STADT THUN

GEMEINDERAT

Rathausplatz 1, 3600 Thun
Telefon 033 225 82 20
gemeinderat@thun.ch

thun.ch

Stadtratssitzung vom 17. September 2026

Interpellation I 05/2026

Interpellation betreffend strategischen Handlungsbedarf bei der Cybersicherheit der Stadt Thun

Mathias Berger (SVP) und Fraktion SVP vom 26. März 2026; Beantwortung

Wortlaut der Interpellation

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

1. Lagebeurteilung und konkrete Betroffenheit
   - 1.1 Wie beurteilt der Gemeinderat die aktuelle Bedrohungslage für die Stadt Thun im Vergleich zu anderen Schweizer Städten und Gemeinden?
   - 1.2 Gab es in den letzten fünf Jahren konkrete Cybervorfälle, Angriffsversuche oder sicherheitsrelevante Ereignisse innerhalb der Stadtverwaltung oder bei beauftragten IT-Dienstleistern?
2. Risikoanalyse
   - 2.1 Liegt für die Stadt Thun eine systematische Risikoanalyse im Bereich Cybersecurity vor (z. B. Risiko von Ransomware, Datenabfluss, Systemausfall)?
   - 2.2 Welche Szenarien werden als kritisch eingestuft (z. B. Totalausfall der Verwaltung, Verlust sensibler Daten, längerer Ausfall von Online-Diensten)?
   - 2.3 Welche potenziellen Schäden (finanziell, operativ, reputativ) werden dabei angenommen?
3. Kosten und finanzielle Auswirkungen
   - 3.1 Welche direkten und indirekten Kosten wären im Falle eines grösseren Cyberangriffs auf die Stadt Thun zu erwarten (z. B. Betriebsunterbruch, Wiederherstellung, externe Spezialisten, Kommunikationsmassnahmen)?
   - 3.2 Gibt es Schätzungen oder Szenarien auf Basis vergleichbarer Vorfälle in anderen Gemeinden?
   - 3.3 Verfügt die Stadt über eine Cyberversicherung, und wenn ja, in welchem Umfang sind Schäden gedeckt?
4. Aktuelles Budget und Ressourcen
   - 4.1 Wie hoch ist das aktuelle jährliche Budget der Stadt Thun für IT-Sicherheit (inkl. Personal, Infrastruktur und externe Dienstleistungen)?
   - 4.2 Wie hat sich dieses Budget in den letzten fünf Jahren entwickelt?
   - 4.3 Wie viele Vollzeitstellen (oder Stellenprozente) sind explizit für Cybersecurity bzw. Informationssicherheit vorgesehen (auch allf. externe Beauftragte)?
5. Schutzmassnahmen
   - 5.1 Welche konkreten technischen und organisatorischen Massnahmen sind implementiert (z. B. Multi-Faktor-Authentifizierung, Netzwerksegmentierung, regelmässige Backups, Patch-Management, Schulungen und Überprüfung der Mitarbeitenden)?

STADT THUN

5.2 Werden anerkannte Standards oder Frameworks angewendet (z. B. ISO 27001, NIST)?
6. Erkennung und Reaktion
   6.1 Wie werden sicherheitsrelevante Ereignisse erkannt (Monitoring, Logging, Security Operations Center etc.)?
   6.2 Existiert ein Incident-Response-Plan, und wurde dieser in den letzten Jahren praktisch getestet (z. B. durch Übungen, Externe)?
7. Abhängigkeiten und Drittparteien
   7.1 Welche kritischen IT-Dienstleistungen sind an externe Anbieter ausgelagert?
   7.2 Wie wird sichergestellt, dass auch diese Anbieter angemessene Sicherheitsstandards einhalten?
8. Datenschutz
   8.1 Wie wird der Schutz besonders sensibler Personendaten (z. B. Sozialdienste, Einwohnerregister) gewährleistet?
   8.2 Welche Prozesse bestehen im Falle eines Datenabflusses hinsichtlich Information der Betroffenen und Öffentlichkeit?
9. Strategische Weiterentwicklung
   9.1 Welche zusätzlichen Massnahmen sind geplant, um die Cyberresilienz der Stadt Thun in den kommenden Jahren zu stärken?
   9.2 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 zei-

STADT THUN

gen konkrete Vorfälle in der Schweiz, dass Cyberangriffe zu erheblichen finanziellen Schäden, Betriebsunterbrüchen und Datenschutzverletzungen führen können.

