Telefon: 233 – 782423

IT-Referat

Für ein sicheres digitales München – Ausbau des Informationssicherheitsmanagements der LHM

IT-Sicherheit priorisieren
Antrag Nr. 20-26 / A 00730 von Frau StRin Sabine Bär, Herrn StR Thomas Schmid, Herrn StR Hans Hammer, Herrn StR Leo Agerer vom 24.11.2020, eingegangen am 24.11.2020

Sitzungsvorlage Nr. 20-26 / V 03022

1 Anlage

- Stadtratsantrag IT-Sicherheit priorisieren

Beschluss des IT-Ausschusses vom 22.09.2021 (VB)

Öffentliche Sitzung

Inhaltsverzeichnis

I. Vortrag des Referenten

Öffentliche und nichtöffentliche Vorlage

Diese Vorlage ist öffentlich. Zugehörige nichtöffentliche Informationen werden gemäß § 46 Abs. 3 Nr. 2 GeschO in nichtöffentlicher Sitzung zu behandeln, da sie die Grundlage für die Vergabe von Lieferung und Leistungen darstellen. Die nicht-öffentlichen Informationen zur Vorlage sind in der BV-Nr. 20-26 / V 03752 dargestellt.

Zusammenfassung

Die Gewährleistung der Informationssicherheit ist inzwischen eine Kernaufgabe der öffentlichen Verwaltung. Dies fordert nicht nur der Gesetzgeber ein. Es wird auch zu Recht von Bürger*innen sowie ansässigen Unternehmen und Partnerorganisationen Münchens, deren sensible Daten die LHM verarbeitet und speichert, erwartet. Mit zunehmender Digitalisierung müssen daher sichere und verlässliche Online-Services angeboten werden, um digitale Souveränität gewährleisten zu können.

Die LHM hat die Verpflichtung, sich im Bereich der Informationssicherheit in gleicher Weise weiter zu entwickeln, wie es auch der Bereich der Cyberkriminalität tut. Das IT-Sicherheitsniveau der LHM muss durch den Aufbau von Kompetenzen und den Einsatz intelligenter Technologien kontinuierlich gesteigert werden, um als Organisation in der Lage sein zu können, der stetig wachsenden Gefährdungslage im Cyberraum adäquat zu begegnen.

Vor diesem Hintergrund werden in der vorliegenden Beschlussvorlage wesentliche Handlungsschwerpunkte dargestellt, deren Entwicklungen im Rahmen des Informationsmanagements zeitnah notwendig sind. Gegliedert nach den Sicherheitsdisziplinen Prävention, Detektion, Reaktion und Adaption werden die folgenden Schwerpunkte thematisiert:

- Sichere Authentisierung und digitale Prozesse
- Risikomanagement IT-Sicherheit
- IT-Sicherheitsarchitektur und Offensive Security
- Security Orchestration Automation and Response (SOAR)
- Endpoint Protection
- ISM Governance
- Cloud Security Management

In der Gesamtheit bilden diese Themen die inhaltlichen Eckpfeiler für das im Stadtratsantrag angesprochene Umsetzungskonzept im Bereich der Informationssicherheit.

Die Sachmittelbedarfe, die durch die Weiterentwicklung der IT-Sicherheit entstehen werden, sind in der nicht-öffentlichen Vorlage angegeben.

Die zusätzlichen Personalmittelbedarfe für 7 VZÄ liegen bei etwa 640.000 € laufend und werden in der öffentlichen Vorlage dargestellt..

1. Ausgangslage im Bereich der Informationssicherheit

In der heutigen Zeit ist die Gewährleistung der Informationssicherheit eine Kernaufgabe der öffentlichen Verwaltung.

Diese Aussage ist auf den ersten Blick einfach nachvollziehbar im Jahr 2021, in dem die Digitalisierung zurecht eine der zentralen Zielsetzungen in der Verwaltung darstellt. Es ist

jedoch nicht so, dass Informationssicherheit lediglich wegen oder im Verlauf der greifenden Digitalisierung an Bedeutung zunimmt. Informationssicherheit stellt vielmehr eine der Voraussetzungen dafür dar, dass eine erfolgreiche Digitalisierung überhaupt erfolgen kann. Denn nur wenn Informationen sicher erfasst, verarbeitet und übertragen werden, können bei der LHM verlässliche digitale Services für Bürger*innen Stadtgesellschaft, Unternehmen und Partnerorganisationen angeboten werden. Diese grundlegende Position wird durch den Gesetzgeber eingefordert und durch die Informationssicherheitsleitlinie der LHM dokumentiert.

Den erstgenannten Aspekt unterstreichen die Aussagen des IT-Planungsrats des Bundes und der Länder, die in der "Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung" getroffen werden. Darüber hinaus ist die LHM als Betreiber digitaler Dienste sowie im Speziellen mit ihren kritischen Infrastrukturen über das BSI-Gesetz (BSIG) verpflichtet, entsprechende Standards in der IT-Sicherheit einzuhalten. Zusätzlich wird im Bayerischen E-Government-Gesetz (BayEGovG, Art. 11 Abs. 1) grundsätzlich gefordert, dass die IT-Sicherheit informationstechnischer Systeme sicherzustellen ist. Und schließlich werden auch im Rahmen der Datenschutzgrundverordnung (DSGVO) hohe Anforderungen an die Sicherheitsmaßnahmen in unserer Organisation gestellt.

