Kleine Anfrage

# Cyberwehr-Anlaufstelle für Liechtenstein

| | |
|---|---|
| Frage von | Landtagsabgeordneter Günter Vogt |
| Antwort von | Regierungsrätin Dominique Hasler |

## Frage vom 05. Dezember 2018

Die Landesregierung in Baden-Württemberg initiierte im September 2017 eine Cyberwehr-Anlaufstelle, welche als Kontakt- und Beratungsstelle vor allem für kleine und mittlere Unternehmen sowie eine landesweite Koordinierungsstelle bei Hackerangriffen Hilfestellungen leisten sollte. Aber auch Privatpersonen sind immer wieder von solchen Angriffen betroffen. Dabei soll diese Cyberwehr eng mit Sicherheitsbehörden, Wirtschaft und Wissenschaft vernetzt werden. Auch Liechtenstein geht einen Weg zu einer digitalen Leitregion und dazu besteht eine Digitalisierungsstrategie der Regierung. Eine wichtige Voraussetzung dabei ist die Cybersicherheit vor Gefahren und Angriffen aus dem Netz. Diesen Angriffen müssen wir uns gezielt entgegenstellen, denn Cyberattacken verunsichern Bürgerinnen und Bürger und sie gefährden Geschäftsmodelle. Für jedes digitale Projekt ist die Daten- und Übertragungssicherheit eine notwendige Grundlage. Digitale Assistenzsysteme in der Pflege, das autonome Fahren oder beispielsweise Smart-Home-Anwendungen, das alles wird nur funktionieren, wenn es auch sicher ist. Deshalb sollte Liechtenstein im Bereich der Cybersicherheit Massnahmen ergreifen. Dazu meine Fragen:

1. Es besteht eine hohe Dunkelziffer bei Hackerangriffen. Laut Onlinebefragungen zur Lage der IT-Sicherheit wurde bekannt, dass 66% von Institutionen bereits Ziel von Angriffen waren und die Hälfte dieser Angriffe auch erfolgreich war. Wie sieht die Regierung diese Bedrohungslage?
2. Besteht eine Statistik zu Anfragen bei der Landespolizei in Bezug auf Cyberattacken oder generell zu Gefahren und Angriffen aus dem Netz?
3. Ziel von Cyberangriffen sind nicht nur Grossunternehmen, sondern beispielsweise auch Handwerksbetriebe, niedergelassene Ärzte oder kleine und mittlere Unternehmen sowie auch Privatpersonen. Könnte eine verlässliche und kompetente Kontaktstelle die Rahmenbedingungen der Digitalisierungsstrategie hier unterstützen?
4. Wäre es nicht notwendig hier vermehrt Sensibilisierungsanstrengungen und eine Anlaufstelle zu schaffen, welche mit Cyberspezialisten aus Wirtschaft, Forschung und Verwaltung an standardisierten Vorgehen bei

Hackerangriffen arbeitet, Qualitätsanforderungen für die digitale Notfallhilfe definiert und mögliche Zertifizierungen für regionale Experten durchführt?

5. Um die Schlagkraft im Bereich der Cybersicherheit zu erhöhen, werden in anderen Regionen auch ganz gezielt innovative Start-ups aus dem Bereich der IT-Sicherheit gefördert. Wie könnte Liechtenstein solche Innovationen stärken?

## Antwort vom 06. Dezember 2018

Einleitung: Wie bei der Beantwortung der Kleinen Anfrage der Stv. Abgeordneten Helen Konzett im Oktober 2018 schon erwähnt, gibt es in der Landesverwaltung verschiedene Zuständigkeiten, die ihren Beitrag zur Gefahrenabwehr leisten. Das Innenministerium übernimmt trotz der unterschiedlichen Zuständigkeiten erneut die Beantwortung der gegenständlichen Kleinen Anfrage.

Zu Frage 1:

Cyber-Angriffe gehören zum Alltag. Es gibt nach wie vor eine hohe Dynamik der Angreifer bei der Weiterentwicklung von Angriffswegen. Wie bei der Beantwortung der Kleinen Anfrage im Oktober 2018 bereits ausgeführt wurde, stellt die Landesverwaltung fast täglich eine Vielzahl von Angriffen mit unterschiedlichen Methoden fest. Bei der Beurteilung der Bedrohungslage stützt sich das Amt für Informatik nicht zuletzt auf die Einschätzungen der Melde- und Analysestelle für Informationssicherung (Melani) des Bundes; die Bedrohung wird von dieser als akut bezeichnet.

