Grosser Gemeinderat Muri bei Bern
Sitzung vom 23. November 2021 Geschäft Nr. 9

# Interpellation Eugster (FDP), Koelbing (forum), Lauper (SVP) und Schmid (SP): Schutz der digitalen Daten im Verantwortungsbereich der Gemeinde vor unbefugtem Zugriff

## 1 TEXT

*Der Gemeinderat wird **um Auskunft darüber gebeten**,*

1. *wie er den Schutz der Daten, welche die Gemeindebehörden und die in der Verantwortung oder im Besitz der Gemeinde (oder in deren Beteiligung) stehenden Institutionen und Infrastrukturen (Schulen, Heime, Gemeindebetriebe) bearbeiten, vor **unbefugtem Zugriff**, insb. vor Cyberangriffen, **sicherstellt, überwacht** und **laufend verbessert**;*
2. *welche Notfallplanung er für den Fall eines Cyberangriffs zur Hand hat, bzw. wie und innerhalb welcher Fristen er die Notfallplanung für den Fall eines Cyberangriffs an die Hand zu nehmen gedenkt.*

*Begründung:*

***Anlass***

1. *Der Bund hat im Juni bekannt gegeben, dass er Alibaba und Amazon für eine Public-Cloud-Lösung den Zuschlag erteile. Dieser Entscheid hat bei Datenschutzfachleuten weitherum Kopfschütteln ausgelöst, zumal der Datenhunger der chinesischen und amerikanischen Nachrichtendienste bekannt ist.*
2. *Vor einem Monat kam es zu einem verheerenden Cyberangriff auf die Gemeinde Rolle (VD). Deren Server wurden gehackt, die darauf gespeicherten Daten gestohlen und verschlüsselt. Im Darknet sind nun persönliche Daten der Bürgerinnen und Bürger, Angestellten und Schülerinnen und Schüler von Rolle verfügbar sowie sensible Geschäftsvorgänge, die in der Gemeindeverwaltung behandelt werden (persönliche Daten inkl. Kreditkartenangaben, Unterlagen zu Rechtsstreitigkeiten, Mailverkehr der Gemeindeangestellten, Leistungsbeurteilungen, Schulzeugnisse usw.). Die Gemeindebehörden von Rolle wurden durch den Cyberangriff völlig überrumpelt und reagierten mangels eines existierenden Notfallmanagements hilflos darauf. Entsprechend harsch und spöttisch fielen die Reaktionen in der Westschweiz aus.*

***Folgen***

*Die Folgen eines Angriffs, wie ihn Rolle erlebt hat, wiegen schwer. Die gestohlenen Daten bilden im Darknet eine hervorragende Bresche für Kriminelle, die sie für weiterführende Angriffe auf die betroffenen Personen und Institutionen verwenden können. Damit stellt sich die Frage nach der Haftung der Gemeinde bei solchen Straftaten – sei es, dass «Leaks» von*

*schulischen Daten potenziell der künftigen Karriere von Schülerinnen und Schülern schaden, oder sei es, dass durch die Offenlegung von Daten aus dem Sozialen Dienst oder aus dem Erbschaftsdienst besonders schützenswerte Daten und damit sensible Situationen von Gemeindebürgerinnen und -bürgern offengelegt werden.*

***Bedrohungslage***
*Gemäss dem Nationalen Zentrum für Cybersicherheit (NSCS) lässt sich seit einigen Monaten ein signifikanter Anstieg der Cyberangriffe, wie sie Rolle erlebt hat (Ramsomware-Angriffe kombiniert mit Publikation im Darknet), auf Schweizer Institutionen und Firmen feststellen.*

*Der Kanton Bern hat angesichts der steigenden Cyberkriminalität einen spezialisierten Staatsanwalt eingesetzt, um auf diese Gefahr zu reagieren.*

