STADTRECHNUNGSHOF
WIEN

MA 01, Prüfung der Organisation der Fernwartung von IKT-Systemen

StRH I - 677982-2023

Impressum

Stadtrechnungshof Wien
Landesgerichtsstraße 10
1082 Wien
Telefon: +43 1 4000 82911
E-Mail: post@stadtrechnungshof.wien.at
www.stadtrechnungshof.wien.at

Der vorliegende Bericht ist ein Beitrag für den StRH Wien - Tätigkeitsbericht 2024.

Kurzfassung

Die MA 01 - Wien Digital war gemäß Geschäftseinteilung für den Magistrat der Stadt Wien für alle Belange der IKT der Stadt Wien zuständig. Darunter fiel auch die Fernwartung von IKT-Systemen und die damit verbundene Organisation der Verwaltung und des Betriebes der dafür notwendigen operativen wie technischen Infrastruktur.

Der StRH Wien überprüfte die Organisation der Fernwartung von IKT-Systemen hinsichtlich ihrer Vorgaben, ihrer Aufbau- und Ablauforganisation sowie ihrer operativen Umsetzung im Rahmen einer gesamtheitlichen Organisationsprüfung.

Die Abbildung und Umsetzung des Regelwerkes (Policy) der MA 01 - Wien Digital bzgl. der Fernwartung wurde anhand der gesetzlichen Grundlagen sowie der Vorgaben der Stadt Wien überprüft. Dazu wurden in weiterer Folge die Aufbau- und Ablauforganisation, die Überwachung und die operativ-technische Umsetzung durch Datenanalysen, Vor-Ort-Einschauen und stichprobenartige Überprüfungen beurteilt.

Keine Aussagen wurden vom StRH Wien zu Inhalten und Zielerreichungen der einzelnen vertraglich geregelten Fernwartungen getroffen. Die Fernwartung der Betriebstechnik (Operational Technologie-Systeme bzw. OT-Systeme) wurde ausschließlich hinsichtlich deren Regelungen in die Prüfung miteinbezogen.

Aufgrund von aufgetretenen Auffälligkeiten bei der Informationssicherheit bzw. beim Datenschutz im Zuge der Dokumentenrecherche wurde der Prüfungsgegenstand um die Aufarbeitung und Überprüfung dieses Sicherheitsvorfalles erweitert. Basierend auf den Ergebnissen dieser Prüfung begann die MA 01 - Wien Digital entsprechende Maßnahmen umzusetzen.

Dem StRH Wien lagen Zertifikate über das Informationssicherheitsmanagement und das Business Continue Management sowie Dokumente zu Testaten der ISAE 3402 (Regelungen zur Prüfung des IKS einer Dienstleistungsorganisation) vor.

Die Prüfung des StRH Wien ergab, dass ein grundlegendes Regelwerk zur Fernwartung (Fernwartungspolicy mit weiteren detailisierenden Regelungen) der MA 01 - Wien Digital vorlag. Hinsichtlich der Fernwartungspolicy wurden Verbesserungen in den zugrunde lie-

genden Soll-Vorgaben, den Inhalten, der Struktur und der Konsistenz sowie der ordnungsgemäßen Dokumentation gemäß Büroordnung der Stadt Wien und Akten- und Skartierungsplan festgestellt und dementsprechende Empfehlungen ausgesprochen. Des Weiteren wurde die zeitnahe Fertigstellung der Loggingpolicy empfohlen.

Eine Vor-Ort-Einschau zeigte unterschiedliche Aufbewahrungszeiträume in der Überwachungsdokumentation zur Fernwartung auf. Diese standen im Zusammenhang zur bereits angesprochenen Loggingpolicy. Eine unangekündigte Vor-Ort-Überprüfung der Verwaltung des Datums von gültigen Fernwartungsusern im führenden IKT-System ergab keine Beanstandungen. Im Rahmen der Vor-Ort-Einschau ins Security Information und Event Management sowie einer vom StRH Wien durchgeführten Datenanalyse wurden von der MA 01 - Wien Digital Verbesserungen erkannt und zur Evaluierung aufgenommen.

Der StRH Wien sprach ferner Empfehlungen hinsichtlich der Fernwartung der Betriebstechnik (Operational Technologie-Systeme) bezüglich der organisatorischen wie technischen Anforderungen in den zugrunde liegenden Regelungen und der vollständigen Erfassung von derartigen Systemen aus.

Der StRH Wien unterzog die Organisation der Fernwartung von IKT-Systemen durch die MA 01 - Wien Digital einer stichprobenweisen Prüfung und teilte das Ergebnis seiner Wahrnehmungen nach Abhaltung einer diesbezüglichen Schlussbesprechung der geprüften Stelle mit. Die von der geprüften Stelle abgegebene Stellungnahme wurde berücksichtigt. Allfällige Rundungsdifferenzen bei der Darstellung von Berechnungen wurden nicht ausgeglichen.

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
Art.	Artikel
A-SIT	A-SIT Zentrum für sichere Informationstechnologie - Austria
BCM	Business Continue Management
BGBl.	Bundesgesetzblatt
bspw.	beispielsweise
bzgl.	bezüglich
bzw.	beziehungsweise
ca.	circa
CERT	Computer Emergency Response Team
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
ELAK	Elektronischer Akt
E-Mail	Elektronische Post
EU	Europäische Union
Ggf.	gegebenenfalls
GmbH	Gesellschaft mit beschränkter Haftung
GZ	Geschäftszahl
Hrsg.	Herausgeber
html	Hypertext Markup Language
https	Hypertext Transfer Protocol Secure
ID	Identifikationsnummer
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IKT	Informations- und Kommunikationstechnologie
inkl.	inklusive
ISAE	International Standard on Assurance Engagements
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Informationstechnik
lt.	laut
Ltd.	Limited
MA	Magistratsabteilung

MC	Metadaten und Content
MDK	Magistratsdirektion - Gruppe Koordination
MD-OS	Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit
MD-OS/PIKT	Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Prozessmanagement und IKT-Strategie
NIS	Netz- und Informationssicherheit
NISG	Netz- und Informationssicherheitsgesetz
NISV	Netz- und Informationssicherheitsverordnung
Nr.	Nummer
o.a.	oben angeführt
OT	Operational Technology
PAM	Privilege Access Management
rd.	rund
RFC	Request for Comments
s.	siehe
SAP CCoe	Customer Center of Expertise
SAP IS-H	Industry Solution - Healthcare
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
sog.	sogenannte
StRH	Stadtrechnungshof
u.a.	unter anderem
usw.	und so weiter
VZÄ	Vollzeitäquivalent
Wiener Gesundheitsverbund	Unternehmungen Wiener Gesundheitsverbund
WiGeV	Wiener Gesundheitsverbund
WStV	Wiener Stadtverfassung
www	World Wide Web
z.B.	zum Beispiel
z.T.	zum Teil

Literaturverzeichnis

Big Bird Westfalen, Kreis Soest, Büro der Landrätin, Presse und Medien (22. September 2023). *Friendly User Test*, abgerufen am 22. September 2023 von https://bigbirdwestfalen.nrw/friendly-user-test/#:~:text=Was%20ist%20ein%20Friendly%20User,es%20f%C3%BCr%20alle%20erh%C3%A4ltlich%20ist.

Bradner, S. (März 1997). *RFC 2119 Key words for use in RFCs to Indicate Requirement Levels*. (I. Datatracker, Herausgeber), abgerufen am 20. November 2023 von https://datatracker.ietf.org/doc/rfc2119/

Bundesamt für Sicherheit in der Informationstechnik. (2023). *IT-Grundschutz-Bausteine,* abgerufen am 2. August 2023 von https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html

Bundeskanzleramt Österreich. (23. Februar 2023). *Österreichisches Informationssicherheitshandbuch,* abgerufen am 2. August 2023 von https://www.sicherheitshandbuch.gv.at

Bundeskanzleramt, Bundesministerium für Inneres. (9. September 2023). *Fragen und Antworten, Für Betreiber wesentlicher Dienste*, abgerufen am 9. September 2023 von https://www.nis.gv.at/fragen-und-antworten/fuer-betreiber-wesentlicher-dienste.html

Bundeskanzleramt; Bundesministerium für Inneres. (2023). *Rechtliches und Dokumente,* abgerufen am 10. August 2023 von https://www.nis.gv.at/rechtliches-und-dokumente.html

Bundesministerium für Finanzen; A-SIT Zentrum für sichere Informationstechnologie - Austria. (25. Juli 2022). *WienCERT,* abgerufen am 9. August 2023 von https://www.onlinesicherheit.gv.at/Themen/Erste-Hilfe/CERTs/WienCERT.html

Codemi GmbH. (2023). *Werktage Rechner*, abgerufen am 7. Dezember 2023 von https://www.ferienwiki.at/tools/werktagerechner

Cyberark Software Ltd. (21. November 2023). *Was ist PAM? Privileged Access Management erklärt*, abgerufen am 21. November 2023 von https://www.cyberark.com/de/what-is/privileged-access-management/

Internationale Organisation für Normung. (9. September 2023). *Was ist ISO/IEC 27001*, abgerufen am 9. September 2023 von https://www.iso.org/standard/27001

ITwissen.info. (2023). *Betriebstechnik.* (D. B. GmbH, Hrsg.), abgerufen am 2. August 2023 von https://www.itwissen.info/Betriebstechnik-operational-technology-OT.html

PwC. (2023). *Continous Auditing*, abgerufen am 28. November 2023 von https://www.pwc.com/vn/en/services/consulting/continuous-audit-monitoring.html

StepStone Deutschland GmbH. (2023). *Service Delivery Manager*, abgerufen am 30. November 2023 von https://www.gehalt.de/beruf/service-delivery-manager

Sursaieva, A. (14. Juni 2023). *Difference between generic and customized software product*. (Axon, Hrsg.), abgerufen am 24. November 2023 von https://www.axon.dev/blog/difference-between-generic-and-customized-software-product

Wikipedia. (10. Oktober 2022). *Benutzerrolle*, abgerufen am 9. September 2023 von https://de.wikipedia.org/wiki/Benutzerrolle

Wikipedia. (8. Juli 2022). *Hotfix,* abgerufen am 7. August 2023 von https://de.wikipedia.org/wiki/Hotfix

Wikipedia. (10. Oktober 2022). *ISO/IEC-27000-Reihe*, abgerufen am 11. August 2023 von https://de.wikipedia.org/wiki/ISO/IEC-27000-Reihe

Wikipedia. (6. Juli 2023). *Anwendungsfall*, abgerufen am 23. November 2023 von https://de.wikipedia.org/wiki/Anwendungsfall

Wikipedia. (28. März 2023). *Bastion Host*, abgerufen am 10. August 2023 von https://de.wikipedia.org/wiki/Bastion_Host

Wikipedia. (11. Mai 2023). *Betriebliches Kontinuitätsmanagement*, abgerufen am 17. Oktober 2023 von https://de.wikipedia.org/wiki/Betriebliches_Kontinuit%C3%A4tsmanagement

Wikipedia. (13. September 2023). *Beurteilung eines binären Klassifikators*, abgerufen am 23. November 2023 von https://de.wikipedia.org/wiki/Beurteilung_eines_bin%C3%A4ren_Klassifikators

Wikipedia. (8. Juli 2023). *Content Management System.* (Wikipedia, Hrsg.), abgerufen am 8. August 2023 von https://de.wikipedia.org/wiki/Content-Management-System

Wikipedia. (22. März 2023). *Dashboard*, abgerufen am 29. November 2023 von https://de.wikipedia.org/wiki/Dashboard_(Informationsmanagement)

Wikipedia. (30. Oktober 2023). *Defense in depth (computing)*, abgerufen am 23. November 2023 von https://en.wikipedia.org/wiki/Defense_in_depth_(computing)

Wikipedia. (1. Juni 2023). *Dispatcher*, abgerufen am 22. September 2023 von https://de.wikipedia.org/wiki/Dispatcher

Wikipedia. (6. April 2023). *ISAE 3402*, abgerufen am 4. September 2023 von https://de.wikipedia.org/wiki/ISAE_3402

Wikipedia. (3. August 2023). Logging, abgerufen am 29. September 2023 von https://de.wikipedia.org/wiki/Logging

Wikipedia. (27. Februar 2023). *Monitoring,* abgerufen am 2. August 2023 von https://de.wikipedia.org/wiki/Monitoring
Wikipedia. (13. Juli 2023). *Plattform (Computer)*, abgerufen am 25. September 2023 von https://de.wikipedia.org/wiki/Plattform_(Computer)
Wikipedia. (30. Mai 2023). *Programmfehler,* abgerufen am 7. August 2023 von https://de.wikipedia.org/wiki/Programmfehler
Wikipedia. (13. September 2023). *Request for Comments*, abgerufen am 16. Oktober 2023 von https://de.wikipedia.org/wiki/Request_for_Comments
Wikipedia. (11. Oktober 2023). *Service Level Agreement*, abgerufen am 17. Oktober 2023 von https://de.wikipedia.org/wiki/Service-Level-Agreement
Wikipedia. (13. Juni 2023). *Support*, abgerufen am 22. September 2023 von https://de.wikipedia.org/wiki/Support_(Dienstleistung)
Wikipedia. (27. Juli 2023). *Verfügbarkeit*, abgerufen am 17. Oktober 2023 von https://de.wikipedia.org/wiki/Verf%C3%BCgbarkeit
Wikipedia. (1. April 2023). *Widget,* abgerufen am 7. August 2023 von https://de.wikipedia.org/wiki/Widget

Glossar

BCM

Unter dem BCM werden in der Betriebswirtschaftslehre die Überlegungen zu den Strategien, Prozessen und Maßnahmen verstanden, die die Unterbrechung des üblichen und normalen Betriebsablaufes mit alternativen Abläufen und Handlungsmaßnahmen schützen bzw. weitestgehend aufrechterhalten.

Betriebstechnik bzw. OT

Bei der Betriebstechnik bzw. OT geht es um Hard- und Software für die Überwachung, Verwaltung und Kontrolle von physikalischen Geräten, Prozessen und Ereignissen von Anlagen und Systemen im industriellen Umfeld. Die Betriebstechnik bzw. OT umfasste in der MA 01 - Wien Digital auch entsprechende medizinische Anlagen und Systeme.

Content Management System

Unter einem Content Management System wird eine Software zur gemeinschaftlichen Erstellung, Bearbeitung, Organisation und Darstellung digitaler Inhalte zumeist für Internet- bzw. Intranetseiten verstanden.

Continuous Auditing

Unter „Continuous Auditing“ wird der Ansatz von Audits verstanden, welcher auf einer kontinuierlichen Basis prüferische Aktivitäten durchführt. In der Regel umfasst dieser Ansatz die Komponenten der Risikoüberwachung mit z.B. entsprechenden Key Performance Indicators, der Kontrollüberwachung, der Transaktions- oder Aktivitätsüberwachung, der Untersuchung potenziell unangemessener Aktivitäten, die festgestellt wurden sowie der Berichterstattung an die Stakeholder.

Dashboard

Unter einem Dashboard wird eine grafische Benutzeroberfläche verstanden, die zur Visualisierung von Daten und Informationen bzw. Key Performance Indicators dient.

Defense in Depth

Unter „Defense in Depth“ wird ein Konzept der Cybersicherheitsstrategie zur Informationssicherheit verstanden, bei der in mehreren Kontrollebenen entsprechende Sicherheitsmechanismen zur Erkennung, Überwachung und Verteidigung in einem IT- bzw. IKT-System oder IT- bzw. IKT-Verbund angeordnet sind. Durch die Staffelung derartiger Ebenen wird

eine entsprechende Redundanz für den Ausfall oder das Überwinden der jeweiligen Ebene sichergestellt. Die Ebenen umfassen dabei die Aspekte der personellen, prozessualen, technischen und physischen Sicherheit für den gesamten Lebenszyklus des Systems.

Dispatcher

Unter einem Dispatcher wird die Funktion einer Person verstanden, die im sachlichen Kontext der Aufgabenstellung - wie z.B. des IT-Service-Managements - den optimalen Einsatz der Mittel und den Informationsfluss zur Abwicklung, Bearbeitung und Behebung der gegenständlichen Thematik sicherstellt.

False Positive

Ein „False Positive“ ist eine Art der Fehlerklassifikation in z.B. einem Softwareprozess, welche eine falsch durchgeführte Beurteilung eines Parameters als richtig ausweist. Eine „False Positive“ Fehlerklassifikation stellt neben der weiteren „False Negative“ Fehlerklassifikation Ergebnisse dar, die die ordnungsgemäße Funktion bzw. dieses Ablaufes infrage stellen.

Friendly User

Unter „Friendly User“ werden Personen verstanden, die dem zu testenden Produkt bzw. der für das Produkt verantwortlichen Stelle freundlich und positiv eingestellt bzw. gesinnt sind und entsprechendes Feedback zum Produkt vor der offiziellen Bereitstellung bzw. Verwendung geben.

generisch

Unter „generisch“ (wie „generische Software“, „generische Programmierung“ oder „generischer Use Case“) wird in der Informatik ein entwickeltes Produkt verstanden, welches allgemeingültig von Organisationen in verschiedenen Arbeitsbranchen und Arbeitsbereichen mit gleichen Aufgabenstellungen oder mit Anforderungen eines breiten Benutzerspektrums verwendet werden kann.

Incident

Unter einem Incident wird eine Qualitätsminderung oder eine nicht geplante Unterbrechung einer Applikation, eines Services oder Systems verstanden.

Jump Server bzw. Jump Host

Unter einem Jump Server bzw. Jump Host wird ein Server (oder System) verstanden, welcher Dienste für die Verwaltung und den Zugriff eines separaten Bereiches oder einer Sicherheitszone zum öffentlichen Internet oder nicht vertrauenswürdigen anderen Netzumgebungen bereitstellt.

Log bzw. Logging

Unter einem Log bzw. dem Logging wird die automatische Erstellung und Aufzeichnung von Daten zu Ereignissen (Events) in Softwareprozessen von Systemen oder Anwendungen verstanden. Der Log bzw. das Logging dient der revisionssicheren Nachvollziehbarkeit der Zustände (z.B. dem Zugriff) oder Fehler (z.B. Performance) im Softwareprozess von Systemen und Anwendungen.

Mitarbeitendenrolle

Unter einer Mitarbeitendenrolle wird eine zusammenfassende Menge an einzelnen Rechten in einer Software, einem Service oder System verstanden. Diese Vorgangsweise erleichtert ein effizientes und effektives Rechtemanagement des jeweiligen Users.

Monitoring

Unter Monitoring wird die systemische Überwachung und Protokollierung von Vorgängen oder Prozessen mit technischen Hilfsmitteln oder Beobachtungssystemen verstanden.

Normenserie EN ISO/IEC 27000

Die Normenserie der EN ISO/IEC 27000 ist eine Reihe von Standards zur Informationssicherheit im Kontext der Implementierung und des Betriebes eines ISMS.

Privileged Access Management

Unter dem „Privileged Access Management“ wird die umfassende Cybersicherheitsstrategie einer Kontrolle, Überwachung, Sicherung und Prüfung der menschlichen und maschinellen privilegierten Identitäten und Aktivitäten in der geschäftlichen IT- bzw. IKT-Umgebung der Mitarbeitenden, Prozesse und Technologien verstanden. Privilegiert menschliche Identitäten umfassen u.a. Administratorenrollen und Administratorenkonten, Domänenadministratoren, Datenbankadministratoren und Root-Zugriffe.

RFC

Unter einem RFC wird in der Regel eine diskutierte, begutachtete und von der IETF herausgegebene technische Spezifikation meist im Zusammenhang mit dem Internet verstanden.

