

## Vorlage Stadtparlament

Datum	7. April 2021
Beschluss Nr.	415
Aktenplan	152.15.13 Stadtparlament: Einfache Anfragen

### Einfache Anfrage Konstantin Hälgi: Cybersicherheit der Stadt St.Gallen; Beantwortung

Am 25. Februar 2021 reichte Konstantin Hälgi die beiliegende Einfache Anfrage betreffend «Cybersicherheit der Stadt St.Gallen» ein.

Der Stadtrat beantwortet die Einfache Anfrage wie folgt:

#### 1 Einleitung und Ausgangslage

Digitalisierung und Automatisierung machen auch vor und in der Allgemeinen Verwaltung, den Volksschulen und den städtischen Betrieben nicht Halt. Sie sind stetige Begleiter bei der unentwegten Implementierung von Transformations- und Optimierungsprozessen. Der zunehmenden digitalen Durchdringung, gepaart mit der exponentiell wachsenden Bedrohungslage im ICT-Sicherheitsbereich, wird seit Jahren höchste Aufmerksamkeit geschenkt.

#### 2 Beantwortung der Fragen

1. *Für welche Infrastrukturen muss die Stadt den Schutz im Cyberspace selbst gewährleisten und für welche stellt diesen der Bund sicher? (Ich gehe davon aus, dass die Stadtwerke als kritische Infrastruktur gelten)*

Aufgaben, Verantwortung und Kompetenzen für ICT-Infrastrukturen<sup>1</sup> sind in der Stadtverwaltung klar geregelt. Dabei gehören die verwaltungsspezifischen Aspekte der Büroautomation in die Zuständigkeit der Informatikdienste (IDS). Die Betriebe (sgsw, VBSG, KHK) oder die Stadtpolizei zeichnen mit ihren Spezialsystemen für ihren eigenen Bereich verantwortlich. Für technische Steuerungen wie z. B. Lichtsignalanlagen sind die jeweiligen Dienststellen zusammen mit ihren Lieferanten zuständig. Die Abraxas Informatik AG ist als Betreiberin der zentralen Gemeindefachanwendungen verantwortlich (z. B. Softwarelösung für Steueramt, Bevölkerungsdienste, Betreuungswesen, Wahlen und Abstimmungen etc.). Der Verein «Kommunikationsnetz St.Gallen» (KOM SG<sup>2</sup>) ist für den Bereich des kantonalen Kommunikationsnetzes zuständig und das Bundesamt für Informatik und Telekommunikation (BIT<sup>3</sup>) stellt einzig alle Themen rund um die Bundesapplikationen (z. B. RiPol, Polizeifahndungs-

---

<sup>1</sup> information and communications technology / Informations- und Kommunikationstechnologie

<sup>2</sup> [KOM SG | WIR BÜNDELN DATENKOMMUNIKATIONSDIENSTE VERSCHIEDENER ANBIETER](#)

<sup>3</sup> [Bundesamt für Informatik und Telekommunikation BIT \(admin.ch\)](#)

system bei der Stadtpolizei oder ZivisPro, Zivilstandeswesen) für die Stadtverwaltung sicher. Ein aktiver Schutz der kritischen Infrastrukturen der Werke durch den Bund ist – zumindest in Friedenszeiten – nicht möglich.

## *2. Welche Abteilung der Stadt ist für die Cybersicherheit verantwortlich?*

Für die ICT-Sicherheit im Bereich der Büroautomation sind die IDS zuständig. Sie verfügen über einen sehr gut ausgebildeten CISO<sup>4</sup> und auch über speziell ausgebildete Systemengineers in der operativen Umsetzung im Betrieb. Die IDS stützen sich auf die regelmässige Gremienarbeit im städtischen Ausschuss für die Sicherheit von Informatiksystemen (ASI) ab. Der regelmässige Austausch in verschiedenen Arbeitsgruppen (bspw. Deutschschweizer Arbeitsgruppe Informatiksicherheitsbeauftragte, Erfahrungsaustauschgruppe ICT-Sicherheit Nordostschweiz) und zu übergeordneten Informationsnetzwerken wie z. B. dem Nationalen Zentrum für Cybersicherheit (heute NCSC<sup>5</sup>, ehemals MELANI<sup>6</sup>) stellt ein zentrales Element in der täglichen Arbeit dar.

Für die vielfältigen technischen Spezialsysteme sind die jeweiligen betreibenden Bereiche zusammen mit ihren Zulieferanten verantwortlich.

Bei den sgsw ist ein Nachhaltigkeits- und Risikomanagementsystem (NRM) als Matrixorganisation implementiert, mit der alle Sicherheitsbereiche bzw. -themen abgedeckt werden (z. B. Arbeitssicherheit, Trinkwasserqualität). Für jeden Sicherheitsbereich gibt es eine verantwortliche Person, die jeweils der Unternehmensleitung Bericht erstattet. Der Sicherheitsbereich «Digitale Sicherheit» befasst sich spezifisch mit dem Thema Cybersecurity. Das Nachhaltigkeits- und Risikomanagementsystem wird durch Jahresziele gesteuert.

## *3. Hat es bereits erfolgreiche Angriffe gegeben, bei denen Schäden entstanden beziehungsweise Daten abgeflossen sind?*

Nein, bisher gab es weder erfolgreiche Angriffe noch sind nach heutigem Kenntnisstand städtische Daten abgeflossen.

---

<sup>4</sup> Ein Chief Information Security Officer (CISO) bezeichnet die Rolle des Gesamtverantwortlichen für Informationssicherheit.

