Gemeinde
Riehen

Reg. Nr. 1.3.1.12 **CMI: 4321** **Nr. 18-22.785.02**

Bericht des Gemeinderats zum Anzug Noé Pollheimer und Kons. betreffend Cybersicherheit – Ist die Gemeinde Riehen gerüstet?

(überwiesen am 15. Dezember 2021)

1. Anzug

An seiner Sitzung vom 15. Dezember 2021 hat der Einwohnerrat den nachfolgenden Anzug Noé Pollheimer und Kons. betreffend Cybersicherheit – Ist die Gemeinde Riehen gerüstet? überwiesen:

Wortlaut:

"Mit der Gemeinde Montreux wurde bereits die zweite Gemeinde nach Rolle (VD) in der Schweiz innert kurzer Zeit Opfer eines Cyberangriffs. Potenziell sind auch 9 weitere Gemeinden aus der Riviera betroffen. Kurz nach den Cyberangriffen sind hochsensible Daten der Gemeinden im Darknet aufgetaucht. Neben Informationen über Verhandlungen der Gemeinde mit privaten Unternehmen waren auch persönliche Informationen (Identität, Nationalität, Staatsangehörigkeit, Geburtsdatum, AHV & Steuernummer etc.) von Einwohner*innen betroffen. Erschreckend in beiden Fällen ist, dass die betroffenen Gemeinden nur passiv kommuniziert, bzw. die Angriffe der Öffentlichkeit gegenüber kleingeredet sowie das Ausmass der Angriffe massiv unterschätzt und vertuscht haben.

Die beiden Fälle zeigen beispielhaft auf, wie viele Gemeinden mit den Herausforderungen der Digitalisierung und Cybersicherheit überfordert sind und wie sehr die Ressourcen und das nötige Knowhow fehlen. Auch im Jahr 2021 unterschätzen Gemeinden das Risiko eines Cyberangriffes massiv: Sie führen unzureichende Sicherheitskonzepte und hoffen weiterhin, dass es die eigene Gemeinde nicht trifft. Leider bleibt dadurch die Cybersicherheit auf der Strecke und damit die Sicherheit höchstsensibler Daten von allen Einwohnenden. Der Bundesrat hat dies in einer kürzlich veröffentlichen Stellungnahme bestätigt.

Auch der Bund hat dies erkannt und baut aktuell ein Nationales Zentrum für Cybersicherheit (NCSC) auf, welches mittelfristig auch Kantone und Gemeinden in diesen Belangen unterstützen kann. Auch die Gemeinde Riehen muss sich die Cybersicherheit auf die Fahne schreiben und ihr Konzept zur Cybersicherheit überprüfen und verbessern. Dabei sollen nachhaltige Partnerschaften mit dem Kanton, anderen Gemeinden und der Privatwirtschaft angestrebt werden.

Die Unterzeichnenden bitten den Gemeinderat, zu prüfen und berichten:

1. Welche Massnahmen die Gemeinde gegen die benutzten Methoden in den Fällen der Gemeinde Montreux und Rolle ergreifen kann?

2. Wie die Gemeinde in Zukunft gegen Cyberangriffe gerüstet sein kann und sichergestellt ist, dass das Datensicherheitskonzept immer dem aktuellen Stand entspricht?

3. Wie die Gemeinde ihre Mitarbeiter*innen und die Bevölkerung zu dieser Thematik wirkungsvoll sensibilisieren kann?“

sig. Noé Pollheimer, Susanne Fisch, Andreas Hupfer, Martin Leschhorn Strebel, Heinz Oehen, Regina Rahmen, Paul Spring, Rebecca Stankowski

2. Bericht des Gemeinderats

Die Stärkung der Cyber- und Datensicherheit ist für den öffentlichen Sektor eine der größten Herausforderungen der Gegenwart. So sehen auch viele Versicherungsgesellschaften ein stark erhöhtes systematisches Risiko und die Gefahr von Cyberterrorismus und Spionageangriffen auch im Bereich der öffentlichen Hand. Cyberangriffe sind somit eine reale und wachsende Bedrohung. Aus diesem Grund erachtet auch der Gemeinderat die Cybersicherheit als wichtige und grosse Herausforderung für die Gemeinde Riehen.