RFC 2119 - Schlüsselwörter zur Verwendung und zur Angabe von Anforderungsniveaus

In dieser Spezifikation werden Schlüsselwörter in Großbuchstaben wie z.B. MUSS, DARF NICHT/DARF NUR/DARF WEDER …NOCH, SOLL/SOLL NICHT/SOLL KEIN, KANN definiert, welche das Niveau und die Priorität der Anforderungen und der kompensierenden Maßnahmen für die Umsetzung in dem entsprechenden Text standardisieren, darlegen und verdeutlichen.

Service Delivery Manager

Unter einem Service Delivery Manager wird die Schnittstelle zwischen der Steuerung der internen Abläufe zur Erbringung von Dienstleistungen - meist IT- bzw. IKT-Serviceleistungen - und der Kundin bzw. dem Kunden verstanden.

Service Level Agreement

Unter einem Service Level Agreement wird ein Vertrag zwischen einer Dienstleistungsanbieterin bzw. einem Dienstleistungsanbieter und dessen Kundinnen bzw. Kunden verstanden. In diesem Vertrag sind entsprechende Dienstleistungsstandards definiert.

Software Plattform

Unter einer Software Plattform wird eine einheitliche Grundlagenebene von verschiedenen Softwaremechanismen bzw. Softwarekomponenten verstanden. Daraus resultieren entsprechende Softwareprodukte, die zur Verfügung gestellt werden.

Use Case

Unter einem „Use Case“ wird ein Anwendungsfall verstanden, der alle möglichen Szenarien mit einem Akteur mit einem betroffenen System zu einer Erreichung eines bestimmten Zieles beschreibt. Dabei wird der Anwendungsfall in der Zielerreichung insbesondere von konkret technischen Lösungen abstrahiert und dargelegt.

Verfügbarkeit

Die Verfügbarkeit ist eine Kennzahl eines technischen Systems, wann das System für seinen Zweck operativ im Verhältnis zur jeweiligen Bezugszeit - meist ein Kalenderjahr - zur

Verfügung gestanden ist. In diesem Zusammenhang ist anzumerken, dass dabei geplante sowie ungeplante Nichtverfügbarkeiten berücksichtigt werden. Nur eine ungeplant auftretende Nichtverfügbarkeit wird als Ausfallszeit gerechnet.

Widget

Ein Widget ist eine mittels Fenstertechnik („window“) verfügbare Komponente („gadget“) einer grafischen Benutzeroberfläche zur Anzeige und Speicherung von Daten bzw. Informationen.

WienCERT

Das WienCERT ist eine Stelle der MA 01 - Wien Digital im Auftrag der Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, die sich als zentrale Anlaufstelle mit technischen und organisatorischen Fragen zur IKT-Sicherheit in der Stadt Wien befasst.

2nd-Level-Support

Unter dem 2nd-Level-Support wird die Betreuung und Unterstützung der Kundinnen bzw. Kunden in der 2. Ebene verstanden. Durch diese 2. Ebene wird der 1st-Level-Support (1. Ebene) durch eine erweiterte und vertiefende Expertise für die Bearbeitung von komplexeren Anfragen unterstützt.

Prüfungsergebnis

1. Prüfungsgrundlagen des StRH Wien

1.1 Prüfungsgegenstand

Die Entscheidung zur Durchführung der gegenständlichen Prüfung wurde in Anwendung der risikoorientierten Prüfungsthemenauswahl des StRH Wien getroffen.

Gegenstand der vorliegenden Prüfung war die Organisation der Fernwartung von IKT-Systemen des Magistrats der Stadt Wien bei den erforderlichen Wartungstätigkeiten des geplanten regulären und kontinuierlich aufrechtzuerhaltenden Geschäftsbetriebes von IKT-Systemen. Diese Organisationsprüfung umfasste die Darstellung und Prüfung der Vorgaben (u.a. Gesetze, Verordnungen, Dienstanweisungen, Policies, Zertifizierungen, vertragliche Vereinbarungen der Fernwartung, Standards), die zugrunde gelegte Aufbau- und Ablauforganisation (u.a. die Organisationsstruktur und die Prozesse), das eingesetzte interne und externe Personal, die statistische Analyse sowie das Monitoring und das Audit bei Fernwartungen.

Nicht Gegenstand der Prüfung war die Organisation der Fernwartung von IKT-Systemen des Magistrats der Stadt Wien im Rahmen der Krisenvorsorge von nicht regulären Betriebszuständen oder des Betriebsausfalles durch ungeplante Ereignisse wie Katastrophen, Unfälle oder Cyberangriffe. Des Weiteren wurden bzgl. der Fernwartung im industriellen Umfeld der Betriebstechnik bzw. OT nur deren Regelungen in die Prüfung einbezogen. Außerdem wurden die Vergabe von Beschaffungen der Hard- und Software und juristische Aspekte der Wartungsverträge, des Datenschutzes und der Haftung bei der Fernwartung von IKT-Systemen nicht überprüft.

Im Zuge der Prüfungsvorbereitung traten Auffälligkeiten in Bezug zur Informationssicherheit bzw. des Datenschutzes von Daten bzw. Informationen auf und der Prüfungsgegenstand wurde daher um die Aufarbeitung und Überprüfung dieser aufgetretenen Auffälligkeiten und deren Umstände erweitert.

1.2 Prüfungszeitraum

Die gegenständliche Prüfung wurde im 2. Halbjahr 2023 von der Abteilung Kultur und Bildung des StRH Wien durchgeführt. Das Eröffnungsgespräch mit der geprüften Stelle fand am 29. Juni 2023 statt. Die Schlussbesprechung wurde am 3. Jänner 2024 durchgeführt.

Der Betrachtungszeitraum umfasste die Jahre 2020 bis 2022, wobei gegebenenfalls bzw. notwendigerweise auch spätere bzw. aktuelle Entwicklungen in die Prüfung bzw. Einschau einbezogen wurden.

Die Prüfungshandlungen umfassten Internet-, Intranet- und Literaturrecherchen sowie deren Analyse, Interviews und Besprechungen, Dokumentenanalysen und Datenanalysen bei der geprüften Stelle. Ein Ortsaugenschein fand am 5. Juli 2023 und am 6. Oktober 2023 in der MA 01 - Wien Digital statt.

Der StRH Wien führte ferner am 5. Dezember 2023 eine Prüfung an Ort und Stelle ohne vorige Anmeldung bei der MA 01 - Wien Digital gemäß Geschäftsordnung für den Magistrat der Stadt Wien Anhang I Sonderbestimmungen für das Kontrollamt § 4 Abs. 2 durch.

Die geprüfte Stelle legte die geforderten Unterlagen überwiegend zeitgerecht vor. Aufgrund der aktuellen Entwicklungen bei den regulatorischen Grundlagen und der dazu laufenden Arbeiten durch die MA 01 - Wien Digital ergaben sich Verzögerungen im Prüfungsablauf.

1.3 Prüfungsbefugnis

Die Prüfungsbefugnis für diese Gebarungsprüfung ist in § 73b Abs. 1 WStV festgeschrieben.

1.4 Vorberichte

Zum gegenständlichen Prüfungsgegenstand lagen dem StRH Wien für die vergangenen 10 Jahre keine ausschließlich diesem Prüfungsgegenstand zugeordneten und relevanten Prüfungsberichte vor.

2. Feststellungen und Empfehlungen im Rahmen der Prüfungsvorbereitung

2.1 Verdacht eines Sicherheitsvorfalles

Im Rahmen der Prüfungsvorbereitungen des StRH Wien zur gegenständlichen Prüfung wurden im Zuge der Ausarbeitung des Prüfungskonzeptes inhaltliche Erstrecherchearbeiten im Intranet der Stadt Wien durchgeführt.

Dabei wurden über die Suchfunktion des internen Intranetservices der Stadt Wien elektronische Dokumente - mit inhaltlichem Bezug zum Prüfungsgegenstand - aufgefunden, die infolge der gewährten Zugriffs- und Downloadberechtigung, der angezeigten Strukturierung und Bezeichnung des Ablageortes und des letztlich dargelegten Inhaltes der Dokumente den Verdacht von falsch gesetzten Zugriffsberechtigungen für nicht in dieser Form ausgewiesene, aufruf- und downloadbare elektronische Dokumente darlegten.

Am 25. Mai 2023 wurde vom StRH Wien per elektronischer Meldung ein Sicherheitsvorfall mit dem Verdacht auf falsch gesetzter Zugriffsberechtigungen an den zuständigen Servicedesk der MA 01 - Wien Digital übermittelt. Diese Meldung wurde am gleichen Tag als Incident mit entsprechendem Ticket im IT-Service-Management erfasst und dokumentiert. Am selbigen Tag wurde der gemeldete Sicherheitsvorfall mit der Meldung *„…folgender Information gelöst: Ma01 Datenschutz wurde per E-Mail kontaktiert“* als gelöst rückgemeldet.

Am 29. Juni 2023 wurden durch den StRH Wien - vor dem an diesem Tag zur gegenständlichen Prüfung stattfindenden Eröffnungsgespräch - die Suche und der Zugriff in der bereits beschriebenen Weise wiederholt. Der Zugriff war in dieser - wie vorher beschriebenen - Weise auf die gleichen Dokumente möglich.

Im Zuge des Eröffnungsgespräches wurde dieser Umstand angesprochen und der Zugriff live vor Ort bei der geprüften Stelle durchgeführt. Im Zuge dieser Live-Präsentation wurden einige dieser Dokumente besprochen. Dabei wurde insbesondere auf ein aufgerufenes Dokument der Leitungssitzung der MA 01 - Wien Digital aufmerksam gemacht, das u.a. Inhalte über Personalentscheidungen mit angeführten Personennamen der MA 01 - Wien Digital enthielt.

Für den StRH Wien lag daher der Verdacht weiterhin vor, dass es sich dabei um Dokumente mit Ablagestrukturen des internen Dienstbetriebes der MA 01 - Wien Digital handelte und diese - nach Ansicht des StRH Wien - nicht im Intranet der Stadt Wien für die darin angelegten User zum Aufruf zur Verfügung stehen sollten. Es waren daher folglich seit der ursprünglichen Meldung durch den StRH Wien am 25. Mai 2023 (in einem Zeitraum von 26 Werktagen) keinerlei Behebungsmaßnahmen des Sicherheitsvorfalles erkennbar bzw. umgesetzt worden.

Die MA 01 - Wien Digital wurde vom StRH Wien im Eröffnungsgespräch ersucht, den Vorfall und insbesondere die fehlende Umsetzung von Behebungsmaßnahmen dieses gemeldeten Verdachtes eines Sicherheitsvorfalles aufzuarbeiten und im Zuge der weiteren Prüfungsarbeiten das Ergebnis der Aufarbeitung entsprechend nachvollziehbar darzulegen.

Am 30. Juni 2023 wurde von der MA 01 - Wien Digital ein neues Ticket im IT-Service-Management betreffend die Wiederaufnahme der Bearbeitung zur ursprünglichen Meldung zum Sicherheitsvorfall erstellt.

Am 4. Juli 2023 wurde die Lösung aus dem Ticketsystem des IT-Service-Managements mit der Information *„… mit folgender Information gelöst: 'private Dokumente' sind nicht mehr für fremde Dienststellen sichtbar. öffentliche Dokumente sind weiterhin für Dyn.User sichtbar. einfache Dokumente sind weiterhin für alle Dienststellen sichtbar.“* rückgemeldet.

2.2 Aufarbeitung des Sicherheitsvorfalles

Grundsätzlicher Auslöser des dargelegten Sicherheitsvorfalles war nach Angaben der MA 01 - Wien Digital die redaktionelle Erstellung, Bearbeitung und anschließende Publikation einer Intranetseite zum Strategiedialog 2023 in der Stadt Wien vom 12. April 2023. Diese Intranetseite sollte nach Angabe der MA 01 - Wien Digital nach der Erstellung so schnell als möglich für alle Dienststellen der Stadt Wien freigeschalten und erreichbar sein.

In der redaktionellen Erstellung, Bearbeitung und Publikation dieser Internetseite kam es zu mehreren grundlegenden Einstellungsfehlern in den Attributen zur Steuerung dieser Publikation. Dies betraf u.a. auch den zum damaligen Zeitpunkt standardmäßigen Vorgabewert „öffentlich“ des Attributes für die Sichtbarkeit von Dokumenten bzw. Inhalten. Mit 14. April 2023 wurde eine entsprechende Störung an die MA 01 - Wien Digital gemeldet und um Behebung ersucht.

Von der MA 01 - Wien Digital wurde im Zusammenhang mit den Attributen für die Sichtbarkeit von Dokumenten bzw. Inhalten mitgeteilt, dass der zu diesem Zeitpunkt standardmäßige gültige Vorgabewert „öffentlich“ die grundsätzliche Sichtbarkeit von Dokumenten bzw. Inhalten für alle Mitarbeitenden im Intranetservice der Stadt Wien festlegte.

Bei der Erstellung derartiger Publikationen bestand die Möglichkeit einer manuellen Abänderung auf andere Werte für dieses Attribut (wie z.B. „privat“, der die Sichtbarkeit von Dokumenten bzw. Inhalten auf einen bestimmten Personenkreis einschränkte).

Aufgrund der voran dargelegten Einstellungsfehler wurde in der Verwendungsabsicht mit dem Aufruf der entsprechenden Seite zum Strategiedialog 2023 infolge ein weiterer Fehler im Abruf zur Darstellung dieser fertiggestellten Inhalte der Publikation ausgelöst und am 5. Mai 2023 vom beauftragten Dienstleiter des 2nd-Level Supports des Intranetservices der Stadt Wien entdeckt.

Darüber hinaus wurde festgestellt, dass nicht ausreichende bzw. falsche Berechtigungen für alle User des Magistrats der Stadt Wien in der bereitgestellten Mitarbeitendenrolle im Intranetservice der Stadt Wien zur Anzeige der „öffentlichen“ Inhalte dieser fertiggestellten Publikation bzw. der damit im Zusammenhang stehenden Dokumente der Dokumentenbibliothek vorlagen.

Am 10. Mai 2023 wurde von der MA 01 - Wien Digital ein verbessertes Such-Widget des Intranetservices der Stadt Wien produktiv gesetzt. Die Verwendung dieses neuen Such-Widgets führte letztlich zu einem unerwartenden Suchergebnis mit der fehlerhaften Anzeige und der fälschlichen Abrufmöglichkeit dieser anfangs angesprochenen Dokumente im Zuge der inhaltlichen Erstrecherchearbeiten des StRH Wien.

Die MA 01 - Wien Digital führte ergänzend dazu aus, dass die Redakteurinnen bzw. Redakteure der jeweiligen Organisationseinheiten bzw. der Dienststellen der Stadt Wien für das Management des Intranetservices der Stadt Wien in den verpflichtenden Schulungen ausdrücklich auf die korrekte Verwendung von Attributen bei Dokumenten und Berechtigungen hingewiesen wurden.

Zum Abfragezeitpunkt waren von den rd. 183.000 eingetragenen Dokumenten des Intranetservices der Stadt Wien potenziell 13.423 Dokumente lt. Erhebung der MA 01 - Wien Digital von diesem Umstand bzw. vom resultierenden Fehler betroffen.

Am 10. Mai 2023 wurden die Berechtigungen der Mitarbeitendenrolle von der MA 01 - Wien Digital in Zusammenarbeit mit dem beauftragten Dienstleister des 2nd-Level Supports des Intranetservices der Stadt Wien abgeändert. Diese bezog sich nicht auf die Abänderung der bestehenden Attribute der Sichtbarkeit der eingetragenen Dokumente in der Dokumentenbibliothek des Intranetservices der Stadt Wien.

Am 25. Mai 2023 wurde das vom StRH Wien gemeldete Ticket im IT-Service-Management in der Betriebskategorie „Security“ klassifiziert und zunächst der Stelle „Security und Safety“ in der MA 01 - Wien Digital zugewiesen. Von der Stelle „Security and Safety“ wurde das Ticket bearbeitet und eine Abstimmung mit dem „Datenschutz-Team“ empfohlen. Infolge wurde durch einen Dispatcher des Servicedesks der MA 01 - Wien Digital dieses Ticket betreffend den Datenschutz fälschlicher Weise an das Vorstandsressort Informations- und Medizintechnik-Management des Wiener Gesundheitsverbundes zur Bearbeitung zugewiesen. Diese fälschliche Zuweisung wurde vom Vorstandsressort Informations- und Medizintechnik-Management des Wiener Gesundheitsverbundes innerhalb kurzer Zeit erkannt und dem Servicedesk der MA 01 - Wien Digital wieder rücküberwiesen. Im Anschluss wurde betreffend den Datenschutz das Team „Recht, Vertrags- und Lizenzmanagement“ der MA 01 - Wien Digital per E-Mail kontaktiert. Dabei war der Status im Ticket bereits als „gelöst“ gesetzt worden. Außerhalb des Ticketbearbeitungsablaufes wurde parallel dazu in der MA 01 - Wien Digital das Team „Web-Content Management System“ per E-Mail kontaktiert und das Problem gelöst.

Da aufgrund der vorliegenden Information nicht davon ausgegangen wurde, dass personenbezogene Daten betroffen waren, wurde von der Datenschutzverantwortlichen der MA 01 - Wien Digital der gemeldete Sicherheitsvorfall nicht als eine notwendige *„Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde“* gemäß Art. 33 der Datenschutz-Grundverordnung eingestuft und keine weitere Maßnahme gesetzt.

Nach dem Hinweis des StRH Wien im Rahmen des Eröffnungsgespräches am 29. Juni 2023 wurde am 30. Juni 2023 ein 2. Ticket eröffnet. Dieses 2. Ticket wurde wieder dem Team „Web-Content Management System“ der MA 01 - Wien Digital zugewiesen. Dabei wurden die

Berechtigungen des Dokumententyps „Private Dokumente“ als Auslöser für den vorliegenden Fehler identifiziert.

Mit der neuen Meldung wurde auch eine weitere Prüfung durch die Datenschutzverantwortliche der MA 01 - Wien Digital durchgeführt. Diese ergab, dass Kontaktdaten von Mitarbeitenden des Magistrats der Stadt Wien betroffen waren, die in Dokumenten des Dokumententyps „Private Dokumente“ magistratsweit einsehbar waren. Dieser Vorfall wurde der MA 63 - Gewerberecht, Datenschutz und Personenstand zur weiteren Beurteilung hinsichtlich des Vorliegens einer verpflichteten *„Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde“* gemäß Art. 33 Datenschutz-Grundverordnung zur Kenntnis gebracht. Nach Auskunft der MA 01 - Wien Digital erfolgte keine Meldung des Vorfalls an die Datenschutzbehörde durch die MA 63 - Gewerberecht, Datenschutz und Personenstand.

Am 3. Juli 2023 wurden die Berechtigungen der Mitarbeitendenrolle im Intranetservice der Stadt Wien korrigiert, entsprechend getestet und die Sichtbarkeit der Dokumente entsprach wieder den Vorgaben. Am 4. Juli 2023 wurde das 2. Ticket geschlossen.

Am 13. Juli 2023 wurden die Berechtigungen der Mitarbeitendenrolle durch die MA 01 - Wien Digital nochmalig eingeschränkt.

Am 18. August 2023 wurde von der MA 01 - Wien Digital an alle Redakteurinnen bzw. Redakteure der Stadt Wien kommuniziert, dass im Zuge der Umsetzung von Sicherheitsfeatures im Intranetservice der Stadt Wien mit 29. August 2023 das Setzen von Berechtigungen bzgl. der Intranetinhalte der Organisationseinheiten bzw. Dienststellen und der Intranetinhalte der Stadt Wien besonders zu prüfen, abzuändern und in Zukunft auf eine korrekte Verwendung zu achten wäre.

