STADT GERMERING

Kämmerei
Datum 07.11.2022

Beschluss-Vorlage 2022/0392 zur Sitzung am 01.12.2022
des HAUPTAUSSCHUSSES

TOP 7 öffentlich

Betreff:	Bericht über die überörtliche Prüfung der Jahresrechnungen und Jahresabschlüsse 2014 bis 2019 durch den Bayer. Kommunalen Prüfungsverband für die Prüfungsgebiete Bauausgaben und allg. Verwaltung - Stellungnahmen der Verwaltung

Finanzielle Auswirkungen?	Ja	Nein

Kosten laut Beschlussvorschlag:	Kosten der Gesamtmaßnahme	Folgekosten
Euro	(nur bei Teilvergaben)	einmalig
Kosten lt. Kostenschätzung		lfd. jährl.
Euro	Euro	Euro

Veranschlagt			Produktkonto
im Ergebnis-HH	im Investitions-HH	mit	Haushaltsansatz
2022	2022	Euro	Bereits vergeben

Der zuständige Referent / Die zuständige Referentin		
wurde gehört	hat zugestimmt	hat nicht zugestimmt

Sachverhalt:

Über die Grundzüge und Inhalte der Prüfung wurde in der letzten Sitzung des Hauptausschusses berichtet und bereits einzelne Stellungnahmen zur Kenntnis genommen.

Zu folgenden, weiteren Prüfungserinnerungen und Feststellungen des Bayerischen Kommunalen Prüfungsverbandes (Textziffern/TZ) kann eine Stellungnahme durch die zuständigen Ämter erfolgen:

TZ 12 Organisation des IT-Betriebs

a) Erstellen der notwendigen Informationssicherheitskonzepte

Bei der Stadt waren die gesetzlich vorgeschriebenen Informationssicherheitskonzepte zwar bereits 2018 erstellt, seitdem jedoch nicht in Kraft gesetzt worden. Dies wurde seitens der Stadt mit der bislang unbesetzten Stelle des Informationssicherheitsbeauftragten begründet.

Die Stadt sollte noch mit Nachdruck auf die Erstellung und die Inkraftsetzung eines aktuellen Informationssicherheitskonzeptes (sowie davon abgeleitete Detailkonzepte, wie z.B. zu den Themen Notfallvorsorge, Datensicherung, Sicherheitsgateway, Virenschutz, infrastrukturelle Sicherungsmaßnahmen, Datenschutz) hinwirken. Die gesetzliche Verpflichtung, die Sicherheit der IT-Systeme im Rahmen der Verhältnismäßigkeit sicherzustellen, besteht bereits seit 30.12.2015. Zu diesem Zweck hätten spätestens bis 01.01.2020 angemessene technische und organisatorische Maßnahmen getroffen und die hierzu erforderlichen Informationssicherheitskonzepte erstellt werden müssen (vgl. Art. 11 Abs. 1 i.V. mit Art. 19 Abs. 2 Satz 2 Nr. 3 BayEGovG).

In diesem Zusammenhang wird auf das im Rahmen der Prüfung überlassene BKPV-Merkblatt „Anforderungen an die Informationssicherheitskonzepte“ verwiesen.
Zur Besetzung des Informationssicherheitsbeauftragten bieten sich neben dem Einsatz eigenen Personals auch Modelle der interkommunalen Zusammenarbeit an.

b) Organisatorische Regelungen

Eine Dienstanweisung, die nähere Regelungen über den Einsatz automatisierter Verfahren, deren Sicherung und Kontrolle i.S. von § 33 Abs. 2 KommHV-Doppik enthält und einen ordnungsgemäßen und sicheren IT-Betrieb unterstützt, war zum Prüfungszeitpunkt zwar vorhanden, entsprach allerdings seit längerem nicht mehr den örtlichen Verhältnissen. Wir empfehlen, die IT-Dienstanweisung neu zu erlassen. Wegen der notwendigen Regelungsinhalte wird auf § 33 Abs. 1 und 2 KommHV-Doppik verwiesen. Was die allgemeinen Regelungen zum sicheren IT-Betrieb und zur ordnungsgemäßen Internet-/E-Mail-Nutzung betrifft, empfehlen wir, sich hierbei an den von den Bayerischen Kommunalen Spitzenverbänden veröffentlichten Muster-Dienstanweisungen zu orientieren und diese ggf. an die örtlichen Verhältnisse anzupassen. Die Bayerischen Kommunalen Spitzenverbände bieten ihren Mitgliedern diese Muster-Dienstanweisungen in elektronischer Form auch zum Download an.

c) Elektronische Aktenführung

Bei der Stadt kam zum Zeitpunkt unserer Prüfung, mit Ausnahme des elektronischen Kassenbelegarchivs (Docuware), für die Aktenführung sowie für die allgemeine Schriftgutverwaltung bislang noch kein Dokumentenmanagementsystem (DMS) zum Einsatz. Auch bereichsspezifische Lösungen zur elektronischen Aktenführung (eAkte), wie z.B. in Verbindung mit den eingesetzten Vorgangssachbearbeitungssystemen, kamen nur vereinzelt zum Einsatz.
Insbesondere die Anforderungen des Bayer. E-Government-Gesetzes (BayEGovG) bzw. des angekündigten Bayer. Digitalgesetzes (BayDiG), die rasant fortschreitende Digitalisierung sowie die Anforderungen aus dem Onlinezugangsgesetz (OZG) als auch an die eigene Verwaltungsökonomie machen es u.E. erforderlich, sich mit der Einführung eines DMS zu beschäftigen und diese priorisiert voranzutreiben.

Mit einem künftigen fachbereichsübergreifenden Einsatz eines DMS sehen wir insbesondere folgende Vorteile:

- Optimierungen der Geschäftsprozesse und der behördeninternen Kooperation sowie der Zusammenarbeit
- Abbau von Aktenbergen und Ersparnis an Lagerfläche für die Akten
- Reduzierung von Druck- und Kopierkosten (weitere Synergien, z.B. mit E-Postbrief)
- Möglichkeiten zur vollständigen und medienbruchfreien elektronischen Aktenführung (inkl. E-Mails) und der medienbruchfreien Übernahme von Online-Anträgen im Rahmen des OZG

- Rechtskonforme Aufbewahrung von elektronischen Rechnungen und Kontoauszügen (vgl. TZ 18 b)
- Arbeitserleichterungen durch papierarme Abläufe
- Schnellere Recherche von Dokumenten (u.a. Volltextsuche)
- Gleichzeitiges Arbeiten an derselben Akte
- Entlastung der Beschäftigten von Nebentätigkeiten (z.B. manuelle Ablage)
- (Medienbruchfreie) digitale Vernetzung mit anderen Behörden aller Ebenen
- Fernzugriff auf die im DMS/Archiv gespeicherten Dokumente, Vorgänge oder Akten sowie deren Bearbeitung von anderen Orten (z.B. mobiles Arbeiten, Home-Office)
-

Wir empfehlen daher der Stadt den Ausbau der elektronischen Aktenführung.

