st.gallen
Stadtrat

Vorlage Stadtparlament

Datum	10. September 2024
Beschluss Nr.	4296
Aktenplan	152.15.13 Stadtparlament: Einfache Anfragen

Einfache Anfrage Louis Stähelin und Beat Rütsche: Geopolitische Risiken – Ist St.Gallen vorbereitet?; Beantwortung

Am 5. Juni 2024 reichten Louis Stähelin und Beat Rütsche die beiliegende Einfache Anfrage betreffend «Geopolitische Risiken – Ist St.Gallen vorbereitet?» ein.

Der Stadtrat beantwortet die Einfache Anfrage wie folgt:

1 Ausgangslage

Unter geopolitischen Risiken werden die potenziellen Bedrohungen und Unsicherheiten verstanden, die aus politischen und wirtschaftlichen Spannungen zwischen Ländern oder Regionen entstehen. Diese Risiken können durch verschiedene Faktoren, namentlich durch Konflikte und Kriege, politische Instabilität, Wirtschaftssanktionen, Ressourcenkonflikte oder terroristische Aktivitäten beeinflusst werden. Seit dem russischen Angriffskrieg gegen die Ukraine haben sich die geopolitischen Risiken in Europa, und damit auch in der Schweiz, wesentlich erhöht. In seinem Lagebericht 2023 beschreibt der Nachrichtendienst des Bundes (NDB), dass die vertrauens- und kooperationsbasierte Sicherheitsarchitektur in Europa zerstört worden sei und das sicherheitspolitische Umfeld in der Schweiz sich fundamental und nachhaltig negativ verändert habe. Der NDB listet als dringlichste Gefahren die Bedrohung der Sicherheit durch Terrorismus, die Bedrohung für kritische Infrastrukturen in der Schweiz durch kriminelle Gruppierungen und mögliche Übertragungs-Effekte von staatlichen Aktionen im Krieg gegen die Ukraine sowie Bedrohungen durch verbotenen Nachrichtendienst[1] auf.

Die zentralen Instrumente zur Abwehr von Gefahren sind auf nationaler und kantonaler Ebene angesiedelt. Die innere und äussere Sicherheit des Landes obliegt dem Bundesrat und der Bundesversammlung, die Lagebeurteilung und Prävention in sicherheitspolitischen Fragen dem NDB und die innere Sicherheit eines Gebiets in erster Linie den Kantonen als Träger der Polizeihoheit. Auf dem Gebiet der Stadt St.Gallen erfüllt die Stadtpolizei die gemeindepolizeilichen Aufgaben im Sinne von Art. 13 des Polizeigesetzes (PG; sGS 451.1). Für sicherheitspolizeiliche Vorkommnisse mit besonderem Gefahrenpotenzial verfügt die Stadtpolizei über eine spezialisierte Interventionseinheit (SE STEP).

[1] Nachrichtendienst des Bundes (2023): *Sicherheit Schweiz. Lagebericht des Nachrichtendienstes des Bundes*, S. 7 ff.

2 Beantwortung der Fragen

1. *Wie ist das Management der geopolitischen Risiken in Stadtrat und den jeweiligen Geschäftsleitungen verankert? Wie fliessen mögliche geopolitische Risiken in die strategischen und finanziellen Ziele der Stadt ein?*

Das Risikomanagement der Stadt St.Gallen ist sowohl zentral als auch dezentral organisiert. Dezentral liegt es in der Verantwortung der Direktionen und Dienststellen, Risiken zu identifizieren, zu bewerten und basierend darauf eine Risikostrategie mit Massnahmen zu definieren. Auf gesamtstädtischer Ebene führt der Stadtrat zentral ein Risikomanagement. Einmal jährlich wird unter der Federführung der Dienststelle Organisationsentwicklung ein Risikoreport erstellt, in dessen Rahmen die Dienststellen Risiken und Massnahmen in den Kategorien «Finanzen», «Sicherheit», «Reputation» und «Technisches» erfassen und aktualisieren. Der Stadtrat prüft in der Folge, ob die im Risikoreport erfassten Massnahmen angemessen sind und wirksam umgesetzt werden. Einzelne Dienststellen wie die Informatikdienste (IDS) oder Feuerwehr und Zivilschutz (FWZSSG) verfügen über ein eigenes, branchenübliches zertifiziertes Risikomanagement.

Die Sicherheitslage wird von der Stadtpolizei mit Blick auf aktuelle (auch «übergeordnete») Risiken fortlaufend beurteilt, wobei aus diversen Informationsquellen (vgl. auch Frage 2) geschöpft wird. Auch in anderen Dienststellen mit potenziell von geopolitischen Risiken betroffenen Tätigkeitsbereichen sind entsprechende Vorkehrungen in Strategie, Finanzplanung und operativem Tagesgeschäft verankert.

