STADTRECHNUNGSHOF WIEN
Landesgerichtsstraße 10
A-1082 Wien

Tel.: 01 4000 82829 FAX: 01 4000 99 82810
E-Mail: post@stadtrechnungshof.wien.at
www.stadtrechnungshof.wien.at

StRH I - 13/18

MA 01, Prüfung von Steuerungssystemen

KURZFASSUNG

Im Rahmen der gegenständlichen Prüfung wurden die im Magistrat der Stadt Wien eingesetzten Supervisory Control and Data Acquisition-Systeme bzw. die damit im Zusammenhang stehenden Mess-, Steuer- und Regelungssysteme hinsichtlich der Einhaltung der Vorgaben der Informations- und Kommunikationstechnologie-Sicherheit einer Prüfung unterzogen.

Dabei war festzustellen, dass die gegenständliche Prüfungsthematik aufgeteilt in der Verantwortung der Magistratsabteilung 01, der Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Prozessmanagement und Informations- und Kommunikationstechnologie-Strategie bzw. dem Chief Information Security Officer der Stadt Wien sowie der jeweilig betroffenen bzw. betriebsführenden Dienststelle und weiteren allenfalls damit beauftragten Fremdfirmen lag. Von Seiten der Magistratsabteilung 01 wurde proaktiv die Thematik für den eigenen Wirkungsbereich erarbeitet und mittels einer grundlegenden Policy bzw. Leitfaden entsprechend für die allfällig weiteren betroffenen Organisationseinheiten (zum Beispiel betriebsführenden Dienststellen) bereitgestellt.

Verbesserungspotenzial bestand bei der Magistratsabteilung 01 in der Dokumentation der Vorgänge (Aktendokumentation) und der Bereitstellung und Aktualisierung der entsprechenden Fachexpertise in den Vorgaben der Informations- und Kommunikationstechnologie-Sicherheit für die Wissensvermittlung (Intranet) von im Magistrat der Stadt Wien bei den jeweils betriebsverantwortlichen Dienststellen eingesetzten Automatisierungssystemen (Supervisory Control and Data Acquisition- bzw. Mess-, Steuer- und Regelungssystemen).

Insbesondere ergingen Empfehlungen zum ganzheitlichen Management (unter anderem der Organisation und Koordination), in der inhaltlichen Ausgestaltung der Grundlagen und Vorgaben, der Verbindlichkeit der Anwendung, der Erfassung und der Kategorisierung der Thematik der Informations- und Kommunikationstechnologie-Sicherheit bei im

Magistrat der Stadt Wien eingesetzten Automatisierungssystemen (Supervisory Control and Data Acquisition- bzw. Mess-, Steuer- und Regelungssystemen). Deren Umsetzung sollte unter Berücksichtigung einer entsprechenden Abstimmung mit der Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Prozessmanagement und Informations- und Kommunikationstechnologie-Strategie bzw. dem Chief Information Security Officer der Stadt Wien erfolgen.

Der Stadtrechnungshof Wien unterzog die Magistratsabteilung 01 hinsichtlich der IKT-Sicherheit bei verwendeten Steuerungssystemen der Stadt Wien 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

1. Prüfungsgrundlagen des Stadtrechnungshofes Wien 13
1.1 Prüfungsgegenstand 13
1.2 Prüfungszeitraum 14
1.3 Prüfungshandlungen 14
1.4 Prüfungsbefugnis 15
1.5 Vorberichte 15
2. Allgemeines 15
2.1 Geschichtlicher Hintergrund der Automatisierung 15
2.2 Ebenen der Automatisierung 17
2.3 Mess-, Steuer- und Regelungssysteme (LEVEL 1) 19
2.4 Supervisory Control and Data Acquisition-Systeme (LEVEL 2) 20
2.5 Abgrenzung von Automatisierungssystemen 21
2.6 Kommunikation innerhalb von Automatisierungssystemen 21
2.7 Weitere technische Ausprägungen bei Automatisierungssystemen 22
2.8 Gesamtes Zusammenwirken in Automatisierungssystemen 22
2.9 Lebensdauer bzw. Lebenszyklus von Automatisierungssystemen 23
2.10 Schutzinteressen in Automatisierungssystemen 23
2.11 Kritische Infrastruktur 24
3. Rechtliche Grundlagen 25
3.1 Allgemeines 25
3.2 Europäische Union 26

3.3 Österreichische Strategie für Cyber Sicherheit 26
3.4 Netz- und Informationssystemsicherheit 26
3.5 Normen bzw. Erlässe des Magistrats der Stadt Wien 27
3.6 Regelwerke bzw. Leitfäden 28
3.7 International Electrotechnical Commission 62443 Industrielle Kommunikationsnetze - Informationstechnologie Sicherheit für Netze und Systeme 29
4. Organisatorische Feststellungen 29
4.1 Verantwortungen innerhalb der Stadt Wien 29
4.2 Definition von Supervisory Control and Data Acquisition- bzw. Mess-, Steuer- und Regelungssystemen durch die Magistratsabteilung 01 32
4.3 Sensibilisierung im Hinblick auf das Thema Sicherheit bei Supervisory Control and Data Acquisition- bzw. Mess-, Steuer- und Regelungssystemen 34
4.4 Erstellung und Gültigkeit der Policy bzw. Richtlinie der Magistratsabteilung 01 35
4.5 Erfassung der eingesetzten Supervisory Control and Data Acquisition- bzw. Mess-, Steuer- und Regelungssysteme 37
4.6 Kategorisierung bzw. Priorisierung der erfassten Supervisory Control and Data Acquisition- bzw. Mess-, Steuer- und Regelungssysteme 38
4.7 System- bzw. Sicherheitsprüfungen (Penetrationstests) 40
5. Stichprobenweise Überprüfung eines Supervisory Control and Data Acquisition- bzw. Mess-, Steuer- und Regelungssystems 44
6. Zusammenfassung der Empfehlungen 46

ABBILDUNGSVERZEICHNIS

Abbildung 1: Eingabe-Verarbeitung-Ausgabe Prinzip in der Automatisierung 17
Abbildung 2: Ebenen der Automatisierung (Automatisierungspyramide) 17
Abbildung 3: Zusammenwirken der einzelnen Systeme in der Automatisierung bzw. der Operational Technology 23

ABKÜRZUNGSVERZEICHNIS

Abs.	Absatz
AKH-DTI	Allgemeines Krankenhaus - Technik und Informatik
APCIP	Austrian Program for Critical Infrastructure Protection
BCM	Business Continuity Management
bzw.	beziehungsweise
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPS	Cyber Physisches System
E	Electronic
E-Mail	Elektronische Post
ERP	Enterprise Resource Planning
etc.	et cetera
EVA	Eingabe-Verarbeitung-Ausgabe
GmbH	Gesellschaft mit beschränkter Haftung
https	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
IKS	Internes Kontrollsystem
IKT	Informations- und Kommunikationstechnologie
IMK	Ingenieurbüro für Mechatronik und Kybernetik
Inc.	Incorparated
IoT	Internet of Things
ISMS	Informations Sicherheits Management System
ISO	International Organization for Standardization

IT	Informationstechnologie
KA	Kontrollamt
KAV-IT	Unternehmung Wiener Krankenanstaltenverbund - Informationstechnologie
Krankenanstaltenverbund	Unternehmung Wiener Krankenanstaltenverbund
MDK	Magistratsdirektor - Gruppe Koordination
MD-OS	Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit
MSR-System	Mess-, Steuer- und Regelungssystem
NISG	Netz- und Informationssystemsicherheitsgesetz
Nr.	Nummer
o.a.	oben angeführt
OT	Operational Technology
PAC	Programmable Automation Controller
PLC	Programmable Logic Controller
QR	Quick Response
rd.	rund
s.	siehe
SCADA	Supervisory Control and Data Acquisition
SCM	Service Continuity Management
SPS	Speicherprogrammierbare Steuerung
u.a.	unter anderem
URL	Uniform Resource Locator
usw.	und so weiter
VPN	Virtual Private Network
WAN	Wide Area Network
WienCERT	Wien Computer Emergency Response Team
www	World Wide Web
z.B.	zum Beispiel
Zl.	Zahl

LITERATURVERZEICHNIS

Gabler Wirtschaftslexikon; Spinger Gabler | Springer Fachmedien Wiesbaden GmbH, Cyberspace, (Online) 19. Februar 2018 (Zitat vom: 31. Dezember 2019), https://wirtschaftslexikon.gabler.de/definition/cyberspace-31826/version-255377

Wikimedia Foundation Inc. Cyberspace, (Online) 9. August 2018 (Zitat vom: 31. Dezember 2019), https://de.wikipedia.org/wiki/Cyberspace

Vogel IT-Medien GmbH. Was ist das Internet of Things? (Online) 1. September 2016 (Zitat vom: 2. Jänner 2020), https://www.bigdata-insider.de/was-ist-das-internet-of-things-a-590806/

Was ist das Industrial Internet of Things (IIoT)? (Online) 20. Oktober 2017 (Zitat vom: 2. Jänner 2020), https://www.bigdata-insider.de/was-ist-das-industrial-internet-of-things-iiot-a-654986/

Verein Industrie 4.0 Österreich - die Plattform für intelligente Produktion, Was ist Industrie 4.0? (Online) 2019 (Zitat vom: 2. Jänner 2020), https://plattform-industrie40.at/was-ist-industrie-4-0/