Perspektivisch ist hierbei davon auszugehen, dass die Anforderungen von Seiten des Gesetzgebers auf Grund der steigenden Bedrohungslage sukzessive ausgeweitet werden. Zum Zeitpunkt der Beschlusserstellung befindet sich z. B. das IT-Sicherheitsgesetz 2.0 in den finalen Phasen der Fortschreibung. Und auch das Bundesamt für Sicherheit in der Informationstechnik dokumentiert in seinem „Bericht zur Lage der IT-Sicherheit 2020“ eine neue Qualität an Cyber-Angriffen und prognostiziert eine deutliche Steigerung der resultierenden Gefährdungssituation.

Diese Entwicklungen im Bereich der Cyberkriminalität stellen eine sehr reale Verschärfung der Gefährdungslage für die LHM dar. Über 500 sicherheitsrelevante Vorgänge, die im Jahr 2020 durch das Informationssicherheitsmanagement der LHM aktiv behandelt wurden, sowie ein massiver IT-Sicherheitsvorfall im Stadtkonzern zeigen eindringlich, dass die LHM bereits ein veritables Ziel für Cyberkriminelle darstellt.

Und auch im nationalen Umfeld waren nicht nur in der Wirtschaft, sondern auch bei öffentlichen Institutionen in anderen Städten, wie z. B. in Frankfurt, Gießen oder aktuell im April diesen Jahres auch bei der TU Berlin, größere IT-Sicherheitsvorfälle mit finanziellen Schäden, teils im Millionenbereich, beobachtbar. Für die LHM geht es hierbei jedoch nicht nur um die wirtschaftlichen Folgeschäden eines solchen Vorfalls, sondern auch um die Positionierung und Außenwirkung der Verwaltung als verlässlicher Partner in einer zunehmend digitalen Welt.

Die LHM muss daher handeln und sich im Bereich der Informationssicherheit in gleicher Weise weiterentwickeln, wie es auch die Gegenseite tut. Daher ist es unerlässlich, technologisch wie auch organisatorisch Schritt zu halten, Informationssicherheit in unserer Infrastruktur wie auch unseren Prozessen fundiert zu verankern und das IT-Sicherheitsniveau der LHM durch den Aufbau von Kompetenzen und den Einsatz intelligenter Technologien kontinuierlich zu steigern.

Denn nur auf diese Weise kann die LHM der stetig wachsenden Gefährdungslage im Cyberraum adäquat begegnen. Und nur so kann die Verwaltung verlässliche Online-Services anbieten, um von den Chancen der Digitalisierung zu profitieren und gleichzeitig die digitale Souveränität der LHM zu wahren.

2. Aktueller Status zur Umsetzungskonzeption Informationssicherheit

Vor dem Hintergrund der skizzierten Ausgangssituation wurde mit der Gründung des IT-Referats auch der Bereich der Informationssicherheit neu strukturiert und auf die eingangs beschriebenen Herausforderungen ausgerichtet. Durch den im RIT zusammengeführten Bereich des Informationssicherheitsmanagements (ISM) sowie das im Aufbau befindliche Cyber Security Center bei it@M (CSC) wurden in 2020 wichtige Themenbereiche der Informationssicherheit adressiert, IT-Sicherheitsprozesse entwickelt und neue IT-Sicherheitstechnologien zum Einsatz gebracht.

Durch die pandemiebedingten Haushaltseinschnitte in 2021 konnten diese Entwicklungen jedoch nicht wie fachlich notwendig weiterverfolgt werden. In der Konsequenz können in 2021 laufende Initiativen zwar fortgeführt und in dedizierten Bereichen auch punktuelle Verbesserungen erzielt werden, die notwendige Steigerung des IT-Sicherheitsniveaus der LHM ist auf dieser Grundlage in 2021 jedoch nicht möglich.

Die notwendigen Entwicklungen müssen somit in 2022 wieder aufgegriffen werden und dabei in die bestehende Informationssicherheitsstrategie der LHM integriert werden. Diese Strategie bildet den langfristigen Rahmen für das Informationssicherheitsmanagement bei der LHM und legt spezifische Zielsetzungen in relevanten Themen wie der Prävention, Detektion und Reaktion im Sicherheitsbereich (vgl. Kapitel 3) fest. Entwickelt und verfolgt wird diese Strategie durch die oben genannten Einheiten im RIT (ISM) sowie bei it@M (CSC), die auch dafür Sorge tragen, dass die Informationssicherheitsstrategie die konkreten Anwendungsszenarien und Zielsetzungen der LHM, z. B. in den Bereichen der Digitalisierung oder mobiler Arbeitsplatzkonzepte, im Blick hält und aktiv unterstützt.

Das im Antrag geforderte Umsetzungskonzept zur IT-Sicherheit stellt in diesem Zusammenhang konkrete IT-Sicherheitsmaßnahmen in den Mittelpunkt, die in die bestehende Strategie integriert bzw. im Hinblick auf ihre Umsetzbarkeit im nächsten Jahr konzipiert und geprüft werden müssen. Hierbei geht es nicht nur um den Einsatz neuer, intelligenter Technologien, sondern ebenfalls um organisatorische Entwicklungen, die stattfinden müssen, um die Schutzwirkung etablierter IT-Sicherheitsmechanismen zu maximieren. Es bestehen somit Abhängigkeiten eines solchen Umsetzungskonzepts zu Entwicklungen in der IT-Infrastruktur selbst bzw. der IT- sowie Informationssicherheitsorganisation.

In den folgenden Abschnitten werden die wesentlichen inhaltlichen Eckpunkte eines solchen Umsetzungskonzepts im Einklang mit der Informationssicherheitsstrategie der LHM dargestellt.

3. Handlungsschwerpunkte in der Entwicklung der Informationssicherheit

Informationssicherheit gliedert sich aus fachlicher Sicht bei der LHM in vier logische Segmente und wird über diese Einteilung durch das ISM auch gesteuert. Die Kernaufgaben der Informationssicherheit lassen sich dabei in die drei zentralen Bereiche „Prävention“, „Detektion“ und „Reaktion“ unterteilen. Querschnittlich hierzu liegt der Bereich der „Adaption“, der für eine kontinuierliche Anpassung in den drei Kernbereichen Sorge trägt.

