Telefon: 233 - 787777

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

4 Anlagen

Beschluss des IT-Ausschusses vom 19.05.2021 (SB)

Öffentliche Sitzung

Inhaltsverzeichnis

I. Vortrag des Referenten

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 Bürgerinnen und Bürgern sowie ansässigen Unternehmen und Partnern 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 weiterentwickeln, 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. Zum Zeitpunkt der Beschlussvorlagenerstellung sind die hierfür notwendigen Planungen sowie die Integration in die Informationssicherheitsstrategie jedoch nicht vollständig abgeschlossen. Aus diesem Grund bleibt der Stadtratsantrag Nr. 20-26 / A 00730 mit der vorliegenden Beschlussvorlage aufgegriffen. Eine abschließende Beschlussfassung wird im Rahmen der Verfahren zur Haushaltsbildung 2022 stattfinden.

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 Bürgerinnen und Bürger, Unternehmen und Partner 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 Berlin, 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 des 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.

Vor diesem Hintergrund können zum Zeitpunkt der Beschlussvorlagenerstellung noch keine durchgängig belastbaren Aussagen zu konkreten Umsetzungskonzepten getroffen werden, da die entsprechenden Prüfungen bzw. Planungen noch nicht abgeschlossen sind. Auch resultierende Mittelbedarfe sind noch nicht belastbar, sie bewegen sich nach aktueller Schätzung im einstelligen Millionenbereich.

In den folgenden Abschnitten werden die wesentlichen inhaltlichen Eckpunkte eines solchen Umsetzungskonzepts im Einklang mit der Informationssicherheitsstrategie dargestellt. Diese Eckpunkte werden Stand heute auch die inhaltlichen Schwerpunkte einer Beschlussvorlage bilden, die durch das ISM im Rahmen der üblichen Verfahren zur Haushaltsbildung für das Jahr 2022 eingebracht und damit dem Stadtrat vorgelegt werden.

Auf Grundlage der Inhalte der vorliegenden Beschlussvorlage bleibt der zugehörige Antrag Nr. 20-26 / A 00730 somit aufgegriffen, bis die finale Beschlussvorlage zum Haushalt 2022 gegen Ende des Jahres eingebracht wird. Das folgende Kapitel stellt im Ausblick die wesentlichen Handlungsschwerpunkte zum heutigen Stand dar.

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.

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 Nutzer 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 eAkte. 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 eines Risikomanagers 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.

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 Erfolgsfaktoren, 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.

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 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.

4. Beteiligungen

Die Beschlussvorlage wurde mit dem Direktorium (Anlage 2), der Stadtkämmerei (Anlage 3) und dem Gesamtpersonalrat (Anlage 4) abgestimmt.

Korreferent und Verwaltungsbeirat

Die Korreferentin des IT-Referates, Frau Stadträtin Sabine Bär und der Verwaltungsbeirat des IT-Referates Herr Stadtrat Lars Mentrup 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. Mit diesem Beschluss bleibt der Stadtratsantrag Nr. 20-26 / A 00730 der CSU-Fraktion vom 24.11.2020 „IT-Sicherheit priorisieren“ bis zum 30.12.2021 aufgegriffen. Eine abschließende Beschlussfassung wird im Rahmen der Verfahren zur Haushaltsbildung 2022 stattfinden.
2. Der Beschluss unterliegt nicht 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. - IT-Referat Beschlusswesen