Telefon: 233 - 76 77 77

IT-Referat

IT-Sicherheit bei der Landeshauptstadt München

Sitzungsvorlage Nr. 08-14 / V 16068

2 Anlagen
- Eckdatenblatt IT-Sicherheit
- Stellungnahmen

Beschluss des IT-Ausschusses vom 16.10.2019 (SB)

Öffentliche Sitzung

Inhaltsverzeichnis

I. Vortrag des Referenten

Zusammenfassung

Die Gewährleistung von IT-Sicherheit bei der Landeshauptstadt München ist eine Kernaufgabe der öffentlichen Verwaltung und unstrittige Voraussetzung für die Digitalisierung. Dies bedeutet, dass die Informationen bei der Verarbeitung und Speicherung in den IT-Systemen der LHM mit einem ausreichenden Schutzniveau versehen und gespeichert werden. Bei den Informationen handelt es sich z. B. um hochsensible personenbezogene Daten unserer Bürgerinnen und Bürger.

Um diese Anforderung zukünftig für die anstehenden Aufgaben wie z. B. die Digitalisierung gewährleisten zu können, muss die IT-Sicherheit der LHM konsequent geplant, gesteuert und kontrolliert werden. Die Neustrukturierung der IT-Sicherheit bei der LHM im Rahmen der Reorganisation der IT ist dafür eine erforderliche und im IT-Gutachten als wichtige Maßnahme

festgelegte Bedingung. In diesem Zusammenhang wird bei RIT-I eine neue Abteilung „IT-Sicherheitsmanagement“ geschaffen, bei it@M wird ein „Cyber Security Center“ aufgebaut.

In RIT-I sind zunächst 2 Vollzeitäquivalente (VZÄ) dauerhaft erforderlich. Sach- und Dienstleistungen werden zunächst im Umfang von 1,5 Mio. € benötigt.

1. Hintergrund

Die Relevanz der IT-Sicherheit für die LHM und insbesondere ihre Bedeutung für die Digitalisierung ist unumstritten. Dies unterstreichen nicht zuletzt die Aussagen des IT-Planungsrats, die in der "Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung" getroffen werden. Darüber hinaus ist die LHM durch das IT-Sicherheitsgesetz insbesondere auch mit ihren kritischen Infrastrukturen über die BSI-Kritisverordnung (BSI-KritisV) verpflichtet, entsprechende Standards in der IT-Sicherheit einzuhalten. Die MSE betreibt kritische Infrastrukturen und es wurde im 2. Quartal 2019 zwischen dem IT-Referent und der Werkleitung von MSE abgestimmt, dass die hierfür notwendige IT-Unterstützung bereit gestellt wird. Zusätzlich wird im Bayerischen E-Government-Gesetz (BayEGovG, Art. 11 Abs. 1) grundsätzlich gefordert, dass die IT-Sicherheit informationstechnischer Systeme sicherzustellen ist.

Diese gesetzlich verankerten Anforderungen verdeutlichen, dass die Gewährleistung von IT-Sicherheit in heutigen Zeiten eine der Kernaufgaben der öffentlichen Verwaltung darstellt. Bürgerinnen und Bürger, Unternehmen und weitere Partner erwarten zu Recht von der LHM, dass ihre Informationen bei der Verwaltung mit einem ausreichenden Schutzniveau verarbeitet und gespeichert werden.

Die LHM kann diese Anforderungen nur umsetzen, indem die IT-Sicherheit der LHM konsequent geplant, gesteuert und auch kontrolliert wird. Dies betrifft als Pflicht- sowie als Daueraufgabe sowohl den Bereich des (strategischen) IT-Sicherheitsmanagements wie auch die taktischen und operativen Aspekte der IT-Sicherheit.

