Kanton Zürich
Regierungsrat

Kantonale Cybersicherheits-strategie

4. Mai 2022

Inhalt

1. Allgemeine Bestimmungen

Zweck und Einbettung

Die kantonale Cybersicherheitsstrategie bildet den Rahmen, damit Regierung und Verwaltung im Bereich der Cyberrisiken[1] vorausschauend und wirksam handeln können.

Die Strategie legt Vision, Ziele, Grundhaltungen und Handlungsfelder fest, die dafür sorgen, dass der Kanton Zürich widerstandsfähig gegenüber Cyberrisiken ist und dass seine Handlungsfähigkeit gewährleistet bleibt.

Die Strategie ist abgestimmt mit der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken, dem daraus abgeleiteten Umsetzungsplan der Kantone sowie auf kantonaler Ebene mit den Richtlinien der Regierungspolitik 2019–2023 (Legislaturziel 10: Datensicherheit und Vertrauen), der Strategie Digitale Verwaltung (2018–2023) und der kantonalen IKT-Strategie vom 25. April 2018.

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 (IDG; LS 170.4) sowie §§ 12 und 13 der Verordnung über die Informationsverwaltung und -sicherheit vom 3. September 2019 (IVSV; LS 170.8).

Auftrag

Mit der kantonalen Cybersicherheitsstrategie schafft der Kanton eine gemeinsame Grundlage für Entscheide mit Bezug zu Cyberrisiken. Diese betreffen

a. den Umgang mit Cyberrisiken,

b. die Planung, Steuerung und den Ressourceneinsatz zum Umgang mit Cyberrisiken in der kantonalen Verwaltung,

c. die Aufgaben, Kompetenzen und Verantwortlichkeiten der jeweiligen Organe.

Geltungsbereich

Die kantonale Cybersicherheitsstrategie richtet sich an

a. die Direktionen des Regierungsrates und die Staatskanzlei,

b. die unselbstständigen Anstalten und weitere Träger öffentlicher Aufgaben, soweit der Kanton sie beaufsichtigt.

Der Regierungsrat kann Ausnahmen vom Geltungsbereich bewilligen. Der Geltungsbereich der Cybersicherheitsstrategie ist regelmässig zu prüfen.

Jede Organisation, die an Lösungen der kantonalen Verwaltung in spezifischen Bereichen partizipiert, wie z.B. selbstständige Anstalten, ist verpflichtet, sich in diesem Bereich an die Vorgaben der kantonalen Cybersicherheitsstrategie zu halten.

[1] Schlüsselbegriffe und Abkürzungen sind im Anhang erläutert.

Zielgruppen ausserhalb der kantonalen Verwaltung

Der Kanton Zürich arbeitet mit folgenden Zielgruppen ausserhalb des oben beschriebenen Geltungsbereichs zusammen:

- Betreiber kritischer Infrastrukturen des Kantons Zürich
- Städten und Gemeinden
- Wirtschaft und Gewerbe des Kantons Zürich
- Zürcher Wohn- und Arbeitsbevölkerung

Er stimmt sich bei dieser Zusammenarbeit mit den Aktivitäten des Bundes zum Schutz vor Cyberrisiken ab.

Die Eigenverantwortung der Zielgruppen bleibt unangetastet.

Erfahrungsaustausch und Zusammenarbeit

Der Kanton Zürich pflegt den Erfahrungsaustausch und bei Bedarf die Zusammenarbeit mit:

- Hochschulen (insbesondere mit der ETH und UZH)
- Bund
- anderen Kantone
- nationalen und internationalen Expertengremien und Behörden

2. Vision, Ziele, Grundsätze

2.1 Vision

Gestalten und Stärken

Der Kanton Zürich gestaltet und stärkt mit dem Bund, den Kantonen, den Gemeinden und weiteren Partnern die Widerstandsfähigkeit gegen Cyberrisiken zum Nutzen der Bevölkerung, der Wirtschaft und der eigenen Mitarbeiterinnen und Mitarbeiter.

Der Kanton Zürich schützt sich vor Cyberrisiken und stärkt damit seine Stellung als weltoffener, innovativer, wirtschaftlich, kulturell und sozial starker Kanton. Digitalisierung als strategischer Schwerpunkt des Regierungsrates setzt Cybersicherheit voraus. Deshalb sichern Investitionen in die Cybersicherheit und die Informationssicherheit die Zukunftsfähigkeit und stärken den Kanton Zürich als hochwertigen und vertrauensvollen Partner auch in der digitalen Welt.