Die Direktion Technische Betriebe betreibt für die Stadt kritische Infrastrukturen in den Bereichen «Energieversorgung», «Trinkwasserproduktion» und «Entsorgung». Diese Anlagen sind seit jeher potenzielle Ziele von Sabotageakten und Cyberangriffen. Um die aktuell erhöhten geopolitischen Risiken für die Versorgungssicherheit zu reduzieren, wurden eine Reihe von organisatorischen und technischen Massnahmen ergriffen, die nötigen Mittel budgetiert sowie die Zusammenarbeit innerhalb der Branche und mit Bundesstellen intensiviert. Zu diesen konkreten Massnahmen gehören die Vorbereitung des Stromnetzes auf eine Strommangellage, die Ausstattung der Unterwerke mit Notstromaggregaten, eine Aufstockung der Brennstofflager für die Fernwärmeproduktion, die rasche Umsetzung der vom Bund vorgegebenen Minimalstandards für die Informations- und Kommunikationstechnik (IKT) in allen Unternehmen[2] der Direktion Technische Betriebe, der Ausbau der Cyberabwehr im Bereich Technischer Informatik (OT) – insbesondere durch Schaffung der Stelle eines Chief Information Security Officer (CISO) – und verstärkte Zusammenarbeit[3].

Im Bereich des Bevölkerungsschutzes hat der Kanton St.Gallen Defizite erkannt und in den vergangenen Monaten Bestrebungen zur Erhöhung seiner Resilienz unternommen. Dabei stehen besonders der Schutz der kritischen Infrastrukturen und generell das Funktionieren des Alltags bei Mangellagen im Fokus – unter anderem durch eine umfassende Bevölkerungsschutzstrategie. Mit dem St.Galler Zivilschutz 2015 Plus wurden Strukturen, Bestände und Doktrin des Zivilschutzes konsequent auf Einsätze (Katastrophen und Notlagen) ausgerichtet und in abgelaufenen Einsätzen der vergangenen vier Jahre erfolgreich einem Realitätscheck unterzogen.

---

[2] bereits durchgeführt: ARA, SWW Frasnacht, Netz Elektrizität

[3] Zum Thema Resilienz insbesondere mit OSTRA, der Organisation für Stromversorgung in Ausserordentlichen Lagen und dem VSE, dem national und international anerkannten Branchendachverband der Schweizer Stromwirtschaft, zum Thema Cybersecurity insbesondere mit anderen EVUs, dem SWITCH-CERT, welches als eines von zwei nationalen CERT kritische IT-Infrastrukturen in der Schweiz schützt, dem Bundesamt für Cybersicherheit BACS sowie mit Universitäten und Lieferanten.

2. *Wie hat sich die Beurteilung der städtischen Sicherheitslage in den letzten beiden Jahren verändert? Welche Schlüsse wurden daraus gezogen, und welche Massnahmen wurden implementiert?*

Trotz Veränderungen der globalen Sicherheitslage in den letzten zwei Jahren präsentiert sich die allgemeine Sicherheitslage in der Stadt St.Gallen aus Sicht der Stadtpolizei im Grunde als stabil, gerade weil potenziell betroffene Dienststellen schon zuvor grossen Wert auf das Erkennen von Risiken und vorbereitende Massnahmen gelegt haben. Die Stadtpolizei hat gegen die erwähnten Bedrohungen wie Terrorismus etablierte Massnahmen zur Hand. Die Informationsbeschaffung erfolgt insbesondere über den NDB, polizeiliche Gremien sowie andere Polizeikorps und Amtsstellen. Von Vorteil ist dabei nicht zuletzt auch die Vernetzung der Stadtpolizei mit anderen städtischen Amtsstellen. Im Rahmen eines Bedrohungs- und Risikomanagements wird bei entsprechenden Hinweisen der Kontakt zu Gefährdern gesucht, um eine zielgerichtete Gewalt möglichst verhindern bzw. eine Radikalisierung erkennen zu können. Mit einer angemessen hohen Polizeipräsenz sowie Schwerpunktsetzungen gewährleistet die Stadtpolizei neben der polizeilichen Präventionstätigkeit auch eine rasche Interventionsfähigkeit. Die Stadtpolizei verfügt über die nötigen korpsinternen Spezialistinnen und Spezialisten.

