Kleine Anfrage

Cybersicherheit in Liechtenstein

Frage von	Landtagsabgeordneter Günter Vogt
Antwort von	Regierungschef Daniel Risch

Frage vom 06. März 2024

Gemäss einem Artikel in einer Liechtensteiner Tageszeitung vom 6. Februar sorgte ein Cyberangriff für einen Ausfall bei der Lichtsignalanlage des Tunnels Gnalp-Steg für ausserordentliche Aufwendungen. Dieser Vorfall zeige, ich zitiere, "dass sich Liechtenstein beim Thema Cybersicherheit am Anfang befinde". Gemäss den Angaben der Herstellerfirma sorgte eine Schadsoftware auf dem Betreiberserver für diesen Ausfall. Gemäss Experten stand der Server schon seit längerer Zeit mit offenen Türen im Netz. Damit scheint dieses konkrete Problem erst einmal geklärt. Allerdings ist die grundsätzliche Gefahr von Hackerangriffen auf Server in Liechtenstein dadurch nicht gebannt.

Ich hatte schon in der Debatte über die Cybersicherheit sowie der ENISA Verordnung im letzten Jahr erwähnt, dass die IT-Resilienz Liechtensteins strukturell gestärkt werden muss. Erinnern Sie sich auch an den Hackerangriff auf die Universität Liechtensteins im Jahr 2021? Die Regierung hatte im September 2021 dazu ausgeführt, dass die Infrastruktur der LLV mit erprobten technischen Sicherheitsmechanismen gegen Angriffe geschützt werde. Ebenso würden die Prozesse laufend überwacht und die sich ändernden Entwicklungen der Informationstechnologie analysiert. Mit diesen Vorkehrungen könne das Risiko eines Angriffs minimiert werden. Dazu meine Fragen:

* Wie ist es möglich, dass trotz der Einführung von Sicherheitsmassnahmen ein Server der Liechtensteinischen Landesverwaltung mit offenen Ports im Netz steht?
* Beurteilt die Regierung den aktuell definierten Schutzbedarfs von systemrelevanter Infrastruktur im Blickwinkel des Sicherheitskonzepts sowie der getroffenen Massnahmen immer noch für ausreichend?
* Werden aktuell Audits und Penetrationstests zur Cybersicherheit in Liechtenstein durch unabhängige Firmen durchgeführt und falls nein, wieso nicht?
* Die Stabsstelle Cyber-Sicherheit sowie das Amt für Informatik ist zuständig für den Schutz der Infrastruktur der Landesverwaltung. Erachtet die Regierung im Kontext der erwähnten Sicherheitsvorfälle, welche auf eine hohe Cyberanfälligkeit und somit ein Risiko in Liechtenstein hinweisen, die vorhandenen Mittel, Ressourcen für genügend?

* Sieht die Regierung Verbesserungspotenzial in der Definition von Disaster Recovery und Business-Continuity-Plänen sowohl für Unternehmen und der staatlichen Organisation in Liechtenstein, und falls ja, wie gedenkt Sie, dieses Potential und mit welchen Massnahmen zu unterstützen?

Antwort vom 08. März 2024

Zu Frage 1:

Im konkreten Fall dieses Cyberangriffs auf die Lichtsignalanlage des Tunnels Gnalp-Steg handelte es sich beim betroffenen System nicht um einen klassischen Server in einem Rechenzentrum, sondern um einen PC mit offenem Fernwartungszugang, welcher autonom betrieben wurde und direkt über das Internet erreichbar war. Der Betrieb und die Wartung des Systems erfolgten durch die dafür verantwortliche Amtsstelle in Zusammenarbeit mit einem externen Dienstleister und nicht durch das Amt für Informatik.

Zu Frage 2:

Das vom Cyberangriff betroffene System wurde zwischenzeitlich neu installiert und in das Rechenzentrum des Amtes für Informatik gezügelt. Die direkte Erreichbarkeit des Systems über das Internet ist dadurch eingeschränkt. Dabei kommen nun auch dem Schutzbedarf entsprechende Schutzmassnahmen zur Anwendung.

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. Ebenso wurde kürzlich erstmals ein sogenanntes Bug-Bounty-Programm durchgeführt, um auch die nicht offensichtlichen oder automatisiert erkennbaren Schwachstellen und Verwundbarkeiten aufzudecken. 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.

Zu Frage 4:

Bei beiden erwähnten Sicherheitsvorfällen – Lichtsignalanlage des Tunnels Gnalp-Steg und Universität – waren keine vom Amt für Informatik betreuten Systeme betroffen. Aus diesem Grund kann nicht direkt darauf geschlossen werden, dass diese Vorfälle auf "eine hohe Cyberanfälligkeit und somit ein Risiko in Liechtenstein hinweisen". 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.

Die Stabsstelle Cyber-Sicherheit soll nach etwa zwei Jahren des organisatorischen und technischen Aufbaus zeitnah von einer Aufbauorganisation in den laufenden Betrieb überführt und die Handlungsfähigkeit auch nachhaltig auf einem angemessenen Maturitätsniveau gesichert werden. Dabei werden unabhängig der erwähnten Sicherheitsvorfälle die dafür notwendigen Mittel und Ressourcen evaluiert und gegebenenfalls auch angepasst.

Zu Frage 5:

Business Continuity Pläne sind an verschiedenen Stellen in der Landesverwaltung bereits umgesetzt oder in Umsetzung. Die Regierung wird überdies zeitnah die Überarbeitung der Nationalen Strategie für Liechtenstein zum Schutz vor Cyber-Risiken aus dem Jahr 2020 anstossen. Bei dieser Überarbeitung werden auch die Themen Disaster Recovery, Business Continuity sowie die Ereignisbewältigung im weitesten Sinn diskutiert werden.