

Interpellation Die Mitte-EVP-Fraktion vom 19. Februar 2024

Netz-Basisinfrastruktur: Wie sicher ist der Kanton St.Gallen?

Schriftliche Antwort der Regierung vom 2. April 2024

Die Mitte-EVP-Fraktion erkundigt sich in ihrer Interpellation vom 19. Februar 2024 nach den Sicherheitsvorkehrungen und der Datensicherheit im Bereich der Netz-Basisinfrastruktur. Es wird in diesem Zusammenhang auch auf problematische Hacker-Angriffe und auf Anbieter aus China Bezug genommen.

Die Regierung antwortet wie folgt:

Die Leistungen der Netz-Basisinfrastruktur werden im Kanton St.Gallen durch die KOM SG erbracht. Die «Interessengemeinschaft KOM SG» (KOM SG) ist ein Verein mit Sitz in St.Gallen, der den Zweck verfolgt, seinen Mitgliedern eine effiziente, wirtschaftliche und bedarfsgerechte Datenkommunikation bereitzustellen. Ziele, Organe, Finanzen und Organisation des Vereins sind in den Statuten geregelt. Mitglieder der KOM SG sind der Kanton St.Gallen und die St.Galler Gemeinden (vertreten durch die Vereinigung St.Galler Gemeindepräsidenten). Neben den Mitgliedern, die gleichzeitig auch Kunden der KOM SG sind, zählen weitere Organisationen zum Kundenkreis der KOM SG – namentlich Universität, Spitäler, Pflegeheime oder Schulen.

Seit der Gründung der KOM SG haben sich sowohl das technologische Umfeld als auch die Anforderungen und Erwartungen der Kunden verändert. KOM SG, als dienstleistungsorientierter Verein, hat das Aufgabenportfolio, seine Schwerpunkte und die organisatorischen Rahmenbedingungen stetig und pragmatisch weiterentwickelt. Für die Sicherstellung der Datenkommunikation bietet der Verein auch Netzdienste an. Netzdienste sind nebst dem Netzzugang zur KOM SG auch Dienste wie Internetzugang, E-Mail, Konferenzsysteme und Remote-Access-Verbindungen gemäss dem jeweils gültigen Dienstleistungsangebot.

Zu den einzelnen Fragen:

1. Das neue «KOMSG 2022»-Netzwerk wird mit Komponenten, Systemen und Software von CISCO betrieben. Der Rollout ist im Gange und wird per Mitte 2024 abgeschlossen sein. Auch bisher waren CISCO-Komponenten im Einsatz. CISCO ist ein US-amerikanisches Unternehmen. Das «KOMSG 2022»-Netzwerk wird nach Abschluss des Rollouts einem intensiven Security Audit unterzogen. Die Netzwerke der kantonalen Berufsfachschulen und Mittelschulen werden grossmehrheitlich mit Komponenten von CISCO und Hewlett Packard Enterprise betrieben. Eine Schule setzt Produkte von Huawei ein. Ein Ersatz der Huawei-Komponenten ist für das Jahr 2025 geplant. Die von den Gemeinden in ihren lokalen Netzwerken eingesetzten Lösungen (Komponenten) sind dabei nur teilweise bekannt.
2. Es wird sehr viel unternommen, um mögliche Angriffe auf diese zentralen Infrastrukturen abzuhalten. So bringt der laufende Rollout unter anderem eine neue Segmentierung des Netzwerks sowie NAC (Network Access Control, Zugriffskontrolle auf Basis der eindeutigen Hardwareadresse) und SDA (Software Defined Access, spezifischer Zugang zum Netz über Management-Software gesteuert), dies zumindest auf den kantonalen Netzwerk-Segmenten. Es ist noch zu klären, ob zum Beispiel auf der Grundlage von Art. 24 des kantonalen E-Government-Gesetzes (sGS 142.3; abgekürzt E-GovG) die Gemeinden

verpflichtet werden können, bei den neuen Sicherheitstechnologien und -methoden nachzuziehen. Ausserdem werden ab Ende 2024 die Netzwerk-Überwachungsmeldungen ins «SIEM/SOC» einfließen und aktiv überwacht, dies rund um die Uhr (7x24). «SIEM/SOC» steht für Security Information and Event Management / Security Operations Center. Mit diesem zeitgemässen Werkzeug wird das Netz permanent überwacht (Monitoring) und unübliche Meldungsmuster werden sofort an eine 7x24-Organisation gemeldet. Hierzu wurde ein Beschaffungsvorhaben mit fünf weiteren Ostschweizer Kantonen abgewickelt.

3. Seitens Bund sind keine Vorschriften bezüglich der Beschaffung von entsprechenden Infrastrukturen bekannt. Hingegen werden bei der Ausschreibung und Beschaffung von sicherheitsrelevanten Komponenten grundsätzlich die Standards Common Criteria (CC) ISO/IEC 15408:2022, ITSEC (Information Technology Security Evaluation Criteria, Kriterien / Zertifikate mit europäischer Anerkennung) sowie die Empfehlungen des Deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) berücksichtigt.
4. Die Basis-Infrastruktur der KOM SG wurde erst kürzlich neu beschafft. Vor diesem Hintergrund wurde noch keine weitere neue Strategie für Beschaffungen festgelegt. Es ist aber auf jeden Fall zentral, bei künftigen Beschaffungen dem Thema Datensicherheit ein sehr hohes Gewicht beizumessen.