Gemeinde
Köniz

Parlamentssitzung vom 18. August 2025 **Traktandum 11**

V2514 Interpellation (EVP-GLP-Mitte-Fraktion) "Informations- und Cybersicherheit in der Gemeinde Köniz"
Beantwortung; Direktion Umwelt und Betriebe

Vorstosstext

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-Attacke 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 Meldeketten, 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, 01.04.2025

koeniz 0.3.2.2.2 / 286.12 / 990822

Eingereicht

05.05.2025

Unterschrieben von 23 Parlamentsmitgliedern

Sladjan Petrovic, Andreas Hauser, Roland Akeret, Fabienne Marti Locher, Katja Streiff, Toni Eder, Roger Tanner, Matthias Müller, Sandra Röthlisberger, Janka Hamm, Bülent Celik, Géraldine Boesch, Arlette Münger, Klaus von Muralt, Sara Gasser, Laura Hoffman, Lukas Erni, Christina Aebischer, Monika Röthlisberger, Heidi Eberhard, Casimir von Arx, Christine Müller, Selin López

Antwort des Gemeinderates

1. Frage

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?

In den letzten drei Jahren hat die Gemeinde Köniz umfassende Massnahmen ergriffen, um die Informations- und Cybersicherheit in der Verwaltung zu verbessern. Diese umfassen Schritte auf allen Ebenen, von der Prävention über die abgestimmte IT-Architektur bis hin zur Bewältigung von Cyberangriffen. Diese Bemühungen zielen darauf ab, alle Facetten der Informations- und Cybersicherheit zu stärken und die Mitarbeitenden für Cyberrisiken zu sensibilisieren, um die Verwaltung auf höchstem Niveau zu schützen.

Folgend werden Schwerpunkte aufgelistet, die einen Überblick über getroffene Massnahmen / Aktivitäten geben:

- Neu geschaffene Stelle eines Sicherheitsbeauftragten (Security Officer)
- Entwicklung einer umfassenden Weisung/Strategie für die Informations- und Cybersicherheit, um den spezifischen Bedürfnissen und Risiken der Verwaltung gerecht zu werden.
- Aufbau und Weiterentwicklung eines Informationssicherheits-Managementsystems (ISMS).
- Abschluss eines Vertrags mit einem spezialisierten externen Partner zur Unterstützung bei Security Incidents.
- Aufbau eines Computer Security Incident-Response-Teams (CSIRT), welches sich auf die Vorbereitung und Reaktion auf Sicherheitsvorfälle in IT-Systemen konzentriert. Dies mit dem Ziel, Schäden und Ausfallzeiten zu minimieren und den Geschäftsbetrieb wiederherzustellen. Im Team sind Mitarbeitende des Informatikzentrum vertreten wie der IT-Sicherheitsbeauftragte, Netzwerk- und Systemadministratoren, die Fachstellen Recht, Kommunikation und externe Security Experten.
- Organisation von regelmässigen Schulungen und Sensibilisierungsaktionen mittels obligatorischer e-Learnings, um die Mitarbeitenden über Cyberrisiken und die Bedeutung der Informations- und Cybersicherheit aufzuklären. Dazu wurden auch Phishing-Simulationen bei den Mitarbeitenden der Gemeindeverwaltung durchgeführt.
- Durchführung von Netzwerk- und Sicherheitsaudits, um Schwachstellen und Risiken zu identifizieren und zu beheben. Dazu wurde eine externe Firma beauftragt.
- Implementierung von Sicherheitsmassnahmen, wie zum Beispiel:
    - Firewalls und Intrusion-Detection-Systeme
    - Verschlüsselung von Daten
    - Sichere Authentifizierung und Autorisierung
    - Regelmässige Updates und Patches für Software und Systeme

- Einführung eines neuen Backup-Systems mit isolierten und schreibgeschützten Laufwerken.

2. Frage

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?

Die Gemeinde Köniz führt Sicherheitsüberprüfungen in flexiblen Intervallen durch, je nach Themenbereich und in Abhängigkeit von laufenden Umsetzungsmassnahmen. Die Ergebnisse dieser Überprüfungen werden vertraulich behandelt und dienen als Grundlage zur Verbesserung der Sicherheit unserer IT-Systeme und -Anwendungen.