d) Zentrale Vertragsverwaltung

Stichprobenweise haben wir Vertragsunterlagen (z.B. Überlassungs- und Pflegeverträge) der eingesetzten automatisierten Verfahren angefordert. Die Stadt konnte uns teilweise keine bzw. keine vollständigen Unterlagen zu den lizenzierten Programmen und den vertraglich vereinbarten Preisen vorlegen. Um die fristgerechte Erfüllung der vertraglich vereinbarten Leistungen, die korrekte Abrechnung der Lieferungen und Leistungen sowie die vorhandenen Lizenzen sachgerecht zu prüfen oder zu überwachen, empfehlen wir, eine zentrale und ggf. IT-gestützte Vertragsverwaltung für den Bereich der IT aufzubauen und diese Aufgabe dem Sachgebiet Information und Kommunikation zu übertragen. Im Idealfall bietet eine IT-gestützte Vertragsverwaltung Folgendes:

- Eine schnelle Suche von Verträgen nach unterschiedlichen Kriterien, Metadaten und Volltexten
- Eine strukturierte Ablage aller Dokumente, des begleitenden Schriftverkehrs und aller E-Mails
- Gegebenenfalls eine Termin- und Fristenüberwachung
- Ein effizientes Vertragscontrolling
- Anbindung an das Dokumentenmanagementsystem

Neben einer eigenen Softwarelösung (mit erweiterten Funktionalitäten) könnte die Vertragsverwaltung auch über ein noch einzuführendes Dokumentenmanagementsystem realisiert werden (vgl. die Ausführungen unter Buchst. c).

e) Strategische Ausrichtung zur Betreuung der IT

Wie den nachfolgenden Feststellungen zu entnehmen ist, bestand beim IT-Betrieb v.a. im Bereich der System-, Verfahrens- und Netzwerkadministration teils größerer Handlungsbedarf (vgl. TZ 13, TZ 14 sowie TZ 15). Eine proaktive Administration der IT-Systeme war zum Prüfungszeitpunkt nur bedingt gewährleistet. Wir weisen daher darauf hin, dass die Stadt die Verantwortung dafür trägt, dass ein ordnungsgemäßer und wirtschaftlicher IT-Betrieb sichergestellt wird und die finanzwirksamen Verfahren nach den haushaltsrechtlichen Vorschriften betrieben werden.

Zur dauerhaften Sicherstellung eines ordnungsgemäßen IT-Betriebs sowie zur innovativen Weiterentwicklung der städtischen IT (z.B. Dokumentenmanagementsystem, elektronische Signaturen) empfehlen wir der Stadt, für die Systembetreuung vor Ort dauerhaft und unter Berücksichtigung entsprechender Stellenanteile ausreichend eigene Kernkompetenzen vorzuhalten.

In diesem Zuge sollte die Stadt festlegen, ob vermehrt Fremdunterstützung (wie bisher bei den Stadtwerken und der Stadtbibliothek) oder verstärkt eigenes Personal zur Systembetreuung der städtischen

IT eingesetzt werden soll. Die Entscheidung sollte ggf. mit einer Wirtschaftlichkeitsbetrachtung unterstützt werden. Den notwendigen Stellenbedarf für die örtliche IT-Betreuung empfehlen wir hierzu noch zu ermitteln.

Da für den angetroffenen IT-Betrieb und dessen Organisation eine Reihe an z.T. weitreichenden strategischen Entscheidungen anstehen, empfehlen wir das weitere Vorgehen durch ein nachvollziehbares, über einen Mehrjahreszeitraum fortgeschriebenes ITKonzept zu unterstützen, das von den zuständigen Gremien beschlossen wird. Das ITKonzept sollte aufgestellt, fortlaufend aktualisiert und nach den enthaltenen Planungen realisiert werden.

Das Verwaltungs- und Rechtsamt / Sachgebiet Information und Kommunikation (SG IuK) nimmt dazu wie folgt Stellung:

zu TZ 12 a):

Das Informationssicherheitskonzept ist erstellt und wurde aktuell überprüft. Es kann erst durch den/die Informationssicherheitsbeauftragte(n) (ISB) in Kraft gesetzt werden. Eine Stellenausschreibung ISB ist zum wiederholten Mal erfolglos geblieben. Auch der Versuch einer interkommunalen Zusammenarbeit war bislang nicht erfolgreich. Eine erneute Stellenausschreibung mit dem Anforderungsprofil „ISB & Digitalisierungsbeauftragte(r)“ ist in Kürze beabsichtigt.

zu TZ12 b):

Die bestehende IT-Dienstanweisung wird überarbeitet und an neue Vorgaben angepasst.

zu TZ12 c):

Die Besetzung der o. g. Stelle zentrale(r) Digitalisierungsbeauftragte(r) ist zur Umsetzung notwendig.

zu TZ12 d):

Ein Archiv „Zentrale Vertragsverwaltung“ wird im Dokumentenmanagementsystem erstellt. Dort werden alle vorhandenen Verträge digital abgelegt (eine Rückfrage durch den BKPV wegen fehlender Unterlagen ist leider nicht erfolgt).

zu TZ12 e):

Das IT-Konzept ergibt sich wie bisher aus der mehrjährig aufgestellten Haushaltsplanung.

TZ 13 Schwachstellen beim Datensicherungskonzept

Die Datensicherung der virtuellen Serversysteme wurde bei der Stadt unter Einsatz der Sicherungssoftware „VEEAM Backup & Replication V 9.5“ arbeitstäglich um 18.15 Uhr auf ein im Serverraum im „Zenja“-Gebäude (Rathaus Unterpfaffenhofen) untergebrachtes Netzwerkspeichersystem (NAS) vorgenommen und direkt im Anschluss auf externe Sicherungsbänder geschrieben. Hierzu kam ein Multibandwechsler zum Einsatz. Die Sicherungsbänder wurden jeweils am Montag aus dem Bandwechsler

entnommen und zugriffsgeschützt in den Räumlichkeiten der Stadtwerke aufbewahrt. Ergänzend wurde die gleiche Gruppe der Serversysteme ebenfalls arbeitstäglich durch den Sicherungsjob „Wochenrepository Server System“ auf das o.g. NAS gesichert. Auf dem NAS selbst wurden 60 Sicherungspunkte gespeichert. Für die SQL-Server Datenbanken waren sog. Wartungspläne eingerichtet. Die über den SQL-Server erzeugten Vollsicherungen und untertäglich erzeugten Transaktionslogs wurden über diese Wartungspläne direkt auf ein weiteres NAS, das ebenfalls im „Zenja“-Gebäude untergebracht war, gesichert.

Wir sehen noch folgende Verbesserungspotenziale:

- Nicht alle Sicherungsdaten wurden arbeitstäglich in einen anderen Brandabschnitt ausgelagert und wären bei größeren Schadensereignissen (z.B. Brand, Blitzschlag) ggf. gefährdet.
- Die beiden o.g. Sicherungsjobs produzierten bereits seit mehreren Monaten Warn- sowie Fehlermeldungen und wiesen ein ungewöhnliches Laufzeitverhalten auf.
- Zwischen den im Microsoft SQL-Server Management Studio konfigurierten Wartungsplänen und den o.g. Sicherungsjobs kam es zu zeitlichen Überschneidungen.
- Einzelne Systeme wurden nicht gesichert. Es war nicht zweifelsfrei erkennbar, bei welchen Systemen es sich um Test- bzw. Altsysteme handelte.
- Die über das Microsoft SQL-Server Management Studio erzeugten und über Wartungspläne gesicherten Transaktionsprotokolle wurden zwar auf einem separaten NAS und damit nicht auf den produktiven Datenbankservern selbst gespeichert, allerdings waren die Abstände, in denen die Sicherungen erzeugt wurden, für die Datenbanken der Stadt sehr unterschiedlich konfiguriert. Für einige der Datenbanken waren hingegen keinerlei Wartungspläne eingerichtet.
- Das Sicherungskonzept war unnötig komplex.
- Eine Dokumentation des Sicherungskonzeptes und der hinterlegten Einstellungen war zwar vorhanden, allerdings unvollständig und nicht mehr aktuell.

