Philip C. Brunner, Kantonsrat, Zug
Gregor Bruhin, Kantonsrat, Zug
Alex Haslimann, Kantonsrat, Risch
Hans Jörg Villiger, Kantonsrat, Cham

Vorlage Nr. 4167.1
Laufnummer 18708
Eingang 11. August 2026

Zug, 11.8.2026

Interpellation betreffend IT-Sicherheit und Schutz sensibler Registerdaten beim Amt für Informatik und Organisation (AIO) – Lehren aus dem Vorfall in Liechtenstein

Am 7. August 2026 wurde ein gravierender Sicherheitsvorfall beim Register der wirtschaftlich berechtigten Personen (VwbP) im Fürstentum Liechtenstein bekannt. Durch eklatante Lücken bei der Berechtigungsvergabe, fehlendes Rate-Limiting sowie unzureichende Anomalie-Erkennung (SIEM/Monitoring) konnten unbefugte Dritte in kurzer Zeit zehntausende hochsensible Datensätze automatisiert abgreifen.

Der Kanton Zug verwaltet über seine Amtsstellen und zentral über das **Amt für Informatik und Organisation (AIO)** ebenfalls eine Vielzahl an hochsensiblen Datenbeständen (u.a. Steuerdaten, Handelsregisterdaten, Einwohner- und Personendatenbanken usw.). Ein vergleichbarer Datenabfluss würde für den Wirtschafts- und Wohnstandort Zug einen immensen Reputations- und Vertrauensschaden bedeuten. Vor diesem Hintergrund wird der Regierungsrat um die Beantwortung folgender Fragen gebeten:

1. Fragen zu den Zugriffskonzepte und der Authentifizierung

Welcher Authentifizierungsstandard (z. B. Zwei-/Mehrfaktor-Authentifizierung mit Hardware-Token, FIDO2/Passkeys, ZUG-Login) kommt bei extern zugänglichen Portalen und Registern des Kantons Zug zum Einsatz?

Wie ist das Rollen- und Berechtigungskonzept für neu erstellte oder neu registrierte Benutzerkonten bei kantonalen Online-Diensten ausgestaltet? Sind Massenabfragen von Grund auf technisch ausgeschlossen?

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

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?

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?

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

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

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

4. Zum Vorfallmanagement und Verantwortlichkeiten

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

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

Wir bedanken uns beim Regierungsrat für die Beantwortung unserer Fragen und weiteren Informationen zur Thematik der IT-Sicherheit und verbleiben - mit freundlichen Grüssen

Die Interpellanten: Philip C. Brunner, Kantonsrat, Zug
Gregor Bruhin, Kantonsrat, Zug
Alex Haslimann, Kantonsrat, Risch
Hans Jörg Villiger, Kantonsrat, Cham