

Anfrage Forster Eva und Mit. über die Cyber- und Informationssicherheit im Kanton Luzern

eröffnet am 24. März 2025

Die fortschreitende Digitalisierung und Vernetzung der Verwaltung, der Gemeinden und öffentlicher Institutionen führen zu einer zunehmenden Bedrohung durch Cybervorfälle.

In den Antworten auf die Anfragen A 6 von Rahel Estermann über die Cybersicherheit der öffentlichen Verwaltung und der Infrastruktur im Kanton Luzern sowie A 20 von Simon Howald über das Abwehren von Cyberattacken in der kantonalen Verwaltung durch neue Technologien wird ausgeführt, dass der Kanton Luzern internationale Sicherheitsstandards wie ISO/IEC 27001 und ISO/IEC 27002 befolgt, um Cybervorfälle bestmöglich zu verhindern. Diese Standards betonen die Notwendigkeit präventiver Massnahmen, insbesondere durch proaktives Risikomanagement, effektive Schulungen und klar definierte Meldeprozesse für Schwachstellen. Der Bund hat mit der Einführung des Informationssicherheitsgesetzes (ISG) und der Informationsverordnung (ISV) per 1. Januar 2024 eine einheitliche Grundlage für die Sicherheit in der Bundesverwaltung geschaffen und verbindliche Mindeststandards definiert.

In diesem Zusammenhang stellen sich folgende Fragen:

1. In der Verwaltung und in öffentlichen Institutionen können Schwachstellen in der IT-Sicherheit auftreten, welche von Fachpersonen in der Bevölkerung und ethischen Hackern entdeckt werden. Gibt es Bestrebungen, eine zentrale, niederschwellige und öffentliche Meldestelle (z. B. per Onlineformular) für Sicherheitslücken in der kantonalen Verwaltung und öffentlichen Institutionen zu erstellen? Falls nein, wie sollen entdeckte Schwachstellen und Sicherheitsrisiken gemeldet werden?
2. Die kantonale Verordnung über die Informatiksicherheit und die Nutzung von Informatikmitteln wurde per 1. Januar 2025 angepasst, wobei primär die Datenkategorisierung präzisiert wurde. Wieso wurde in Artikel 6 zur Schulungs-, Informations- und Sensibilisierungspflicht keine Konkretisierung analog zu Artikel 10 der ISV vorgenommen? Werden die bestehenden Schulungsmassnahmen bereits nach den Grundsätzen von ISO/IEC 27001 und ISO/IEC 27002 durchgeführt, insbesondere in Bezug auf regelmässige Schulungen, dokumentierte Teilnahmen und eine gezielte Sensibilisierung für aktuelle Bedrohungsszenarien? Falls nein, sind entsprechende Anpassungen geplant, um die Wirksamkeit der Präventionsmassnahmen sicherzustellen?
3. Gemäss der Antwort auf die Anfrage A 20 befindet sich ein Informationssicherheitsmanagementsystem (ISMS) in Umsetzung. Ist eine externe Überprüfung geplant, um die Wirksamkeit und Konformität sicherzustellen?
4. Gemäss den Statistiken des Nationalen Cybersecurity Center (NCSC) und anderer Quellen bleibt eine Vielzahl an Cyberdelikten unentdeckt oder wird nicht gemeldet. Gibt es Zahlen wie viele Cybervorfälle in den letzten fünf Jahren von der Luzerner Bevölkerung gemeldet

wurden? In wie vielen Fällen kam es zu einer Anzeige? In wie vielen Fällen konnten die Täter ermittelt werden? In wie vielen dieser Fälle führte es zu einer Verurteilung?

Forster Eva

Arnold Sarah, Erni Roger, Tanner Beat, Scherer Heidi, Amrein Ruedi, Räber Franz, Koller-Felder Nadine, Gut-Rogger Ramona, Boos-Braun Sibylle, Dubach Georg, Hauser Patrick, Bärtschi Andreas, Theiler Jacqueline, Hunkeler Damian, Cozzio Mario