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

Antwort des Gemeinderates

Zu Frage 1: Lagebeurteilung und konkrete Betroffenheit

1.1 Wie beurteilt der Gemeinderat die aktuelle Bedrohungslage für die Stadt Thun im Vergleich zu anderen Schweizer Städten und Gemeinden?

Cyberbedrohungen betreffen alle Gemeinden und Städte in ähnlicher Weise, da Angriffe meist opportunistisch erfolgen. Unterschiede ergeben sich aufgrund der Grösse einer Gemeinde/Stadt, des Grads der Digitalisierung (E-Government-Angebot) und der Relevanz der erbrachten Dienstleistungen (z. B. Energie-/Wasserversorgung, Verkehrsbetriebe, Sozialdienste).

Die Stadt Thun ist im Vergleich zu international bekannteren Schweizer Städten wie Bern, Zürich oder Genf global weniger sichtbar und deshalb tendenziell weniger ein Ziel für politisch motivierte Cyberangriffe.

Die konkreten Bedrohungen lassen sich aufgrund der Häufigkeit und des potenziellen Schadens wie folgt unterteilen:

1. Hohe Häufigkeit, tiefer Schaden: Hierzu gehören die verschiedenen Ausprägungen von Phishing und Betrugsversuchen.
2. Mittlere Häufigkeit, mittlerer Schaden: Überlastangriffe (DDoS), Befall einzelner Geräte mit Schadsoftware durch Ausnützen von Schwachstellen oder durch Social Engineering.
3. Tiefe Häufigkeit, hoher Schaden: Ransomware und Datenabfluss

Schnell verändern kann sich die Bedrohungslage in Bezug auf Hacktivisten und ausländische staatliche Akteure. Dies kann dann der Fall sein, wenn sich die Stadt Thun in einem internationalen Konflikt (z. B. RUS-UKR, ISR/USA–IRN) mit Hilfsgütern, politischen Beschlüssen oder ähnlichen Handlungen öffentlich auf die Seite einer der Konfliktparteien stellt. In solchen Fällen kann es sein, dass die nicht unterstützte Konfliktpartei oder Hacktivisten mit Cyberangriffen (häufig Überlastangriffe/DDoS) reagieren.

1.2 Gab es in den letzten fünf Jahren konkrete Cybervorfälle, Angriffsversuche oder sicherheitsrelevante Ereignisse innerhalb der Stadtverwaltung oder bei beauftragten IT-Dienstleistern?

Grundsätzlich ist festzuhalten, dass alle ans Internet angebundenen Systeme fortlaufend automatisierten Angriffsversuchen ausgesetzt sind. Auch die Stadtverwaltung Thun ist hiervon betroffen.

Die eingesetzten Sicherheitssysteme blockieren monatlich rund 13 Millionen unerwünschte Netzwerkverbindungen sowie etwa 240'000 E-Mails, die als Spam oder potenziell schädlich eingestuft

STADT THUN

werden. Dabei handelt es sich überwiegend um automatisierte, unspezifische Angriffe ohne direkten Bezug zur Stadt Thun.

In den letzten fünf Jahren kam es vereinzelt zu sicherheitsrelevanten Ereignissen, die jedoch frühzeitig erkannt und ohne nachhaltige Auswirkungen eingedämmt werden konnten. Es sind keine Fälle bekannt, bei denen ein signifikanter Schaden oder ein umfassender Abfluss von Daten entstanden ist.

Ein meldepflichtiger Vorfall ereignete sich im Dezember 2025 und wurde gemäss den Vorgaben an das Nationale Zentrum für Cybersicherheit (NCSC) gemeldet. Dabei wurde ein Serversystem über eine zum damaligen Zeitpunkt unbekannte Schwachstelle (sog. Zero-Day-Lücke) angegriffen. Nach aktuellem Kenntnisstand beschränkte sich der Angriff auf einen initialen Zugriff. Weitergehende, bösartige Aktivitäten oder eine Ausbreitung auf andere Systeme konnten nicht festgestellt werden.

Der Vorfall wurde umgehend analysiert und die notwendigen Massnahmen zur Behebung und zur weiteren Härtung der Systeme wurden zeitnah umgesetzt.

Zu Frage 2: Risikoanalyse

2.1 Liegt für die Stadt Thun eine systematische Risikoanalyse im Bereich Cybersecurity vor (z. B. Risiko von Ransomware, Datenabfluss, Systemausfall)?