Gemäss Reglement über die Informationssicherheit der Gemeinde Riehen (Informationssicherheitsreglement) vom 1. August 2021 trägt der Gemeinderat die Gesamtverantwortung für die Informationssicherheit. Dies umfasst auch den Aufbau und die Sicherstellung eines entsprechenden Informationssicherheits- und Risikomanagementsystems in der Gemeindeverwaltung. Die IT-Sicherheit ist ein Teilbereich der Informationssicherheit, die sich auf die elektronisch gespeicherten Informationen und IT-Systeme bezieht. Die Cyber-Sicherheit bezieht sich prinzipiell auf den gleichen Bereich wie die IT-Sicherheit, erfasst jedoch auch den gesamten Bereich des Internets und jeglicher Netzwerke. Die übergreifenden Prozesse und Organisationen zur Informationssicherheit auf kommunaler Ebene werden von der Gemeinde Riehen eigenständig aufgebaut, koordiniert und verantwortet. Dafür müssen jedoch die notwendigen finanziellen Mittel zur Verfügung gestellt und die technologischen Instrumente angeschafft werden.

Hinsichtlich einer umfassenden Risiko-Abschätzung und zukünftigen Stärkung auf dem Gebiet der Cyber- und Datensicherheit in der Gemeinde Riehen muss das Zusammenspiel der EDV-Riehen mit der Informatik des Kanton Basel-Stadt beachtet werden. Bei der Gemeindeinformatik handelt es sich nicht um einen in sich geschlossenen IT-Querdienstleister für die Gemeindeverwaltung. Die Synergien mit der Kantonsinformatik und damit auch die Abhängigkeit der Gemeindeinformatik zum Kanton Basel-Stadt sind sehr ausgeprägt. Die Gemeindeverwaltung Riehen nutzt seit 2001 das Verwaltungsnetzwerk und den Internetzugang des Kanton Basel-Stadt (DANEBS) und ist somit darauf angewiesen, dass der Kanton für einen sicheren Betrieb des kantonalen Netzwerkes sorgt. Mit der Informationssicherheitsstrategie 2020+ stellt die Verwaltung des Kantons Basel-Stadt sicher, dass mit grundlegenden Zielen und stabilen Vorgaben die Richtung und Leitplanken für die langfristige Entwicklung der integralen Informationssicherheit im Kanton verfolgt werden, wobei sich die Informationssicherheit des Kantons auf die Empfehlungen der Standards «NIST Cyber Security Framework»

und ISO/IEC 27001 stützt. Mittels Service Level Agreement (SLA) stellen die IT.BS und die Gemeindeverwaltung Riehen sicher, dass die Sicherheitsvorgaben gemäss Verordnung über die Informationssicherheit (ISV) §10 eingehalten werden. Die Gemeindeverwaltung Riehen betreibt seit 2014 eine eigene Server-Infrastruktur, welche sich aus Sicherheitsüberlegungen redundant auf zwei Standorte in den Rechenzentren IWB in Basel-Stadt und der EBM in Münchenstein verteilt. Somit ist die Gemeindeinformatik für die Sicherheit der Basisinfrastruktur in der Verwaltung verantwortlich, welche den Betrieb der Server, die Zurverfügungstellung der Arbeitsplätze, Drucker und des WLAN-Netzes an den verschiedenen Standorten der Gemeinde Riehen beinhaltet. Für die Riehener Schulen erbringt das Erziehungsdepartement (ED) des Kanton Basel-Stadt Informatikdienstleistungen. Sie umfassen das schuleigene Netzwerk «eduBS» sowie die dazugehörigen Arbeitsstationen für Lehrpersonen und Schülerinnen und Schüler.

Mit wenigen Ausnahmen nehmen somit praktisch alle Verwaltungsaufgaben der Gemeinde, auch geschäftskritische, Informatik- und Kommunikations-Mittel (IKT) in Anspruch, welche massgeblich in den Rechenzentren (RZ) des Kanton Basel-Stadt betrieben werden. In diesem Kontext der vielfältigen IKT-Schnittstellen und Abhängigkeiten zur Kantonsinformatik gilt es die Herausforderungen der Digitalisierung und Cybersicherheit auf der kommunalen Ebene anzugehen.

