Beschluss Nr. 373/2021
Schwyz, 1. Juni 2021 / ju

Interpellation I 28/20: Sind die Kantonale Verwaltung und die Schulen genügend gegen Cyberrisiken gewappnet?
Beantwortung

1. Wortlaut der Interpellation

Am 17. Dezember 2020 haben die Kantonsräte Roland Lutz, Thomas Hänggi und Roman Bürgi folgende Interpellation eingereicht:

«*In den letzten Jahren häuften sich Vorfälle im Bereich Cybersicherheit in der Schweiz. Die Folgen waren Betriebsunterbrüche, Datenverlust, finanzielle Schäden und Datenschutzverstösse. Angriffsziele sind IT-Systeme im weiteren Sinne.*

Gefahren bergen vor allem die Zunahme von Verbindungen ins Internet.

Schulen:
- *Im Besonderen steigen die Risiken durch die vermehrte Unterrichtsgestaltung mit Fernunterricht und die Nutzung von eigenen - und somit individuell gegen Risiken geschützten – Geräten der Schüler und Lehrer.*
- *Systemausfälle und Betriebsunterbrüche würden somit auch den Fernunterricht beinträchtigen.*

Kantonale Verwaltung:
- *Ähnliches gilt für die kantonale Verwaltung mit der Zunahme der Homeoffice-Tätigkeit. Hier wären Systemausfälle und Betriebsunterbrüche ebenfalls unerwünscht und Schadsoftware u.Ä. könnten Daten verfälschen oder unbrauchbar machen.*

Fragen an den Regierungsrat

1. *Erlangt der Regierungsrat periodisch Kenntnis über den Stand der Bemühungen zur Minimierung von Cyberrisiken und somit der Qualität der Cybersicherheit in der kantonalen Verwaltung und in den Schulen?*

2. *Gibt es spezifische (Minimal-)Vorgaben im Themenkomplex „Cybersicherheit" ...*
   a. *zur periodischen Prüfung, Beurteilung und allenfalls Rapportierung?*
   b. *Audits durch interne / externe Prüfinstanzen oder dergleichen?*

3. *Sind seitens Regierung Prozesse etabliert, die der laufenden Anpassung der Beurteilungskriterien aufgrund der steigenden Risiken und der Komplexität Rechnung tragen, namentlich in den Bereichen...*
   a. *Beschaffungsmanagement?*
   b. *Datenschutz & IT Risiko Management?*

Für die Beantwortung danken wir im Voraus.»

2. Antwort des Regierungsrates

2.1 Allgemeine Bemerkungen

Unter Cyberrisiken sind die Gefahren zu verstehen, die durch moderne Informations- und Kommunikation-Technologien (IKT) entstehen. Dabei stehen insbesondere böswillige Angriffe zur Unterbrechung der Systeme oder zum ungerechtfertigten Zugriff auf Daten im Fokus der Diskussion. Der Schutz gegen Cyberrisiken – die Cybersicherheit – ist in der kantonalen Verwaltung und an den kantonalen Schulen schon seit langem ein zentrales Thema. Die wachsende Vernetzung von Informatiksystemen sowie die zentrale Bedeutung einer funktionierenden Informatik hat entsprechend zu einem massgebenden Anstieg der Risiken durch Cybergefahren geführt. Die kantonale Verwaltung sowie die Schulen begegnen diesen Risiken in mehreren Bereichen:

- Im Technikbereich sind diverse Sicherheitsgerätschaften und -programme speziell für die Abwehr von Cyber-Angriffen im Einsatz. Die IT-Systeme werden im Standardbetrieb stets mit Sicherheitspatches (Softwareergänzung zur Schliessung von allfälligen Lücken) aktualisiert und neue Gerätschaften auf sicherheitsrelevante Aspekte geprüft.
- Die notwendigen Kommunikationskanäle (Anschluss Internet, E-Mailverkehr etc.) werden permanent auf Sicherheitsrisiken überwacht. Aufgrund des bestehenden Monitoring- und Protokollierungssystems können Meldungen zu aktuellen Bedrohungen zeitnah verfolgt und beurteilt werden.
- Der Wissensaustausch zwischen kantonsinternen und -externen Stellen sowie Experten wird aktiv gepflegt. So ist die kantonale Verwaltung Mitglied in diversen Fachgremien wie z. B. der Melde- und Analysestelle Informationssicherung (MELANI) im Nationalen Zentrum für Cybersicherheit (NCSC) und in der Arbeitsgruppe «Informations- und Cybersicherheit» der Schweizerischen Informatikkonferenz (SIK). Diese Kontakte erleichtern die Alarmierung sowie die Beurteilung und Planung von Abwehrmassnahmen gegenüber neuen Bedrohungen. Ein Expertenteam des NCSC würde zudem der Kantonsverwaltung bei einem konkreten Cyber-Vorfall mit seinem Fachwissen zur technischen Störungsbehebung zur Verfügung stehen. Des Weiteren besteht ein aktiver Austausch mit den Betriebskommissionen der beiden Schulrechenzentren Ausser- und Innerschwyz.
- Die Mitarbeitenden der Verwaltung und Schulen werden durch gezielte Schulungs- und Aufklärungskampagnen für sicherheitsrelevante Themen sensibilisiert.