Für das interne Kontrollsystem der Finanzverwaltung (IKS) führen die Informatikdienste (IDT) Risiken mit Bezug zu Cybersicherheit und Datenschutz auf.

Risikoanalysen werden für kritische Systeme und Plattformen durchgeführt, wenn eine Risikoanalyse in der obligatorischen Schutzbedarfsanalyse als notwendig angezeigt wird. Darin werden konkrete Sicherheitskonzepte und Massnahmen definiert, deren Umsetzung zwingend ist.

Ergänzend dazu ist derzeit der Aufbau eines umfassenden Managementsystems für Informationssicherheit (ISMS) nach ISO 27001 in Bearbeitung. Ziel ist die Vereinheitlichung der bestehenden Risikoanalysen, deren systematische Ausweitung auf die gesamte IT-Infrastruktur sowie die weitere organisatorische Stärkung der städtischen Informationssicherheit.

2.2 Welche Szenarien werden als kritisch eingestuft (z. B. Totalausfall der Verwaltung, Verlust sensibler Daten, längerer Ausfall von Online-Diensten)?

Auf Basis der bestehenden Schutzbedarfs- und Betriebsanalysen sowie der bekannten IT-Architektur werden folgende Szenarien als kritisch eingestuft:

- Ausfall zentraler IT-Infrastrukturen wie Storage- und Firewall-Systeme, das Kommunikationsnetzwerk oder die zentrale Benutzer- und Berechtigungsverwaltung,
- Ausfall oder starke Beeinträchtigung von Kernapplikationen der Stadtverwaltung,
- Ransomware-Angriffe mit Verschlüsselung grosser Datenbestände sowie anschliessenden Erpressungsversuchen,
- unbefugter Abfluss sensibler oder umfangreicher Daten aus den Kernapplikationen.

STADT THUN

Eine abschliessende Priorisierung der Massnahmen aufgrund einer konsolidierten Gesamt-Risikoanalyse liegt derzeit noch nicht in finalisierter Form vor und ist Bestandteil des laufenden Aufbaus des Informationssicherheitsmanagementsystems.

2.3 Welche potenziellen Schäden (finanziell, operativ, reputativ) werden dabei angenommen?

Aufgrund der bekannten Abhängigkeiten in der städtischen IT-Infrastruktur lassen sich die Grössenordnungen der möglichen Auswirkungen wie folgt umschreiben:

- *Operative Schäden:* Bei einem Ausfall zentraler IT-Systeme ist mit erheblichen Einschränkungen des Verwaltungsbetriebs zu rechnen. Dies kann zu einem weitgehenden Produktivitätsverlust führen, bis Systeme wiederhergestellt oder ersatzweise betrieben werden können. Die Dauer solcher Wiederherstellungen kann je nach Ausmass mehrere Tage bis Wochen dauern.
- *Finanzielle Schäden:* Neben dem operativen Ausfall entstehen Kosten insbesondere durch externe IT-Spezialistinnen und -spezialisten, Wiederherstellung von Systemen sowie allfällige Notfallmassnahmen. In einem schweren Szenario können sich diese Kosten insgesamt auf einen mittleren bis höheren sechsstelligen Betrag belaufen. Zusätzlich ist mit erheblichen, indirekten Kosten durch Betriebsunterbruch zu rechnen.
- *Reputationsschäden:* Reputative Auswirkungen sind naturgemäss schwer quantifizierbar. Sie können sich insbesondere in einem Vertrauensverlust der Bevölkerung gegenüber dem Gemeinderat und der Stadtverwaltung, erhöhter medialer Aufmerksamkeit sowie politischen und organisatorischen Konsequenzen manifestieren.

Im Worst-Case-Szenario eines vollständigen Verschlüsselungs- und Erpressungsangriffs (Ransomware) ist von einer mehrwöchigen Beeinträchtigung des Verwaltungsbetriebs auszugehen, verbunden mit entsprechend hohen operativen und finanziellen Gesamtauswirkungen.

Zu Frage 3: Kosten und finanzielle Auswirkungen

3.1 Welche direkten und indirekten Kosten wären im Falle eines grösseren Cyberangriffs auf die Stadt Thun zu erwarten (z. B. Betriebsunterbruch, Wiederherstellung, externe Spezialisten, Kommunikationsmassnahmen)?

