**Auszug aus dem Protokoll**
**des Regierungsrates des Kantons Zürich**

Sitzung vom 4. Mai 2022

## 676. Cybersicherheitsstrategie (Festsetzung, Umsetzung, Stellenplan, Ausgabenbewilligung)

### 1. Ausgangslage

Studien wie das «Risikobarometer 2021» der Allianz-Versicherungen oder der «Global Risks Report 2021» des World Economic Forum zeigen auf, dass die Bedrohung durch Cyberangriffe steigt. Die Spannweite der Cyberrisiken reicht von der Cyberkriminalität zur finanziellen Bereicherung über Desinformations- und Propagandakampagnen und Spionagetätigkeiten mithilfe von Cyberangriffen bis hin zur Cybersabotage von kritischen Infrastrukturen. Wer die Chancen der Digitalisierung nutzen will, muss sich vor diesen Bedrohungen schützen.

Der Schutz vor Cyberrisiken trägt zur digitalen Sicherheit bei. Er schafft Vertrauen in digitale Prozesse, vermindert organisatorische und technische Risiken sowie Risiken bei der Auslagerung von Aufgaben und ermöglicht moderne und flexible Arbeitsformen. Der Schutz vor Cyberrisiken ist eine gemeinsame Aufgabe von Staat, Wirtschaft, Wissenschaft und Gesellschaft. Mit der Cybersicherheitsstrategie stärkt der Kanton Zürich seinen Weg der Digitalisierung.

Mit Beschluss Nr. 129/2015 genehmigte der Regierungsrat das Organisationskonzept für die Informatiksicherheit in der kantonalen Verwaltung und damit die Schaffung eines Competence Center IT-Sicherheit in der Finanzdirektion. Die Stelle der oder des Informatik-Sicherheitsbeauftragten des Kantons Zürich (heute: Informationssicherheitsbeauftragte/r des Kantons Zürich) wurde mit RRB Nr. 379/2015 geschaffen. Diese Stelle wirkt als zentrale Ansprechperson für alle Fragen der Informationssicherheit in der kantonalen Verwaltung und leitet das Competence Center für Informatiksicherheit sowie die Fachgruppe Informationssicherheit.

Mit Beschluss Nr. 1193/2020 bewilligte der Regierungsrat für die Umsetzung des Geschäftsorganisationskonzepts Informationssicherheit 7,0 unbefristete Stellen in den Direktionen und der Staatskanzlei (Informatikspezialist/in mbA, Informationssicherheitsbeauftragte/r der Direktion) sowie eine gebundene Ausgabe von Fr. 3 211 200 für externe Dienstleistungen zur Umsetzung der Besonderen Informationssicherheitsrichtlinien in den Direktionen und der Staatskanzlei.

Gestützt auf diese Beschlüsse sowie die Empfehlungen des Sicherheitsverbundes Schweiz erarbeitete eine verwaltungsinterne Projektgruppe unter der Leitung des kantonalen Informationssicherheitsbeauftragten, in der das Amt für Informatik (AFI), die Kantonspolizei, die Kantonale Führungsorganisation und die Staatsanwaltschaft mitwirkten, eine Cybersicherheitsstrategie und eine Umsetzungsplanung.

Die Direktionen und die Staatskanzlei sowie die Finanzkontrolle und die Datenschutzbeauftragte wurden im Rahmen eines Mitberichtsverfahrens eingeladen, zum Entwurf der Cybersichersicherheitsstrategie Stellung zu nehmen. Der Entwurf der Cybersicherheitsstrategie und die Umsetzungsplanung wurden zudem Vertreterinnen und Vertretern von Städten und Gemeinden, Wirtschaftsverbänden, kritischen Infrastrukturen, Hochschulen und weiteren Fachleuten zur Stellungnahme unterbreitet und von diesen begrüsst. Verschiedene Bemerkungen wurden eingearbeitet.

Die kantonale Cybersicherheitsstrategie ist abgestimmt mit der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018–2022, dem daraus abgeleiteten Umsetzungsplan der Kantone sowie auf kantonaler Ebene mit den Richtlinien der Regierungspolitik 2019–2023 (Legislaturziel 10), der Strategie Digitale Verwaltung 2018–2023 und der kantonalen IKT-Strategie. Sie ergänzt diese Grundlagen und bildet den Rahmen, damit Regierung und Verwaltung im Bereich Cyberrisiken vorausschauend und wirksam handeln können. Die Cybersicherheitsstrategie dient der Umsetzung der gesetzlichen Regelungen zur Informationssicherheit in der kantonalen Verwaltung. Dies sind namentlich:

– § 7 des Gesetzes über die Information und den Datenschutz vom 12. Februar 2007 (LS 170.4)
– §§ 12 und 13 der Verordnung über die Informationsverwaltung und -sicherheit vom 3. September 2019 (LS 170.8)

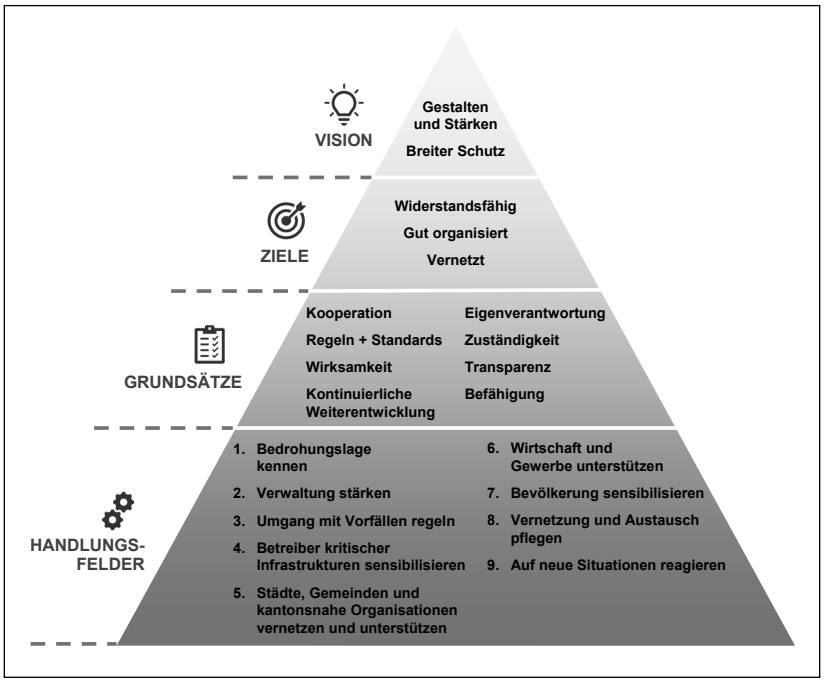
Das verwaltungsweite Kontinuitätsmanagement (Business Continuity Management) ist nicht Teil der Cybersicherheitsstrategie. Diese übergeordnete Sicherstellung des Verwaltungsbetriebs wird durch einen separaten Auftrag weiterverfolgt (vgl. RRB Nr. 172/2021, Empfehlung 8).

## 2. Cybersicherheitsstrategie

### *2.1 Elemente der Strategie*

Die Cybersicherheitsstrategie ist im gesonderten Dokument «Kantonale Cybersicherheitsstrategie» vom 26. April 2022 enthalten. Die wesentlichen Bestandteile der Strategie sind in der folgenden Abbildung dargestellt:

Abbildung 1: Kantonale Cybersicherheitsstrategie mit Vision, Zielen, Grundsätzen und Handlungsfeldern.




Vision, Ziel, Grundsätze und Handlungsfelder sind im Dokument «Kantonale Cybersicherheitsstrategie» weiter dargelegt.

### *2.2 Umsetzung der Strategie*

Im Dokument «Kantonale Cybersicherheitsstrategie – Organisation und Umsetzung» («Umsetzungsplanung») ist beschrieben, wie die Umsetzung der Strategie erfolgt. In einer ersten Phase richten sich die Tätigkeiten nach innen an die kantonale Verwaltung; in einer zweiten Phase ab 2024 werden die Betreiberinnen und Betreiber von kritischen Infrastrukturen, die Städte, Gemeinden und kantonsnahen Organisationen, die Wirtschaft und das Gewerbe sowie die Zürcher Wohn- und Arbeitsbevölkerung angesprochen.

Die kantonale Cybersicherheitsstrategie und die dazugehörige Umsetzungsplanung werden auf den 1. Juli 2022 in Kraft gesetzt. Zugleich sind die notwendigen Mittel zum Aufbau und Betrieb der Organisation zum Schutz vor Cyber-Risiken zu bewilligen. Die Umsetzung der Strategie wird jährlich durch eine externe Qualitätsmanagerin oder einen externen Qualitätsmanager überprüft. Die kantonale Cybersicherheitsstrategie ist mehrjährig ausgelegt. Sie wird aktualisiert, wenn besondere

Umstände oder neue Erkenntnisse dies erfordern, jedoch spätestens nach drei Jahren. Die Steuerung der Überarbeitung liegt beim Steuerungsgremium Digitale Verwaltung und IKT (SDI), ihre operative Führung bei der Finanzdirektion.