2.2 Beantwortung der Fragen

2.2.1 Erlangt der Regierungsrat periodisch Kenntnis über den Stand der Bemühungen zur Minimierung von Cyberrisiken und somit der Qualität der Cybersicherheit in der kantonalen Verwaltung und in den Schulen?

Der Regierungsrat wird über den Stand der Bemühungen über einen jährlichen, verwaltungsweiten Bericht zum Controlling und zur Risikobeurteilung über den Status zu Cyberrisiken informiert. Weitergehende Informationen zu aktuellen, spezifischen Cyberrisiken werden dem Regierungsrat bei Bedarf durch den Vorsteher des Finanzdepartements, dessen Departement das Amt für Informatik zugewiesen ist, zur Kenntnis gebracht.

2.2.2 Gibt es spezifische (Minimal-)Vorgaben im Themenkomplex „Cybersicherheit" ...
a. zur periodischen Prüfung, Beurteilung und allenfalls Rapportierung?
b. Audits durch interne / externe Prüfinstanzen oder dergleichen?

Sowohl die kantonale Verwaltung als auch die Schulen besitzen interne Vorgaben und Richtlinien im Umgang mit Informatiksystemen. Diese beinhalten neben technischen auch organisatorische Sicherheitsanforderungen zur Cybersicherheit. Um den Schutz über alle Verwaltungseinheiten in organisatorischer Hinsicht unter einen Schirm zu stellen und die institutionelle Einbindung zu optimieren, konsolidiert das Amt für Informatik aktuell die Vorgaben zur Cybersicherheit.

Periodisch finden Prüfungen durch interne (Finanzkontrolle) und externe Kontrollinstanzen statt. Diese orientieren sich neben organisationsinternen Vorgaben auch an international gültigen Standards (z. B. Sicherheitsnormen der International Organisation for Standardization, ISO).

2.2.3 Sind seitens Regierung Prozesse etabliert, die der laufenden Anpassung der Beurteilungskriterien aufgrund der steigenden Risiken und der Komplexität Rechnung tragen, namentlich in den Bereichen...
a. Beschaffungsmanagement?
b. Datenschutz & IT Risiko Management?

Die der Beurteilung zugrundeliegenden Normen und Standards werden den sich ändernden Rahmenbedingungen angepasst. Dadurch ist sichergestellt, dass die mit den Audits vorgenommenen Kontrollen der IKT-Installationen von Verwaltung und Schulen aktuelle Bedrohungslagen bestmöglich berücksichtigen.

Im Beschaffungsmanagement werden die IKT-Sicherheitsthemen als wichtiger Bestandteil des Projektmanagements ausreichend berücksichtigt. Bei der in der Verwaltung zum Einsatz kommenden Projektmanagementmethode HERMES sind die entsprechenden Module im Basissetting enthalten und zwingend zu bearbeiten. Integrative Tests in einer geschützten Umgebung, Machbarkeitsstudien und Prototypen sind dabei Standardwerkzeuge.

In allen Bereichen der Verwaltung wird auf die Einhaltung der Datenschutzvorgaben geachtet. Im Rahmen des verwaltungsweiten Risikomanagementsystems werden identifizierte Risiken aufgeführt und bewirtschaftet. Das Risikomanagement beinhaltet eine jährliche Neubeurteilung vorhandener Risiken als auch die Ergänzung neu identifizierter Risiken unter Berücksichtigung der aktuellen Bedrohungslage.

Beschluss des Regierungsrates

1. Der Vorsteher des Finanzdepartements wird beauftragt, die Antwort im Kantonsrat zu vertreten.

2. Zustellung: Mitglieder des Kantonsrates.

3. Zustellung elektronisch: Mitglieder des Regierungsrates; Staatsschreiber; Sekretariat des Kantonsrates; Staatskanzlei; Departemente; Amt für Informatik.

Im Namen des Regierungsrates:

Dr. Mathias E. Brun
Staatsschreiber