Unter Prävention werden alle Maßnahmen subsumiert, die dazu dienen, einen Schaden an den von der LHM verarbeiteten Informationen zu verhindern. Ein Beispiel hierfür ist etwa die Härtung unserer IT-Systeme oder die Durchführung von Penetrationstests, um etwa die Vertraulichkeit der verarbeiteten Informationen sicherzustellen.

Im Bereich Detektion sind alle Maßnahmen positioniert, die für die Erkennung von sicherheitsrelevanten Ereignissen und Vorfällen notwendig sind. Hierzu gehören zum Beispiel

Malwareschutz-Komponenten, die einen Befall von Schadsoftware auf IT-Systemen erkennen können.

Unter Reaktion fallen alle Maßnahmen, um zeitnah und angemessen auf IT-Sicherheitsereignisse und -vorfälle zu reagieren. Hierzu gehören Tätigkeiten wie die Analyse der Gefährdungslage, Schwachstellenmanagement und die sofortige – automatisierte – Einleitung notwendiger Gegenmaßnahmen.

Unter Adaption wird schließlich die Steuerung aller Aktivitäten zusammengefasst, die in der gesamten IT-Organisation sowie in den drei genannten Kernbereichen notwendig sind, um das Sicherheitsniveau der LHM kontinuierlich zu verbessern. Diese Aktivitäten beziehen sich in der Regel sowohl auf Technologien und Prozesse, wie auch auf organisatorische Aspekte und relevante Regularien im Bereich der Informationssicherheit.

Die nachfolgenden Abschnitte stellen die Handlungsschwerpunkte für 2022 anhand der vier Bereiche im Überblick dar.

Für jedes Handlungsfeld, in dem Personalbedarfe im Hoheitsbereich entstehen, werden diese am Ende des jeweiligen Abschnitts ausgewiesen. Die zugehörigen Sachmittel sind in der nichtöffentlichen Vorlage gemäß den gleichen Handlungsfeldern aufgeschlüsselt.

3.1. Prävention

Sichere Authentisierung und digitale Prozesse

Die Grundlage und auch Voraussetzung für sicheres und flexibles Arbeiten (z. B. im Homeoffice) und damit für die Sicherung des Dienstgeschäfts ist die Feststellung, wer der bzw. die Nutzer*in eines Dienstes (z. B. IKM) eigentlich ist. Dieser Schritt im Rahmen der Authentisierung und die anschließende Berechtigung für den Zugriff ist jedoch nicht nur für die Anmeldung an einem IT-Arbeitsplatz, Betriebssystem oder Online-Dienst wichtig. Zusammen mit kryptografischen Verfahren und weiteren Technologien bildet er auch die Basis für den Einsatz digitaler Signaturen oder elektronischer Siegel, die wiederum notwendig sind für die Implementierung von digitalen Prozessen z. B. im Rechnungswesen oder im Kontext der E-Akte. Zielsetzung aus Sicht des Informationssicherheitsmanagements ist es hier, die technisch einheitlichen Voraussetzungen und Security-Services bei der LHM zu schaffen, um sicheres mobiles Arbeiten und eine sichere Automatisierung von Workflows und Prozessen zu ermöglichen.

In einem ersten Schritt geht es in 2022 in diesem Bereich darum, jeder bzw. jedem Mitarbeitenden die Möglichkeit zur sicheren Authentisierung über einen starken zweiten Faktor (Token) zu geben. Die strategische Plattform der LHM in diesem Bereich ist der Einsatz sogenannter Yubi-Keys (FIDO2-Standard), für die die oben skizzierten Anwendungsfälle auszugestalten sind.

Risikomanagement IT-Sicherheit (ISM)

Das Risikomanagement in der IT-Sicherheit ist bereits heute ein wesentlicher Bestandteil der Entwicklung und des Lifecycles von sicheren IT-Services bei der LHM. Eine Risikoanalyse im Bereich IT-Sicherheit ist in jedem IT-Projekt der LHM verbindlich vorgeschrieben und folgt standardisierten Vorgehensweisen und Methoden. Die Weiterentwicklung und Durchführung dieses zentralen Informationssicherheitsprozesses stellt eine der wesentlichen Aufgabenstellungen des ISM im Kontext der Prävention dar.

In der aktuellen Situation werden die entsprechenden Aufgabenbereiche im Risikomanagement im Wesentlichen durch externe Mitarbeiter*innen übernommen. Durch beauftragungsbedingte Wechsel dieses Personals kommt es unvermeidlich zu Know-how Abflüssen und Mehraufwänden in Bezug auf das Anlernen neuen Personals. Weiterhin sind die verfügbaren Kapazitäten bereits heute nicht mehr ausreichend, um alle erforderlichen Risikoanalysen in ausreichender Qualität und auch Geschwindigkeit durchzuführen. Im Kontext der steigenden Digitalisierung ist davon auszugehen, dass die aktuellen Fallzahlen in Zukunft noch deutlich ansteigen werden.

In diesem Bereich ist es daher notwendig, die bestehenden Kapazitäten aufzustocken und vor allem die entsprechenden Kompetenzen intern aufzubauen. Weiterhin ist die Etablierung einer zentralen Softwareplattform notwendig, um die Durchführungen und auch Ergebnisse der zahlreichen Risikoanalysen pro Jahr integrieren zu können.