## 3. Handlungsfelder und Aufgaben

Im Folgenden werden die Handlungsfelder mit den zugehörigen Aufgaben beschrieben sowie die Sachkosten (Hardware, Software-Grundlizenzen, Informatiknutzungsaufwand, Software-Wartungslizenzen) und die Kosten für externe Dienstleistungen (Honorare) ausgewiesen. Wo zusätzliche Stellen notwendig sind, werden diese aufgeführt. Die bei den Aufgaben erwähnten Zuständigkeiten beziehen sich auf die zukünftige Cybersicherheitsorganisation, die in Ziff. 4.1 erläutert sind.

### *3.1 Handlungsfeld 1 – Bedrohungslage kennen*

Der Kanton Zürich ist vertraut mit den wesentlichen Entwicklungen in der Informationstechnologie, den damit verbundenen Risiken und den möglichen Schutzmassnahmen. Er kennt die aktuellen Cyberbedrohungen für die kantonale Verwaltung. Er führt ein Bedrohungslagebild nach, um Cyberangriffe zu erkennen und um Massnahmen zum Schutz, zur Abwehr und zur Bewältigung von Cyberangriffen auszulösen.

– ***A 1.1 – Bedrohungslagebild:*** Die Cyber-Koordinatorin oder der Cyber-Koordinator oder die von ihr oder ihm angewiesenen Stellen führen das Bedrohungslagebild nach und führen spezifische Gefährdungsanalysen durch. Sie kennen Bedrohungen, relevante aktuelle Entwicklungen und Schwachstellen.

| Kostenart | Projektkosten (einmalig, in Franken) | | | Betriebskosten, (wiederkehrend, in Franken) |
|---|---|---|---|---|
| | 2022 | 2023 | 2024 | ab 2025 |
| Sachkosten | | 25 000 | 25 000 | 25 000 |
| Externe Dienstleistungen | 50 000 | 50 000 | | |

### *3.2 Handlungsfeld 2 – Verwaltung stärken*

Der Kanton Zürich stärkt den Schutz vor Cyberrisiken innerhalb der Verwaltung. Er fördert eine Sicherheitskultur, in der Risiken erkannt, offengelegt und bewältigt werden, und er informiert, sensibilisiert und schult seine Mitarbeitenden entsprechend. Er stellt eine sichere IKT-Infrastruktur und Cybersicherheitsdienstleistungen bereit und lagert gegebenenfalls Cybersicherheitsdienstleistungen an spezialisierte Dritte aus.

– ***A 2.1 – Weiterentwicklung:*** Die Kerngruppe Cyber überprüft im Auftrag des SDI regelmässig die Cybersicherheitsstrategie sowie das Umsetzungsdokument und entwickelt diese weiter.

| Kostenart | Projektkosten (einmalig, in Franken) | | Betriebskosten, (wiederkehrend, in Franken) |
|---|---|---|---|
| | 2023 | 2024 | ab 2025 |
| Externe Dienstleistungen | 25 000 | 25 000 | 25 000 |

– ***A 2.2 – Regelwerk Informationssicherheit:*** Die Cyber-Koordinatorin oder der Cyber-Koordinator hält das verwaltungsinterne Regelwerk Informationssicherheit aktuell und richtet es auf neue Technologien und Bedrohungen aus. Sie oder er standardisiert, priorisiert und misst die Umsetzung der internen Richtlinien in den Direktionen und der Staatskanzlei.

| Kostenart | Projektkosten (einmalig, in Franken) | Betriebskosten, (wiederkehrend, in Franken) |
|---|---|---|
| | 2024 | ab 2025 |
| Externe Dienstleistungen | 100 000 | 100 000 |

– ***A 2.3 – Risikomanagement Informationssicherheit:*** Es wird eine neue Stelle Leiterin oder Leiter des kantonalen Risikomanagements Informationssicherheit geschaffen. Sie oder er etabliert ein integriertes, technisch gestütztes Risikomanagement zur Informationssicherheit, gleicht den Umgang mit den Risiken mit dem übergeordneten Risikomanagement sowie dem internen Kontrollsystem (IKS) ab und nutzt Synergien z. B. im Bereich des betrieblichen Kontinuitätsmanagements. Zusätzlich unterstützen drei Expertinnen und Experten Informationsrisikomanagement die Informationssicherheitsbeauftragten der Direktionen und der Staatskanzlei bei der Umsetzung des kantonalen Informationsrisikomanagements in der jeweiligen Direktion und der Staatskanzlei. Sie führen u. a. Schulungen durch, legen den Umgang mit Informationsrisiken mit den Direktionen und der Staatskanzlei fest, moderieren Risikomanagement-Workshops, dokumentieren und bewerten Risiken in Zusammenarbeit mit den Direktionen und der Staatskanzlei und unterstützen bei der Erstellung von Risikoberichten.

| Kostenart | Projektkosten (einmalig, in Franken) | | | Betriebskosten, (wiederkehrend, in Franken) |
|---|---|---|---|---|
| | 2022 | 2023 | 2024 | ab 2025 |
| Sachkosten | 125 000 | 250 000 | 250 000 | 250 000 |
| Externe Dienstleistungen | 350 000 | 50 000 | 50 000 | 50 000 |

| Zusätzliche Stellen | ab 1. Juli 2022 | 2023 | ab 2024 |
|---|---|---|---|
| Anzahl Stellen gesamt | 2,0 | 3,0 | 4,0 |
| Jährliche Personalkosten (in Franken) | 185 000 | 550 000 | 730 000 |

– ***A 2.4 – Kantonale Sicherheitskultur:*** Es wird eine neue Stelle Spezialistin oder Spezialist Security Awareness geschaffen. Sie oder er stärkt die Sicherheitskultur in der kantonalen Verwaltung, indem sie oder er die im Konzept Sicherheitskultur als notwendig erkannten Massnahmen umsetzt.

| Kostenart | Projektkosten (einmalig, in Franken) | | | Betriebskosten, (wiederkehrend, in Franken) |
|---|---|---|---|---|
| | 2022 | 2023 | 2024 | ab 2025 |
| Sachkosten | 50 000 | 100 000 | 100 000 | 100 000 |
| Externe Dienstleistungen | 75 000 | 150 000 | 150 000 | 150 000 |

| Zusätzliche Stellen | ab 1. Juli 2022 | ab 2023 |
|---|---|---|
| Anzahl Stellen | 1,0 | 1,0 |
| Jährliche Personalkosten (in Franken) | 90 000 | 180 000 |

– ***A 2.5 – Audits im Bereich Informationssicherheit:*** Es wird eine neue Stelle Leiterin oder Leiter der internen Audit-Funktion im Bereich Informationssicherheit geschaffen. Sie oder er entwickelt ein Audit-Programm, mit dem der Handlungsbedarf in der kantonalen Verwaltung im Bereich Informationssicherheit erkannt werden kann, und führt im Bereich Informationssicherheit Audits im Auftrag der Kerngruppe Cyber durch.

| Kostenart | Projektkosten (einmalig, in Franken) | | | Betriebskosten, (wiederkehrend, in Franken) |
|---|---|---|---|---|
| | 2022 | 2023 | 2024 | ab 2025 |
| Externe Dienstleistungen | 175 000 | 350 000 | 350 000 | 350 000 |

| Zusätzliche Stellen | ab 1. Juli 2022 | ab 2023 |
|---|---|---|
| Anzahl Stellen | 1,0 | 1,0 |
| Jährliche Personalkosten (in Franken) | 90 000 | 180 000 |

– ***A 2.6 – Expertenpool Informationssicherheit:*** Es wird zur Verstärkung des direktionsübergreifenden Expertenpool Informationssicherheit eine neue Stelle für eine Spezialistin oder einen Spezialisten Informationssicherheit geschaffen.

| Zusätzliche Stellen | ab 2024 |
|---|---|
| Anzahl Stellen | 1,0 |
| Jährliche Personalkosten (in Franken) | 180 000 |

– ***A 2.7 – Bug-Bounty-Programm:*** Die Leiterin oder der Leiter des Cyber Defence Centers des AFI startet eine Initiative zur Identifizierung und Behebung von Sicherheitslücken in Software, die mit klassischen Testmethoden verborgen bleiben.