Beantwortung der Anzugsfragen

1. *Welche Massnahmen die Gemeinde gegen die benutzten Methoden in den Fällen der Gemeinden Montreux und Rolle ergreifen kann?*

Bei den Cyberangriffen auf die Informatiksysteme der Gemeinden Montreux und Rolle handelte es sich um sogenannte Ransom-Attacken, verursacht durch kriminelle Hacker. Dabei verschlüsseln die Hacker die Daten des Nutzers und fordern danach Lösegeld, damit die Daten wieder entschlüsselt werden. Bei einem Ransomware-Angriff verschafft sich die Malware[1] Zugang zu den Informatiksystemen. Dieser Vorgang kann über verschiedene Wege geschehen, beispielsweise über einen als legitim getarnten, aber mit Malware infizierten E-Mail-Anhang, ein sogenannter Phishing-Angriff, oder über manipulierte und bösartige Websites sowie unsichere WLAN-Netzwerke.
Die Einschätzung des Risikos eines potentiellen Cyberangriffs auf die Gemeinde Riehen und wie gut diese bereits dagegen gerüstet ist, ist vor allem durch die zahlreichen Schnittstellen und der engen Verzahnung mit der Kantonsinformatik vielschichtig und anspruchsvoll. Das grosse Aufgabenspektrum und die zunehmende Komplexität bei den steigenden Herausforderungen in den Themenbereichen der Informations- und Cybersicherheit machen es schwierig, in allen Aufgabenfelder die nötigen Kompetenzen und Routine auch auf der kommunalen Ebene aufzubauen und zu erhalten. Aus diesen Gründen und um die Datensicherheit der

[1] Malware ist ein Sammelbegriff für "bösartige" Programme, die dazu entwickelt wurden, Nutzern Schaden zuzufügen. Es gibt zahlreiche Unterarten von Malware - zum Beispiel Viren, Trojaner, Rootkits, Würmer, Botnets, Ransomware, Adware oder Spyware.

Gemeinde in Anbetracht des steigenden Risikos eines Cyberangriffs zu erhöhen, hat der Gemeinderat die Verwaltung im Frühling 2022 beauftragt, eine schon länger geplante IT-Sicherheitsüberprüfung in der Gemeindeverwaltung durchzuführen. Die Durchführung einer IT-Sicherheitsüberprüfung in der Gemeindeverwaltung wurde nämlich sowohl von der BDO AG als Revisionsstelle wie auch vom kantonalen Datenschutzbeauftragten empfohlen. In der Folge wurde die externe Firma Swiss Infosec AG beauftragt, in der Gemeindeverwaltung diese IT-Sicherheitsüberprüfung durchzuführen. Die Swiss Infosec AG verfügt auf dem Gebiet der IT-Sicherheit über eine grosse Expertise und ist auch mit den kantonalen Vorgaben und Gegebenheiten hinsichtlich der technischen Vernetzung der IT-Infrastruktur der Gemeinde Riehen mit dem Kanton bestens vertraut.

Die IT-Sicherheitsüberprüfung wurde im Sommer 2022 durchgeführt und umfasste eine breitflächige Prüfung der Cyber-Gesundheit der Gemeinde IKT-Infrastruktur. Dies beinhaltete die Durchführung eines IT-Sicherheitsaudits, eine Verwundbarkeitsanalyse (Vulnerability Scanning) auf die IT-Systeme der Gemeinde Riehen sowie ein simulierter Phising[2]-Angriff auf die Mitarbeitenden der Gemeindeverwaltung. Die Feststellungen der IT-Sicherheitsüberprüfung wurden in einem als vertraulich klassifizierten Abschlussbericht zusammengefasst. Hinsichtlich des Ergebnisses der Schwachstellenanalyse kann an dieser Stelle erwähnt werden, dass die Gemeinde Riehen im Vergleich zu anderen Organisationen der öffentlichen Verwaltung im Mittelfeld liegt. Die bereits bestehenden Sicherheitsprozesse in der Gemeindeverwaltung haben zwar bereits einen fortgeschrittenen Reifezustand erreicht, so liegen bspw. durchdachte Konzepte in Bereichen der Datensicherung und Wiederherstellung oder Netzwerksicherheitsverfahren vor, aber dennoch weist die Cyberhygiene der Gemeinde einen gewissen Optimierungsbedarf auf. Die Ergebnisse der IT-Sicherheitsüberprüfung bilden somit eine wesentliche Grundlage, um die entsprechenden Massnahmen einzuleiten, damit die Gemeinde Riehen auch in Zukunft gut gegen Ransom-Attacken gewappnet sein wird.

