

Beschluss Nr. 747/2023

Schwyz, 24. Oktober 2023 / ju

Postulat P 9/23: Aufbau einer zentralen Cyber-Abwehrorganisation

Beantwortung

1. Wortlaut des Postulats

Am 1. Mai 2023 haben Kantonsrat Michael Fedier und fünf Mitunterzeichnende folgendes Postulat eingereicht:

«Der Regierungsrat wird beauftragt, eine kantonale oder interkantonale Cyber-Organisation nach den Empfehlungen des Sicherheitsverbundes Schweiz (SVS) einzurichten.

Begründung: In Zeiten von zunehmender Digitalisierung und Vernetzung ist die Sicherheit unserer IT-Systeme von entscheidender Bedeutung. Kriminelle oder terroristische Cyberangriffe können Privatpersonen, Unternehmen, Behörden und besonders auch kritische Infrastrukturen betreffen und erhebliche Schäden verursachen. Die staatlichen Einrichtungen standen im Jahr 2022 vermehrt im Fokus von Cyber-Attacken, u.a. RUAG, SBB sowie die EasyGov Plattform, aber auch Gemeinden wie Bad Zurzach, Bülach, Bottmingen, Bubendorf und die Stadt Montreux. Es besteht dringlicher Handlungsbedarf, auch im Kanton Schwyz. Der Regierungsrat soll daher die notwendigen Schritte in die Wege leiten und aktiv Massnahmen ergreifen, um die Cybersicherheit zu erhöhen und seine Informatik besser zu schützen.

Der Sicherheitsverbund Schweiz (SVS) ist eine Koordinationsplattform, die es Bund und Kantonen ermöglicht, bei Bedrohungen der inneren Sicherheit gemeinsam zu handeln. Der SVS arbeitet mit allen 26 Kantonen zusammen. Einige Kantone haben bereits nach den Empfehlungen des SVS eine Cyber-Organisation eingerichtet, namentlich Zürich, Luzern, Bern, Genf und St. Gallen. Der Kanton Genf geht sogar einen Schritt weiter und hat gemeinsam mit Vertretern aus Forschung, IT, Wirtschaft und NGO's dem Bund vorgeschlagen, Genf zum Hub für Digital Governance zu machen.

Wir fordern den Regierungsrat deshalb auf, im Kanton Schwyz eine Cyber-Organisation nach den Empfehlungen des SVS einzurichten. Dabei ist auch eine interkantonale Zusammenarbeit denkbar, um gemeinsam Synergien nutzen zu können.

Es sollen insbesondere folgende Vorgehens- und Implementierungsschritte aus den Empfehlungen übernommen werden:

- Gründung einer ständigen Projektgruppe: Es soll eine Projektgruppe aus Vertretern von Kanton, Bezirken, Gemeinden sowie öffentlichen Körperschaften eingesetzt werden. Diese Gruppe soll die Vorbereitung, Durchführung und Umsetzung der Massnahmen koordinieren.*
- Risikoanalyse: Eine Risikoanalyse soll durchgeführt werden, um die Bedrohungen und Schwachstellen in Kanton, Bezirken, Gemeinden und den öffentlichen Körperschaften zu identifizieren. Hierbei können auch bestehende Risikoanalysen und Erfahrungen von anderen Kantonen genutzt werden.*
- Erstellung eines Konzepts: Auf Basis der Risikoanalyse soll ein Konzept erstellt werden, das die Struktur und Aufgaben der Cyber-Organisation beschreibt. Hierbei sollen auch die Aufgaben der einzelnen beteiligten Stellen definiert werden.*
- Personalressourcen: Es sollen ausreichend Personalressourcen bereitgestellt werden, um die Umsetzung des Konzepts zu gewährleisten. Hierbei sollen auch Schulungen und Weiterbildungen für die beteiligten Mitarbeiterinnen und Mitarbeiter eingeplant werden. Zur Finanzierung dieser Massnahmen soll sich der Kanton Schwyz auch um Fördermittel auf Bundesebene bemühen. Eine wichtige Institution hierfür ist das Programm "Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken" des Bundesamtes für Bevölkerungsschutz (BABS). Dieses Programm bietet den Kantonen Unterstützung bei der Umsetzung von Massnahmen zur Stärkung der Cybersicherheit an.*
- Technische Ausstattung: Die Cyber-Organisation benötigt eine geeignete technische Ausstattung, um Cyberbedrohungen erkennen und bekämpfen zu können. Hierbei sollen auch technische Standards und Normen beachtet werden.*
- Zusammenarbeit mit anderen Kantonen: Der Kanton Schwyz soll eng mit anderen Kantonen und dem Bund zusammenarbeiten, um ein koordiniertes Vorgehen bei Cyberbedrohungen zu gewährleisten.*
- Übungen und Tests: Regelmässige Übungen und Tests sollten durchgeführt werden, um die Wirksamkeit der Massnahmen zu überprüfen und das Personal zu schulen.*

