Auszug aus dem Protokoll des Regierungsrates des Kantons Zürich

KR-Nr. 261/2026

Sitzung vom 21. Oktober 2026

1096. Anfrage (Cyberbedrohung – wie schützt sich der Kanton Zürich)

Kantonsrätin Barbara Franzen, Niederweningen, sowie die Kantonsräte Martin Huber, Neftenbach, und Thomas Huber, Rümlang, haben am 29. Juni 2026 folgende Anfrage eingereicht:

Wie kann sich der Kanton Zürich als Organisation und seine Bevölkerung vor Cyberbedrohungen schützen? Diese Frage stellt sich angesichts der zunehmenden Digitalisierung kritischer Infrastrukturen je länger je mehr als Herausforderung. Zudem wären die Auswirkungen eines entsprechenden Angriffs nicht auf die Infrastruktur markant, sondern auch im Bereich der Verwaltung, der Schulen, bei der Bevölkerung. Bei der Beantwortung der untenstehenden Fragen versteht es sich von selbst, dass es im Sinne der Sicherheit nicht um Bekanntgabe von Sicherheitsdispositivs geht, sondern um organisatorische Fragen.

Wir bitten den Regierungsrat in diesem Zusammenhang, folgende Fragen zu beantworten:

1. Die Cyberkriminalität ist zwar 2025 gemäss Statistik der Kantonspolizei leicht gesunken (2,5 Prozent), bleibt aber auf hohem Niveau. Wie schützt der Kanton Zürich die Bevölkerung weiterhin aktiv?
2. Wie schützt der Kanton Zürich kritische Infrastrukturanlagen – Energieproduktionsanlagen, Datencenterschadenslagen, Spitäler etc. -, die zu einem Ausfall der Strom-, Trinkwasser-, Lebensmittel- oder Medikamentenproduktion führen könnten, vor Cyberangriffen?
3. Welche Zusammenarbeitsformen wurde nach Beantwortung der Anfrage 43/2023 weiter vertieft insbesondere zwischen dem Kanton und privaten Betreibern von Anlagen (Spitäler, Datencenter)?
4. Wie arbeitet der Kanton mit dem Bund zusammen? Über welche Kanäle läuft die Zusammenarbeit, beispielsweise mit dem Nationalen Zentrum für Cybersicherheit (NCSC)?
5. Wo steht die Umsetzung der «Kantonalen Cybersicherheitsstrategie leisten», die der Zürcher Regierungsrat im Mai 2022 verabschiedet hat?
6. Welche Schwerpunkte will der Kanton bei der Bekämpfung von Cyberkriminalität setzen?
7. Welche Erkenntnisse schöpft der Kanton Zürich aus den Forschungsprojekten der angesiedelten Hochschulen (ZHAW, UZH, ETH)?

8. Wie organisiert der Kanton im Falle einer Grossschadenslage durch einen Cyberangriff die Bekämpfung einer solchen Notsituation? Welche Erkenntnisse liefert das neue Cyber Resilience Network des Kantons Zürich (CYREN-ZH)?

Auf Antrag der Finanzdirektion

beschliesst der Regierungsrat:

I. Die Anfrage Barbara Franzen, Niederweningen, Martin Huber, Neftenbach, und Thomas Huber, Rümlang, wird wie folgt beantwortet:

Zu Frage 1:

Der Kanton Zürich setzt beim Schutz der Bevölkerung weiterhin auf einen mehrstufigen Ansatz mit Prävention, einfachen Melde- und Anzeigemöglichkeiten sowie einer spezialisierten Strafverfolgung.