Wikimedia Foundation Inc. Operational Technology, (Online) 25. November 2019 (Zitat vom: 30. Dezember 2019), https://en.wikipedia.org/wiki/Operational_Technology

Gartner Inc. Operational Technologie (ot), (Online) 2019 (Zitat vom: 30. Dezember 2019), https://www.gartner.com/en/information-technology/glossary/operational-technology-ot

Dipl. Ing. Christian Perst, itEXPERsT, Penetrationstest in Österreich und Deutschland - Auf Herz und Nieren geprüft, (Online) 2019 (Zitat vom: 30. Juli 2019), https://www.itexperst.at/leistungen/penetrationstest

Wikimedia Foundation Inc. Resilienz (Ingenieurwissenschaften), (Online) 9. Mai 2019 (Zitat vom: 31. Dezember 2019), https://de.wikipedia.org/wiki/Resilienz_(Ingenieurwissenschaften)

EVA-Prinzip, (Online) 14. Juni 2019 (Zitat vom: 1. August 2019), https://de.wikipedia.org/wiki/EVA-Prinzip

Klaus Hirling, Gottlieb-Daymler Gymnasium Bad Canstatt, Steuerung, (Online) 2013 (Zitat vom: 1. August 2019), http://www.roboter-im-unter-richt.de/steuerung.html

Wikimedia Foundation Inc. Automatisierungspyramide, (Online) 13. Oktober 2019 (Zitat vom: 30. Dezember 2019), https://de.wikipedia.org/wiki/Automatisierungspyramide

IMK - Ingenieurbüro für Mechatronik und Kybernetik, Industrie 4.0, (Online) 2019 (Zitat vom: 30. Dezember 2019), https://imk.engineering/industrie-4.0.html

Trend Micro. Industrial Control System, (Online) 2019 (Zitat vom: 1. August 2019), https://www.trendmicro.com/vinfo/us/security/definition/industrial-control-system

Wikimedia Foundation Inc. Chief Information Officer, (Online) 18. Juli 2018 (Zitat vom: 8. August 2019), https://de.wikipedia.org/wiki/Chief_Information_Officer

Chief Information Security Officer, (Online) 18. Juli 2018 (Zitat vom: 8. August 2019), https://de.wikipedia.org/wiki/Chief_Information_Security_Officer

Cyber-physisches System, (Online) 16. November 2018 (Zitat vom: 2. Jänner 2020), https://de.wikipedia.org/wiki/Cyber-physisches_System

GLOSSAR

CIO

Der CIO (IT-Leiter) ist in einem Unternehmen üblicherweise für die strategische und operative Führung der IT im Unternehmen verantwortlich.

CISO

Der CISO ist in einem Unternehmen für die gesamte Informationssicherheit zuständig. Dies inkludiert u.a. das darunter zugeordnete Thema der IT-Sicherheit. Dieser ist in einem Unternehmen meistens der Geschäftsführerin bzw. dem Geschäftsführer gegenüber verantwortlich.

CPS

Ein CPS stellt einen Verbund von Komponenten dar, bei dem ein Informationssystem (Daten bzw. Informationen mit der entsprechenden Hard- und Software) ein Objekt mit realen mechanischen und elektrischen bzw. elektronischen Bauteilen mit den jeweiligen Vorgängen beeinflusst (z.B. Schrankenanlage eines Bahnüberganges).

Cyber Raum (Cyberspace)

Als Cyber Raum wird ein Bereich definiert der eine nicht real existierende Welt (Scheinwelt) abbildet und nur unter Zuhilfenahme von Hard- und Software und den betreffenden Daten bzw. Informationen benutzt werden kann.

IoT

Das IoT ist die Vernetzung von Gegenständen des täglichen Alltags vorwiegend für die Interaktion (Austausch von Informationen) von Menschen mit den entsprechenden Geräten bzw. Objekten.

IIoT

Das IIoT stellt die industrielle Ausprägung des IoT dar. Dabei stehen nicht die verbraucher- bzw. anwenderorientierten Interessen im Vordergrund, sondern die Interessen des produzierenden bzw. industriellen Umfeldes und deren Prozesse in der Interaktion von Maschinen und Geräten (Echtzeit-Interaktion).

Industrie 4.0

Industrie 4.0 digitalisiert und vernetzt die gesamte Wertschöpfungskette industrieller Produktionsprozesse.

OT

Unter OT wird "Hardware und Software, die eine Änderung durch die direkte Überwachung und/oder Kontrolle von physikalischen Geräten, Prozessen und Ereignissen im Unternehmen erkennen oder verursachen" verstanden.

Penetrationstest (Pentest)

Unter einem Penetrationstest wird ein umfassender Test der Sicherheit möglichst aller Systemteile (Hardware) und Anwendungen (Software) von Informationssystemen, IKT Endgeräten bzw. eines Netzwerkes verstanden. Dabei gelangen Mittel und Methoden zum Einsatz, die eine Angreiferin bzw. ein Angreifer ("Hacker") anwenden würde, um in das betreffende Informationssystem, das IKT Endgerät bzw. eines Netzwerkes unautorisiert einzudringen (Penetration) versucht. Dabei werden unterschiedliche Werkzeuge eingesetzt, um die im Lauf der Zeit bekannt gewordenen, jeweiligen Angriffsmuster, z.B. das Ausprobieren von im Internet nicht autorisiert veröffentlichten Zugangsdaten (Datenbanken mit Leaks von Username und Passwort), anzuwenden.

Resilienz

Resilienz - im Zusammenhang mit technischen Systemen - steht dabei im Wesentlichen für die Fähigkeit eines Systems, welches Gefahren ausgesetzt ist, deren Folgen zeitgerecht und wirkungsvoll zu bewältigen, mit ihnen umzugehen, sich ihnen anzupassen und sich von ihnen zu erholen, ohne vollständig zu versagen.

PRÜFUNGSERGEBNIS

1. Prüfungsgrundlagen des Stadtrechnungshofes Wien

1.1 Prüfungsgegenstand

Prüfungsgegenstand waren die im Magistrat der Stadt Wien eingesetzten SCADA-Systeme bzw. die damit in Zusammenhang stehenden MSR-Systeme hinsichtlich der Einhaltung der Vorgaben der IKT-Sicherheit.

Ziel der gegenständlichen Prüfung war es, jene unmittelbar mit der IKT-Sicherheit von SCADA-Systemen bzw. MSR-Systemen im Zusammenhang stehenden Verantwortungs- bzw. Zuständigkeitsbereiche, als auch die daraus getätigten Maßnahmen zu eruieren.

Die Schwerpunkte der Prüfung lagen dabei vorwiegend auf die Gewährleistung der Betriebskontinuität - BCM - dieser SCADA- bzw. MSR-Systeme und auf den für den Fachbereich der IKT maßgebenden Angriffssicherheit (Security als Schutz des betreffenden Objektes vor der Umgebung). Dabei wurde beurteilt, inwieweit die betriebsführenden Dienststellen jenen durch die Magistratsabteilung 01 ausgearbeiteten "Securityvorgaben für Regelungs-, Steuerungs- und Messsysteme" nachkommen und in welcher Form die aus durchgeführten System- bzw. Sicherheitsprüfungen (Penetrationstests) hervorgegangenen Mängel behoben wurden.

Von der Magistratsabteilung 01 wurden mit 1. Juli 2018 entsprechende Aufgaben der "KAV-IT" und der "AKH-DTI" übernommen.

Nichtziel der Prüfung war in diesem Zusammenhang die Überprüfung von SCADA- bzw. MSR-Systemen jener Organisationseinheiten, die von der Magistratsabteilung 01 übernommen wurden. Ebenso wurden die SCADA- bzw. MSR-Systeme der Unternehmungen der Stadt Wien von der Prüfung ausgenommen.

Nichtziel der Prüfung war ferner die Beurteilung der Beschaffungsvorgänge der von der Magistratsabteilung 01 bzw. von den Magistratsdienststellen des Magistrats der Stadt Wien betriebenen SCADA- bzw. MSR-Systeme.

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

Die gegenständliche Prüfung wurde von der Gruppe Gebarung (Abteilung Kultur und Bildung) und der Gruppe Sicherheitstechnik (Abteilung Behörden und Kommunaltechnik) des Stadtrechnungshofes Wien durchgeführt.

1.2 Prüfungszeitraum

Die gegenständliche Prüfung erfolgte vom vierten Quartal 2018 bis zum zweiten Quartal 2019. Das Eröffnungsgespräch mit der geprüften Stelle fand im Dezember 2018 statt. Die Schlussbesprechung wurde im ersten Quartal 2020 durchgeführt.

Der Betrachtungszeitraum umfasste den aktuellen Stand zum Prüfungszeitpunkt und die aktuellen Entwicklungen sowie die zurückreichenden Ereignisse (Historie) der vorangegangenen Jahre.

1.3 Prüfungshandlungen

Die Prüfungshandlungen umfassten Dokumenten- und Datenanalysen, Literatur-, Internet- und Intranetrecherchen sowie Interviews mit den verantwortlichen Personen der geprüften als auch der betriebsführenden Dienststelle.

Des Weiteren wurde anhand eines im Magistrat der Stadt Wien in Betrieb stehenden SCADA- bzw. MSR-Systems beurteilt, inwieweit und in welcher Form die in den durchgeführten System- bzw. Sicherheitsprüfungen (Penetrationstest) aufgezeigten Mängel behoben wurden.

1.4 Prüfungsbefugnis

Die Prüfungsbefugnis für diese Prüfung ist in § 73b Abs. 1 sowie in § 73c der Wiener Stadtverfassung festgeschrieben.