➔ **In diesem Handlungsfeld sind 5 VZÄ erforderlich.**

IT-Sicherheitsarchitektur und Offensive Security (CSC)

Im Rahmen des Informationssicherheitsmanagements im IT-Referat soll das CSC zur zentralen Steuerungseinheit für die Informationssicherheit bei it@M entwickelt werden. Im Kontext der Prävention sind hierbei insbesondere in den beiden CSC-Bereichen „IT-Sicherheitsarchitektur“ und „Offensive Security“ Entwicklungen notwendig.

Unter der IT-Sicherheitsarchitektur der LHM werden alle Technologien verstanden, die zur Gewährleistung des Sicherheitsniveaus der von der LHM verarbeiteten Information beitragen. Beispiele solcher Technologiebereiche sind etwa der Malwareschutz auf Endgeräten, Filtertechnologien auf Netzwerkebene (Firewall) oder auch der Einsatz von sicheren zweiten Faktoren zur Authentisierung von Nutzer*innen im Homeoffice.

Diese Sicherheitstechnologien erfüllen unterschiedliche Funktionen, müssen mit der IT-Architektur eng verzahnt sein und ineinander greifen, um eine umfassende Schutzfunktion realisieren zu können. Die IT-Sicherheitsarchitektur muss daher strukturiert geplant sowie ihr Ausbau strategisch konzipiert und gesteuert werden. Hierzu müssen Kompetenzen aufgebaut werden, um fachlichen Roadmaps zum Einsatz von IT-Sicherheitstechnologien entwickeln sowie Beratungs- und Konzeptionsleistungen zur IT-Sicherheitsarchitektur der LHM erbringen zu können.

Im Bereich der Offensive Security geht es aus fachlicher Sicht darum, durch (interne) Sicherheitsüberprüfungen proaktiv und koordiniert existierende Schwachstellen in der IT-Infrastruktur der LHM aufzudecken und zu beheben. Eine Tätigkeit in diesem Bereich ist das sogenannte „Penetration Testing“ (Pentesting), bei dem es um die gezielte Sicherheitsüberprüfung von einzelnen IT-Services geht. In diesem Zusammenhang ist es notwendig, dass die vorhandenen Kapazitäten für die Beauftragung externer Pentests gesteigert werden, um relevante Online-Services der LHM vor Produktivsetzung ausreichenden Sicherheitsüberprüfungen unterziehen zu können.

3.2. Detektion und Reaktion

Security Orchestration Automation and Response (SOAR)

Die Erkennungsmöglichkeiten von sicherheitsrelevanten Ereignissen sowie die Geschwindigkeit in der Reaktion durch die IT-Sicherheitsorganisation der LHM sind zentrale Er-

folgsfaktoren, wenn es um die erfolgreiche Behandlung von IT-Security Events und IT-Security Incidents geht.

Im Zielbild sollen im Security Operations Center (SOC) des CSC alle sicherheitsrelevanten Ereignisse in der städtischen IT-Infrastruktur mittels technischer Sensoren und Logdaten detektiert und analysiert werden. Diese Daten müssen um Informationen aus externen Quellen zu Sicherheitsbedrohungen angereichert werden, z. B. von Herstellern, EU-CERT oder auch aus Quellen der bundesweiten IT-Sicherheitsarchitektur des Landesamts für Sicherheit in der Informationstechnik (LSI) und des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Auf der Grundlage einer solchen Anbindung an nationale und internationale IT-Sicherheitsstrukturen können dann Technologien und Verfahren der sog. „Security Orchestration Automation and Response“ (SOAR) etabliert werden. Bei SOAR geht es darum, durch den Einsatz intelligenter Technologien (KI) eine maschinell unterstütze Reaktionsmöglichkeit auf sicherheitsrelevante Ereignisse und Sicherheitsvorfälle zu schaffen, um die Behandlung von Vorfällen standardisierbar, priorisierbar und vor allem automatisierbar zu machen. Ziel ist es, die Effizienz aller Sicherheitsoperationen zu verbessern, um möglichst schnell und automatisch auf eine veränderte Sicherheitslage reagieren zu können.

Um diese Zielsetzungen umsetzen zu können, müssen im SOC sowohl Kompetenzen als auch Technologien stark erweitert werden. Im Zielbild ist hier eine zentrale SOAR-Plattform zu etablieren, über die an zentraler Stelle die Ergebnisse des sicherheitsrelevanten Monitorings stadtweit gesammelt werden und notwendige Reaktionen automatisiert veranlasst werden können.

Endpoint Protection

Die Sicherheit unserer Endgeräte ist ein zentraler Faktor für das IT-Sicherheitsniveau der LHM. Hierbei geht es zum einen um den Schutz vor Schadsoftware, es geht aber auch um die sichere lokale Verarbeitung und Speicherung von Daten, wenn die Endgeräte ohne Zugriff auf das Verwaltungsnetz genutzt werden. Weiterhin muss eine deutlich bessere Steuerbarkeit der Geräte aus IT-Sicherheitsperspektive erreicht werden, z. B. wenn die Abschaltung bestimmter Funktionen oder auch eine Isolation des Endgeräts im Kontext eines IT-Sicherheitsvorfalls notwendig wird.

In diesem Zusammenhang sind entsprechende Projekte im Kontext der sog. „Endpoint Detection & Response“ (EDR) notwendig. Durch EDR wird die Möglichkeit geschaffen, kontinuierlich sicherheitsrelevante Endpunktdaten zu erfassen und zu analysieren, um auf Grundlage von Bedrohungsmustern automatisierte Reaktionen auf kritische Sicherheitszustände am Endpunkt veranlassen zu können. Die hierzu notwendigen Technologien sind dabei sowohl auf dem Endpunkt zu etablieren wie auch in der oben skizzierten SOAR-Plattform zu integrieren.