Zur Verbesserung der Datensicherung verweisen wir auf die Anforderungen und Umsetzungshinweise in unserem im Rahmen der Prüfung ausgehändigten BKPV-Merkblatt „Anforderungen an die Datensicherung“.

Das Verwaltungs- und Rechtsamt / SG IuK nimmt dazu wie folgt Stellung:

zu TZ 13:

Die Verbesserungsvorschläge wurden zum Großteil bereits umgesetzt, mit Investitionen verbundene Verbesserungen befinden sich in Umsetzung.

TZ 14 Unzureichender Zugriffsschutz auf Fachverfahren und Datenbanken finanzwirksamer Verfahren

a) Einsatz eines ungeeigneten Datenbanksystems

Die Datenhaltung der Verfahren adebisKITA (Kindergartenverwaltung) und ElFried (Friedhofsverwaltung) war über eine zum installierten Datenbanktreiber Microsoft Visual FoxPro kompatible Datenbank (Btrieve-Datenbank) realisiert. Bei diesem dateibasierten Datenbanksystem kann über den Windows Datei-Explorer auch auf die Programm- und Datenbankdateien des Verfahrens zugegriffen werden,

sodass ein geeigneter (gekapselter) Zugriffsschutz, wie z.B. bei einem zugangsgeschützten Datenbanksystem (Oracle Database, SQL-Server), nicht besteht. Auf die Installationsverzeichnisse der beiden Verfahren und die zugehörigen Unterverzeichnisse, die auch die Dateien des Datenbanksystems enthielten, besaßen die Benutzerkonten der Verfahrensanwender Schreib- und Leserechte.
Beide Verfahren dienten der Ermittlung von Zahlungsansprüchen und werden daher als finanzwirksame Verfahren vom Anwendungsbereich des § 33 Abs. 1 KommHVDoppik erfasst. Derart umfangreiche Zugriffsrechte auf die Datenbank (Struktur und Inhalte) eines finanzwirksamen Verfahrens sind weder mit den haushaltsrechtlichen Sicherheitsanforderungen (vgl. § 33 Abs. 1 Nrn. 4 und 5 KommHV-Doppik) noch mit den allgemeinen Anforderungen an die Informationssicherheit (vgl. Art. 11 Abs. 1 BayEGovG) vereinbar.

b) Unzureichende Absicherung des abgelösten Finanzverfahrens „TDV HKR“

Der Zugang zur Datenbank des bereits abgelösten teildezentralen Verfahrens für das Haushalts-, Kassen- und Rechnungswesen „TDV HKR“ war mit dem privilegierten Benutzerkonto „hkrsys“ und einem unter AKDB-Anwendern überörtlich bekannten und zudem sehr leicht zu erratenden Passwort möglich. Dieser ungeeignet abgesicherte Zugang würde dem jeweiligen Benutzer z.T. einen umfassenden direkten Zugriff (Lesen, Ändern, Löschen) auf die gespeicherten Daten auch außerhalb einer Anmeldung am Verfahren, den dort hinterlegten Zugriffs- und Plausibilitätskontrollen sowie verfahrensinternen Protokollierung ermöglichen.

c) Absicherung administrativer Verfahrenszugänge

Die Anmeldung am Finanzverfahren OK.FIS war unter administrativen Rechten mit dem administrativen Benutzerkonto „zssadmin“ und zugehörigem, unter AKDB-Anwendern überörtlich bekannten bzw. sehr leicht zu erratenden Standardpasswort möglich, da das übliche Standardpasswort nach der Inbetriebnahme des Verfahrens und auch in der Folgezeit weder von der Stadt noch vom Verfahrensanbieter geändert worden war. Gleiches galt für die privilegierten Benutzerkonten „admin“ und „ght“ in der Verwaltungssoftware „CPS 2.5“ des Kassenautomaten.

d) Direkter Zugriff auf Verfahrensdatenbanken über die Windows-Authentifizierung möglich

Über das Office-Programm „Microsoft Excel“ oder weitere frei verfügbare Datenbankzugriffsprogramme war auch der Zugang zur Datenbank des Fachverfahrens „OKWAHL“ sowie des Geoinformationssystems (GIS) über die im Datenbanksystem hinterlegte „Windows-Authentifizierung“ für alle Domänen-Benutzer bzw. die Mitglieder der Domänen-Benutzergruppe „GG_APP_VM_GIS_Benutzer“ möglich. Der Zugang würde dem jeweiligen Domänen-Benutzer z.T. einen direkten und umfassenden Zugriff (Lesen, Ändern, Löschen) auf die in den o.g. Verfahrensdatenbanken gespeicherten Daten auch außerhalb einer Anmeldung am jeweiligen Verfahren ermöglichen.

Zu Buchstaben a) bis d):

Die dauerhafte Verwendung von Initial- oder Standardpasswörtern oder einem größeren Benutzerkreis bekannten Passwörtern, die ungeeignete Absicherung der Datenbanken bzw. der Einsatz ungeeigneter Datenbanksysteme stellen allgemein ein erhöhtes Risiko für die Vertraulichkeit, Verfügbarkeit und Integrität der automatisierten Verfahren und deren Daten dar. Der Zugriff auf die Fachverfahren und Datenbanken wäre ggf. in Zusammenarbeit mit den Verfahrensanbietern insgesamt zu überprüfen und - soweit notwendig - mit einer ausreichend sicheren Authentifizierungsmethode, ausreichend sicheren und

geheimen Passwörtern bzw. einem adäquaten Berechtigungskonzept abzusichern, um die haushaltsrechtlichen und allgemeinen IT-Sicherheitsanforderungen zu gewährleisten (vgl. insbesondere § 33 Abs. 1 Nrn. 3, 5 und 6 KommHV-Doppik, Art. 11 Abs. 1 BayEGovG). Ergänzend verweisen wir auf unsere BKPV-Mitteilungen 4/1998, RdNr. 30, S. 16 ff., und 2/2002, RdNr. 15 Nr. 2, S. 29 f.

Regelmäßige Sicherheitsüberprüfungen der Verfahrenszugänge und der zugrundeliegenden Datenbanksysteme sollten zusätzlich proaktiv als administrative Aufgabe wahrgenommen werden (vgl. auch die Basis-Anforderungen APP.4.3.A20 „Regelmäßige Audits“ des BSI-Kompendiums, Edition 2020). Der Verfahrensanbieter AKDB bietet adebisKITA zwischenzeitlich auch mit einer SQLServer Datenbank an, die bei entsprechender Konfiguration einen gesicherten (gekapselten) Zugriff auf die Datenbank ermöglicht. Die Stadt sollte diese Umstiegsmöglichkeit wahrnehmen (vgl. § 33 Abs. 1 und § 57 Abs. 4 KommHV-Doppik, Art. 11 Abs. 1 BayEGovG).