| Kostenart | Projektkosten (einmalig, in Franken) | | | Betriebskosten, (wiederkehrend, in Franken) |
|---|---|---|---|---|
| | 2022 | 2023 | 2024 | ab 2025 |
| Sachkosten | 75 000 | 75 000 | 75 000 | 75 000 |
| Externe Dienstleistungen | 125 000 | 250 000 | 250 000 | 250 000 |

– ***A 2.8 – Identity and Access Management:*** Die Leiterin oder der Leiter des Cyber Defence Centers des AFI entwickelt das vorhandene Identitäts- und Zugriffsmanagement weiter (Anschlussprojekte an das Projekt «Identitäts- und Zugriffsmanagement IAM» im Rahmen des Programms zur Umsetzung der IKT-Strategie RRB Nr. 625/2019). Neben der Weiterentwicklung der Dienstleistung sind sowohl vorhandene als auch neue Anwendungen in der kantonalen Verwaltung mit dem zentralen IAM zu verbinden. Daraus ergibt sich ein erhöhter personeller und finanzieller Mittelbedarf, um die im Zuge der Zentralisierung notwendigen konzeptionellen und betrieblichen Anforderungen umsetzen zu können.

| Kostenart | Projektkosten (einmalig, in Franken) | | Betriebskosten, (wiederkehrend, in Franken) |
|---|---|---|---|
| | 2023 | 2024 | ab 2025 |
| Sachkosten | 700 000 | 700 000 | 700 000 |
| Externe Dienstleistungen | 200 000 | 200 000 | |

| Zusätzliche Stellen | 2023 | ab 2024 |
|---|---|---|
| Anzahl Stellen | 1,0 | 2,0 |
| Jährliche Personalkosten (in Franken) | 170 000 | 340 000 |

– ***A 2.9 – Security Operations Center und Cyber Defence Center:*** Die Leiterin oder der Leiter des Cyber Defence Centers (CDC) des AFI entwickelt das im Rahmen des Programms zur Umsetzung der IKT-Strategie aufgebaute Security Operations Center zu einem CDC weiter. Synergien zum Security Operations Center der Kantonspolizei werden geprüft und wo sinnvoll genutzt. Durch den Ausbau des CDC werden zusätzliche digitale Leistungsangebote der kantonalen Verwaltung überwacht. Daraus ergibt sich ein erhöhter personeller und finanzieller Mittelbedarf, um die Analyse- und Reaktionsfähigkeit des CDC gewährleisten zu können.

| Kostenart | Projektkosten (einmalig, in Franken) | | Betriebskosten, (wiederkehrend, in Franken) |
|---|---|---|---|
| | 2023 | 2024 | ab 2025 |
| Sachkosten | 800 000 | 800 000 | 800 000 |
| Externe Dienstleistungen | 200 000 | 200 000 | |

| Zusätzliche Stellen | ab 1. Juli 2022 | 2023 | ab 2024 |
|---|---|---|---|
| Anzahl Stellen gesamt | 1,0 | 3,0 | 4,0 |
| Jährliche Personalkosten (in Franken) | 85 000 | 510 000 | 680 000 |

– ***A 2.10 – Public Key Infrastructure Services:*** Die Leiterin oder der Leiter des CDC des AFI baut die Public-Key-Infrastructure-Dienstleistungen aus, um den erhöhten Bedarf an digitalen Identitäten mittels Zertifikaten abzudecken. Dies führt zu einem höheren personellen und finanziellen Mittelbedarf, damit die Dienstleistung in einer vertrauensbildenden Qualität der kantonalen Verwaltung angeboten werden kann.

| Kostenart | Projektkosten (einmalig, in Franken) | | Betriebskosten, (wiederkehrend, in Franken) |
|---|---|---|---|
| | 2023 | 2024 | ab 2025 |
| Sachkosten | 350 000 | 350 000 | 350 000 |
| Externe Dienstleistungen | 125 000 | 75 000 | |

| Zusätzliche Stellen | 2023 | ab 2024 |
|---|---|---|
| Anzahl Stellen gesamt | 1,0 | 2,0 |
| Jährliche Personalkosten (in Franken) | 170 000 | 340 000 |

– ***A 2.11 – Führen der Geschäftsstelle:*** Es werden drei neue Stellen geschaffen für die Geschäftsstelle, welche die Cyber-Koordinatorin oder den Cyber-Koordinator bei der Programmleitung unterstützt, das Projektmanagement-Office führt und die Koordination und Kommunikation sicherstellt.

| Kostenart | Projektkosten (einmalig, in Franken) | | | Betriebskosten, (wiederkehrend, in Franken) |
|---|---|---|---|---|
| | 2022 | 2023 | 2024 | ab 2025 |
| Externe Dienstleistungen | 25 000 | 25 000 | 25 000 | 25 000 |

| Zusätzliche Stellen | ab 1. Juli 2022 | 2023 | ab 2024 |
|---|---|---|---|
| Anzahl Stellen gesamt | 1,0 | 2,0 | 3,0 |
| Jährliche Personalkosten (in Franken) | 80 000 | 320 000 | 420 000 |

### *3.3 Handlungsfeld 3 – Umgang mit Vorfällen regeln*

Der Kanton Zürich verfügt über die Mittel, um auf Vorfälle und Cyberangriffe auf die Verwaltung angemessen reagieren zu können und die Wiederherstellung nach Cyberangriffen zu gewährleisten. Es erfolgt eine enge Zusammenarbeit mit der Kantonspolizei und der Staatsanwaltschaft.

– ***A 3.1 – Umgang mit Vorfällen regeln:*** Das operative Gremium definiert das Vorgehen im Ereignisfall für alle Eskalationsstufen. Für diese Aufgabe entstehen keine Sachkosten, keine Kosten für externe Dienstleistungen, und es werden keine zusätzlichen personellen Mittel benötigt.

– ***A 3.2 – Cyberkrisenmanagement:*** Die Cyber-Koordinatorin oder der Cyber-Koordinator erstellt ein Konzept zum Cyberkrisenmanagement. Das operative Gremium führt Cybersimulationsübungen durch. Die Cyber-Koordinatorin oder der Cyber-Koordinator erarbeitet ein Regelwerk, das den IKT-Betreiberinnen und -Betreibern als Grundlage für den Aufbau und Betrieb einer widerstandsfähigen IKT-Infrastruktur dient (RRB Nr. 172/2021, Empfehlung 8b). Das Regelwerk soll auch Vorlagen für die Kontinuitätspläne der IT-Services enthalten und später auch für die Beurteilung von Fachapplikationen dienen.

| Kostenart | Projektkosten (einmalig, in Franken) | | | Betriebskosten, (wiederkehrend, in Franken) |
|---|---|---|---|---|
| | 2022 | 2023 | 2024 | ab 2025 |
| Externe Dienstleistungen | 50 000 | 100 000 | 100 000 | 100 000 |

### *3.4 Handlungsfeld 4 – Betreiber kritischer Infrastrukturen sensibilisieren*

Der Kanton Zürich kennt seine kritischen Infrastrukturen und die Cyberrisiken, die sie bedrohen, und er pflegt den regelmässigen Kontakt mit ihren Betreiberinnen und Betreibern. Er nimmt am Erfahrungsaustausch im Rahmen von massgeblichen Konferenzen teil und unterstützt den Bund bei den Massnahmen zur Verbesserung der IKT-Resilienz der kritischen Infrastrukturen.

– ***A 4.1 – Betreiber kritischer Infrastrukturen unterstützen:*** Die Cyber-Koordinatorin oder der Cyber-Koordinator pflegt den Austausch mit den Betreiberinnen und Betreibern der kritischen Infrastrukturen im Kanton Zürich und kennt deren Risiken. Die Verantwortung für den Schutz kritischer Infrastrukturen liegt in erster Linie bei den Betreiberinnen und Betreibern selbst. Für diese Aufgabe entsteht ein einmaliger Aufwand von Fr. 25 000 für die Erstellung eines Konzepts zur Zusammenarbeit mit dieser Zielgruppe.

### *3.5 Handlungsfeld 5 – Städte, Gemeinden und kantonsnahe Organisationen vernetzen und unterstützen*

Die kantonale Verwaltung pflegt einen regelmässigen Austausch mit Vertreterinnen und Vertretern der Städte und Gemeinden des Kantons Zürich, dem Kantonsrat, den Parlamentsdiensten sowie den kantonalen Gerichten und Notariaten über den Schutz vor Cyberrisiken. Dienstleistungen, die der kantonalen Verwaltung angeboten werden, können zu einem späteren Zeitpunkt im Rahmen der rechtlichen Möglichkeiten auch von den Städten und Gemeinden sowie kantonsnahen Organisationen genutzt werden.

