Kleine Anfrage

Cyberangriffe auf Liechtenstein

Frage von	Landtagsabgeordneter Dietmar Hasler
Antwort von	Regierungschefin Brigitte Haas

Frage vom 07. Mai 2025

Die fortschreitende Digitalisierung durchdringt immer mehr Lebensbereiche und bietet immense Chancen für Effizienzsteigerung und Bürgerfreundlichkeit. Gleichzeitig birgt sie jedoch auch Risiken, insbesondere im Hinblick auf den Schutz persönlicher Daten und die Sicherheit digitaler Infrastrukturen der Landesverwaltung und Regierung. Angesichts der zunehmenden Cyberangriffe und der Sensibilität der Informationen ist es unerlässlich, dass unser Staat die Sicherheitsmassnahmen kontinuierlich überprüft und anpasst. Vor diesem Hintergrund sind Informationen über die aktuellen Strategien und Massnahmen der Regierung im Bereich der Cybersicherheit von öffentlichem Interesse.

* Welche konkreten Massnahmen hat die Regierung in den letzten zwei Jahren ergriffen, um die Cybersicherheit der staatlichen Infrastruktur und der digitalen Dienste für Bürgerinnen und Bürger zu erhöhen?
* Wie bewertet die Regierung die aktuelle Bedrohungslage im Bereich der Cybersicherheit für Liechtenstein und welche spezifischen Risikobereiche sieht sie als besonders kritisch an?
* Inwieweit werden bei der Entwicklung und Implementierung neuer digitaler Dienste und Anwendungen von staatlicher Seite Aspekte der Datensicherheit und des Datenschutzes von Beginn an berücksichtigt?
* Welche Mechanismen und Ressourcen stehen Liechtenstein zur Verfügung, um im Falle eines erfolgreichen Cyberangriffs schnell und effektiv zu reagieren und die Auswirkungen minimieren zu können?
* Werden regelmässig Informationskampagnen oder Schulungsangebote für Mitarbeiterinnen und Mitarbeiter der Landesverwaltung durchgeführt, um ihr Bewusstsein für Cybersicherheit zu stärken und sie im sicheren Umgang mit digitalen Technologien präventiv zu schulen?

Antwort vom 09. Mai 2025

zu Frage 1:

Seit dem Jahr 2021 wurde der Personalbestand der innerhalb des Amts für Informatik auf strategischer und taktischer Ebene mit dem Thema Cybersicherheit betrauten Personen von einem Vollzeitäquivalent auf 2 ½ Vollzeitäquivalente ausgebaut. Zusätzlich wurde im Bereich Datenschutz eine Vollzeitäquivalentstelle geschaffen. Neben dieser Erhöhung der personellen Ressourcen wurden durch eine Reorganisation innerhalb des Amts für Informatik die beiden Abteilungen Network & Security Services sowie Cloud Services geschaffen, welche sich beide intensiv mit dem Thema Cybersicherheit auf operativer Ebene auseinandersetzen.

Details zu den effektiv ergriffenen und umgesetzten technischen wie organisatorischen Massnahmen werden weder durch die Stabsstelle Cyber-Sicherheit noch durch das Amt für Informatik kommentiert, da solche Informationen durch einen potenziellen Angreifer missbraucht werden könnten.

zu Frage 2:

Die gegenwärtige Bedrohungslage im Bereich der Cybersicherheit spiegelt das allgegenwärtige Mass an Aktivitäten und Bedrohungen im Internet wider. Es ist wichtig, dass sowohl Unternehmen als auch Privatpersonen wachsam bleiben und geeignete Sicherheitsmassnahmen ergreifen.

Zwischen Februar 2023 und Februar 2024 erarbeitete die Stabsstelle Cyber-Sicherheit eine Cyberrisikoanalyse. Es konnten zwölf Gefährdungen bzw. Cyberbedrohungen identifiziert werden, die als wesentlich für Liechtenstein eingeschätzt werden. Diejenigen mit den grössten Risiken sind: Ransomware, Lieferketten-Angriffe, Cyber-Spionage, Angriffe auf die kritische Infrastruktur und technische Störung oder Ausfall. Die vollständige Liste der Gefährdungen sowie weitere Ausführungen dazu finden sich in der öffentlich verfügbaren Gefährdungs- und Risikoanalyse Bevölkerungsschutz vom April 2024.

zu Frage 3:

Das Amt für Informatik arbeitet nach der Hermes-Projektmanagement-Methodik der Schweizerischen Bundesverwaltung. Hermes ist ein offener Standard zur Führung und Abwicklung von IT-Projekten. Dies gewährleistet einen „Security by Design“-Ansatz, da alle Projektphasen durch verbindliche Dokumente wie Schutzbedarfsanalyse, Informationssicherheits- und Datenschutzkonzept sowie Datenschutz-Folgenabschätzung abgesichert werden.

