BESCHLUSS
VOM 11. NOVEMBER 2021

GESCH.-NR.	2021-1559
BESCHLUSS-NR.	2021-227
IDG-STATUS	öffentlich

SIGNATUR	**16**	**GEMEINDEORGANISATION**
	16.04	**Grosser Gemeinderat**
	16.04.23	**Interpellationen**

BETRIFFT **Interpellation Simon Binder, SVP, und Mitunterzeichnende, betreffend IT-Sicherheit zur Prävention von Hackerangriffen auf unsere Stadt; Beantwortung des Vorstosses; Verabschiedung zu Handen des Grossen Gemeinderates**

VORSTOSS

Gemeinderat Simon Binder, SVP, und Mitunterzeichnende, reichen mit Schreiben vom 8. September 2021 nachfolgende Interpellation beim Büro des Grossen Gemeinderates ein (GGR-Geschäft-Nr. 2021/139):

In der Nacht von Samstag, den 29. auf Sonntag, den 30. Mai 2021 wurde die Gemeinde Rolle (VD) Opfer eines Hackerangriffs. In den vergangenen Wochen stellte sich mehr und mehr heraus, dass die Cyberattacke für die Gemeinde wohl weit gravierender sein dürfte, als bisher angenommen: dutzende Gigabyte an teils sensiblen Daten von rund 5'500 Bürgerinnen und Bürger von Rolle wie Name, Adresse, Geburtsdatum, AHV-Nummer, Personalbeurteilungen, Schulnoten, Kreditkarteninformationen, Passfotos usw. sind im Darknet frei zugänglich. Nach erfolgtem Angriff fehlte der Gemeinde dem vernehmen nach ein entsprechendes Notfalldispositiv, um mit geeigneten Sofortmassnahmen die Betroffenen adäquat zu Informieren und das Schadensausmass schnellstmöglich einzudämmen. [1]Nun kündigt die Hackergruppe namens «Vice Society», welche den Angriff auf Rolle für sich reklamiert an, dass sie auch andere Schweizer Gemeinden attackieren könnten.[2]

Die Bedrohung durch Cyberkriminalität nimmt zu. Jüngst berichteten die Medien von Angriffen auf namhafte Unternehmen wie Huber+Suhner, dem Medienkonzern TX Group und Stadler Rail.[3] Insbesondere Betreiber kritischer Infrastrukturen rüsten deshalb auf: So vermeldete beispielsweise der im 2019 gehackte Spital Wetzikon die erfolgte Ausarbeitung eines «IT-Notfallplans»,[4] oder die Stromnetzbetreiberin Swissgrid beauftragt aktuell mit Millionenaufträgen Informatikunternehmen für Belastungstests ihrer digitalen Sicherheitsinfrastruktur.[5] Während sich in der Privatwirtschaft das Wettrüsten gegen Hackergruppen schon deutlich abzeichnet, scheint das Thema Cybersicherheit für die Gemeinden erst mit dem «Fall Rolle» wieder Fahrt aufzunehmen.

[1] Vom Darknet-Leak zum Daten-GAU? Cyberangriff auf Gemeinde entpuppt sich als noch schlimmer, Watson, 30. August 2021.
[2] «Si nous avons accès à d'autres villes suisses que Rolle, nous les attaquerons aussi». Le Temps, 6. September 2021.
[3] Die internationale Cybermafia: Hackerangriff auf Firmen nehmen in der Schweiz bedrohliche Züge an, Luzerner Zeitung, 14. Januar 2021.
[4] Spitäler im Fokus der Hacker – so können Sie sich schützen, Zürich Versicherung, 10. Juni 2021.
[5] Angst vor Blackout: Stromnetzbetreiberin zahlt Millionen für Profi-Angreifer, Watson, 06. September 2021

Stadthaus
Märtplatz 29
Postfach
8307 Effretikon

Telefon 052 354 24 11
praesidiales@ilef.ch
www.ilef.ch
facebook.com/stadtilef

BESCHLUSS
VOM 11. NOVEMBER 2021

GESCH.-NR. 2021-1559
BESCHLUSS-NR. 2021-227

Zur Klärung der Sachlage in unserer Kommune bitte ich deshalb den Stadtrat um die schriftliche Beantwortung folgender Fragen:

1. Wie hoch schätzt der Stadtrat die Gefahr eines Hackerangriffs auf Illnau-Effretikon ein?
2. Ist dem Stadtrat bekannt, ob unsere Stadt bereits einmal Opfer eines Hackerangriffs wurde oder ob es in der Vergangenheit entsprechende Angriffsversuche gab?
3. Sind ausgelöst durch den Angriff auf Rolle in unserer Stadt bereits Präventionsmassnahmen erfolgt oder sind solche geplant?
4. Wann und in welchem Umfang erfolgte in unserer Stadt die letzte Überprüfung oder Überarbeitung der IT-Sicherheitssysteme?
5. Erfolgt für Mitarbeitende der städtischen Verwaltung bei Stellenantritt und in regelmässigen Abständen eine Schulung, bzw. Auffrischung zur Cybersicherheit? Besteht ein IT-Konzept bez. Datensicherheit und Umgang mit sensiblen Daten? In welchem Rhythmus werden diese geprüft?
6. Verfügt unsere Stadt im Falle eines Datenverlusts über ein Notfalldispositiv, um Schäden schnellstmöglich und bestmöglich einzudämmen?
7. Welches Ressort der Exekutive ist verantwortlich für die gesamte IT-Infrastruktur der Stadt?
8. Sind die Verantwortlichkeiten bzgl. Informatikstruktur in der Stadtverwaltung klar geregelt?
9. Wie erfolgt die Speicherung hochsensibler Daten (z.B. Steuererklärungen)? Wie kann ein Fremdzugriff ausgeschlossen werden? Wie wird der Restore des Backups überprüft?

URHEBER:	Gemeinderat Simon Binder, SVP
MITUNTERZEICHNENDE:	Gemeinderat Yves Cornioley, SVP Gemeinderat René Truninger, SVP Gemeinderat Paul Rohner, SVP Gemeinderat Thomas Schumacher, SVP
EINGANG RATSBÜRO:	08.09.2021
BEGRÜNDUNG IM RAT:	07.10.2021
FRIST:	07.01.2022

BESCHLUSS
VOM 11. NOVEMBER 2021

GESCH.-NR. 2021-1559
BESCHLUSS-NR. 2021-227

DER STADTRAT ILLNAU-EFFRETIKON
ANTWORTET WIE FOLGT:

VORBEMERKUNG

Der Stadtrat erachtet es aus sicherheitsrelevanten Gründen als kritisch, öffentlich zu detailliert über die einzelnen Konzepte und Massnahmen zur Informatiksicherheit zu berichten. Er bittet um Verständnis, dass er deshalb gewisse Fragen teilweise in allgemeiner Form beantwortet.

ZUR FRAGE 1:
Wie hoch schätzt der Stadtrat die Gefahr eines Hackerangriffs auf Illnau-Effretikon ein?

Die Gefahr von Cyberangriffen auf die IT-Infrastruktur der Stadt wird als real eingeschätzt. Für den Stadtrat und die Stadtverwaltung geniesst das Thema deshalb hohe Priorität.

Generelle Statistiken zu Cybermeldungen sind zu finden auf der Webseite des nationalen Zentrums für Cybersicherheit: https://www.ncsc.admin.ch/ncsc/de/home.html

ZUR FRAGE 2:
Ist dem Stadtrat bekannt, ob unsere Stadt bereits einmal Opfer eines Hackerangriffs wurde oder ob es in der Vergangenheit entsprechende Angriffsversuche gab?

In der langjährigen Zusammenarbeit zwischen der Stadt und der OBT AG als Fulloutsourcing-Partnerin war die Stadt noch nie Opfer eines Hackerangriffs geworden. Es sind auch keine Angriffsversuche bekannt. Es kann aber nicht ausgeschlossen werden, dass es solche Versuche gab. Dasselbe gilt für die IT-Systeme der Schule.

ZUR FRAGE 3:
Sind ausgelöst durch den Angriff auf Rolle in unserer Stadt bereits Präventionsmassnahmen erfolgt oder sind solche geplant?