Unterstützend zu dieser vorigen Vorgangsweise wurde auch die Suchfunktion des Intranetservices der Stadt Wien vom 4. August 2023 bis zum 29. August 2023 und kurz darauf ein weiteres Mal vom 30. August 2023 bis 5. September 2023 deaktiviert.

Damit wurde gewährleistet, dass alle Redakteurinnen bzw. Redakteure der Stadt Wien die entsprechende Zeit zur Korrektur der Berechtigungen der jeweiligen Intranetinhalte der Organisationseinheiten bzw. der Dienststellen hatten. Diese Deaktivierung der Suchfunktion hatte insbesondere den sicherheitstechnisch unterstützenden Aspekt, dass damit über die

Suchfunktion des Intranetservices der Stadt Wien die Auslieferung von Intranetinhalten der Organisationseinheiten bzw. Dienststellen mit fehlerhaft gesetzten Berechtigungen hintangehalten wurde.

Die Suchfunktion des Intranetservices der Stadt Wien stand in Summe an 18 Werktagen vollständig und an weiteren 4 Werktagen partiell - entspricht in der Gesamtbetrachtung einem Zeitraum von rd. 4 Wochen - nicht zur Verfügung.

Am 29. August 2023 wurden die Sicherheitsmerkmale im entsprechenden Release des Intranetservices der Stadt Wien umgesetzt. Der StRH Wien wurde von der MA 01 - Wien Digital insbesondere auf die Abänderung der Standardvorgabe des Attributes zur Sichtbarkeit auf „privat“ von allen ab diesen Zeitpunkt neu hochgeladenen Dokumenten in der Dokumentenbibliothek bzw. den jeweiligen Inhalten der Intranetseite hingewiesen.

Im Zusammenhang mit der Berechnung und Beurteilung der Verfügbarkeit des Intranetservices der Stadt Wien für alle 129.559 User (Stand: 1. Dezember 2023) war vom StRH Wien festzustellen, dass diesbezüglich kein Service Level Agreement mit der MA 01 - Wien Digital abgeschlossen wurde. Gemäß Auskunft der MA 01 - Wien Digital war für das Intranetservice des Wiener Gesundheitsverbundes ein entsprechendes Service Level Agreement der Kategorie C (Verfügbarkeit des Services in der Zeit von 7.00 Uhr bis 17.00 Uhr an den Werktagen eines Kalenderjahres) vereinbart worden.

Empfehlung:
Der StRH Wien empfahl der MA 01 - Wien Digital, den Abschluss eines Service Level Agreements für das Intranetservice der Stadt Wien zu evaluieren.

Die Stellungnahme zu dieser Empfehlung wurde im Punkt Zusammenfassung der Empfehlungen eingearbeitet.

In der Betrachtung der gesamten Bearbeitungsdauer dieses Sicherheitsvorfalls war vom StRH Wien festzustellen, dass - von der Erstmeldung am 25. Mai 2023 bis zur endgültigen Behebung und der vollständigen regulären Betriebswiederaufnahme des Intranetservices

der Stadt Wien mit 5. September 2023 - in der Bearbeitung des 1. Tickets rd. 24 Werktage und des 2. wiederaufgenommenen Tickets weitere rd. 47 Werktage und somit insgesamt rd. 71 Werktage benötigt wurden.

Wird auf die zugrunde liegende Erstmeldung vom 14. April 2023 Bezug genommen, so sind es weitere 27 Werktage und damit insgesamt rd. 98 Werktage. In der Gesamtbetrachtung betraf dies einen Zeitraum von rd. 20 Wochen (mit Samstagen, Sonntagen und Feiertagen).

In Bezug zur regulären Betriebswiederaufnahme bzw. zum damit für derartige IKT-Services der Stadt Wien zu führende BCM war vom StRH Wien anzumerken, dass die MA 01 - Wien Digital als zentraler IKT-Dienstleister der Stadt Wien eine Zertifizierung nach ISO 22301:2012 BCM mit der Registrier-Nummer BCM-00008/0 führte. Die Überprüfung der Gültigkeit dieses Zertifikates wurde vom StRH Wien über eine elektronische Abfrage des im Internet verfügbaren Registers der Zertifizierungsstelle überprüft. Die Prüfung ergab, dass das Suchergebnis der Abfrage das recherchierte Zertifikat als gültig ausgewiesen wurde.

Als Schlussergebnis und Konsequenz der weiteren Aufarbeitung des Sicherheitsvorfalles plante die MA 01 - Wien Digital die verstärkte Automatisierung bei Tests von Abänderungen. Demnach sollen nach jedem Release des gesamten Intranetservices der Stadt Wien sowohl der jeweilige Intranetcluster als auch der Internetcluster getestet werden. Dabei sollen u.a. Tests über verschiedene Rollenkonzepte verschiedener Dienststellen - die in der Software-Plattform des Intranetservices der Stadt Wien über eine zur Verfügung stehenden Standardfunktion imitiert werden - durchgeführt werden. Zudem unterstützen ergänzend „Friendly User“ in verschiedenen Dienststellen derartige Testungen. Diese Vorgangsweise bzw. die Automatisierung derartiger Tests befand sich zu diesem Zeitpunkt in der Konzeptionsphase. Weiters wurde von der MA 01 - Wien Digital mitgeteilt, dass die Schulungsunterlagen für die Redakteurinnen bzw. Redakteure bzgl. der Klassifizierung von Dokumenten bzw. Inhalten und zur Auswahl des richtigen Systems für die Verwendung bzw. der Ablage von Dokumenten verbessert werden sollen.

Der StRH Wien begrüßte die bereits durchgeführten Behebungen bzw. die vorgesehenen Verbesserungen der MA 01 - Wien Digital zum gemeldeten Sicherheitsvorfalles ausdrücklich.

Empfehlung:
Der StRH Wien empfahl der MA 01 - Wien Digital, generische Überlegungen zur Verkürzung der bereitgestellten bzw. benötigten Zeitdauer bei notwendigen, sicherheitsrelevanten und daher zeitnah zu setzenden Maßnahmen unter Einbeziehung der relevanten Kundinnen bzw. Kunden anzustellen. Diese sollten im Rahmen der Strategien, Prozesse und Maßnahmen des BCM einfließen, um damit auch die Verfügbarkeit der entsprechenden IKT-Services gemäß den Service Level Agreements sicherzustellen.

Die Stellungnahme zu dieser Empfehlung wurde im Punkt Zusammenfassung der Empfehlungen eingearbeitet.

Empfehlung:
Der StRH Wien empfahl der MA 01 - Wien Digital, die geplanten Maßnahmen hinsichtlich der Automatisierung bei Tests von Abänderungen im Intranetservice der Stadt Wien konsequent zu verfolgen.

Die Stellungnahme zu dieser Empfehlung wurde im Punkt Zusammenfassung der Empfehlungen eingearbeitet.

Empfehlung:
Der StRH Wien empfahl der MA 01 - Wien Digital, die geplante Umsetzung der Verbesserung der Schulungsunterlagen für die Redakteurinnen bzw. Redakteure des Intranetservices der Stadt Wien hinsichtlich der Klassifizierung von Dokumenten bzw. Inhalten sowie der Auswahl des richtigen Systems für die Verwendung bzw. die Ablage von Dokumenten konsequent zu verfolgen.

Die Stellungnahme zu dieser Empfehlung wurde im Punkt Zusammenfassung der Empfehlungen eingearbeitet.

3. Grundlagen zur Thematik der Fernwartung

3.1 Österreichisches Informationssicherheitshandbuch

Das öffentlich frei im Internet unter https://www.sicherheitshandbuch.gv.at/ verfügbare Österreichische Informationssicherheitshandbuch des Bundeskanzleramtes Österreich stellte ein anerkanntes Standardwerk zur Informationssicherheit dar und diente als Wissensbasis und Grundlage für das IKT-Sicherheitsbewusstsein.

Der Inhalt des Österreichischen Informationssicherheitshandbuches basierte auf den aktuellen internationalen Entwicklungen in der Informationssicherheit sowie auf Kooperationen mit dem Bundesamt für Sicherheit der Bundesrepublik Deutschland und dem Informatikstrategieorgan des Bundes der Schweizerischen Eidgenossenschaft. Das Österreichische Informationssicherheitshandbuch beschrieb die detaillierte Vorgehensweise zur Etablierung eines umfassenden ISMS und orientierte sich an der Struktur der Sicherheitsnorm ISO/IEC 27001:2013 in Unternehmen und der öffentlichen Verwaltung.

Das A-SIT Zentrum für sichere Informationstechnologie - Austria (kooperierender Partner des Bundeskanzleramtes Österreich in der Bereitstellung des Österreichischen Informationssicherheitshandbuches) stellte dem StRH Wien für den Betrachtungszeitraum der vorlie-

genden Prüfung 7 archivierte Versionen (von Version 4.1.1 vom 19. Dezember 2019 bis Version 4.3.2 vom 11. November 2022) des Österreichischen Informationssicherheitshandbuches kostenfrei zur Verfügung. Zur Berichtsfertigstellung war die Version 4.4.0 vom 6. November 2023 die aktuell gültige publizierte Fassung des Österreichischen Informationssicherheitshandbuches.

Die Einschau in die Versionen zeigte, dass das Österreichische Informationssicherheitshandbuch regelmäßig einer Evaluierung bzw. Aktualisierung unterzogen wurde. In den Inhalten war weiters erkennbar, dass die Thematik der Fernwartung bzw. des Fernzugriffs im Betrachtungszeitraum in den entsprechenden Versionen durchgängig - mit sehr geringfügigen Änderungen bzw. Aktualisierungen - bis zur aktuell publizierten Fassung abgebildet war.

3.1.1 Fernwartung

Im Österreichischen Informationssicherheitshandbuch wurde zur Fernwartung unter dem Kapitel Wartung ausgeführt, dass eine ordnungsgemäße Durchführung von Wartungsarbeiten eine besondere Bedeutung als vorbeugende Maßnahme darstelle, um IT-Systeme vor Störungen zu bewahren. Diese umfasste im Wesentlichen folgende Aufgabenstellungen:

„im Falle von Hardware:

- *die Instandhaltung (vorbeugende Wartung zur Aufrechterhaltung der Betriebstüchtigkeit) und*
- *die Instandsetzung (Behebung von Störungen und Fehlern zur Wiederherstellung der Betriebstüchtigkeit) durch Reparatur und Ersatz schadhafter IT-Komponenten,*

im Falle von Software:

- *die Behebung von Störungen bzw. Hilfe bei deren Umgehung,*
- *die Beratung der Auftraggeberin bzw. des Auftraggebers beim Einsatz der IT-Komponenten sowie allenfalls, abhängig von den vertraglichen Vereinbarungen,*
- *die Behebung von Fehlern,*
- *die Einrichtung und den Betrieb einer Hotline sowie*
- *die Weiterentwicklung und notwendigen Anpassungen“.*

Das Bundesamt für Sicherheit in der Informationstechnik der Bundesrepublik Deutschland beschrieb im Rahmen des IT-Grundschutz-Bausteines „OPS.1.2.5 Fernwartung“ des IT-Grundschutz-Kompendiums - Werkzeuge für Informationssicherheit Edition 2023 den Begriff der Fernwartung wie folgt:

„Mit dem Begriff Fernwartung wird ein zeitlich begrenzter Zugriff auf IT-Systeme und die darauf laufenden Anwendungen bezeichnet, der von einem anderen IT-System aus erfolgt. Der Zugriff kann z.B. dazu dienen, Konfigurations-, Wartungs- oder Reparaturarbeiten durchzuführen.“

In diesem Zusammenhang war vom StRH Wien anzumerken, dass vom Bundesamt für Sicherheit in der Informationstechnik der Bundesrepublik Deutschland für die Fernwartung von Betriebstechnik bzw. OT ein weiterer gesonderter IT-Grundschutz-Baustein „IND.3.2 Fernwartung im industriellen Umfeld“ zur Verfügung stand.

Im Kapitel Fernwartung des Österreichischen Informationssicherheitshandbuches waren bzgl. der Anwendung der Fernwartung von IKT-Systemen die besonderen Sicherheitsrisiken und die zu treffenden Sicherungsmaßnahmen näher dargelegt. Dies umfasste u.a. Informationen zu den Sicherungsfunktionen der abgesicherten Kommunikationsverbindungen, zur Authentisierung, Verschlüsselung, Protokollierung, zu Sicherheitssperren bei Zugangsversuchen und Zeitspannen sowie zu Rechteeinschränkungen.

Ergänzend war vom StRH Wien anzumerken, dass das Österreichische Informationssicherheitshandbuch für die Fernwartung von Betriebstechnik bzw. OT die Sicherheitsrisiken und zu treffenden Sicherungsmaßnahmen nicht weiter detaillierte.

3.1.2 Fernzugriff

Um die Fernwartung als operatives Instrument der Wartung anwenden zu können, war ein eingerichteter Fernzugriff mit entsprechendem Fernwartungsuser auf das jeweilige IKT-System notwendig.

Im Kapitel Fernwartung des Österreichischen Informationssicherheitshandbuches wurde die Thematik des Fernzugriffs mit einem eigenen Kapitel und entsprechender Untergliederung mit Informationen zu den anzuwendenden Sicherungsmaßnahmen weiter dargelegt. Dies

betraf u.a. Informationen zu Authentisierungsservices und der verwendeten Hardware, technischen Kommunikationsprotokollen zum Einsatz und zur Konfiguration der Kommunikationshardware und Kommunikationssoftware.

3.2 Organisatorische Grundlagen

Im Zusammenhang zum vorliegenden Prüfungsgegenstand waren bei der geprüften Stelle der MA 01 - Wien Digital in der Geschäftseinteilung für den Magistrat der Stadt Wien die entsprechenden Geschäftsaufgaben wie folgt umfasst:

- Bereitstellung von IKT-Services für den Magistrat, einschließlich der Unternehmungen der Stadt Wien,
- Mitwirkung bei der Weiterentwicklung der IKT-Strategie,
- Erstellung und Weiterentwicklung der strategischen Planung des IKT-Einsatzes,
- Mitwirkung beim strategischen IKT-Projektportfoliomanagement,
- Beratung und Begleitung der Kundinnen bzw. Kunden beim IKT-Einsatz zur Digitalisierung ihrer Geschäftsprozesse,
- Sicherstellung eines stabilen und sicheren Betriebes der IKT-Services, insbesondere der technischen Verfügbarkeit der Arbeitsplatzausstattung, der notwendigen Business Services und der notwendigen Infrastruktur,
- Planung, Beschaffung, Errichtung, Installation, Betriebsführung und Erhaltung von Einrichtungen der IKT (Hardware und Software) sowie Abschluss von entsprechenden Vereinbarungen und Verträgen,
- Genehmigung der Beschaffung von Einrichtungen der IKT sowie des Abschlusses von entsprechenden Vereinbarungen und Verträgen, sofern mit Unternehmungen der Stadt Wien nicht etwas anderes vereinbart wird,
- Projektmanagement für IKT-Projekte im Magistrat,
- Festlegung und Weiterentwicklung der IKT-Architektur für den Magistrat,
- Festlegung von Richtlinien für einen wirtschaftlichen und effizienten Einsatz der IKT für den Magistrat,
- Innovationsmanagement im Bereich der IKT,
- Sicherstellung der IKT-Sicherheit und der
- Koordination der internen IKT-organisatorischen und IKT-technischen Maßnahmen des Magistrats sowohl zwischen Magistratsdienststellen als auch zwischen dem Magistrat und Einrichtungen außerhalb des Magistrats.

Die MA 01 - Wien Digital hatte die zu erbringenden Dienstleistungen im Bereich der Fernwartung für die Dienststellen des Magistrats der Stadt Wien, den Wiener Gesundheitsverbund und die sonstigen weiteren Organe der Stadt Wien (z.B. dem Verwaltungsgericht Wien, Wiener Umweltanwaltschaft) bereitzustellen.

3.3 Regulatorische Grundlagen

3.3.1 NISG

Auf Basis der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union wurde in Österreich das NISG mit BGBl. I Nr. 111/2018 vom 29. Dezember 2018 umgesetzt und kundgemacht.

Mit diesem Bundesgesetz wurden Maßnahmen festgelegt, welche ein hohes Sicherheitsniveau von Netz- und Informationssystemen von Betreibern wesentlicher Dienste in den Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserversorgung und digitale Infrastruktur sowie von Anbietern digitaler Dienste und Einrichtungen der öffentlichen Verwaltung gewährleisten sollte. Die Identifizierung und Festlegung von Betreibern wesentlicher Dienste erfolgte mittels Bescheid durch das Bundeskanzleramt nach Befassung des jeweils zuständigen Bundesministeriums der genannten Sektoren.

Betreiber wesentlicher Dienste hatten geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen, die den Stand der Technik berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar war, angemessen waren. Die zu treffenden Sicherheitsvorkehrungen gemäß § 17 Abs. 1 NISG wurden infolge durch die NISV umgesetzt und festgelegt.

Ein Betreiber eines wesentlichen Dienstes hatte mindestens alle 3 Jahre nach Zustellung des Bescheides die Erfüllung der Anforderungen nachzuweisen. Dazu waren Aufstellungen der vorhandenen Sicherheitsvorkehrungen durch Zertifizierungsnachweise oder durchgeführte Überprüfungen der dazu qualifizierten Stellen zu übermitteln. In weiterer Folge konnte der Bundesminister für Inneres zur Kontrolle der Einhaltung der Anforderungen eine entsprechende Einschau in die diesbezüglichen Unterlagen und Netz- und Informationssysteme vornehmen lassen. Bei Nichterfüllung dieser Vorgaben konnte der Bundesminister für Inneres

Handlungsempfehlungen aussprechen. Eine Weigerung der Erfüllung dieser Vorgaben stellte eine Verwaltungsübertretung dar.

Für den Betrachtungszeitraum bzw. zum Prüfungszeitpunkt lag für die MA 01 - Wien Digital selbst kein Bescheid als Betreiber wesentlicher Dienste vor. Dem StRH Wien wurde hingegen ein Bescheid des Wiener Gesundheitsverbundes als Betreiber wesentlicher Dienste im Sektor Gesundheitswesen vom 10. Dezember 2020 (GZ 2020-0.698.328) vorgelegt. In der Umsetzung bzw. der Anwendung der vorher genannten Sicherheitsvorkehrungen zur Netz- und Informationssicherheit bediente sich der Wiener Gesundheitsverbund seit 1. Juli 2018 der Dienstleistungen der MA 01 - Wien Digital.

Ergänzend war vom StRH Wien anzumerken, dass basierend auf der angeführten NISG Richtlinie die nachfolgende Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) mit 16. Jänner 2023 bereits in Kraft getreten und von den Mitgliedstaaten bis zum 17. Oktober 2024 ins nationale Recht umzusetzen war. Diese Richtlinie soll den bestehenden regulatorischen Defiziten - u.a. aufgrund von unterschiedlichen Umsetzungen in den Mitgliedstaaten der EU - harmonisierend entgegenwirken. Durch den österreichischen Gesetzgeber wurden die grundlegenden Arbeiten zur nationalen Umsetzung bereits begonnen.

