



EVP-GLP- Mitte-Fraktion

Interpellation

Informations- und Cybersicherheit in der Gemeinde Köniz

Im Zuge der zunehmenden Digitalisierung und der wachsenden Bedrohung durch Cyberangriffe ist die Sicherheit der IT-Infrastruktur und der Schutz sensibler Daten von hoher Bedeutung. Gemeinden stehen dabei vermehrt im Fokus von Cyberkriminellen, sei es aus finanziellen oder politisch motivierten Gründen. So wurde Ende 2023 die Gemeinde Zollikofen durch eine Ransomware-Attäcke schwer getroffen: Trotz zuvor getroffener Sicherheitsvorkehrungen mussten sämtliche IT-Systeme heruntergefahren werden, es entstanden hohe Kosten, ein Reputationsschaden und ein Vertrauensverlust in der Bevölkerung.

Auch die Stadt Bern sowie weitere Gemeinden melden jährlich zahlreiche Cyberangriffe. Viele kommunale Systeme – etwa zur Wasser- und Stromversorgung oder zur Steuerung der öffentlichen Beleuchtung – sind mit dem Internet verbunden und daher besonders anfällig.

Köniz betreibt gemeinsam mit Muri-Gümligen eine Informatikzone (IZ), welche zusätzlich 17 weitere Gemeinden umfasst. Die Verantwortung ist somit breit abgestützt – ein gezieltes Sicherheitsmanagement zentral. Bereits im Jahr 2022 wurde im Gemeinderat Muri eine thematisch verwandte Interpellation behandelt (vgl. [GGR 2022/02-06](#)). Auch der Kanton Bern hat eine Wegleitung zur Cybersicherheit publiziert, an der sich Gemeinden orientieren können.

Vor diesem Hintergrund bitte ich den Gemeinderat um die Beantwortung folgender Fragen:

1. Welche Massnahmen hat die Gemeinde Köniz in den letzten drei Jahren ergriffen, um die Informations- und Cybersicherheit in der Verwaltung zu verbessern und die Mitarbeitenden für Cyberrisiken zu sensibilisieren?
2. In welchem Rhythmus und in welcher Form werden interne oder externe Sicherheitsüberprüfungen der IT-Systeme (z. B. Penetrationstests, Bug-Bounty-Programme, Audits) durchgeführt, und welche Massnahmen wurden aufgrund allfälliger Erkenntnisse umgesetzt?
3. Welche Massnahmen bestehen zum Schutz vor gängigen Angriffsformen wie Schadsoftware, DDoS-Attacken, Ransomware und Phishing, und wie regelmässig werden diese auf ihre Wirksamkeit geprüft?
4. Werden durch das Informatik-Zentrum amerikanische oder ausser-europäische Cloud-Dienste genutzt, und wie beurteilt der Gemeinderat die damit verbundenen Risiken in Bezug auf Datenschutz, Zugriff durch ausländische Behörden (z. B. Cloud Act) und die allgemeine Cybersicherheit?
5. Welche konkreten Notfallpläne (z. B. IT-Notfallhandbuch, definierte Meldekette, Wiederanlaufstrategien, Krisenkommunikation) bestehen in der Gemeinde Köniz für den Fall

eines Cyberangriffs – insbesondere auch für kritische Infrastrukturen wie Schulen, Heime oder technische Betriebe?

6. Gibt es eine übergreifende Risikoanalyse oder ein IT-Sicherheitskonzept, das auf alle kommunalen Einrichtungen (inkl. Schulen, Heime, Verwaltung und externe Partner) abgestimmt ist – und wer trägt die Gesamtverantwortung für die Koordination im Krisenfall?

Ich danke Ihnen für die Beantwortung dieser Fragen.

Freundliche Grüsse

Sladjan Petrovic

Liebefeld, 05.05.2025

Ruedi Hauer, R. A.

~~Dr. A.~~

T. Felle

Markus

A. Hult

Ch.

S. aus

Janka Hauer

Entenshofen, b. Basel

Anger

h n A

Grasse C. Hoffmann

St. A.

Albion N. R. J.

St. A.

Casimiro von Auz

C. Müller