Die Kantonspolizei informiert über ihre Webseite, ihre Medienarbeit, Kampagnen und Präventionsveranstaltungen über aktuelle Formen der Cyberkriminalität und geeignete Schutzmassnahmen. Einzelne Präventionsangebote richten sich gezielt an besonders gefährdete Bevölkerungsgruppen, beispielsweise an ältere Menschen. Gemeinsam mit anderen Polizeikorps betreibt sie zudem die Plattform cybercrimepolice.ch. Diese wurde 2025 national ausgerichtet und in das Netzwerk für die Ermittlungsunterstützung in der digitalen Kriminalitätsbekämpfung integriert. Über die Plattform wurden 2025 gesamtschweizerisch rund 33 000 Anfragen aus der Bevölkerung beantwortet. Geschädigte können sich daneben auch einfach an jeden Polizeiposten, an den Online-Polizeiposten oder in dringenden Fällen an die Notrufnummer 117 wenden.

Die Kantonspolizei arbeitet eng mit der Staatsanwaltschaft zusammen und bekämpft konsequent die Cyberkriminalität. Innerhalb der Staatsanwaltschaft ist die Bearbeitung von Cyberkriminalität insbesondere bei der spezialisierten Staatsanwaltschaft II angesiedelt. Zusätzlich verfügt jede regionale Staatsanwaltschaft über eine auf Cyberkriminalität spezialisierte Stelle. Damit steht das erforderliche Fachwissen sowohl zentral als auch in den Regionen zur Verfügung.

Zu Frage 2:

Beim Schutz kritischer Infrastrukturen vor Cyberangriffen nehmen Betreiberinnen und Betreiber, Kanton, Bund und weitere zuständige Stellen je eigene Rollen wahr. Die Verantwortung für den sicheren Betrieb sowie für die erforderlichen technischen und organisatorischen Sicherheitsmassnahmen liegt bei den jeweiligen Betreiberorganisationen. Der Kanton Zürich unterstützt die Organisationen insbesondere durch die Umsetzung der kantonalen Cybersicherheitsstrategie, den Austausch zur Bedrohungslage sowie die Vernetzung und Sensibilisierung von Be-

treiberinnen und Betreibern kritischer Infrastrukturen. Die konkrete Ausgestaltung der Schutzmassnahmen richtet sich nach dem jeweiligen Schutzbedarf, den Risiken sowie den gesetzlichen und sektorspezifischen Anforderungen. Je nach Sektor sind dabei insbesondere die anwendbaren Vorgaben und IKT-Minimalstandards des Bundes zu berücksichtigen. Aufgrund der unterschiedlichen Aufgaben, Technologien und Betriebsmodelle gibt es keine einheitliche technische Schutzlösung für sämtliche kritischen Infrastrukturen.

Für die Infrastrukturen, Systeme und Leistungen in seinem eigenen Zuständigkeitsbereich legt der Kanton risikobasiert Schutzmassnahmen fest und überprüft diese regelmässig. In Bereichen, in denen der Kanton über gesetzliche Zuständigkeiten verfügt, legt er zusätzliche Anforderungen fest. Dies gilt beispielsweise für die Anforderungen des Regierungsrates an die Listenspitäler zum Datenschutz und zur Informationssicherheit. Die Zürcher Spitäler führen ihren Betrieb eigenständig und sind daher selbst für den Schutz ihrer Infrastruktur und Systeme vor Cyberangriffen verantwortlich. Sie sind bundesrechtlich verpflichtet, erhebliche Cyberangriffe innert 24 Stunden nach deren Entdeckung dem Bundesamt für Cybersicherheit (BACS) zu melden (Art. 74b Abs. 1 Bst. c, f und g in Verbindung mit Art. 74e Informationssicherheitsgesetz vom 18. Dezember 2020 [SR 128]). Die Meldungen tragen zu einem gesamtschweizerischen Lagebild bei. Der Regierungsrat legt die Anforderungen an die Listenspitäler gestützt auf § 7 Abs. 1 lit. c des Spitalplanungs- und -finanzierungsgesetzes vom 2. Mai 2011 (LS 813.20) fest, darunter auch betreffend Datenschutz und Informationssicherheit. Gegenüber den vier kantonalen Spitälern formuliert der Regierungsrat zusätzlich die Erwartung, dass die Synergien unter den Spitälern insbesondere im Bereich der Cybersicherheit ausgeschöpft werden (vgl. beispielhaft RRB Nr. 568/2026 für das Universitätsspital Zürich).