Als Folge des Angriffs auf die Gemeinde Rolle VD und weitere Kommunen erfolgten keine unmittelbaren weiteren Präventionsmassnahmen. Um eine hohe Betriebs- und Datensicherheit zu erfüllen, sind stetige Optimierungen und Anpassungen notwendig.

Die OBT AG betreibt ein Informationssicherheits-Managementsystem, das nach ISO 27001 zertifiziert ist. Dieses dient dazu, Informationen vertraulich zu behandeln und vor Bedrohungen aufgrund der aktuellen Risikoeinschätzung zu schützen. Es beinhaltet Sicherheitsvorkehrungen in den beiden georedundanten Datencentern, Massnahmen im Bereich Informationssicherheit sowie technische Sicherheitsvorkehrungen. Damit wird eine kontinuierliche Informationssicherheit sichergestellt und gegenüber den Kunden dokumentiert.

Die Sicherheit der Schul-IT-Systeme wird ebenfalls laufend optimiert und den neusten Erkenntnissen angepasst.

BESCHLUSS
VOM 11. NOVEMBER 2021

GESCH.-NR. 2021-1559
BESCHLUSS-NR. 2021-227

ZUR FRAGE 4:
Wann und in welchem Umfang erfolgte in unserer Stadt die letzte Überprüfung oder Überarbeitung der IT-Sicherheitssysteme?

Der Datenschutzbeauftragte des Kantons Zürich führte zuletzt im Jahr 2018 ein komplettes Audit über den Datenschutz und die Datensicherheit in der Stadtverwaltung durch. Dabei wurde festgestellt, dass die Stadtverwaltung über einen gut geregelten Informatikbetrieb verfügt und dafür ausreichende vertragliche Regelungen bestehen. Diverse im Rahmen des Audits empfohlene Optimierungen wurden zeitgerecht umgesetzt und vom Datenschutzbeauftragten verifiziert.

Die OBT AG führt regelmässig sogenannte Penetrationstests durch. Diese dienen dazu, Spionage vorzubeugen und Sabotage durch Eindringlinge zu unterbinden. In der Regel werden solche Tests nach erfolgtem Auf- und/oder Ausbau eines kritischen, wichtigen Systems in Auftrag gegeben. Die Erkenntnisse aus den Tests, welche die Datensicherheit erhöhen, werden umgehend an die Hand genommen und umgesetzt.

Die Schule hat im letzten Jahr neue Serversysteme angeschafft. Die Datensicherheit bildete einen zentralen Punkt bei der Planung und Umsetzung.

ZUR FRAGE 5:
Erfolgt für Mitarbeitende der städtischen Verwaltung bei Stellenantritt und in regelmässigen Abständen eine Schulung, bzw. Auffrischung zur Cybersicherheit? Besteht ein IT-Konzept bez. Datensicherheit und Umgang mit sensiblen Daten? In welchem Rhythmus werden diese geprüft?

Die Sensibilisierung aller Informatiknutzenden wird als wichtigste Massnahme zur Abwehr von Cyberangriffen erachtet. Der Mensch ist bei einer Cyberbedrohung oft das schwächste Glied in der Kette.

Alle städtischen Mitarbeitende müssen in den ersten Wochen nach Stellenantritt einen Onlinekurs zum Thema «Informatiksicherheit» erfolgreich abschliessen. Dadurch erlangen sie das notwendige Fachwissen und sie werden auf die Informatiksicherheit sensibilisiert. Über aktuelle Bedrohungen und Informatikthemen generell werden die Mitarbeitenden nach Bedarf schriftlich und mündlich orientiert. Momentan wird geprüft, das Wissen der Mitarbeitenden über Datenschutz und Datensicherheit in kürzeren Abständen gezielt zu testen.

Die Stadt verfügt über ein IT-Konzept, eine Leitlinie und eine Weisung zur Informationssicherheit. Letztere ist auch integrierender Bestandteil der Anstellungsverfügungen für alle Mitarbeitenden. Die Unterlagen werden nach Bedarf überprüft und aktualisiert. Die im Sommer 2021 durchgeführte externe Analyse und Standortbestimmung des ICT-Betriebs zeigt, dass dieser strategisch und operativ einen vergleichsweise sehr guten Standard bei unterdurchschnittlichen Kosten aufweist.