3.3.2 NISV

Auf Basis des NISG wurde die NISV mit BGBl. II Nr. 215/2019 am 18. Juli 2019 in Kraft gesetzt. In der Anlage 1 zur NISV waren die konkreten Sicherheitsmaßnahmen zu verschiedenen Kategorien der Sicherheitsvorkehrungen gemäß § 17 Abs. 1 NISG enthalten. Dabei wurde in der 6. Kategorie „Systemwartung und Betrieb“ zum Punkt Fernzugriff Folgendes ausgeführt:

„Fernzugriff ist eingeschränkt nach dem Minimalrechtsprinzip und zeitlich beschränkt zu vergeben. Die Fernzugriffsrechte sind periodisch zu überprüfen und gegebenenfalls anzupassen. Die Sicherheit des Fernzugriffs ist zu gewährleisten.“

Darüber hinaus stand für die nähere Erläuterung der Umsetzung der Vorgaben der in der Anlage 1 der NISV genannten Sicherheitsvorkehrungen das *„NIS Fact Sheet 9/2022“* des Bundeskanzleramtes bzw. des Bundesministeriums für Inneres vom September 2022 zur Verfügung.

In dieser Erläuterung waren zum o.a. Punkt „Fernzugriff“ in der Anlage 1 zur NISV weitere konkretere Sicherheitsvorkehrungen erläutert:

„Der Betreiber etabliert Prozesse zur Verwaltung von Fernzugriffen. Insbesondere stellt er Techniken zur Verfügung, die Fernzugriffe auf Netz- und Informationssysteme nur nach dem Minimalrechtsprinzip autorisiert und zeitlich beschränkt ermöglichen.

Die Authentifizierung im Rahmen des Fernzugriffs wird mittels Zwei-Faktor-Authentifizierung umgesetzt. Jeglicher unautorisierte Zugriff wird unterbunden.

Für Wartungsarbeiten, die über Fernzugriffe erfolgen, stellt der Betreiber sicher, dass alle Tätigkeiten und Operationen aufgezeichnet und dokumentiert werden. Alle Zugriffe externer Personen können nur unter Kontrolle der Systemverantwortlichen erfolgen.

Der Einsatz von sog. „Jumpservern“/„Jumphosts“, bspw. für die Durchführung administrativer Tätigkeiten, ist durchaus möglich. Die Konfiguration der Jumpserver/Jumphosts für die Nutzung durch MitarbeiterInnen, welche sich aus einem Netzwerkabschnitt mit geringerem Schutzbedarf von einem Gerät verbinden bzw. der Einsatz von Sicherheitsmaßnahmen bei ebenjenen, hat den Vorgaben zur Fernwartung von Externen zu entsprechen.“

Im Zusammenhang mit der Umsetzung der voran dargelegten Sicherheitsmaßnahmen wies das *„NIS Fact Sheet 9/2022“* auf folgenden Umstand hin:

„Bei allen im NIS Fact Sheet beschriebenen Sicherheitsmaßnahmen ist bei der Umsetzung im Sinne des § 17 Abs. 1 NISG auf ein angemessenes Verhältnis zwischen dem feststellbaren Ausmaß einer Bedrohung und der wirtschaftlichen Belastung Wert zu legen. Wenn aus technischen oder betrieblichen Gründen die Umsetzung der die Sicherheitsmaßnahmen beschreibenden Ausführungen nicht gänzlich möglich ist, sind die dadurch bedingten Abweichungen bei der Umsetzung durch risikominimierende und/oder kompensierende Maßnahmen auszugleichen und dies entsprechend in den zu erbringenden Nachweisen (Aufstellung samt Prüfbericht) darzustellen und glaubhaft zu begründen.“

Anzumerken war, dass abschließend im Punkt Fernzugriff des *„NIS Fact Sheet 9/2022“* Bezug auf nationale und internationale Informationssicherheitsstandards und Best Practises (wie u.a. auf das Österreichische Informationssicherheitshandbuch, die ISO/IEC 27001) genommen wurde.

3.3.3 Dienstanweisung Fernwartung im Wiener Gesundheitsverbund

Im Betrachtungszeitraum und im Zusammenhang zur Bereitstellung und Verwendung der Dienstleistung Fernwartung durch die MA 01 - Wien Digital wurde die Dienstanweisung „GED-DA-087-21-IMT Fernzugänge zur Wartung, Störungsbehebung und Analyse von technischen Einrichtungen und IT-Systemen“ mit 1. August 2021 im Wiener Gesundheitsverbund im Sinn des NISG bzw. der NISV als Betreiber wesentlicher Dienste erlassen und in Kraft gesetzt.

In dieser Dienstanweisung wurden u.a. folgende wesentliche technische Vorgaben ausgeführt:

„Es sind alle Fernzugriffe auf IT-Systeme und auf alle anderen technischen Einrichtungen des Wiener Gesundheitsverbundes, die in das EDV - Netzwerk der Stadt Wien (im folgenden „allgemeines Netzwerk“ genannt) eingebunden sind, über die von Wien Digital betriebenen und für diesen Zweck vorgesehenen, zentralen Fernzugänge abzuwickeln.“

„Die Verwendung von Einrichtungen, die Fernzugriffe ermöglichen (z.B. Modems, Router), welche in den jeweiligen Systemen lokal installiert sind, ist nicht gestattet. Ausnahmen sind hinsichtlich der Notwendigkeit einer Sonderlösung zu begründen, und bedürfen der ausdrücklichen und schriftlichen Zustimmung von Wien Digital. Die Begründung muss auch eine Darstellung beinhalten, wie die Aspekte des Datenschutzes und der IT-Sicherheit bei dieser Sonderlösung im Sinne der Stadt Wien sichergestellt werden. Die Zustimmung von Wien Digital ist im Wege des Vorstandsressorts IMT-Management einzuholen.“

Im Bereich der rechtlichen Rahmenbedingungen waren folgende Vorgaben dargelegt:

„Im Hinblick auf die datenschutzrechtlichen und sicherheitstechnischen Erfordernisse ist vor der erstmaligen Durchführung eines Fernzugriffes zwischen dem Auftraggeber und dem Auftragsverarbeiter (=Dienstleister, der die Fernzugriffe durchführt) ein ‚Fernzugriffsvertrag‘ ab-

zuschließen. Wenn bei dieser Dienstleistung dem Auftragsverarbeiter auch personenbezogene Daten zur Einsicht bzw. zur Kenntnis gelangen können, ist außerdem ein ‚Auftragsverarbeitervertrag' (ehemals Datenschutzvertrag) abzuschließen."

„Fernzugriffsverträge werden für den gesamten Wirkungsbereich des Wiener Gesundheitsverbundes von Wien Digital abgeschlossen. (Dies gilt auch für Fernzugänge, die in genehmigten Einzelfällen, nicht über das von Wien Digital betriebene allgemeine Netzwerk realisiert werden.)"

„Ggf. notwendige Auftragsverarbeiterverträge werden vom Vorstandsressort Recht und Compliance, Fachbereich Datenschutz abgeschlossen."

3.3.4 Zertifizierung der MA 01 - Wien Digital nach ISO/IEC 27001

Die ISO/IEC 27001 war ein Standard für die Anforderungen bzgl. der Implementierung, Aufrechterhaltung und kontinuierlichen Verbesserung eines ISMS in einer Organisation. Die Konformität bzw. eine Zertifizierung nach diesem Standard bedeutete, dass die jeweilige Organisation ein System zum Management der Risiken in Bezug auf die Sicherheit von vorhandenen und verarbeiteten Daten der Organisation eingerichtet hatte und dieses System entsprechend den dargelegten Anforderungen betrieb. Die Gültigkeit eines solchen Zertifikates wurde durch jährliche Überwachungsaudits sichergestellt und musste durch ein Rezertifizierungsaudit nach 3 Jahren erneuert werden.

Die MA 01 - Wien Digital hielt gemäß Recherche des StRH Wien im Intranet der Stadt Wien ein Zertifikat unter der Registriernummer I-00416/0 zu einem wirksamen Informationssicherheitsmanagement und betrieb dieses entsprechend den Anforderungen nach ISO/IEC 27001:2013. Die Erstausstellung dieses Zertifikates erfolgte am 15. April 2019. Das vorliegende Zertifikat war bis 15. April 2025 gültig.

Die Gültigkeit des entsprechenden Zertifikates der MA 01 - Wien Digital wurde vom StRH Wien über eine elektronische Abfrage des im Internet verfügbaren Registers der Zertifizierungsstelle überprüft. Die Prüfung ergab, dass das recherchierte Zertifikat als gültig ausgewiesen wurde.

3.3.5 Testate der MA 01 - Wien Digital nach ISAE 3402

Die ISAE 3402 beschrieb Regelungen zur Prüfung des IKS einer Dienstleistungsorganisation, die eine qualifizierte Referenz für die Beauftragung von entsprechenden Dienstleistungen durch weitere andere Organisationen darlegte und dokumentierte.

Bei einem Typ 1 ISAE 3402 Testat wurde zu einem bestimmten Zeitpunkt die sachgerechte Konzeption, Ausgestaltung und die Einrichtung der angemessenen Kontrollen eines dienstleistungsbezogenen IKS geprüft und bestätigt (Prüfung des Aufbaus des dienstleistungsbezogenen IKS). Bei einem Typ 2 ISAE 3402 Testat wurde zusätzlich über einen Prüfungszeitraum die Wirksamkeit der Kontrollen geprüft und bestätigt (Prüfung der Funktion der Kontrollen des dienstleistungsbezogenen IKS).

Die MA 01 - Wien Digital hatte sich im Betrachtungszeitraum im Jahr 2020 einer Typ 1 Prüfung und in den Jahren 2021 und 2022 Typ 2 Prüfungen gemäß ISAE 3402 durch externe Wirtschaftsprüfungsunternehmen unterzogen.

Dem StRH Wien lag ein Testat der Typ 1 ISAE 3402 Prüfung zum Stichtag 31. Dezember 2020 zu den ausgewählten Services der SAP Basis, SAP CCoE, SAP IS-H Patientenabrechnung und Verwaltung integrierter Personaldaten/Wiener Integriertes Personalinformationssystem über den Betrieb der Gehaltsverrechnung und Personalverwaltung vor.

Im Zusammenhang mit dem Prüfungsgegenstand des StRH Wien war gemäß dem zugrunde liegenden Prüfungsbericht des Typ 1 ISAE 3402 Testats unter der Domäne des Betriebes die Subdomäne des Fernzugriffs dokumentiert.

Das Typ 1 ISAE 3402 Testat bestätigte, dass in der Kontrollbeschreibung die Fernwartungszugriffe:

- für Mitarbeitende mit Zwei-Faktor-Authentifizierung nur über abgesicherte Zugänge erfolgten,
- von Firmen mit Fernwartungszugängen nur nach vorheriger Freischaltung der User erfolgten,
- über ein Monitoring verfügten und
- dass alle Zugänge personenbezogen waren.

Dem StRH Wien lag außerdem je ein Testat der Typ 2 ISAE 3402 Prüfung für den Zeitraum von 1. Jänner 2021 bis 31. Dezember 2021 sowie 1. Jänner 2022 bis 31. Dezember 2022 zu den ausgewählten Services der SAP Basis, SAP CCoE, SAP IS-H Patientenabrechnung und Verwaltung integrierter Personaldaten/Wiener Integriertes Personalinformationssystem zum Betrieb der Gehaltsverrechnung und Personalverwaltung vor.

Den Prüfungsberichten der entsprechenden Zertifikate war zusätzlich zu den bereits o.a. Kontrollbeschreibungen der Fernwartungszugriffe zu entnehmen, dass die Fernwartungszugänge auf eine Gültigkeitsdauer von 1 Jahr eingeschränkt waren.

In den Prüfungsberichten war unter dem dienstleistungsbezogenen IKS der MA 01 - Wien Digital die Kontrolle ID 60 *„Zugriff für Firmen via Fernwartungszugriff“* mit den voran genannten Kontrollbeschreibungen mit einem anlassbezogenen präventiven Kontrolltyp dokumentiert. Im Rahmen der Prüfung der Wirksamkeit der Kontrolle ID 60 *„Zugriff für Firmen via Fernwartungszugriff“* wurden die zuständigen Personen befragt sowie Einsicht in den Prozess *„Fernzugriffe managen“* und die Liste der aktiven Fernwartungsuser genommen. Dabei erfolgte eine stichprobenartige Einschau in die dazugehörigen Anforderungsformulare und Anforderungen für eine Verlängerung bzw. Löschung von Fernwartungszugängen.

Die beiden Typ 2 ISAE 3402 Testate für die Jahre 2021 und 2022 bestätigten, dass bei der Prüfung der Kontrolle ID 60 *„Zugriff für Firmen via Fernwartungszugriff“* keine Ausnahmen festgestellt wurden.

Von der MA 01 - Wien Digital wurde mitgeteilt, dass die Typ 2 ISAE 3402 Attestierung jährlich erneuert wird und die nächste Attestierung im Frühjahr 2024 geplant war.

4. Fernwartungspolicy

Dem StRH Wien lagen als weitere heranzuziehende Beurteilungsgrundlage zum Prüfungsgegenstand die:

- *„Fernwartungspolicy der MA 01 - Wien Digital Fernwartung durch Vertragspartnerinnen und -partner auf Produktivsystemen“* in der Version 1.0.0 (gültig vom 21. September 2021 bis 28. Juni 2023) sowie die
- *„Fernwartungspolicy der MA 01 - Wien Digital Fernwartung durch externe Partner*innen auf Produktivsystemen“* in der Version 1.1.0 (gültig ab 28. Juni 2023) vor.

Für den Betrachtungszeitrum der vorliegenden Prüfung war festzustellen, dass im Zeitraum vom 1. Jänner 2020 bis 20. September 2021 keine gültige und ordnungsgemäß dokumentierte regulatorische Grundlage von der MA 01 - Wien Digital zu dieser Thematik vorgelegt werden konnte. Die MA 01 - Wien Digital teilte diesbezüglich mit, dass es für diesen betreffenden Zeitraum bereits Regelungen gab, diese aber nicht in einer dokumentierten bzw. archivierten Fassung dem StRH Wien vorgelegt werden konnten.

4.1.1 Rahmenbedingungen

Die Fernwartungspolicy definierte im Kapitel Rahmenbedingungen die zugrunde gelegten Bestimmungen und Regelungen. Diese waren:

- die externen gesetzlichen Bestimmungen und Regelungen
  - des Bundesgesetzes zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und
  - der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG vom 4. Mai 2016,
- die internen Bestimmungen und Regelungen der Stadt Wien
  - des Erlasses Datenschutzes im Magistrat der Stadt Wien (MDK-420907-1/18) und
  - des Erlasses Sicherheit in der Informations- und Kommunikationstechnologie (MD-OS 51600-2013-1) sowie
- die Bestimmungen und Regelungen der MA 01 - Wien Digital hinsichtlich
  - der Policy User- und Berechtigungsverwaltung der MA 01 - Wien Digital,
  - der Zusammenarbeit mit externen Dienstleisterinnen bzw. Dienstleistern - Arbeitsmodelle,
  - der Arbeitsregelung zu Klassifizierungsstufen,
  - der Arbeitsregelung für Sicherheitsüberprüfungen,
  - der Arbeitsregelung für Kennwörter,
  - der Vorgaben des Rechts-, Vertrags- und Lizenzmanagements sowie
  - des Business Servicekatalogs der MA 01 - Wien Digital.

Es war festzustellen, dass im Kapitel Rahmenbedingungen über die zugrunde gelegten gesetzlichen Bestimmungen und Regelungen das NISG bzw. die NISV nicht angeführt waren. Diese betraf ebenso die nachfolgende Version 1.1.0 der Fernwartungspolicy.

Der StRH Wien führte diesbezüglich aus, dass die zum Prüfungszeitpunkt geltenden gesetzlichen Grundlagen (NISG und NISV) die Thematik der Fernwartung mit Sicherungsmaßnahmen bereits entsprechend umfassten. Außerdem erbrachte die MA 01 - Wien Digital IKT-Dienstleistungen für den Wiener Gesundheitsverbund, welcher gemäß NISG als Betreiber wesentlicher Dienste bestimmt wurde und die Dienstanweisung zur Fernwartung über die MA 01 - Wien Digital dies entsprechend auch festlegte (s. Punkt 3.3.3 Dienstanweisung Fernwartung im Wiener Gesundheitsverbund).

Empfehlung:
Der StRH Wien empfahl der MA 01 - Wien Digital, das Kapitel Rahmenbedingungen in der Fernwartungspolicy bei Aktualisierung der externen gesetzlichen Bestimmungen und Regelungen im Hinblick auf das NISG und die NISV anzupassen.

Die Stellungnahme zu dieser Empfehlung wurde im Punkt Zusammenfassung der Empfehlungen eingearbeitet.

Der StRH Wien stellte im Zusammenhang zu den internen Bestimmungen und Regelungen der Stadt Wien fest, dass in der Version 1.0.0 der Fernwartungspolicy keine entsprechende Aktualisierung im Gültigkeitszeitraum beim Bezug zum gültigen Erlass des Datenschutzes im Magistrat in einer eigenen Version der Fernwartungspolicy erfolgte.

In der folgenden Version 1.1.0 der Fernwartungspolicy wurde diesem Umstand Rechnung getragen, jedoch in der Versionshistorie der Grund der Änderungen nicht vermerkt.

Empfehlung:
Der StRH Wien empfahl der MA 01 - Wien Digital, bei Änderungen der Fernwartungspolicy sowohl auf die rechtzeitige Aktualisierung dieses Dokuments in entsprechenden Versionen als auch auf die ordnungsgemäße Führung der Versionshistorie zu achten.

Die Stellungnahme zu dieser Empfehlung wurde im Punkt Zusammenfassung der Empfehlungen eingearbeitet.

4.1.2 Inhaltliche Abgrenzung

Die Fernwartungspolicy in der Version 1.0.0 regelte zusammenfassend den Inhalt wie folgt:

„Diese Policy regelt die Fernwartung von Produktivsystemen durch Vertragspartnerinnen und -partner der MA 01-Wien Digital. Sie beschreibt die Rahmenbedingungen für die Einrichtung von Fernwartungsusern mit Zwei-Faktor-Authentifizierung sowie die Überwachung von Fernwartungsaktivitäten."

Diese Policy galt *„… für die komplette Organisation der MA 01-Wien Digital sowie für das beauftragte Fremdpersonal und für beauftragte Dienstleisterinnen und Dienstleister, insbesondere für jene Personen, die im Bereich Fernwartung Aufgaben wahrnehmen.*

Diese Aufgaben umfassen u.a.

- *die Ausschreibung von Wartungsdienstleistungen, welche Fernwartung beinhaltet,*
- *den Abschluss von entsprechenden Verträgen,*
- *die Einrichtung von Fernwartungsusern sowie*
- *die Durchführung von Wartungsarbeiten via Fernwartung."*

In diesem Zusammenhang wurde von der MA 01 - Wien Digital mitgeteilt, dass sich die vorliegende Fernwartungspolicy inhaltlich bzw. thematisch auf die Fernwartung bzw. den Fernzugriff auf Server und Services aus dem IT- bzw. IKT-Bereich bezog.

Die Fernwartung bzw. der Fernzugriff von Anlagen und Systemen der Betriebstechnik bzw. OT-Systeme wurden damit nicht umfasst und waren gemäß MA 01 - Wien Digital durch die *„Security-Vorgaben für OT-Systeme, Lastenheft für Auftragnehmerinnen und Auftragnehmer"* der MD-OS/PIKT - freigegeben am 26. März 2021 - entsprechend abgedeckt.

Die Gültigkeit der in diesem Dokument angegebenen Vorgaben bezog sich auf *„… alle auftragnehmenden Stellen bei Neuanschaffung oder umfangreicher Erweiterung und Erneuerung eines OT-Systems. Die Erfüllung der Anforderungen dieses Dokuments ist verpflichtend und Teil des Vertrages bei einer Neubeauftragung"*.