Zu Frage 2:

Die Landespolizei ist für die Strafverfolgung, begangen im oder durch Nutzung des Internets, zuständig. Insofern besteht bei der Landespolizei keine Statistik über Cyberattacken oder Angriffe über das Internet. Im Bereich der Cyberdelikte unterscheidet die Landespolizei zwischen Internetdelikten im engeren Sinne – darunter fallen Angriffe auf Daten- oder Computersysteme über das Internet, um Daten zu beschädigen oder IT-Systeme zu hacken sowie eigentliche DDos-Attacken (Distributed Denial of Service Attack), um Computersysteme zum Absturz zu bringen – und Internetdelikte im weiteren Sinne. Bei Letzteren wird Informations- und Kommunikationstechnik zur Planung, Vorbereitung und Ausführung ‚normaler' Kriminaldelikte eingesetzt (Betrug, Erpressung, Drohung, Phishing, verbotene Pornografie, Cyber-Grooming, Sextortion, Cyber-Mobbing usw.).

Die Landespolizei hat im laufenden Jahr bisher 57 Fälle als Cyberdelikte registriert. Davon sind lediglich drei Fälle Cyberdelikte im engeren Sinne. Allerdings geht die Landespolizei von einem erheblichen Dunkelfeld bei diesen Delikten aus.

Zu Frage 3:

Die Regierung pflegt den Austausch mit der Wirtschaft auf verschiedenen Ebenen und wird dies auch in der Digitalstrategie adressieren. Dabei kommt dem Schutz der kritischen Infrastruktur eine besondere Bedeutung zu.

Im Rahmen der Umsetzung der europäischen Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) arbeitet eine Arbeitsgruppe der Landesverwaltung unter anderem auch am Thema Meldestelle Cyberangriffe für die Wirtschaft. Diesbezüglich gilt es, eine grössenverträgliche Strategie für Liechtenstein zu prüfen. Die Materie als solche ist jedoch ministerien- und ämterübergreifend und betrifft zahlreiche weitere Stellen.

Zu Frage 4:

Die Landesverwaltung ist als Mitglied des Sicherheitsverbundes Schweiz aktiv an der Umsetzung der Nationalen Strategie der Schweiz vor Cyber-Risiken beteiligt. In Bezug auf die Landesverwaltung kümmert sich das Amt für Informatik um den Schutz der Infrastruktur der Landesverwaltung. Dazu gehören auch Kampagnen zur Sensibilisierung der Landesverwaltung. Von der Schweizer Strategie abgeleitet wurde das Projekt „Schutz von kritischen Infrastrukturen“ unter der Leitung des Amtes für Bevölkerungsschutz. Im Rahmen dieses Projektes erfolgte eine Inventarisierung kritischer Infrastrukturen. Punktuell wurden Gespräche mit Betreibern von kritischen Infrastrukturen geführt.

Die Universität Liechtenstein baut aktuell einen Kompetenzbereich auf dem Gebiet «Cyber Security» auf. Den Anstoss gab die Einrichtung des Hilti Lehrstuhls für Daten- und Applikationssicherheit am Institut für Wirtschaftsinformatik, wo gegenwärtig ein Kompetenzzentrum für «Secure Digital Innovation» entsteht. Ziel des Kompetenzzentrums ist die Kooperation von Partnern aus Wirtschaft, Gesellschaft und der Regierung, um Anforderungen im Bereich der IT-Sicherheit zu analysieren und konkrete Lösungen für das Land zu erarbeiten. Über die Beratung bestehender Unternehmen hinaus ist auch eine breite gesellschaftliche Sensibilisierung für dieses Thema angezielt. Nicht nur Technologien, sondern auch das Verhalten von Mitarbeiterinnen und Mitarbeitern sowie von Bürgerinnen und Bürgern spielen für Abwehrstrategien eine wichtige Rolle. Daher wird das Kompetenzzentrum an der Universität auch ein Weiterbildungsportfolio anbieten, das durch öffentliche Anlässe ergänzt wird. IT-Sicherheit wird zukünftig auch durch zahlreiche Lehrveranstaltungen in die konsekutive Lehre an der Universität integriert, insbesondere im Masterstudiengang Wirtschaftsinformatik, um zusätzliche «hauseigene» IT-Sicherheitsexperten für Liechtenstein auszubilden.

Der Aufbau des Kompetenzzentrums bei der Universität Liechtenstein, welches bezweckt, den Standort Liechtenstein auf diesem wichtigen Zukunftsgebiet weiter zu stärken und konkrete Unterstützung bei Sicherheitsprojekten im Land zu leisten, wird seitens der Regierung sehr begrüsst und diese steht diesbezüglich mit der Universität in Kontakt.

Zu Frage 5:

Durch den Aufbau der Forschungstätigkeit auf dem Gebiet der IT-Sicherheit an der Universität Liechtenstein werden die technologischen Voraussetzungen zur Gründung von innovativen Startups verbessert. Zudem wird ein Eco-System geschaffen, in dem Experten auf dem Gebiet «Cyber Security» an der Universität zusammenarbeiten, speziell am Kompetenzzentrum für «Secure Digital Innovation».