Bund, Kantone, Gemeinden, zuständige Fachbehörden und Branchenorganisationen nehmen je nach Versorgungsbereich unterschiedliche Aufgaben wahr. Das BACS unterstützt den nationalen Informationsaustausch zu Cyberbedrohungen und stellt Informationen und Hilfsmittel zur Verfügung. Das Bundesamt für Bevölkerungsschutz koordiniert im Rahmen der nationalen Strategie zum Schutz kritischer Infrastrukturen die periodische Betrachtung der Widerstandsfähigkeit der verschiedenen Sektoren. Die Überprüfungen werden durch die jeweils zuständigen Fachstellen durchgeführt.

Der Informations- und Erfahrungsaustausch wird zudem durch sektorspezifische Cyber Security Centers unterstützt. Entsprechende Strukturen bestehen unter anderem im Finanzsektor (Swiss Financial Sector Cyber Security Centre) und im Gesundheitswesen (Healthcare Cyber Security Center). Sie berücksichtigen die besonderen Bedürfnisse ihres jeweiligen Sektors und arbeiten mit dem BACS zusammen.

Zu Frage 3:

Seit der Beantwortung der Anfrage KR-Nr. 243/2023 betreffend Wie sicher ist der Kanton Zürich vor Cyberangriffen? wurden verschiedene Formen der Zusammenarbeit geschaffen, auf die nachfolgend kurz exemplarisch eingegangen wird. Ausserdem wird im Rahmen der kantonalen Cybersicherheitsstrategie die Zusammenarbeit mit den Betreiberinnen und Betreibern laufend weiterentwickelt. Im Vordergrund stehen dabei der Informations- und Erfahrungsaustausch, die Sensibilisierung für aktuelle Cyberrisiken sowie die Vernetzung der zuständigen Stellen und Betreiberorganisationen.

Im Gesundheitsbereich ist der regelmässige Austausch zwischen der Gesundheitsdirektion, den vier kantonalen Spitälern und dem Kinderspital in einer Vernetzungsgruppe institutionalisiert. Zudem wurde 2025 der nationale Verein «Healthcare Cyber Security Center» gegründet, dem unter anderem die vier kantonalen Spitäler sowie zahlreiche weitere Zürcher Spitäler angehören. Damit wird die kantonale Zusammenarbeit durch eine nationale und sektorspezifische Vernetzung ergänzt.

Die bereits 2023 im Rahmen eines Pilotversuchs begonnene Zusammenarbeit zu Cyberrisiken in der Lieferkette wurde unter Einbezug der kantonalen Spitäler weitergeführt. Dabei geht es insbesondere darum, Risiken im Zusammenhang mit externen Lieferantinnen, Lieferanten und Leistungserbringenden zu beurteilen und angemessen zu behandeln.

Mit Beschluss Nr. 834/2026 hat der Regierungsrat zudem die stärkere Vernetzung staatlicher Stellen mit Wirtschaft und Forschung im sicherheitspolitischen Bereich beschlossen. Die vorgesehenen Aktivitäten gliedern sich in die Stossrichtungen Sensibilisierung, Schutz und Vernetzung und beziehen die Cybersicherheit von Unternehmen ausdrücklich ein.

Zu Frage 4:

Das in der Anfrage erwähnte Nationale Zentrum für Cybersicherheit wurde per 1. Januar 2024 ins BACS überführt und ist heute im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport angesiedelt. Das BACS ist die zentrale Ansprechstelle des Bundes für Cybersicherheit. Die Zusammenarbeit des Kantons Zürich mit dem Bund erfolgt über drei Ebenen: die strategische Mitwirkung, den Austausch von Informationen zur Bedrohungslage sowie die Nutzung von technischen Sicherheitsangeboten des Bundes.