Alle Direktionsleitungen der kantonalen Verwaltung und die Staatskanzlei tragen das Thema mit und handeln entlang den nachfolgenden Zielen und Grundsätzen.

Breiter Schutz

Der Kanton Zürich ist auch in der digitalen Welt ein sicherer, vertrauensvoller und attraktiver Partner, indem er

- die Verwaltung vor Cyberrisiken schützt und seine Handlungsfähigkeit auch im Ereignisfall wahrt,
- eine positive Sicherheitskultur schafft,
- seine Widerstandsfähigkeit und die Widerstandsfähigkeit der Zielgruppen stärkt, damit alle die Errungenschaften und Chancen der Digitalisierung nutzen können.

2.2 Ziele

Widerstandsfähig

Der Kanton Zürich ist widerstandsfähig; Regierung und Verwaltung kennen die Cyberrisiken und verfügen über die Fähigkeiten, mit aktuellen Cyberrisiken und neuen Bedrohungen umzugehen.

Der Kanton betreibt ein sicheres und hochverfügbares digitales Leistungsangebot, er handelt proaktiv, er beobachtet laufend die Bedrohungslage, er schützt sich mit präventiven Massnahmen und kann im Ereignisfall Schaden abwenden oder eingrenzen, Verursacher identifizieren und verfolgen und einen sicheren Zustand wiederherstellen.

Gut organisiert

Der Kanton Zürich ist zweckmässig organisiert; er verfügt über die notwendigen Ressourcen und Sachkenntnisse, um mit Cyberrisiken im normalen Betrieb und im Ereignisfall umzugehen. Die zugehörigen internen und externen Aufgaben, Kompetenzen und Verantwortlichkeiten sind geregelt.

Vernetzt

Der Kanton Zürich ist vertrauenswürdig. Er ist nach innen und nach aussen vernetzt, er stärkt die Kooperation zwischen den Akteuren, er geht Lösungen gemeinsam und ganzheitlich mit seinen Partnern an, und er bewältigt die Cyberrisiken im gegenseitigen Austausch mit ihnen.

2.3 Grundsätze

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

Grundsätze für das Handeln von Regierung und Verwaltung

Kooperation: Der Kanton Zürich verfolgt einen kooperativen Ansatz. Er arbeitet mit dem Bund, anderen Kantonen, Städten und Gemeinden, Hochschulen, nationalen und internationalen Organisationen und Unternehmen zusammen, um die Vernetzung zu stärken. Er stellt die verwaltungsinternen Lösungen und Cybersicherheitsdienstleistungen, wo gesetzlich möglich und erwünscht, den Zielgruppen und Partnern zur Verfügung.

Regeln und Standards: Der Kanton Zürich hält sich an anerkannte Regeln und Standards des Risikomanagements, der Informationssicherheit und der Cybersicherheit. Er hält sich an die entsprechenden gesetzlichen Bestimmungen.

Wirksamkeit: Der Kanton setzt seine Ressourcen zum Schutz vor Cyberrisiken risikobasiert und kostenwirksam ein. Er nutzt bestehende Organisationen und Abläufe.

Kontinuierliche Weiterentwicklung: Der Kanton Zürich weiss, dass Cyberrisiken sich stetig verändern, er setzt sich mit neuen Entwicklungen auseinander, er pflegt bestehende Massnahmen, entwickelt sie kontinuierlich weiter und erarbeitet neue Massnahmen.

Eigenverantwortung: Der Kanton Zürich unterstützt das eigenverantwortliche Handeln der Zielgruppen.

Zuständigkeit: Der Kanton Zürich regelt, welche Aufgaben er selbst bewältigt und wo er sich von Dritten unterstützen lässt.

Transparenz: Der Kanton Zürich informiert offen und klar über seine Anstrengungen im Bereich Cybersicherheit sowie über Risiken und wichtige Vorfälle und ihre Auswirkungen.

Befähigung: Der Kanton Zürich befähigt die Mitarbeitenden der kantonalen Verwaltung, sich selbst zu schützen. Er unterstützt Aus- und Weiterbildungen.