1.5 Vorberichte

Im Zusammenhang zur vorliegenden Prüfung ist der Bericht des damaligen Kontrollamtes der Stadt Wien mit dem Titel

- Unternehmung "Wien Kanal", Auswirkung von Starkregenereignissen auf das Wiener Kanalnetz, KA V - WK-1/12

zu erwähnen. Bei diesem Bericht ergibt sich der thematische Zusammenhang derart, dass die in diesem Bericht angeführte "Kanalnetzsteuerung" durch ein dementsprechendes SCADA-System vorgenommen wird. Infolgedessen hatte dieses SCADA-System die IKT-Sollvorgaben des vorliegenden Prüfungsgegenstandes entsprechend zu berücksichtigen, um die Betriebskontinuität der Kanalnetzsteuerung bei den auftretenden und zu bewältigenden Ereignissen (Starkregenereignisse etc.) aufrecht zu erhalten.

2. Allgemeines

2.1 Geschichtlicher Hintergrund der Automatisierung

Der Begriff der Automatisierung geht bis in das antike Griechenland zurück, wo der griechische Gelehrte Aristoteles in einem seiner Werke formulierte: "Wenn jedes Werkzeug auf Geheiß, oder auch vorausahnend, das ihm zukommende Werk verrichten könnte, wie des Dädalus Kunstwerke sich von selbst bewegten oder die Dreifüße des Hephästos aus eignem Antrieb an die heilige Arbeit gingen, wenn so die Weberschiffe von selbst webten, so bedürfte es weder für den Werkmeister der Gehilfen noch für die Herren der Sklaven". Die Aussagen der Gelehrten zu dieser Zeit waren großteils von Abstraktheit geprägt, bildeten jedoch die Basis für das Voranschreiten der Wissenschaften.

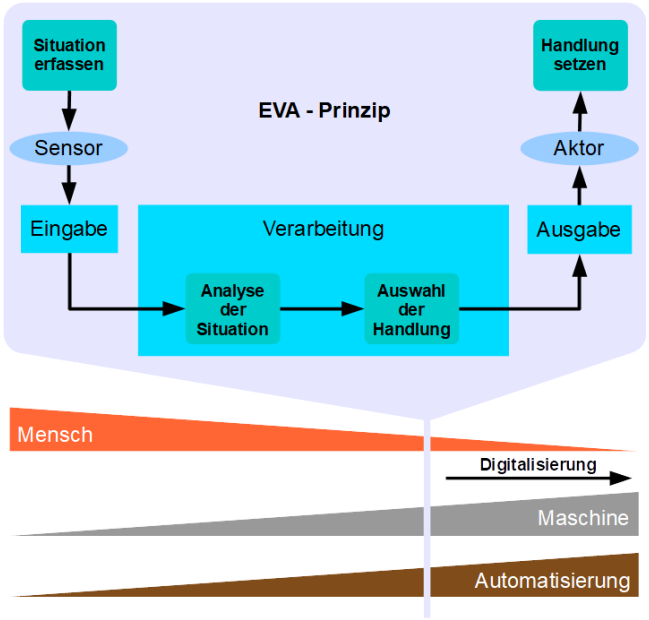
Im Jahr 1745 gelang es einem Engländer durch die Erfindung einer Vorrichtung, durch die sich Windmühlen selbstständig in den Wind drehten, die ersten Schritte der Automatisierung einzuleiten. Durch ein zusätzliches Windrad mit Getriebe, reagierte die Maschine dann selbstständig auf Änderungen ihrer Umgebung, wie es zur Erfüllung ihrer Aufgabe erforderlich war.

Mit der Erfindung neuer Antriebstechniken wie die Dampfmaschine und den generellen Fortschritten in der Mechanik hielt das Zeitalter der Industrialisierung Einzug. Tierische und menschliche Kraft wurde immer mehr durch Motoren ersetzt, was eine Massenproduktion in den Fabriken ermöglichte. Der Beginn der Automatisierung der Arbeitsprozesse in der industriellen Produktion erfolgte im Jahr 1787 durch die Erfindung einer automatisch betriebenen Webmaschine.

Die Entdeckung der Elektrizität und Erfindungen der Elektrotechnik machten den Versand von Energie über weite Strecken möglich, wodurch Produktionen dezentralisiert werden konnten. Zunehmend wurden über Versuche Erfahrungen gemacht, die Elektrizität für Mess-, Steuer- und Regelungszwecke einzusetzen.

Neuerungen in der Elektronik führten schlussendlich zur Verkleinerung von zuvor überdimensional großen elektrischen Schaltungen, wobei die Entwicklung von integrierten Schaltkreisen maßgeblich daran beteiligt war, Geräte mit entsprechendem logischen Verhalten auszustatten. Die Digital- bzw. Computer- und Softwaretechnik (Digitalisierung) und die dadurch mögliche Kommunikation mit Sensoren und Aktoren - im Zusammenhang zum EVA Prinzip - wurden bevorzugtes Mittel der Automatisierung (s. Abbildung 1), die sich Zug um Zug von der Industrie auch auf Privathaushalte ausdehnte.

Abbildung 1: Eingabe-Verarbeitung-Ausgabe Prinzip in der Automatisierung

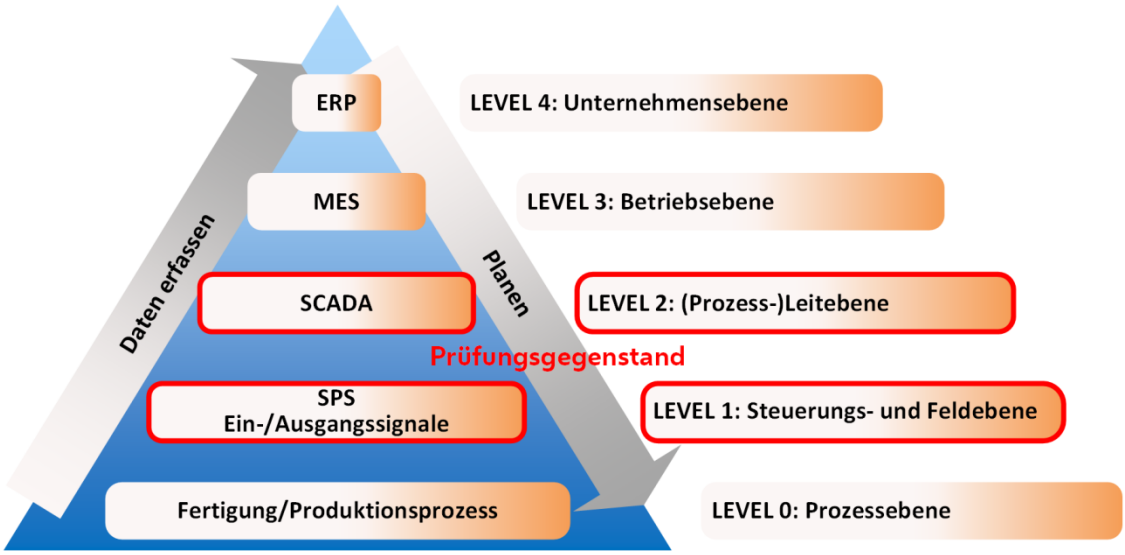


Quelle: Eigene erweiterte Darstellung Stadtrechnungshof Wien

2.2 Ebenen der Automatisierung

Die in der Fachliteratur als Automatisierungspyramide bezeichnete Darstellung der System- bzw. Kommunikationsebenen veranschaulicht im Wesentlichen das Zusammenspiel und den untereinander stattfindenden Informationsaustausch der jeweilig verwendeten Systeme in der Automatisierung (s. Abbildung 2).

Abbildung 2: Ebenen der Automatisierung (Automatisierungspyramide)



Quelle: Eigene Darstellung Stadtrechnungshof Wien

Die Basis dieser Pyramide bildet das LEVEL 0: Prozessebene, wo die tatsächliche Fertigung bzw. die Produktion - über Sensoren und Aktoren - erfolgt.

Übergeordnet zur Fertigung und Produktion steht das LEVEL 1: Steuerungs- und Feldebene, in der u.a. SPS für das Messen, Steuern und Regeln anhand der entsprechenden Ein- bzw. Ausgangssignale der einzelnen Produktionsschritte zum Einsatz kommen.

Die gegenständlichen SCADA-Systeme sind Teil des LEVEL 2: (Prozess-)Leitebene und ermöglichen die Bedienung bzw. das Beobachten des gesamten Prozessablaufes, das Visualisieren der einzelnen Betriebs- bzw. Anlagenzustände und die Protokollierung bzw. Archivierung von Mess- und Ereignisdaten.

Gemäß Punkt "1.1 Prüfungsgegenstand" befasst sich die vorliegende Prüfung mit der IKT-Sicherheit der Systeme des LEVEL 1: Steuerungs- und Feldebene (Messen, Steuern, Regeln) und des LEVEL 2: (Prozess-)Leitebene (SCADA).

Das LEVEL 3: Betriebsebene bzw. das sogenannte Manufacturing Execution System ermöglicht die Führung, Lenkung, Steuerung und Kontrolle der gesamten Produktion in Echtzeit. Dazu zählt u.a. die klassische Erfassung und Aufbereitung der Daten aus dem Produktionsbetrieb, die eine zeitnahe Auswirkung auf den Fertigungs- und Produktionsprozess haben.

