

Auszug aus dem Protokoll

Sitzungsdatum	Traktandum	Beschlussnummer	Geschäftsnummer	Ordnungsnummer
27.08.2025	7	44	4687	00.06.04

Interpellation Stéphanie Anliker (FDP) und Mitunterzeichnende betreffend «Cyberangriff auf Gemeinden – Was tut Zollikofen?», Antwort

Ausgangslage

Am 30. April 2025 wurde folgende Interpellation eingereicht:

Erstunterzeichnerin: Stéphanie Anliker (FDP)

Mitunterzeichnende: Marcel Remund (FDP), Rolf Stettler (FDP)

«Antrag

Der Gemeinderat wird gebeten, die folgenden Fragen zu beantworten:

- 1. Wie wird die seit dem 1. April 2025 geltende Meldepflicht für Cybervorfälle in Zollikofen umgesetzt?*
- 2. Welche Massnahmen hat der Gemeinderat nach dem Hackerangriff vom November 2023 konkret ergriffen, um das Risiko für weitere Angriffe zu reduzieren?*
- 3. Erachtet der Gemeinderat das Label «CyberSafe» (<https://www.cyber-safe.ch/de/willkommen/>) für Zollikofen als sinnvoll?*

Wenn ja, bis wann gedenkt er, dieses Label zu erlangen?

Wenn nein, weshalb kam er zu diesem Schluss?

Begründung

Cyberangriffe auf Behörden sind mittlerweile regelmässige Vorkommnisse. Zollkofen musste dies bereits schmerzlich erfahren. Solche Vorfälle sind unter anderem auch deshalb so gravierend, weil sie das Vertrauen der Bürgerinnen und Bürger in staatliche Institutionen schwächen kann. Deshalb ist es umso wichtiger, dass Gemeinden den Schutz der Daten, die sie verwalten, sehr ernst nehmen.

«Aufgrund der zunehmenden Bedrohung durch Cybervorfälle, und um eine bessere Übersicht über die Cyberbedrohungslage zu erhalten, hat der Bundesrat per 1. April 2025 die Meldepflicht für Cyberangriffe auf kritische Infrastrukturen in Kraft gesetzt. Betreiberinnen und Betreiber kritischer Infrastrukturen, zu denen auch die Gemeinden gehören, sind damit verpflichtet, Cyberangriffe innerhalb von 24 Stunden nach ihrer Entdeckung dem Bundesamt für Cybersicherheit (BACS) zu melden» (Zitat von https://www.chgemeinden.ch/de/newsroom/beitrag/2025_04_10_Seit-dem-1.-April-gilt-die-Meldepflicht-fuer-Cyberattacken.php).»

Antwort Gemeinderat

Frage 1

Wie wird die seit dem 1. April 2025 geltende Meldepflicht für Cybervorfälle in Zollikofen umgesetzt?

Die Meldepflicht ist der Gemeinde Zollikofen bekannt. Ein Cyberangriff muss dann gemeldet werden, wenn er die Funktionsfähigkeit der kritischen Infrastruktur gefährdet, eine Manipulation oder einen

Abfluss von Informationen verursacht oder mit Erpressung, Drohung oder Nötigung einhergeht. Seit dem letzten Angriff im November 2023 gab es keine Vorkommnisse. Der Angriff vom November 2023 wurde bereits damals, ohne dass eine obligatorische Meldepflicht bestand, den Aufsichtsbehörden von Kanton und Bund gemeldet.

Frage 2

Welche Massnahmen hat der Gemeinderat nach dem Hackerangriff vom November 2023 konkret ergriffen, um das Risiko für weitere Angriffe zu reduzieren?

Folgende organisatorische und technische Massnahmen (sogenannte Härtungsmassnahmen) wurden beim Wiederaufbau der Serverinfrastruktur umgesetzt:

Exchange Online (E-Mails, Kalender, Kontakte, Aufgaben)

Migration von Exchange Server (lokale Installation) auf Exchange Online. Exchange Online ist die gehostete Cloud-Lösung von Microsoft Exchange Server und ermöglicht ein Level an Sicherheit, welches bei einem lokalen Exchange Server nie erreicht werden kann.

Multi-Factor-Authentication (MFA)

Um die Sicherheit zu erhöhen, wurden alle Dienste in Microsoft 365 und der Fernzugriff (Citrix) mit einer zusätzlichen Authentifizierung mittels MFA gesichert.

Behördenlösung der Gemeinde Zollikofen

Die Behördenlösung wurde zusätzlich mittels DMZ (demilitarisierte Zone) abgesichert. In Computernetzwerken bezeichnet DMZ eine «neutrale Zone» zwischen dem Netzwerk und externen öffentlichen Netzwerken. Sie verhindern den direkten Zugriff auf einen Server mit Unternehmensdaten durch externe Nutzer. Eine DMZ bietet im Hinblick auf Firewalls zusätzliche Sicherheit.

Antivirus Microsoft Defender

Migration auf das Antivirusprogramm Microsoft Defender for Endpoint. Dieses bietet den grösseren Funktionsumfang sowie bessere Erkennungsmöglichkeiten betreffend Malware (Schadsoftware) und verdächtigem Verhalten als die bisherige Antivirus-Lösung. Durch den Einsatz von Microsoft Defender wird die ICT-Infrastruktur von einem Security Operation Center 24/7 überwacht (SOC-Anbindung).

Passwortrichtlinien

Die Passwortrichtlinien wurden verschärft, indem die Passwörter über mehr Zeichen (inkl. Zahlen und Sonderzeichen) verfügen müssen als bisher.