Für eine wohlwollende und pragmatische Aufnahme unseres Anliegens für eine signifikante Erhöhung der Cybersicherheit für den Kanton Schwyz und somit auch für unsere Bevölkerung danken wir freundlich.

Quellen:

Empfehlungen für die Umsetzung zur kantonalen: https://www.svs.admin.ch/content/svs-internet/de/themen/cybersicherheit/cybersicherheit-kantone/_jcr_content/content-Par/tabs/items/441_1612790888827/tabPar/downloadlist_1137108/download/items/303_1615194437757.download/Empfehlung%20Cyber-Organisation.pdf

Kanton Zürich: <https://www.zh.ch/de/news-uebersicht/medienmitteilungen/2022/07/der-kanton-zuerich-baut-ein-kantonales-zentrum-fuer-cybersicherheit-auf.html>

Genf soll zum "sicheren digitalen Raum" werden: <https://www.inside-it.ch/genf-soll-zum-sicheren-digitalen-raum-werden-20220506>»

2. Antwort des Regierungsrates

2.1 Ausgangslage

Das Thema Cybersicherheit ist vielschichtig und überschneidet sich mit anderen Themengebieten, weshalb vorab eine Abgrenzung angezeigt ist.

Unter dem Begriff IT-Sicherheit werden Methoden und Verfahren zusammengefasst, die dazu dienen, die «inneren» IT-Systeme zu schützen. Mit technischen Systemen und Lösungen werden elektronisch gespeicherte Informationen geschützt. Die IT-Sicherheit selbst ist ein Teilgebiet der übergeordneten Informationssicherheit, welche den Schutz sämtlicher Informationen zum Ziel hat – unabhängig davon, ob diese in digitaler oder analoger Form vorliegen. Die Informationen werden entsprechend den Schutzzielen Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit betrachtet.

Der Begriff Cybersicherheit wiederum beschreibt eine übergreifende Perspektive und geht über die Grenzen der eigenen Organisation hinaus. Die Cybersicherheit hat zum Ziel, die Betrachtung der Sicherheit auf den Cyber-Raum auszuweiten und so auch ausserhalb der eigenen Organisation Vernetzungen, Prozesse und Abhängigkeiten in das Sicherheitsdispositiv einzubeziehen.

Die kantonale Verwaltung agierte bis anhin hauptsächlich im Feld der IT- und Informationssicherheit. Verstärkt wurde dies im Jahr 2022 durch die Besetzung der Stelle des IT-Sicherheitsbeauftragten im Amt für Informatik. Der Bereich der Informationssicherheit soll im Rahmen der weiteren Arbeit zukünftig ebenfalls weiter gestärkt werden.

Die vorgeschlagenen Massnahmen aus dem von den Postulanten referenzierten Konzept «Empfehlung für die Umsetzung zur kantonalen Cyber-Organisation» des Sicherheitsverbund Schweiz (SVS) adressieren das Thema der Cybersicherheit und gehen gezielt auf die organisationsübergreifende Thematik ein. Insbesondere wird die Einführung der Rolle des Cyber-Koordinators vorgeschlagen, welche nebst dem Aufgabengebiet innerhalb der kantonalen Verwaltung auch eine Vernetzung zwischen den staatlichen und privaten Akteuren sicherstellen soll.

Die aktuelle Organisationsform wie auch das Handlungsfeld der IT-, bzw. der Informationssicherheit ergeben sich aus der Verordnung über die Informations- und Kommunikations-Technologie vom 1. September 2015 (IKTV, SRSZ 143.113) sowie dem Gesetz über die Öffentlichkeit der Verwaltung und den Datenschutz vom 23. Mai 2007 (ÖDSG, SRSZ 140.410). Eine übergreifende Funktion mit Einbezug der verschiedenen privaten und staatlichen Akteure ist aufgrund der vorliegenden Gesetzeslage nicht vorgesehen.