Zum einen wirkt der Kanton an der Umsetzung der Nationalen Cyberstrategie mit. Er beteiligt sich am mehrmals jährlich stattfindenden Umsetzungsforum des Bundes und bringt seine Erfahrung über strukturierte Workshops und die daraus folgenden Arbeiten ein. Ergänzend

liefert der Kanton dem strategischen Controlling des Bundes quartalsweise ein Reporting zu ausgewählten Sicherheitsmassnahmen. Damit trägt er zur gesamtschweizerischen Überprüfung der Fortschritte bei und gestaltet die Weiterentwicklung der nationalen Vorgaben aktiv mit.

Zum anderen besteht ein regelmässiger Austausch zur aktuellen Bedrohungslage. Die zentrale Sicherheitsüberwachung des Kantons (Security Operations Center) ist in den vertraulichen Informationsaustausch des Bundes mit Betreiberinnen und Betreibern kritischer Infrastrukturen eingebunden. Sie erhält dadurch frühzeitig Warnungen, Lageinformationen und Handlungsempfehlungen. Der Kanton kann neue Bedrohungen damit frühzeitig beurteilen und seine Schutzmassnahmen bei Bedarf anpassen. Der Informationsfluss verläuft in beide Richtungen: Seit dem 1. April 2025 sind die Verwaltungen der Kantone und Gemeinden gesetzlich verpflichtet, Cyberangriffe innerhalb von 24 Stunden nach ihrer Entdeckung dem BACS zu melden. Der Kanton Zürich verfügt über eingespielte interne Abläufe, um sicherheitsrelevante Vorfälle rasch zu erkennen, zu beurteilen und fristgerecht zu melden. Er erfüllt damit nicht nur seine gesetzliche Pflicht, sondern leistet auch einen Beitrag zum nationalen Lagebild.

Schliesslich nutzt der Kanton die technischen Sicherheitsangebote des Bundes, die das BACS Betreiberinnen und Betreibern kritischer Infrastrukturen zur Verfügung stellt. Sie sind in die Sicherheitsvorkehrungen der kantonalen Verwaltung eingebunden und unterstützen den Kanton dabei, Cyberangriffe frühzeitig zu erkennen und das Risiko erfolgreicher Angriffe zu vermindern.

Neben diesen institutionalisierten Kanälen bestehen etablierte fachliche Kontakte zwischen den zuständigen Stellen des Kantons und des Bundes. Sie ermöglichen kurze Wege und eine rasche Abstimmung, sowohl im Alltag als auch im Ereignisfall.

Zu Frage 5:

Der Regierungsrat hat den Entwicklungsschwerpunkt zur Umsetzung der kantonalen Cybersicherheitsstrategie gemäss RRB Nr. 676/2022 im Geschäftsbericht 2025 als abgeschlossen ausgewiesen. Die damit verbundenen Aufbauarbeiten wurden weitgehend umgesetzt. Bereits etablierte Leistungen werden im ordentlichen Betrieb weitergeführt und bedarfsgerecht weiterentwickelt. Noch laufende Aktivitäten sollen, soweit sie für die künftige Ausrichtung weiterhin erforderlich sind, in die mit der neuen Strategie Informationssicherheit zu schaffende Umsetzungsorganisation überführt werden. Informations- und Cybersicherheit bleiben damit Daueraufgaben.

Ein Schwerpunkt lag auf der Stärkung der Sicherheitskultur, da Cyberangriffe häufig mit Täuschungsversuchen wie gefälschten E-Mails beginnen. Ergänzend wurde der Aufbau weiterer zentraler Sicherheitsdienstleistungen vorangetrieben, um Synergien innerhalb der Verwaltung zu nutzen und ein abgestimmtes Schutzniveau in den Direktionen und der Staatskanzlei zu fördern.

Die Cybersicherheitsstrategie soll im Abstand von drei Jahren überprüft und aktualisiert werden. Seit der Festsetzung im Mai 2022 haben sich die Bedrohungslage, die technologischen Möglichkeiten, die regulatorischen Rahmenbedingungen und die Abhängigkeiten von externen Leistungserbringenden weiterentwickelt. Die Revision erfolgt somit sowohl im vorgesehenen Aktualisierungszyklus als auch aufgrund der veränderten Rahmenbedingungen.