<sup>5</sup> National Cyber Security Center (NCSC)

<sup>6</sup> Melde- und Analysestelle Informationssicherung (MELANI)

4. *Viele Angriffe können durch einfache Massnahmen wie Firewall, Virenschanner, Passwortmanager sowie Aufklärung der Mitarbeitenden verhindert oder abgemildert werden. Hat die Stadt solche Mindeststandards? Wenn ja, wie sehen diese aus?*

Die IDS sind seit dem Jahr 2012 mit dem ICT-Sicherheits-Standard ISO/IEC 27001<sup>7</sup>-zertifiziert. Diese Norm verlangt u.a. ein vollintegriertes ISMS<sup>8</sup> inkl. Risiko-Management. Die jährlichen ISO-Audits wurden ausnahmslos ohne Auflagen bestanden. Darüber hinaus beruhen die ICT-Sicherheitskonzepte und Umsetzungsempfehlungen auf den Standards der renommierten Norm ISO/IEC 27002<sup>9</sup>. Die verbindlichen städtischen Grundsatzweisungen im Sinne von Mindeststandards basieren u.a. auf dem Grundsatz des BSI (Bundesamt für Sicherheit).

Für die technische Infrastruktur verfügen die IDS über ein mehrstufiges, technisches ICT-Sicherheitsdispositiv, welches letztmals im Jahr 2020 durch externe ICT-Sicherheits-Spezialisten überprüft wurde. Die Erkenntnisse daraus dienen der weiteren Härtung des Dispositivs. Regelmässige interne und externe Audits (z.B. Penetrationstests mit jeweils sehr guten Resultaten) stellen einen wichtigen Baustein im Gesamtsystem der IDS dar. Veränderungen an technischen Systemen, u.a. durch neue Vorhaben ausgelöst (bspw. Projekte wie «Robotik» oder «Chatbot»), werden bei ihrer Entstehung strukturiert begleitet (bspw. mittels Durchführung eines Security-Sign-Offs oder strukturierte Prüfung von Cloud- bzw. SaaS<sup>10</sup>-Vorhaben).

Das Benutzendenverhalten ist und bleibt das grösste Risiko, denn vielfach genügt bereits ein vermeidbarer Klick, um städtische ICT-Systeme und Daten zu gefährden. Regulatorische Vorgaben für die städtischen Endanwendenden sind in den entsprechenden, vom Stadtrat beschlossenen ICT-Reglementen und in ILA-Weisungen (Informatik-Lenkungsausschuss) festgehalten und bilden einen integralen Bestandteil des durchgängigen ICT-Sicherheitsdispositivs. Seit mehreren Jahren führen die IDS Security-Awareness-Kampagnen zur Sensibilisierung des städtischen Personals durch. Ansprechende E-Learning-Einheiten mit Erfolgskontrolle und Zertifikaten, sowie Auswertungen an die jeweiligen Vorgesetzten gehören ebenso dazu, wie die Durchführung von Schulungen und Phishing-Simulationen.

5. *Im Wissen darum, dass Sicherheitslücken kaum komplett vermieden werden können: Hat die Stadt ein Handlungskonzept, das im Falle von gelungenen Cyber-Angriffen zum Tragen käme?*

Im Fall eines erfolgreichen Angriffs verfügen die IDS über eine Alarm- und Notfallorganisation, vorbereitete Notfallhandbücher (Alarmstufenprozesse) und Wiederanlaufpläne (ICT-Service Continuity Management). Der IDS-Führungsstab steht in ausserordentlichen Lagen 24 h zum Einsatz bereit; auch realistische Angriffs-Situationen werden regelmässig trainiert.

---

<sup>7</sup> [ISO/IEC 27001 – Wikipedia](#)

<sup>8</sup> Ein Managementsystem für Informationssicherheit, das dazu dient, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

<sup>9</sup> [ISO/IEC 27002 – Wikipedia](#)

<sup>10</sup> Software as a Service: Basiert auf dem Grundsatz, dass die Software und die IT-Infrastruktur bei einem externen IT-Dienstleister betrieben und vom Kunden als Dienstleistung genutzt wird.

Sollte ein Cyber-Angriff wider Erwarten erfolgreich sein, bestehen seitens IDS entsprechende Verträge, bspw. für forensische Analysen durch externe Spezialistinnen und Spezialisten mit sogenannten «Computer Security Incident Response Teams (CSIRT<sup>11</sup>)», um ein Ereignis geordnet zu lenken und die Rückführung in den Normalbetrieb zu unterstützen.

In der Direktion Technische Betriebe sind angesichts der besonders hohen Sicherheitsanforderungen an die technische IT zusätzliche spezifische Abwehrmassnahmen und -prozesse in Entwicklung. Dabei wird eng mit dem SWITCH Energy-CERT zusammengearbeitet. In diesem CERT (Computer Emergency Response Team) teilen die Stadtwerke und die Betreiber von Kernkraftwerken vertrauliche Informationen und werden über aktuelle Bedrohungen sowie kritische Vorfälle informiert. SWITCH hat Zugriff auf ein internationales Expertennetzwerk und bietet im Ernstfall aktive Unterstützung bei der Bewältigung einer Krise.

Die Stadtpräsidentin:  
Maria Pappa

Der Stadtschreiber:  
Manfred Linke

Beilage:

- Einfache Anfrage vom 25. Februar 2021

---

<sup>11</sup> Ein Computer Security Incident Response Team, oder abgekürzt CSIRT, ist eine Organisation, die Informationen über Sicherheitsvorfälle sammelt, Analysen durchführt und auf Anfragen der Einsender reagiert. Ein CSIRT kann entweder dauerhaft eingerichtet oder nur in besonderen Situationen aufgestellt werden.