Schwachstellen-Scan (Network Vulnerability Trust)

Nach den umgesetzten Härtungsmassnahmen wurde am 16. Februar 2024 ein Schwachstellen-Scan durchgeführt. Dieser Scan prüfte die Erreichbarkeit von aussen auf die ICT-Infrastruktur der Gemeinde Zollikofen. Es sind keine Schwachstellen von aussen ersichtlich (Critical/High/Medium/Low). Der Schwachstellen-Scan hat mit dem bestmöglichen Resultat abgeschlossen.

Datensicherung (Backup)

Am 26. August 2024 wurde die Datensicherung (Backup) ersetzt. Vom Datenspeicher (Storage) wird auf den Backup-Server und von dort in ein Immutable Storage (unveränderlicher Speicher) gesichert. Als Sicherheitsmassnahme kann das Backup weder gelöscht noch manipuliert werden. Mit diesem Backup-System sind die Datensicherungen stets wiederherstellbar und vollständig vor einem Cyber-Vorfall (Ransomware) geschützt.

Phishing-Kampagne

Die meisten Cyberangriffe beginnen mit Phishing-Mails. Als «Phishing» bezeichnet man das Versenden betrügerischer Nachrichten, die scheinbar von einer legitimen und seriösen Quelle stammen. Dies geschieht in der Regel per E-Mail. Ziel des Angreifers ist es, Zugriff auf vertrauliche Daten und Anmeldeinformationen zu erhalten oder Schadsoftware auf dem Gerät des Opfers zu installieren.

Mittels Awareness-Kampagnen (z. B. Phishing-Kampagne) werden die Mitarbeitenden fortwährend sensibilisiert. Die Kampagnen werden mindestens einmal jährlich durchgeführt.

Schulung Mitarbeitende (bereits vor dem Cyberangriff bestehend)

Neueintretende Mitarbeitende absolvieren im Rahmen des Einführungsprogramms zwei eLearning-Module zwecks Sensibilisierung in Bezug auf Cybersicherheit.

Frage 3

Erachtet der Gemeinderat das Label «CyberSafe» (<https://www.cyber-safe.ch/de/willkommen/>) für Zollikofen als sinnvoll?

Wenn ja, bis wann gedenkt er, dieses Label zu erlangen?

Wenn nein, weshalb kam er zu diesem Schluss?

Nein.

Der Weg zum Label ist wie folgt beschrieben:

Technische Diagnose	Interner und externer Scan zum Aufspüren von Sicherheitslücken
Kompetenzen Diagnose	Phishing-Kampagne, Berichte und weiterführende Informationen
Governance Diagnose	- Ermittlung Risikoprofil und des Grads der Gefährdung (und des Verbesserungspotenzials) - Bewertung von organisatorischen Massnahmen (Passwort-Policy, etc.) - Bewertung der Beträge, die bei IT-Problemen auf dem Spiel stehen (Evaluierungsplattform)
Priorisierte Aktionen und korrektive Massnahmen	- Liste der priorisierten Massnahmen zur Verbesserung der IT und des Unternehmens - Organisatorische, technische und menschliche Massnahmen zur Verbesserung der eigenen Resilienz - Präsentationssitzung der priorisierten Aktionen und korrektiven Massnahmen
Cybersecurity-Audit	Ein abschliessendes Validierungs-Audit
Vergabe des Labels	Die Entscheidung zur Vergabe des Labels basiert auf dem Audit-Report
Kosten	Von der Diagnose bis zum Audit betragen die Kosten einmalig Fr. 4'000.00

Durch die Identifizierung von Schwachstellen können gezielte Massnahmen ergriffen werden, um die Sicherheit der ICT-Infrastruktur und der Daten zu erhöhen. Nach den Härtungsmassnahmen durch den Cyber-Angriff im November 2023 wurden viele Punkte/Massnahmen analog eines Cybersecurity-Checks durchgeführt. Der Gemeinderat ist nicht abgeneigt, die ICT-Sicherheit mittels einer externen Überprüfung durch eine neutrale Firma zu einem späteren Zeitpunkt durchführen zu lassen. Eine Zertifizierung in Form eines Labels (Gültigkeit 2 Jahre) erachtet der Gemeinderat als nicht nötig.

Beratung

GGR-Präsident Andreas Buser (GLP): Wir warten kurz, bis die Schülerinnen und Schüler den Raum verlassen haben. Vertreter des Gemeinderats ist Markus Burren. Das Eintreten ist vorgegeben. Wir kommen zur Geschäftsberatung. Die Antwort des Gemeinderats liegt vor. Hat der Gemeinderat Ergänzungen zur schriftlichen Antwort? Keine. Ist die Interpellantin mit der Antwort zufrieden? Sie kann das hier vorne kurz begründen.

Stéphanie Anliker (FDP): Herr Präsident, Herr Gemeindepräsident, geschätzte Mitglieder des Gemeinderats, werde Kolleginnen und Kollegen aus dem Rat. Ich danke dem Gemeinderat ganz herzlich für die Beantwortung meiner Interpellation. Es freut mich sehr zu sehen, dass nach dem Cyber-Angriff

im 2023 so viel passiert ist. Die Härtung der Systeme und die Sensibilisierung der Mitarbeitenden sind nur zwei Beispiele unter all den Massnahmen, die ergriffen worden und in der Antwort eindrücklich aufgelistet sind. Das ist ein wichtiger Schritt und zeigt mir auch, dass Cyber-Sicherheit ernst genommen wird in diesem Gremium. Das freut mich, ich möchte hier auch betonen: Cyber-Sicherheit kann keine einmalige Aufgabe sein, sondern ist eine Daueraufgabe. Es ist mir wichtig, dass man sich kontinuierlich dafür einsetzt. Danke vielmals, dass ihr das tut.

Kenntnisnahme

Die Antwort des Gemeinderats wird zur Kenntnis genommen.