Das Verwaltungs- und Rechtsamt / SG IuK nimmt dazu wie folgt Stellung:

<u>zu TZ 14 a):</u>

Die Verfahrensanbieter wurden bereits zur Umstellung kontaktiert. Diese werden in 2022 / 2023 umgestellt.

<u>Zu TZ 14 b):</u>

Das Benutzerpasswort für das alte System TDV / HKR (Altdaten lesen) wird in Zusammenarbeit mit der Stadtkämmerei geändert. In Zusammenarbeit mit der Stadtkämmerei wird geprüft, ob eine Verwendung noch notwendig ist.

<u>zu TZ 14 d):</u>

OK-WAHL ist nicht mehr im Einsatz (wurde durch OK-VOTE ersetzt) und kann in Zusammenarbeit mit VuR abgeschaltet werden.
Die Zugriffsrechte der Domänengruppe „GG_APP_VM_GIS_BENUTZER“ wurden in Zusammenarbeit mit dem Bauamt auf die notwendigen Zugriffsmöglichkeiten überprüft und angepasst. Dieses wiederum wird zur kommenden Landtagswahl durch akdb ELECT abgelöst.

Die Finanzverwaltung nimmt wie folgt Stellung:

<u>zu TZ 14 c):</u>

Die angesprochenen Verfahrenszugänge wurden nach Möglichkeit selbst angepasst bzw. werden noch angepasst durch den Softwareanbieter.

TZ 15 Weitere notwendige Maßnahmen zur Behebung von Gefährdungspotenzialen bei der System- und Netzwerksicherheit

a) Infrastrukturelle Sicherheit der Serverräume

Die produktiven Serversysteme der Stadt waren in zwei Serverräumen im ersten bzw. fünften Obergeschoss des Rathauses untergebracht. In der Außenstelle „Rathaus Unterpfaffenhofen“ (Zenja-Gebäude) waren die Sicherungssysteme sowie ein zur Speicherung produktiver Datenbestände eingesetztes Speichersystem untergebracht. Im Kellergeschoss waren in einem weiteren Raum die Internetanschlüsse sowie die Firewallsysteme der Stadt eingerichtet bzw. untergebracht. In keinem der Räume war eine Brand- oder Gefahrenmeldeanlage installiert.

Eine Auswertung der Schließberechtigungen nach ausgegebenen Schließ-Transpondern aus dem elektronischen Schließsystem „Simons Voss“ ergab folgende Schließberechtigungen:

Raum	Schließberechtigung
Serverraum 5. OG	30 Transponder
Serverraum 1. OG	33 Transponder
Serverraum „Zenja“	23 Transponder
Hausanschluss Keller	29 Transponder
Serverraum Stadtbibliothek	54 Transponder

Die Serverschränke selbst in den Räumen waren nicht verschlossen. Die infrastrukturelle Sicherheit der Serverräume war somit nicht in vollem Umfang gewährleistet. Den bestehenden Gefährdungen durch Feuer sowie Zugangs- und Zugriffsmöglichkeiten durch Unbefugte sollte Rechnung getragen werden. Zudem sollte der Zugang zu Datenverarbeitungs- und Datenspeicherungsanlagen nur den berechtigten Personen vorbehalten sein und nur soweit dies im Rahmen der Aufgabenerfüllung erforderlich ist (vgl. § 33 Abs. 1 Nrn. 3 und 4 und § 39 Abs. 1 Nr. 3 KommHV-Doppik, Art. 11 Abs. 1 BayEGovG).

Der Zugang zu Serversystemen und Speichersystemen zur Datensicherung wäre daher auf den berechtigten Personenkreis einzuschränken. Ergänzend verweisen wir auf die Basis-Anforderungen INF.2.A6 „Zutrittskontrolle“, INF.2.A7 „Verschließen und Sichern“ sowie INF.2.A8 „Einsatz einer Brandmeldeanlage“ des Bausteins „INF.2 Rechenzentrum sowie Serverraum“ des BSI-Kompendiums.

b) Ablösung nicht mehr unterstützter Betriebssysteme und Softwarelösungen

Die Stadt setzte auf mindestens zwei Server- sowie vier Client-Systemen noch die Betriebssysteme „Microsoft Windows Server 2008 R2“ bzw. „Microsoft Windows 7 Professional“ ein. Auf einem der virtuellen Datenbankserver (APP-VM) kam als Datenbankmanagementsystem (DBMS) zudem noch die Version „Microsoft SQL Servers 2008 R2“ zum Einsatz. Darüber hinaus wurden noch Microsoft Office 2010 sowie Microsoft Exchange Server 2010 eingesetzt.

Für diese Betriebssysteme, das DBMS, die Office-Version sowie die o.g. Version des Exchange Servers werden vom Hersteller seit längerem keine Programm- und Sicherheitsupdates mehr angeboten. Dies hat zur Folge, dass die Stadt vom Hersteller

- keine Aktualisierungen bei Sicherheitsproblemen,
- keine Produktupdates zur Behebung von Fehlern (sog. Hotfixes),

− keine telefonische Unterstützung im Problemfall und
− keine online verfügbaren, aktuellen technischen Dokumente zur Problembehebung mehr erhält.

Aus den vorstehenden Gründen empfehlen wir die zeitnahe Ablösung der noch eingesetzten veralteten Betriebssysteme, des DBMS und der weiteren veralteten Softwarelösungen sowie die Migration auf aktuelle und vom Hersteller unterstützte Lösungen.

c) Fernzugriff auf Sicherheitsgateway

Die Stadt setzte am Übergang in Fremdnetze zwei Appliances vom Typ „Sophos SG330" im Cluster ein. Im Rahmen der Prüfung stellten wir fest, dass der Zugriff auf die Administrationskonsole der Firewall vom Internet und damit aus Fremdnetzen, z.B. über das Protokoll „https", uneingeschränkt möglich war. Die Administration der eingesetzten Firewall über direkten Internetzugriff ist nicht erforderlich, da dies aus dem eigenen Netzwerk heraus problemlos möglich ist. Zudem stellt die Adressierbarkeit der Firewallsysteme aus dem Internet ein erhöhtes Sicherheitsrisiko dar. Der Zugriff auf die Verwaltungskonsole sollte nur aus vertrauenswürdigen Netzen möglich sein und möglichst restriktiv gefasst werden. Wir empfehlen eine Einschränkung auf den IP-Adressbereich der IT-Systemverantwortlichen bzw. die Administration über ein Management-LAN (vgl. die Basis-Anforderung des Bausteins NET.3.2.A6 „Schutz der Administrationsschnittstellen" des BSI-Kompendiums).

d) Protokollierung bedeutsamer Systemereignisse

Eine Protokollierung von bedeutsamen oder sicherheitsrelevanten Systemereignissen war zum Prüfungszeitpunkt nicht aktiviert (z.B. Aufzeichnung fehlerhafter Login-Versuche von normalen und administrativen Benutzerkonten, vgl. dazu die Basis-Anforderungen des Prozess-Bausteins OPS.1.1.5 des BSI-Kompendiums).