2. *Wie die Gemeinde in Zukunft gegen Cyberangriffe gerüstet sein kann und sichergestellt ist, dass das Datensicherheitskonzept immer dem aktuellen Stand entspricht?*

Im Rahmen des laufenden Datenschutz- und Informationsprojektes in der Verwaltung werden seit 2020 sukzessive verschiedene Massnahmen umgesetzt, damit die Gemeinde Riehen den steigenden Anforderungen im Bereich der Informationssicherheit auch in Zukunft genügen wird. So konnten bereits mit der Erarbeitung der kommunalen Vorgaben und Konzepte zur Umsetzung der Informationssicherheitsziele wichtige Grundlagen geschaffen werden. Weitere Projektziele beinhalten die Erarbeitung der erforderlichen Informationssicherheitsdokumente (Zugriffsberechtigungs-, Aufbewahrungs-, Lösch- und Notfallkonzepte) auf der operativen Ebene sowie die Einführung eines Regelwerks für die Benutzer- und Berechtigungsadministrationsprozesse in der gesamten Verwaltung. Die Abteilungen werden bei der Umsetzung der notwendigen Sicherheitsprozesse durch den kommunalen Informationssichereitsbeauftragten (ISB) unterstützt. Auf der obersten Führungsebene der Verwaltung wurde gestützt

[2] Phishing-Angriff; unter dem Begriff Phishing versteht man Versuche, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdiger Kommunikationspartner in einer elektronischen Kommunikation auszugeben. Ziel des Betrugs ist es z. B. an persönliche Daten eines Internet-Benutzers zu gelangen oder ihn z. B. zur Ausführung einer schädlichen Aktion zu bewegen.

auf das neue Reglement über die Informationssicherheit der Gemeinde Riehen vom 6. Juli 2021 der Fachausschuss für «Information Governance[3]» im Jahr 2022 gebildet, welcher Themen der digitalen Transformation und der «Information Governance» behandeln wird. Mit der Einsetzung dieses Fachausschusses stellt die Verwaltung sicher, dass die strategischen Ziele des Gemeinderats, die operativen Vorgaben und die Anforderungen an die digitale Transformation umgesetzt und auf die Bedürfnisse des Betriebs, der Mitarbeitenden und der Bevölkerung ausgerichtet werden.

Die Überprüfung des in der Verwaltung vorliegenden Datensicherheitskonzepts zeigte auf, dass die Gemeinde im Quervergleich mit anderen Organisationen bei den Cyberhygiene-relevanten organisatorischen und technischen Organisationsabläufe generell gut abschneidet. So entsprechen viele IT-Betriebsabläufe bereits heute der gängigen Best Practice. Die Empfehlungen richten sich hier weniger auf die Optimierung der technischen Sicherheitsmassnahmen, sondern vielmehr auf die Aspekte der Einführung eines umfassenden Sicherheitsmanagements und der nachhaltigen Verankerung der Cybersicherheit in der Organisation. Dies stellt eine Herausforderung dar, der sich alle Organisationen der öffentlichen Hand zukünftig stellen müssen. Die Befunde und Empfehlungen aus der IT-Sicherheitsüberprüfung werden jetzt sorgfältig geprüft und risikobasiert, bei stimmigem Kosten- / Nutzen-Verhältnis, wird deren Umsetzung in der Verwaltung angegangen. Zusätzlich wird die Einführung und Umsetzung eines strukturierten Ausbildungsprogramms für IT-Sicherheitsthemen in der Verwaltung geprüft.