Die Reorganisation der IT berücksichtigt dies bei der Umstrukturierung der IT-Sicherheit der LHM. In diesem Zusammenhang wird bei RIT-I eine neue Abteilung „IT-Sicherheitsmanagement“ (ISM) für das strategische IT-Sicherheitsmanagement der LHM geschaffen, bei it@M wird ein "Cyber Security Center" (CSC) aufgebaut für die taktischen und operativen Aspekte der IT-Sicherheit.

Der Abteilung werden neben den im RIT bereits bestehenden Aufgaben zur IT-Sicherheit, z. B. die IT-Sicherheitsstrategie oder das stadtweite Informationssicherheits-Managementsystem (ISMS), weitere Aufgaben zugeordnet. Im Zielbild werden neben dem stadtweiten IT-Sicherheitsmanagement ebenfalls das IT-Sicherheitsmanagement für das RIT sowie das IT-Sicherheitsmanagement von it@M in dieser Abteilung zusammengeführt.

Die Aufgaben des bei it@M aufzubauenden Cyber Security Centers sind im Vergleich etwas technischer ausgestaltet. Sie beziehen sich im Kern darauf, das IT-Sicherheitsniveau der LHM durch präventive Gefährdungsanalysen, konsistente IT-Sicherheitsarchitekturen sowie durch koordinierte Reaktionen auf eingetretene Schadwirkungen zu optimieren. Um diese Aufgaben im Rahmen des IT-Sicherheitsmanagements umzusetzen ist geplant, das CSC in Form der drei Bereiche IT-Sicherheitsarchitektur, Security Operation Center (SOC) und Offensive Security aufzubauen.

Die beantragten Mittel bilden die Grundlage für diese Reorganisation und damit für die Weiterentwicklung des IT-Sicherheitsmanagements der LHM sowie für die Etablierung des Cyber Security Centers bei it@M, in den nächsten Jahren sind dafür weitere Mittel erforderlich.

Aufgrund des Eckdatenbeschlusses der Stadtkämmerei vom 24.07.2019 wurde eine Reduzierung der vom IT-Referat geplanten Personalzuschaltungen auf 13 VZÄ vorgenommen. Diese Beschlussvorlage behandelt davon zwei Stellen.

2. Zielbild und Maßnahmen

Mit der Neustrukturierung der IT-Sicherheit (Aufgabenverteilung und -bündelung in ISM und CSC) werden insbesondere zwei wesentliche Zielsetzungen adressiert. Zum einen folgt dieser Ansatz notwendigerweise den aktuellen Reorganisationen in der IT (Gründung RIT, Leistungsschnitt, Programm neoIT). Er stellt sicher, dass die IT-Sicherheit auch in den neuen organisatorischen Strukturen und Prozessen in der IT in allen relevanten Bereichen und in effizienter Art und Weise verankert ist. Des Weiteren wird durch die Etablierung des CSC ein wesentliches Bindeglied geschaffen zwischen dem IT-Sicherheitsmanagement im RIT und dem operativen Betrieb von IT-Sicherheitstechnologien bei it@M.

Auf diese Weise wird eine einheitliche IT-Sicherheitsarchitektur realisiert, die eine kontinuierliche Prüfung und Entwicklung des IT-Sicherheitsniveaus (proaktiv) sowie ein konsistentes Management von IT-Sicherheitsvorfällen (reaktiv) ermöglicht. Beide Punkte stellen wesentliche Voraussetzungen dar, um die IT-Sicherheit in der LHM auch zukünftig gewährleisten zu können. Darüber hinaus bilden diese Aspekte die Grundlage dafür, wenn perspektivisch gesehen eine IT-Sicherheitszertifizierung von relevanten Teilbereichen von it@M angestrebt wird.

Um diese Zielsetzungen zu erreichen, sind neue Aufgabenstellungen anzugehen, sowohl im Hinblick auf den Aufbau des CSC wie auch in Bezug auf die Weiterentwicklung zentraler IT-Sicherheitsprozesse. Im Ergebnis werden die Grundlagen geschaffen, um gesetzlichen Anforderungen im Hinblick auf die IT-Sicherheit auch weiterhin erfüllen zu können sowie um die Einbindung der IT-Sicherheit in alle IT-Lösungen der LHM effizient und angemessen zu gestalten.

