

Auszug aus dem Protokoll des Regierungsrates des Kantons Zürich

Sitzung vom 30. September 2020

965. Security Operations Center (Ausgabenbewilligung, Vergabe)

1. Ausgangslage

Der Regierungsrat hat mit Beschluss Nr. 383/2018 eine neue kantonale IKT-Strategie festgelegt und die Finanzdirektion mit deren Umsetzung beauftragt. Die IKT-Strategie wird in einem Programm mit zwölf Projekten umgesetzt (vgl. RRB Nr. 625/2019). Eine der zentralen strategischen Stossrichtungen bildet das verwaltungsweite Management der IKT-Sicherheit (Ziff. 3.6 der IKT-Strategie). Dazu wird auch eine operative IKT-Sicherheitsstelle, das sogenannte «Security Operations Center (SOC)», im Amt für Informatik (AFI) aufgebaut.

Für den Betrieb des SOC und weitere Dienstleistungen in der operativen Informationssicherheit, insbesondere die Weiterentwicklung des SOC, ist externe Unterstützung erforderlich (vgl. RRB Nr. 625/2019, Ziff. 3.4).

2. Öffentliche Ausschreibung und Vergabe

Am 1. Juni 2020 wurde die Ausschreibung «Managed Security Services für SOC» im offenen Verfahren im Staatsvertragsbereich auf der Plattform simap.ch publiziert. Interessierte Unternehmen haben die Ausschreibungsunterlagen nach Unterzeichnung einer Vertraulichkeitserklärung erhalten.

Der Leistungsbezug ist in zwei Varianten möglich: In der Variante 1 wird die SOC-Anwendung in den Rechenzentren des Kantons durch die Leistungserbringerin betrieben; in der Variante 2 werden nur die Log-Daten lokal verwaltet und die SOC-Anwendung als Service von der Leistungserbringerin bezogen. Angebote waren für eine der Varianten oder für beide Varianten zulässig.

Bis zur Eingabefrist am 13. Juli 2020 sind zehn Angebote eingegangen; neun für die Variante 1 und eines für die Variante 2. Das einzige Angebot für Variante 2 umfasst eine technisch wenig passende und unwirtschaftliche Lösung, womit eine Grundsatzdiskussion zur Variantenwahl entfällt.

Bei der Bewertung der Variante 1 erreichte die ISPIN AG, Bassersdorf, die höchste Punktzahl. Ihr Angebot ist damit das wirtschaftlich günstigste und erhält den Zuschlag.

Mit der Zuschlagsempfängerin wird ein Rahmenvertrag abgeschlossen, der die übergreifenden Elemente der Zusammenarbeit regelt. Gestützt auf diesen Rahmenvertrag werden Einzelverträge abgeschlossen. Verträge für wiederkehrende Betriebsleistungen können mit einer Laufzeit von vier Jahren abgeschlossen und optional viermal um ein Jahr verlängert werden. Ob die Vertragsverlängerung beansprucht wird, entscheidet die Vergabestelle zu gegebener Zeit. Zusätzlich werden zwei ausgeschriebene optionale Leistungen vergeben: eine Lösung zum Schutz von Endgeräten (Option 2) und ein Schwachstellenscanner, um Sicherheitslücken in der IKT-Infrastruktur zu erkennen (Option 3).

3. Finanzielles

Für die Vergaben werden einzelne Ausgaben ausserhalb des Programms zur Umsetzung der kantonalen IKT-Strategie bewilligt (vgl. RRB Nrn. 492/2020 und 623/2020). Der Leistungsbezug und damit auch die Vertragslaufzeit sind vom Programm und von anderen Beschaffungen wie der IKT-Grundversorgung unabhängig, sodass sie nicht als Einheit betrachtet werden müssen (§ 40 Gesetz über Controlling und Rechnungslegung [CRG, LS 611]).

Die Weiterentwicklung des SOC richtet sich nach den künftigen Bedürfnissen und Bedrohungslagen, sodass derzeit nur Schätzungen möglich sind. Aus diesem Grund wird eine Reserve für Unvorhergesehenes berücksichtigt.

	in Franken
Angebot der Zuschlagsempfängerin (einschliesslich 7,7% MWSt)	4 389 518
rund 10% Reserve	410 482
Total Ausgaben einschliesslich Reserven	4 800 000

Für die Vergabe ist eine gebundene Ausgabe von 4,8 Mio. Franken zu bewilligen. Professionelle SOC-Services gehören zur zeitgemässen Verwaltungstätigkeit und sichern die eingesetzten Sachmittel zur Erfüllung der gesetzlich vorgeschriebenen Aufgaben (§ 37 Abs. 2 lit. a CRG). Mit der fortschreitenden Digitalisierung vergrössern sich die Angriffsflächen und damit auch die Risiken für die Sicherstellung der Aufgabenerfüllung des Kantons. In solchen Bedrohungslagen sind neben Prävention ein schnelles Erkennen und Reagieren auf Vorfälle unabdingbar.

Die Ausgabe geht zulasten der Erfolgsrechnung. Sie enthält neben Projekt- und Betriebsleistungen auch die Softwarelizenzen, die monatlich abhängig von der benötigten Stückzahl vergütet werden. Die Hardware stellt das AFI in den eigenen Rechenzentren gestützt auf die Vergabe zur Backend-Infrastruktur bereit (RRB Nr. 492/2020).

Nach verschiedenen Vorarbeiten ist die Betriebsübernahme durch die Zuschlagsempfängerin im Verlaufe des Jahres 2021 für vier Jahre geplant. Der entsprechende Mittelbedarf ist in den Folgejahren nur teilweise gedeckt. Die in der Leistungsgruppe Nr. 4610, Amt für Informatik, eingestellten Mittel reichen für die Jahre 2020 (Budget 2020) und 2021 (Budgetentwurf 2021 und Konsolidierter Entwicklungs- und Finanzplan [KEF] 2021–2024). Für die weiteren Jahre wird das AFI im KEF 2022–2025 die zusätzlich benötigten Mittel einstellen.

	2020	2021	2022	2023	2024	2025
Mittelbedarf pro Jahr	25 000	740 000	910 000	1 000 000	1 300 000	820 000
Budget 2020; Budgetentwurf 2021 und KEF 2021–2024	40 000	745 000	445 000	445 000	445 000	
Abweichung (–Minderbedarf; +Mehrbedarf)	–15 000	–5 000	465 000	555 000	855 000	820 000

4. Gremien

Das Gremium Steuerung Digitale Verwaltung und IKT (SDI) hat den vorliegenden Antrag an seiner Sitzung vom 23. September 2020 zuhanden des Regierungsrates vorberaten und diesem zugestimmt.

Auf Antrag der Finanzdirektion

beschliesst der Regierungsrat:

I. Die «Managed Security Services für SOC» werden gemäss Angebot vom 10. Juli 2020 zu Fr. 4389518 an die ISPIN AG, Bassersdorf, vergeben. Die Vergabesumme kann sich für Unvorhergesehenes auf Fr. 4800000 erhöhen.

II. Für die «Managed Security Services für SOC» wird eine gebundene Ausgabe von Fr. 4800000 zulasten der Erfolgsrechnung der Leistungsgruppe Nr. 4610, Amt für Informatik, bewilligt.

III. Dieser Beschluss ist bis zur Veröffentlichung des Zuschlags auf simap.ch nicht öffentlich.

IV. Mitteilung an die Finanzdirektion.



Vor dem Regierungsrat
Die Staatsschreiberin:

Kathrin Arioli