– ***A 5.1 – Städte und Gemeinden unterstützen:*** Die Cyber-Koordinatorin oder der Cyber-Koordinator pflegt den Austausch mit den Städten und Gemeinden des Kantons Zürich, dem Kantonsrat, den Parlamentsdiensten sowie den kantonalen Gerichten und Notariaten. Sie oder er fördert die Vernetzung der kantonalen und kommunalen Fachpersonen. Bei Bedarf und unter Einhaltung der rechtlichen Rahmenbedingungen kann der Kanton die Städte und Gemeinden, den Kantonsrat, die Parlamentsdienste sowie die kantonalen Gerichte und Notariate mit den kantonalen Cybersicherheitsdienstleistungen unterstützen. Für diese Aufgabe entsteht ein einmaliger Aufwand von Fr. 25 000 für die Erstellung eines Konzepts zur Zusammenarbeit mit diesen Zielgruppen.

### *3.6 Handlungsfeld 6 – Wirtschaft und Gewerbe unterstützen*

Der Kanton Zürich pflegt einen regelmässigen Austausch mit Vertreterinnen und Vertretern aus der Wirtschaft und dem Gewerbe über den Schutz vor Cyberrisiken. Er unterstützt Informationskampagnen und fördert die Vernetzung zum Schutz vor Cyberrisiken in den Branchen.

– ***A 6.1 – Wirtschaft und Gewerbe unterstützen:*** Die Cyber-Koordinatorin oder der Cyber-Koordinator pflegt den Austausch mit der Zürcher Wirtschaft und dem Gewerbe des Kantons Zürich und fördert die Vernetzung in den Branchen. Der Kanton unterstützt Informationskampagnen der Wirtschaft und des Gewerbes. Für diese Aufgabe entsteht ein einmaliger Aufwand von Fr. 25 000 für die Erstellung eines Konzepts zur Zusammenarbeit mit dieser Zielgruppe.

### *3.7 Handlungsfeld 7 – Bevölkerung sensibilisieren*

Der Kanton Zürich fördert die Aus- und Weiterbildung zum Thema Cybersicherheit auf allen Stufen des kantonalen Bildungssystems und unterstützt die entsprechende Forschung. Er fördert und unterstützt Kampagnen zum Thema Cybersicherheit.

– ***A 7.1 – Bevölkerung sensibilisieren:*** Die Cyber-Koordinatorin oder der Cyber-Koordinator koordiniert die Anstrengungen des Kantons im Bereich der Förderung der Aus- und Weiterbildung im Bereich «Cybersicherheit» und bei Informationskampagnen. Sie oder er ist federführend bei Informationskampagnen des Kantons. Für diese Aufgabe entsteht ein einmaliger Aufwand von Fr. 25 000 für die Erstellung eines Konzepts.

### *3.8 Handlungsfeld 8 – Vernetzung und Austausch pflegen*

Der Kanton Zürich pflegt den Austausch im Cyberbereich.

– ***A 8.1 – Vernetzung und Austausch pflegen:*** Die Cyber-Koordinatorin oder der Cyber-Koordinator pflegt aktiv den Erfahrungsaustausch mit dem Bund, anderen Kantonen und den Nachbarländern sowie mit nationalen und internationalen Gremien und Fachleuten im Cyberbereich. Für diese Aufgabe entstehen keine Sachkosten, keine Kosten für externe Dienstleistungen, und es werden keine zusätzlichen personellen Mittel benötigt.

### *3.9 Handlungsfeld 9 – Auf neue Situationen reagieren*

Der Kanton Zürich verfügt über Mittel, um rasch und wirksam auf neue Bedrohungslagen oder neue Entwicklungen reagieren zu können.

– ***A 9.1 – Auf neue Situationen reagieren (Reserve):*** Das kantonale Zentrum für Cybersicherheit kann zusätzliche Mittel beantragen, um auf neue Bedrohungslagen oder neue Entwicklungen rasch und wirksam reagieren zu können. Die Kerngruppe Cyber entscheidet über die Freigabe der Mittel.

| Kostenart | Projektkosten (einmalig, in Franken) | | | Betriebskosten, (wiederkehrend, in Franken) |
|---|---|---|---|---|
| | 2022 | 2023 | 2024 | ab 2025 |
| Externe Dienstleistungen | 100 000 | 200 000 | 200 000 | 200 000 |

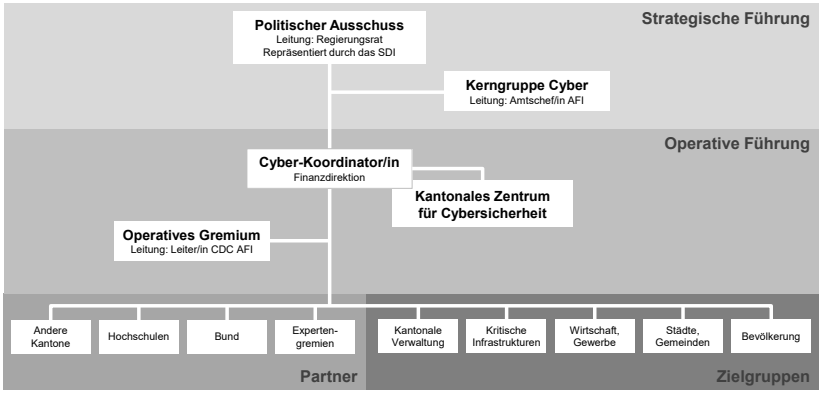
## 4. Aufbau der Organisation gemäss Cybersicherheitsstrategie

Um die Cybersicherheitsstrategie mit den zugehörigen Handlungsfeldern umzusetzen und die Aufgaben auch nach dem Aufbau in den laufenden Betrieb zu übernehmen, wird eine Cybersicherheitsorganisation aufgebaut. Die Organisation und die zu den einzelnen Organisationselementen gehörenden Aufgaben werden im Folgenden beschrieben.

### *4.1 Organisationsstruktur*

Der Kanton Zürich schafft eine übergeordnete Organisation im Bereich Cybersicherheit. Die Verantwortlichkeiten für die Aufgaben sowie die organisatorische Einbettung der Rollen orientiert sich an der übergeordneten Organisation des Bundes.

Abbildung 2: Organigramm der kantonalen Cyberorganisation




### *4.1.1 Politischer Ausschuss*

Im Kanton Zürich nimmt der Regierungsrat die übergeordnete politische Verantwortung für die Cybersicherheit wahr. Die strategische Führung wird dem Gremium SDI übertragen.

### *4.1.2 Kerngruppe Cyber*

Die Kerngruppe Cyber ist ein beratendes Gremium und unterstützt das SDI bei strategischen Entscheiden im Bereich Cybersicherheit. Die Kerngruppe stärkt die Zusammenarbeit innerhalb der kantonalen Verwaltung zwischen den drei Bereichen Cybersicherheit, Strafverfolgung und Cyber Defence sowie mit den Zielgruppen ausserhalb der kantonalen Verwaltung. Sie wird von der Amtschefin oder dem Amtschef des AFI geleitet. Zusätzliche Mitglieder sind die Cyber-Koordinatorin oder der Cyber-Koordinator, leitende Personen aus relevanten Verwaltungseinheiten (Staatsanwaltschaft, Polizei und Kantonale Führungsorganisation), die oder der Kommunikationsverantwortliche des kantonalen Zentrums für Cybersicherheit sowie eine Vertreterin oder ein Vertreter einer kantonalen kritischen Infrastruktur.

Die Kerngruppe Cyber sorgt für die Erarbeitung der gesetzlichen und anderer Rahmenbedingungen und beantragt diese beim SDI bzw. dem Regierungsrat zur Umsetzung. Die Kerngruppe Cyber berät das SDI zu Anträgen aus der Fachgruppe Informationssicherheit. Im Auftrag des SDI definiert sie das Dienstleistungsangebot im Bereich Cybersicherheit und überprüft die operative Umsetzung anhand der definierten bzw. erreichten Ziele der Cybersicherheitsstrategie; die Kerngruppe Cyber genehmigt zudem den von der Fachgruppe Informationssicherheit vorgelegten jährlichen Audit-Plan, beurteilt die Bewältigung von Cybervorfällen, zieht Lehren aus den Cybervorfällen der eigenen Organisation oder der Umwelt und unterstützt bei Differenzen in der kantonalen Cyberorganisation.

Das Gesamtprogramm und die Umsetzung der Cybersicherheitsstrategie sowie der Betrieb werden regelmässig durch eine externe Qualitätsmanagerin oder einen externen Qualitätsmanager überprüft. Auftraggeberin für diese Überprüfung ist die Kerngruppe Cyber.

