1 05/2026

Interpellation betr. strategischem Handlungsbedarf bei der Cybersicherheit der Stadt Thun

Mathias Berger (SVP) und SVP-Fraktion

Fragen

Der Gemeinderat wird gebeten, zur Cybersicherheit der Stadt Thun folgende Fragen zu beantworten:

1. Lagebeurteilung und konkrete Betroffenheit

- Wie beurteilt der Gemeinderat die aktuelle Bedrohungslage für die Stadt Thun im Vergleich zu anderen Schweizer Städten und Gemeinden?
- Gab es in den letzten fünf Jahren konkrete Cybervorfälle, Angriffsversuche oder sicherheitsrelevante Ereignisse innerhalb der Stadtverwaltung oder bei beauftragten IT-Dienstleistern?

2. Risikoanalyse

- Liegt für die Stadt Thun eine systematische Risikoanalyse im Bereich Cybersecurity vor (z. B. Risiko von Ransomware, Datenabfluss, Systemausfall)?
- Welche Szenarien werden als kritisch eingestuft (z. B. Totalausfall der Verwaltung, Verlust sensibler Daten, längerer Ausfall von Online-Diensten)?
- Welche potenziellen Schäden (finanziell, operativ, reputativ) werden dabei angenommen?

3. Kosten und finanzielle Auswirkungen

- Welche direkten und indirekten Kosten wären im Falle eines grösseren Cyberangriffs auf die Stadt Thun zu erwarten (z. B. Betriebsunterbruch, Wiederherstellung, externe Spezialisten, Kommunikationsmassnahmen)?
- Gibt es Schätzungen oder Szenarien auf Basis vergleichbarer Vorfälle in anderen Gemeinden?
- Verfügt die Stadt über eine Cyberversicherung, und wenn ja, in welchem Umfang sind Schäden gedeckt?

4. Aktuelles Budget und Ressourcen

- Wie hoch ist das aktuelle jährliche Budget der Stadt Thun für IT-Sicherheit (inkl. Personal, Infrastruktur und externe Dienstleistungen)?
- Wie hat sich dieses Budget in den letzten fünf Jahren entwickelt?
- Wie viele Vollzeitstellen (oder Stellenprozente) sind explizit für Cybersecurity bzw. Informationssicherheit vorgesehen (auch allf. externe Beauftragte)?

5. Schutzmassnahmen

- Welche konkreten technischen und organisatorischen Massnahmen sind implementiert (z. B. Multi-Faktor-Authentifizierung, Netzwerksegmentierung, regelmässige Backups, Patch-Management, Schulungen und Überprüfung der Mitarbeitenden)?
- Werden anerkannte Standards oder Frameworks angewendet (z. B. ISO 27001, NIST)?

6. Erkennung und Reaktion

- Wie werden sicherheitsrelevante Ereignisse erkannt (Monitoring, Logging, Security Operations Center etc.)?
- Existiert ein Incident-Response-Plan, und wurde dieser in den letzten Jahren praktisch getestet (z. B. durch Übungen, Externe)?

7. Abhängigkeiten und Drittparteien

- Welche kritischen IT-Dienstleistungen sind an externe Anbieter ausgelagert?
- Wie wird sichergestellt, dass auch diese Anbieter angemessene Sicherheitsstandards einhalten?

8. Datenschutz

- Wie wird der Schutz besonders sensibler Personendaten (z. B. Sozialdienste, Einwohnerregister) gewährleistet?
- Welche Prozesse bestehen im Falle eines Datenabflusses hinsichtlich Information der Betroffenen und Öffentlichkeit?

9. Strategische Weiterentwicklung

- Welche zusätzlichen Massnahmen sind geplant, um die Cyberresilienz der Stadt Thun in den kommenden Jahren zu stärken?
- Ist eine Erhöhung der finanziellen und personellen Ressourcen im Bereich Cybersicherheit vorgesehen?

Begründung

Cyberangriffe auf Schweizer Städte und Gemeinden haben in den letzten Jahren deutlich zugenommen. Aktuelle Beispiele zeigen die konkrete Bedrohungslage:

- Villars-sur-Glâne (FR, 2025): Unautorisierte Zugriffe auf Gemeindeserver führten dazu, dass zentrale Systeme mehrere Tage abgeschaltet werden mussten; der Verwaltungsbetrieb war stark eingeschränkt.
- Schweizweite Angriffe auf Behörden (2025): DDoS-Angriffe legten wiederholt Websites und Online-Dienste von Verwaltungen lahm.
- Zollikofen (BE, 2023): Ransomware-Angriff führte zu einem weitgehenden Stillstand der Verwaltung und verursachte Kosten im sechsstelligen Bereich.
- Kanton Bern – DDoS-Angriffe auf zentrale Dienste (2024) Fall: Betroffen unter anderem die Online-Steuererklärung.
- Kantonspolizei Bern – Datenabfluss (2023): Fall: Sicherheitslücke in Mobile-App, Daten von ca. 2'800 Mitarbeitenden abgeflossen

Diese Vorfälle verdeutlichen, dass Cyberangriffe nicht nur theoretische Risiken darstellen, sondern zu konkreten Betriebsunterbrüchen, erheblichen Kosten oder erheblichen Datenschutzverletzungen führen können. Gleichzeitig zeigt die aktuelle Lage, dass öffentliche Verwaltungen zunehmend ins Visier geraten: Rund die Hälfte aller Cyberangriffe sind finanziell motiviert (z. B. Ransomware), wobei gezielt Daten abgegriffen und für Erpressung genutzt werden.

Die Stadt Thun betreibt zahlreiche kritische Informatiksysteme mit sensiblen Personendaten und ist in hohem Masse von deren Verfügbarkeit abhängig. Die zunehmende Digitalisierung der Verwaltung führt zu einer wachsenden Abhängigkeit von funktionierenden IT-Systemen. Gleichzeitig zeigen konkrete Vorfälle in der Schweiz, dass Cyberangriffe zu erheblichen finanziellen Schäden, Betriebsunterbrüchen und Datenschutzverletzungen führen können.

Eine transparente Darstellung der Risiken, Kosten und Massnahmen ist notwendig, um die Handlungsfähigkeit der Stadtverwaltung sowie den Schutz der Bevölkerung nachhaltig sicherzustellen.

Thun, 26.3.2026

(Mathias Berger) (Peter Aegerter)

Dringlichkeit: wird verlangt ☐ ja ☒ nein