Auch im Cyber-Bereich existieren reelle Gefahren, gegen die sich die Stadt rüstet. Das Bundesamt für Cybersicherheit (BACS) belegte bereits in seinem Halbjahresbericht 2023/1 politisch relevante Ereignisse wie Angriffe auf mehrere Webseiten von Bundesämtern, dem Parlament, von Kantonen und Städten.[4] Eine dieser gezielt angegriffenen Webseiten war der extern gehostete Internetauftritt der Stadt St.Gallen. Zur Abwehr ebensolcher Angriffe legen die IDS grossen Wert auf die Qualifizierung ihrer Mitarbeitenden. Sowohl die Führung als auch die ICT-Fachspezialistinnen und Fachspezialisten der IDS haben erfolgreich Weiterbildungen im Bereich der ICT-Sicherheit absolviert und tauschen sich regelmässig mit ICT-Sicherheitsspezialisten verschiedener Städte, Kantone, des Bundes sowie von Schweizer Unternehmen aus. Um die verschiedenen ICT-Services sowie die städtischen Daten gegen die stetig zunehmende Bedrohungslage und die immer professionelleren Cyberangriffe auch in Zukunft zu schützen, überprüfen, optimieren und entwickeln die IDS ihre umfangreichen Sicherheitsvorkehrungen stetig weiter. Neben den technischen Vorkehrungen ist auch die permanente Sensibilisierung der städtischen Mitarbeitenden durch eine Awareness-Kampagne, verpflichtende Lerneinheiten und E-Mail-Phishing-Simulationen elementar. Die IDS betreiben selbst keine kritischen ICT-Infrastrukturen, ihr Leistungsauftrag beschränkt sich hauptsächlich auf den Betrieb der städtischen ICT-Büroautomation. Die Risikobeurteilung sowie konkrete Massnahmen im Bereich derjenigen kritischen Infrastrukturen; im Verantwortungsbereich der Technischen Betriebe wurden unter Frage 1 dargelegt.

Zum Thema eines möglichen Energiemangels wurden entsprechende Vorkehrungen planerischer Natur getroffen. FWZSSG verfügt seit Anfang 2024 über fünf mobile Notstromgeneratoren, wovon drei für dienststelleninterne Zwecke benötigt würden.

[4] Online unter: Halbjahresbericht 2023/1 (admin.ch).

3. Wie wird das Risikomanagement auf Best Practice hin überprüft?

Der jährliche Zyklus des Risikoreports bringt eine regelmässige Überprüfung der Beurteilung von Risiken und der entsprechenden Massnahmen mit sich. Überall da, wo das Funktionieren von kritischen Infrastrukturen betroffen ist, besteht basierend auf der Bundesverfassung und dem Landesversorgungsgesetz eine staatliche Verantwortung. Die Prüfung im Sinne von Best Practice findet demnach je nach Risikobereich und den entsprechenden gesetzlichen Vorgaben oder branchenüblichen Praktiken durch Zertifizierung, die Anwendung von Standards, simulierte Angriffen oder Austausch statt:

- Die Stadtpolizei beispielsweise überprüft ihr Risikomanagement neben der Informationsbeschaffung gleichermassen durch den Informationsaustausch mit den bereits erwähnten polizeilichen bzw. polizeinahen Stellen und Gremien, wobei Best Practices ausgetauscht werden.
- Bei den IDS ist die ICT-Sicherheit ein wesentlicher Inhalt des Alltags. Dies widerspiegelt sich ebenfalls darin, dass die IDS bereits seit 2012 gemäss der international anerkannten ISO-Sicherheitsnorm 27001 zertifiziert sind und dieses Jahr (2024) die Re-Zertifizierung erfolgreich bestanden haben. Ein wesentlicher Bestandteil des zertifizierten Informationssicherheitsmanagement-Systems (ISMS) der IDS ist das IT-Risikomanagement.
- Im Jahr 2024 wurde pan-europäisch der Ernstfall eines Cyberangriffs auf kritische Infrastrukturen der Gas- und Stromversorgung simuliert. Mit dabei war auch ein Team der St.Galler Stadtwerke und des Stabs Technische Betriebe. Die Erkenntnisse aus dieser praxisnahen Übung werden in die Prozesse der Betriebe eingearbeitet.
- Best Practice wird bei FWZSSG im Rahmen der bestehenden Aufträge gesetzlich verankert betrieben. An den gesetzlichen Grundlagen hat sich im Verlaufe der letzten Jahre nichts verändert. Auf kantonaler Stufe soll im Jahr 2024 die Konzeption «GRAL» (Gesundheits- und Rettungswesen in ausserordentlichen Lagen) unter der Leitung des Kantonsarztamtes überprüft werden.

Die Stadtpräsidentin:
Maria Pappa

Der Stadtschreiber-Stellvertreter:
Andy Markwalder

Beilage:
- Einfache Anfrage vom 5. Juni 2024