3. *Wie die Gemeinde ihre Mitarbeiter*innen und die Bevölkerung zu dieser Thematik wirkungsvoll sensibilisieren kann?*

In der IT-Sicherheit spielt der „Faktor Mensch“ eine zentrale Rolle, da Cyberattacken darauf ausgelegt sind, Schwachstellen auszumachen und auszunutzen. In vielen Fällen sind dies keine technischen Schwachstellen, sondern der Mensch. Unwissen und Unaufmerksamkeit führen zu Fehlern, die von Cyberkriminellen gezielt ausgenutzt werden, um an Daten oder Zugänge zu gelangen. Als Ergänzung zu den klassischen Schutzmassnahmen wie Firewall, E-Mail und Webschutz liess die Gemeindeverwaltung den «Faktor Mensch als Sicherheitsrisiko» im Rahmen einer Phishing-Kampagne überprüfen. Dabei wurde überprüft, welches Sicherheitsbewusstsein die Mitarbeitenden haben. Die IT-Sicherheitsüberprüfung beinhaltete die Durchführung einer Phishing-Kampagne mit dem Ergebnis, dass die Sensibilisierung der Mitarbeitenden der Gemeinde für Bedrohungen im (digitalen) Tagesgeschäft ein deutliches Potenzial bietet, das Risikoprofil der Gemeindeverwaltung in Bezug auf Cyberangriffe zu reduzieren. Als nächste Massnahme werden gezielte Nachschulungen für die Mitarbeitenden in allen Abteilungen erfolgen. Zusätzlich ist mit einem systematischen Ansatz geplant, die Mitarbeitenden in der Verwaltung für die Bedrohungen im (digitalen) Arbeitsalltag mit einem langfristigen Awareness-Programm zu sensibilisieren.

[3] Information Governance (IG) ist die Gesamtstrategie für Informationen in einer Organisation und umfasst die Themen Informationssicherheit und -schutz, Compliance, Datenqualität, Data Governance, elektronische Erkennung, Risikomanagement, Datenschutz, Datenspeicherung und -archivierung.

Bedingt durch das enge Zusammenspiel und den vielfältigen Schnittstellen zwischen der Gemeindeinformatik mit der Kantonsinformatik besteht bereits heute eine nachhaltige Partnerschaft mit dem Kanton. So partizipiert die Gemeindeverwaltung Riehen an kantonalen Projekten im Bereich der Informationssicherheit und eine wichtige Aufgabe des kommunalen ISB besteht darin, den aktiven Wissensaustausch auf dem Gebiet der Informationssicherheit mit diversen externen Stellen (IT.BS, kantonaler Datenschutzbeauftragter, kantonaler ISB, andere Gemeinden und Firmen) anzustreben und zu etablieren. Auf der kantonalen Ebene hat die Basler Regierung gemäss Regierungsratsbeschluss vom 30. August 2022 dem Grossen Rat beantragt, sich die Motion Philip Karger und Konsorten betreffend Stärkung der Cybersicherheit für Staatliche Verwaltungen, Firmen und Privaten in Basel-Stadt als Anzug überweisen zu lassen. Unter Anderem schlagen die Unterzeichnenden den Aufbau eines Kompetenzzentrums Cybercrime im Bereich JSD vor. Ebenso soll der Kanton im Rahmen von regelmässigen Awareness-Kampagnen auf die Cyberbedrohungen aufmerksam machen und so die Bürgerinnen und Bürger sensibilisieren, dabei sollen Prävention und Vorsichtsmassnahmen im Vordergrund stehen. Die Gemeinde wird die Entwicklungen auf der kantonalen Ebene hinsichtlich des Aufbaus dieser Awareness-Kampagnen auf dem Gebiet der Cybersicherheit eng verfolgen, um allfällige Synergien auch auf kommunaler Ebene nutzen zu können.

3. Antrag

Der Gemeinderat beantragt, den Anzug **abzuschreiben**.

Riehen, 15. November 2022

Gemeinderat Riehen

Die Präsidentin:	Der Generalsekretär:
	
Christine Kaufmann	Patrick Breitenstein