Vor diesem Hintergrund sollen im Jahr 2020 insbesondere die folgenden Themen im Bereich der IT-Sicherheit der LHM adressiert werden.

Verankerung des Risikomanagements IT-Sicherheit bei RIT-I

Das Management von Risiken stellt ein zentrales Paradigma im Rahmen des IT-Sicherheitsmanagements dar und ist ein wesentlicher Bestandteil der Entwicklung und des Lifecycles von IT-Services bei der LHM. Eine Risikoanalyse im Bereich IT-Sicherheit ist in jedem IT-Vorhaben der LHM verbindlich vorgeschrieben. Mit der Neuorganisation des IT-Sicherheitsmanagements soll der diesbezüglich etablierte IT-Sicherheitsprozess den gesetzlichen Vorgaben gemäß strukturiert werden und im Sinne der neuen Rolle der IT eine Zentralisierung im RIT erfahren. Auf diese Weise werden ebenfalls dringend notwendige Effizienzsteigerungen erzielt, die zum Beispiel auch dazu führen werden, die Durchlaufzeiten in der IT-Lösungsentwicklung zu verbessern.

Heute werden die entsprechenden Aufgabenbereiche der Rolle „Risikomanager IT-Sicherheit“ durch vier externe Mitarbeiter übernommen. Durch beauftragungsbedingte Wechsel dieses Personals kommt es unvermeidlich zu Know-how Abflüssen und Mehr-

aufwänden in Bezug auf das Anlernen neuen Personals. Es ist aus strategischer Sicht daher zielführend, Kapazitäten und entsprechendes Know-how für einen solchen elementaren Aufgabenbereich in der IT-Sicherheit intern aufzubauen. Weiterhin ist es notwendig, die entsprechenden Aufgaben an zentraler Stelle zu verankern, um Effizienzsteigerungen im Rahmen der stadtweiten Steuerung des „Risikomanagements IT-Sicherheit“ zu erzielen.

Um das Ziel, diese Kapazitäten intern aufzubauen, zu erreichen, sollen in 2020 zwei dauerhafte Stellen für „Risikomanager IT-Sicherheit“ bei RIT-I geschaffen werden.

Etablierung des Cyber Security Centers

Wie eingangs in Kapitel 1 beschrieben, sehen die Planungen vor, die Aufgabenbereiche des CSC in drei Segmente zu unterteilen.

Im Bereich „IT-Sicherheitsarchitektur“ werden Beratungs- und Konzeptionsleistungen zur IT-Sicherheitsarchitektur der LHM sowie die Entwicklung von fachlichen Roadmaps zum Einsatz von IT-Sicherheitstechnologien angesiedelt.

Der Bereich „Security Operation Center“ adressiert das operativ orientierte zentrale IT-Sicherheitsmonitoring, das sicherheitsrelevante Meldungen und Ereignisse aus der gesamten IT-Infrastruktur zentral aufnimmt und analysiert. Anhand dieser Analyseergebnisse werden dann standardisierte Verfahren zur Behandlung von IT-Sicherheitsvorfällen umgesetzt.

Im Rahmen des Bereichs „Offensive Security“ sind Aufgaben angesiedelt, die sich mit der proaktiven Erkennung von Schwachstellen in der IT-Infrastruktur der LHM, z. B. durch Penetration Tests, sowie mit deren Management befassen.

Für die Etablierung der skizzierten Aufgabenbereiche wird zum Start eine personelle Basisausstattung benötigt. Im CSC-Bereich IT-Sicherheitsarchitektur sind dies IT-Ingenieure IT-Sicherheit, im Bereich Security Operation Center IT-Sicherheitsanalysten sowie im Bereich Offensive Security IT-Ingenieure IT-Sicherheit.

