Grosser Gemeinderat Muri bei Bern
Sitzung vom 22. Februar 2022 Geschäft Nr. 6

Interpellation EUGSTER (FDP), KOELBING (Forum), Reto LAUPER (SVP) und SCHMID (SP): Schutz der digitalen Daten im Verantwortungsbereich der Gemeinde vor unbefugtem Zugriff – Ersuchen um vollständige Beantwortung der Frage

1 TEXT

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

1. *wie er den **Schutz und die Sicherheit der Daten**, welche 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 **auf eine der obengenannten Institutionen** zur Hand hat, bzw. wie und innerhalb welcher Fristen er die Notfallplanung für den Fall eines solchen Cyberangriffs an die Hand zu nehmen gedenkt.*

Begründung:

Der Gemeinderat ist in seiner Antwort auf die am 21.09.2021 eingereichte Interpellation EUGSTER (FDP), KOELBING (Forum), Reto LAUPER (SVP) und SCHMID (SP) mit keinem Wort auf den Schutz und die Sicherheit der Daten der in der Verantwortung oder im Besitz der Gemeinde (oder in deren Beteiligung) stehenden Institutionen eingegangen. Dieser Aspekt bildet aber einen wesentlichen Teil der Frage.

Muri bei Bern, den 23.11.2021 *S. Eugster, M. Koelbing, R. Lauper, E. Schmid*

U. Grütter, R. Racine, W. Thut, B. Häuselmann, B. Gantner, G. Grossen, K. Künti, A. Zaccaria, S. Fankhauser, J. Brunner, H. Beck, Ch. Spycher, R. Mäder, L. Bircher, B. Schmitter, L. Held, A. Bärtschi, B. Legler, R. Buff, M. Reimers, R. Weibel, D. Arn, E. Zloczower, M. Gubler, Ch. Siebenrock (29)

2 STELLUNGNAHME DES GEMEINDERATS

Der Gemeinderat hat sich gestützt auf die vorliegende zweite Interpellation zur Datensicherheit erneut mit dem Informatikzentrum Köniz-Muri bezüglich der gestellten Fragen ausgetauscht. Betreffend Schutz und Sicherheit der Daten, welche durch die Gemeindeverwaltung bearbeitet werden, kann er keine weiteren Ergänzungen der Antworten tätigen, ohne sich zu wiederholen. Daher verweist der Gemeinderat für die Beantwortung des Vorstosses in erster Linie auf seine Antwort an der GGR-Sitzung vom 23. November 2021.

Schutz und Sicherheit der Daten der Gemeindebetriebe (gbm), Schulen und Alenia

gbm:
Die Gemeindebetriebe sind wie die Gemeindeverwaltung Office-technisch am Informatikzentrum Köniz-Muri angeschlossen. Der Gemeinderat verweist daher i.S. gbm auf seine Antwort an der GGR-Sitzung vom 23. November 2021.
Die Gemeindebetriebe beziehen weitere Systemdienstleistungen wie zum Beispiel die Geoinformationssysteme für die Erfassung von Werkleitungen (Bichsel Bigler und Partner), die Glasfaserverwaltung (AND) und das Leitsystem für die Überwachung der Netzsysteme (Rittmeyer). Diese Systeme werden von den beauftragten Unternehmungen getrennt voneinander betrieben und gewartet. Hier bestehen Verträge bezüglich Haftung, Datensicherheit und Systemwiederherstellung.

Schulen:
Die heiklen Personendaten werden via Informatikzentrum Köniz-Muri (Schulverwaltung → Schulverwaltungssoftware Scolaris) gesichert. Die Beurteilungsdaten der Schülerinnen und Schüler sind auf dem Server der Bildungs- und Kulturdirektion (BKD, vormals ERZ) gesichert. In diesen beiden Fällen gelten die Sicherheitsrichtlinien via Zweifachidentifikation der entsprechenden Betreiber. Die weiteren Daten der Lehrpersonen und Schulleitungen sind auf der internen Cloud von Microsoft 365 gespeichert. Es bleibt der Hinweis, dass Schweizer Schulen den Cloud-Dienst Microsoft 365 datenschutzrechtlich offiziell einsetzen dürfen. Die schweizerischen Datenschützer konnten bei Microsoft im Jahr 2014 entsprechende Änderungen durchsetzen. Wie Privatim, die Vereinigung der schweizerischen Datenschutzbeauftragten, damals mitteilte, stellen die neuen Vertragsbedingungen verschiedene für den Datenschutz wichtige Punkte sicher. Die Verantwortlichkeiten sind klar geregelt, es gibt Kontrollmöglichkeiten und es wird festgehalten, wo in Europa die Datenbearbeitung erfolgt. In Streitfällen gilt zudem Schweizer Recht und der Gerichtsstand liegt in der Schweiz. Die Anpassungen gelten laut damaliger Mitteilung speziell für den Schweizer Bildungsbereich. Der technische Unterhalt von Microsoft 365 wird durch professionellen Support sichergestellt und gehört in den Aufgabenbereich des Second Level Supports.