*Vor diesem Hintergrund und angesichts der einschlägigen datenschutzrechtlichen Vorgaben erachten wir die Speicherung von Daten von Gemeindebürgerinnen und -bürgern, darunter auch jene von Schülerinnen und Schülern, in Cloud-Lösungen mit Servern im Ausland als ungeeignet.*

***Erkenntnisse***
*Guter Schutz vor unbefugtem Zugriff beruht auf folgenden Grundsätzen:*

1. *Laufend aktualisierte und überwachte Zuteilung von Zugriffsrechten;*
2. *Kontrolle bzw. Hoheit über die physische Speicherung der Daten (Vermeiden von Cloud-Lösungen grosser internationaler Anbieter);*
3. *Regelmässige Überprüfung des Gesamtsystems mittels externer Audits.*

*Guter Cyberschutz beruht auf folgenden Grundsätzen:*

1. *Ausbildung und Sensibilisierung der Mitarbeitenden (der Mensch ist die grösste Schwachstelle);*
2. *permanente Aufdatierung der Systeme (bekannte Sicherheitslücken müssen rasch geschlossen werden) und regelmässiges Erstellen von Sicherheitskopien;*
3. *regelmässige Überprüfung des Gesamtsystems mittels externer Audits (inkl. Probeangriffe) und Notfallübungen.*

*Muri bei Bern, den 21. September 2021* *S. Eugster, M. Koelbing, R. Lauper, E. Schmid*

*A. Bärtschi, R. Buff, L. Bircher, R. Weibel, A. von Gunten, U. Grütter, Ch. Spycher, Ch. Siebenrock, D. Arn, E. Zloczower, M. Gubler, B. Legler, W. Thut, P. Rösli, B. Häuselmann, H. Beck, G. Grossen, K. Künti, A. Zaccaria, S. Fankhauser, J. Brunner, H. Meichtry, F. Grossenbacher, H. Gashi, R. Mäder, D. Bärtschi, P. Messerli, K. Stein, R. Racine (33)*

## 2 STELLUNGNAHME DES GEMEINDERATS

Der Gemeinderat dankt für die Lancierung des interessanten, von allen an der GGR-Sitzung vom 21. September 2021 anwesenden Ratsmitgliedern unterzeichneten Vorstosses und sichert zu, dass sowohl dem Datenschutz als auch der Datensicherheit grosse Beachtung geschenkt wird.

### 2.1 Informatikzentrum Köniz-Muri

Die beiden Gemeinden Köniz und Muri bei Bern betreiben seit 1997 ein gemeinsames Informatikzentrum.

Seine Gründung verdankt es der Weitsicht der damaligen Könizer und Muriger Politiker, die zum Schluss kamen, dass nicht jede Gemeinde eigenständig die ganze Informatik-Infrastruktur aufbauen und verwalten solle, sondern dass sich durch den gemeinsamen Betrieb eines Rechenzentrums Kosten und Aufwand optimieren lassen. Heute werden sämtliche Informatik-Dienstleistungen für die Gemeinden Köniz und Muri sowie für weitere Kunden durch das IZ Köniz-Muri erbracht.

Das IZ stellt mit seinen Mitarbeitenden (1230 Stellenprozente) die gesamte Informatikinfrastruktur für die am IZ-Netzwerk angeschlossenen ca. 850 Verwaltungs-EDV-Arbeitsplätze zur Verfügung, sorgt für den reibungslosen Betrieb der Server und der eingesetzten Applikationen, betreut das umfangreiche Netzwerk, unterstützt die User bei Problemen und arbeitet in Projektteams an den laufend nötigen Informatikerneuerungen für die Zukunft und ist für die Datensicherheit zuständig.

Als strategisches Organ ist der Führungs- und Koordinationsausschuss Informatik eingesetzt. Dieser setzt sich aus je einem Vertreter des Gemeinderates von Köniz und Muri b. Bern (Köniz: GR Hansueli Pestalozzi, Muri b. Bern GP Thomas Hanke) und der beiden Verwaltungen (Köniz: Pascal Arnold, Gemeindeschreiber, Muri b. Bern, Corina Bühler, Leiterin Zentrale Dienste), dem Leiter IZ und einem externen Berater zusammen.

