen und geeignete Gegenmassnahmen einzuleiten.

2. Fragen zu den technischen Schutzmechanismen und der Bot-Abwehr

2.1. Welche konkreten Schutzmassnahmen (z. B. Rate Limiting, Captchas, API-Gateway-Drosselung) verhindern im Kanton Zug das automatisierte Auslesen (Scraping/Massen-download) von Datenbeständen mittels Skripten oder Werkzeugen?

2.2. Werden Zugriffe auf sensible Registerdaten in Echtzeit durch ein SIEM-System (Security Information and Event Management) überwacht, und existieren automatische Mechanismen (z. B. KI- oder regelbasierte Anomalie-Erkennung), die auffällige Konten bei ungewöhnlich hohen Suchanfragen sofort sperren und das Incident-Response-Team alarmieren?

Zum Schutz vor dem automatisierten Auslesen von Datenbeständen setzt der Kanton Zug verschiedene technische und organisatorische Sicherheitsmassnahmen ein. Dazu gehören erweiterte Zugriffsregeln, Firewall-Schutz, Netzwerksegmentierung, Endpunktschutz sowie die Protokollierung und Überwachung von Zugriffen. Bei den meisten öffentlich zugänglichen Anwendungen werden zusätzlich Invisible Completely Automated Public Turing test to tell Computers and Humans Apart (unsichtbare CAPTCHA) sowie weitere Schutzmechanismen gegen automatisierte Zugriffe und DDoS-Angriffe (Distributed Denial of Service) eingesetzt. Diese Massnahmen erschweren den Einsatz von Skripten oder automatisierten Werkzeugen für Massenabfragen und tragen dazu bei, missbräuchliche Aktivitäten frühzeitig zu erkennen und einzudämmen.

Sicherheitsrelevante Ereignisse werden durch das Security Operations Center (SOC) rund um die Uhr überwacht. Dabei kommen unter anderem verhaltensbasierte Erkennungsverfahren und Anomalie-Analysen zum Einsatz, um verdächtige Aktivitäten frühzeitig zu identifizieren. Bei Bedarf können umgehend Gegenmassnahmen eingeleitet werden, beispielsweise die Blockierung verdächtiger Zugriffe oder die Isolation betroffener Systeme und Geräte.

Die Überwachung und Analyse von Benutzerverhalten und Zugriffsmustern wird kontinuierlich weiterentwickelt. Dabei werden auch neue Bedrohungen berücksichtigt, die sich aus dem Einsatz künstlicher Intelligenz (KI) ergeben können. Der Kanton Zug überprüft seine bestehenden Sicherheitsmassnahmen gezielt im Hinblick auf KI-gestützte Angriffsformen und setzt dort, wo erforderlich, zusätzliche Schutz- und Überwachungsmassnahmen um. Ziel ist es, ungewöhnliche Zugriffsmuster, automatisierte Massenabfragen und andere missbräuchliche Aktivitäten noch früher zu erkennen und wirksam zu unterbinden.

3. Fragen zum Zero-Trust-Ansatz und externen Audits

3.1. Inwieweit verfolgen das AIO und die externen IT-Dienstleister des Kantons Zug einen konsequenten «Zero-Trust-Ansatz» bei der Architektur von E-Government-Portalen?

3.2. Wann wurden die extern erreichbaren Schnittstellen und Registerlösungen des Kantons Zug letztmals durch unabhängige Dritte einem Penetrationstest beziehungsweise IT-Sicherheitsaudit unterzogen?

Der Kanton Zug verfolgt bei seinen E-Government-Portalen und digitalen Dienstleistungen einen Sicherheitsansatz, der wesentliche Elemente des Zero-Trust-Prinzips umfasst. Zugriffe werden konsequent überprüft, Berechtigungen nach dem Need-to-know-Prinzip und rollenbasiert vergeben, externe Zugriffe durch Mehrfaktor-Authentisierung geschützt sowie Netzwerke und Systeme segmentiert. Zugriffe von Lieferanten erfolgen ausschliesslich über definierte und geschützte Verbindungen.