3.3. Adaption

ISM Governance

Die frühzeitige Verankerung der Informationssicherheit im Rahmen von relevanten Entwicklungen im IT-Bereich ist ein wichtiger Faktor. Beispiele hierfür sind strategische Themen wie die Digitalisierung als Megatrend, IT-Sourcing durch die Nutzung von Cloud Services, Ansätze im Bereich New Work oder auch aktuelle Bestrebungen zum verstärkten

Einsatz von Open Source in der Verwaltung. Alle diese Themenbereiche haben Auswirkungen auf oder Anforderungen an die Informationssicherheit bzw. werden von ihr wiederum beeinflusst.

In diesem Zusammenhang geht es für das ISM auf der einen Seite darum, die Belange der Informationssicherheit frühzeitig in die entsprechenden Entscheidungsprozesse zu diesen Themen einzubringen. Auf der anderen Seite geht es dann aber auch darum, die resultierenden Positionen und Ansätze in die IT- und Informationssicherheitsorganisation zu integrieren. Der letztgenannte Aspekt bezieht sich somit auch darauf, die Informationssicherheit bei den Mitarbeitenden in der IT in der täglichen Arbeit so zu verankern, dass die festgelegten Positionen unterstützt und das angestrebte IT-Sicherheitsniveau erreicht werden kann.

Ein Beispiel hierfür sind etwa die getroffenen Festlegungen zum Umgang mit Cloud Services. Hierbei muss aus IT-Sicherheitssicht eine Prüfung des Cloud Providers erfolgen sowie eine Prüfung des Cloud Services an sich. Beide Prüfschritte müssen inhaltlich ausgestaltet werden sowie in den IT- und auch Vergabeprozessen so platziert werden, dass sie bei allen Aktivitäten in diesem Bereich in der Organisation gelebt werden können.

Für diese steuernden Aktivitäten, die im Ergebnis dafür sorgen, dass relevante Entwicklungen in der IT bestmöglich durch die Informationssicherheit unterstützt werden, sind im ISM der LHM zusätzlich Kompetenzen notwendig.

➔ In diesem Handlungsfeld ist 1 VZÄ erforderlich.

Cloud Security Management

Cloud Computing ist in unterschiedlichsten Varianten, Servicemodellen und Bereitstellungsformen verfügbar und ist auch in Zukunft im IT-Serviceportfolio der LHM nicht mehr wegzudenken. Aus Informationssicherheitssicht ist es notwendig, die Verlässlichkeit von Cloud Anbietern zu verifizieren, die Security Events in der Cloud in unsere lokalen Verfahren einzubinden, unsere Nutzer*innen sicher an den Cloud-Diensten zu authentisieren und jederzeit die Hoheit über unsere Daten zu behalten (Digitale Souveränität). Gleichermaßen muss der Aufbau und Betrieb von hybriden Cloud-Systemen, d. h. einer Mischform von Systemen aus der eigenen Infrastruktur (München Cloud) sowie von Systemen kommerzieller Cloud-Anbieter, sicherheitstechnisch steuerbar sein.

Dieser perspektivisch wichtige Bereich wird zum aktuellen Zeitpunkt im Rahmen der bestehenden Verfahren und Ansätze im Rahmen des Informationssicherheitsmanagements adressiert. Auf Grund der strategischen Bedeutung des Themas für die Verwaltung, muss das Thema Cloud Security jedoch in einem eigenständigen Aufgabenfeld im ISM verankert werden. Hierfür ist ein entsprechender Kompetenzaufbau im ISM notwendig.

➔ In diesem Handlungsfeld ist 1 VZÄ erforderlich.

4. Umsetzung des Antrags

4.1. Entscheidungsvorschlag

Die dringend erforderlichen Investitionen im Bereich der Sachmittel (nicht-öffentliche Vorlage) und im Bereich der Personalmittel (hier in der öffentlichen Vorlage) werden genehmigt, um die IT-Sicherheit in den angegebenen Handlungsfeldern analog zur wachsenden Bedrohungslage weiter entwickeln zu können.

4.2. Personalbedarfe

Folgende Stellenbedarfe sollen mittels einer Stellenneuschaffung und einer Bereitstellung von zusätzlichem Personalbudget umgesetzt werden. Hierfür ist eine Ausnahme vom stadtweiten Besetzungsstopp erforderlich. Die Dringlichkeit ergibt sich aus der unten angegeben Darstellung zur Unabweisbarkeit.

Die Stellenschaffungen wurden bereits seit mehreren Jahre eingeplant aber ebenso in jedem Jahr zurückgestellt mit Rücksicht auf die Haushaltslage. Die Schaffung der fünf Stellen im Bereich des Risikomanagements ist zudem wirtschaftlich, da die Aufgaben aktuell von externen Dienstleistern wahrgenommen werden.

Aufgrund der aktuellen Arbeitsmarktlage im Bereich der IT-Security ist davon auszugehen, dass nur eine schrittweise Stellenbesetzung möglich ist. Mit jeder erfolgten Stellenbesetzung im Bereich Risikomanagment kann ein Ausgleich über entfallende Sachkosten für die entsprechenden externen Dienstleistung, die heute zu dem Zweck eingesetzt werden, der Höhe und dem Zeitpunkt nach mit der SKA abgestimmt werden. Eine Darstellung, wann diese Nutzeneffekte eintreten, ist im Rahmen dieser Beschlussvorlage nicht möglich, da bei der Marktlage in Bezug auf IT-Security-Spezialist*innen nicht kalkulierbar ist, wann die entsprechenden Stellen besetzt werden können und damit, wann die externen Dienstleitungen entfallen können, und bisher eine Gegenrechnung von Personalmitteln und Sachmitteln nicht in der Haushaltssystematik vorgesehen ist.
Das IT-Referat schlägt vor, die freiwerdenden Mittel ab dem Zeitpunkt der jeweiligen Stellenbesetzung dem POR und der SKA zu melden.