Die vorliegende Botschaft ist daher in enger Zusammenarbeit mit dem Leiter des IZ Köniz-Muri, Herrn Pascal Wenger, erarbeitet worden.

### 2.2 *Frage 1: Wie er den Schutz der Daten, welche die Gemeindebehörden und die in der Verantwortung oder im Besitz der Gemeinde (oder in deren Beteiligung) stehenden Institutionen und Infrastrukturen (Schulen, Heime, Gemeindebetriebe) bearbeiten, vor unbefugtem Zugriff, insb. vor Cyberangriffen, sicherstellt, überwacht und laufend verbessert?*

#### 2.21 Schutzmassnahmen für eine angemessene Datensicherheit

Das Informatikzentrum Köniz-Muri (folgend IZ genannt) ist sich der Verantwortung für einen sorgfältigen Umgang mit jeglicher Art von Daten bewusst.

- Begriff - Datensicherheit
  Der Begriff Datensicherheit umschreibt den generellen Schutz von Daten, unabhängig davon, ob diese einen Personenbezug haben oder nicht. Dabei geht es bei dem Thema Datensicherheit nicht um die Frage, ob Daten überhaupt erhoben und verarbeitet werden dürfen. Vielmehr geht es um die Frage, welche Massnahmen ergriffen werden

müssen, um den Schutz der Daten zu gewährleisten, um damit schliesslich die bestmögliche Datensicherheit zu erreichen. Dieser angestrebte Zustand kann durch eine Vielzahl an Massnahmen erreicht werden.
Datensicherheit hat das primäre Ziel, Daten jeglicher Art gegen Manipulation, Verlust, Diebstahl und andere Bedrohungen zu sichern.

- Datensicherheit vs. Datenschutz
  Datenschutz und Datensicherheit stehen in enger Abhängigkeit zueinander. So lässt sich der Zustand der Datensicherheit nicht ohne die Massnahmen des Datenschutzes erreichen. Umgekehrt ist ein angemessenes Mass an Datensicherheit die Voraussetzung für effektive Datenschutzmassnahmen.

Gefahren für die Datensicherheit entstehen in unterschiedlicher Form. Entsprechend werden durch das IZ unterschiedliche Schutzmassnahmen (technische und organisatorische) ergriffen. Dies mit dem Ziel, einen illegalen Zugriff, die Löschung, das Kopieren sowie der physische Verlust der Daten zu verhindern.

2.221 Organisation

- <u>Datenschutz</u>
  Der Grosse Gemeinderat von Muri b. Bern hat am 22. November 2016 das Datenschutzreglement und der Gemeinderat am 12. Dezember 2016 die Datenschutzverordnung erlassen bzw. diese am 7. Dezember 2020 einer Teilrevision unterzogen.

  Gemäss Art. 12 des Datenschutzreglements ist die Geschäftsprüfungskommission Aufsichtsstelle für den Datenschutz. Verwaltungsseitig ist für den Bereich des Datenschutzes die Gemeindeschreiberei zuständig.

- <u>Datensicherheit</u>
  Der Gemeinderat hat am 22. September 2017 die Verordnung Datensicherheit erlassen, welche für die Anwendung aller Hardware und Software, die im Netzwerk des IZ betrieben werden, gilt und den Umgang mit diesen Informatikmitteln regelt (User). Diese Verordnung muss aufgrund der Einführung von GEVER einer Teilrevision unterzogen werden.

  Im 4. Quartal 2015 ist für das IZ ein externes Audit für die Datensicherheit bzw. die Informatiksicherheit erarbeitet worden.