Die revidierte Strategie soll Cyber- und Informationssicherheit in einem gemeinsamen Rahmen zusammenführen. Damit sollen Digitalisierung und Informationssicherheit noch enger miteinander verbunden werden. Die neue Steuerung soll eine regelmässige Überprüfung und Anpassung der Schwerpunkte und Massnahmen ermöglichen. Ein Entwurf liegt vor und befindet sich in Konsultation. Die Festsetzung durch den Regierungsrat ist für Ende 2026 geplant.

Zu Frage 6:

Der Kanton setzt bei der Bekämpfung der Cyberkriminalität auf zwei Ebenen Schwerpunkte. Im Rahmen der Legislaturziele des Regierungsrates (RRZ) für die Legislaturperiode 2023–2027 wurden Projekte zur digitalen Beweisführung, zum Umgang mit digitalen Spuren und Kryptowährungen, zum Schutz älterer Menschen sowie zur Bekämpfung der Pädokriminalität im Internet angestossen (vgl. Richtlinien der Regierungspolitik 2023–2027 [RRB Nr. 871/2023], Massnahmen zu RRZ 1). Mit diesen Projekten wurden wertvolle Methoden und Ansätze für die Strafverfolgung entwickelt und wichtige Impulse gegeben. Die Kantonspolizei legt dabei einen besonderen Schwerpunkt auf die konsequente digitale Beweisführung.

Daneben betreibt die Staatsanwaltschaft in enger Abstimmung mit der Kantonspolizei ein strategisches Ressourcen- und Schwerpunktmanagement. Gemeinsame Planungsinstrumente wie der Kriminalitätsradar unterstützen die Strafverfolgungsbehörden dabei, neue Entwicklungen frühzeitig zu erkennen und ihre Prioritäten entsprechend festzulegen.

Bei der Strafverfolgung im Bereich Cybercrime, mit Schwerpunkt in den Bereichen der virtuellen Pädokriminalität, der digitalisierten Betrugsformen und Ransomware, setzt der Kanton sechs spezialisierte Staatsanwältinnen und Staatsanwälte ein. Ergänzend dazu werden für vorgelagerte Phänomene (wie z. B. Money Mules, Verdachtsmeldungen

des National Center for Missing & Exploited Children usw.) und Massendelinquenz, wie beispielsweise Betrugsfälle auf Onlineplattformen, auf regionaler Ebene vier Cybercrime-Spezialistinnen und -Spezialisten eingesetzt.

Da sich die Erscheinungsformen der Cyberkriminalität rasch verändern, überprüfen Kantonspolizei und Staatsanwaltschaft ihre Schwerpunkte und den Einsatz ihrer Mittel laufend. Dies ermöglicht es ihnen, sowohl im operativen Alltag als auch in der längerfristigen Planung flexibel auf neue Entwicklungen zu reagieren.

Zu Frage 7:

Mit der ETH Zürich, der Universität Zürich und der Zürcher Hochschule für Angewandte Wissenschaften verfügt der Kanton über ausgewiesene Forschungskompetenzen im Bereich der Cybersicherheit. Der Austausch erfolgt über verschiedene Gefässe, wie über das Cyber Resilience Network des Kantons Zürich (CYREN-ZH), über gemeinsame Fach- und Weiterbildungsveranstaltungen, über die gemeinsame Mitwirkung in nationalen Gremien, wie dem Umsetzungsforum der Nationalen Cyberstrategie, sowie über den direkten fachlichen Kontakt zwischen den zuständigen Stellen der Verwaltung und den Forschungsinstituten. Die Hochschulen ergänzen die verwaltungsinterne Fachkompetenz durch wissenschaftliche Expertise und ermöglichen den Zugang zu aktuellen Forschungserkenntnissen.