Funktionsbezeichnung	Anzahl in VZÄ	Einwertung	JMB	Benötigt ab	Aufgaben
Risikomanagment	5 VZÄ	E13, Stufe 4	444.750 €	01.01.2022	Durchführung von Risikoanalysen (stadtweit ca. 250 / Jahr)
Cloud Security Management	1 VZÄ	E13, Stufe 4	88.950 €	01.01.2022	Durchführung von Risikoanalysen im Cloud-Umfeld, strategischer Aufbau der Managementdisziplin i. R. Des ISM (neue Aufgabe)
ISM Governance	1 VZÄ	E14, Stufe 5	101.670 €	01.01.2022	Konzeption und Etablierung der gesamtstädtischen Security-Governance als eigener Aufgabenbereich im ISM. Insbesondere relevant im Hinblick auf die Zentralisierungsansätze in der IT der LHM (BV Doppelstrukturen vermeiden)

Durch die beantragten Stellen wird kein zusätzlicher Flächenbedarf ausgelöst. Die Arbeitsplätze können aus Sicht des IT-Referats durch Nachverdichtung im Südgebäude des IT-Referats untergebracht werden. Der zusätzliche Büroraumbedarf wird beim Kommunalreferat nicht angemeldet.

4.3. Personalmittelbedarfe

	dauerhaft	einmalig	befristet
Vollkosten Planung und Erstellung			
Davon Personalvollkosten			
Summe Stellenschaffungen	∑ 635.370 €		
im RIT-I-A4 (5 VZÄ)	444.750 € ab 2022		
im RIT-I-A4 (1 VZÄ)	88.950 € ab 2022		
im RIT-I-A4 (1 VZÄ)	101.670 € ab 2022		
Davon Sachvollkosten siehe nichtöffentliche vorlage			
Nachrichtlich Vollzeitäquivalente	7	-	-

Sachmittelbedarfe werden in der nicht-öffentlichen Vorlage dargestellt.

Zusammenfassung

Mit den dargestellten Finanzierungen aus dem öffentlichen und dem nicht-öffentlichen Teil können im Jahr 2022 die Grundlagen geschaffen werden, um durch weiterführende Sicherheitsprojekte in 2023 die Fähigkeiten der LHM in den vier Sicherheitssegmenten Prävention, Detektion, Reaktion und Adaption weiter auszubauen. Auf diese Weise können die dringend notwendigen Entwicklungen im Bereich des Informationssicherheitsmanagements der LHM auf den Weg gebracht werden.

5. Darstellung der Kosten und der Finanzierung

5.1. Zahlungswirksame Kosten im Bereich der laufenden Verwaltungstätigkeit

	dauerhaft	einmalig	befristet
Summe zahlungswirksame Kosten	635.370 € ab 2022		
davon:			
Personalauszahlungen (Zeile 9)*	635.370 € ab 2022		
Auszahlungen für Sach- und Dienstleistungen (Zeile 11)**			
Transferauszahlungen (Zeile 12)			
Sonstige Auszahlungen aus lfd. Verwaltungstätigkeit (Zeile 13)			
Zinsen und sonstige Finanzauszahlungen (Zeile 14)			
Nachrichtlich Vollzeitäquivalente	7		

5.2. Unabweisbarkeit

Die Weiterentwicklung der ISM-Organisation ist unabweisbar.

Wie bereits in Kapitel 1 dargestellt ist die Gewährleistung der Informationssicherheit auch aus gesetzlicher Perspektive eine Pflichtaufgabe für die LHM (IT-Sicherheitsgesetz, KRITIS, Bayerisches E-Government-Gesetz). Ohne die Umsetzung der Planungen in den skizzierten Handlungsfelder wird die LHM diesen gesetzlichen Anforderungen nicht gerecht. Die hierzu notwendigen fachlichen Aufgaben unterliegen einer hohen Dynamik, die durch die stetig steigende und sich stetig verändernde Bedrohungslage im Cyberraum bedingt ist.

Insbesondere im Bereich der Cloud-Security entstehen zudem neue Aufgaben, die wahrgenommen werden müssen, um die digitale Souveränität der Landeshauptstadt sicher zu stellen. Weitere fachliche Zukunftsbereiche wie z. B. mobiles Arbeiten, E-Akte und andere Effekte der zunehmenden Digitalisierung der Verwaltung erfordern alle ein angemessenes IT-Sicherheitsniveau, das kontinuierlich in immer neuen sicherheitsrelevanten Themenfeldern entwickelt werden muss.

5.3. Finanzierung

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

Die Inhalte dieser Beschlussvorlage sind konsistent mit den Mittelbedarfen des zur IT-Sicherheit gehörende Eckdatenblatts (ISM). Lediglich wurden Projektaufwände von 2022 nach 2023 verschoben.

Das Eckdatenblatt beinhaltet für die IT-Sicherheit 231.000 € Personalkosten pauschaliert kalkuliert nach den Vorgaben des POR plus 19.600 € personenbezogene Sachkosten. Die Angaben in 2022 berücksichtigen in Verbindung mit der Mittelbeantragung der Beschlussvorlage für 2022, 2023 und ff. das Gebot, im Hinblick auf die Haushaltslage nur die unbedingt erforderlichen Mittelbedarfe (Hinweis: Eckdatenblatt siehe Nr. 3 der Liste der geplanten Beschlüsse des IT-Referats).

Die zusätzlich benötigten Auszahlungsmittel (Sachmittel und Personalmittel) werden genehmigt und in den Haushaltsplan 2022 ff. aufgenommen.

