Kleine Anfrage

Schutz der IT in der Landesverwaltung und den Schulen

Frage von	Stv. Landtagsabgeordneter Thomas Hasler
Antwort von	Regierungschef Daniel Risch

Frage vom 10. April 2024

IT-Sicherheit ist nicht erst seit dem bei uns noch in schlechtester Erinnerung verbliebenen Angriff auf die Universität Liechtenstein ein grosses Thema. Liechtenstein hat 2023 aufgrund einer EWR-Richtlinie ein Cybersicherheitsgesetz erlassen. Jüngste Ereignisse in Europa stimmen bezüglich Cyberangriffen nicht zuversichtlich. So wurde Luxemburg kürzlich Opfer eines Cyberangriffs. Verschiedene IT-Systeme des Landes waren im März Ziel einer Attacke. Mehrere Webseiten waren zeitweise nicht verfügbar. Bei dem Angriff handelte es sich um einen DDOS-Angriff, also ein Angriff, der die Computerressourcen der Ziele überlastet. Ende März ist schliesslich auch in Frankreich ein jihadistischer Hacker an zahlreichen Schulen in die digitale Lernplattform eingedrungen und schickte Schülern in Frankreich Enthauptungsvideos und Bombendrohungen. Hierzu meine Fragen:

* Gab es solche Cyberattacken beziehungsweise versuchte Cyberattacken in den letzten Monaten auch auf die IT der liechtensteinischen Landesverwaltungen oder Schulen?
* Was hat die Regierung konkret gegen solche Cyberattacken auf die Landesverwaltung und die Schulen vorgekehrt?
* Werden regelmässige Tests dazu durchgeführt und wie sind die Ergebnisse?
* Wie ist der Umsetzungsstand beziehungsweise wie sind die Erfahrungen mit dem Cybersicherheitsgesetz vom 4. Mai 2023, das die kritische Infrastruktur schützen soll?

Antwort vom 12. April 2024

Zu Frage 1:

Cyberangriffe gehören in der heutigen Zeit leider zum Alltag. Hiervon sind nicht nur öffentliche Verwaltungen, sondern auch privatwirtschaftliche Unternehmen, Schulen und Universitäten sowie Privatpersonen betroffen. Die IT Systeme der Landesverwaltung und der Schulen sind ständig Cyber-Angriffen ausgesetzt. In Zuge der angespannten geopolitischen Lage wurde sowohl eine deutliche Zunahme der Anzahl Angriffe als auch eine Veränderung der Qualität der Angriffe festgestellt. So finden sich nicht nur generische Angriffsmuster, sondern auch Angriffsmuster, die gezielt auf Liechtenstein zielen.

Bisher waren wir weder mit massiven DDoS Attacken noch mit dem Spoofing von jihadistischen Inhalten konfrontiert.

Zu Frage 2:

Wie in der Vergangenheit bereits mehrfach bei der Beantwortung von Kleinen Anfragen ausgeführt, werden zur Abwehr solcher Cyberattacken eine Vielzahl von organisatorischen wie auch technischen Massnahmen ergriffen. Diese Massnahmen betreffen den Schutz der gesamten Infrastruktur als auch den Schutz einzelner Systeme.

Details zu den ergriffenen und umgesetzten Massnahmen gibt die Regierung keine an, da diese Ausführungen durch einen potentiellen 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 ändernden Gegebenheiten anpassen. Die Herausforderung besteht nun darin, mit den vorhandenen Ressourcen die aktuellen Sicherheitsthemen risikobasiert zu adressieren.

Zu Frage 3:

Audits und Penetrationstests werden durch das Amt für Informatik regelmässig in Auftrag gegeben. Diese werden durch eine unabhängige spezialisierte Firma nach einem international anerkannten Standard durchgeführt. Beispielsweise werden im Rahmen von Projekten Penetrationstests für sämtliche Systeme mit erhöhtem Schutzbedarf routinemässig durchgeführt. Weiters werden Schwachstellenscanner und andere Werkzeuge eingesetzt, die mögliche Angriffsvektoren und Schwachstellen toolbasiert erkennen. Daneben führt die Finanzkontrolle gemeinsam mit externen Revisionsgesellschaften regelmässige Audits von Informatik-Projekten durch. Neben Governance Themen stehen dabei auch technische Zweckmässigkeit und Informationssicherheit im Fokus.

Die durchgeführten Tests bescheinigen der LLV ein gutes, durchdachtes Sicherheitsdispositiv, welches die entsprechenden Gefahren mit organisatorischen wie auch technischen Massnahmen risikobasiert mitigiert. Dies wird auch regelmässig durch Audits von externen Behörden und Organisationen wie bspw. der Europäischen Kommission im Rahmen Schengen/Dublin, des Sicherheitsverbundes der Schweiz oder der OECD bestätigt. Obwohl diese Audits mehrheitlich die Sicherheitsmassnahmen spezifischer Systeme und/oder Umgebungen überprüfen, wird dabei der ganzheitliche Ansatz des internen Information Security Management Systems (ISMS) selbstverständlich in die Überprüfung miteinbezogen.

Zu Frage 4:

Das Cyber-Sicherheitsgesetz (CSG) trat am 1. Juli 2023 sowie die entsprechende Verordnung im September 2023 in Kraft. Die Verordnung definiert näher, welche Unternehmen in Liechtenstein als sogenannte Betreiber wesentlicher Dienste zu qualifizieren sind und welche Unternehmen in weiterer Folge geeignete und verhältnismässige technische und organisatorische Sicherheitsnassnahmen einzuhalten haben. Die Betreiber wesentlicher Dienste wurden durch die Stabsstelle Cyber-Sicherheit identifiziert und Ende 2023 fand bereits das erste Vernetzungstreffen statt. Die Stabsstelle steht im ständigen Kontakt mit den Betreibern. Gemeinsam mit der Universität Liechtenstein erarbeitete die Stabsstelle Cyber-Sicherheit eine Methodik zur Messung der Resilienz von Unternehmen. In einem ersten Schritt soll noch vor der Sommerpause die Resilienz, sprich die Widerstandsfähigkeit der kritischen Infrastruktur in Liechtenstein, wozu auch die LLV zählt, erhoben und bewertet werden.