In diesem Dokument war die Thematik des Fernzugriffs in einem eigenen Kapitel *„Sicherer Fernzugriff/Remote Access"* dargestellt und legte folgende Anforderungen fest:

1. *„Wird ein Fernzugriff auf Komponenten benötigt, MUSS dieser in Abstimmung mit der MA 01 realisiert werden.*
2. *Es DÜRFEN nur von der MA 01 freigegebene Fernzugriffsmöglichkeiten und -applikationen eingesetzt werden.*
3. *Alle Fernzugriffs-Möglichkeiten MÜSSEN autorisiert, authentifiziert, verschlüsselt und dokumentiert werden."*

Die Formulierungen der 3 o.a. Anforderungen waren an die RFC 2119 - Schlüsselwörter zur Verwendung und zur Angabe von Anforderungsniveaus (MÜSSEN, DÜRFEN) angelehnt und in der Umsetzungspriorität entsprechend kategorisiert.

Entsprechend dieser Anforderungen war die MA 01 - Wien Digital seit dem 26. März 2021 bei neuen und umfangreich erweiterten OT-Systemen miteinbezogen und konnte damit ihre entsprechende Kenntnis und Dokumentation von OT-Systemen mit Fernwartung bzw. Fernzugriff innerhalb der Stadt Wien sukzessive erweitern.

Im Zuge der Prüfung teilte die MA 01 - Wien Digital dem StRH Wien mit, dass eine 2. Regelung zu Vorgaben betreffend OT-Systeme durch die MD-OS/PIKT im Intranet der Stadt Wien publiziert wurde.

Eine diesbezügliche Intranetrecherche des StRH Wien führte zu einer neu publizierten 2. Regelung (*„OT-Security Konzept der Stadt Wien Regeln, Maßnahmenempfehlung und Umsetzungsvorschläge für industrielle und kritische Infrastrukturen, inkl. Vereinfachten Umsetzungsgrad"* in der Version 1.0 mit einem weiteren Tabellendokument für ein Self-Assessment eines OT-Security Konzeptes). Diese Regelung wurde gemäß Versionshistorie initial neu erstellt, vom WienCERT der MA 01 - Wien Digital überprüft, durch den Chief Information Security Officer der Stadt Wien am 31. Mai 2023 freigegeben und sollte *„ab Sicherheitserlass 2023"* die Gültigkeit erlangen. Weiters war festzustellen, dass die 1. Regelung zu OT-Systemen nicht mehr auf diesen betreffenden Intranetseiten der Stadt Wien bereitgestellt und abrufbar war.

In dieser neu publizierten 2. Regelung war kein formaler Zusammenhang bzw. Verweis auf die 1. Regelung bzw. auf die Fernwartungspolicy als Ganzes oder in Teilen zur Fernwartung bzw. zum Fernzugriff und auf die weitere Gültigkeit der 1. Regelung ersichtlich.

Diese 2. Regelung zu einem OT-Security Konzept - mit ebenso inhaltlichen Detailaspekten zur Fernwartung bzw. zum Fernzugriff - lag nach Ansicht des StRH Wien zum Prüfungszeitpunkt in Ergänzung zur 1. Regelung vor, besaß jedoch für den Betrachtungszeitraum keine Gültigkeit.

Vom StRH Wien war in diesem Zusammenhang zu ergänzen, dass im Zuge bzw. kurz vor dem Ende der Prüfungsarbeiten mit 23. November 2023 der Erlass „Sicherheit in der Informations- und Kommunikationstechnologie" (MD-OS 51600-2013-1) außer Kraft gesetzt und durch den Erlass „Sicherheit in der Informations- und Kommunikationstechnologie" (MD-OS 1416182-2023) abgelöst wurde.

Mit diesem neuen bzw. aktualisierten Erlass wurde auf der Grundlage der Empfehlungen des Berichtes des StRH Wien (MA 01, Prüfung von Steuerungssystemen; StRH I - 13/18) eine ganzheitliche strukturierte und nachvollziehbare Koordination von OT-Systemen innerhalb der Stadt Wien umgesetzt.

In der inhaltlichen Darlegung dieser neu publizierten 2. Regelung war in der Präambel Folgendes dargelegt:

„Die Stadt Wien betreibt zur Erfüllung ihrer vielfältigen Aufgabenbereiche eine große Anzahl an OT-Systemen. Darunter fallen Kontrollsysteme, Prozessleitsysteme, SCADA-Systeme, industrielle Geräte, Medizingeräte (WiGeV), technische IT-Geräte sowie Standard-IT-Geräte, die im Rahmen eines OT-Systems eingesetzt werden. Teilweise sind diese Systeme auch mit dem Internet vernetzt. Einige dieser OT-Systeme werden für den Betrieb kritischer Infrastrukturen bzw. im Gesundheitswesen der Stadt Wien eingesetzt und können somit Gegenstand des Netz- und Informationssystemsicherheitsgesetzes (NISG1), sowie anderen gesetzlichen Vorgaben sein.

Das NIS-Gesetz (NISG) verpflichtet Betreiber wesentlicher Dienste, geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen und umzusetzen.“

Der Gültigkeitsbereich dieser neu publizierten 2. Regelung war wie folgt festgelegt:

„Das vorliegende Dokument gilt für alle Dienststellen, welche ein OT-System betreiben bzw. dafür verantwortlich sind. Die Erfüllung der Anforderungen dieses Dokuments ist verpflichtend. Dies kann aufgrund anderer erfüllter Standards oder Vorgaben schon erfüllt sein. Dann ist ein Verweis auf diese umgesetzten Standards oder Vorgaben ausreichend.“

Im Zusammenhang mit der Thematik der Fernwartung bzw. des Fernzugriffs war im Kapitel „Systemgrenzen“ eine Anforderung hinsichtlich der Identifikation und Dokumentation aller Schnittstellen (Datenflüsse) des OT-Systems als MUSS Anforderung definiert.

Des Weiteren war unter dem Kapitel „Systemwartung und Betrieb“ ein Subkapitel „Fernzugriff“ ausgewiesen. In diesem waren 2 Anforderungen in der Abstufung des Schutzbedarfes wie folgt dokumentiert:

- OT-Systeme mit Basisschutzbedarf
  „Die Dienststelle SOLL sicherstellen, dass Fernzugriffe niemals direkt stattfinden, sondern stattdessen ein Jump-Host Konzept (z.B. Standardlösung der MA 01) eingesetzt wird. Sollte es unmöglich sein, einen direkten Fernzugriff zu vermeiden, MÜSSEN kompensierende Maßnahmen eingepflegt werden.“ und

- OT-Systeme mit hohem bzw. sehr hohem Schutzbedarf
  „Die Dienststelle MUSS die Sicherheit von Fernzugriffen gewährleisten. Dazu ist der Einsatz

der Standardlösung der MA 01 zu bevorzugen. Ist eine Anbindung an die Infrastruktur der MA 01 nicht möglich, MUSS ein Fernwartungskonzept eingeführt werden, welches zumindest folgende Anforderungen erfüllt:

- *Keine direkte Verbindung zu OT-Systemen aus dem Internet bzw. der IT (Jump-Host Konzept),*
- *Transportsicherheit und Verschlüsselung auf dem Stand der Technik,*
- *Unterstützung einer Zwei-Faktor-Authentifizierung sowie*
- *Minimalrechtsprinzip und zeitliche Beschränkung".*

Die MA 01 - Wien Digital teilte mit, dass keine eigenen OT-Systeme mit Fernwartung bzw. Fernzugriff in der vorliegenden Organisation und Struktur vorlagen bzw. verwaltet wurden.

Die MA 01 - Wien Digital arbeitete aktuell an der Inventarisierung der OT-Systeme in der Stadt Wien. Eine taxativ vollständige Erfassung von OT-Systemen mit dem Teilaspekt der Fernwartung bzw. Fernzugriff erfolgte zum Prüfungszeitpunkt nicht.

Der StRH Wien anerkannte die Bemühungen und Arbeiten der MD-OS/PIKT und der MA 01 - Wien Digital hinsichtlich der zugrunde liegenden Regelungen, Detailvorgaben und Erfassung von OT-Systemen insbesondere im Zusammenhang zur Fernwartung bzw. zum Fernzugriff bei OT-Systemen.

Der StRH Wien hatte den Eindruck gewonnen, dass in Bezug auf die Organisation der Fernwartung insbesondere im Zusammenhang zu bzw. bei OT-Systemen die Ausgestaltung, Darlegung und Gültigkeit der grundlegenden Regelungen und Detailvorgaben sowie die Erfassung und Inventarisierung zum Prüfungszeitpunkt nicht zur Gänze eindeutig und klar ausgestaltet und organisiert war.

Aus Sicht des StRH Wien erschien es unter dem Gesichtspunkt der gesetzlichen Vorgabe des NISG bzw. in Vorbereitung der sich in Umsetzung befindlichen NIS-2-Richtlinie (s. Punkt 3.3.1 NISG und 3.3.2 NISV) sinnvoll, die notwendigen Arbeiten insbesondere für OT-Systeme in Bezug zur Fernwartung bzw. zum Fernzugriff zeitnah verstärkter in den Fokus zu rücken.

Empfehlung:
Der StRH Wien empfahl der MA 01 - Wien Digital, die organisatorischen und technischen Anforderungen hinsichtlich Fernwartung bzw. Fernzugriff bei OT-Systemen in den zugrunde liegenden Regelungen, den entsprechenden Detailvorgaben und der weiteren Umsetzung zeitnah und nachvollziehbar zu definieren.

Die Stellungnahme zu dieser Empfehlung wurde im Punkt Zusammenfassung der Empfehlungen eingearbeitet.

Empfehlung:
Der StRH Wien empfahl der MA 01 - Wien Digital, eine Evaluierung einer taxativ vollständigen Erfassung bzw. Inventarisierung von OT-Systemen mit Fernwartung bzw. Fernzugriff durch die MA 01 - Wien Digital vorzunehmen.

Die Stellungnahme zu dieser Empfehlung wurde im Punkt Zusammenfassung der Empfehlungen eingearbeitet.

4.1.3 Weiterführende Regelungen

Bezüglich des Punktes „Bestimmungen und Regelungen der MA 01 - Wien Digital“ in der Fernwartungspolicy war vom StRH Wien festzustellen, dass diese weiteren Bestimmungen und Regelungen unter dem Kapitel der bereits vorher angeführten „Rahmenbedingungen“, in einem weiteren Kapitel „organisatorische Einbettung“, in anderen inhaltlichen Kapiteln mit Einzelangaben und im Kapitel „Linkverzeichnis“ angeführt waren. Diese Angaben waren in den Kapiteln z.T. unterschiedlich, nur einzeln aber auch mehrfach wiederholend enthalten. Dies betraf die Fernwartungspolicy der Version 1.0.0 und der Version 1.1.0.

Empfehlung:
Der StRH Wien empfahl der MA 01 - Wien Digital, bei den abgebildeten Bezügen zu weiteren Bestimmungen, Regelungen, Verlinkungen usw. in der Fernwartungspolicy auf eine ordnungsgemäße bzw. konsistente Darstellung zu achten.

Die Stellungnahme zu dieser Empfehlung wurde im Punkt Zusammenfassung der Empfehlungen eingearbeitet.

In der Version 1.0.0 der Fernwartungspolicy wurde im Kapitel zur Überwachung von Fernwartungsverbindungen auf die weiterführende Regelung der Loggingpolicy verwiesen. In der vorgelegten Version 1.1.0 der Fernwartungspolicy war dieser Verweis auf diese Policy nicht mehr enthalten. Die vorgelegte Loggingpolicy der MA 01 - Wien Digital zeigte, dass es sich bei dieser um eine unvollständige und nicht freigegebene Version 1.0.0 handelte.

Die MA 01 - Wien Digital teilte mit, dass diese Policy zum Prüfungszeitpunkt noch durch die Dienststellenleitung der MA 01 - Wien Digital bearbeitet wurde. Diese Loggingpolicy sollte nach Angabe der MA 01 - Wien Digital noch im Jahr 2023 in Kraft treten.

Inhaltlich legte die Loggingpolicy die technologieunabhängigen Anforderungen der organisatorischen und technischen Anforderungen für die Umsetzung des Loggings (z.B. die Aufbewahrungsfrist von Logs von Systemen und Anwendungen) fest. Diese Loggingpolicy stellte damit eine wichtige Grundlage und maßgebende Vorgabe zum genannten Kapitel als auch zur Fernwartungspolicy dar.

Der StRH Wien qualifizierte eine Loggingpolicy als einen wesentlichen Bestandteil der letztlich zu treffenden bzw. abzuleitenden Sicherheitsmaßnahmen, da eine derartige Loggingpolicy mit den darin enthaltenen Vorgaben die Grundlage für eine revisionssichere und nachvollziehbare Beurteilung, Prüfung und Dokumentation darstellte.

Die Wichtigkeit des Loggings - und damit einer entsprechenden grundliegenden Loggingpolicy - wurde durch die Publikation „Log-Daten als Grundlage für Incident Response“ Schriftenreihe „Cybersicherheit“ aus dem Februar 2022 des Bundesministeriums für Inneres auf

der Internetseite der NISG-Informationen des Bundeskanzleramtes von Österreich sowie durch das Open Web Application Security Projekt verdeutlicht. Das Open Web Application Security Projekt wies ein fehlendes bzw. nicht ordnungsgemäß implementiertes Logging und deren Überwachung in den Top 10 der bedeutsamsten und kritischen Sicherheitsrisiken, Angriffsvektoren und Schwachstellen aus.

Zum Prüfungszeitpunkt wurden seitens der MA 01 - Wien Digital diese Top 10 in den Vorgaben der *„Arbeitsregelung zur Entwicklung sicherer Software“* in der Version 1.2.0 vom 2. Dezember 2019 bereits entsprechend berücksichtigt.

Empfehlung:
Der StRH Wien empfahl der MA 01 - Wien Digital, die Fertigstellung der Loggingpolicy voranzutreiben und diese zeitnah im Betrieb der betreffenden Systeme - insbesondere im Zusammenhang zur Thematik der Fernwartung bzw. des Fernzugriffs - umzusetzen und anzuwenden.

Die Stellungnahme zu dieser Empfehlung wurde im Punkt Zusammenfassung der Empfehlungen eingearbeitet.

4.1.4 Dokumentation, Archivierung und Skartierung

Die Überprüfung der ordnungsgemäßen Dokumentation, Archivierung und Skartierung der Fernwartungspolicy war gemäß den Vorgaben des Erlasses „Büroordnung für den Magistrat der Stadt Wien“ vom 4. Jänner 2013 (MDK-168759-1/12) durchzuführen und zu beurteilen. Damit im Zusammenhang stand der Erlass „Allgemeine Vorschrift für das Ausscheiden von Akten (Skartierungsordnung)“ (MD-OS - 104/2010) Neuregelung vom 31. März 2010 gültig bis zum 28. März 2020 und der nachfolgende Erlass „Allgemeine Vorschrift für das Ausscheiden von Unterlagen (Skartierungsordnung)“ (MD-OS - 74746-2020) gültig ab 1. März 2020.

Entsprechend der beiden o.a. Erlässe zur Skartierungsordnung war ein entsprechender Akten- und Skartierungsplan für die MA 01 - Wien Digital in Abstimmung mit der MA 8 - Wiener Stadt- und Landesarchiv zu erstellen und anzuwenden.

Die Überprüfung des Auszugs aus dem ELAK zum Akten- und Skartierungsplan ergab, dass im, bis zum 17. September 2020, gültigen Akten- und Skartierungsplan die Fernwartungspolicy dem Sachgebiet „Abteilungsleitung: Dienstanweisungen“ mit einer Aufbewahrungsfrist von *„3 Jahre ab Ende der Gültigkeit“* und der archivarischen Bewertung *„archivwürdig“* in der MA 01 - Wien Digital zugeordnet war.

Im, ab 18. September 2020, vorliegenden gültigen Akten- und Skartierungsplan war die vorliegende Fernwartungspolicy V 1.0.0 dem Sachgebiet *„Abteilungsleitung: Klasse „A-Dokumente“* mit einer Aufbewahrungsfrist von *„Auf Dauer der Gültigkeit + 12 Jahre“*, der archivarischen Bewertung *„archivwürdig“* und der Schutzfristkategorie von ELAK-Daten mit *„Archivwürdig (MC)“* zugeordnet. Dieses Sachgebiet umfasste Dokumente zu allgemeinen Organisationsakten (Referatseinteilungen, Organigramme), Dienstanweisungen und Dienstvorschriften, Policies, Rollenbeschreibungen, Zieldokumenten, IKS Erhebungsbögen und Managementreviews.

Mit Inkrafttreten der Fernwartungspolicy V 1.0.0 mit 21. September 2021 wäre entsprechend des Akten- bzw. Skartierungsplanes die vorangegangene - nicht mehr gültige - Fernwartungspolicy bis zum 21. September 2033 in der unmittelbaren Aufbewahrung und der Zugriff über die mit Wirksamkeit vom 23. August 2001 genehmigte elektronische Aktenführung in der MA 01 - Wien Digital vorzuhalten.

Empfehlung:
Der StRH Wien empfahl der MA 01 - Wien Digital, auf die ordnungsgemäße Dokumentation und Aufbewahrung mittels elektronischer Aktenführung - insbesondere der entsprechenden Policies, Regelungen und Vorgaben betreffend die Fernwartung - gemäß Büroordnung der Stadt Wien und Akten- und Skartierungsplan zu achten.

Die Stellungnahme zu dieser Empfehlung wurde im Punkt Zusammenfassung der Empfehlungen eingearbeitet.

Im ELAK-Auszug zur Fernwartungspolicy war für den StRH Wien erkennbar, dass eine weitere zur Thematik der Fernwartung zuordenbare alte Policy mit dem *Titel „Ablauf Auswertung Fernwartungszugriffe“* mit 2. März 2023 (kurz vor dem Beginn der Prüfungsdurchführung) außer Kraft gesetzt wurde. Diesbezüglich war in diesem ELAK-Auszug dokumentiert, dass diese Inhalte durch die bereits gültige Fernwartungspolicy V 1.0.0 vom 21. September 2021 abgedeckt wurden.

Der StRH Wien merkte an, dass eine entsprechende gültige eigene Arbeitsregelung für die Auswertung von Fernwartungszugriffen bestand. Diese lag dem StRH Wien in der Version 1.0.1 mit Freigabe vom 19. Dezember 2018 durch das Team Security, Safety und Compliance der MA 01 - Wien Digital vor.

Im ELAK-Auszug war weiters feststellbar, dass die Dokumentation der Fernwartungspolicy (V 1.0.0 und V 1.1.0) in Form von entsprechenden Geschäftsstücken vorlag und dass diese im zugehörigen und wie vorher dargelegten Sachgebiet im ELAK erst am 28. Juni 2023 - im Zuge der laufenden Prüfung durch den StRH Wien - ordnungsgemäß zugeordnet bzw. umprotokolliert wurde.

Empfehlung:
Der StRH Wien empfahl der MA 01 - Wien Digital, bei der Protokollierung von Inhalten zur Fernwartung in der elektronischen Aktenführung auf die ordnungsgemäße und zeitnahe Zuordnung im Zuge der erstmaligen Erstellung des entsprechenden vorgegebenen Sachgebietes des Akten- und Skartierungsplanes zu achten.

Die Stellungnahme zu dieser Empfehlung wurde im Punkt Zusammenfassung der Empfehlungen eingearbeitet.