6. Beteiligungen

Die Beschlussvorlage wurde mit gleichem Inhalt bis auf die Stellenschaffungen bereits mit dem Direktorium, der Stadtkämmerei und dem Gesamtpersonalrat abgestimmt.

Die Erweiterung der Beschlussvorlage um Personalkosten und Sachkosten wurde zusätzlich mit dem POR und erneut mit der SKA abgestimmt.

Das Direktorium und der Gesamtpersonalrat stimmen der Beschlussvorlage zu. Die Stadtkämmerei und das Personal- und Organisationsreferat lehnen die Beschlussvorlage ab.

REF/ PR	Excerpt aus Stellungnahme	Antwort / Kommentar
DIR	Das Direktorium möchte jedoch, zusätzlich zu den in der Beschlussvorlage genannten Textpassagen, explizit auf die enge Verbindung von Informationssicherheit und Datenschutz hinweisen, insbesondere nach Art. 5, 24, 25 und 32 DSGVO.	Das IT-Referat bedankt sich für die Mitzeichnung und bestätigt die enge Verbindung der Themen Datenschutz und Informationssicherheit.
GPR	Der Gesamtpersonalrat unterstützt ausdrücklich die vorgeschlagene Vorgehensweise. In der heutigen Zeit ist (...) die Gewährleistung der Informationssicherheit eine Kernaufgabe der öffentlichen Verwaltung. Nur durch den gezielten Aufbau eigener Kompetenzen und den Einsatz intelligenter Technologien können wir den wachsenden Anforderungen adäquat begegnen. Ungeachtet der derzeitigen Haushaltslage müssen eingeschlagene Entwicklungen gesichert und konsequent weiterverfolgt werden. Eine kontinuierliche Bereitstellung ausreichender Mittel ist notwendiger Garant für ein gleichbleibend hohes IT-Sicherheitsniveau und Grundlage einer erfolgreichen Digitalisierung. Hier darf nicht am falschen Ende gespart werden! Unsere Daten sind ein wertvolles Gut. Bei deren Schutz dürfen wir die Zügel nicht aus der Hand geben! Genau das liegt auch im Interesse unserer Beschäftigten.	Das IT-Referat bedankt sich für die Unterstützung durch den Gesamtpersonalrat.
POR	Für den Haushalt 2021 und voraussichtlich für künftige Jahre besteht aus Sicht des Personal- und Organisationsreferates aufgrund der angespannten Haushaltslage daher kein Spielraum für weitere Ausweitungen.	Das IT-Referat erkennt die schwierige Haushaltslage an, sieht aber aufgrund der sich verschärfenden Bedrohungslage keine andere Wahl, als die Beschlussvorlage mit der Beantragung einer gegenüber den Eckdaten gekürzten Finanzierung von Personal- und Sachmittel dem Stadtrat zur Entscheidung vorzulegen.
SKA	Die Stadtkämmerei erkennt den Bedarf für den Ausbau von Informationssicherheit zur Sicherstellung dieser Pflichtleistung grundsätzlich an.	Das IT-Referat bedankt sich für die Grundsätzliche Anerkennung des Bedarfes für den Ausbau von Informationssicherheit. Es ist festzuhalten, dass die SKA der dargelegten Unabweisbarkeit in der Beschlussvorlage nicht widersprochen hat.
SKA	Die Beschlussvorlage wird nachfolgend dennoch abgelehnt, da damit Festlegungen des Eckdatenbeschlusses für den Haushalt 2022 vorweggegriffen werden und ...	Die Beschlussvorlage zur IT-Sicherheit soll im selben Sitzungszyklus und der selben Vollversammlung wie die Eckdaten des Haushalts endgültig beschlossen werden. Insofern ist eine Parallelität gegeben, aber kein Vorweggreifen.
SKA	… (und) die in diesem Zusammenhang beantragte Finanzierung nicht realisierbar ist.	Das IT-Referat erkennt die schwierige Haushaltslage an, sieht aber auf-

REF/ PR	Excerpt aus Stellungnahme	Antwort / Kommentar
		grund der sich verschärfenden Bedrohungslage keine andere Wahl, als die Beschlussvorlage mit der Beantragung einer gegenüber den Eckdaten gekürzten Finanzierung von Personal- und Sachmittel dem Stadtrat zur Entscheidung vorzulegen. Das IT-Referat weist auf die unwidersprochene Unabweisbarkeit zum Thema Informationssicherheit hin.
SKA	Vorliegend handelt es sich um eine Maßnahme, die ab 2022 über eine Haushaltsausweitung finanziert werden soll. Damit unterliegt der Beschluss dem stadtweit festgelegten Verfahren für den Eckdatenbeschluss. (...) Das IT-Referat hat diese Maßnahme der Stadtkämmerei zwar für den Eckdatenbeschluss bereits gemeldet. Der Beschluss soll jedoch nun außerhalb des Verfahrens eingebracht werden, ohne dass der Stadtrat über Festlegungen oder das weitere Vorgehen zum Haushalt 2022 entschieden hat. Dies ist nicht zulässig. (...) Eine Entscheidung vorweg würde dieses Verfahren konterkarieren.	Die thematisch und inhaltlich gleiche Beschlussvorlage war als reine Antragsbehandlung (Stadtratsantrag Nr. 20-26 / A 00730) am 19.05.2021 fristgerecht im IT-Ausschuss. Die Beschlussvorlage wurde in dem Ausschuss qualifiziert vertagt auf den Ausschuss am 21.07.2021 und der ausdrücklichen Bitte des Stadtrates, die mit dem Thema IT-Sicherheit in Verbindung stehenden Kosten in der BV im Juli auszuweisen. Das IT-Referat kommt lediglich der Bitte des Stadtrates nach.
SKA	Auch die beantragte Finanzierung über eine Haushaltsausweitung wird abgelehnt.	Antragsziffern zur Finanzierung wurden im öffentlichen wie im nicht-öffentlichen Teil des Beschlussthemas dahingehend angepasst, dass die Finanzierung nur vorbehaltlich einer haushaltsmäßigen Beschlussfassung erfolgen soll.
SKA	Eine Zustimmung kann von Seiten der Stadtkämmerei nur erfolgen, wenn Kompensationsvorschläge für die Finanzierung benannt werden können.	Eine Kompensation innerhalb des Teilhaushalts des IT-Referats ist nicht möglich.
SKA	Die Stadtkämmerei wird somit das Direktorium D-HAII-V1 (Beschlusswesen) bitten, die Beschlussvorlage nicht auf die Tagesordnung des IT-Ausschusses zu nehmen (bzw. von der Tagesordnung abzusetzen).	Das IT-Referat bittet das Direktorium, die Beschlussvorlage auf die Tagesordnung des IT-Ausschusses im Juli zu nehmen (bzw. auf der Tagesordnung zu belassen).