Die Kosten eines Cyberangriffs auf die Stadtverwaltung Thun hängen stark vom konkreten Szenario, dem Ausmass der Beeinträchtigung sowie der Dauer des Betriebsunterbruchs ab. Eine exakte Voraussage ist daher nicht möglich.

Die direkten und indirekten Kosten lassen sich in folgende Kategorien einteilen:

- *Betriebsunterbruch:* Kosten aufgrund eingeschränkter oder nicht verfügbarer Verwaltungsleistungen sowie des resultierenden Produktivitätsverlusts,
- *Wiederherstellung:* Aufwände für die Wiederherstellung oder Neuinstallation von Systemen und Daten,
- *Externe Spezialisten:* Support externer Cybersecurity-Dienstleister für die IT-Forensik und Wiederherstellung,

STADT THUN

- *Kommunikation und Krisenmanagement: rechtliche Abklärungen, Unterstützung im Krisenstab, interne und externe Kommunikation.*

Cybervorfälle im öffentlichen Sektor können Schätzungen von Cybersecurity and Infrastructure Security Agency (CISA) mit Sitz in Arlington, Virginia (USA), zufolge je nach Ausmass im Bereich eines tiefen sechs- bis siebenstelligen Betrags liegen. Diese Werte sind als grobe Orientierungsgrössen zu verstehen.

3.2 Gibt es Schätzungen oder Szenarien auf Basis vergleichbarer Vorfälle in anderen Gemeinden?

Direkt vergleichbare und übertragbare Kostenangaben aus anderen Schweizer Städten/Gemeinden sind der IDT nicht bekannt. Cybervorfälle hängen sehr stark von den jeweiligen Rahmenbedingungen ab (Grösse der betroffenen Organisation, Digitalisierungsgrad, IT-Architektur, vorhandene Notfallprozesse und Schutzmassnahmen) und werden nur sehr selten in einer standardisierten Form öffentlich ausgewiesen. Aufgrund dieser Tatsache sind direkte Vergleiche zwischen Städten/Gemeinden nur eingeschränkt aussagekräftig.

3.3 Verfügt die Stadt über eine Cyberversicherung, und wenn ja, in welchem Umfang sind Schäden gedeckt?

Die Stadtverwaltung Thun verfügt über eine Datenversicherung. Diese deckt insbesondere den internen Aufwand (Arbeitsstunden) zur Wiederherstellung von Systemen und Daten nach einem Schadenereignis ab.

Zu Frage 4: Aktuelles Budget und Ressourcen

4.1 Wie hoch ist das aktuelle jährliche Budget der Stadt Thun für IT-Sicherheit (inkl. Personal, Infrastruktur und externe Dienstleistungen)?

Die Informatikdienste der Stadtverwaltung Thun führen kein separates, isoliertes Budget für IT-Sicherheit. Die entsprechenden Aufwände sind integraler Bestandteil der gesamten IT-Leistungen und werden über verschiedene Produkte und Organisationseinheiten erbracht.

Die Aufwendungen für IT-Sicherheit umfassen insbesondere:

- technische Schutzmassnahmen (Netzwerk- und Systemschutz, E-Mail-Sicherheit, Server- und Endgeräteschutz),
- organisatorische Sicherheitsmassnahmen (wie Administrations- und Berechtigungskonzept),
- Datensicherung und Wiederherstellungsmechanismen,
- Sensibilisierung und Schulung der Mitarbeitenden (z. B. Phishing Simulationen),
- personelle Ressourcen (CISO, Security Engineers),
- externe Dienstleistungen (spezialisierte Security-Analysen und Härtungsmassnahmen – Penetrationstests).

Die daraus resultierenden jährlichen Gesamtkosten für die IT-Sicherheit betragen rund 1,2 Millio-

STADT THUN

nen Franken – dies sind im Jahr 2026 etwa 13,3 Prozent des IT-Budgets.

Aufgrund der zunehmenden Bedrohungslage wird die Weiterentwicklung der IT-Sicherheitsmassnahmen laufend überprüft und bei Bedarf angepasst. Aktuell wird ein Beschaffungsverfahren für Security-Operations-Center (SOC) Dienstleistungen vorbereitet, um die Fähigkeiten in Bezug auf die Überwachung von und die Reaktion auf Cybervorfälle gezielt weiter zu stärken.