### *4.1.3 Cyber-Koordinatorin/Cyber-Koordinator*

Die Cyber-Koordinatorin oder der Cyber-Koordinator nimmt innerhalb des Kantons, aber auch im Verhältnis zu den Behörden auf Bundesebene, die Rolle der zentralen Anlaufstelle ein und stellt die Vernetzung zwischen den staatlichen und privaten Akteurinnen und Akteuren sicher. Sie oder er steht dem kantonalen Zentrum für Cybersicherheit vor und wird von diesem bei ihren bzw. seinen Aufgaben unterstützt. Die Cyber-Koordinatorin oder der Cyber-Koordinator rapportiert direkt an die Finanzdirektorin oder den Finanzdirektor. Ihre oder seine Rolle wird von der oder dem Informationssicherheitsbeauftragten des Kantons wahrgenommen.

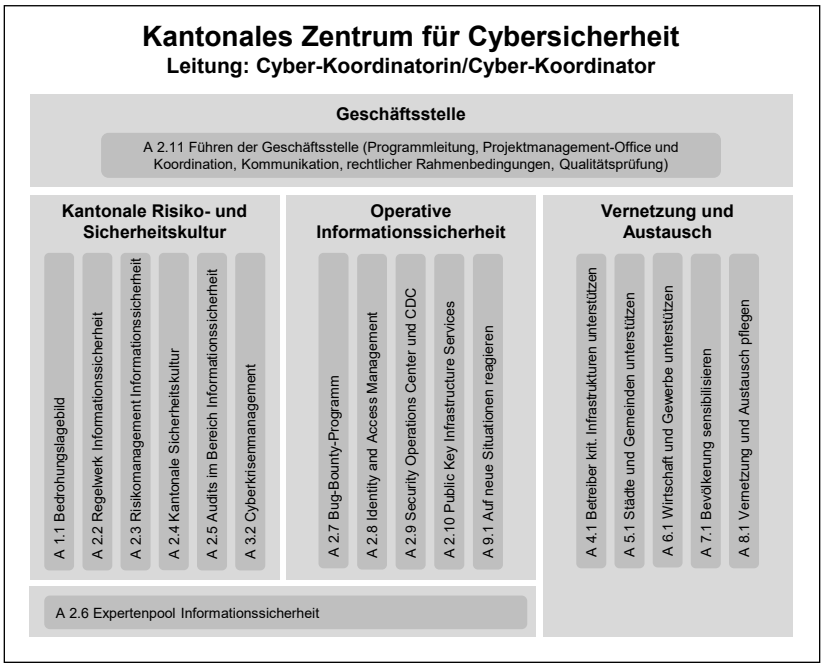
Die Cyber-Koordinatorin oder der Cyber-Koordinator führt das kantonale Zentrum für Cybersicherheit. Zudem pflegt sie oder er den Austausch mit den Stellen des Bundes, der Schweizerischen Informatikkonferenz, dem Sicherheitsverbund Schweiz, den Kantonen, der Wirtschaft, den kantonalen kritischen Infrastrukturen sowie den Hochschulen und Forschungsgruppen. Schliesslich repräsentiert sie oder er den Kanton Zürich in Cyberbelangen.

### *4.1.4 Kantonales Zentrum für Cybersicherheit*

Das kantonale Zentrum für Cybersicherheit fördert die kantonale Risiko- und Sicherheitskultur, stärkt die operative Informationssicherheit, pflegt die Vernetzung und den Austausch und führt die Geschäftsstelle einschliesslich Programmleitung, Projektmanagement-Office und Koordination.

Das kantonale Zentrum für Cybersicherheit baut entsprechend den Empfehlungen des Sicherheitsverbundes Schweiz auf den bereits bestehenden Strukturen innerhalb der kantonalen Verwaltung auf. Dem kantonalen Zentrum für Cybersicherheit steht neben den eigenen Mitarbeitenden ein Pool mit Fachleuten der Informationssicherheit zur Verfügung.

Abbildung 3: Gliederung und Aufgaben des kantonalen Zentrums für Cybersicherheit



Das kantonale Zentrum für Cybersicherheit ist organisatorisch in die Finanzdirektion eingegliedert. Der Umgang mit Cyberrisken bedingt einen engen Austausch mit den Fachexpertinnen und -experten im AFI, erfordert ein Abwägen zwischen geeigneten Massnahmen und kann finanzielle und personelle Konsequenzen nach sich ziehen; aus diesen Gründen ist die Eingliederung in die Finanzdirektion zweckmässig. Diese Eingliederung folgt auch dem Ansatz des Bundes, wo das nationale Zentrum für Cybersicherheit dem Eidgenössischen Finanzdepartement unterstellt ist.

#### *4.1.5 Operatives Gremium*

Das operative Gremium wird geleitet von der Leiterin oder dem Leiter Cyber Defence Center des AFI. Die Mitglieder stammen aus der Kantonalen Führungsorganisation, der Informatik (Cybersicherheit und Kommunikation) und bei Bedarf aus der Staatsanwaltschaft und der Kantonspolizei. Die Kantonale Führungsorganisation ist dann in die Bewältigung von Krisenfällen einbezogen und übernimmt die Führung, wenn der Krisenfall von Belang für den Bevölkerungsschutz ist. Bei den weiteren Aufgaben nimmt sie keine aktive Rolle ein. Sie stellt jedoch sicher, dass der Wissensaustausch mit den anderen Mitgliedern zuverlässig funktioniert.

Das operative Gremium verfolgt die Cyberbedrohungslage, beurteilt die Cyberentwicklung in ihren Bereichen sowie Massnahmen zum Schutz vor Cyberrisiken, bewältigt Cybervorfälle und unterstützt in einem schweren Cyberereignis (ausserordentliche Lage).

#### *4.1.6 Zielgruppen und Partner*

Der Kanton Zürich sucht die Zusammenarbeit im Bereich Cybersicherheit. Er pflegt den Austausch mit dem Bund, anderen Kantonen, Städten und Gemeinden, Organisationen und Unternehmen, national und international, um die Vernetzung im Bereich Cybersicherheit zu verstärken. Insbesondere unterstützt der Kanton Zürich das eigenverantwortliche Handeln der Zielgruppen. Er informiert und sensibilisiert, fördert und vernetzt und kann bei Bedarf gezielt unterstützen.

Klarer Schwerpunkt liegt auf der Unterstützung der kantonalen Verwaltung und den kantonsnahen Organisationen. Hier wird ein Grossteil der vorgesehenen Mittel eingesetzt.

Daneben pflegt er eine Zusammenarbeit mit den Betreiberinnen und Betreibern kritischer Infrastrukturen im Kanton Zürich, den Städten und Gemeinden, der Zürcher Wirtschaft und der Zürcher Wohn- und Arbeitsbevölkerung. Zudem pflegt der Kanton den Erfahrungsaustausch mit den Hochschulen (insbesondere der Universität Zürich und der ETH Zürich), den anderen Kantonen, dem Bund sowie den nationalen und internationalen Fachgremien und Behörden.

#### *4.1.7 Zusammenspiel mit dem Geschäftsorganisationskonzept Informationssicherheit*

Die Cybersicherheitsstrategie erlaubt die Vernetzung aller relevanten Cyberakteurinnen und -akteure innerhalb der Verwaltung (Sicherheit, Verfolgung und Verteidigung), ermöglicht den Einbezug aller externen Zielgruppen (kritische Infrastrukturen usw.) und schafft die Grundlage für eine zentrale Bereitstellung von Dienstleistungen durch das kantonale Zentrum für Cybersicherheit.

Dazu werden die bestehenden Strukturen und Prozesse genutzt. Das Geschäftsorganisationskonzept Informationssicherheit (vgl. auch RRB Nrn. 625/2019 und 1193/2020) beschreibt die Ablauforganisation der Informationssicherheit in der kantonalen Verwaltung. Diese Organisation sowie die definierten Prozesse und Rollen bleiben bestehen. Sie werden erweitert mit den zusätzlichen Gremien und Strukturen. Mit der Cybersicherheitsstrategie werden bestehende Strukturen entlastet, und Cybersicherheitsdienstleistungen können zentral in hoher Qualität für alle Direktionen und die Staatskanzlei bereitgestellt werden.

#### *4.1.8 Zusammenarbeit mit der Kantonalen Führungsorganisation*

Das kantonale Zentrum für Cybersicherheit stellt sicher, dass die Umsetzung der Cybersicherheitsstrategie den Ansprüchen des integralen Risikomanagements und dem Risikomanagement Bevölkerungsschutz genügt. Es deckt als Fachstelle das Management des Teils «Cyberrisiken» ab und sorgt dafür, dass das benötigte Expertenwissen eingebracht wird und keine inhaltlichen oder methodischen Widersprüche entstehen. Die Zusammenarbeit ist über die Mitwirkung im Fachstab der Kantonalen Führungsorganisation geregelt.

Bei der Führung im Ereignisfall (ausserordentliche Lage und andere Lagen gemäss Bevölkerungsschutzgesetz [LS 520]) und der Bewältigung gelten unverändert die gesetzlichen Zuständigkeiten.