Die Einhaltung der Sicherheitsgrundlagen wird durch Sicherheitsaudits sichergestellt, welche durch das Amt für Informatik oder die Finanzkontrolle veranlasst werden. Die Sicherheitsgrundlagen werden kontinuierlich an die aktuellen Gegebenheiten angepasst und weiterentwickelt. Alle von aussen über das Internet zugänglichen Systeme werden regelmässig durch gezielte Penetrationstests auf Sicherheitsmängel überprüft.

zu Frage 4:

Zur Abwehr von Cyberattacken besteht eine Vielzahl von organisatorischen wie auch technischen Massnahmen. Diese Massnahmen betreffen sowohl den Schutz der gesamten Infrastruktur als auch den Schutz von einzelnen Systemen.

Details zu den ergriffenen und umgesetzten Massnahmen werden weder durch die Stabsstelle Cyber-Sicherheit noch durch das Amt für Informatik kommentiert, da solche Informationen durch einen potenziellen Angreifer missbraucht werden könnten.

Zu erwähnen ist, dass Informationssicherheit und Cybersicherheit dynamische Prozesse sind, und keine statischen Zustände. Da sich sowohl die verwalteten Systeme, der Stand der Technik, die Schwachstellen und Verwundbarkeiten als auch die Bedrohungslagen ständig ändern, muss sich die Informationssicherheit und die Cybersicherheit ständig diesen sich ändernden Gegebenheiten anpassen. Die Herausforderung besteht nun darin, mit den vorhandenen Ressourcen die aktuellen Sicherheitsthemen risikobasiert zu adressieren.

Abschliessend wird darauf hingewiesen, dass das Cyber-Sicherheitsgesetz für die kritische Infrastruktur eine Meldepflicht für erhebliche Sicherheitsvorfälle bzw. Cyberangriffe vorsieht. So hat beispielsweise das Amt für Informatik Sicherheitsvorfälle der Stabsstelle Cyber-Sicherheit unverzüglich zu melden. Das bei der Stabsstelle Cyber-Sicherheit eingerichtete Computer-Notfallteam – das sogenannte CSIRT - leistet in weiterer Folge im Rahmen seiner Möglichkeiten allgemeine oder technische Unterstützung bei der Reaktion auf einen Sicherheitsvorfall.

zu Frage 5:

Mitarbeitende der LLV nehmen beim Eintritt in die Organisation an einem Kurs über Informationssicherheit und einem Kurs über Datenschutz teil. Spezifische Informationen, wie z.B. die Bedrohung durch bestimmte Phishing-Angriffe, werden von der Abteilung für Informationssicherheit beim Amt für Informatik allen Mitarbeitenden zeitnah zur Verfügung gestellt. Darüber hinaus werden in der internen Mitarbeiterzeitschrift regelmässig aktuelle Themen der Informationssicherheit aufgegriffen.

Zusätzlich zu den oben genannten Massnahmen werden etliche vor Ort- wie auch Online-Schulungen angeboten. So umfasst das interne Schulungsprogramm die Themengebiete Cyber Security für Privathaushalte und Datenschutz. Innerhalb der LLV-Akademie stehen den Mitarbeitenden zusätzlich Online-Kurse wie beispielsweise Informationssicherheit, Fake News, Datenschutzgrundverordnung, Künstliche Intelligenz, digitale Kompetenzen, Aktenverwaltung, M365 und etliche mehr zur Verfügung.

Seit letztem Herbst arbeitet zudem die Arbeitsgruppe Security Awareness an einem mehrjährigen «Security Awareness Action Plan». Dieser Plan soll für alle LLV-Mitarbeitenden verpflichtend sein.