4.2 Wie hat sich dieses Budget in den letzten fünf Jahren entwickelt?

Die Aufwände im IT-Budget der Stadtverwaltung Thun sind im Zeitraum von 2021 bis 2026 von rund 7,2 Millionen Franken auf rund 9,0 Millionen Franken angestiegen. Dies sind die Gesamtkosten inkl. Leistungen für andere Gemeinden, die kostendeckend entschädigt werden.

Der Anteil der Aufwendungen für IT-Sicherheit hat sich im gleichen Zeitraum überproportional entwickelt und mehr als verdoppelt. Diese Entwicklung ist insbesondere auf den gezielten Ausbau personeller Ressourcen im Bereich IT-Security (CISO, IT-Security Engineer), die Durchführung von Sicherheitsprüfungen (Penetrationstests) sowie verstärkte Investitionen in Sensibilisierung und Schulung der Mitarbeitenden zurückzuführen.

4.3 Wie viele Vollzeitstellen (oder Stellenprozente) sind explizit für Cybersecurity bzw. Informationssicherheit vorgesehen (auch allf. externe Beauftragte)?

Der gesamte Stellenetat im IT-Bereich der Stadtverwaltung Thun beträgt 3'090 Stellenprozente.

Für den Bereich Cybersecurity bzw. Informationssicherheit sind derzeit zwei Vollzeitstellen explizit ausgewiesen (CISO und IT-Security Engineer). Darüber hinaus werden IT-Sicherheitsaufgaben auch durch Mitarbeitende in verschiedenen IT-Fachbereichen (insbesondere Netzwerk, Cloud, Client- und Server-Betrieb) wahrgenommen. Diese Leistungen sind integraler Bestandteil des jeweiligen Betriebs und werden nicht separat als dedizierte Stellenprozente für IT-Sicherheit geführt.

Ergänzend werden bei Bedarf externe Fachspezialisten für spezifische Fragestellungen und Projekte im Bereich IT-Sicherheit beigezogen.

Insgesamt ergibt sich damit ein kombinierter Ressourceneinsatz aus dedizierten und anteiligen Stellen sowie externen Leistungen, wobei eine exakte Quantifizierung der anteiligen Aufwände nur eingeschränkt möglich ist. Aufgrund grober Schätzung kann davon ausgegangen werden, dass ein mittlerer zweistelliger Porzentsatz der IT-Personalkapazitäten in IT-Sicherheitsaufgaben fliesst.

Zu Frage 5: Schutzmassnahmen

5.1 Welche konkreten technischen und organisatorischen Massnahmen sind implementiert (z. B. Multi-Faktor-Authentifizierung, Netzwerksegmentierung, regelmässige Backups, Patch-Management, Schulungen und Überprüfung der Mitarbeitenden)?

Die Stadtverwaltung Thun setzt eine Vielzahl technischer und organisatorischer Massnahmen zur Gewährleistung der IT-Sicherheit um. Darunter befinden sich unter anderem die in der Frage er-

STADT THUN

wähnten Massnahmen. Aus Sicherheitsgründen werden keine detaillierten Angaben zu einzelnen Schutzmechanismen und deren konkreter Ausgestaltung öffentlich gemacht, da dies potenziell Rückschlüsse auf die Sicherheitsarchitektur ermöglichen würde.

Die konkreten Ausprägungen und Weiterentwicklungen dieser Massnahmen können bei Bedarf in der Sachkommission Finanzen Ressourcen Umwelt vertieft erläutert werden.

5.2 Werden anerkannte Standards oder Frameworks angewendet (z. B. ISO 27001, NIST)?

Im Bereich des Informationssicherheitsmanagements orientieren sich die Informatikdienste der Stadt Thun an den Grundsätzen und den Kontrollzielen der ISO/IEC 27001.

Auf technischer Ebene werden international anerkannte Sicherheitsstandards und Best Practices angewendet. Dazu gehören insbesondere die CIS Controls, plattformspezifische Sicherheitsvorgaben (z. B. Microsoft Security Baselines) sowie der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Die angewendeten Standards und Massnahmen werden regelmässig überprüft und im Rahmen der kontinuierlichen Weiterentwicklung der IT-Sicherheit angepasst.