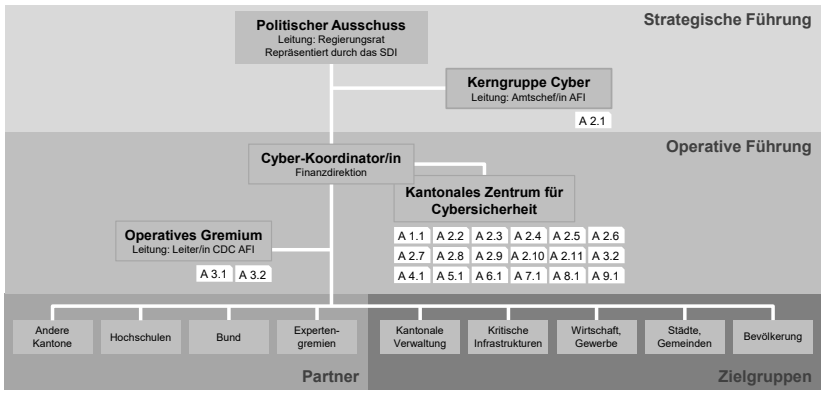
### *4.2 Bereitstellung der Dienstleistungen und Zuordnung der Aufgaben*

Das kantonale Zentrum für Cybersicherheit stellt den Direktionen und der Staatskanzlei verschiedene Dienstleistungen im Bereich Cybersicherheit zur Verfügung, die sie nutzen können. Damit werden die Direktionen und die Staatskanzlei bei Cybersicherheitsaufgaben unterstützt und können sich auf ihre Kernaufgaben konzentrieren. Gleichzeitig wird die Wahrung der Sorgfaltspflicht in der Informationssicherheit gewährleistet. Die Zusammenarbeit innerhalb der kantonalen Verwaltung ist im Geschäftsorganisationskonzept Informationssicherheit festgelegt.

Um die in der kantonalen Cybersicherheitsstrategie beschriebenen Ziele zu erreichen, müssen in den neun Handlungsfeldern die in Ziff. 3.1 bis 3.9 aufgeführten Aufgaben erfüllt werden. Dafür werden entweder neue Projekte gestartet oder die Aufgaben werden durch bereits bestehende Projekte abgedeckt. Langfristige Aufgaben können entweder in bestehende Linienfunktionen integriert werden oder es werden neue Stellen geschaffen.

Die folgende Abbildung zeigt die Zuordnung der Aufgaben zu den verschiedenen Organisationselementen der zukünftigen Cybersicherheitsorganisation. Dabei entsprechen die Bezeichnungen in den weissen Kästchen den Aufgaben gemäss Ziff. 3.1–3.9:

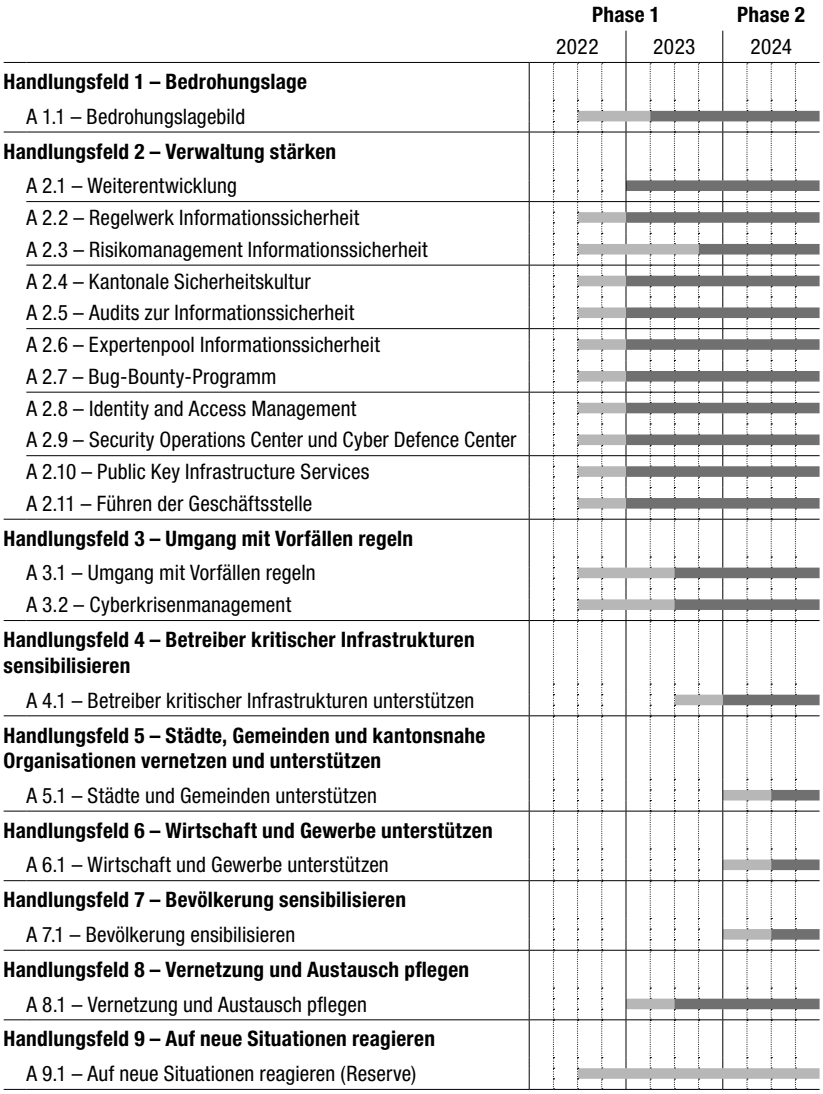
Abbildung 4: Zuständigkeiten der Organisationseinheiten für die Aufgaben in den Handlungsfeldern




## 5. Umsetzungsschritte

Der Schwerpunkt liegt in der ersten Phase auf den Handlungsfeldern 1, 2 und 3, bei denen es um die Bedrohungslage, die Stärkung der kantonalen Verwaltung und den Umgang mit Vorfällen geht. In einer zweiten Phase ab 2024 richten sich die Anstrengungen zusätzlich auf die weiteren Zielgruppen, insbesondere auf die kritischen Infrastrukturen. Im Hinblick auf diese Phase muss auch die Organisationsstruktur im Bereich Cybersicherheit überprüft werden.

Abbildung 5: Zeitplan zur Umsetzung der Strategie mit Schwerpunkt der Zielgruppen



## 6. Mittelbedarf

### *6.1 Personal*

Es sind 18 unbefristete Stellen zu schaffen. Die Stellenpläne werden wie folgt erweitert:

Tabelle 1: Übersicht über die zu schaffenden Stellen

| Anzahl Stellen | Aufgabe | Richtpositionsumschreibung / Rolle | Leistungs-gruppe | Klasse VVO |
|---|---|---|---|---|
| **Sicherheitsdirektion** | | | | |
| 1,0 | A 2.9 | Informatikspezialist/in mbA (Informationssicherheits-Experte/-Expertin «SOC / CDC / Security Incident Analyst») | 3100 | 21 |
| **Finanzdirektion** | | | | |
| 1,0 | A 2.3 | Informatikspezialist/in mbA (Leiter/Leiterin Informations-sicherheits-Experte/-Expertin «Risikomanagement») | 4620 | 23 |
| 3,0 | A 2.3 | Informatikspezialist/in mbA (Informationssicherheits-Experte/-Expertin «Risikomanagement») | 4620 | 22 |
| 1,0 | A 2.4 | Informatikspezialist/in mbA (Informationssicherheits-Experte/-Expertin «Security-Awareness») | 4620 | 22 |
| 1,0 | A 2.5 | Informatikspezialist/in mbA (Informationssicherheits-Experte/-Expertin «Audit») | 4620 | 22 |
| 1,0 | A 2.6 | Informatikspezialist/in mbA (Informationssicherheits-Experte/-Expertin Verstärkung Expertenpool Informationssicherheit) | 4620 | 22 |
| 2,0 | A 2.8 | Informatikspezialist/in mbA (Informationssicherheits-Experte/-Expertin «IAM») | 4610 | 21 |
| 3,0 | A 2.9 | Informatikspezialist/in mbA (Informationssicherheits-Experte/-Expertin «SOC / CDC / Security Incident Analyst») | 4610 | 21 |
| 2,0 | A 2.10 | Informatikspezialist/in mbA (Informationssicherheits-Experte/-Expertin «PKI») | 4610 | 21 |
| 1,0 | A 2.11 | Informatikspezialist/in (Programm-Manager/in) | 4620 | 20 |
| 1,0 | A 2.11 | Verwaltungsassistent/in (Experte/Expertin Projek-management-Office, Koordination) | 4620 | 13 |
| 1,0 | A 2.11 | Adjunkt/in (Experte/Expertin Kommunikation) | 4620 | 20 |
| **18,0 unbefristete Vollzeitstellen** | | | | |

Die Stellenbesetzung soll parallel zu den vorgesehenen Umsetzungsschritten erfolgen. Angestrebt wird eine Staffelung mit der Besetzung von sechs Stellen ab 1. Juli 2022, sechs Stellen ab 1. Januar 2023 und sechs Stellen ab 1. Januar 2024.