Arbeiten der Hochschulen zu Cybersicherheit, Desinformation und Datenschutz helfen dem Kanton dabei, Entwicklungen frühzeitig einzuordnen und komplexe Fragestellungen fachlich fundiert zu beurteilen. Ebenso entstehen aus der Zusammenarbeit der Hochschulen mit Behörden und Zürcher Unternehmen neue Ansätze und Werkzeuge, wie zum Beispiel Verfahren zur Beurteilung von Bedrohungsinformationen, zur Analyse von Cyberangriffen und zur Bestimmung angemessener Schutzmassnahmen. Diese kann der Kanton anschliessend bei Eignung in die eigenen Prozesse übernehmen.

Die Zusammenarbeit entfaltet auch über die kantonale Verwaltung hinaus Wirkung. Ein konkretes Beispiel ist die Cybersecurity Clinic von CYREN-ZH. Studierende bearbeiten dort unter fachlicher Begleitung Sicherheitsfragestellungen von Gemeinden, kleinen und mittleren Unternehmen sowie gemeinnützigen Organisationen und erarbeiten praxistaugliche Empfehlungen. Die beteiligten Organisationen erhalten Unterstützung bei konkreten Sicherheitsfragen, während die Studierenden Praxiserfahrung sammeln.

Die Aus- und Weiterbildungsangebote der Hochschulen, Fachworkshops und die Summer School leisten darüber hinaus einen Beitrag zur Ausbildung von Fachkräften. Diese Angebote werden auch von Mitarbeitenden der kantonalen Verwaltung genutzt.

Der Regierungsrat misst dem Austausch mit den Hochschulen grosse Bedeutung bei. Die gewonnenen Erkenntnisse werden bei der Weiterentwicklung der kantonalen Vorgaben und Massnahmen im Bereich der Informationssicherheit berücksichtigt. Der Austausch mit den Hochschulen soll auch künftig fortgeführt werden.

Zu Frage 8:

Im Rahmen des integralen Risikomanagements wird ein einheitlicher Ansatz für das Krisenmanagement der kantonalen Verwaltung erarbeitet. Dabei werden die Anforderungen an die Krisenmanagementfähigkeit, eine geeignete direktionsübergreifende Krisenorganisation und die entsprechenden Verfahren festgelegt.

Wird ein grossangelegter Cyberangriff als Krise mit Auswirkungen über eine einzelne Direktion hinaus beurteilt, erfolgt die übergeordnete Bewältigung durch diese Krisenorganisation. Die technische und operative Behandlung des Cybervorfalls erfolgt durch die für die betroffenen Systeme oder Leistungen zuständigen Stellen. Je nach betroffener Leistung sind dies das Amt für Informatik oder der zuständige externe Leistungserbringer. Die betroffenen internen Stellen werden einbezogen.

Neben der Krisenorganisation der Verwaltung setzt der Kanton auf die kantonsweite Vernetzung. Das Projekt CYREN-ZH hat untersucht, unter welchen Voraussetzungen freiwillige Cyberfachkräfte in einer Grossschadenslage beigezogen werden könnten. Dabei zeigte sich, dass grundsätzlich Interesse und Fachkompetenz vorhanden sind, gegenwärtig aber die notwendigen rechtlichen und organisatorischen Grundlagen fehlen. Insbesondere sind Fragen der Haftung, des Versicherungsschutzes und des Arbeitsrechts zu klären.

CYREN-ZH konzentriert sich deshalb derzeit auf die Prävention, den Wissensaustausch und den Aufbau von Netzwerken. Die gewonnenen Erfahrungen und Kontakte können für die Krisenvorsorge und eine mögliche spätere Weiterentwicklung genutzt werden. Ein operativer Einsatz freiwilliger Fachkräfte würde vorgängig eine vertiefte Prüfung der rechtlichen, organisatorischen und finanziellen Voraussetzungen erfordern.

II. Mitteilung an die Mitglieder des Kantonsrates und des Regierungsrates sowie an die Finanzdirektion.

Vor dem Regierungsrat
Die Staatsschreiberin:
Kathrin Arioli