Wir empfehlen, im Rahmen der Schutzbedarfsermittlung zu den Informationssicherheitskonzepten den notwendigen Umfang an eine Protokollierung zu ermitteln. Hierbei sollte auch festgelegt werden, inwieweit regelmäßig Auswertungen von sicherheitsrelevanten Ereignissen vorgenommen und festgestellte Unregelmäßigkeiten näher untersucht werden sollen.

e) Patchmanagement

Die Sicherheitsupdates und Patches für die Windows-Betriebssysteme sowie Microsoft Anwendungen (z.B. Office) wurden bei der Stadt über den Dienst „Windows Server Update Services" (WSUS) eingespielt. Im Rahmen unserer Prüfung stellten wir fest, dass für zahlreiche Systeme im WSUS kein aktueller Statusbericht verfügbar war. Dies betraf auch Systeme, die zum Zeitpunkt unserer Einsichtnahme eingeschaltet waren. Eine zentrale Überwachung des Ausbringungsstandes war über den WSUS somit nicht möglich. Darüber hinaus standen bei mehreren Clients jeweils noch mehr als 100 Updates zur Installation aus (vgl. Status „erforderlich"). Darunter befanden sich auch eine Vielzahl sicherheitsrelevanter Updates.

Im Hinblick auf die Abhängigkeit der Stadt von der Funktionsfähigkeit der IT-Systeme und die wiederkehrend auftretenden Sicherheitslücken bei weit verbreiteten StandardSystemen sollten die verfügbaren Sicherheitsupdates im Rahmen einer proaktiven Serveradministration für alle Systeme zeitnah eingespielt werden (vgl. die Basis-Anforderungen des Bausteins OPS.1.1.3 Patch- und Änderungsmanagement des BSI-Kompendiums). Wir empfehlen, künftig auch eigene Überprüfungen vorzunehmen, ob tatsächlich alle Updates eingespielt wurden.

f) Aktualität der Benutzerkontenverwaltung im allgemeinen Verzeichnisdienst des lokalen Netzwerks (Active Directory)

Im allgemeinen Verzeichnisdienst waren noch zahlreiche Benutzerkonten für Beschäftigte eingerichtet und aktiv, die zwischenzeitlich ausgeschieden oder längerfristig abwesend waren (z.B. Elternzeit). Zum Teil wurden auch funktionsbezogene Benutzerkonten verwendet.

Domänen-Benutzerkonten für ausgeschiedene oder langfristig abwesende Beschäftigte sollten zumindest deaktiviert werden. Wir empfehlen, die Benutzerverwaltung aktuell zu halten und regelmäßige Überprüfungen im Rahmen einer proaktiven Systemadministration vorzunehmen. Darüber hinaus empfehlen wir, nach Möglichkeit ausschließlich individuell zuordenbare Benutzerkonten zu verwenden.

Das Verwaltungs- und Rechtsamt / SG IuK nimmt dazu wie folgt Stellung:

zu TZ15a):

Zugriffrechte aller Räume wurden überprüft und geändert / entzogen.

zu TZ15b):

Die veralteten Serversysteme werden nach Umstellung der darauf laufenden Verfahren abgeschaltet. Dies ist ein dauerhafter und fortlaufender Prozess, welcher den Vorgaben der Softwareanbieter unterliegt.

zu TZ15c):

Der Zugriff auf die Administrierbarkeit der Firewall aus dem Internet wurde zeitnah geschlossen. Ein Management-Lan befindet sich im Aufbau.

zu TZ15 d):

Die Protokollierung ist aktiv und wird ständig überprüft. Die Einführung einer Monitoring-Software (Paessler) ist in Planung und wird nach Schulung eines neuen Kollegen/einer neuen Kollegin eingeführt.

zu TZ15 e):

Aufgrund des erhöhten Bedarfs an Homeofficearbeitsplätzen wurden die bestehenden Arbeitsplätze zum Teil nie neu gestartet. Ein Update findet nur bei Neustart der Arbeitsplätze statt.
*Der mit den Updates beauftrage Mitarbeiter wurde angewiesen die Systeme zu kontrollieren und Anwender*innen darauf hinzuweisen, ihre Arbeitsplätze bei Bedarf neu zu starten. Ein möglicher automatischer Zwangsneustart könnte vereinzelt zu Datenverlust führen. Die Serverupdates müssen manuell außerhalb der Dienstzeit installiert werden. Dabei kann es vereinzelt zu Verzögerungen kommen.*

zu TZ15 f):

Die Benutzerkonten werden deaktiviert sobald das SG IuK von der Abwesenheit Kenntnis erlangt. Eine Verbesserung des Workflows ist in Arbeit.

TZ 16 Schwachstellen bei der Nutzung des Kassenautomaten

Die Stadt setzte im Hauptgebäude einen Kassenautomaten der Firma GHT ein. Während der Vorgangsbearbeitung in den einzelnen Sachgebieten wurde für bar auszuzahlende oder anzunehmende Beträge über das Erfassungsprogramm des Kassenautomaten „CPS-Charge“ der jeweilige Betrag einer elektronischen Zahlkarte zugeordnet. Mittels dieser Zahlkarte entrichtete der Bürger den ermittelten Betrag am Kassenautomaten und erhielt eine Quittung (sog. Gebührenmarke), die er wiederum dem jeweiligen Sachbearbeiter als Nachweis der erfolgten Einzahlung vorlegte. Keines der bei der Stadt eingesetzten Fachverfahren verfügte über eine direkte Schnittstellenanbindung an den Kassenautomaten.

Im Rahmen der Prüfung haben wir die hinterlegte Systemkonfiguration des Kassenautomaten und die hinterlegten Rechte im Verwaltungsprogramm zum Kassenautomaten stichprobenweise angesehen. Dabei haben wir folgende Sachverhalte angetroffen:

a) Berücksichtigung der Funktionstrennung

Die Administration des Kassenautomaten und der hierfür zentral installierten, modular aufgebauten Verwaltungssoftware „CPS 2.5“ erfolgte durch Beschäftigte der Stadtkasse. Ebenso hatten Beschäftigte der Stadtkasse lokalen Zugriff am Automaten selbst unter Verwendung einer administrativen Benutzerkennung.

Die Administration durch Beschäftigte der Kasse bzw. durch Beschäftigte, die mit Kassenabschlussaufgaben betraut sind, halten wir aus Gründen der Kassensicherheit für problematisch. Unsere grundsätzlichen Bedenken richten sich v.a. gegen das Zusammentreffen von „geldnahen Tätigkeiten“ (Entnahme und Einbringen der Barbestände in den Kassenautomaten) und den hier vorliegenden weitreichenden (administrativen) Rechten im Kassensystem (Anlegen von Benutzern, Durchführen von Gegenbuchungen etc.). Die Wahrnehmung beider Aufgaben durch Beschäftigte der Kasse bzw. durch Beschäftigte, die mit Kassenabschlussaufgaben betraut sind, verstößt gegen den Grundsatz der Funktionstrennung (§ 33 Abs. 1 Nr. 10 KommHV-Doppik). Auf unsere BKPV-Mitteilungen 4/1998, S. 4 ff. sowie auf TZ 17 0 dürfen wir in diesem Zusammenhang verweisen.

b) Sichere Authentifizierung

- Für 15 von insgesamt 43 Benutzerkonten wurden bei der Anmeldung an den Gebühren- und Auszahlungsmodulen zum Kassenautomaten z.T. die gleichen Passwörter, in jedem Fall aber Trivialpasswörter verwendet.

- Die administrativen Benutzerkonten „admin“ und „ght“ waren jeweils nur mit einem Initialkennwort, das darüber hinaus leicht zu erraten war, vor unbefugter Verwendung geschützt.

