Kleine Anfrage

Cyber Resilienz Liechtensteins

Frage von	Stv. Landtagsabgeordnete Helen Konzett
Antwort von	Regierungsrätin Dominique Gantenbein

Frage vom 03. Oktober 2018

Am 8. Mai 2018 fand auf Einladung der Parlamentarischen Versammlung der OSZE (Organisation für Sicherheit und Zusammenarbeit in Europa) sowie auf Einladung des Portugiesischen Parlamentes in Lissabon eine Konferenz zur «Digitalen Resilienz eines demokratischen Staates» statt. Als Delegationsmitglied der Parlamentarischen Versammlung der OSZE durfte ich Liechtenstein an der Konferenz vertreten. Cyber-Bedrohungen respektive die Antworten demokratischer Staaten auf die Bedrohung wurden im Beisein von rund 20 internationalen und nationalen Fachpersonen diskutiert und in einen aktuellen Bezug gestellt. Nicht nur Firmen, sondern auch demokratische Errungenschaften unserer Staaten können direkt im Zentrum der Attacken oder Angriffe im Netz stehen. Sie können auf die Lahmlegung von Softwareprogrammen öffentlicher Verwaltungen zielen oder auf die Destabilisierung von Staaten durch im grossen Stil im Internet verbreiteten Fake News. Auch Liechtenstein ist betroffen beziehungsweise kann betroffen sein. Meine Fragen:

1. Welche Modelle, Konzepte und Aktivitäten zur Erhöhung der Widerstandsfähigkeit in Liechtenstein gegen Cyberattacken gibt es schon und auf welchen Ebenen sind diese angesiedelt, national oder supranational?
2. Könnte die 2004 in Kraft getretene und im Jahr 2016 von Liechtenstein ratifizierte Budapest Konvention aus Sicht der Regierung innerhalb der OSZE-Länder in der Bekämpfung des Cyber-Terrorismus einen guten Ausgangsrahmen darstellen, bei deren Weiterentwicklung auch Liechtenstein als kleines Land eine bedeutende Rolle spielen könnte?
3. Gemäss der Portugiesischen Ombudsstelle für kriminelle Cyberaktivitäten sind bei rund 4'000 Attacken täglich bisher schon rund 80% der Unternehmen Portugals Opfer von Cyberangriffen geworden. Wie hoch ist die Zahl der Attacken auf Liechtensteins Unternehmen in der Landesverwaltung und den angeschlossenen Betrieben sowie in den Gemeindeverwaltungen?
4. Gibt es Modelle, Konzepte und Aktivitäten zur Erhöhung der Widerstandsfähigkeit der Liechtensteiner Unternehmen und Finanzinstitute oder von Verbänden, von welchen die Regierung weiss oder an welchen sie beteiligt ist?

5. Die Universität Liechtenstein plant am 27. November 2018 die erste Cyber Security-Konferenz in Liechtenstein. Gibt es einen Wissenstransfer bei den zuständigen Landesverwaltungsstellen mit der Universität zum Thema?

Antwort vom 05. Oktober 2018

Cyber Resilienz ist ein umfassender Begriff im Bereich der Cyberkriminalität. In diesem Zusammenhang gibt es verschiedene Zuständigkeiten, die - wie folgend aufgezeigt - alle ihren Beitrag zur Gefahrenabwehr leisten. Resilienz wird als abstrakter Begriff in der Sicherheitspolitik verwendet, weshalb das Innenministerium trotz der unterschiedlichen Verantwortlichkeiten in diesem Bereich die Beantwortung der gegenständlichen Kleinen Anfrage übernimmt.

Zu Frage 1:

Die Widerstandsfähigkeit gegen Cyber Attacken wird seitens der Regierung auf verschiedenen Ebenen angegangen. Im Zentrum steht dabei die Cyber-Sicherheit für die Landesverwaltung sowie der Schutz der kritischen Infrastrukturen vor Cyber-Angriffen. Darüber hinaus muss sich jedes Unternehmen eigenverantwortlich mit den Bedrohungen auseinandersetzen und Massnahmen zum Schutz vor Cyber-Angriffen ergreifen.

Von der Schweizer Strategie abgeleitet wurde das Projekt „Schutz von kritischen Infrastrukturen“ unter der Leitung des Amtes für Bevölkerungsschutz. Im Rahmen dieses Projekts erfolgte eine Inventarisierung kritischer Infrastrukturen. Punktuell wurden Gespräche mit Betreibern von kritischen Infrastrukturen geführt.