Zu Frage 6: Erkennung und Reaktion

6.1 Wie werden sicherheitsrelevante Ereignisse erkannt (Monitoring, Logging, Security Operations Center etc.)?

Die Stadtverwaltung Thun setzt verschiedene technische und organisatorische Massnahmen ein, um sicherheitsrelevante Ereignisse frühzeitig zu erkennen. Dazu gehören ein zentrales Monitoring sowie system- und applikationsspezifische Logging- und Überwachungslösungen. Ergänzend werden Sicherheitskomponenten auf Netzwerk- und Endpunktebene zur Erkennung verdächtiger Aktivitäten eingesetzt. Zudem werden sicherheitsrelevante Benutzeraktivitäten überwacht und protokolliert.

Eine detaillierte Beschreibung einzelner sicherheitskritischer Konfigurationen erfolgt aus Sicherheitsgründen nicht öffentlich, kann jedoch in der Sachkommission Finanzen Ressourcen Umwelt erläutert werden.

6.2 Existiert ein Incident-Response-Plan, und wurde dieser in den letzten Jahren praktisch getestet (z. B. durch Übungen, Externe)?

Die Stadtverwaltung Thun verfügt über definierte Reaktionsprozesse für sicherheitsrelevante Ereignisse und Cybervorfälle. Diese Prozesse regeln insbesondere Erkennung, Eskalation, Koordination sowie Wiederherstellung des Normalbetriebs im Ereignisfall. Für sehr grosse Vorfälle, bei denen grosse Teile der IT-Infrastruktur nicht mehr verfügbar wären, wurden durch Business-Continuity-Management-Arbeiten vitale Aufgaben identifiziert und Ersatzprozesse definiert und trainiert, die auch ohne digitale Infrastruktur funktionieren.

STADT THUN

Die bestehenden Prozesse werden regelmässig überprüft und weiterentwickelt.

Praktische Überprüfungen einzelner Teilaspekte erfolgen insbesondere im Zusammenhang mit regelmässigen Wiederherstellungstests der gesicherten Daten und Systeme. Diese dienen gleichzeitig als wichtiger Bestandteil der Sicherstellung der Handlungsfähigkeit im Ereignisfall.

Eine weitergehende systematische Weiterentwicklung eines umfassenden Incident-Response-Frameworks sowie dessen vertiefte Operationalisierung ist vorgesehen und soll im Zusammenhang mit der geplanten Einführung bzw. Evaluation eines Security-Operations-Center-(SOC)-Dienstes weiter konkretisiert und abgestimmt werden.

Detaillierte Angaben zu operativen Abläufen und sicherheitskritischen Reaktionsmechanismen werden aus Sicherheitsgründen nicht öffentlich gemacht, können jedoch in der Sachkommission Finanzen Ressourcen Umwelt erläutert werden.

Zu Frage 7: Abhängigkeiten und Drittparteien

7.1 Welche kritischen IT-Dienstleistungen sind an externe Anbieter ausgelagert?

Die Stadtverwaltung Thun betreibt die kritischen IT-Grundlagen sowie zentrale Kernsysteme grundsätzlich in eigener Verantwortung und auf eigener Infrastruktur. Dazu zählen insbesondere Netzwerk- und Sicherheitsinfrastruktur sowie wesentliche Fachanwendungen wie das Einwohnerregister und das Geschäftsverwaltungssystem.

Für den Betrieb und den Unterhalt einzelner Kernapplikationen werden ausgewählte externe Anbieterinnen und Anbieter im Rahmen von Wartungs- und Supportleistungen beigezogen. Diese erhalten dabei kontrollierte, rollenbasierte und zeitlich eingeschränkte Zugriffsrechte. Jede zugriffsberechtigte Person ist verpflichtet, die von der Stadtverwaltung Thun vorgegebenen, schriftlich festgehaltenen Zusammenarbeits- und Sicherheitsvereinbarungen zu akzeptieren. Für die Einhaltung dieser Vorgaben wird eine schriftliche Bestätigung (Unterzeichnung der entsprechenden Vereinbarung) eingeholt.

Einzelne IT-Dienstleistungen sind an externe Anbieterinnen oder Anbieter ausgelagert, insbesondere:

- das IT-Ticketing-System, welches bei einem externen Anbieter in einem Rechenzentrum in der Schweiz betrieben wird,
- bestimmte Cloud-basierte Basisdienste im Bereich Identitäts- und Zugriffsmanagement (z. B. Microsoft Entra ID zur Authentifizierung und Benutzerverwaltung).

Zudem werden Cloud- und Kollaborationsdienste schrittweise ergänzt bzw. erweitert (u. a. Microsoft 365), wobei der Zugriff und die Nutzung über zentrale Identitäts- und Sicherheitsmechanismen gesteuert werden.