Die Datensicherung (Backups) von Scolaris und der Schülerinnen- und Schülerbeurteilungen obliegt dem IZ Köniz-Muri. Die weiteren Daten der Lehrpersonen und Schulleitungen werden via Microsoft 365 geschützt. Ferner wurde jeder Lehrperson und Schulleitung empfohlen, periodisch eine Datensicherung auf einer externen, netzunabhängigen Festplatte vorzunehmen.

Alterszentrum Alenia:
Das Alterszentrum Alenia hat mit der Genossenschaft dedica einen Dienstleistungsvertrag im Bereich der Informatik abgeschlossen und so mit einem professionellen Anbieter wesentliche Elemente des Schutzes von digitalen Daten sichergestellt.

Die Leistung des Partners dedica umfasst im Wesentlichen die folgenden Eckpunkte, welche die Fragestellung direkt oder indirekt beantworten:

- Verfügbarkeit der Systeme von 99.7 %
- Support 7*24*365
- Serverfarm in Hochsicherheitsanlage Colobern (georedundant[1])
- Spam-Firewall, welche die grosse Mehrheit der Angriffsversuche blockiert
- Hohe Standards für Sicherheitsupdates
- Gerätewartung
- Tägliche Backups (bei Filesystemen: Jahressicherung bis 10 Jahre)
- Sensibilisierungen und Informationen für Anwender
- Penetrationstests

Die Anbindung an die Serverfarm erfolgt via LAN-1-Leitung (IPSS) der Swisscom.

Im Rahmen der Geschäftsbeziehung zwischen Alenia und dedica ist die Bearbeitung von Personendaten durch dedica (datenschutzrechtlich als Verantwortliche) explizit geregelt.
Dedica verpflichtet sich, die datenschutzrechtlichen Bestimmungen jederzeit einzuhalten. Dies umfasst die Vornahme der nötigen technischen und organisatorischen Sicherheitsmassnahmen und die Sicherstellung der Einhaltung der einschlägigen Bestimmungen durch Mitarbeitende und Dritte, die ihre Angebote und Systeme nutzen.

Die Sicherheitsmassnahmen für den Datenschutz in Bezug auf Hackerangriffe liegt neben den technischen Massnahmen (Spam-Firewall), welche von dedica sichergestellt wird, beim Nutzer des Systems (Alenia), insbesondere in der Stärke des Passwortes, regelmässiges Ändern des Passwortes, Speicherung des Passwortes und weitere Massnahmen. Alle Nutzer im Alenia werden in regelmässigen Rundschreiben (2x pro Quartal) und zusätzlich unmittelbar bei jeweils aktuell aufgetretenen Ereignissen über die Gefahren und Vorsichtsmassnahmen informiert und sensibilisiert.

Der Partner dedica legt Wert darauf, dass die Daten in Rechenzentren in der Schweiz gespeichert werden. Insbesondere in Zusammenhang mit der Nutzung von Office 365 kann dies allerdings nicht garantiert werden, da dedica keinen Einfluss darauf hat, auf welchen Servern in welchen Ländern Microsoft diese Daten speichert. Alenia hat aber einer Datenweitergabe ins Ausland in diesem Fall ausdrücklich zuzustimmen.

Sollte trotz aller Massnahmen gleichwohl ein Angriff auf die Daten von Alenia erfolgen (z. B. durch unsachgemässes Handling unsicherer E-Mails) so ist mit der Georedundanz und den hohen Sicherheitslevels eine rasche Wiederherstellung der Daten ohne wesentliche Einschränkung des Betriebes oder ohne hohe Kosten möglich.

[1] georedundant: Einsatz von zwei oder mehreren vollständig funktionsfähigen Datencenter an entfernten Standorten, um Beeinträchtigungen der Funktionsfähigkeit und Sicherheit zu vermeiden

Aktuell besteht in webbasierten Java-Applikationen eine Sicherheitslücke, die als äusserst kritisch beurteilt wird (sog. Log4Shell-Lücke). Davon betroffen sind beispielsweise Lichtrufanlagen, Brandmeldeanlagen, Hausleitsysteme, Schliesssysteme, Kassensysteme und verschiedene andere Überwachungssysteme. Nachdem Alenia über diese Sicherheitslücke von dedica in Kenntnis gesetzt war, hat die IT-Verantwortliche umgehend alle Anbieter von im Alenia im Einsatz stehenden Anwendungen angeschrieben und um eine Stellungnahme zu dieser Sicherheitslücke gebeten. Alle Anbieter bestätigten, dass diese Sicherheitslücke in allen von Alenia genutzten Anwendungen geschlossen werden konnte.

Alenia hat mit dem IT-Partner dedica sichergestellt, dass die Systeme während 24 h überwacht und regelmässig den neusten Anforderungen angepasst werden.

Weitere Informationen sind auf der dedica Webseite https://www.dedica.ch/de/datenschutz/ ersichtlich.

Muri bei Bern, 24. Januar 2022

GEMEINDERAT MURI BEI BERN
Der Präsident Die Sekretärin

Thomas Hanke Corina Bühler