Kleine Anfrage

Cyber-Resilienz der Landesverwaltung und Konsequenzen aus dem Hacker-Angriff

Frage von	Landtagsabgeordneter Erich Hasler
Antwort von	Regierungschefin Brigitte Haas

Frage vom 02. September 2026

Beim gezielten Angriff auf das Verzeichnis wirtschaftlich berechtigter Personen wurden in der Nacht auf den 30. Juli 2026 Datenkopien von rund 31'000 Rechtsträgern abgegriffen. Als potenzielles Einfallstor wurde das über das offene Internet erreichbare Erfassungsportal identifiziert. Zugriffsberechtigt auf das Verzeichnis selbst sind ohnehin nur klar definierte Stellen – Behörden, Banken und Sorgfaltspflichtige. Der Vorfall wirft damit über den Einzelfall hinaus die Frage auf, wie exponiert die Fachanwendungen der Landesverwaltung insgesamt sind, nach welchen Kriterien dies entschieden wird und welche Konsequenzen aus dem Vorfall gezogen werden.

Dazu meine Fragen:

* Bei wie vielen Fachanwendungen der Landesverwaltung, die besonders schützenswerte Personendaten führen, ist der Zugang für externe Nutzer heute grundsätzlich aus dem offenen Internet möglich, und bei wie vielen ist er auf einen technisch abgeschlossenen Kreis vorab authentifizierter Teilnehmer beschränkt?
* Nach welchen Kriterien und durch welche Stelle wird entschieden, ob eine Fachanwendung mit definiertem, geschlossenem Nutzerkreis öffentlich im Internet publiziert oder über beschränkte Zugangswege angebunden wird, beziehungsweise existiert für diesen Entscheid eine verbindliche Vorgabe?
* Wie viele in Liechtenstein ansässige IT- und Telekommunikationsunternehmen haben in den Jahren 2024 bis 2026 technische Lösungsansätze und Sicherheitskonzepte an das Amt für Informatik herantragen, wer hat diese beurteilt und wie viele dieser Vorschläge wurden weiterverfolgt?
* Werden Datensouveränität, inländische Betriebsführung und die Nachvollziehbarkeit der Datenwege bei Beschaffungen des Amts für Informatik als gewichtete Zuschlagskriterien berücksichtigt, und wenn ja, mit welchem Gewicht?

* Welche konkreten, mit Zeitplan und Kosten hinterlegten Massnahmen zur Reduktion der Angriffsfläche leitet die Regierung aus dem Hacker-Angriff ab, insbesondere hinsichtlich der Verringerung öffentlich exponierter Zugänge und der Reduktion der Abhängigkeit von ausländischen Anbietern grosser Cloud-Infrastrukturen?

Antwort vom 04. September 2026

zu Frage 1:

Eine zentrale Statistik über die Anzahl der Fachanwendungen in den jeweiligen Kategorien wird nicht geführt. Unabhängig vom gewählten Zugangsmodell werden die Anwendungen anhand ihres Schutzbedarfs beurteilt und durch technische und organisatorische Sicherheitsmassnahmen geschützt. Dabei kommen je nach Anwendungsfall unterschiedliche Zugangsmodelle zum Einsatz. Anwendungen für einen definierten Benutzerkreis, wie beispielsweise Register- oder Meldeportale für Unternehmen und deren Vertretungen, können einen Zugang über das Internet erfordern, werden jedoch durch Authentisierungs- und Sicherheitsmechanismen geschützt. Demgegenüber bestehen Anwendungen, die ausschliesslich für einen technisch abgegrenzten Kreis berechtigter Teilnehmer zugänglich sind, beispielsweise über dedizierte Netzanbindungen, Zertifikate oder andere geschlossene Zugangslösungen. Dabei werden auch die Vorgaben der DSGVO und die geltenden nationalen datenschutzrechtlichen Bestimmungen vollumfänglich eingehalten.

zu Frage 2:

Die Anbindungsform wird im Rahmen der Projekt-, der Architektur- und der Sicherheitsbeurteilung festgelegt. Massgeblich sind insbesondere der Schutzbedarf der verarbeiteten Daten, die vorgesehenen Nutzergruppen, die gesetzlichen Zugriffsrechte, die Benutzerfreundlichkeit, die Anforderungen an Datenschutz, Informationssicherheit, Verfügbarkeit und Nachvollziehbarkeit sowie die betrieblichen Rahmenbedingungen. In die Beurteilung werden die fachlich zuständige Amtsstelle, das Amt für Informatik und bei Bedarf weitere spezialisierte Stellen einbezogen.

zu Frage 3:

Das Amt für Informatik steht im regelmässigen Austausch mit Marktteilnehmern und prüft im Rahmen von Beschaffungen, Projekten und Technologieevaluierungen fortlaufend verschiedene technische Lösungsansätze und Sicherheitskonzepte. Eine statistische Erfassung nach Herkunft der Unternehmen wird dabei nicht geführt.

zu Frage 4:

Die Zuschlags- und Eignungskriterien werden im Rahmen von Auftragsvergabeverfahren jeweils gemeinsam mit dem zuständigen Fachbereich beziehungsweise der zuständigen Amtsstelle anhand des konkreten Beschaffungsgegenstands, des Schutzbedarfs der Daten, der fachlichen und betrieblichen Anforderungen sowie im Einklang mit den rechtlichen Vorgaben festgelegt. Die Kriterien können somit je nach Projekt unterschiedlich ausgestaltet sein.

zu Frage 5:

Aus dem Cyberangriff wurden verschiedene zusätzliche technische, organisatorische und sicherheitsbezogene Massnahmen abgeleitet. Hinsichtlich der Nutzung externer Cloud-Dienste verfolgt die Regierung weiterhin den Grundsatz, für jede Lösung eine risikobasierte Einzelfallbeurteilung vorzunehmen. Dabei werden insbesondere Anforderungen an Informationssicherheit, Datenschutz, Verfügbarkeit, digitale Souveränität, Wirtschaftlichkeit sowie gesetzliche Vorgaben berücksichtigt. Direkt aus dem Angriff abgeleitete Massnahmen waren unter anderem die vorsorgliche Offlinenahme von kritischen Systemen, zusätzliche Pen-Tests und die Einführung von zusätzlichen Sicherheitsmassnahmen wie die Vorschaltung des eID-Gates oder die Verstärkung der Webapplikation Firewall. Mögliche zukünftige Massnahmen werden aktuell analysiert und zeitnah umgesetzt.