Die Stadtverwaltung Thun stellt dabei sicher, dass die Kontrolle über kritische Systeme, Daten und Zugriffsrechte jederzeit bei der internen IT-Organisation verbleibt und externe Dienstleisterinnen

STADT THUN

und Dienstleister nur im definierten und überwachten Rahmen tätig sind.

7.2 Wie wird sichergestellt, dass auch diese Anbieter angemessene Sicherheitsstandards einhalten?

Die Stadtverwaltung Thun stellt sicher, dass externe Anbieterinnen und Anbieter angemessene Sicherheitsstandards einhalten, indem der Zugriff auf städtische Systeme ausschliesslich auf Basis vertraglich und organisatorisch definierter Vorgaben erfolgt.

Grundlage bilden schriftlich festgehaltene Zusammenarbeits-, Sicherheits- und Datenschutzvereinbarungen, welche von den jeweiligen Unternehmen resp. von den innerhalb dieser Organisationen zugriffsberechtigten Mitarbeitenden zu akzeptieren und zu unterzeichnen sind.

Diese Vereinbarungen regeln insbesondere Anforderungen in Bezug auf Vertraulichkeit, Zugriffsschutz und sichere Datenverarbeitung sowie den Umgang mit städtischen Informationen und Systemen.

Zugriffsrechte werden zudem nach dem Need-to-know- und Least-Privilege-Prinzip vergeben, rollenbasiert und zeitlich begrenzt.

Die Einhaltung der Vorgaben wird durch technische Zugriffskontrollen, Protokollierung sicherheitsrelevanter Aktivitäten sowie regelmässige Überprüfung der Berechtigungen unterstützt.

Externe Dienstleisterinnen und Dienstleister werden insbesondere im Rahmen öffentlich-rechtlicher Ausschreibungsverfahren nach internen Sicherheitsanforderungen und etablierten Standards ausgewählt und beurteilt, wobei sicherheitsrelevante Eignungs- und Zuschlagskriterien berücksichtigt werden.

Zu Frage 8: Datenschutz

8.1 Wie wird der Schutz besonders sensibler Personendaten (z. B. Sozialdienste, Einwohnerregister) gewährleistet?

Der Schutz besonders schützenswerter Personendaten (z. B. im Bereich Sozialdienste oder Einwohnerregister) erfolgt auf den Vorgaben des kantonalen Datenschutzrechts (KDSG) sowie der entsprechenden datenschutzrechtlichen Aufsicht durch den Datenschutzbeauftragten der Stadt Thun.

Für Systeme, in denen solche Daten bearbeitet werden, wird jeweils ein Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) erstellt bzw. angewendet. Dieses dient dazu, Risiken systematisch zu erfassen, angemessene technische und organisatorische Schutzmassnahmen zu definieren sowie verbleibende Restrisiken nachvollziehbar zu dokumentieren.

Der Schutz dieser Daten wird insbesondere durch geeignete technische und organisatorische Massnahmen gewährleistet, wie etwa Zugriffsbeschränkungen nach dem Need-to-know-Prinzip, rollenbasierte Berechtigungskonzepte, Protokollierung von Zugriffen sowie Einsatz gesicherter und kontrollierter Systemumgebungen.

STADT THUN

Besonders schützenswerte Personendaten werden nur in geprüften, besonders geschützten Systemumgebungen verarbeitet.

Die Umsetzung und die Einhaltung dieser Vorgaben werden regelmässig überprüft (mind. alle fünf Jahre) und im Rahmen der kontinuierlichen Weiterentwicklung der IT-Sicherheits- und Datenschutzmassnahmen sichergestellt.

8.2 Welche Prozesse bestehen im Falle eines Datenabflusses hinsichtlich Information der Betroffenen und Öffentlichkeit?

Im Falle eines Cybervorfalls bestehen definierte interne Prozesse zur Beurteilung, Eindämmung und Bearbeitung des Ereignisses. Die Einbindung der relevanten internen Fachstellen (Informatikdienste, Rechtsdienst, Stadtmarketing und Kommunikation) sowie – je nach Art und Umfang des Ereignisses – der Beizug und/oder die Information externer Fachstellen und Behörden (Datenschutzbeauftragter, Bundesamt für Cybersicherheit, Strafverfolgungsbehörden) erfolgen lageabhängig.

