Adriano Prandi
Belmitestrasse 1
6460 Altdorf

Interpellation

„Datensicherheit in der Kantonalen Verwaltung"

Cyberspionage ist Realität. In den vergangenen MELANI-Halbjahresberichten wurde mehrmals über verschiedene Fälle berichtet. Auch der Jahresbericht des Nachrichtendienstes des Bundes (NDB) befasst sich mit dieser Thematik. Dabei ist Prävention eine äussert wichtige Komponente im Kampf gegen Cyber-Spionage. Hierbei ist der erste und wichtigste Schritt die Erkenntnis, dass es sich um eine reale und nicht um eine hypothetische Gefahr handelt.

Öffentliche Verwaltungen, Banken, Industriebetriebe, Soziale Medien usw. waren und sind immer wieder das Ziel von professionellen kriminellen Datendieben. Das Ziel ist es, an Passwörter und Informationen zu gelangen. Diverse Beispiele im In- und Ausland haben gezeigt, dass der Schutz nicht so einfach ist.

Die Angriffe sind vielfältig, wie zum Beispiel ein Angriff auf Computer-Systeme mit dem erklärten Ziel, deren Verfügbarkeit zu stören (DDoS Distributed Denial of Service = Verweigerung des Dienstes). Ein gravierendes Beispiel könnte die Serverinfrastruktur eines Spitals sein.
Oder Verschlüsselungstrojaner (auch „Erpressungstrojaner" genannt), die zur unfreiwilligen Verschlüsselung der Daten führen. Ein Zugriff auf die Daten der Kantonalen Verwaltung wäre dann nicht mehr möglich und würde erst wieder frei gegeben, wenn eine erpresste Summe bezahlt wird.

Der Austausch von Daten auf elektronischem Weg wird weiter zunehmen und es ist deshalb wichtig, dass die Kantonale Verwaltung seine Daten gut schützt. Dies muss zentral an einem Ort erfolgen und von höchstmöglicher Kompetenz sein.

Antrag

Gestützt auf Art. 127 ff. der Geschäftsordnung des Urner Landrats wird der Regierungsrat ersucht, die folgenden Fragen zu beantworten:

1. Wie schützt sich die Kantonale Verwaltung vor Angriffen aus dem Netz?

2. Wie wird sichergestellt, dass die IT-Sicherheit ein höchstmögliches Niveau und Qualität hat und auch laufend aktualisiert wird?

3. Wurden in der Vergangenheit spezialisierte Firmen beauftragt, die Sicherheit zu testen, in dem man sie versuchen liess, ins System einzudringen?

4. Wurde in Erwägung gezogen, für das WLAN- und Extranet Login ein zweistufiges Authentisierungsverfahren mit PIN-Code (per SMS) einzuführen?

Dem Regierungsrat wird im Voraus für die Beantwortung der Fragen gedankt.

Altdorf, 2. November 2016

Erstunterzeichner/In
Adriano Prandi

.....
Unterschrift

Zweitunterzeichner/In
Marco Roeleven

.....
Unterschrift