4.1.5 Abbildung von Soll-Kriterien

In den folgenden Kapiteln und Unterkapiteln der „Fernwartungspolicy“ sowie in den weiteren angeführten Regelungen (s. Punkt 4.1.3 Weiterführende Regelungen) waren detailliertere Informationen zu vertragsrechtlichen Aspekten, zur Fernwartungslösung, zur Verrechnung der Fernwartung und zu den Fernwartungsusern angeführt. Diese enthielten auch weiterführende Informationen zu den Prozessen der Fernwartung sowie die Unterlagen der Fernwartungslösung, der Fernwartungsarchitektur und des Datenaustausches in organisatorischer und technischer Weise.

Der StRH Wien merkte zu diesen Informationen in den Kapiteln und Unterkapiteln der Fernwartungspolicy an, dass die Prinzipien der Normenserie ISO/IEC 27000 und des Österreichischen Informationssicherheitshandbuches in diesem Erlass angeführt wurden. Gemäß Beurteilung des StRH Wien waren diese Prinzipien grundsätzlich als rechtsverbindliche Vorgabe anzusehen.

Die MA 01 - Wien Digital teilte nach interner rechtlicher Abstimmung bzw. Rücksprache mit der MD-OS/PIKT diese rechtsverbindliche Berücksichtigung - insbesondere der im Österreichischen Informationssicherheitshandbuch dargelegten detaillierten Kriterien zur Thematik der Fernwartung bzw. des Fernzugriffs - nicht. Dennoch versuchte sie als sicherheitsbewusste IKT-Dienstleisterin der Stadt Wien nach eigenen Angaben, einen Großteil der allgemeinen internationalen und nationalen Normen und Vorgaben - auch ohne dahingehende Verpflichtung - abzudecken.

Im neuen bzw. aktualisierten Erlass „Sicherheit in der Informations- und Kommunikationstechnologie“ (MD-OS 1416182-2023) war die Berücksichtigung der Prinzipien des Österreichischen Informationssicherheitshandbuches ersatzlos gestrichen worden. Die MD-OS/PIKT teilte diesbezüglich mit, dass mit der Berücksichtigung des Österreichischen Informationssicherheitshandbuches zum Zeitpunkt der Erstellung des alten Erlasses (Datum des Inkrafttretens: 28. Jänner 2013) grundlegend nicht das Ansinnen bestand, diese als zu berücksichtigende Soll-Vorgaben für eine Umsetzung der Inhalte des Österreichischen Informationssicherheitshandbuches festzulegen.

Aufgrund der zugrunde gelegten NISV sowie des damit in Bezug stehenden *„NIS Fact Sheets 9/2022“* und des darin angeführten Österreichischen Informationssicherheitshandbuches sah der StRH Wien die Streichung dieser Prinzipien als inhaltliche Referenz - insbesondere

im Hinblick auf strukturiertere und detailliertere Vorgaben für eine effektive operative Umsetzung - kritisch.

Der StRH Wien stellte im Zusammenhang mit der Zertifizierung der MA 01 - Wien Digital nach ISO/IEC 27001:2013 in Durchsicht und Beurteilung der damit referenzierten und in Verbindung stehenden ISO/IEC 27002:2013 - *„Informationstechnik - Sicherheitsverfahren - Leitfaden für Informationssicherheitsmaßnahmen“* im Vergleich fest, dass in den Informationssicherheitsmaßnahmen nach ISO/IEC 27002 im Vergleich zum Österreichischen Informationssicherheitshandbuch keine konkretisierende Sicherheitsmaßnahmen für die praktische Umsetzung zur Thematik der Fernwartung bzw. des Fernzugriffs von Mobilgeräten und der Telearbeit enthalten waren.

In diesem Zusammenhang legte das Österreichische Informationssicherheitshandbuch im Kapitel 1.1.4 *„Quellen, Verträglichkeiten, Abgrenzungen“* diese Sichtweise in ähnlicher Weise wie folgt dar:

„Die Normenfamilie ISO/IEC 27000 besteht vereinfacht aus fünf grundlegenden Bereichen:

- *Terminologie und Aufbau über ISO/IEC 27000 (‚Überblick und Vokabular‘)*
- *Zertifizierbarer ISO/IEC 27001 (‚Anforderungen‘ in Verbindung mit den Anforderungen an Audit und Zertifizierung aus ISO/IEC 27006)*
- *Standards im Sinne für ‚Allgemeine Richtlinien‘ (ISO/IEC 27002 bis ISO/IEC 27005, ISO/IEC 27007 und ISO/IEC 27008)*
- *Spezifische Standards für ausgewählte ‚Branchen‘ (ISO/IEC 27011, ISO/IEC 27015, ISO/IEC 27019)*
- *Subnormen ‚Supporting Standards‘ (z.B. ISO/IEC 27032 für ‚Cyber Security‘ und*
- *ISO/IEC 27036 für ‚Outsourcing‘)“.*

Des Weiteren wurde diese Sichtweise wie folgt durch das Österreichische Informationssicherheitshandbuch ausgeführt:

„ISO/IEC 27002 (vormals ISO 17799) ‚Information technology - Security techniques - Code of practice for information security controls‘ befasst sich als Rahmenwerk für das Informationssicherheitsmanagement hauptsächlich mit den erforderlichen Schritten, um ein funktionierendes Informationssicherheitsmanagement aufzubauen und in der Organisation zu verankern. Die erforderlichen Informationssicherheitsmaßnahmen werden eher kurz auf ca. 80 Seiten

skizziert angerissen. Die Empfehlungen sind für Managementebenen formuliert und enthalten nur wenige konkrete technische Hinweise. Ihre Umsetzung ist auch nur eine von vielen Möglichkeiten, die Anforderungen des ISO/IEC-Standards 27001 zu erfüllen.“

„Das Informationssicherheitshandbuch geht in Aufbau, Struktur und Abhandlung der generellen Themen konform mit ISO/IEC 27001 und 27002, bietet allerdings in einer kompakten Form auch technische und organisatorische Hinweise und Ratschläge zur Implementierung.“

Aus Sicht des StRH Wien stellte zudem das Österreichische Informationssicherheitshandbuch des Bundeskanzleramtes Österreich das Pendant zu den IT-Grundschutz-Bausteinen des Bundesamtes für Sicherheit der Bundesrepublik Deutschland mit einem ähnlichen Detaillierungsgrad an konkreten Vorgaben zur Umsetzung dar. Zuletzt verwies der StRH Wien auf die bevorstehenden Änderungen zur NIS-2-Richtlinie.

Empfehlung:
Der StRH Wien empfahl der MA 01 - Wien Digital, die Aufnahme von konkreten Vorgaben zur effektiven operativen Umsetzung von Maßnahmen zur Fernwartung bzw. des Fernzugriffs (wie Österreichisches Informationssicherheitshandbuch oder IT - Grundschutz-Baustein des Bundesamtes für Sicherheit der Bundesrepublik Deutschland) in den entsprechenden Regelungen zu evaluieren.

Die Stellungnahme zu dieser Empfehlung wurde im Punkt Zusammenfassung der Empfehlungen eingearbeitet.

In der Auslegung der Berücksichtigung der Prinzipien der Normenserie ISO/IEC 27000 waren durch den vorliegenden Nachweis der Zertifizierung zu einem wirksamen und betriebenen Informationssicherheitsmanagement die Anforderungen nach ISO/IEC 27001:2013 erbracht und nachgewiesen (s. Punkt 3.3.4 Zertifizierung der MA 01 - Wien Digital nach ISO/IEC 27001).

In der Auslegung der Berücksichtigung der Prinzipien des Österreichischen Informationssicherheitshandbuches ging der StRH Wien daher infolge der weiteren Prüfung davon aus, dass die dargelegten detaillierten Kriterien zur Thematik der Fernwartung bzw. des Fernzugriffs des Erlasses als entsprechende verpflichtende Soll-Vorgaben (s. Punkt 5. Umsetzung der Vorgaben zur Fernwartung) anzusehen waren.

4.1.6 Begriffsdefinitionen

Die Begriffe „Fernwartung“, „Fernzugriff“ und „Fernwartungsuser“ waren in der Fernwartungspolicy im Kapitel Begriffsdefinitionen definiert. Darüber hinaus waren die Begriffe „Abweichung“ und „Ausnahme“ für ein differenziertes Vorgehen in der Fernwartung dokumentiert.

Die Fernwartungspolicy gab für die Anwendung der Fernwartung eine von der MA 01 - Wien Digital definierte und damit standardisierte Fernwartungslösung vor. Wenn mit dieser Lösung die externen Vertragspartnerinnen bzw. Vertragspartner nicht das Auslangen fanden, konnten diese einerseits über „Abweichungen“ (Adaptierung der Fernwartungslösung der MA 01 - Wien Digital) und andererseits über die „Ausnahmen“ (Einsatz einer anderen Fernwartungsvariante) eine entsprechende Umsetzung wählen.

Bei einer „Abweichung“ war die Vorgehensweise durch das WienCERT der MA 01 - Wien Digital einer Prüfung zu unterziehen und zu genehmigen. Für „Ausnahmen“ war diese Vorgangsweise an dieser Stelle im Dokument nicht dargelegt.

Die beiden Begriffe wurden in einem weiteren folgenden Kapitel „Umgang mit Abweichungen und Ausnahmen“ inhaltlich näher beschrieben. Demnach war für die „Abweichungen“ und für die „Ausnahmen“ eine Prüfung und Genehmigung des WienCERT erforderlich. Dies betraf die Fernwartungspolicy der Version 1.0.0 und der Version 1.1.0.

Empfehlung:
Der StRH Wien empfahl der MA 01 - Wien Digital, auf eine ordnungsgemäße und konsistente Abbildung der Vorgehensweise bei „Abweichungen“ und „Ausnahmen“ in der Fernwartungspolicy zu achten.

Die Stellungnahme zu dieser Empfehlung wurde im Punkt Zusammenfassung der Empfehlungen eingearbeitet.

Die MA 01 - Wien Digital hatte keine Fälle von „Abweichungen“ erfasst und dokumentiert. Für „Ausnahmen“ waren hingegen 93 Fälle dokumentiert. 8 „Ausnahmen“ betrafen den Magistrat der Stadt Wien und 85 „Ausnahmen“ den Wiener Gesundheitsverbund (davon 19 „Ausnahmen“ die Teilunternehmung Allgemeines Krankenhaus Wien).

In Verbindung mit den Vorgaben zur Fernwartung bzw. zum Fernzugriff für OT-Systeme der Regelungen *„Security-Vorgaben für OT-System, Lastenheft für Auftragnehmerinnen und Auftragnehmer“* und *„OT-Security Konzept der Stadt Wien Regeln, Maßnahmenempfehlung und Umsetzungsvorschläge für industrielle und kritische Infrastrukturen, inkl. Vereinfachten Umsetzungsgrad“* der MD-OS/PIKT (s. Punkt 4.1.2 Inhaltliche Abgrenzung) war für den StRH Wien ein organisatorischer und inhaltlicher Zusammenhang zur Definition und Abgrenzung über diese „Ausnahmen“ und „Abweichungen“ der Fernwartungspolicy zu erkennen.

Zusammenfassend war für den StRH Wien dieser Zusammenhang derart gegeben, dass auch bei OT-Systemen die Standardlösung der Fernwartungslösung der MA 01 - Wien Digital anzuwenden bzw. zu bevorzugen war oder eine eigene Fernwartungsvariante gefunden und eingesetzt werden musste. Eine Einbindung, Kenntnis und Prüfung sowie Genehmigung durch das WienCERT für diese „Ausnahmen“ und „Abweichungen“ hinsichtlich Fernwartungen bzw. Fernzugriffen bei OT-Systemen war daher organisatorisch und technisch in gleicher Weise erforderlich.

Empfehlung:
Der StRH Wien empfahl der MA 01 - Wien Digital, eine Prüfung und Genehmigung durch das WienCERT der MA 01 - Wien Digital bei „Ausnahmen“ und „Abweichungen“ hinsichtlich Fernwartungen bzw. Fernzugriffen bei OT-Systemen zu evaluieren.

Die Stellungnahme zu dieser Empfehlung wurde im Punkt Zusammenfassung der Empfehlungen eingearbeitet.

5. Umsetzung der Vorgaben zur Fernwartung

5.1 Umsetzung in der Aufbauorganisation

In der Aufbauorganisation war zwischen den administrativen Aufgaben der Verwaltung und den operativen Aufgaben der Durchführung der eigentlichen Fernwartung zu unterscheiden.

5.1.1 Administrative Aufgaben

In der Aufbauorganisation der Administration war die Thematik der Fernwartung nach Auskunft der MA 01 - Wien Digital bzw. gemäß Organisationshandbuch nicht einer eigenen Organisationseinheit zugeordnet.

Zum Prüfungszeitpunkt waren folgende Organisationseinheiten mit den entsprechenden Aufgaben betraut:

Geschäftsbereich Steuerung

- Das Team Personaladministration der Gruppe Managementsysteme war für die Administration in allen personellen Angelegenheiten verantwortlich. Im Zusammenhang mit den Fernwartungen wurde die Verwaltung der externen Mitarbeitenden sowie der Fernwartungsuser mit 0,50 VZÄ durchgeführt.

- Das Team Interne IKT-Beratung der Gruppe interne Services war mit 4 VZÄ internes und 1 VZÄ externes Personal insbesondere für die Zurverfügungstellung von organisatorischen Informationen und Betriebsmittel für Mitarbeitende der MA 01 - Wien Digital zuständig. In den Zuständigkeitsbereich des Teams fiel beispielsweise auch die Berechtigungsverwaltung für externe User und Fernwartungsuser.

- Das Team Vendormanagement der Gruppe Betriebswirtschaft, Beschaffung und Recht war mit 0,50 VZÄ für die Abklärung der Datenschutzbestimmungen (Datenschutzvertrag

oder Geheimhaltungsverpflichtung) sowie für den Abschluss von Fernzugriffsvereinbarungen zuständig.

Geschäftsbereich Betrieb

- Das Team Service Desk der Gruppe Betriebssteuerung war mit 0,27 VZÄ für die Freischaltung von Fernwartungszugängen und der Dokumentation dieser sowie für die Überprüfung der Fernwartungszugänge hinsichtlich der Betriebssicherheit und des Datenschutzes zuständig.

- Das Team Netzwerk Sicherheit der Gruppe Infrastruktur Netzwerk war mit 0,04 VZÄ für die Fernwartung via Firewall bzw. für die damit im Zusammenhang stehende zentrale organisatorische und technische Sicherheitsinfrastruktur (wie dem WienCERT) zuständig.

- Das Team Server Windows der Gruppe Server Windows war mit 0,50 VZÄ für die operativen Aufgaben und die strategische Ausrichtung der Betriebsführung von Microsoft Windows Servern zuständig. Für diese Aufgaben wurde die Fernwartung bzw. der Fernzugriff als Betriebsmittel verwaltet und eingesetzt.

Für die administrativen Tätigkeiten der Fernwartung bzw. des Fernzugriffs waren damit insgesamt 5,81 VZÄ interne Mitarbeitende der MA 01 - Wien Digital und 1 VZÄ externes Personal eingesetzt.

Der StRH Wien stellte fest, dass im bereitgestellten Organisationshandbuch (Version 2.0) der MA 01 - Wien Digital die Tätigkeiten des Teams Server Windows des Geschäftsbereiches Betrieb der Gruppe Server Windows im Zusammenhang zum Prüfungsgegenstand nicht eindeutig zu erkennen bzw. dargelegt waren. Die MA 01 - Wien Digital teilte diesbezüglich mit, dass das für den Betrachtungszeitraum gültige Organisationshandbuch nicht mehr den aktuellen Stand zum Prüfungszeitpunkt darstellte.

Empfehlung:
Der StRH Wien empfahl der MA 01 - Wien Digital, im Organisationshandbuch auf die durchgängige Dokumentation bzw. inhaltliche Abbildung der Thematik der Fernwartung bzw. des Fernzugriffs in den jeweiligen Kapiteln der Organisationseinheiten der MA 01 - Wien Digital zu achten.

Die Stellungnahme zu dieser Empfehlung wurde im Punkt Zusammenfassung der Empfehlungen eingearbeitet.

5.1.2 Operative Durchführung

Für die Beurteilung der operativen Durchführung der Fernwartung durch die jeweiligen beauftragten externen Partnerinnen bzw. Partner stand dem StRH Wien eine Auswertung über Fernwartungsuser (Stand 18. Oktober 2023) der MA 01 - Wien Digital zur Verfügung. Diese wies 202 Fernwartungszugänge für die unterschiedlichsten Services für die MA 01 - Wien Digital und 79 Fernwartungszugänge für 26 weitere Dienststellen des Magistrats der Stadt Wien, einen Fonds und einer Unternehmung aus.

Bezüglich der eingesetzten VZÄ bzw. Aufwandsstunden für operativ getätigte Fernwartungen im Betrachtungszeitraum teilte die MA 01 - Wien Digital mit, dass auf Grundlage der jeweiligen Wartungsverträge unterschiedliche Verrechnungsmodalitäten (z.B. Pauschalvereinbarung, nach Bedarf) vereinbart wurden und daher eine entsprechende gesamtheitliche Darstellung nur mit erheblichem Aufwand aus den einzelnen Verträgen zu erstellen wäre.

5.2 Umsetzung in der Ablauforganisation

Die MA 01 - Wien Digital stellte dem StRH Wien für die Darstellung der Ablauforganisation des Prüfungsgegenstandes die Dokumentation des Prozesses *„Fernzugriff managen“* aus der Prozessmanagementplattform in der Version 1.0 (Stand 3. Juli 2023) zur Verfügung. Gemäß der Versionshistorie wurde dieser Prozess am 17. Mai 2021 angelegt und am 30. Sep-

tember 2021 vom Management Board der MA 01 - Wien Digital freigegeben. Zum Prüfungszeitpunkt lag für den genannten Prozess die Version 1.02 mit der Freigabe vom 6. Oktober 2023 vor.

Im Rahmen der Prüfung der Typ 2 ISAE 3402 Testate (s. Punkt 3.3.5 Testate der MA 01 - Wien Digital nach ISAE 3402) durch ein Wirtschaftsprüfungsunternehmen wurde in den o.a. Prozess Einschau genommen und infolge entsprechende Unterlagen stichprobenartig geprüft. Die beiden Typ 2 ISAE 3402 Testate zeigten keine Beanstandungen auf.

Für den StRH Wien war auf Grundlage dieser Testate die Ordnungsmäßigkeit des Prozesses sichergestellt.

5.3 Regulatorische Umsetzung

Der StRH Wien erarbeitete eine Auflistung von Kriterien zur Thematik der Fernwartung bzw. des Fernzugriffs auf Basis der einzelnen detaillierten Maßnahmen des Österreichischen Informationssicherheitshandbuches. Dabei wurden 48 Kriterien als MUSS, 20 als SOLL und 5 als KANN Kriterien (gemäß RFC 2119 Schlüsselwörter zur Verwendung und zur Angabe von Anforderungsniveaus) interpretiert und kategorisiert.

Im Rahmen dieser Kategorisierung stellte der StRH Wien fest, dass die textlichen Ausführungen zu den einzelnen Maßnahmen im Österreichischen Informationssicherheitshandbuch gemäß RFC 2119 Schlüsselwörter zur Verwendung und zur Angabe von Anforderungsniveaus mit den betreffenden Schlüsselwörtern nicht immer eindeutig klar formuliert zu erkennen und einzuordnen waren.