  Um in Sachen Datensicherheit auf dem aktuellsten Stand zu sein und vor allem gegen die stetig wachsenden Risiken von Cyberangriffen gewappnet zu sein, arbeitet das IZ eng mit spezialisierten Firmen zusammen.
  Die Vorgaben / Leitlinien zur Informationssicherheit in der Gemeinde sind in Arbeit (4. Quartal 2021) bzw. der Leiter des IZ beauftragte eine externe Stelle mit der Überprüfung (Schwachstellenanalyse) der Informatiksicherheit (2. Quartal 2021).

2.231 Datensicherung / Backup
Daten werden mindestens einmal täglich gesichert. Durch das tägliche Backup (Redundant) werden dabei die Anforderungen an eine redundante Sicherung der Daten erfüllt.

2.241 IT-Infrastruktur

Alle IT-Infrastrukturen des IZ sind mit ausreichender Sicherung von Gebäuden und Räumen mit überwachten Einbruchsschutz ausgestattet (Zutrittskontrolle). Das aktive Management der Zugangskontrolle (Passwort, 2-Factor Authentifizierung) auf den Kernapplikationen verhindert, dass Unbefugte Datenverarbeitungsapplikationen (Software) in Betrieb nehmen oder diese verwenden können.
Die Server-Infrastruktur verfügt über eine unterbrechungsfreie Stromversorgung (begrenzt), eine moderne Brandschutzanlage basierend auf Inergen-Gas und ist durch ein Zutrittskontrollsystem gegen unbefugten Zutritt geschützt. Eine Überprüfung des Gesamtsystems mittels internen und externen Schwachstellenscans wurde im 2. und 3. Quartal 2021 durchgeführt (Massnahmen sind in Umsetzung).

2.251 Arbeitsplatz - Client

- Bei der Nutzung von mobilen Geräten (Laptops) werden gesicherte Zugriffe / Verbindungen wie VDI (Virtual Desktop Infrastructure) eingesetzt. Bei der VDI wird die Rechenleistung und die Speichervorgänge von einem zentralen Server im Rechenzentrum des IZ übernommen, welches entsprechend gesichert ist.
- Eine Firewall, täglich aktualisierte Virenscanner und Spamfilter gehören zur Grundausstattung jedes PCs welcher durch das IZ betreut wird.

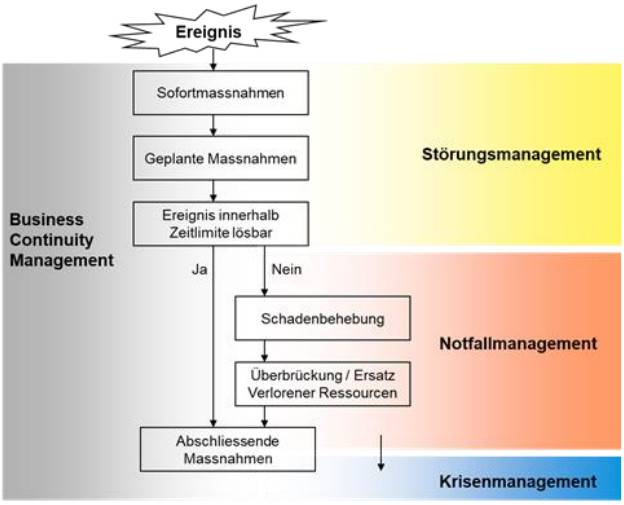
2.261 Kunden / Mitarbeitende

- Die Nutzung der Informatikmittel und der Umgang mit Intranet und personenbezogene Daten ist für die Mitarbeitenden in einer Nutzungsrichtlinie (Verhaltensvorgabe) festgelegt (in Überarbeitung 4. Quartal 2021).
- Der Gemeinderat wie die Mitarbeitenden werden periodisch über neue Bedrohungsszenarien aufgrund technischer Weiterentwicklungen informiert.
- Mit festgelegten Regelungen / Prozessen wird sichergestellt, dass nur berechtigte Personen Einblick in Daten erhalten und diese nur ihrer Berechtigung entsprechend nutzen können (Grundprinzip der ausschliesslich zweckgebundenen Nutzung von Daten).
- Für jeden Mitarbeitenden wird ein eigener Benutzer-Account angelegt, der so konfiguriert ist, dass nur der Account-Besitzer Aktionen ausführen darf. Damit ist jederzeit nachvollziehbar wer, wann, was an Daten geändert hat.
- Sensibilisierung und Schulung: Das Schaffen eines generellen Bewusstseins bei den Mitarbeitenden für das Thema Datensicherheit ist im Aufbau (4. Quartal 2021). Regelmässige Schulungen sind vorgesehen.