Aus Sicht des RIT als Auftraggeber für die Etablierung des CSC ergibt sich für IT-Stellen und sonstige Aufwände zum Aufbau des CSC bei it@M ein Betrag in Höhe von 1,5 Mio. €.

Die Zeitspanne bis zu der Besetzung der Stellen muss durch externe Kapazitäten abgedeckt werden.

2.1. Personal

Bei RIT- HA-I, Abteilung 4 werden 2 VZÄ als „Risikomanager/-in IT-Sicherheit“ in der Einwertung E13 TVöD dauerhaft benötigt.

2.1.1. Bemessungsgrundlage

Die Stellenbemessung ist nach Vorgaben des POR für planerisch-konzeptionelle Aufgaben erfolgt, die entsprechenden Begründungen für die Bedarfe sind in den angehängten Eckdatenblättern dargestellt. Die Stellenbedarfe wurden vom RIT mit dem POR abgestimmt.

2.1.2. Flächenbedarf

Durch die beantragten Stellen wird Flächenbedarf für zwei Arbeitsplätze ausgelöst. Die Arbeitsplätze können aus Sicht des IT-Referats nur durch **vorübergehende** Nachverdichtung im Südgebäude des IT-Referats untergebracht werden. Zusätzlicher Büroraumbedarf wird daher beim Kommunalreferat angemeldet.

2.2. Feststellung der Wirtschaftlichkeit

Für die Digitalisierung ist eine funktionierende IT-Sicherheit bei der LHM eine unabdingbare Voraussetzung. Um die Informationssicherheit in der öffentlichen Verwaltung und deren gesetzliche Anforderungen (z. B. kritische Infrastrukturen oder Bayerisches E-Government-Gesetz) für die Informationstechnischen Systeme der LHM sicherzustellen, sind die umzusetzenden Maßnahmen unerlässlich.

Der Nutzen der IT-Sicherheit liegt in der Erfüllung der gesetzlichen Vorgaben (z. B. IT-Sicherheitsgesetz), ständiger Bereitstellung aktueller IT-Sicherheitsstandards zur Abwehr von Bedrohungen bzw. Beseitigung von eingetretenen Schadwirkungen und schafft somit die Voraussetzung für die Digitalisierung bei der LHM.

3. Sozialverträglichkeit

Der Gesamtpersonalrat wird über die Abstimmung der Beschlussvorlage mit einbezogen.

Zustimmung GPR liegt vor : ja ☒ nein ☐

4. Darstellung der Kosten und der Finanzierung

4.1. Zahlungswirksame Kosten im Bereich der laufenden Verwaltungstätigkeit

	dauerhaft	einmalig	befristet
Summe zahlungswirksame Kosten	1.665.370 € ab 2020	4.000 € in 2020	
davon:			
Personalauszahlungen (Zeile 9)*	163.770 € ab 2020		
Auszahlungen für Sach- und Dienstleistungen (Zeile 11)**	1.500.000 € ab 2020		
Transferauszahlungen (Zeile 12)			
Sonstige Auszahlungen aus lfd. Verwaltungstätigkeit (Zeile 13)	1.600 € ab 2020	4.000 € in 2020	
Zinsen und sonstige Finanzauszahlungen (Zeile 14)			
Nachrichtlich Vollzeitäquivalente	2		

Es werden zwei dauerhafte Stellen für die Rolle „Risikomanager/-in IT-Sicherheit im RIT benötigt.

Aus Sicht des RIT als Auftraggeber für die Etablierung des CSC ergibt sich für IT-Stellen bei it@M ein Betrag in Höhe von 1,5 Mio. €.

4.2. Finanzierung

Die Finanzierung kann weder durch Einsparungen noch aus dem eigenen Referatsbudget erfolgen.