Die Information der betroffenen Personen sowie der Öffentlichkeit erfolgt unter Einbezug der genannten Stellen und richtet sich nach den jeweils anwendbaren rechtlichen Vorgaben und Meldepflichten.

Die weitergehende formalisierte Ausarbeitung und Dokumentation der Kommunikationsprozesse werden im Rahmen der laufenden Weiterentwicklung des Informationssicherheits- und Incident-Managements weiter präzisiert.

Zu Frage 9: Strategische Weiterentwicklung

9.1 Welche zusätzlichen Massnahmen sind geplant, um die Cyberresilienz der Stadt Thun in den kommenden Jahren zu stärken?

Die Stärkung der Cyberresilienz hat innerhalb der Stadt Thun eine hohe Priorität und wird kontinuierlich weiterentwickelt. Mit der Schaffung und Besetzung einer CISO-Stelle sowie der Anstellung eines IT-Security Engineers wurden in den letzten Jahren bereits wesentliche organisatorische und strukturelle Grundlagen geschaffen.

Für die kommenden Jahre sind insbesondere folgende Weiterentwicklungen vorgesehen:

- Aufbau bzw. Einbezug eines Security-Operations-Center-(SOC)-Dienstleisters zur kontinuierlichen Überwachung der IT-Systeme sowie zur verbesserten Reaktionsfähigkeit bei sicherheitsrelevanten Ereignissen. Im Aufgaben- und Finanzplan 2026-2029 wurde im Februar 2025 ein Betrag für das Projekt "Security Operation Center" eingestellt.
- Weiterer Ausbau der technischen Sicherheitsmassnahmen zur frühzeitigen Erkennung und Abwehr von Cyberangriffen.
- Regelmässige Durchführung von Sicherheitsüberprüfungen (z. B. Penetrationstests) zur Identifikation und Behebung von Schwachstellen.

STADT THUN

- Weiterentwicklung der organisatorischen Prozesse im Bereich Incident Response und Krisenmanagement.
- Fortführung und Ausbau von Sensibilisierungs- und Schulungsmassnahmen für Mitarbeitende. Die Schulungsmassnahmen werden unter anderem durch die Einführung eines Learning Management Systems (LMS) ausgebaut, in welchem die Mitarbeitenden selbstständig obligatorische Cybersicherheitsschulungen absolvieren werden.
- Schrittweiser Ausbau eines Managementsystem für Informationssicherheit (ISMS) nach ISO 27001 zur nachhaltigen und systematischen Steuerung der Informationssicherheit.

Die geplanten Massnahmen orientieren sich an der aktuellen Bedrohungslage sowie an etablierten Standards und Best Practices und werden im Rahmen der strategischen Weiterentwicklung der IT-Sicherheit schrittweise umgesetzt. Zusätzliche Massnahmen werden kontinuierlich geprüft und umgesetzt.

9.2 Ist eine Erhöhung der finanziellen und personellen Ressourcen im Bereich Cybersicherheit vorgesehen?

Die Anforderungen im Bereich Cybersicherheit haben in den letzten Jahren deutlich zugenommen und werden sich voraussichtlich weiter erhöhen. Um dieser Entwicklung gerecht zu werden, ist eine gezielte Weiterentwicklung der finanziellen und der personellen Ressourcen vorgesehen.

Mit der geplanten Einführung bzw. dem Einbezug eines Security-Operations-Center-(SOC)-Dienstes ist insbesondere im Bereich der externen Dienstleistungen mit einem Anstieg der finanziellen Aufwendungen zu rechnen.

Gleichzeitig wird geprüft, in welchem Umfang zusätzliche personelle Ressourcen erforderlich sind, um die steigenden Anforderungen in Bereichen wie Sicherheitsüberprüfungen (z. B. Penetrationstests), Schwachstellenmanagement sowie Betrieb und Weiterentwicklung der Sicherheitsmassnahmen nachhaltig und risikogerecht bewältigen zu können. Dies erfolgt auch im Hinblick auf die Weiterführung des schrittweisen Ausbaus unseres Managementsystem für Informationssicherheit (ISMS) nach ISO 27001.

Die konkrete Ausgestaltung erfolgt im Rahmen der ordentlichen Budget- und Planungsprozesse der Stadt Thun.

Thun, 24. Juni 2026

Für den Gemeinderat der Stadt Thun

Die Vizestadtpräsidentin	Der Stadtschreiber
Katharina Ali-Oesch	Bruno Huwyler Müller