Diese Vorgehensweise des StRH Wien wurde aufgrund der Ausführungen zur 1. und 2. Regelung der OT-Security der MD-OS/PIKT in entsprechender gleicher Weise angewendet.

Empfehlung:
Der StRH Wien empfahl der MA 01 - Wien Digital, die Anwendung der RFC 2119 Schlüsselwörter zur Verwendung und zur Angabe von Anforderungsniveaus in der Fernwartungspolicy sowie den damit in Verbindung stehenden bzw. der damit referenzierten weiteren Richtlinien und Policies zu evaluieren.

Die Stellungnahme zu dieser Empfehlung wurde im Punkt Zusammenfassung der Empfehlungen eingearbeitet.

Auf der Grundlage dieser Kriterien bzw. dieser Kategorisierung führte der StRH Wien ein Dokumentenaudit durch. Dieses umfasste die inhaltliche Umsetzung der o.a. 73 Kriterien in den jeweiligen Dokumenten (z.B. Fernwartungspolicy, Policy User- und Berechtigungsverwaltung, Arbeitsregelung für Kennwörter) der MA 01 - Wien Digital.

Das Dokumentenaudit durch den StRH Wien ergab, dass die Kriterien in den Dokumenten der entsprechenden Policies, Arbeitsregelungen, Vorgaben, Architekturbeschreibungen usw. abgebildet bzw. dargelegt waren.

Die MA 01 - Wien Digital machte den StRH Wien auf technisch nicht mehr zeitgemäße Anforderungen einzelner Kriterien des Österreichischen Informationssicherheitshandbuches (z.B. lokale Modem- und Routerzugänge) aufmerksam. Dabei wurde mitgeteilt, dass derartige Anforderungen aufgrund des nicht mehr aktuellen Standes der Technik nicht in allen Belangen durch die MA 01 - Wien Digital berücksichtigt werden. Zudem wurde von der MA 01 - Wien Digital auf das Dokument *„OT-Security Konzept der Stadt Wien Regeln, Maßnahmenempfehlung und Umsetzungsvorschläge für industrielle und kritische Infrastrukturen, inkl. Vereinfachten Umsetzungsgrad“* in der Version 1.0 mit entsprechenden Vorgaben zur Fernwartung bzw. zum Fernzugriff verwiesen (s. Punkt 4.1.2 Inhaltliche Abgrenzung).

In der Folge führte der StRH Wien weitere Vor-Ort-Prüfungen bzw. Überprüfungen (Konformitätsaudits) in ausgewählten Themenbereichen durch (s. Punkt 5.5 Operativ-technische Umsetzung).

5.4 Überwachung

Im Betrachtungszeitraum wurden keine internen Überprüfungen bzw. Audits durch das Team Interne Revision der MA 01 - Wien Digital zum Themenfeld (Fernwartung bzw. Fernzugriff) durchgeführt. Außerdem fanden keine speziellen Audits im Zusammenhang mit dem Datenschutz oder der Fernwartung bzw. des Fernzugriffs statt.

Die MA 01 - Wien Digital begann mit der Zustellung des Bescheides (Betreiber wesentlicher Dienste) an den Wiener Gesundheitsverbund im Dezember 2020 entsprechende Maßnahmen in Vorbereitung auf die Prüfung gemäß NISG bzw. der NISV zu setzen (s. Punkte 3.3.1 NISG, 3.3.2 NISV und 3.3.3 Dienstanweisung Fernwartung im Wiener Gesundheitsverbund). Im Zusammenhang mit dem Prüfungsgegenstand betraf dies 2 Labor-Informations-Systeme. Dabei wurden in Beauftragung der MA 01 - Wien Digital durch den Wiener Gesundheitsverbund im Juli 2021 Penetrationstests, im April 2022 eine externe NISG-Teilprüfung und im Oktober 2023 ein externes NISG Gesamtaudit durchgeführt. Dem StRH Wien lagen keine abschließenden Berichte zu den Ergebnissen dieser externen Audits vor.

Im Rahmen des Prozesses „*Externe PartnerInnen auditieren*“ wurden bis zum Prüfungszeitpunkt zur Thematik der Fernwartung bzw. des Fernzugriffs ebenfalls keine Audits durch die MA 01 - Wien Digital durchgeführt.

Im Zusammenhang zum IKS der MA 01 - Wien Digital wurde von der MA 01 - Wien Digital auf die Typ 1 und Typ 2 ISAE 3402 Attestierungen (s. Punkt 3.3.5 Testate der MA 01 - Wien Digital nach ISAE 3402) verwiesen.

Vom WienCERT der MA 01 - Wien Digital wurden bis zum Prüfungszeitpunkt keine Sicherheitsvorfälle erfasst, die eine Einschau in die Dokumentation nötig gemacht hätten.

Für den Betrachtungszeitraum wurden im Zusammenhang zum Prüfungsgegenstand keine Penetrationstests durch oder in Beauftragung der MA 01 - Wien Digital durchgeführt.

Die MA 01 - Wien Digital teilte weiters mit, dass für den Betrachtungszeitraum keine gerichtlichen Verfahren im Zusammenhang mit Fernwartungsverträgen anhängig waren.

5.5 Operativ-technische Umsetzung

5.5.1 Fernwartungslösung

Der StRH Wien führte am 5. Juli 2023 eine Vor-Ort-Einschau in die Fernwartungslösung der MA 01 - Wien Digital durch.

Die von der MA 01 - Wien Digital eingesetzte Fernwartungslösung basierte auf dem Ansatz eines zentralen Zuganges über ein Fernwartungsportal mittels Jump Host Konzept in einer entsprechenden weiteren Applikationsumgebung. Durch das Fernwartungsportal und der daran anschließenden Applikationsumgebung war ein zentraler und alleiniger Zugangspunkt „Single Point of Contact“ für den jeweiligen Fernwartungsuser zu den betreffenden zu verwaltenden bzw. zu wartenden Systemen mit Zwei-Faktor-Authentifizierung, entsprechender Überwachungsdokumentation, redundant und lastverteilend realisiert. Diese Fernwartungslösung befand sich gemäß MA 01 - Wien Digital seit rd. 10 Jahren im Einsatz.

Die diesbezügliche Überwachungsdokumentation bestand aus einem Applikationsteil zur Dokumentation des Loggings der jeweiligen Daten (Metadaten) der Fernwartungsaktivitäten (z.B. Session Start Date and Time, Session End Date and Time, Userkennung) sowie einem Applikationsteil der Aufzeichnung und Ablage des audiovisuellen Mitschnitts (Video) der jeweiligen Session der Fernwartungsaktivitäten.

Die MA 01 - Wien Digital sah als Soll-Vorgabe eine Aufbewahrungsdauer von 400 Tage (vom aktuellem Datum rückwärts gerechnet) für beide Applikationsteile der Überwachungsdokumentation vor. Im Zuge der Einschau des StRH Wien war festzustellen, dass die Vorgabe für die Aufbewahrungsdauer der Daten der Fernwartungsaktivitäten auf 90 Tage und die Vorgabe für die Aufbewahrungsdauer für den audiovisuellen Mitschnitt auf 400 Tage gesetzt war.

Die Verantwortlichen für die Fernwartungen in der MA 01 - Wien Digital erhöhten als 1. Maßnahmen nach dem Eröffnungsgespräch am 29. Juni 2023 die Aufbewahrungsdauer für die Daten der Fernwartungsaktivitäten auf 180 Tage.

Um eine effektive und effiziente Bereitstellung der Überwachungsdokumentation im Anlassfall sowie deren Nachvollziehbarkeit sicherzustellen, erachtete es der StRH Wien als notwendig, gleiche Aufbewahrungsdauern für die beiden Teile der Überwachungsdokumentation der Fernwartungsaktivitäten vorzugeben.

Empfehlung:
Der StRH Wien empfahl der MA 01 - Wien Digital, eine Evaluierung der Harmonisierung der unterschiedlichen Aufbewahrungszeiträume der beiden Teile der Überwachungsdokumentation von Fernwartungsaktivitäten durchzuführen.

Die Stellungnahme zu dieser Empfehlung wurde im Punkt Zusammenfassung der Empfehlungen eingearbeitet.

Die Harmonisierung der unterschiedlichen Aufbewahrungszeiträume stand im Zusammenhang mit der zum Prüfungszeitpunkt in Bearbeitung befindlichen Loggingpolicy (s. Punkt 4.1.3 Weiterführende Regelungen). Aus Sicht des StRH Wien wäre es notwendig, die divergierenden Aufbewahrungszeiträume bei thematisch verknüpften und zu erfassenden Daten bzw. Aufzeichnungen in der Loggingpolicy als entsprechende Soll-Vorgabe abzubilden.

Die Durchsicht der bereitgestellten Entwurfsfassung der Loggingpolicy zeigte, dass eine entsprechende Vorgabe nicht enthalten war.

Die Definition des Aufbewahrungszeitraumes als Soll-Kriterium von einem Jahr bzw. 365 Tagen war in der Entwurfsfassung der Loggingpolicy unter dem Kapitel *„Speicherdauer“* für *„… Logs, die personenbezogenen Daten enthalten …“* angeführt und mit dem Ist-Parameter von 400 Tagen zumindest bei einem Teil der Überwachungsdokumentation (audiovisueller Mitschnitt) grundsätzlich ordnungsgemäß angewendet.

Empfehlung:
Der StRH Wien empfahl der MA 01 - Wien Digital, die Harmonisierung von Aufbewahrungszeiträumen bei thematisch verketteten Teilen der Überwachungsdokumentation als entsprechende Soll-Vorgabe in der Loggingpolicy zu evaluieren.

Die Stellungnahme zu dieser Empfehlung wurde im Punkt Zusammenfassung der Empfehlungen eingearbeitet.

Im vorliegenden Fall hätte nach Ansicht des StRH Wien dieser Umstand auch als erfasstes Risiko im Rahmen des Risikomanagements und der z.B. betreffenden internen definierten regelmäßigen oder fallweisen Kontrollen der Betriebsparameter der Fernwartungslösung erkannt werden müssen.

Der StRH Wien verkannte in diesem Zusammenhang nicht, dass eine dokumentierte Soll-Vorgabe - wie z.B. in einer Loggingpolicy - nicht von einer regelmäßigen Wartung und Überprüfung dieser Parameter entbindet.

Der StRH Wien verzichtete aufgrund der umgehend gesetzten Erstmaßnahmen der MA 01 - Wien Digital auf eine weitere tiefergehende Überprüfung dieser Thematik im Risikomanagement und im IKS der MA 01 - Wien Digital.

Empfehlung:
Der StRH Wien empfahl der MA 01 - Wien Digital, die Harmonisierung von divergierenden Aufbewahrungszeiträumen bei thematisch verketteten Teilen einer Überwachungsdokumentation bzw. von Logs und/oder Aufzeichnungen im Risikomanagement und im IKS der MA 01 - Wien Digital zu evaluieren.

Die Stellungnahme zu dieser Empfehlung wurde im Punkt Zusammenfassung der Empfehlungen eingearbeitet.

Die Einschau in die vorhandenen Funktionalitäten für die Überwachungsdokumentation der Applikationsumgebung durch den StRH Wien zeigte, dass diese nicht vollumfänglich verwendet wurden, da mit den beiden o.a. Teilen der Überwachung und der Dokumentation bis dato das Auslangen gefunden wurde.

Die MA 01 - Wien Digital teilte diesbezüglich mit, dass zum Prüfungszeitpunkt an einer Ablöse dieser Fernwartungslösung gearbeitet wird, welche im Jahr 2024 in Betrieb genommen werden soll. Mit dieser neuen Fernwartungslösung wird u.a. für die Fernwartung bzw. den Fernzugriff die Verwaltung, Überwachung und Aufzeichnung von privilegierten Usern (Privileged Access Management) mittels entsprechender Applikationen und Services ein detaillierteres Session Monitoring der Tätigkeiten der Fernwartungsuser und damit auch des Betriebsablaufes der jeweiligen fernzuwartenden Systeme (Server, Clients, Services, Applikationen usw.) eingeführt.

Neben den privilegierten Usern der Fernwartung bzw. des Fernzugriffs werden künftig auch alle anderen privilegierten User aller Systeme - die in der Betriebsverantwortung der MA 01- Wien Digital stehen - entsprechend verwaltet, überwacht und aufgezeichnet.

5.5.2 Fernwartungsuser

Die für die Fernwartung bzw. den Fernzugriff notwendigen Fernwartungsuser unterlagen einem entsprechenden Anforderungs- und Verwaltungsmanagement durch die MA 01 - Wien Digital. Die Prüfung dieses Managements war u.a. Teil der bereits im Bericht angeführten Typ 1 und Typ 2 ISAE 3402 Testate der MA 01 - Wien Digital.

Der StRH Wien forderte in Ergänzung zu diesen Prüfungen eine Auswertung der im Applikationsteil zur Dokumentation von Fernwartungsaktivitäten der Fernwartungslösung gespeicherten Logdaten über die MA 01 - Wien Digital an.

Aufgrund der bereits dargelegten nicht ordnungsgemäß gesetzten Aufbewahrungsfrist dieser Logdaten der Fernwartungsaktivitäten (90 Tage vom aktuellen Datum rückwärts gerechnet) war eine Prüfung des Prüfungsgegenstandes durch den StRH Wien für den Betrachtungszeitraum nicht möglich.

Die MA 01 - Wien Digital stellte daher die Daten mit Stichtag 5. Juli 2023 für den Zeitraum vom 1. April 2023 bis 5. Juli 2023 (96 Tage) bereit. Weiters wurde eine Liste der Fernwartungsuser vom Team Infrastruktur Datacenter - Server Windows der MA 01 - Wien Digital zum gleichen Stichtag erstellt.

Im Rahmen der Datenanalyse durch den StRH Wien wurden die Logdaten der durchgeführten Sessions (Session Start Date and Time sowie Session End Date and Time) über die Userkennung mit dem Beginn- und Ende-Datum und Uhrzeit der Gültigkeit der jeweiligen Fernwartungsuser verbunden und für die explorative Analyse aufbereitet.

Die Datenanalyse des StRH Wien ergab, dass dabei mehr als 60 % der Fernwartungssessions mit ungültigen Fernwartungsusern ausgewiesen wurden. Die weiteren Auffälligkeiten betrafen insbesondere den Zeitpunkt (Wochentag und Uhrzeit) sowie die Zeitdauer von Fernwartungsaktivitäten.

In der folgenden Überprüfung dieser Auffälligkeiten durch die MA 01 - Wien Digital wurde mitgeteilt, dass die betreffenden Spalten der Verrechnung in der bereit gestellten Liste der Fernwartungsuser vom Team Infrastruktur Datacenter - Server Windows aktualisiert wurden, jedoch die Spalten der Gültigkeit mit den Datums- und Zeitangaben von Fernwartungsusern nicht entsprechend gepflegt waren. Dies war lt. MA 01 - Wien Digital dadurch begründet, dass diese Gültigkeitsdaten der Fernwartungsuser in einer entsprechenden weiteren Applikation durch das Team Betriebswirtschaft, Beschaffung und Recht - Vendormanagement eingepflegt bzw. verwaltet wurden.

Seitens der MA 01 - Wien Digital wurden mit 7. Juli 2023 die Datenquellen für die Liste der Fernwartungsuser neu zusammengeführt, sodass in Hinkunft bei jedem neuen Aufruf auch die aktuellen gültigen Fernwartungsuser vom Team Betriebswirtschaft, Beschaffung und Recht - Vendormanagement angezeigt werden.

Die MA 01 - Wien Digital teilte mit, dass als bereits bestehende Maßnahme des IKS das Team Betriebswirtschaft, Beschaffung und Recht - Vendormanagement 1-mal jährlich 1 Monat vor

Ablauf der Gültigkeit eines Fernwartungsusers dem zuständigen Service Delivery Manager eine Information zur Aufforderung der Überprüfung der User ausgesendet wurde. Im Fall einer fehlenden Antwort erfolgte eine Sperre des betroffenden Fernwartungsusers.

Vom StRH Wien wurde am 5. Dezember 2023 ohne vorige Anmeldung bei der MA 01 - Wien Digital gemäß Geschäftsordnung für den Magistrat der Stadt Wien Anhang I Sonderbestimmungen für das Kontrollamt § 4 Abs. 2 über die Gültigkeit der Datumsangaben von Fernwartungsusern im zugrunde liegenden führenden IKT-System des Personalmanagements der Stadt Wien eine entsprechende Einschau vorgenommen.

Im Rahmen dieser Vor-Ort-Prüfung wurden im Mehraugenprinzip in Anwesenheit der MA 01 - Wien Digital (Leiterin der Internen Revision, Datenschutzverantwortliche sowie Gruppenleiter Infrastruktur und Datacenter) und den Prüfern des StRH Wien aus insgesamt 227 Fernwartungsuserkennungen 15 Stück nach dem Zufallsprinzip ausgewählt.

Alle ausgewählten 15 Fernwartungsuserkennungen waren mit den korrekten Datumswerten im führenden System der Verwaltung integrierter Personaldaten/Wiener Integriertes Personalinformationssystem eingetragen. Diese Datumswerte konnten auch in der weiteren Applikation des Teams Betriebswirtschaft, Beschaffung und Recht - Vendormanagement der MA 01 - Wien Digital entsprechend gegengeprüft werden.

Die Vor-Ort-Einschau durch den StRH Wien führte hinsichtlich der Gültigkeit der Fernwartungsuserkennung des Personalmanagements und der Gegenprüfung dieser in der Applikation des Teams Betriebswirtschaft, Beschaffung und Recht - Vendormanagement der MA 01 - Wien Digital zu keinen Beanstandungen.

5.5.3 Security Information und Event Management

Neben den in der Fernwartungslösung implementierten Teilen der Überwachung und der Dokumentation in der Applikationsumgebung (s. Punkt 5.5.1 Fernwartungslösung) wurde während der Prüfung des StRH Wien mit Juli 2023 ein SIEM-System von der MA 01 - Wien Digital produktiv gesetzt bzw. in Betrieb genommen.

Ein SIEM System stellte eine Sicherheitslösung (im Gesamtzusammenhang des ISMS der MA 01 - Wien Digital) dar, welches anhand von Daten der Sicherheitsinformationen (z.B. der Sicherheitsregeln als Soll-Vorgabe) und Daten aus Sicherheitsereignissen (z.B. der Logdaten

der einzelnen Systeme) eine Echtzeitanalyse und Überwachung der darin eingebundenen Systeme ermöglichte. Auf Basis dieser Echtzeitanalyse wurden im Rahmen der Überwachung entsprechend der definierten Eskalationsstufen Hinweise, Meldungen, Warnungen bis hin zu Alarmen generiert und den jeweiligen Betreffenden (wie z.B. bei schwerwiegenden Sicherheitsvorfällen das WienCERT der MA 01 - Wien Digital) alarmiert. Dieses System diente nicht ausschließlich der Verwaltung, Überwachung und Aufzeichnung der Tätigkeiten und dem Betriebsgeschehen der Systeme der Fernwartung bzw. des Fernzugriffs, sondern allen in der Betriebsverantwortung der MA 01 - Wien Digital stehenden Systemen.

Für den StRH Wien war erkennbar, dass mit der Inbetriebnahme des SIEM-Systems - in Ergänzung zur Überwachung und Dokumentation in der Applikationsumgebung der Fernwartung - das Konzept der Cybersicherheitsstrategie „Defense in Depth“ verfolgt, weiter ausgebaut und verbessert wurde.

Die MA 01 - Wien Digital legte die SIEM-Architektur redundant und lastverteilend auf Basis der Dokumentation der organisatorischen Systemarchitektur der SIEM-Lösung dem StRH Wien dar. Eine vertiefende detailliertere Einschau und Prüfung dieser SIEM-Systemarchitektur wurde nicht durchgeführt.