3. Handlungsfelder

Um die gesteckten Ziele zu erreichen, gliedert der Kanton Zürich seine Tätigkeiten in neun Handlungsfelder. In jedem Handlungsfeld ist erläutert, wie der Kanton den Schutz vor Cyberrisiken stärken will. Die spezifischen Aufgaben und Zuständigkeiten sind im Umsetzungsdokument näher erläutert.[2]

Die Umsetzung und Wirksamkeit der Arbeiten innerhalb der Handlungsfelder werden von einer Qualitäts- und Risikomanagerin oder einem Qualitäts- und Risikomanager regelmässig überprüft.

3.1 Handlungsfeld 1: Bedrohungslage kennen

Der Kanton Zürich kennt die aktuellen Cyberbedrohungen für die kantonale Verwaltung, und er ist vertraut mit den wesentlichen Entwicklungen in der Informationstechnologie, den damit verbundenen Risiken und den möglichen Schutzmassnahmen. Er führt ein Bedrohungslagebild nach, um Cyberangriffe zu erkennen und um Massnahmen zum Schutz, zur Abwehr und zur Bewältigung von Cyberangriffen auszulösen. Er kann die relevanten Akteure gezielt informieren, Empfehlungen und Hinweise geben und vor Gefahren warnen.

Der Kanton Zürich betreibt eine eigene Erkennung, Schutz, Abwehr und Bewältigung von Cyberangriffen.

Der Kanton Zürich führt bei Bedarf spezifische Gefährdungsanalysen durch und regt entsprechende Massnahmen an.

[2] Wichtige Grundlagen wurden bereits im Rahmen der IKT-Strategie erarbeitet, und es wurden Stellen geschaffen, die sich mit Aufgaben zum Schutz vor Cyberrisiken auseinandersetzen. Im Umsetzungsdokument wird ausgewiesen, was bereits besteht und was durch die Cybersicherheitsstrategie ergänzend dazukommt.

3.2 Handlungsfeld 2: Verwaltung stärken

Der Kanton Zürich stärkt den Schutz vor Cyberrisiken innerhalb der Verwaltung, indem er die Mitarbeitenden befähigt, die Organisation stärkt sowie Systeme und Daten schützt.

Er fördert eine Sicherheitskultur, in der Risiken erkannt, offengelegt und bewältigt werden. Er informiert, sensibilisiert, schult und trainiert seine Mitarbeitenden und kann für externe Lieferanten Vorgaben machen.

Er stellt eine sichere und hochverfügbare IKT-Infrastruktur und Cybersicherheitsdienstleistungen bereit, die von der Verwaltung genutzt werden können. Er lagert gegebenenfalls Cybersicherheitsdienstleistungen unter definierten Bedingungen an spezialisierte Dritte aus.

Er definiert einen Grundschutz zur Informationssicherheit, setzt ihn um und entwickelt ihn weiter.

Er vernetzt die zuständigen Ansprechpersonen innerhalb der Verwaltung, begleitet und unterstützt sie und regt einen Austausch an.

Er stärkt diejenigen Stellen, die sich mit dem Schutz vor Cyberrisiken auseinandersetzen, damit diese rasch und situationsgerecht auf Gefährdungen reagieren können.

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. Er arbeitet eng mit der für die Strafverfolgung zuständigen Kantonspolizei und der Staatsanwaltschaft zusammen und koordiniert sich mit ihnen.

Die Aufgaben, Kompetenzen und Verantwortlichkeiten für den Ereignisfall sind geregelt, das betrifft auch die Unterstützung durch externe Partner im Eskalationsfall. Der Kanton führt mit ausgewählten Partnern regelmässig Krisenübungen durch.

3.4 Handlungsfeld 4: Betreiber kritischer Infrastrukturen sensibilisieren

Der Kanton Zürich kennt seine kritischen Infrastrukturen und die Cyberrisiken, die sie bedrohen.

Der Kanton Zürich pflegt den regelmässigen Kontakt mit den Betreibern seiner kritischen Infrastrukturen und tauscht sich über aktuelle Entwicklungen im Zusammenhang mit Cyberrisiken aus.

Der Kanton Zürich sensibilisiert die Betreiber der kritischen Infrastrukturen über den Schutz vor Cyberrisiken. Der Kanton spricht sich dabei vorgängig mit dem Bund und dem Sicherheitsverbund Schweiz ab.

Der Kanton Zürich nimmt am Erfahrungsaustausch im Rahmen der Schweizerischen Informatikkonferenz sowie an massgeblichen Konferenzen mit der Forschung teil, wo die Zusammenarbeit zur Stärkung der IKT-Resilienz gefördert werden soll.