*2.3* *Frage 2: Welche Notfallplanung er für den Fall eines Cyberangriffs zur Hand hat, bzw. wie und innerhalb welcher Fristen er die Notfallplanung für den Fall eines Cyberangriffs an die Hand zu nehmen gedenkt.?*

2.31 Begriff - Betriebliches Kontinuitätsmanagement

Der Begriff Betriebliches Kontinuitätsmanagement (Business Continuity Management (BCM) beschreibt einen Managementprozess, der sicherstellt, dass kritische Geschäftsprozesse und Geschäftsfunktionen auch in Notsituationen verfügbar bleiben oder rechtzeitig wieder verfügbar sind.




2.331 Störung

Alle Ereignisse, die von Anfang an nicht als Notfall bezeichnet werden, stellen Störungen dar. Eine Störung ist ein Ereignis, dessen Schaden innerhalb der kritischen Wiederanlaufzeiten behoben werden kann.

- Eine Störung ist ein in der Regel beherrschbares Ereignis.
- Eine Störung lässt sich durch die Linienorganisation beheben.
- Jede Störung kann in ihrer Entwicklung oder nach Überschreiten der kritischen Wiederanlaufzeit zu einem Notfall eskalieren.

2.341 Notfall

Ein Notfall tritt ein, wenn innerhalb einer festgelegten Zeit eine Wiederherstellung des Betriebs nicht möglich ist und dies von der verantwortlichen Stelle festgestellt und eskaliert wird.

- Ein Notfall kann eine eskalierte Störung sein.
- Ein Notfall erfordert i.d.R. ein entsprechendes Notfallmanagement.

2.351 Krise

Eine Krise stellt ein Ereignis dar, welches jederzeit eintreten kann und für das kein Ablaufplan existiert.

- Für eine Krise existieren nur Rahmenweisungen und -bedingungen zur Bewältigung.
- Auch eine Krise muss durch den Krisenstab als solche festgestellt werden.
- Eine Krise erfordert immer ein entsprechendes Krisenmanagement.

Das IZ-Abwehrdispositiv setzt bereits vor einem möglichen Cyber Angriff an (Informationssicherheit, Datensicherheit). Die aktuellen Cyber Angriffsrisiken und -taktiken müssen ständig überwacht und alle relevanten Cyber Ereignisse genau analysiert werden. Um in Sachen Cyber Angriffsrisiken auf dem aktuellsten Stand zu sein und vor allem zu bleiben, arbeitet das IZ eng mit spezialisierten Firmen zusammen.

Das IZ hat ein "Disaster-Recovery Konzept", in welchem potentielle Risiken für einen Totalausfall des IZ erfasst wurden und mit entsprechenden Optionen zu deren Verhinderung resp. Szenarien für eine entsprechende Vorgehensweise festgehalten sind. Die durchgeführte Analyse durch den IZ-Leiter (1. Quartal 2021) zeigt, dass bestehende Sicherheitskonzepte weiter mit dem Themenbereichen IT-Risikomanagement, IT Krisenmanagement / Cyber Krisenmanagement ausgebaut werden müssen.
Die Inhalte der verschiedenen Aktivitäten / Schritte sind zwingend in die bestehenden Organisationstrukturen wie z.B. Krisenkommunikation einzubinden (Überarbeitung ist offen).

Muri bei Bern, 25. Oktober 2021

GEMEINDERAT MURI BEI BERN
Der Präsident Die Sekretärin

Thomas Hanke Corina Bühler