Kanton Schaffhausen
Regierungsrat

Beschluss vom 8. März 2022

Kleine Anfrage Nr. 2022/6
betreffend «Ist die Kantonale Verwaltung genügend gegen Cyberrisiken gewappnet?»

In einer Kleinen Anfrage vom 23. Januar 2022 erkundigt sich Kantonsrat René Schmidt im Hinblick auf die zunehmende Digitalisierung und die damit einhergehende wachsende Gefahr der Cyber-Kriminalität nach den Bemühungen der öffentlichen Verwaltung, um die Sicherheit ihrer IT-Systeme zu gewährleisten.

Der Regierungsrat

a n t w o r t e t :

Frage 1: Wie beurteilt der Regierungsrat die Cyber-Sicherheit bei den IT-Systemen des Kantons?

Die Verantwortung für die IT-Systeme des Kantons liegt bei der KSD. Die KSD ist ISO/IEC 27001 zertifiziert. Dies ist ein weltweit anerkannter Standard für Informationssicherheit und die wichtigste Cyber-Security-Zertifizierung. Bei diesem Standard handelt es sich um ein Kontrollsystem, welches ein systematisches Vorgehen für den Schutz von Informationen vorgibt. Er bietet Organisationen aller Grössen klare Leitlinien für die Planung, Umsetzung, Überwachung und Verbesserung ihrer Informationssicherheit. Diese Anforderungen sind generell anwendbar und helfen, die Informationssicherheit und IT-Security systematisch und strukturiert zu optimieren.

Mit der erfüllten ISO-Zertifizierung gewährleistet die KSD einen hohen Informationsschutz für die Daten der Verwaltung.

Verwaltungsintern werden die Mitarbeitenden regelmässig mittels "Awareness-Kampagnen" für die Risiken, welche sich im Arbeitsalltag ergeben können, sensibilisiert.

Frage 2: Wie ist die Zuständigkeit der IT-Sicherheit in der Energie- und Wasserversorgung und im Gesundheitsbereich geregelt?

Die KSD stellt im Bereich der Energie- und Wasserversorgung keine ICT-Dienstleistungen zur Verfügung. Die Energie- und Wasserversorgung ist Sache der Gemeinden.

Im Gesundheitsbereich (bspw. Spitäler, Spitex, Pflegezentren) ist die KSD als Servicedienstleisterin verantwortlich für alle über die KSD bezogenen Services, für die richtige Infrastruktur und für die entsprechende technische Sicherheit. Die Gesundheitszentren wiederum sind in

der Verantwortung, «Awareness» bei ihren Mitarbeitenden zu schaffen und sicherzustellen, dass im persönlichen Verhalten die Sicherheitsregeln eingehalten werden. Mit anderen Worten: Die KSD stellt ein sicheres Werkzeug zur Verfügung und ist für dessen Unterhalt verantwortlich. Der bestimmungsgemässe Gebrauch desselben liegt jedoch in der Verantwortung der Organisation, welche das Werkzeug nutzt.

Frage 3: Werden regelmässig externe Überprüfungen der technischen Sicherheit vorgenommen?

Die KSD wird regelmässig von externen Firmen auf Schwachstellen auditiert. Die daraus resultierenden Empfehlungsvorschläge werden in einen Verbesserungskatalog aufgenommen, bewertet und angemessen umgesetzt, dies risikobasiert.

Frage 4: Werden diese Berichte und die Umsetzung des festgestellten Verbesserungspotenzials von der Kantonalen Finanzkontrolle überprüft?

Nach Aufforderung werden die Berichte der Finanzkontrolle im Rahmen ihrer Abschlussprüfung und der damit einhergehenden Prüfungen der minimalen ITGCs (IT General Controls) vorgelegt. Diese fliessen entsprechend in die Risikoüberlegung hinsichtlich der Prüfung der Jahresrechnung ein. Zeichnet sich eine wesentliche Auswirkung auf die Erstellung der Jahresrechnung bzw. ein dringender Handlungsbedarf ab, erfolgen weitere Überprüfungen bzw.werden entsprechende Massnahmen eingeleitet.

Der aktuelle Fragebogen zur ITGC-Prüfung wurde um diverse Fragestellungen zur Cybersicherheit erweitert bzw. angepasst. Die Finanzkontrolle legt der KSD jährlich einen Fragekatalog in diesem Bereich vor, welcher von der KSD beantwortet wird. Nach den Audits und einem gegebenenfalls vorliegenden Verbesserungskatalog definiert die KSD Massnahmen, wie sie allfällige Feststellungen der Finanzkontrolle korrigieren und künftig verhindern kann. Die Finanzkontrolle überprüft die Berichte, die definierten Massnahmen, deren Status der Umsetzung und das entsprechende Verbesserungspotenzial.

Frage 5: Wie sieht die Abstimmung und Koordination mit den Nachbarkantonen aus?

Die KSD ist Teil der Informatikkonferenz Ost (IK-Ost) und auch Teil der Schweizerischen Informatikkonferenz (SIK). Es wird eng mit den Kantonen im Rahmen dieser Konferenzen zusammengearbeitet. Die Verantwortlichen für die Daten- und Informationssicherheit (Chief Information Security Officer, kurz CISO) dieser Kantone tauschen sich regelmässig aus und stellen sich gegenseitig Berichte zur Verfügung. Neu wird die KSD auch gemeinsam mit dem Kanton Zürich zusammenarbeiten und dort Synergien bilden.

Des Weiteren pflegt die KSD mit externen Security-Fachgruppen (z.B. der Melde- und Analysestelle des Bundes "MELANI"; neu NCSC) einen steten Austausch, um am Puls des aktuellen Cyber-Geschehens zu bleiben.

Frage 6: In welchen Bereichen sieht der Regierungsrat in Bezug auf das Thema der Cyber-Sicherheit den höchsten Handlungsbedarf, und welche Massnahmen zur Erhöhung der Cyber-Sicherheit sind geplant?

Die KSD würde die Schaffung einer koordinativen Stelle für strategische und regulatorische Fragen der Informationssicherheit (Informationssicherheitsbeauftragter des Kantons Schaffhausen) begrüssen. Diese Stelle wäre departementsübergreifend wirksam. Entsprechende Abklärungen sind im Gange.

Frage 7: Wie wird die Widerstandsfähigkeit bei einem Cyber-Angriff beurteilt?

Grundsätzlich ist die Verwaltung gut gegen einen Cyber-Angriff gewappnet und es bestehen die notwendigen Vorkehrungen, um Cyber-Angriffe abzuwehren.

Frage 8: Sind durch Hackerangriffe verursachte Eigen- und Fremdschäden mit einer Cyber-Versicherung gedeckt?

Zurzeit besteht keine Cyber-Versicherung für den Kanton Schaffhausen. Die zuständigen kantonalen Stellen befassen sich momentan mit der Beurteilung des Cyberrisikos. Im Anschluss soll evaluiert werden, ob der Abschluss einer Cyberversicherung - wie von § 18 Abs. 2 der Finanzhaushaltsverordnung (SHR 611.103) verlangt - hinsichtlich Preis-Leistungs-Verhältnis sinnvoll ist.

Schaffhausen, 8. März 2022

Der Staatsschreiber

Dr. Stefan Bilger