Der Kanton Zürich unterstützt den Bund bei den Massnahmen zur Verbesserung der IKT-Resilienz der kritischen Infrastrukturen.

3.5 Handlungsfeld 5: Städte, Gemeinden und kantonsnahe Organisationen vernetzen und unterstützen

Der Kanton Zürich pflegt einen regelmässigen Austausch mit Vertretenden der Städte und Gemeinden des Kantons Zürich, dem Kantonsrat, den Parlamentsdiensten sowie den kantonalen Gerichten und Notariaten über den Schutz vor Cyberrisiken. Er unterstützt und fördert deren Vernetzung zur Stärkung der IKT-Resilienz.

Cybersicherheitsdienstleistungen, die der kantonalen Verwaltung angeboten werden, können zu einem späteren Zeitpunkt im Rahmen der rechtlichen Möglichkeiten auch von den Städten und Gemeinden, dem Kantonsrat, den Parlamentsdiensten sowie den kantonalen Gerichten und Notariaten genutzt werden.

Der Kanton Zürich kann den Städten und Gemeinden, dem Kantonsrat, den Parlamentsdiensten sowie den kantonalen Gerichten und Notariaten Cybersicherheitsdienstleistungen vermitteln.

3.6 Handlungsfeld 6: Wirtschaft und Gewerbe unterstützen

Der Kanton Zürich pflegt einen regelmässigen Austausch mit Vertretenden aus Wirtschaft und Gewerbe über den Schutz vor Cyberrisiken.

Der Kanton Zürich unterstützt und fördert die Vernetzung zum Schutz vor Cyberrisiken in den Branchen.

Der Kanton Zürich unterstützt und fördert Informationskampagnen der Wirtschaft und des Gewerbes zum Schutz vor Cyberrisiken.

3.7 Handlungsfeld 7: Bevölkerung sensibilisieren

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

Der Kanton Zürich fördert und unterstützt Kampagnen zum Thema Cybersicherheit. Bei Bedarf führt er selbst Kampagnen durch. Der Kanton spricht sich dabei vorgängig mit seinen Städten und Gemeinden, der Wirtschaft und dem Gewerbe sowie dem Bund und den anderen Kantonen ab.

3.8 Handlungsfeld 8: Vernetzung und Austausch pflegen

Der Kanton Zürich pflegt den Austausch mit seinen Nachbarkantonen sowie mit nationalen und internationalen Gremien und Expertinnen und Experten im Cyberbereich.

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.

4. Umsetzung der Strategie

Umsetzung und Etappierung

Die kantonale Cybersicherheitsstrategie tritt durch den Beschluss des Regierungsrates (RRB «Cybersicherheitsstrategie» Festsetzung, Umsetzung, Stellenplan, Ausgabenbewilligung; 26. April 2022) in Kraft. Mit dem Entscheid werden auch die notwendigen Ressourcen zum Aufbau und Betrieb der Organisation zum Schutz vor Cyberrisiken bereitgestellt.

Die Umsetzung der Strategie erfolgt gemäss dem Dokument «Kantonale Cybersicherheitsstrategie – Organisation und Umsetzung (26. April 2022)» in Etappen; in einer ersten Phase (2022–2023) liegt der Schwerpunkt auf den Handlungsfeldern 1, 2 und 3, wo 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 Betreiber kritischer Infrastrukturen, die Städte, Gemeinden und kantonsnahen Organisationen, die Wirtschaft und das Gewerbe sowie die Zürcher Wohn- und Arbeitsbevölkerung.

Steuerung, Führung und Umsetzung

Die Steuerung der Umsetzung liegt beim Steuerungsgremium Digitale Verwaltung und IKT (SDI), die operative Führung der Umsetzung erfolgt durch die Finanzdirektion.

Die Umsetzung der Strategie wird regelmässig durch eine externe Qualitätsmanagerin oder einen externen Qualitätsmanager überprüft, die oder der vom strategischen Cyberausschuss beauftragt wird.

Die Finanzdirektion und das Steuerungsgremium Digitale Verwaltung und IKT stellen die regelmässige Berichterstattung an den Regierungsrat sicher.