Es wäre künftig zwingend auf die Einhaltung der haushaltsrechtlichen Sicherheitsanforderungen hinzuwirken, die eine sichere und eindeutige Authentifizierung bei den finanzwirksamen Verfahren voraussetzen. Die Einstellungen zur sicheren Authentifizierung wären entsprechend zu überarbeiten (§ 33 Abs. 1 Nrn. 3 bis 5 KommHV-Doppik, § 39 Abs. 1 Nr. 3 KommHV-Doppik). Zudem muss stets nachvollziehbar sein, wer wann welche Daten erfasst oder verändert hat. Demnach sollten die Passwörter der Benutzerkonten nur dem jeweiligen Inhaber bekannt sein und nicht bei mehreren Benutzerkonten einheitlich verwendet werden.

Zur Verwendung von Standardpasswörtern bei privilegierten Benutzerkonten verweisen wir auf die Ausführungen unter TZ 14 c).

c) Einsatz von Schnittstellen und Wahrnehmung von Kontrollen

Soweit technisch möglich und organisatorisch sinnvoll, empfehlen wir grundsätzlich, Schnittstellen zwischen den Anwendungsverfahren und dem Kassenautomaten bzw. dem Kassenautomaten und dem eingesetzten Finanzverfahren zu nutzen. Dies hätte aus unserer Sicht folgende Vorteile:

- Etwaige Fehleingaben können vermieden werden, da die festzusetzenden Gebühren direkt im Zusammenhang mit der Vorgangsbearbeitung in den Anwendungsverfahren auf automatisiertem Wege ermittelt werden können.
- Die ordnungsgemäße und vollständige Gebührenfestsetzung könnte besser überwacht werden.
- Die vollständige und richtige Übergabe der Buchungsdaten wäre technisch sichergestellt.
-

Soweit sich eine automatisierte Lösung nicht anbietet, wären im Interesse der Kassensicherheit geeignete organisatorische Maßnahmen zu treffen (z.B. Archivierung der Zweitschrift der Stornoquittung), mit der die ordnungsmäßige und vollständige Festsetzung und Einzahlung der Gebühren sichergestellt wird. Zudem empfehlen wir zur Verbesserung der Kassensicherheit, künftig das Kassensoll anhand der Fallzahlen aus dem Anwendungsverfahren zu ermitteln und regelmäßig mit den erfassten Zahlungen abzugleichen.

d) Umgang mit Stornobuchungen

Allen stichprobenartig geprüften Benutzerkonten in CPS wurden die Rechte zur Stornierung von Zahlungen eingeräumt. Bislang wurde die darin enthaltene Programmfunktion „Stornierung im Vier-Augen-Prinzip“ nicht genutzt. Hierüber wäre technisch sichergestellt, dass die Stornierung einer Einzahlung nur möglich ist, wenn ein zweiter Beschäftigter diese freigibt.

Die Stadt sollte von dieser technischen Möglichkeit Gebrauch machen und damit künftig sicherstellen, dass Stornierungen grundsätzlich ausschließlich im Vier-Augen-Prinzip vorgenommen werden können. Soweit eine solche technische Umsetzung nicht zweckmäßig ist, wäre das Vier-Augen-Prinzip durch organisatorische Maßnahmen sicherzustellen (z.B. zweifach unterschriebene Stornoquittungen).

e) Technische Hinweise

Auf dem für den Betrieb des Kassenautomaten eingesetzten PC lief noch das vom Betriebssystemanbieter nicht mehr unterstützte Betriebssystem „Microsoft Windows 7 Professional“. Ein lokaler Virenschutz war nicht installiert. Die Netzwerkdosen, die für den Anschluss des Kassenautomaten dienten, waren vom Foyer aus für Beschäftigte sowie Bürger frei zugänglich.
Zu den angetroffenen Sachverhalten merken wir an:

- Da für das Betriebssystem Windows 7 Professional keinerlei Sicherheitsaktualisierungen mehr bereitgestellt und kein Support mehr geleistet wird, wäre dieses zeitnah durch ein aktuelles Betriebssystem abzulösen (vgl. auch TZ 15).

- Ein aktueller Virenschutz sollte auf allen Systemen im lokalen Netzwerk sichergestellt werden. Der Arbeitsplatzrechner sollte zeitnah ins örtliche Virenschutzkonzept eingebunden werden.

- Die Netzwerkanschlüsse des Kassenautomaten sollten zugriffsgeschützt gestaltet werden. Die Schnittstellen/Adapter des Automaten sollten nur den jeweils Befugten (mit administrativen Aufgaben beauftragten Beschäftigten) zugänglich sein (§ 39 Abs. 1 Nr. 3 KommHV-Doppik).

Die Finanzverwaltung nimmt dazu wie folgt Stellung:

Zu TZ 16 a) b) c) und d):

Aufgrund der Anregungen des Prüfungsverbandes wurde die Administration von der Stadtkasse in die Stadtkämmerei verlegt und so die Funktionstrennung gesichert. Die Anpassung der Anforderungen an die Kennwörter wird mit dem Anbieter des Automaten - dieser bietet auch das Programm „CPS 2.5" an - geklärt, ebenso die Möglichkeit einer Schnittstelle zum Finanzverfahren und Freischaltung der „Stornierung im Vier-Augen-Prinzip".

Das Verwaltungs- und Rechtsamt / SG IuK nimmt dazu wie folgt Stellung:

zu TZ 16 e):

Das Betriebssystem wurde ausgetauscht und der Computer in das zentrale Virenschutzmanagement eingebunden. Die offenen Netzwerkanschlüsse im Haus werden künftig mit einem Schloss versehen.

TZ 19 IT-Sicherheit in der Stadtbücherei

In der Stadtbücherei kamen mehrere Verwaltungs-PC sowie ein physikalisches Serversystem, das als Virtualisierungshost fungierte und mehrere virtuelle Serversysteme bereitstellte, zum Einsatz. Das Netzwerk der Stadtbibliothek war über eine VPN-Verbindung an das Verwaltungsnetzwerk der Stadt angebunden. Als Bibliotheksverwaltungsprogramm wurde „SISIS-SunRise" der Firma O. eingesetzt. Über die Internetseite der Bibliothek war ferner eine OPAC-Webauskunft (SISIS-SunRise webOPAC) realisiert, die Internetbenutzer zur Recherche und zur Reservierung der vorhandenen Medien in der Stadtbücherei nutzen konnten. Hierzu wurde auf einem virtuellen Server ein eigener Webserver betrieben. Alle o.g. Systeme befanden sich im gleichen Netzwerksegment und griffen auf den gleichen Internetanschluss zurück. Darüber hinaus kamen diverse öffentliche Internet-PC zum Einsatz, die lt. den erhaltenen Auskünften physikalisch vom Verwaltungsnetzwerk getrennt betrieben wurden und einen eigenen Internetanschluss nutzten. Für die Systembetreuung des dezentralen Domänennetzwerks in der Stadtbibliothek hat die Stadt mit der Firma A. einen externen IT-Dienstleister beauftragt.

In der Stadtbücherei war eine eigene Zahlstelle eingerichtet. Zahlungen wurden bar und mit EC-Karte entgegengenommen.