2.2 Haltung des Regierungsrates

Der Regierungsrat ist sich der zunehmenden Bedeutung des Thema Cybersicherheit bewusst. Eine isolierte Sicht auf die internen Strukturen wird längerfristig nicht mehr ausreichend sein, um ein angemessenes Sicherheitsdispositiv zu betreiben.

Das Konzept «Empfehlung für die Umsetzung zur kantonalen Cyber-Organisation» ist dem Regierungsrat bekannt. Einige Massnahmen daraus wurden bereits umgesetzt. So nimmt der IT-Sicherheitsbeauftragte einige der im erwähnten Konzept vorgeschlagenen Aufgabengebiete der Rolle des Cyber-Koordinators wahr. Beispielsweise ist er zentrale Anlaufstelle (Single Point of Contact) innerhalb des Kantons, aber auch zu den Behörden auf nationaler Ebene, insbesondere dem Nationalen Zentrum für Cybersicherheit (NCSC). Zudem verfolgt er die Entwicklungen der Cybersicherheit auf strategischer Ebene, nimmt Einsitz in der Arbeitsgruppe Informations- und Cybersicherheit der Digitalen Verwaltung Schweiz (DVS) und beurteilt das Sicherheitsdispositiv der kantonalen Verwaltung.

Eine weitere Komponente aus dem erwähnten Konzept des SVS behandelt die kantonale Krisenorganisation, in der die Rolle des Cyber-Koordinators eine führende Rolle bei einem Cyber-Vorfall übernimmt. Diese Anforderung deckt der Kanton Schwyz seit längerem ab, indem das Amt für Informatik im Kantonalen Führungsstab Schwyz vertreten ist. Für das Jahr 2024 ist eine Notfallübung im Bereich Business Continuity Management (BCM) geplant. Im Rahmen der Übung wird

ein Cyber-Vorfall simuliert und das Vorgehen sowie das Zusammenspiel der verschiedenen Akteure in einem solchen Falle trainiert.

Der Regierungsrat anerkennt das grundlegende Anliegen aus dem vorliegenden Postulat, die Cybersicherheit weiter zu erhöhen und hat bereits entsprechende Massnahmen ergriffen. In einer ersten Phase muss der Fokus jedoch auf die Stärkung der internen Strukturen und Prozesse gelegt werden, um das Qualitätsniveau in den Bereichen Informations- und Cybersicherheit in der Kantonsverwaltung weiter zu erhöhen sowie günstige Voraussetzungen für eine übergeordnete Koordination zu schaffen. Aktuell ist die Erstellung eines Informations-Sicherheits-Management-Systems (ISMS) in Erarbeitung, welches Vorgaben und Richtlinien für die kantonale Verwaltung definiert. Des Weiteren wird eine engere Zusammenarbeit zwischen dem Dienst Cybercrime der Kriminalpolizei und der Stabsstelle IT-Sicherheit beim Amt für Informatik derzeit geprüft, um zusätzliche Synergien zu erschliessen.

Eine starre Umsetzung der Empfehlungen aus dem Konzept des SVS hinsichtlich der Organisationsform ist in der gegenwärtigen Phase nicht zielführend. Die geschilderten Mindestanforderungen für eine erfolgreiche Cyberorganisation werden durch verschiedene Massnahmen und Aktivitäten bereits erarbeitet oder sind schon vorhanden. Die Zusammenarbeit und Koordination ist bereits eng und wird stetig intensiviert. Es ist als nicht zielführend zu beurteilen, den jetzigen Bestrebungen künstlich eine Organisationsform zu überstülpen und zusätzlichen Personalbedarf zu schaffen. Der Regierungsrat schliesst eine vergleichbare Organisationsform zukünftig nicht aus, diese muss sich jedoch zielgerichtet und aufgabenorientiert in einer für den Kanton geeigneten Form ergeben. Aus diesen Gründen wird dem Kantonsrat beantragt, das vorliegende Postulat für nicht erheblich zu erklären.

Beschluss des Regierungsrates

1. Dem Kantonsrat wird beantragt, das Postulat P 9/23 für nicht erheblich zu erklären.
2. Zustellung: Mitglieder des Kantonsrates.
3. Zustellung elektronisch: Mitglieder des Regierungsrates; Staatsschreiber; Sekretariat des Kantonsrates; Sicherheitsdepartement; Finanzdepartement; Amt für Informatik.

Im Namen des Regierungsrates:

Dr. Mathias E. Brun
Staatsschreiber