Die oberste Ebene bildet das LEVEL 4: Unternehmensebene, in der die sogenannten ERP-Systeme zum Einsatz kommen. Die unternehmerische Aufgabe dabei ist es, Ressourcen wie Kapital, Personal, Betriebsmittel, Material im Sinn des Unternehmenszwecks rechtzeitig und bedarfsgerecht zu planen und zu steuern. Die hiefür eingesetzten ERP-Systeme - wie z.B. die betriebswirtschaftliche Software SAP - sind komplexe Anwendungen oder eine Vielzahl miteinander kommunizierender Informationssysteme zur Unterstützung der Ressourcenplanung.

2.3 Mess-, Steuer- und Regelungssysteme (LEVEL 1)

Die MSR-Systeme stellen einen Bereich der Automatisierungstechnik dar und sind überwiegend ein Teil der Elektrotechnik. Den einzelnen Techniken werden auch verschiedene Aufgaben zugeschrieben.

2.3.1 Die Aufgabe der Messtechnik besteht im Wesentlichen darin, sich mit Geräten und Methoden zu befassen, die den Informationsgewinn über bestimmte Messobjekte zulassen. Beispielsweise handelt es sich dabei um die Messung von elektrischen und nichtelektrischen Größen wie Länge, Masse, Kraft, Druck, Temperatur und Zeit. Üblicherweise werden diese gemessenen Größen in Form von elektrischen Signalen abgebildet und einer weiteren Signalverarbeitung zugeführt.

2.3.2 Die Steuerungstechnikaufgaben bestehen darin, bestimmte Abläufe in einem Prozess zu erzwingen. Dies erfolgt durch die Verarbeitung von digitalen Messsignalen mittels Sensoren (Erfassungsglieder) und deren logischer Informationsverarbeitung in Form von sogenannten Steuerungsprogrammen. Die Verarbeitung der Informationen in den Programmen führt dazu, dass verschiedene Aktoren (Stellglieder) angesteuert werden, um einzelne Prozessgrößen zu beeinflussen (s. Punkt 2.1). Diese für viele Anwendungen der Steuerungstechnik eingesetzten Geräte werden als speicherprogrammierbare Steuerung bezeichnet. Die speicherprogrammierbare Steuerung ist prinzipiell ein kleiner Computer, der über eine zentrale Verarbeitungseinheit und über einen entsprechenden Speicher für das Steuerungsprogramm und die Steuerungsparameter verfügt. Zudem verfügen diese Geräte über Ein- bzw. Ausgangsmodule für Sensor- und Aktorsignale, Mensch-Maschine-Schnittstellen zur Bedienung und Schnittstellen zur industriellen Kommunikation für die Programmierung und Vernetzung.

2.3.3 Die Hauptaufgabe der Regelungstechnik besteht darin, in einer sogenannten Regelstrecke (z.B. Regelung der Raumtemperatur) für einen stabilen und von Störgrößen unbeeinflussten Ablauf zu sorgen. Die Regelung ist gekennzeichnet durch eine Rückkopplung der beeinflussten Größe (Regelgröße oder Ist-Wert), wodurch ein geschlossener Regelkreis vorliegt. Von der Regelgröße wird mittels der Messtechnik

ein Ist-Wert ermittelt, mit einem vorgegebenen Referenzwert (Führungsgröße oder Soll-Wert) verglichen und durch den Regler die Stellgröße derart beeinflusst, dass die Abweichung zwischen Ist-Wert und Soll-Wert möglichst gering wird.

Inzwischen beinhalten nahezu alle Geräte, Einrichtungen und Anlagen im industriellen sowie im privaten Umfeld Mess-, Steuer- und Regelungskomponenten, bei denen es um die Erfassung von Größen, deren Weiterverarbeitung sowie die Beeinflussung von Systemen und deren Verhalten geht. Eine Heizungsregelung kann beispielsweise die aktuelle Raumtemperatur erfassen und mit der Vorgabe eines gewünschten Temperatur-Soll-Werts vergleichen und daraus die Heizkörpertemperatur derart verstellen, dass sich die gewünschte Raumtemperatur einstellt. Dies erfolgt weitgehend unabhängig von vorliegenden Störgrößen wie veränderlicher Außentemperatur oder Sonneneinstrahlung.

2.4 Supervisory Control and Data Acquisition-Systeme (LEVEL 2)

SCADA-Systeme werden heute in nahezu allen Bereichen der Erzeugung und Versorgung (Gas, Wasser, Strom, Öl usw.), der Entsorgung (Müll, Abwässer usw.), der Produkterzeugung (Chemie, Lebensmittel usw.), des Transports (Straßenverkehr, öffentlicher Verkehr, Aufzüge usw.) und des Gebäudemanagements (Kühlen, Heizen, Licht usw.) verwendet.

SCADA ist keine bestimmte Technologie, sondern ein Anwendungstypus der für die übergeordnete (Überwachungs-)Steuerung und Datenerfassung steht. Jede Anwendung, die Betriebsdaten aus einem MSR-System erfasst, um dieses System zu beeinflussen bzw. zu optimieren, ist eine SCADA-Anwendung.

Im Allgemeinen werden unter SCADA-Systeme Computer- bzw. Informationssysteme verstanden, die technische Prozesse überwachen, steuern und regeln. Das Zusammenspiel der einzelnen Geräte der MSR-Systeme erzeugt Wechselwirkungen, die einen Informationsaustausch bewirken. Diese Informationen betreffen im Wesentlichen Erkenntnisse über den jeweiligen Prozesszustand bzw. Anweisungen über vorzunehmende Prozesseingriffe. Zudem können über entsprechende Messsysteme

auch Informationen aus der Umgebung gewonnen werden, wodurch eine noch vielfältigere und komplexere Kommunikation stattfinden kann.

Die dabei erlangten Informationen können sodann in den Subsystemen aufgabengerecht zu neuen Informationen weiterverarbeitet und bereitgestellt werden. Ein über die Überwachung, Steuerung und Regelung hinausgehendes wichtiges Merkmal von SCADA-Systemen ist die Möglichkeit der Visualisierung von Anlagenzuständen, Alarmen, Messwerten, Ereignissen etc.

2.5 Abgrenzung von Automatisierungssystemen

Der Begriff "OT" legt die Abgrenzung der technischen und funktionalen Unterschiede von Automatisierungssystemen (z.B. Maschinen und Anlagen der Produktion und Steuerung von Produkten und Gütern) zu der "IT" bzw. "IKT" mit den Informationssystemen (z.B. Hard- und Software zur Verarbeitung von Informationen und Daten) fest.

2.6 Kommunikation innerhalb von Automatisierungssystemen

Das Kommunikationsspektrum innerhalb von Automatisierungssystemen reicht von direkt lokalen Verbindungen bzw. entfernten Anbindungen (Remote Control) über eigene physische Feldbussysteme, bestehende physische Netzwerke bzw. virtuell seperierte Netzwerke VPN bis hin zu den voranschreitenden IoT bzw. IIoT Technologien.

Im Zusammenhang mit SCADA- bzw. MSR-Systemen umfasst die voranschreitende IoT bzw. IIoT Technologie bzw. ein IoT bzw. IIoT System im Wesentlichen physische Objekte (z.B. Sensoren bzw. Aktoren) aber auch nicht physische (virtuelle) Objekte (z.B. Strichcode, QR-Code, Daten aus Datenbanken), die über die Kommunikation des Internets in einem SCADA- bzw. MSR-System eingebunden sind bzw. ein solches abbilden (Stichwort "Cyber Physische Systeme" bzw. "Industrie 4.0").

2.7 Weitere technische Ausprägungen bei Automatisierungssystemen

Im Zusammenhang mit den Automatisierungssystemen bzw. mit der OT sind der Fachliteratur auch folgende weitere Begrifflichkeiten bzw. technischen Ausprägungen zu entnehmen:

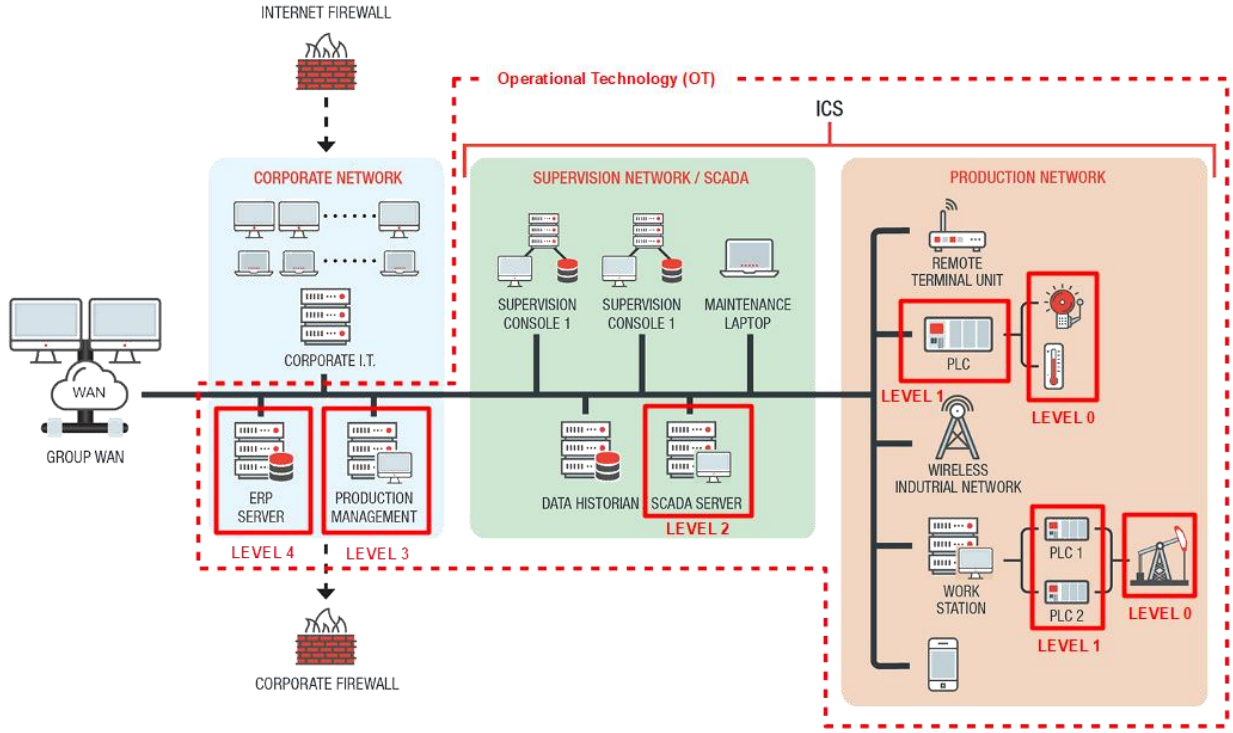
- Industrial Control System, industrielles Computer-Kontrollsystem für die Prozesstechnik,
- Distributed Control System, verteiltes Computer Kontrollsystem für die Prozesstechnik,
- Process Control Network, Kommunikationsnetzwerk als Teil der Prozesstechnik, welche u.a. bei SCADA-System Verwendung findet,
- PAC, Computer Kontrollsystem für die Prozesstechnik auf höherem Instruktionsniveau als ein PLC (PAC als Nachfolgetechnik der PLC),
- PLC, SPS für die Prozesstechnik und
- Remote Terminal Unit, Fernbedienungsterminal für die Prozesstechnik.

Aufgrund der Komplexität des Themenbereiches wird an dieser Stelle auf eine weitere tiefergehende Erläuterung der o.a. Begrifflichkeiten verzichtet.

2.8 Gesamtes Zusammenwirken in Automatisierungssystemen

Die nachfolgende Abbildung stellt das Zusammenwirken der einzelnen Systeme in ihren Automatisierungsebenen aus der Gesamtsicht eines Unternehmens mit den voran angeführten Grundlagen zusammenfassend und beispielhaft dar. Von der Ansteuerung der Sensoren und Aktoren über die Steuerungs- und Feldebene ("Production Network" mit LEVEL 0 und LEVEL 1) zum SCADA System ("Supervision Network/SCADA" mit LEVEL 2) bis hin zur Unternehmensebene ("Corporate Network" mit LEVEL 3 und LEVEL 4).

Abbildung 3: Zusammenwirken der einzelnen Systeme in der Automatisierung bzw. der Operational Technology



Quelle: Erweiterte Darstellung Stadtrechnungshof Wien

2.9 Lebensdauer bzw. Lebenszyklus von Automatisierungssystemen

SCADA- bzw. MSR-Systeme sind aufgrund ihrer Aufgabenstellung vorwiegend für eine Lebensdauer bzw. einem Lebenszyklus von 15 bis 20 Jahren konzipiert.

Diese Anforderung steht im Gegensatz zu den immer schneller verfügbaren technologischen Entwicklungen und den damit einhergehenden Bedrohungsszenarien bzw. Bedrohungsrisiken durch eine steigende Anzahl von Angriffen (Cyber Attacken) auf derartige SCADA- bzw. MSR-Systeme.

2.10 Schutzinteressen in Automatisierungssystemen

Bei Automatisierungssystemen bzw. der OT sind folgende wesentliche Schutzinteressen von Bedeutung:

- Security als Schutz des betreffenden Automatisierungssystems vor der Umgebung mit den Bedrohungsszenarien bzw. Bedrohungsrisiken,
- Safety als Schutz der Umgebung vor dem Betrieb bzw. der Anwendung des betreffenden Automatisierungssystems (Betriebssicherheit) und
- Privacy als Schutz der Daten bzw. Informationen des Automatisierungssystems vor der nicht vorgesehenen Verwendung durch die Umgebung.

Die angeführten Schutzinteressen sind vor allem im Zusammenhang mit der langen Lebensdauer bzw. des Lebenszyklus von SCADA- bzw. MSR-Systemen mit sehr hoher Priorität zu betrachten bzw. mit hohem Risiko zu bewerten.

Das Aufrechterhalten dieser Schutzinteressen steht dabei im Zusammenhang mit der Verfügbarkeit der eingesetzten Hardware (u.a. Ersatzgeräte, Sensoren, Aktoren) und Software (u.a. Updates, Sicherheitspatches) als auch der Systemwartungen (u.a. autarke Systemwartungen bis hin zu Systemwartungen über Fernzugänge).

In der vorliegenden Prüfung war das Schutzinteresse "Security" Prüfungsgegenstand.

2.11 Kritische Infrastruktur

Derartige Automatisierungssysteme (MSR-System [LEVEL 1] und SCADA-System [LEVEL 2]) werden, wie bereits erwähnt, in den Bereichen der Erzeugung und Versorgung (Gas, Wasser, Strom, Öl, Heizung, Be- und Entlüftung etc.), der Entsorgung (Müll, Abwässer etc.), der Produkterzeugung (Chemie, Lebensmittel etc.), des Transports (Straßenverkehr, öffentlicher Verkehr, Aufzüge etc.) und viele mehr verwendet.

Die in diesen Bereichen verwendeten Systeme stehen dabei oftmals in einem unmittelbaren bzw. direkten Zusammenhang mit dem Betrieb von kritischer Infrastruktur.

Zu den kritischen Infrastrukturen zählen dem Grunde nach jene Infrastrukturen oder Teile davon, die eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen haben und deren Störung oder Zerstörung schwerwie-

gende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche oder soziale Wohl der Bevölkerung haben.

Beispielsweise zählen dazu insbesondere die Bereiche Energie, Gesundheit, IT und Telekommunikation, Transport und Verkehr, Wasser, Ernährung, als kritische Infrastruktur Österreichs.

Die Funktionsfähigkeit solcher Infrastrukturen ist u.a. durch Naturkatastrophen, insbesondere wie Hochwasser bzw. Überschwemmungen, Erdbeben, Erdrutsche, den Klimawandel an sich, technische Unfälle, menschliches Versagen, Kriminalität, Terrorismus und in letzter Zeit vermehrt durch Gefahren im sogenannten Cyber Raum gefährdet. Basierend auf diese Umstände erlangt der Schutz kritischer Infrastrukturen daher zunehmend an Bedeutung.

In diesem Zusammenhang nimmt nicht nur die Bedeutung des Schutzes von SCADA- bzw. MSR-Systemen zu, sondern auch die Prüfung der damit im Zusammenhang stehenden Themen, Arbeitsaufgaben, Einrichtungen und Anlagen (z.B. kritische Infrastrukturen im Gesundheitsbereich) der damit befassten Stellen. Maßgebendes Kriterium für derartige Prüfungen sind die Bedrohungen der Gefahr für die Sicherheit des Lebens und der Gesundheit von Menschen (s. dazu Punkt 1.4).

Die Stadt Wien bzw. die jeweilig betriebsverantwortlichen Dienststellen sind ebenso Betreibende kritischer Infrastrukturen, die es entsprechend zu schützen gilt.

3. Rechtliche Grundlagen

3.1 Allgemeines

Die Herstellung, die Instandhaltung und der Betrieb von SCADA- bzw. MSR-Systemen sind durch verschiedene gesetzliche Vorschriften, Normen und Regelwerke organisiert. Durch die Vernetzung der einzelnen Systeme und Ebenen innerhalb der Produktionsstätte und darüber hinaus gewinnt das Thema IKT-Sicherheit im gesamten Cyber Raum immer mehr an Bedeutung. Dies spiegelt sich in den vielen strategischen Zielsetzungen, Programmen und umfassenden Regelwerken, des Bundes,

der Länder, der Gemeinden und der einzelnen Unternehmungen als auch am Fortschritt der technischen Entwicklungen wieder.

3.2 Europäische Union

Aufbauend auf den Auftrag des Europäischen Rates an die Kommission betreffend der Ausarbeitung einer umfassenden Strategie für "Critical Infrastructure Protection" im Juni 2004 und einhergehend mit der Zunahme der Angriffe (Cyber Attacken) im Cyber Raum beschloss das Bundeskanzleramt und das Bundesministerium für Inneres, ein neues "Österreichisches Programm zum Schutz kritischer Infrastrukturen (Masterplan APCIP 2014 vom Jänner 2015)" zu veröffentlichen. Dabei wurden u.a. Erkenntnisse aus den Jahren davor eingearbeitet sowie mit den verschiedensten Organisationen aus Bund, Länder und strategischen Unternehmen akkordiert. Im Jahr 2016 folgte auf Beschluss der Landeshauptleutekonferenz das "Länderprogramm Schutz kritischer Infrastruktur (APCIP Länder)" mit dem Ziel, die Komplementarität zwischen Bund und Länder durch eigene Programme aufrecht zu halten. Im Wesentlichen geht es dabei darum, Maßnahmen zum Schutz der regionalen kritischen Infrastrukturen zu erarbeiten und die Resilienz zu steigern, um im Weiteren auch die Städte und die Gemeinden zu motivieren lokale Programme zu erstellen.