Für die Unterstützung bei der Stellenbesetzung soll ein externer Personaldienstleister beigezogen werden. Dafür wird mit Kosten von Fr. 250 000 zulasten der Erfolgsrechnung der Leistungsgruppe Nr. 4620, IKT-Sicherheitsbeauftragter, gerechnet.

Die Personalkosten lassen sich wie folgt zusammenfassen:

Tabelle 2: Schätzung der anfallenden personellen Kosten (in Franken)

| Zusätzliche Stellen | ab 1. Juli 2022 | 2023 | ab 2024 |
|---|---|---|---|
| Personalkosten; davon: | 530 000 | 2 080 000 | 3 050 000 |
| LG Nr. 3100, Kantonspolizei | | 170 000 | 170 000 |
| LG Nr. 4610, Amt für Informatik | 85 000 | 680 000 | 1 190 000 |
| LG Nr. 4620, Informatik-sicherheitsbeauftragter | 445 000 | 1 230 000 | 1 690 000 |

Die Überprüfung der Einreihung sämtlicher zu schaffenden Stellen erfolgte durch die perinnova compensation GmbH.

Der Vergleich mit der Anzahl Stellen, die sich heute in der Sicherheitsdirektion und der Finanzdirektion mit den Fragen der Cybersicherheit auseinandersetzen, ergibt folgendes Bild:

Tabelle 3: Vergleich mit heutiger Stellenanzahl im Bereich Cybersicherheit

| | Heutige Anzahl Stellen | Anzahl Stellen nach der Umsetzung der Cybersicherheitsstrategie |
|---|---|---|
| **Sicherheitsdirektion** (einschliesslich SOC KAPO) | **5** | **6** |
| **Finanzdirektion** | **8** | **25** |
| – davon Stellen der Cyber-Koordinatorin oder dem Cyber-Koordinator (Leistungsgruppe Nr. 4620) unterstellt | 1 | 11 |
| – davon Stellen der Leiterin oder dem Leiter Cyber Defence Center des AFI (Leistungsgruppe Nr. 4610) unterstellt | 7 | 14 |
| **Fünf weitere Direktionen und Staatskanzlei** | **6** | **6** |
| **Total** | **19** | **37** |

***Benchmarking***

Die Grösse der zukünftigen Cyberorganisation des Kantons Zürich ist vergleichbar mit der Grösse der Cyberorganisationen des Kantons Waadt sowie des Bundes.

Tabelle 4: Vergleich Kenngrössen andere Kantone und Bund

| Verwaltung/Organisation | Anzahl Mitarbeitende mit Cybersicherheitsaufgaben in zentraler Sicherheitsorganisation | Anzahl Mitarbeitende mit Cybersicherheitsaufgaben dezentral in den Departementen, Direktionen und Ämtern | Grösse der Organisation (Anzahl Mitarbeitende) | Anzahl betreute Arbeitsplätze | Anzahl betreute Applikationen | Anzahl Einwohner/innen |
|---|---|---|---|---|---|---|
| Kanton Zürich (Soll gemäss RRB) | 24 | 13 | 30 000 | 20 000 | 1 500 | 1 550 000 |
| Kanton Waadt (Stand Februar 2022) | 30 | | 15 000 | 15 000 | 3 000 | 800 000 |
| Bund (Stand Februar 2022) | 40 | 25 Vollzeitstellen; 76 Teilzeitstellen | 35 000 | 43 000 | 1 200 | 8 600 000 |

### *6.2 Sachkosten und Kosten externer Dienstleistungen*

Einzelne Leistungen werden von externen Dienstleisterinnen und Dienstleistern eingekauft und es entstehen Sachkosten. Die folgende Tabelle zeigt die entsprechenden Kosten für alle ausgewiesen neuen Aufgabenbereiche und Projekte, die im Zusammenhang mit der Cybersicherheitsstrategie stehen.

#### *Externe Dienstleistungen (Honorare)*

Tabelle 5: Schätzung der Kosten für externe Dienstleistungen (in Franken)

| Aufgabenbereich | Projektkosten (einmalig) 2022 | 2023 | 2024 | Total (einmalig) | Betriebskosten (wiederkehrend) ab 2025 |
|---|---|---|---|---|---|
| A 1.1 Bedrohungslagebild | 50 000 | 50 000 | | 100 000 | |
| A 2.1 Überprüfung und Weiterentwicklung Cybersicherheitsstrategie einschliesslich Umsetzungsdokument | | 25 000 | 25 000 | 50 000 | 25 000 |
| A 2.2 Regelwerk Informationssicherheit | | | 100 000 | 100 000 | 100 000 |
| A 2.3 Risikomanagement Informationssicherheit | 350 000 | 50 000 | 50 000 | 450 000 | 50 000 |
| A 2.4 Kantonale Sicherheitskultur | 75 000 | 150 000 | 150 000 | 375 000 | 150 000 |
| A 2.5 Audits im Bereich Informationssicherheit | 175 000 | 350 000 | 350 000 | 875 000 | 350 000 |
| A 2.7 Bug-Bounty-Programm | 125 000 | 250 000 | 250 000 | 625 000 | 250 000 |

| Aufgabenbereich | Projektkosten (einmalig) 2022 | 2023 | 2024 | Total (einmalig) | Betriebskosten (wiederkehrend) ab 2025 |
|---|---|---|---|---|---|
| A 2.8 Identity and Access Management | | 200 000 | 200 000 | 400 000 | |
| A 2.9 Security Operations Center und Cyber Defence Center | | 200 000 | 200 000 | 400 000 | |
| A 2.10 Public Key Infrastructure Services | | 125 000 | 75 000 | 200 000 | |
| A 2.11 Führen der Geschäftsstelle | 25 000 | 25 000 | 25 000 | 75 000 | 25 000 |
| A 3.2 Cyberkrisenmanagement | 50 000 | 100 000 | 100 000 | 250 000 | 100 000 |
| A 4.1 Betreiber kritischer Infrastrukturen unterstützen | | 25 000 | | 25 000 | |
| A 5.1 Städte und Gemeinden unterstützen | | 25 000 | | 25 000 | |
| A 6.1 Wirtschaft und Gewerbe unterstützen | | 25 000 | | 25 000 | |
| A 7.1 Bevölkerung sensibilisieren | | 25 000 | | 25 000 | |
| A 9.1 Auf neue Situationen reagieren (Reserve) | 100 000 | 200 000 | 200 000 | 500 000 | 200 000 |
| **Total** | **950 000** | **1 825 000** | **1 725 000** | **4 500 000** | **1 250 000** |

***Sachkosten (Hardwarekomponenten, Softwarelizenzkosten und Informatiknutzungsaufwand)***

Tabelle 6: Schätzung der anfallenden Sachkosten (in Franken)

| Aufgabenbereich | Projektkosten (einmalig) 2022 | 2023 | 2024 | Total (einmalig) | Betriebskosten (wiederkehrend) ab 2025 |
|---|---|---|---|---|---|
| A 1.1 Bedrohungslagebild | | 25 000 | 25 000 | 50 000 | 25 000 |
| A 2.3 Risikomanagement Informationssicherheit | 125 000 | 250 000 | 250 000 | 625 000 | 250 000 |
| A 2.4 Kantonale Sicherheitskultur | 50 000 | 100 000 | 100 000 | 250 000 | 100 000 |
| A 2.7 Bug-Bounty-Programm | 75 000 | 75 000 | 75 000 | 225 000 | 75 000 |
| A 2.8 Identity and Access Management | | 700 000 | 700 000 | 1 400 000 | 700 000 |
| A 2.9 Security Operations Center und Cyber Defence Center | | 800 000 | 800 000 | 1 600 000 | 800 000 |
| A 2.10 Public Key Infrastructure Services | | 350 000 | 350 000 | 700 000 | 350 000 |
| **Total** | **250 000** | **2 300 000** | **2 300 000** | **4 850 000** | **2 300 000** |

Die Kosten für den externen Personaldienstleister, für externe Dienstleistungen und die Sachkosten lassen sich wie folgt zusammenfassen:

Tabelle 7: Schätzung der anfallenden externen Dienstleistungen und Sachkosten (in Franken)

| | Projektkosten (einmalig) 2022 | 2023 | 2024 | Total (einmalig) | Betriebskosten (wiederkehrend) ab 2025 |
|---|---|---|---|---|---|
| Kosten für externen Personaldienstleister | 125 000 | 125 000 | | 250 000 | |
| Kosten externe Dienstleistungen | 950 000 | 1 825 000 | 1 725 000 | 4 500 000 | 1 250 000 |
| Sachkosten | 250 000 | 2 300 000 | 2 300 000 | 4 850 000 | 2 300 000 |
| **Total** | **1 325 000** | **4 250 000** | **4 025 000** | **9 600 000** | **3 550 000** |

Bei der Finanzierung der externen Dienstleistungen handelt es sich um gebundene Ausgaben gemäss § 37 Abs. 2 lit. a des Gesetzes über Controlling und Rechnungslegung (LS 611). Mit dem kantonalen Zentrum für Cybersicherheit werden zentralisiert Dienstleistungen auf strategischer und operativer Ebene erbracht. Diese Dienstleistungen gehören gemäss den Empfehlungen des Sicherheitsverbundes Schweiz zur zeitgemässen Verwaltungstätigkeit und sichern die eingesetzten Sachmittel zur Erfüllung der gesetzlich vorgeschriebenen Aufgaben.