Im Detail werden die Formen und Methoden unserer internen und externen Überprüfungen aus Sicherheitsüberlegungen an dieser Stelle nicht weiter kommentiert, da dies sensible Informationen über unsere Sicherheitsvorkehrungen und -prozesse enthalten würde, die nicht in Form der vorliegenden öffentlich zugänglichen Interpellationsantwort gemacht werden sollten, um die Sicherheit unserer Systeme und Daten zu gewährleisten. Gerne geben wir aber im vertraulichen Rahmen weitere Auskünfte.

3. Frage

Welche Massnahmen bestehen zum Schutz vor gängigen Angriffsformen wie Schadsoftware, DDoS-Attacken, Ransomware und Phishing, und wie regelmässig werden diese auf ihre Wirksamkeit geprüft?

Die Gemeinde Köniz hat diverse Massnahmen ergriffen, um die Informations- und Cybersicherheit zu gewährleisten, insbesondere im Hinblick auf unterschiedliche Angriffspunkte. Eine neue Weisung zur Informations- und Cybersicherheit wurde verabschiedet, und diverse Richtlinien sind in Arbeit, die sowohl technische als auch organisatorische Massnahmen betreffen. Diese werden in einem übergeordneten Informationssicherheits-Managementsystem (ISMS) verwaltet. Mitarbeitende werden durch E-Learnings und Informationen im Intranet sensibilisiert.

Folgend werden Schwerpunkte aufgelistet, die einen Überblick über unsere Aktivitäten geben:

- Schutz vor Schadsoftware und Viren: Antiviren-Software; Regelmässige Updates und Patches für Software und Systeme
- Netzwerksicherheit: Firewalls und Intrusion-Detection-Systeme; Netzwerk-Segmentierungen; Sichere Authentifizierung und Autorisierung
- Datenschutz: Verschlüsselte Daten; Backup-System mit isolierten und schreibgeschützten Laufwerken
- Verfügbarkeit und Redundanz: Georedundantes Datacenter.
- Zugriffskontrolle: Sichere Authentifizierung und Autorisierung

Die Wirksamkeit dieser Massnahmen wird regelmässig überprüft, wie bereits in Frage 2 erläutert wurde. Diese Überprüfungen helfen die Sicherheitsvorkehrungen kontinuierlich zu verbessern und sicherzustellen, dass diese auf dem neuesten Stand sind, um Systeme und Daten vor verschiedenen Arten von Angriffen zu schützen.

4. Frage

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?

Die Gemeinde Köniz nutzt verschiedene Cloud-Dienste, darunter auch solche von US-amerikanischen Anbietern. Der Bundesrat hat die USA auf die Liste der Länder mit angemessenem

Datenschutzniveau gesetzt hat (News Service Bund – das Portal der Schweizer Regierung), was bei der Auswahl unserer Cloud-Dienste berücksichtigt wird.

Die Gemeinde Köniz ist sich bewusst, dass der Cloud Act und andere ausländische Gesetze potenzielle Risiken für den Datenschutz darstellen. Die Gemeinde Köniz arbeitet kontinuierlich daran, die vorhandenen Sicherheitsvorkehrungen zu verbessern und die Daten zu schützen, und passt Strategien stetig an, um den neuen Herausforderungen gerecht zu werden. Dazu wird eng mit Partnern und Anbietern zusammengearbeitet.

Der Gemeinderat beurteilt die Risiken als moderat, aber nicht unbedeutend, und hat daher verschiedene Massnahmen ergriffen, um diese Risiken zu minimieren. Unter anderem ist eine Richtlinie für die Verwendung von Cloud-Diensten in Arbeit, die die Klassifizierung und Verschlüsselung von Daten sowie Risikobeurteilungen für alle Cloud-Dienste umfasst. Dies insbesondere in Zusammenhang mit den Vorbereitungsarbeiten zur Umstellung auf Microsoft 365.