3.3 Österreichische Strategie für Cyber Sicherheit

Die Österreichische Strategie für Cyber Sicherheit ist ein umfassendes und proaktives Konzept zum Schutz des Cyber Raums und jener Menschen im virtuellen Raum unter Gewährleistung ihrer Menschenrechte basierend auf die Prinzipien des Programmes zum Schutz kritischer Infrastrukturen. Ziel dabei ist, die Sicherheit und die Widerstandskraft der österreichischen Infrastrukturen und Leistungen im Cyber Raum zu verbessern, um dadurch Bewusstsein und Vertrauen in der österreichischen Gesellschaft zu schaffen.

3.4 Netz- und Informationssystemsicherheit

3.4.1 Das Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (NISG), welches im Dezember 2018 beschlossen wurde, soll im Wesentlichen die Sicherheit der kritischen Infrastruktur in Österreich

sicherstellen und die Voraussetzungen für die Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen schaffen.

Damit sollen einheitliche Cybersicherheitsstandards für Unternehmen der kritischen Infrastruktur geschaffen werden, wobei das Gesetz nur auf kritische Infrastrukturen wie Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserversorgung und digitale Infrastrukturbetreiberinnen bzw. Infrastrukturbetreiber abzielt. Im Speziellen auf Betreiberinnen bzw. Betreiber wesentlicher Dienste und digitaler Diensteanbieterinnen bzw. Diensteanbieter.

Im Unterschied zur Situation vor dem NISG ist nun die Umsetzung und die Einhaltung gängiger Standards und Best Practices dem Bundesministerium für Inneres nachzuweisen und Vorfälle von Angriffen auf die digitale Infrastruktur der Unternehmungen sind ehest möglich dem sektorspezifischen CERT zu melden.

3.4.2 Auf Basis des vom Nationalrat beschlossen und kundgemachten NISG wurde weiterführend die Netz- und Informationssystemsicherheitsverordnung am 21. Juli 2019 in Kraft gesetzt. Diese Verordnung dient der Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren sowie zu Sicherheitsvorfällen nach dem NISG.

3.5 Normen bzw. Erlässe des Magistrats der Stadt Wien

Auf Länder- bzw. Kommunalebene verfügt der Magistrat der Stadt Wien ebenfalls über Erlässe und Regelwerke, die den Schutz und die sichere Handhabung der IKT-Infrastruktur zum Ziel haben.

3.5.1 Im Erlass "Sicherheit in der Informations- und Kommunikationstechnologie, Zl. MD-OS 51600-2013-1" aus dem Jahr 2013, handelt es sich um Angelegenheiten der IKT, insbesondere um die Informationssicherheit, die die Vertraulichkeit, Integrität und Verfügbarkeit sicherstellt.

Basis für diesen Erlass sind dabei das Datenschutzgesetz, die Prinzipien der Normenserie ISO/IEC 27000 sowie das Österreichische Informationssicherheitshandbuch. Aus Letzterem wurde beispielsweise die Verpflichtung, ein ISMS zu betreiben, abgeleitet. Beim Informationssicherheitsmanagement stehen IT-Sicherheit, Datensicherheit und Datenschutz im Mittelpunkt. Damit soll gewährleistet werden, dass Daten nur von dafür berechtigten Personen gelesen und bearbeitet, jederzeit verfügbar und nicht beschädigt oder ungewollt verändert werden können.

Die Normenserie ISO/IEC 27000 stellt dabei einen Überblick über ein ISMS und Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung solcher Systeme bereit.

In diesem Zusammenhang erhielt die ehemalige Magistratsabteilung 14 (nunmehr Magistratsabteilung 01) im Jahr 2012 das ISO-27001 Zertifikat für die Implementierung eines ISMS. Des Weiteren wurde im Jahr 2015 ebenso das BCM-System nach ISO 22301 der Magistratsabteilung 14 zertifiziert.

3.5.2 Der Erlass "Datenschutz im Magistrat der Stadt Wien, Zl. MDK-420907-1/18" bildet wie die o.a. Erlässe ebenso eine Basis für die Nutzung von SCADA- bzw. MSR-Systemen.

3.6 Regelwerke bzw. Leitfäden

3.6.1 Ferner wurde von der Magistratsabteilung 01, neben den o.a. Erlässen, eigens für MSR-Systeme eine Policy bzw. Richtlinie proaktiv erarbeitet ("Securityvorgaben für Regelungs-, Steuerungs- und Messsysteme; Vergabe, Implementierung, Betrieb" mit aktuellem Stand 6. Juni 2018), die sich dem Thema Angriffssicherheit bzw. IT-Sicherheit widmet und Empfehlungen hinsichtlich der Security zum Inhalt hat.

Anknüpfungspunkt für die Inhalte dieser Policy bzw. Richtlinie war das Whitepaper "Anforderungen an sichere Steuerungs- und Telekommunikationssysteme" vom deutschen Bundesverband der Energie- und Wasserwirtschaft bzw. der österreichi-

schen E-Wirtschaft. In dieser Policy bzw. Richtlinie der Magistratsabteilung 01 werden Vorgaben für MSR-Systeme (Level: 1) und SCADA Systeme (Level: 2) dargelegt.

3.6.2 Des Weiteren ist beispielhaft zu erwähnen, dass eine Dienststelle für ihren eigenen Wirkungsbereich über einen "Leitfaden für Gebäudeautomation" verfügte, der aus dem Jahr 2017 stammt. Diese Richtlinie hat Vorgaben "… für die Planung, Errichtung und Sanierung von Mess-, Steuer- und Regelungsanlagen speziell zum Thema Regelungstechnik bei Heizung-Lüftung-Klima und Sanitäranlagen in Objekten der Stadt Wien …" die von derselben Dienststelle betreut werden zum Inhalt. Vorgaben zum Schutz der Infrastruktur und Datensicherheit befinden sich nicht in diesem Leitfaden.

3.7 International Electrotechnical Commission 62443 Industrielle Kommunikationsnetze - Informationstechnologie Sicherheit für Netze und Systeme

Die IEC 62443 Normenreihe adressiert insbesondere die technische Spezifikation der "Cybersicherheit (Cybersecurity)" von "Industriellen Automatisierungs- und Steuerungssystemen (Industrial Automation and Control Systems)" die automatisierte, ferngesteuerte oder überwachte Anlagen verwenden.

Die angesprochene Cybersicherheit umfasst dabei die Computer, Netzwerke, Betriebssysteme, Anwendungen und andere programmierbare bzw. konfigurierbare Komponenten des Systems.

Seitens der Magistratsabteilung 01 wurde als langfristiges Ziel eine Verschlankung der Inhalte der vorliegenden Policy bzw. Richtlinie (s. Punkt 3.6.1) sowie eine inhaltliche Überarbeitung unter Berücksichtigung der Normenreihe IEC 62443 angegeben.

4. Organisatorische Feststellungen

4.1 Verantwortungen innerhalb der Stadt Wien

Die mit dieser Prüfungsthematik unmittelbar direkt betroffenen bzw. befassten Dienststellen bzw. Organisationseinheiten waren:

- die Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Prozessmanagement und IKT-Strategie mit der Funktion des CIO der Stadt Wien und der Funktion des CISO der Stadt Wien,
- die Magistratsabteilung 01 als zentraler IKT Dienstleister der Stadt Wien mit dem Referat Security, Safety und Compliance sowie der Funktion des Computer Emergency Response Team (WienCERT) und
- die entsprechenden Magistratsdienststellen in deren Verantwortung der Betrieb des jeweiligen SCADA- bzw. MSR-Systemen gemäß dem jeweiligen Geschäftsaufgabenbereich lag.

Basis dieser Verantwortungen waren die in der Geschäftseinteilung für den Magistrat der Stadt Wien festgelegten Aufgaben:

Im Geschäftsbereich der Magistratsdirektorin bzw. des Magistratsdirektors waren diese in Zusammenhang zur Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Prozessmanagement und IKT-Strategie u.a.

- Entwicklung, laufende Weiterentwicklung und Anpassung der Prozessmanagement- und IKT-Strategie für den gesamten Magistrat der Stadt Wien,
- Festlegung, Koordination und Kommunikation von strategischen Rahmenbedingungen im Bereich des Prozessmanagements sowie der IKT,
- Grundsätzliche Angelegenheiten des Prozessmanagements und der IKT,
- Koordination und Überprüfung hinsichtlich aller organisatorischen und technischen Maßnahmen auf dem Gebiet der IKT,
- Festlegung von Rahmenbedingungen für den zweckmäßigen und wirtschaftlichen Einsatz der IKT und
- Festlegung von Grundsätzen für die von der Magistratsabteilung 01 und dem Krankenanstaltenverbund wahrzunehmenden Koordinationstätigkeiten auf dem Gebiet der IKT.

Der Geschäftsbereich der Magistratsabteilung 01 umfasste dabei u.a. folgende Aufgaben:

- Mitwirkung bei der Weiterentwicklung der IKT-Strategie,
- Erstellung und Weiterentwicklung der strategischen Planung des IKT-Einsatzes,
- Mitwirkung beim strategischen IKT-Projektportfoliomanagement,
- 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). Abschluss von entsprechenden Vereinbarungen und Verträgen sowie
- Sicherstellung der IKT-Sicherheit.