5. Gültigkeit und Weiterentwicklung

Weiterentwicklung

Die kantonale Cybersicherheitsstrategie ist langfristig ausgelegt. Sie wird aktualisiert, wenn besondere Umstände oder neue Erkenntnisse dies notwendig machen, jedoch spätestens nach drei Jahren.

Die Steuerung der Überarbeitung liegt beim Steuerungsgremium Digitale Verwaltung und IKT, ihre operative Führung bei der Finanzdirektion.

A. Anhang: Abkürzungen und Glossar

AFI	Amt für Informatik
CDC	Cyber Defence Center; Weiterentwicklung eines SOC
Cyberangriff	Beabsichtigte unerlaubte Handlung einer Person oder einer Gruppierung im Cyberraum, um die Integrität, Vertraulichkeit oder Verfügbarkeit von Informationen und Daten zu beeinträchtigen; dies kann je nach Art des Angriffs auch zu physischen Auswirkungen führen.
Cyberbedrohung	Vorgang, der zum Eintreten eines Cybervorfalls führen kann.
Cyberkriminalität	Cyberkriminalität im engeren Sinn betrifft Straftaten, die mithilfe der Informations- und Kommunikationstechnologien (IKT) verübt werden oder sich Schwachstellen dieser Technologien zunutze machen. Cyberkriminalität im weiteren Sinn nutzt das Internet als Kommunikationsmittel, wobei die sich bietenden Möglichkeiten wie z.B. der E-Mail-Verkehr oder der Austausch bzw. das Bereitstellen von Dateien für unlautere Zwecke missbraucht werden. Diese Aktivitäten sind nicht neu, aber die dabei verwendeten Tat- und Speichermedien (z.B. E-Mail, Instant-Messaging-Dienste, elektronische Datenträger) sind neu.
Cyberraum	Die Gesamtheit der durch das Internet weltweit erreichbaren Informationsinfrastrukturen
Cyberrisiken	Das Produkt der Eintrittswahrscheinlichkeit und des Schadenausmasses von Cybervorfällen
Cybersicherheit	Die Gesamtheit aller Technologien, Prozesse und Vorgehensweisen, die Netzwerke, Computer, Programme und Daten, die durch das Internet und durch vergleichbare Netze weltweit erreichbar sind, vor Angriffen, Schäden oder unerlaubten Zugriffen schützen sollen.
Cybersicherheits-dienstleistungen	Durch das SOC/CDC erbrachte Dienstleistungen (Security Services)
Cybervorfall	Beabsichtigtes oder unbeabsichtigtes Ereignis, das im Cyberraum zu einem Vorgang führt, der die Integrität, Vertraulichkeit oder Verfügbarkeit von Daten und Informationen beeinträchtigt und zu Fehlfunktionen führen kann.
ETH	Eidgenössische Technische Hochschule Zürich
FAGIS	Fachgruppe IKT-Sicherheit
FD	Finanzdirektion
IDG	Gesetz über die Information und den Datenschutz vom 12. Februar 2007 (LS 170.4)
IKT	Informations- und Kommunikationstechnologien
Informationssicherheit	Informationssicherheit ist die Unversehrtheit der Authentizität, Vertraulichkeit, Integrität und Verfügbarkeit eines informations- und kommunikationstechnischen Systems und der darin verarbeiteten und gespeicherten Daten.

IVSV	Verordnung über die Informationsverwaltung und -sicherheit vom 3. September 2019 (LS 170.8)
Kanton Zürich	Die Regierung und Verwaltung des Kantons Zürich. Dabei mitgemeint sind auch all seine schützenswerten Güter (IKT-Inventar).
Kapo	Kantonspolizei
KFO	Kantonale Führungsorganisation
Krise, Krisenfall	Ein Ereignis, bei dem der ganze Kanton betroffen ist und die KFO involviert wird, weil es relevant für den Bevölkerungsschutz ist.
Kritische Infrastrukturen	Prozesse, Systeme und Einrichtungen, die essenziell für das Wohlergehen der Bevölkerung bzw. das Funktionieren der Wirtschaft sind.
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
NCSC	Nationales Zentrum für Cybersicherheit
Resilienz	Die Fähigkeit eines Systems, einer Organisation oder einer Gesellschaft, Störungen zu widerstehen und die Funktionsfähigkeit möglichst zu erhalten bzw. rasch wieder zu erlangen.
SDI	Gremium Steuerung Digitale Verwaltung und IKT
SIK	Schweizerische Informatikkonferenz
SK	Staatskanzlei
SKI	Schutz kritischer Infrastrukturen
SOC	Security Operations Center
SVS	Sicherheitsverbund Schweiz
UZH	Universität Zürich
Verwaltung	Kantonale Verwaltung des Kantons Zürich; bestehend aus sieben Direktionen und der Staatskanzlei

B. Beteiligte

Die kantonale Cybersicherheitsstrategie wurde vom März bis zum Dezember 2021 durch das unten aufgeführte Projektteam entwickelt. Das Projektteam wurde bei der Erarbeitung der Strategie durch ein breit angelegtes Begleitteam unterstützt.