Die Landesverwaltung ist als Mitglied des Sicherheitsverbundes Schweiz aktiv an der Umsetzung der Nationalen Strategie der Schweiz vor Cyber-Risiken (NCS) 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 Mitarbeitenden im Umgang mit Cyber-Risiken.

Die Landesverwaltung ist in Austausch mit verschiedenen internationalen Stellen. So ist das Amt für Informatik in der Arbeitsgruppe „Informatik-Sicherheit“ der Schweizerischen Informatikkonferenz (SIK) vertreten, welche den Informatikteil der Cyber-Thematik bearbeitet. Ebenfalls ist das Amt für Informatik Mitglied in zwei Arbeitsgruppen zur Umsetzung der „Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken“. Zum einen in der Arbeitsgruppe „Risikoanalyse und Prävention“ zum andern in der Arbeitsgruppe „Krisenmanagement“. Zusätzlich bestehen enge Kontakte mit etlichen weiteren internationalen Sicherheits- und Cyber-Behörden, unter anderen MELANI (CH), BSI (DE), ENISA (EU) und SON-euLISA (EU).

Zu Frage 2:

Die Budapest Konvention des Europarats ist kein Vertrag, der sich speziell auf Bekämpfung von Terrorismus und Cyber-Terrorismus konzentriert. Doch die in der Konvention vorgesehenen Straftatbestände können auch im Rahmen eines Terroraktes von Relevanz sein. So kann beispielsweise der Eingriff in ein Computersystem (Artikel 5 der Konvention) auch ein terroristischer Akt darstellen oder zur Vorbereitung eines solchen dienen. Die in der Konvention enthaltenen Rechtshilfe-Instrumente können auch bei terrorismus-bezogenen Ermittlungen genutzt werden. Dies und der Umstand, dass die Konvention über die Grenzen des Europarats bzw. der OSZE reicht (derzeit haben 61 Länder aus allen Weltregionen die Konvention ratifiziert) zeigt, dass die Budapest Konvention einen guten Ausgangsrahmen darstellt.

Liechtenstein nimmt seit vielen Jahren aktiv an den Vertragsstaatenversammlungen der Budapest Konvention teil und bringt sich konstruktiv ein. Im Juni 2017 wurde beschlossen, Verhandlungen über ein zweites Zusatzprotokoll zum Übereinkommen zu starten. Dieses soll insbesondere eine Verbesserung der internationalen Kooperation mit sich bringen. Liechtenstein verfolgt die Verhandlungen, kann jedoch aus Kapazitätsgründen nicht aktiv daran teilnehmen.

Zu Frage 3:

Cyber-Kriminalität und die damit verbundenen Attacken gehören längst zum Alltag. So stellt auch die Landesverwaltung beinahe täglich eine Vielzahl von Angriffen mit unterschiedlichen Methoden fest. Beispielsweise werden von den 190‘000 E-Mails, die durchschnittlich pro Monat eingehen, etwa 60% herausgefiltert und gelöscht, noch bevor sie überhaupt im Posteingang der Mitarbeitenden landen. Sie stammen entweder von nicht vertrauenswürdigen Absendern oder stellen eine konkrete Bedrohung durch Spam, Viren oder Phishing dar. 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 ihr als akut bezeichnet. Das Amt für Informatik ist laufend dabei, die technischen und organisatorischen Sicherheitsmassnahmen zu überprüfen und an die aktuellen Gegebenheiten anzupassen. Obwohl die Landesverwaltung kontinuierlich angegriffen wird, sind der Regierung keine Attacken bekannt, bei welchen es innerhalb der Landesverwaltung effektiv zu Schäden wie bspw. Betriebsunterbrüchen oder Datenverlusten kam.

Zu Frage 4:

Diesbezüglich wird auf die Beantwortung zu Frage 1 verwiesen.

Zu Frage 5:

Der Aufbau eines Kompetenzzentrums für Cyber Security durch die Universität Liechtenstein und damit zusammenhängende Initiativen und Veranstaltungen werden seitens der Regierung sehr begrüsst. Die Landesverwaltung steht in dieser Thematik mit der Universität Liechtenstein in Kontakt.