Zu den vorgefundenen Sachverhalten merken wir an:

a) Zugriff mehrerer Beschäftigter auf Kassenbehälter
Auskunftsgemäß hatten jeweils mehrere Beschäftigte Zugriff auf die einzelnen Kassenbehälter; die Kassenbehälter waren den Arbeitsplätzen, nicht aber den Personen zugeordnet. Dies galt ebenso für die Anmeldung am Fachverfahren „SISIS-SunRise. Hierzu wurden u.a. die funktionsbezogenen Benutzerkonten „term2“ und „term3“ verwendet.

Mit dieser Vorgehensweise kann ein etwaiger Kassenfehlbetrag nicht zugeordnet werden. Auf die einzelnen Bargeldbestände sollte nur der jeweils verantwortliche Beschäftigte Zugriff nehmen können (vgl. § 39 Abs. 1 KommHV-Doppik mit Verweis auf Erl. 2 zu § 43 KommHV-Kameralistik in Schreml/Bauer/Westner, a.a.O.). Hinsichtlich der Verwendung geteilter Benutzerkennungen verweisen wir auf unsere Ausführungen unter TZ 18 d).

b) Verstoß gegen den Grundsatz der Funktionstrennung

Beschäftigte, die mit Barkassengeschäften betraut waren, administrierten das eingesetzte Fachverfahren „SISIS-SunRise“. Dies widerspricht dem Grundsatz der Funktionstrennung (vgl. TZ 17 0. Die Administration des Fachverfahrens sollte nicht durch Beschäftigte vorgenommen werden, die mit Kassengeschäften betraut sind.

c) Absicherung des Webserver-Zugriffs

Die Tatsache, dass sich der o.g. Webserver im lokalen Netzwerk der Bibliothek zusammen mit den restlichen Verwaltungsarbeitsplatzrechnern befand und von diesen nicht durch entsprechende sicherheitstechnische Maßnahmen, wie z.B. dem Einrichten einer sog. demilitarisierten Zone (DMZ), getrennt war, ist als sicherheitskritisch anzusehen.

Die Serverdienste, welche extern vom Internet erreichbar bleiben sollen, sollten netzwerktechnisch in einer eigenen sog. demilitarisierten Zone (DMZ) betrieben werden. Damit wird eine sicherheitstechnische Trennung vom übrigen Verwaltungsnetzwerk erreicht. Der Sinn einer DMZ besteht darin, auf möglichst sicherer Basis Dienste eines Servers sowohl dem öffentlichen Weitverkehrsnetz (Internet) als auch dem lokalen Netzwerk zur Verfügung zu stellen und Zugriffe von Nutzern des Fremdnetzes in das lokale Netzwerk zu verhindern. Wir empfehlen, den Zugriff auf die OPAC-Webauskunft und den zugrundeliegenden Webserver künftig geeignet abzusichern.

d) Einschränkung von Zutrittsberechtigungen

Hinsichtlich der Zutrittsberechtigungen zum Serverraum verweisen wir auf unsere Ausführungen unter TZ 15 a).

e) Fehlender Wettbewerb bei der Auftragsvergabe

Aufträge zu kleineren IT-Beschaffungen wurden von der zuständigen Beschäftigten der Stadtbibliothek häufig an die bereits mit der Systembetreuung beauftragte Firma A. vergeben. Zum Teil stellte die Firma A. den Investitionsbedarf selbst fest, lieferte hierzu die erforderliche Hardware und erbrachte die für die Inbetriebnahme notwendigen ITDienstleistungen.

Verträge über Lieferungen und Leistungen im IT-Bereich unterhalb der maßgeblichen EU-Schwellenwerte (vgl. § 106 Abs. 2 Nr. 1 GWB, der auf Art. 4 der Richtlinie 2014/24/EU in der jeweils geltenden Fassung verweist) sind grundsätzlich im Wettbewerb zu vergeben (§ 30 Abs. 1 KommHV-Doppik). Dies gilt auch für die dauerhafte externe Systembetreuung.

Für die Ausnahmetatbestände kann auf die Ausnahmebestimmungen des GWB (vgl. Ziff. 2 der Bek des Bayerischen Staatsministeriums des Innern und für Integration über die Vergabe von Aufträgen im kommunalen Bereich vom 31.07.2018 [AllMBl S. 547], die zuletzt durch Bek vom 29.03.2022 [BayMBl Nr. 200] geändert wurde) und die in § 8 Abs. 3 und 4 UVgO angeführten Gründe zurückgegriffen werden. Selbst bei Verhandlungsvergaben soll ein Wettbewerb die Regel sein. Auch hier bleibt der Auftraggeber daher verpflichtet, mehrere - grundsätzlich mindestens drei - Unternehmen nach Prüfung ihrer Eignung zur Abgabe eines Angebots in Textform aufzufordern sowie bei Verhandlungen über den Angebotsinhalt, die im Ermessen des Auftraggebers stehen, alle Bieter gleich zu behandeln (vgl. Ziff. 1.2.5 IMBek 2018).

Ergänzend verweisen wir auf die Informationen zum Vergabe- und Vertragswesen in Bayern des Bayerischen Staatsministeriums für Wohnen, Bau und Verkehr sowie des Staatsministeriums für Wirtschaft, Landesentwicklung und Energie.7

Zu Buchstaben a) bis e):

Im Rahmen unserer Prüfung stellten wir fest, dass bei der Stadt nur rudimentäre Kenntnisse über die Konfiguration der IT-Komponenten in der Stadtbibliothek vorhanden waren. Grundsätzlich war für die Betreuung des dezentralen Domänennetzwerks in der Stadtbibliothek mit der Firma A. ein externer IT-Dienstleister beauftragt.

Nach unserer Auffassung wäre es aus wirtschaftlichen und sicherheitstechnischen Gesichtspunkten zweckmäßiger, das Verwaltungsnetzwerk der Stadtbibliothek in das lokale Netzwerk der Stadt einzubinden und die Administration durch eigenes Personal sicherzustellen. Als Vorteile sehen wir insbesondere:

- Mit der Übernahme der Administrationsaufgaben und laufenden Systembetreuung durch eigenes Personal könnten die Kosten für die Systembetreuung der Stadtbibliothek durch externe IT-Dienstleister vermieden oder zumindest reduziert und eine einheitliche Administration realisiert werden. Allein für die Systembetreuung durch den externen Dienstleister fielen zuletzt pro Jahr rd. 4 T€ an.
- Weiterhin könnten durch die Zusammenlegung beider Netzwerke ein einheitliches Datensicherungskonzept, ein zentrales Virenschutz-Management sowie ein einheitliches Update- und Patchmanagement über den bereits im Einsatz befindlichen WSUS bzw. die Softwareverteilungslösung Baramundi auf einfache Weise umgesetzt und somit Synergieeffekte erzielt werden.
- Daneben wären die Verwendung einheitlicher Gruppen- und Sicherheitsrichtlinien sowie die Einrichtung einer gemeinsamen Infrastruktur zur Dateiablage möglich.
- Auch Beschaffungsvorgänge zur Hard- und Softwareausstattung könnten künftig unter einheitlichen Gesichtspunkten und der fachlichen Begleitung des Sachgebiets IuK durchgeführt und wirtschaftlich sowie vergaberechtskonform umgesetzt werden.

Das Verwaltungs- und Rechtsamt / SG IuK nimmt dazu wie folgt Stellung:

zu TZ 19 a)-e):

Bisher wird die Stadtbibliothek durch einen externen Dienstleister betreut.
Eine Übernahme und Integration in die städtische IT durch das SG IuK ist zu prüfen, auch hinsichtlich der personellen Möglichkeiten.