Die Kosten weichen von den Festlegungen für das IT-Referat im Eckdatenbeschluss für den Haushalt 2020 ab, da sie gekürzt wurden. Die Kürzung repräsentiert in Verbindung mit der Mittelbeantragung der Beschlussvorlage zu diesem Thema und den Kürzungen der weiteren eingebrachten Beschlussvorlagen die beschlossene Obergrenze von 26,51 Mio. € (Hinweis: Eckdatenblatt siehe Nr. 13 der Liste der geplanten Beschlüsse des IT-Referats).

Die zusätzlich benötigten Auszahlungsmittel (Sachmittel und Personalmittel) werden genehmigt und in den Haushaltsplan 2020 aufgenommen.

4.3. Beteiligungen/ Stellungnahmen der Referate

Der Gesamtpersonalrat und die Stadtkämmerei haben der Beschlussvorlage zugestimmt.

Dem POR wurde die Beschlussvorlage fristgerecht zur Stellungnahme vorgelegt.

Anhörung des Bezirksausschusses

In dieser Beratungsangelegenheit ist die Anhörung des Bezirksausschusses nicht vorgesehen (vgl. Anlage 1 der BA-Satzung).

Korreferent und Verwaltungsbeirat

Der Korreferent des IT-Referats, Herr Stadtrat Progl, und die zuständige Verwaltungsbeirätin, Frau Stadträtin Hübner, haben einen Abdruck der Sitzungsvorlage erhalten.

II. Antrag des Referenten

1. Vom Vortrag des Referenten wird Kenntnis genommen.
2. Das IT-Referat wird beauftragt, die dauerhaft erforderlichen Haushaltsmittel zum Rechnungsausgleich an it@M i. H. v. 1.500.000 € beginnend in 2020 im Rahmen des der Haushaltsplanung bei der Stadtkämmerei, beim Produkt Zentrale IT (P42111220) anzumelden.
3. Das IT-Referat wird beauftragt, die dauerhafte Einrichtung von 2 VZÄ für zwei Risikomanager/-in IT-Sicherheit bei RIT-I ab 2020 sowie deren Besetzung beim Personal- und Organisationsreferat zu veranlassen.
4. Das IT-Referat wird beauftragt, die dauerhaft erforderlichen Haushaltsmittel in Höhe von jährlich bis zu 163.760 € entsprechend der tatsächlichen Besetzung der Stelle, im Rahmen der Haushaltsplanung für 2020 anzumelden.

   Im Ergebnishaushalt entsteht bei der Besetzung mit Beamten/-innen zusätzlich zu den Personalauszahlungen je Stelle noch ein Aufwand für Pensions- und Beihilferückstellungen in Höhe von etwa 52.304 € / Jahr (40 % des JMB).
5. Das IT-Referat wird beauftragt, die einmalig erforderlichen personalbezogenen Sachmittel i. H. v. 4.000 € für das Jahr 2020 sowie dauerhaft erforderliche personalbezogene Sachmittel i. H. v. 1.600 € im Rahmen der Haushaltsplanaufstellung bei der Stadtkämmerei, beim Produkt Zentrale IT (P42111220) ab 2020 anzumelden.
6. Das IT-Referat wird beauftragt, den unter Ziffer 2.1.2 des Vortrags dargestellten Flächenbedarf gegenüber dem Kommunalreferat anzumelden.
7. Der Beschluss unterliegt der Beschlussvollzugskontrolle

III. Beschluss

nach Antrag.

Der Stadtrat der Landeshauptstadt München

Der / Die Vorsitzende — Der Referent

Ober-/Bürgermeister/-in
ea. Stadtrat / ea. Stadträtin

Thomas Bönig
Berufsm. Stadtrat

IV. Abdruck von I. mit III.
über die Stadtratsprotokolle

an das Direktorium - Dokumentationsstelle
an die Stadtkämmerei
an das Revisionsamt

z. K.

V. Wv. -

1. Die Übereinstimmung vorstehenden Abdrucks mit der beglaubigten Zweitschrift wird bestätigt.

2. An

z. K.

Am