Die Sicherheitsmassnahmen werden laufend überprüft und an aktuelle Bedrohungslagen angepasst. Dabei berücksichtigt der Kanton Zug sowohl Erkenntnisse aus Sicherheitsvorfällen anderer Verwaltungen und Organisationen als auch Informationen von Fachstellen und Sicherheitsnetzwerken wie dem Nationalen Zentrum für Cybersicherheit (NCSC) und der Cyber Security Community Group Schweiz (CSCG). Werden neue Risiken oder Angriffsmethoden bekannt, wird das bestehende Sicherheitsdispositiv überprüft und bei Bedarf mit geeigneten organisatorischen und technischen Massnahmen verstärkt.

Die Informationssicherheit des Kantons Zug wird regelmässig durch unabhängige externe Stellen überprüft. Im Rahmen des ISO-27001:2022-Überwachungsaudits durch das Swiss Safety Center wurden keine Abweichungen oder Nichtkonformitäten festgestellt. Ergänzend werden die IT-Infrastruktur und Anwendungen mittels einer Vulnerability-Scanning-Lösung kontinuierlich sowohl aus interner als auch aus externer Perspektive auf bekannte Schwachstellen überprüft, damit potenzielle Sicherheitslücken frühzeitig erkannt und zeitnah behoben werden können.

Darüber hinaus führt der Kanton Zug risikobasiert weitergehende technische Sicherheitsprüfungen durch, um die Widerstandsfähigkeit seiner Systeme und Anwendungen laufend zu überprüfen und kontinuierlich zu verbessern.

4. Fragen zum Vorfallmanagement und Verantwortlichkeiten

4.1. Wie ist die Überwachung kritischer IT-Infrastrukturen zeitlich geregelt (24/7 SOC/Incident Response)?

4.2. Welche vertraglichen und technischen Vorgaben macht das AIO externen Software- und Hosting-Anbietern bezüglich der Einhaltung staatlicher Sicherheitsstandards?

Die Überwachung sicherheitsrelevanter Ereignisse erfolgt beim Kanton Zug rund um die Uhr. Ausserhalb der regulären Betriebszeiten, insbesondere nachts sowie an Wochenenden und Feiertagen, wird diese durch spezialisierte externe Partner sichergestellt. Für die Behandlung sicherheitskritischer Vorfälle bestehen definierte Eskalations- und Pikettprozesse. Bei schwerwiegenden Ereignissen können zusätzlich spezialisierte externe Fachkräfte für die Analyse, Eindämmung und Bewältigung von Cyberangriffen beigezogen werden. Dadurch ist gewährleistet, dass auf Sicherheitsvorfälle rasch und angemessen reagiert werden kann.

An externe Software- und Hosting-Anbietende stellt das AIO sowohl technische als auch organisatorische Sicherheitsanforderungen. Dazu gehören unter anderem die Absicherung von Lieferantenzugriffen über geschützte Verbindungen, der Einsatz von Mehrfaktor-Authentisierung sowie die Einhaltung von Vorgaben zur Informationssicherheit und zum Datenschutz. Risiken im Zusammenhang mit Lieferanten und deren Dienstleistungen werden regelmässig bewertet und überwacht.

Bei Ausschreibungen und Beschaffungen orientiert sich der Kanton Zug an den Vorgabedokumenten, Empfehlungen und Rahmenverträgen der Digitalen Verwaltung Schweiz (DVS). Diese bilden die Grundlage für einheitliche Sicherheits-, Datenschutz- und Qualitätsanforderungen an externe Leistungserbringende. Zudem werden die Sicherheitsanforderungen laufend überprüft und an neue technische, regulatorische und sicherheitsrelevante Entwicklungen angepasst, damit die eingesetzten Lösungen den Anforderungen einer modernen und sicheren digitalen Verwaltung entsprechen.

5. Antrag

Kenntnisnahme.

Zug, 8. September 2026

Mit vorzüglicher Hochachtung
Regierungsrat des Kantons Zug

Der Landammann: Andreas Hostettler

Der Landschreiber: Tobias Moser