TZ 22 c)

Hinweise zum Eigenbetrieb SHG

Der Oberbürgermeister besaß eine Einzelverfügungsberechtigung über das Girokonto Nr. 2500710 bei der VR-Bank Fürstenfeldbruck eG.

Zur Vermeidung von Wiederholungen verweisen wir auf die Ausführungen unter Buchst. a). Die Einzelverfügungsberechtigung des Oberbürgermeisters wäre zu widerrufen. Bei dieser Gelegenheit wären auch die (gemeinschaftlichen) Verfügungsberechtigungen der bereits ausgeschiedenen Mitarbeiterin V.S. (Girokonto und EBICS) zu stornieren.

Der Eigenbetrieb Stadthalle nimmt dazu wie folgt Stellung:

Zu TZ 22 c):

Der Oberbürgermeister war aus nicht nachvollziehbaren Gründe als verfügungsberechtigt angelegt, dies wurde umgehend korrigiert.

*Beim Ausscheiden von Mitarbeiter*innen der Stadthalle werden die Kontovollmachten gelöscht, auch die DATEV-Nutzung zur elektronischen Unterschrift, die ohnehin nur von zwei Personen gemeinschaftlich genutzt werden kann, ist nach dem Ausscheiden von Mitarbeiter*innen nicht mehr möglich. Unterschriftsvollmachen werden bei jedem Mitarbeiter*innenwechsel nicht gelöscht oder ergänzt, sondern komplett neu erstellt.*

TZ 36 Ermittlung und Verrechnung von Verwaltungskostenbeiträgen
Im Rahmen unserer Prüfung haben wir auch die von der Stadt verrechneten Verwaltungskostenbeiträge näher untersucht. Die Verwaltungskostenbeiträge wurden örtlich in einem aufwendigen Verfahren anhand tatsächlicher Kosten ermittelt.

Dabei stellten wir Folgendes fest:

- Bei der Berechnung der Verwaltungskostenbeiträge an den Eigenbetrieb SWG (zuletzt rd. 111 T€) berücksichtigte die Stadt anteilige Personal- und Gemeinkosten, jedoch keine Sachkosten des Büroarbeitsplatzes.

- Bei der Berechnung der Verwaltungskostenbeiträge an den Eigenbetrieb SHG (zuletzt rd. 13 T€) berücksichtigte die Stadt weder anteilige Personalkosten noch Sachkosten des Büroarbeitsplatzes, sondern lediglich Gemeinkosten in geringfügigem Umfang (u.a. für Sitzungsdienst

und Weihnachtsfeier). Zusätzlich wurde noch ein Pauschalbetrag von 15.350 € vereinnahmt. Dieser ergab sich durch Verrechnung mit dem an die SHG für die Inanspruchnahme der Werkleiterin als städtische Kulturamtsleiterin zu leistenden Personalkostenersatz in entsprechender Höhe. Die Ermittlung des Betrags konnte nicht mehr nachvollzogen werden.

- Außer in den o.a. Fällen wurden bislang keine weiteren Verwaltungskostenbeiträge haushaltsmäßig durchgebucht (z.B. an die kostenrechnende Einrichtung „Bestattungswesen").

Hierzu stellen wir fest:

Bei der Berechnung von Verwaltungskostenbeiträgen sollte immer auch Aufwand und Nutzen beachtet werden. Damit die Berechnung unter wirtschaftlichen Aspekten durchgeführt werden kann, ist es häufig sinnvoll, nicht die individuellen Verhältnisse eines jeden Stelleninhabers und Arbeitsplatzes in die Berechnung einfließen zu lassen, sondern die Kosten des Arbeitsplatzes anhand von Pauschalwerten zu ermitteln. Aus Wirtschaftlichkeitsgründen dürfte nach unseren überörtlichen Erfahrungen einer pauschalen Ermittlung von Verwaltungskostenbeiträgen grundsätzlich der Vorrang gegenüber einer tendenziell aufwendigeren Berechnung anhand tatsächlicher Kosten einzuräumen sein.

Hilfreiche Ausführungen zur pauschalen Ermittlung von Arbeitsplatzkosten enthält unser Geschäftsberichtsbeitrag 2013, S. 33 ff., „Kosten eines Arbeitsplatzes im Öffentlichen Dienst". Dieser sieht für die Gemeinkosten einen pauschalen Zuschlag von 20 % auf die Personalkosten und für jeden Büroarbeitsplatz eine Sachkostenpauschale von derzeit 9.570 € vor, wovon 5.970 € auf die sonstigen Sachkosten (Raum-, Büro-, Geschäftskosten) und 3.600 € auf die IT-Kosten entfallen. Die Personalkosten wiederum können anhand der regelmäßig in der Fachzeitschrift „Die Gemeindekasse" veröffentlichten Personaldurchschnittskosten ermittelt werden (vgl. z.B. GK 68/2019 und 187/2019). Die auf die vorstehend genannten Größen anzuwendenden individuellen Zeitanteile wären sodann (wie örtlich geschehen) durch die betreffenden Mitarbeiter sorgfältig zu schätzen.

Die Stadt sollte die Verwaltungskosten künftig nach einem einheitlichen Schema ermitteln und vollständig und nachvollziehbar an die kostenrechnenden Einrichtungen und Eigenbetriebe weiter verrechnen. Dabei wäre künftig auch ein sachgerechter Ansatz für die Kosten des Büroarbeitsplatzes zu berücksichtigen. Zudem empfehlen wir der Stadt zu prüfen, ob eine pauschalierte Ermittlung der Verwaltungskostenbeiträge anstelle einer Berechnung anhand tatsächlicher Kosten nicht zu ebenso sachgerechten Ergebnissen führten wurde. Die pauschale Verrechnung des an die SHG für die Werkleiterin zu zahlenden Personalkostenersatzes mit den von der Stadt zu erhebenden Verwaltungskosten wäre einzustellen und die Leistungen wären künftig getrennt voneinander und nachvollziehbar abzurechnen.

Die Finanzverwaltung nimmt dazu wie folgt Stellung:

<u>zu TZ 36:</u>

Die Stadtkämmerei prüft derzeit, inwieweit die Personalsätze aus „Die Gemeindekasse" von den bisher verwendeten Maßstäben abweichen.

Die Umstellung auf die vom Prüfungsverband vorgeschlagene Vereinfachung – sie betrifft vor allem die Abrechnung mit den Eigenbetrieben – wird zu gegebener Zeit erfolgen (Beachtung von Kalkulationszeiträumen).

Die Bearbeitung der noch ausstehenden Prüfungserinnerungen und Feststellungen wird im Rahmen der nächsten Sitzungen des Hauptausschusses öffentlich oder nicht öffentlich zur Beschlussfassung vorgelegt.

Beschlussvorschlag:

Der Hauptausschuss nimmt die Ausführungen der Verwaltung zur Kenntnis. Die Prüfungsfeststellungen zu den Ziffern 12 a)-e), 13, 14 a)-d), 15 a)-f), 16 a)-e), 19 a)-e), 22 c) und 36 im allgemeinen überörtlichen Prüfbericht sind hiermit erledigt.

Mroncz Rene / Sperber Markus / Schütze Bettina genehmigt OB