Korreferent und Verwaltungsbeirat

Die Korreferentin des IT-Referates, Frau Stadträtin Sabine Bär, der Verwaltungsbeirat des IT-Referates Herr Stadtrat Lars Mentrup sowie die Verwaltungsbeirätin von it@M, Frau Stadträtin Judith Greif, haben einen Abdruck der Beschlussvorlage erhalten.

Anhörung des Bezirksausschusses

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

II. Antrag des Referenten

1. Der Stadtrat genehmigt die Umsetzung der Planung zur Fortentwicklung der IT-Sicherheit mit den Handlungsfeldern Sichere Authentisierung und digitale Prozesse, Risikomanagement IT-Sicherheit, IT-Sicherheitsarchitektur und Offensive Security, Security Orchestration Automation and Response, Endpoint Protection, ISM Governance und Cloud Security Management.
2. Der Stadtrat bestätigt die Ausführungen zur Unabweisbarkeit.
3. Unter dem Vorbehalt der haushaltsmäßigen Beschlussfassung wird das IT-Referat beauftragt, die dauerhafte Einrichtung von 5 VZÄ für fünf Risikomanager*innen IT-Sicherheit bei RIT-I ab 2022 sowie deren Besetzung beim Personal- und Organisationsreferat zu veranlassen.

   Das IT-Referat wird beauftragt, die dauerhaft erforderlichen Mittel zur Erhöhung des Personalhaushalts in Höhe von jährlich bis zu 444.750 € entsprechend der tatsächlichen Besetzung der Stelle, im Rahmen der Haushaltsplanung für 2022 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 177.900 € / Jahr (40 % des JMB).
4. Unter dem Vorbehalt der haushaltsmäßigen Beschlussfassung wird das IT-Referat beauftragt, die dauerhafte Einrichtung von 1 VZÄ für eine/n Cloud-Security-Manager*in bei RIT-I ab 2022 sowie deren Besetzung beim Personal- und Organisationsreferat zu veranlassen.

   Das IT-Referat wird beauftragt, die dauerhaft erforderlichen Mittel zur Erhöhung des Personalhaushalts in Höhe von jährlich bis zu 88.950 € entsprechend der tatsächlichen Besetzung der Stelle, im Rahmen der Haushaltsplanung für 2022 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 35.580 € / Jahr (40 % des JMB).
5. Unter dem Vorbehalt der haushaltsmäßigen Beschlussfassung wird das IT-Referat beauftragt, die dauerhafte Einrichtung von 1 VZÄ für eine/n ISMS-Governance-Manager*in bei RIT-I ab 2022 sowie deren Besetzung beim Personal- und Organisationsreferat zu veranlassen.

   Das IT-Referat wird beauftragt, die dauerhaft erforderlichen Mittel zur Erhöhung des Personalhaushalts in Höhe von jährlich bis zu 101.670 € entsprechend der tatsächlichen Besetzung der Stelle, im Rahmen der Haushaltsplanung für 2022 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 40.668 € / Jahr (40 % des JMB).

6. Unter dem Vorbehalt der haushaltsmäßigen Beschlussfassung wird das IT-Referat beauftragt, die einmalig erforderlichen personalbezogenen Sachmittel i. H. v. 14.000 € für das Jahr 2020 sowie dauerhaft erforderliche personalbezogene Sachmittel i. H. v. 5.600 € im Rahmen der Haushaltsplanaufstellung bei der Stadtkämmerei, beim Produkt Zentrale IT (P42111220) ab 2022 anzumelden.
7. Durch die Schaffung und Besetzung der Stellen entsteht kein zusätzlicher Raumbedarf.
8. Erhöhung des Produktkostenbudgets – vorbehaltlich der haushaltsmäßigen Beschlussfassung – beim Produkt Zentrale IT (P42111220) ab 2022 i. H. v.5.399.370 € dauerhaft, sowie zusätzlich einmalig in 2023 von 3.060.000 € (Summe öffentliche und nicht-öffentliche Vorlage).
9. Mit diesem Beschluss wird der Stadtratsantrag Nr. 20-26 / A 00730 der CSU-Fraktion vom 24.11.2020 „IT-Sicherheit priorisieren“ geschäftsordnungsmäßig erledigt.
10. Der Beschluss unterliegt nicht der Beschlussvollzugskontrolle.

III. Beschluss

nach Antrag.

Über den Beratungsgegenstand wird durch die Vollversammlung des Stadtrates endgültig beschlossen.

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. - IT-Referat Beschlusswesen