In den jeweiligen Geschäftsbereichen der betreffenden Dienststellen waren dabei die Aufgaben im Zusammenhang mit dem vorliegenden Prüfungsgegenstand (beispielhaft und auszugsweise für die Magistratsabteilung 34 und die Magistratsabteilung 48 angeführt) wie folgt geregelt:

Magistratsabteilung 34
- Planung, Errichtung, Installation, Betriebsführung, Erhaltung und Begutachtung von wärme-, kälte-, lüftungs-, klima-, maschinen-, sanitär-, elektro-, blitzschutz- und fördertechnischen Anlagen aller Art.

Magistratsabteilung 48
- Planung, Errichtung und Führen von Deponien und Abfallbehandlungseinrichtungen sowie eines Labors und
- Planung, Errichtung und Betrieb von Anlagen zur Verwertung von Abfällen einschließlich der Kompostierung.

Für den Stadtrechnungshof Wien war festzustellen, dass die in der Geschäftseinteilung für den Magistrat der Stadt Wien dargelegten Aufgaben bei der Magistratsabteilung 01 eine mögliche aber nicht eindeutige Zuständigkeit bzw. Verantwortlichkeit im Zusammenhang mit der Thematik von SCADA- bzw. MSR-Systemen bei den je-

weiligen betriebsführenden Dienststellen darlegt (z.B. Aufgabe "Sicherstellung der IKT Sicherheit").

Gleichzeitig war in der Geschäftseinteilung für den Magistrat der Stadt Wien zu erkennen, dass die Aufgaben der jeweiligen Geschäftsbereiche der betreffenden bzw. betriebsführenden Dienststellen auch nicht eindeutig eine Zuständigkeit bzw. Beachtung der IKT-Sicherheit (Informationssicherheit) für die jeweiligen SCADA- bzw. MSR-Systemen im eigenen Wirkungsbereich festlegt.

Im Sinn der Betrachtung der Treue der Einhaltung von Vorschriften und Regeln (Compliance) wäre es daher sinnvoll und notwendig, diese entsprechenden Vorgaben entsprechend zu evaluieren und gegebenenfalls in der Geschäftseinteilung für den Magistrat der Stadt Wien abzuändern bzw. im Rahmen eines "Compliance Management Systems" in der Stadt Wien mitzubetrachten.

Der Stadtrechnungshof Wien empfahl daher der Magistratsabteilung 01, alle notwendigen Schritte zu einer Evaluierung der Geschäftseinteilung für den Magistrat der Stadt Wien hinsichtlich der eindeutigen Zuständigkeiten von IKT-Sicherheit (Informationssicherheit) bei SCADA- bzw. MSR-Systemen einzuleiten. Bei einer diesbezüglichen Evaluierung sollte eine mögliche Umsetzung über die Einhaltung im Rahmen eines "Compliance Management Systems" in der Stadt Wien nicht unbeachtet bleiben.

4.2 Definition von Supervisory Control and Data Acquisition- bzw. Mess-, Steuer- und Regelungssystemen durch die Magistratsabteilung 01

Seitens der Magistratsabteilung 01 wurden unter SCADA- bzw. MSR-Systemen alle jene Systeme verstanden, mit deren Hilfe technische Prozesse gesteuert, geregelt oder gemessen werden.

Von der Magistratsabteilung 01 waren darunter u.a. Aufzüge, Rolltreppen, Wasseraufbereitungen oder das Kanalnetz zu verstehen. Auf solche Systeme können War-

tungsfirmen lokal oder über den Betrieb in einem entsprechenden Netzwerk auf das entsprechende SCADA- bzw. MSR-System zugreifen.

Bei derartigen SCADA- bzw. MSR-Systemen handelt es sich gemäß Aussage der Mitarbeitenden der Magistratsabteilung 01 fast ausschließlich um Systeme, die sich im Verantwortungsbereich ihrer Kundinnen bzw. Kunden - also den verantwortlichen Dienststellen - befinden bzw. durch diese betrieben werden. Für diese Systeme wird allenfalls durch die Magistratsabteilung 01 in verschiedenen Ausprägungen eine entsprechende Basisinfrastruktur (Kommunikationsinfrastruktur mit entsprechenden Netzwerktechnologien wie z.B. VPN oder andere weitere Technologien) in Abstimmung mit der jeweilig verantwortlichen Dienststelle bereitgestellt.

Die Implementierung der eigentlichen SCADA- bzw. MSR-Systeme der jeweiligen Kundinnen bzw. Kunden in die allenfalls von der Magistratsabteilung 01 bereitgestellte Basisinfrastruktur, erfolgt durch externe Dienstleistungen der entsprechenden Firmen. In wenigen Fällen werden auch die notwendigen Netzwerktechnologien - wie die voran angeführten Möglichkeiten der Basisinfrastruktur der Magistratsabteilung 01 - für diese SCADA- bzw. MSR-Systeme ebenso durch externe Dienstleistungen der entsprechenden Firmen erbracht.

Diese Vielzahl an verschiedenen Systemen versucht die Policy bzw. Richtlinie "Securityvorgaben für Regelungs-, Steuerungs- und Messsysteme; Vergabe, Implementierung, Betrieb" vom 6. Juni 2018 entsprechend abzudecken.

Werden für SCADA- bzw. MSR-Systeme entsprechende IoT Systeme herangezogen so adressiert diese voran angeführte Policy bzw. Richtlinie diesen Umstand ebenso. Für alle anderen Einsatzzwecke von IoT-Systemen wird eine eigene weitere Sicherheitsvorgabe (Policy bzw. Richtlinie) von der Magistratsabteilung 01 angewendet.

4.3 Sensibilisierung im Hinblick auf das Thema Sicherheit bei Supervisory Control and Data Acquisition- bzw. Mess-, Steuer- und Regelungssystemen

4.3.1 In einem Schreiben an den Stadtrechnungshof Wien gab die Magistratsabteilung 01 an, dass die damalige Magistratsabteilung 14 alle Dienststellen über die Brisanz des Themas IKT-Sicherheit (Informationssicherheit) bei der im eigenen Wirkungsbereich betriebenen SCADA- bzw. MSR-Systemen informierte. Die Information erfolgte zunächst in bilateralen Gesprächen, teilweise schon vor Veröffentlichung der Policy bzw. Richtlinie (April 2013 bis Dezember 2013).

Seitens der Magistratsabteilung 01 konnte ein Nachweis bzw. eine Dokumentation (Protokolle) über die geführten bilateralen Gespräche mit den Dienststellen nicht vorgelegt werden.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 01, eine entsprechende Dokumentation gemäß den Vorgaben des Erlasses MDK-168759-1/12 Büroordnung für den Magistrat der Stadt Wien sicherzustellen.

4.3.2 Ferner wurden die Dienststellen, zeitgleich mit Veröffentlichung der Policy bzw. Richtlinie, einerseits im Zuge einer gesonderten Veranstaltung (3. Dezember 2013) und andererseits über einen WienCERT - Security Informationen Blog zum Thema "Security für SCADA-Systeme" über das Erscheinen des Dokumentes "Securityvorgaben für Regelungs-, Steuerungs- und Messsysteme" im Intranet der Stadt Wien informiert (30. März 2015).

Darüber hinaus wurden bei diesen Informationen die SCADA- bzw. MSR-Systeme betreibenden und verantwortlichen Dienststellen darauf aufmerksam gemacht, dass an solche Anlagen höchste Anforderungen auf die Folgen eines Systemfehlers zu stellen sind. Diese Anforderungen haben sich jedoch nicht nur auf die reine Betriebs- und Ausfallsicherheit zu beziehen, sondern auch auf den Schutz vor böswilligen Angriffen.

Vom Stadtrechnungshof Wien wurde die betreffende Intranetseite des WienCERT - Security Informationen Blog stichprobenweise aufgerufen. Der in der Intranetseite angeführte Link auf das Dokument "Securityvorgaben für Regelungs-, Steuerungs- und Messsysteme; Vergabe, Implementierung, Betrieb" führte zum Prüfungszeitpunkt auf eine leere Seite und das angegebene Dokument konnte nicht aufgerufen werden.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 01, die vorliegenden Inhalte und Linkverknüpfungen der Intranetseite "Security für SCADA-Systeme" des WienCERT - Security Informationen Blog zu überprüfen.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 01 ferner, den Prozess der Bereitstellung bzw. Aktualisierung der Informationen der Intranetseite "Security für SCADA-Systeme" des WienCERT - Security Informationen Blog mit den Link auf das Dokument "Securityvorgaben für Regelungs-, Steuerungs- und Messsysteme; Vergabe, Implementierung, Betrieb" aufgrund der Bedeutung der Thematik zu evaluieren. Dabei wären wiederkehrend Prüfungen der einwandfreien Funktion bzw. Abrufbarkeit dieser Intranetseite in Betracht zu ziehen.

4.4 Erstellung und Gültigkeit der Policy bzw. Richtlinie der Magistratsabteilung 01

Die Policy bzw. Richtlinie "Securityvorgaben für Regelungs-, Steuerungs- und Messsysteme; Vergabe, Implementierung, Betrieb" wurde am 28. August 2014 als Erstversion erstellt und fortlaufend bis der zum Prüfungszeitpunkt vorliegenden Fassung vom 6. Juni 2018 weitergepflegt. Diese Policy bzw. Richtlinie wurde in Zusammenarbeit mit einer externen Firma aus dem Security Bereich auf Basis des Whitepaper "Anforderungen an sichere Steuerungs- und Telekommunikationssysteme" vom deutschen Bundesverband der Energie- und Wasserwirtschaft bzw. der österreichischen E-Wirtschaft erstellt.