5. Frage

Welche konkreten Notfallpläne (z. B. IT-Notfallhandbuch, definierte Meldeketten, Wiederanlaufstrategien, Krisenkommunikation) bestehen in der Gemeinde Köniz für den Fall eines Cyberangriffs – insbesondere auch für kritische Infrastrukturen wie Schulen, Heime oder technische Betriebe?

Die Gemeinde Köniz behandeln IT-Incidents im laufenden Betrieb, ein IT-Notfall wird separat behandelt. Es besteht ein umfassender IT-Notfallplan für den Fall eines Cyberangriffs, der sowohl strategische, taktische als auch operative Massnahmen umfasst und dieser wird losgelöst vom Gemeindeführungsorgan (GFO) durch das Informatikzentrum bearbeitet. Im IT-Notfall wird das interne Computer Security Incident Response Team (CSIRT) aktiviert, das aus Mitarbeitenden des Informatikzentrums, Fachexperten und externen IT-Experten besteht. Die Gesamtverantwortung für die Koordination in einem IT-Notfall liegt beim Informatikzentrum.

Das IT-Notfallhandbuch und die digitalen Notfallordner enthalten wichtige Dokumente wie Informatik-Checklisten, Incident Response Handbücher und Notfall-Prozesse, sowie Kommunikationslisten und -vorlagen. Damit wird gewährleistet, dass eine schnelle und effektive Reaktion auf Cyberangriffe und das Minimieren der Auswirkungen auf unsere kritischen Infrastrukturen möglich ist. Für die Mitarbeitenden wurde ein IT-Notfallblatt erstellt, das wichtige Verhaltenshinweise für den Umgang mit Notfallsituationen enthält.

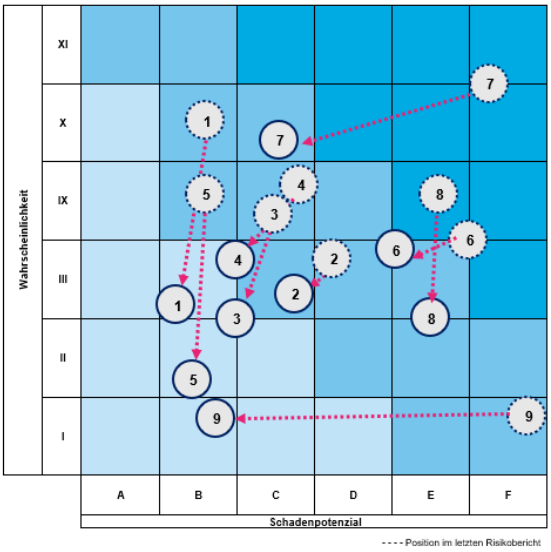
6. Frage

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?

Die Gemeinde Köniz verfügt über eine umfassende IT-Risikoanalyse, die durch das Informatikzentrum quartalsweise durchgeführt wird. Die jährliche Analyse wird in die übergeordnete Risikoanalyse der Gemeinde integriert und dem Gemeinderat berichtet.
Die Risikoanalyse ist ein wichtiger Bestandteil unserer Sicherheitsstrategie, da sie uns ermöglicht, potenzielle Risiken zu identifizieren und gezielte Massnahmen zu ergreifen, um diese zu minimieren.

Es wurden insgesamt 9 wesentliche Risiken identifiziert. Mit der Umsetzung der geplanten Massnahmen können die Risiken wie dargestellt auf ein vertretbares Mass bezüglich Eintretenswahrscheinlichkeit und Schadenpotenzial reduziert werden:

Legende:
1: Fehlendes Fachwissen
2: Datendiebstahl und/oder Datenverlust
3: Technologische Rückstände
4: Inkompatibilität von Teilsystemen
5: Unter- oder Überlizenzierung
6: Ausfall der IT-Systeme
7: Cyberangriffe
8: Verstoss gegen Datenschutzbestimmungen
9: Quantencomputer



Im Falle eines IT-Notfall wird das interne Computer Security Incident Response Team (CSIRT) aktiviert (siehe Frage 5).

Köniz, 06.06.2025

Der Gemeinderat