B.1. Projektteam

- Hansruedi Born, Amt für Informatik, Chief Information Officer
- Philipp Grabher, Amt für Informatik, Chief Information Security Officer
- Serdar Günal Rütsche, Kantonspolizei, Chef Cybercrime
- Jörg Ochsner, Amt für Informatik, Leiter Sicherheit in der Grundversorgung
- Dominik Schwerzmann, Kantonspolizei, Chef Bevölkerungsschutz
- Stephan Walder, Staatsanwaltschaft, Stv. Leitender Staatsanwalt
- Martin Wirz, Kantonspolizei, Chef Informatik
- EBP Schweiz AG, externe Unterstützung

B.2. Begleitteam

- Wolfgang Annighöfer, Generalsekretariat Bildungsdirektion, Leiter Finanzen und Bauten
- Markus Christen, Digital Society Initiative der Universität Zürich, Geschäftsführer
- Daniel Coray, SIX, Head Cyber Security
- Hanspeter Erzinger, Generalsekretariat Volkswirtschaftsdirektion, Stv. Leiter Digitale Transformation
- Erik Dinkel, Universitätsspital Zürich, Chief Information Security Officer
- Juan Galindo, Kaufmännischer Verband Kanton Zürich, Leiter ICT
- René Christian Gehlen, Stadt Zürich, Organisation und Informatik, Leiter IT-Security & Risk
- Lukas Geissmann, Generalsekretariat Sicherheitsdirektion, Generalsekretär
- Beatrice Hasler-Dierauer, Mittelschul- und Berufsbildungsamt, Leiterin Ressourcen
- Thomas Hess, KMU- und Gewerbeverband Kanton Zürich, Geschäftsstelle
- Raphael Iselin, Generalsekretariat Baudirektion, IT Security Officer / Projektleiter

- Urs Isenring, ewz, Chief Information Security Officer
- Peter Kölsch, Stadt Wetzikon, Stabsstellenleiter Informatik
- Anita Martinecz Fehér, Volkswirtschaftsdirektion, Amt für Wirtschaft und Arbeit, Stv. Leiterin Standortförderung, Kooperationsnetzwerk eZürich
- Eva May, Volkswirtschaftsdirektion, Amt für Wirtschaft und Arbeit, Standortförderung, Projektleiterin Cluster Finance
- Marc McGuinness, Chief Information Security Officer, Zürcher Hochschule für Angewandte Wissenschaften (ZHAW)
- Fabio Morandi, Flughafen Zürich, Teamleiter ICT Application Development
- Markus Mösch, Gesundheitsdirektion, Leiter Ressort Digitalisierung
- Christoph Mosimann, Gesundheitsdirektion, Leiter Finanzen & Digital Management
- Matthias Müller, Staatskanzlei, Risikomanager, Informationssicherheitsbeauftragter
- Lars Mülli, Gebäudeversicherung Kanton Zürich, Direktor / Vorsitzender der Geschäftsleitung
- Alessia Neuroni, Staatskanzlei, Leiterin Abteilung Digitale Verwaltung und E-Government
- Gian Schmid, Generalsekretariat Volkswirtschaftsdirektion, Generalsekretär
- Olaf Schwyter, Elektrizitätswerke des Kantons Zürich, Chief Information Security Officer
- Arno Stark, ewz, Leiter Digitalisierung & Informatik
- Lukas Steudler, Leiter Geschäftsstelle egovpartner
- Manuel Suter, Geschäftsstelle NCSC
- Petra Vogel, Volkswirtschaftsdirektion, Amt für Wirtschaft und Arbeit, Wissenschaftliche Mitarbeiterin Amtsleitung
- Lukas Weibel, Staatskanzlei, Leiter Business Engineering und Projekte