KANTON
LUZERN

Regierungsrat

Luzern, 23. September 2025

ANTWORT AUF ANFRAGE A 395

Nummer:	A 395
Protokoll-Nr.:	1037
Eröffnet:	24.03.2025 / Finanzdepartement

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

Zu Frage 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?

In einer zunehmend digitalisierten Verwaltung gewinnen proaktive und transparente Prozesse zur Meldung und Bearbeitung von IT-Schwachstellen an Bedeutung. Immer häufiger identifizieren Fachpersonen aus der Zivilgesellschaft – sogenannte Ethical Hacker oder Security Researchers – Sicherheitslücken in öffentlich zugänglichen IT-Systemen. Ein vertrauensvoller, strukturierter und nachvollziehbarer Umgang mit solchen Meldungen ist ein wesentlicher Beitrag zur Stärkung der Cybersicherheit und zum Schutz sensibler Daten.

Der Kanton Luzern stellt gemäss der Empfehlung des Bundesamtes für Cybersicherheit (Bundesamt für Cybersicherheit BACS) die Kontaktinformationen für Sicherheitsforscherinnen und -forscher in einer strukturierten Textdatei auf der Website zur Verfügung. Diese Datei ist unter https://www.lu.ch/security.txt zu finden.

Der Kanton Luzern beziehungsweise die zuständige Dienststelle Informatik stellt derzeit zudem nachfolgende niederschwellige allgemeine Kanäle zur Verfügung, um mit dem Kanton zu allgemeinen IT-Fragen oder Sicherheitsfragen in Kontakt zu treten:

- Kontaktformular: Kontaktformular Dienststelle Informatik
- Service Desk: Tel 041 228 6999
- Zentrale Dienststelle Informatik: 041 228 5615
- Kontaktformular der Lupol: Luzerner Polizei-Kontaktformular Hinweise

Ein dezidiertes Formular, über das Fachpersonen, Sicherheitsforscher/innen und ethische Hacker Schwachstellen strukturiert melden, existiert im Kanton heute jedoch noch nicht.

Um diesen Personengruppen den Zugang und die strukturierte Meldung von Schwachstellen zu erleichtern, prüft der Kanton Luzern zurzeit, ob ein solches dezidiertes niederschwelliges Kontaktformular nach Vorbild des Bundesamtes für Cybersicherheit erstellt werden soll und auf dem Serviceportal leicht zugänglich zur Verfügung gestellt werden könnte. Alternativ dazu wird auch geprüft, ob die oben aufgelisteten bereits existierenden Formulare entsprechend ergänzt werden können.

Zu Frage 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?

Die am 1. Januar 2025 in Kraft getretene Revision der kantonalen Verordnung über die Informatiksicherheit und die Nutzung von Informatikmitteln (ISV; SRL Nr. 26b) hatte ausschliesslich zum Ziel, die Datenkategorisierung im Sinne einer klareren Definition und Einstufung von Informationen zu präzisieren. Diese Fokussierung war notwendig, um die Grundlage für ein risikobasiertes Sicherheitsmanagement im Sinne der gängigen Standards (z. B. ISO/IEC 27001) zu stärken und die Rahmenbedingungen für das Einführungsprojekt Datenklassifizierung im Zusammenhang mit dem Vorhaben M365 zu präzisieren.

Die bestehenden Schulungsmassnahmen orientieren sich jedoch bereits heute in weiten Teilen an den Grundsätzen der ISO/IEC 27001 und insbesondere an den konkreten Leitlinien der ISO/IEC 27002 (Kap. 6.3: Awareness, education and training). Dies umfasst:

- regelmässige Schulungen für Mitarbeitende mit IT-Zugang, angepasst an deren Rolle und Risiken,
- dokumentierte Teilnahme mittels Schulungsplattform,
- Sensibilisierungskampagnen zu aktuellen Bedrohungsszenarien (z. B. Phishing, Social Engineering), etwa durch E-Learnings, Info-Mails oder gezielte Tests.

Die Verantwortung für die Umsetzung der Schulungsmassnahmen liegt weiterhin beim zuständigen Verwaltungsorgan gemäss § 22 Gesetz über die Organisation von Regierung und Verwaltung (Organisationsgesetz, OG, SRL Nr. 20), die zur Verfügungstellung der Inhalte wird jedoch zentral durch das Programm ISMS verantwortet.

Es ist jedoch denkbar, dass im Zuge der Weiterentwicklung des ISMS in der entsprechenden Verordnung SRL Nr. 26b weitere Anpassungen notwendig und sinnvoll sein werden.

Zu Frage 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?

Ziel eines ISMS ist es, durch strukturierte Prozesse, Verantwortlichkeiten und Richtlinien die Informationssicherheit innerhalb der kantonalen Verwaltung systematisch zu planen, umzusetzen, zu überwachen und kontinuierlich zu verbessern. Die Einführung eines ISMS erfolgt in Anlehnung an etablierte Normen – insbesondere ISO/IEC 27001.

Die externe Überprüfung (Audit) eines ISMS ist zentraler Bestandteil zur Sicherstellung der Wirksamkeit umgesetzter Sicherheitsmassnahmen, Konformität mit Normen und gesetzlicher Vorgaben sowie der Objektivität in der Bewertung der Risiken und Kontrollen. Audits durch eine unabhängige, externe Stelle sind dabei als integraler Bestandteil des ISMS ebenso vorgesehen wie Selbstbeurteilungen gemäss dem PDCA-Zyklus (Plan-Do-Check-Act).

Die Einführung des ISMS erfolgt schrittweise und risikobasiert, ausgerichtet an den spezifischen Anforderungen der verschiedenen Verwaltungseinheiten. Dabei wird eine grundsätzliche Zertifizierbarkeit nach ISO/IEC 27001 angestrebt.

Zu Frage 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?

Gemäss Statistik der Luzerner Polizei (2024 vgl. BFS-Polizeiliche Kriminalstatistik 2024 des Kantons Luzern, S. 51ff.; Vorjahre vgl. Archiv Statistiken Luzerner Polizei) wurden in den letzten fünf Jahren 8'680 Straftaten gemeldet, wobei die durchschnittliche Aufklärungsrate bei 22,7 Prozent liegt. Über die Verurteilungsrate liegen uns keine Statistiken vor.

Digitale Kriminalität – Straftaten	2020	2021	2022	2023	2024	Total
Straftaten* (Anzahl)	1'148	1'159	1'656	2'141	2'576	8'680
Aufklärung in %	58,0 %	21,8 %	17,8 %	20,5 %	12,2 %	22,7 %
* Phishing, Hacking, Malware, Cyberbetrug, Cyber-Sexualdelikte, Cyber-Rufschädigung, weitere						