### *6.3 Budgetdeckung*

Die Finanzdirektion und die Sicherheitsdirektion kompensieren den jeweiligen Aufwand für die zu schaffenden Stellen nach Möglichkeit innerhalb der Budgets im Jahr 2022 in den jeweiligen Leistungsgruppen gemäss Tabelle 1 und stellen den jeweiligen Aufwand im Konsolidierten Entwicklungs- und Finanzplan (KEF) 2023–2026 ein.

Die Sachkosten und die Kosten für externe Dienstleistungen sind hingegen nicht im Budget 2022 der betroffenen Leistungsgruppen enthalten und können auch nicht kompensiert werden. Für die Kosten im Jahr 2022 wird gegebenenfalls ein Nachtragskredit zu beantragen sein. Die Kosten ab 2023 werden in den KEF 2023–2026 eingestellt.

Die wiederkehrenden Kosten belaufen sich ab 2025 auf jährlich Fr. 3 550 000. Von diesen Kosten entfallen Fr. 2 300 000 auf Sachkosten und Fr. 1 250 000 auf externe Dienstleistungen.

## 7. Folgen eines Verzichts auf eine Cybersicherheitsstrategie

Ohne die vorliegende Cybersicherheitsstrategie wäre der Kanton Zürich nicht ausreichend gegen Cyberrisiken geschützt. Im Falle eines Ereignisses könnte der Kanton Zürich nicht auf Daten oder Systeme zugreifen und es wäre mit Verlusten von kritischen Geschäftsinformationen oder Ausfällen von digitalen Dienstleistungen in der kantonalen Verwaltung zu rechnen. Er würde damit an Handlungsfähigkeit einbüssen und würde die Erfüllung seiner Aufgaben gefährden. Es bestände die Gefahr, die Daten seiner Bevölkerung oder im schlimmsten Fall die Bevölkerung selbst nicht angemessen schützen zu können.

Mit einem Verzicht auf die Strategie vergäbe der Kanton Zürich die Chance einer zentralen und fachkundigen Umsetzung wie er sie auch bei der IKT-Strategie verfolgt. Damit würden Synergien zu wenig genutzt und es wäre anspruchsvoller, ein durchgängiges Sicherheitsniveau zu erreichen.

Der Kanton Zürich käme damit den Ansprüchen an eine sorgfältige Verwaltungsführung im Sinne einer «Good Governance» nicht nach und nähme damit eine Beeinträchtigung seines Ansehens und seiner Vertrauenswürdigkeit in Kauf. Die Erfüllung seiner Sorgfaltspflichten wäre nicht sichergestellt und es wäre mit nachteiligen Auswirkungen auf andere Strategien zu rechnen (Strategie Digitale Verwaltung, digitales Zielbild). Der Kanton Zürich würde es verpassen, eine Stellung als fortschrittlicher Kanton mit einer Vorreiterrolle im Bereich der Cybersicherheit einzunehmen. Dem Wunsch der Bevölkerung nach einem höheren Stellenwert der Cybersicherheit in der Verwaltung würde nicht Rechnung getragen. Der Kanton Zürich würde damit als Standort an Anziehungskraft verlieren.

## 8. Steuerungsgremium Digitale Verwaltung und IKT

Das Steuerungsgremium Digitale Verwaltung und IKT hat den vorliegenden Antrag an seiner Sitzung vom 14. März 2022 zuhanden des Regierungsrates vorberaten und diesem zugestimmt.

Auf Antrag der Finanzdirektion

beschliesst der Regierungsrat:

I. Die Cybersicherheitsstrategie und die dazugehörige Umsetzungsplanung werden festgesetzt und auf den 1. Juli 2022 in Kraft gesetzt.

II. Die Finanzdirektion wird beauftragt, die Cybersicherheitsstrategie umzusetzen.

III. Die Organisation wird gemäss Erwägung 4 festgesetzt.

IV. Für die Umsetzung der Strategie und die Bereitstellung der Dienstleistungen gemäss Ziff. 3 und 4.2 der Erwägungen werden folgende Stellen geschaffen:

a. Im Stellenplan des Amtes für Informatik, Leistungsgruppe Nr. 4610, mit Wirkung ab 1. Juli 2022:

| Stellen | Richtposition | Klasse VVO |
|---|---|---|
| 1,0 | Informatikspezialist/in mbA | 21 |

b. Im Stellenplan des Amtes für Informatik, Leistungsgruppe Nr. 4620 IKT-Sicherheitsbeauftragter, mit Wirkung ab 1. Juli 2022:

| Stellen | Richtposition | Klasse VVO |
|---|---|---|
| 1,0 | Informatikspezialist/in mbA | 23 |
| 3,0 | Informatikspezialist/in mbA | 22 |
| 1,0 | Informatikspezialist/in | 20 |

c. Im Stellenplan der Kantonspolizei, Leistungsgruppe Nr. 3100, mit Wirkung ab 1. Januar 2023:

| Stellen | Richtposition | Klasse VVO |
|---|---|---|
| 1,0 | Informatikspezialist/in mbA | 21 |

d. Im Stellenplan des Amtes für Informatik, Leistungsgruppe Nr. 4610, mit Wirkung ab 1. Januar 2023:

| Stellen | Richtposition | Klasse VVO |
|---|---|---|
| 3,0 | Informatikspezialist/in mbA | 21 |

e. Im Stellenplan des Amtes für Informatik, Leistungsgruppe Nr. 4620 IKT-Sicherheitsbeauftragter, mit Wirkung ab 1. Januar 2023:

| Stellen | Richtposition | Klasse VVO |
|---|---|---|
| 1,0 | Informatikspezialist/in mbA | 22 |
| 1,0 | Adjunkt/in | 20 |

f. Im Stellenplan des Amtes für Informatik, Leistungsgruppe Nr. 4610, mit Wirkung ab 1. Januar 2024:

| Stellen | Richtposition | Klasse VVO |
|---|---|---|
| 3,0 | Informatikspezialist/in mbA | 21 |

g. Im Stellenplan des Amtes für Informatik, Leistungsgruppe Nr. 4620, IKT-Sicherheitsbeauftragter, mit Wirkung ab 1. Januar 2024:

| Stellen | Richtposition | Klasse VVO |
|---|---|---|
| 2,0 | Informatikspezialist/in mbA | 22 |
| 1,0 | Verwaltungsassistent/in | 13 |

V. Für die Umsetzung der Strategie und die Bereitstellung der Dienstleistungen gemäss Ziff. 3 und 4.2 der Erwägungen wird eine gebundene Ausgabe von Fr. 9 600 000 zulasten der Erfolgsrechnung der Leistungsgruppe Nr. 4620, IKT-Sicherheitsbeauftragter, bewilligt.

VI. Für den weiteren Betrieb und die Weiterentwicklung der Dienstleistungen gemäss Ziff. 3 und 4.2 der Erwägungen wird ab 2025 eine jährlich wiederkehrende gebundene Ausgabe von Fr. 3 550 000 zulasten der Erfolgsrechnung Leistungsgruppe Nr. 4620, IKT-Sicherheitsbeauftragter, bewilligt.

VII. Die Ausgabenbewilligung gemäss Dispositiv VI wird alle drei Jahre abgerechnet.

VIII. Mitteilung an die Direktionen des Regierungsrates, die Staatskanzlei, die Finanzkontrolle und die Datenschutzbeauftragte.

Vor dem Regierungsrat
Die Staatsschreiberin:

**Kathrin Arioli**