Die MA 01 - Wien Digital stellte dem StRH Wien eine 1. grobe Detailierung der verschiedenen meldenden Systeme - welche u.a. die Systeme mit Fernwartung bzw. Fernzugriff beinhaltete - und deren Statistik bereit.

Mit der Inbetriebnahme der SIEM-Lösung durch die MA 01 - Wien Digital haben mit Stand 6. Oktober 2023 bereits mehr als 70.000 Systeme (Server, Clients, Services, Applikationen usw.) entsprechende Ereignisse übermittelt. Diese Systeme verteilten sich dabei wie folgt:

- rd. 3.900 Microsoft Windows Server mit:
- rd. 2.000 Server im Magistrat der Stadt Wien,
- rd. 1.900 Server im Wiener Gesundheitsverbund (davon rd. 700 Server im Teilunternehmen Allgemeines Krankenhaus Wien),
- rd. 1.500 Linux Server,
- rd. 63.000 Microsoft Windows Clients mit:
- rd. 23.000 Clients im Magistrat der Stadt Wien,
- rd. 26.000 Clients im Wiener Gesundheitsverbund (davon rd. 6.000 Clients im Teilunternehmen Allgemeines Krankenhaus Wien),

- rd. 14.000 Clients der Schulen der Stadt Wien sowie
- weitere zahlreiche Netzwerksysteme wie z.B. Router und Switches, die zum Prüfungszeitpunkt in der Bearbeitung der Einbindung in das SIEM standen.

Neben den voran angeführten Systemen aus hardwaretechnischer Sicht waren entsprechende Systeme aus softwaretechnischer Sicht mit verschiedenen Applikationen und Services eingebunden. Die Vor-Ort-Einschau betreffend die eingebundenen Systeme zeigte, dass neben den standardmäßigen Applikationen bzw. Services der Firewall, des Web Proxy, des Security Event Logs für Windows und Linux, des Virenscanners, des E-Mail Scanners usw. auch die Services bzw. Applikationen aus der Applikationsumgebung der Fernwartung bzw. des Fernzugriffs bereits eingebunden bzw. deren Einbindung vorgesehen waren.

Die an das SIEM angebundene Systeme generierten zu Spitzenzeiten unter Tags rd. 10.000 Events pro Sekunde. Das Lizenzlimit des eingesetzten SIEM-Systems lag zum Prüfungszeitpunkt bei 12.500 Events pro Sekunde. In der Analyse dieser Events über definierte „Use Cases“ wurden in der höchsten Eskalationsstufe ca. 3 Alarme pro Woche an das WienCERT-Ticketsystem zum Prüfungszeitpunkt gemeldet, welche unmittelbar behandelt werden mussten.

Die MA 01 - Wien Digital rechnete in den nächsten Wochen und Monaten mit einem Anstieg dieser Alarmierungen, da immer mehr „Use Cases“ durch die Umsetzung eingesetzt und feinjustiert werden müssen. Die Herausforderung war dabei u.a., die „False Positive“ aus einem „Use Case“ gering zu halten und dadurch eine Überalarmierung und folglich einer Alarmermüdung bzw. Überlastung im WienCERT hintanzuhalten.

Für den StRH Wien war in der Vor-Ort-Einschau das betreffende Produkt aus der Applikationsumgebung der Fernwartungslösung als eingebundener Log Source Typ im SIEM ersichtlich. Zum Zeitpunkt der Vor-Ort-Einschau waren aktuell 400.528 eingemeldete Events innerhalb der letzten Stunde ausgewiesen.

Gemäß Auskunft der MA 01 - Wien Digital war die Einbindung des Privileged Access Management Systems zum Prüfungszeitpunkt in Bearbeitung. Das Privileged Access Management System lieferte als weiterer Log Source Typ erste Events in das SIEM-System. Auch in diesem Zusammenhang werden die definierten bzw. noch zusätzlichen „Use Cases“ eine entsprechende Detailarbeit und Feinjustierung des Privileged Access Management Systems in den nächsten Wochen und Monaten erfordern.

In der Vor-Ort-Einschau des StRH Wien zu den „Use Cases“ des SIEM waren im Zusammenhang zur Fernwartung bzw. zum Fernzugriff entsprechende standardisierte „generische Use Cases“ definiert und bereits im Einsatz. Dies betraf z.B. die „generischen Use Cases“ zur Erfassung, Analyse, Dokumentation und Meldung im Zusammenhang mit Logins oder zum Zugriff von Fernwartungsusern in der Fernwartungslösung als auch am jeweilig fernzuwartenden Zielsystem.

Eine entsprechende Dokumentation aller „Use Cases“ war über ein elektronisches Wiki von der MA 01 - Wien Digital dokumentiert. Neben der inhaltlichen Dokumentation jedes Use Cases mit u.a. eindeutiger Identifikation, Beschreibung, Strukturierung, Log Source Typ, technischer Definition bzw. Programmierung im entsprechenden „Use Case“ Source Code war zusätzlich auch der Stand der Implementierung mit den entsprechenden Stati im Ampelsystem (z.B. Design, Implemented, Monitored, Productive) ausgewiesen.

Infolge der Datenanalyse des StRH Wien (s. Punkt 5.5.2 Fernwartungsuser) wurden weitere 4 „Use Cases“ für die Erweiterung der SIEM-Funktionalität von Verantwortlichen des SIEM identifiziert und in das „Use Cases“ Portfolio des SIEM zur weiteren Beachtung und Evaluierung aufgenommen. Diese „Use Cases“ standen im Zusammenhang mit der Sessionnutzung, der Zeitdauer, dem Zeitpunkt und dem Login.

Der StRH Wien begrüßte die proaktive Identifikation und Aufnahme von weiteren „Use Cases“ im Zuge der Überprüfung der Fernwartung bzw. des Fernzugriffs und sah daher von einer Empfehlung ab.

Die MA 01 - Wien Digital plante in weiterer Folge Hinweise, Meldungen und Warnungen des SIEM an den Helpdesk zur Beurteilung und Veranlassung der Bearbeitung zu übermitteln. Die Erstellung gesonderter Dashboards mit den relevanten und aufbereitenden Daten und Informationen des SIEM für eine innerbetriebliche Sicht der Betriebsgruppen (z.B. der Betriebsgruppe der Fernwartung bzw. des Fernzugriffs oder der Internen Revision aus der Sicht des IKS und dem „Continous Auditing“-Ansatz) war von der MA 01 - Wien Digital nicht vorgesehen.

In diesem Zusammenhang war vom StRH Wien anzumerken, dass mit dem Data Excellence Programm der Stadt Wien die MA 01 - Wien Digital am Aufbau eines Reportingssystems mit

Daten-Dashboards unter Verwendung einer Business-Intelligence-, Analyse- und Reportingssoftware arbeitet. Als Beispiel dafür wären die Arbeiten an Dashboards mit Daten und Informationen zu IKT-Projekten für eine interne Übersicht und Steuerung zu nennen. Vom StRH Wien wurde dazu auf den Punkt 4.3 des Berichtes des StRH Wien (MA 01, Prüfung des Projektmanagements von IKT-Projekten der Dienststellen des Magistrats der Stadt Wien; StRH I - 1135335-2022) hingewiesen.

Mit dem Erlass „Data Excellence im Magistrat der Stadt Wien; Bestellung einer Data Governance - Koordinatorin“ (MDK - 1389385-2023-1) vom 16. November 2023 wurde die Entwicklung der internen Nutzung von Daten und Informationen als zentraler Wert für die Stadt Wien und deren Dienststellen zur Darstellung, Berichtslegung und Grundlage der Steuerung entsprechend weiter Rechnung getragen.

Empfehlung:
Der StRH Wien empfahl der MA 01 - Wien Digital, eine Evaluierung der Nutzung von Daten und Informationen des SIEM und der darin eingebundenen Systeme (im Zusammenhang mit den Arbeiten im Rahmen des Data Excellence Programmes der Stadt Wien) hinsichtlich der verschiedenen Sichtweisen der jeweiligen Betriebsgruppe bzw. der Internen Revision insbesondere in der Thematik der Fernwartung und des Fernzugriffs vorzunehmen.

Die Stellungnahme zu dieser Empfehlung wurde im Punkt Zusammenfassung der Empfehlungen eingearbeitet.

In der weiteren Vor-Ort-Einschau zur Aufbewahrungsfrist war zum Prüfungszeitpunkt in Abstimmung mit dem Team „Recht, Vertrags- und Lizenzmanagement“ der MA 01 - Wien Digital hinsichtlich der Datenschutzvorgaben eine Haltefrist der Events von 1 Jahr definiert und als gesetzter Parameter im SIEM-System ersichtlich.

Der StRH Wien verwies hinsichtlich der Aufbewahrungsfrist auf die Loggingpolicy und der dazu ausgesprochenen Empfehlung im Punkt 4.1.3 Weiterführende Regelungen.

6. Zusammenfassung der Empfehlungen

Empfehlung Nr. 1:
Der Abschluss eines Service Level Agreements für das Intranetservice der Stadt Wien sollte evaluiert werden (s. Punkt 2.2).

Stellungnahme der MA 01 - Wien Digital:
Die Empfehlung wird evaluiert sowie unter Beachtung der Wirtschaftlichkeit umgesetzt.

Empfehlung Nr. 2:
Generische Überlegungen zur Verkürzung der bereitgestellten bzw. benötigten Zeitdauer bei notwendigen, sicherheitsrelevanten und daher zeitnah zu setzenden Maßnahmen unter Einbeziehung der relevanten Kundinnen bzw. Kunden wären anzustellen. Diese sollten im Rahmen der Strategien, Prozesse und Maßnahmen des BCM einfließen, um damit auch die Verfügbarkeit der entsprechenden IKT-Services gemäß den Service Level Agreements sicherzustellen (s. Punkt 2.2).

Stellungnahme der MA 01 - Wien Digital:
Die Empfehlung wird evaluiert sowie unter Beachtung der Wirtschaftlichkeit umgesetzt.

Empfehlung Nr. 3:
Die geplanten Maßnahmen hinsichtlich der Automatisierung bei Tests von Abänderungen im Intranetservice der Stadt Wien sollten konsequent verfolgt werden (s. Punkt 2.2).

Stellungnahme der MA 01 - Wien Digital:
Die Empfehlung wird evaluiert sowie unter Beachtung der Wirtschaftlichkeit umgesetzt.

Empfehlung Nr. 4:
Die geplante Umsetzung der Verbesserung der Schulungsunterlagen für die Redakteurinnen bzw. Redakteure des Intranetservices der Stadt Wien hinsichtlich der Klassifizierung von Dokumenten bzw. Inhalten sowie der Auswahl des richtigen Systems für die Verwendung bzw. die Ablage von Dokumenten wäre konsequent zu verfolgen (s. Punkt 2.2).

Stellungnahme der MA 01 - Wien Digital:
Die Empfehlung wird evaluiert sowie unter Beachtung der Wirtschaftlichkeit umgesetzt.

Empfehlung Nr. 5:
Das Kapitel Rahmenbedingungen in der Fernwartungspolicy wäre bei Aktualisierung der externen gesetzlichen Bestimmungen und Regelungen im Hinblick auf das NISG und die NISV anzupassen (s. Punkt 4.1.1).

Stellungnahme der MA 01 - Wien Digital:
Die Empfehlung wird evaluiert sowie unter Beachtung der Wirtschaftlichkeit umgesetzt.

Empfehlung Nr. 6:
Bei Änderungen der Fernwartungspolicy sollte sowohl auf die rechtzeitige Aktualisierung dieses Dokuments in entsprechenden Versionen als auch auf die ordnungsgemäße Führung der Versionshistorie geachtet werden (s. Punkt 4.1.1).

Stellungnahme der MA 01 - Wien Digital:
Die Empfehlung wird evaluiert sowie unter Beachtung der Wirtschaftlichkeit umgesetzt.

Empfehlung Nr. 7:
Die organisatorischen und technischen Anforderungen hinsichtlich Fernwartung bzw. Fernzugriff bei OT-Systemen in den zugrunde liegenden Regelungen, den entsprechenden Detailvorgaben und der weiteren Umsetzung wären zeitnah und nachvollziehbar zu definieren (s. Punkt 4.1.2).

Stellungnahme der MA 01 - Wien Digital:
Die Empfehlung wird evaluiert sowie unter Beachtung der Wirtschaftlichkeit umgesetzt.

Empfehlung Nr. 8:
Eine Evaluierung einer taxativ vollständigen Erfassung bzw. Inventarisierung von OT-Systemen mit Fernwartung bzw. Fernzugriff durch die MA 01 - Wien Digital sollte vorgenommen werden (s. Punkt 4.1.2).

Stellungnahme der MA 01 - Wien Digital:
Die Empfehlung wird evaluiert sowie unter Beachtung der Wirtschaftlichkeit umgesetzt.

Empfehlung Nr. 9:
Bei den abgebildeten Bezügen zu weiteren Bestimmungen, Regelungen, Verlinkungen usw. in der Fernwartungspolicy wäre auf eine ordnungsgemäße bzw. konsistente Darstellung zu achten (s. Punkt 4.1.3).

Stellungnahme der MA 01 - Wien Digital:
Die Empfehlung wird evaluiert sowie unter Beachtung der Wirtschaftlichkeit umgesetzt.

Empfehlung Nr. 10:
Die Fertigstellung der Loggingpolicy sollte vorangetrieben und diese zeitnah im Betrieb der betreffenden Systeme - insbesondere im Zusammenhang zur Thematik der Fernwartung bzw. des Fernzugriffs - umgesetzt und angewendet werden (s. Punkt 4.1.3).

Stellungnahme der MA 01 - Wien Digital:
Die Empfehlung wird evaluiert sowie unter Beachtung der Wirtschaftlichkeit umgesetzt.

Empfehlung Nr. 11:
Auf die ordnungsgemäße Dokumentation und Aufbewahrung mittels elektronischer Aktenführung - insbesondere der entsprechenden Policies, Regelungen und Vorgaben betreffend die Fernwartung - gemäß Büroordnung der Stadt Wien und Akten- und Skartierungsplan wäre zu achten (s. Punkt 4.1.4).

Stellungnahme der MA 01 - Wien Digital:
Die Empfehlung wird evaluiert sowie unter Beachtung der Wirtschaftlichkeit umgesetzt.

Empfehlung Nr. 12:
Bei der Protokollierung von Inhalten zur Fernwartung in der elektronischen Aktenführung sollte auf die ordnungsgemäße und zeitnahe Zuordnung im Zuge der erstmaligen Erstellung des entsprechenden vorgegebenen Sachgebietes des Akten- und Skartierungsplanes geachtet werden (s. Punkt 4.1.4).

Stellungnahme der MA 01 - Wien Digital:
Die Empfehlung wird evaluiert sowie unter Beachtung der Wirtschaftlichkeit umgesetzt.

Empfehlung Nr. 13:
Die Aufnahme von konkreten Vorgaben zur effektiven operativen Umsetzung von Maßnahmen zur Fernwartung bzw. des Fernzugriffs (wie Österreichisches Informationssicherheitshandbuch oder IT - Grundschutz-Baustein des Bundesamtes für Sicherheit der Bundesrepublik Deutschland) wäre in den entsprechenden Regelungen zu evaluieren (s. Punkt 4.1.5).

Stellungnahme der MA 01 - Wien Digital:
Die Empfehlung wird evaluiert sowie unter Beachtung der Wirtschaftlichkeit umgesetzt.

Empfehlung Nr. 14:
Auf eine ordnungsgemäße und konsistente Abbildung der Vorgehensweise bei „Abweichungen“ und „Ausnahmen“ in der Fernwartungspolicy sollte geachtet werden (s. Punkt 4.1.6).

Stellungnahme der MA 01 - Wien Digital:
Die Empfehlung wird evaluiert sowie unter Beachtung der Wirtschaftlichkeit umgesetzt.

Empfehlung Nr. 15:
Eine Prüfung und Genehmigung durch das WienCERT der MA 01 - Wien Digital bei „Ausnahmen“ und „Abweichungen“ hinsichtlich Fernwartungen bzw. Fernzugriffen wäre bei OT-Systemen zu evaluieren (s. Punkt 4.1.6).

Stellungnahme der MA 01 - Wien Digital:
Die Empfehlung wird evaluiert sowie unter Beachtung der Wirtschaftlichkeit umgesetzt.

Empfehlung Nr. 16:
Im Organisationshandbuch sollte auf die durchgängige Dokumentation bzw. inhaltliche Abbildung der Thematik der Fernwartung bzw. des Fernzugriffs in den jeweiligen Kapiteln der Organisationseinheiten der MA 01 - Wien Digital geachtet werden (s. Punkt 5.1.1).

Stellungnahme der MA 01 - Wien Digital:
Die Empfehlung wird evaluiert sowie unter Beachtung der Wirtschaftlichkeit umgesetzt.

Empfehlung Nr. 17:
Die Anwendung der RFC 2119 Schlüsselwörter zur Verwendung und zur Angabe von Anforderungsniveaus in der Fernwartungspolicy sowie den damit in Verbindung stehenden bzw. der damit referenzierten weiteren Richtlinien und Policies sollte evaluiert werden (s. Punkt 5.3).

Stellungnahme der MA 01 - Wien Digital:
Die Empfehlung wird evaluiert sowie unter Beachtung der Wirtschaftlichkeit umgesetzt.

Empfehlung Nr. 18:
Eine Evaluierung der Harmonisierung der unterschiedlichen Aufbewahrungszeiträume der beiden Teile der Überwachungsdokumentation von Fernwartungsaktivitäten wäre durchzuführen (s. Punkt 5.5.1).

Stellungnahme der MA 01 - Wien Digital:
Die Empfehlung wird evaluiert sowie unter Beachtung der Wirtschaftlichkeit umgesetzt.

Empfehlung Nr. 19:
Die Harmonisierung von Aufbewahrungszeiträumen bei thematisch verketteten Teilen der Überwachungsdokumentation als entsprechende Soll-Vorgabe in der Logginpolicy sollte evaluiert werden (s. Punkt 5.5.1).

Stellungnahme der MA 01 - Wien Digital:
Die Empfehlung wird evaluiert sowie unter Beachtung der Wirtschaftlichkeit umgesetzt.

Empfehlung Nr. 20:
Die Harmonisierung von divergierenden Aufbewahrungszeiträumen bei thematisch verketteten Teilen einer Überwachungsdokumentation bzw. von Logs und/oder Aufzeichnungen im Risikomanagement und im IKS der MA 01 - Wien Digital wäre zu evaluieren (s. Punkt 5.5.1).

Stellungnahme der MA 01 - Wien Digital:
Die Empfehlung wird evaluiert sowie unter Beachtung der Wirtschaftlichkeit umgesetzt.

Empfehlung Nr. 21:
Eine Evaluierung der Nutzung von Daten und Informationen des SIEM und der darin eingebundenen Systeme (im Zusammenhang mit den Arbeiten im Rahmen des Data Excellence Programmes der Stadt Wien) hinsichtlich der verschiedenen Sichtweisen der jeweiligen Betriebsgruppe bzw. der Internen Revision insbesondere in der Thematik der Fernwartung und des Fernzugriffs sollte vorgenommen werden (s. Punkt 5.5.3).

Stellungnahme der MA 01 - Wien Digital:
Die Empfehlung wird evaluiert sowie unter Beachtung der Wirtschaftlichkeit umgesetzt.

Der Stadtrechnungshofdirektor:
Mag. Werner Sedlak, MA
Wien, im Februar 2024