ZUR FRAGE 6:
Verfügt unsere Stadt im Falle eines Datenverlusts über ein Notfalldispositiv, um Schäden schnellstmöglich und bestmöglich einzudämmen?

Ja, die Stadt verfügt über ein Notfallkonzept für den Informatikbetrieb. Dieses trägt dazu bei, bei Vorfällen Schäden zu minimieren.

Die OBT AG verfügt ebenfalls über eine Notfallplanung. Diese verfolgt das Ziel, wonach kritische Services oder Infrastrukturen nach einem Unterbruch innerhalb der definierten Wiederlaufzeit wieder zur Verfügung stehen. Mit regelmässigen Tests und Übungen wird sichergestellt, dass die Wiederherstellung der Daten und die Wiederaufnahme des Betriebs im Notfall reibungslos verläuft.

Die Schule verfügt über mehrfach gesicherte Server. Die externen Anbieter sorgen ebenfalls für eine hohe Sicherheit und Verfügbarkeit.

BESCHLUSS
VOM 11. NOVEMBER 2021

GESCH.-NR. 2021-1559
BESCHLUSS-NR. 2021-227

ZUR FRAGE 7:
Welches Ressort der Exekutive ist verantwortlich für die gesamte IT-Infrastruktur der Stadt?

Zuständig sind das Ressort Präsidiales für die Infrastruktur der Stadtverwaltung sowie das Ressort Bildung für den Teil der Schulinformatik.

ZUR FRAGE 8:
Sind die Verantwortlichkeiten bzgl. Informatikstruktur in der Stadtverwaltung klar geregelt?

Ja. Die Gesamtverantwortung liegt beim Stadtschreiber sowie bei der Leiterin Bildung für die Schulinformatik. Die operative Leitung wird durch den Leiter Informatik sowie durch den Leiter Informatik Schule wahrgenommen.

ZUR FRAGE 9:
Wie erfolgt die Speicherung hochsensibler Daten (z.B. Steuererklärungen)? Wie kann ein Fremdzugriff ausgeschlossen werden? Wie wird der Restore des Backups überprüft?

Steuererklärungen werden direkt über die Kantonsapplikation «ARTS» als Bilddateien auf der kantonalen Serverinfrastruktur abgespeichert. Steuerdaten, die mittels der Applikation «iCity» erfasst werden, oder auch weitere sensible Daten, sind auf den Datenbankservern der OBT gesichert und werden mittels Netbackup durch das Rechenzentrum gesichert.

Ein Fremdzugriff wird durch verschiedene Massnahmen ausgeschlossen. Stichworte dazu sind: Vergabe von Zugriffsrechten unter Einhaltung eines dokumentierten Prozesses, Überwachung sämtlicher Remote-Access-Zugriffe, Zwei-Faktoren-Authentifizierung, Verschlüsselung des Datenverkehrs, Verbindungsverschlüsselung, Datenhaltung ausschliesslich in der Schweiz, physische Sicherheit der Rechenzentren, Einhaltung der Bearbeitungsrichtlinien für «besonders schützenswerte Personendaten».

Es besteht ein definiertes Datensicherungskonzept. Der Restore der Backups wird monatlich getestet und protokolliert. Auch nach einem Update der Backup-Infrastruktur werden Restore-Tests durchgeführt.

BESCHLUSS
VOM 11. NOVEMBER 2021

GESCH.-NR. 2021-1559
BESCHLUSS-NR. 2021-227

DER STADTRAT ILLNAU-EFFRETIKON
AUF ANTRAG DES RESSORTS PRÄSIDIALES
BESCHLIESST:

1. Die vorstehende Antwort wird zu Handen des Grossen Gemeinderates verabschiedet.
2. Als zuständiger Referent für allfällige Auskünfte wird Stadtpräsident Ueli Müller bezeichnet.
3. Mitteilung durch Protokollauszug an:
   a. Abteilung Präsidiales, Ratssekretariat (zur Weiterleitung an den Grossen Gemeinderat)
   b. Stadtschreiber
   c. Abteilung Bildung

Stadtrat Illnau-Effretikon

Ueli Müller
Stadtpräsident

Peter Wettstein
Stadtschreiber

Versandt am: 15.11.2021