Ziel dieser erstellten Policy bzw. Richtlinie war aus Sicht der Magistratsabteilung 01 insbesondere neue SCADA- bzw. MSR-Systeme im Magistrat der Stadt Wien in einem entsprechend aktuellen bzw. dem Stand der Technik - insbesondere in der The-

matik der Security - in Betrieb zu nehmen. Die zu diesem Zeitpunkt in Betrieb stehenden SCADA- bzw. MSR-Systeme (Bestandsanlagen) sollten nach Möglichkeit nach den Vorgaben dieser Policy bzw. Richtlinie entsprechend angepasst werden. Seitens der Magistratsabteilung 01 sollte die vorliegende Policy bzw. Richtlinie den Dienststellen für die in ihrer eigenen Betriebsverantwortung stehenden SCADA- bzw. MSR-Systeme als Hilfestellung zur Erfüllung der Vorgaben des Erlasses "Sicherheit in der Informations- und Kommunikationstechnologie, Zl. MD-OS 51600-2013-1" dienen.

Vom Stadtrechnungshof Wien war festzustellen, dass diese Policy bzw. Richtlinie eine Empfehlung zur Anwendung darstellte und nicht - wie z.B. als Erlass im Magistrat der Stadt Wien - als verbindlich vorlag.

Aus Sicht des Stadtrechnungshofes Wien sind SCADA- bzw. MSR-Systeme aufgrund der in Punkt 2. dargelegten Grundlagen als auch der in Punkt 3. angeführten Vorgaben als Aufgabenstellung mit hoher Priorität zu betrachten.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 01, alle Maßnahmen zu einer Evaluierung einer verbindlichen Anwendung der Policy bzw. Richtlinie "Securityvorgaben für Regelungs-, Steuerungs- und Messsysteme; Vergabe, Implementierung, Betrieb" für SCADA- bzw. MSR-Systeme im Magistrat der Stadt Wien vorzunehmen.

Dies sollte in Abstimmung mit den weiteren verantwortlichen Stellen und Funktionen (z.B. Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Prozessmanagement und IKT-Strategie bzw. mit dem CISO der Stadt Wien) veranlasst werden (z.B. als eigener Erlass oder als Verweis in einem entsprechend anderen oder weiteren verpflichtenden Erlass). In einer allfälligen Umsetzung sollte dabei auf die Geschwindigkeit der Entwicklungen des Standes der Technik und der damit in Zusammenhang notwendigen Aktualisierung der vorliegenden Policy bzw. Richtlinie Rücksicht genommen werden.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 01 weiters, das bereits gesetzte Ziel der Einbindung bzw. Berücksichtigung der Normenreihe IEC 62443 in der Policy bzw. Richtlinie "Securityvorgaben für Regelungs-, Steuerungs- und Messsysteme; Vergabe, Implementierung, Betrieb" verstärkt zu verfolgen bzw. voranzutreiben.

4.5 Erfassung der eingesetzten Supervisory Control and Data Acquisition- bzw. Mess-, Steuer- und Regelungssysteme

Im Antwortschreiben auf einen Fragenkatalog des Stadtrechnungshofes Wien gab die Magistratsabteilung 01 an, dass die damalige Magistratsabteilung 14 im Zuge ihrer Sicherheitsüberlegungen darauf achtete, SCADA- bzw. MSR-Systeme nicht im klassischen Verwaltungsnetz zu etablieren.

In einem ersten Schritt wurden Anfang des Jahres 2013 die bestehenden Kunden-VPNs innerhalb der Magistratsabteilung 14 erhoben. Die Erhebung der Kunden-VPNs implizierte dabei die Annahme der Magistratsabteilung 14, dass es sich mit hoher Wahrscheinlichkeit um ein SCADA- bzw. MSR-System handle. Ergänzend dazu wurden einige Monate später die Dienststellen per E-Mail aufgefordert, die in ihrem Verantwortungsbereich vorhandenen Netzwerke zu melden und die Eckdaten darüber in eine vorgefertigte Liste einzutragen. Die Interpretation, ob es sich bei den angegebenen Systemen um ein SCADA- bzw. MSR-System handle oder nicht, wurde den jeweilig betriebsführenden Dienststellen überlassen. Eine neuerliche in den Folgejahren durchgeführte Abfrage erfolgte seitens der Magistratsabteilung 01 nicht.

Die Evaluierung lieferte - aus Sicht der jeweilig betriebsführenden Dienststellen des Magistrats der Stadt Wien - im Wesentlichen eine Auflistung von jenen SCADA- bzw. MSR-Systemen, die in der Stadt Wien betrieben werden. Ob im Weg der Evaluierung alle in der Stadt Wien betriebenen SCADA- bzw. MSR-Systeme erfasst wurden, konnte die Magistratsabteilung 01 nicht bestätigen.

Aus Sicht des Stadtrechnungshofes Wien ist aufgrund der Bedeutung der in Punkt 2. dargelegten Grundlagen als auch der in Punkt 3. angeführten Vorgaben eine detaillierte und vollständige Erfassung von SCADA- bzw. MSR-Systemen in der Stadt Wien für die Umsetzung entsprechender Maßnahmen aus der angeführten Policy bzw. Richtlinie notwendig.

Vom Stadtrechnungshof Wien ist in diesem Zusammenhang auf die allfällig fehlende Sichtweise bzw. Erfassung von SCADA- bzw. MSR-Systemen jener Organisationseinheiten, die von der Magistratsabteilung 01 mit 1. Juli 2018 übernommen bzw. den allfällig weiteren von der Magistratsabteilung 01 betreuten und von der Prüfung ausgenommenen Stellen hinzuweisen (s. Punkt 1.1).

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 01, alle Maßnahmen für eine detaillierte und vollständige Erfassung von SCADA- bzw. MSR-Systemen sowohl der im Magistrat der Stadt Wien, als auch in den von der Magistratsabteilung 01 mit 1. Juli 2018 übernommenen Bereichen bzw. allenfalls weiteren betreuten Stellen in Abstimmung mit den weiteren verantwortlichen Stellen und Funktionen zu veranlassen.

Dabei wären die Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Prozessmanagement und IKT-Strategie bzw. mit der CISO der Stadt Wien einzubinden.

4.6 Kategorisierung bzw. Priorisierung der erfassten Supervisory Control and Data Acquisition- bzw. Mess-, Steuer- und Regelungssysteme

All jene im Weg der Evaluierung erfassten Systeme wurden vom Referat Security, Safety und Compliance der Magistratsabteilung 01 und in Zusammenarbeit mit der Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Prozessmanagement und IKT-Strategie (CISO der Stadt Wien) bearbeitet und dahingehend priorisiert, ob es sich um ein infrastrukturkritisches SCADA- bzw. MSR-System handle oder nicht. Ziel der Priorisierung war es, entsprechenden System- bzw. Sicherheits-

prüfungen an den infrastrukturkritischen SCADA- bzw. MSR-Systemen durchführen zu lassen.

Eine Aufstellung über die Kategorisierung bzw. Priorisierung der einzelnen SCADA- bzw. MSR-Systeme wurde dem Stadtrechnungshof Wien in Form einer Tabelle übergeben. Diese hatte Informationen wie die betreibende Stelle, die Netzwerkbezeichnung, die Kurzbeschreibung des Systems sowie Informationen ob bzw. wann und durch wen eine Überprüfung des Systems durchgeführt wurde. Ferner wurden die angeführten Anlagen nach deren Auswirkungen bei einem Schadensfall priorisiert. Eine Matrix, welche Kriterien der Priorisierung der einzelnen Anlagen zugrunde liegen, konnte dem Stadtrechnungshof Wien nicht vorgelegt werden. Eine z.B. detaillierte Tabelle bzw. Datenbank mit Metainformationen zu kritische Infrastruktur Kategorisierung, NISG Kategorisierung, Informationen zu Maßnahmen gemäß der Policy bzw. Richtlinie, Informationen Securitycheck, Informationen zu System- bzw. Sicherheitsprüfungen (Penetrationstests), Informationen zu Sicherheitsberichten, Informationen zur Aktenlage, Informationen zur Anlage wie Inbetriebnahmedatum, finanztechnische Information usw.) lag zum Prüfungszeitpunkt nicht vor.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 01 alle Maßnahmen einzuleiten, um auf Basis der rechtlichen Vorgaben bzw. weiterer relevanter Regelwerke (z.B. NISG, IEC 62443 usw.) und den Erfordernissen der Verwaltung (Management) und des Betriebes von SCADA- bzw. MSR-Systemen gemäß dem Aufgabengebiet der Magistratsabteilung 01 eine entsprechende Aufstellung über die Kategorisierung bzw. Priorisierung in Verbindung mit dem jeweiligen SCADA- bzw. MSR-System mit den jeweils notwendigen Informationen in Abstimmung mit den weiteren verantwortlichen Stellen und Funktionen zu veranlassen. Dabei wären die Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Prozessmanagement und IKT-Strategie bzw. mit dem CISO der Stadt Wien einzubinden.

Stellungnahme der Magistratsabteilung 01:
Die Aufstellung der einzelnen SCADA- bzw. MSR-Systeme enthielt auch Angaben, welche Kriterien der Priorisierung der einzelnen Anlagen zugrunde liegen.

4.7 System- bzw. Sicherheitsprüfungen (Penetrationstests)

4.7.1 Auf Basis der Erhebung und der ersten Priorisierung der erfassten SCADA- bzw. MSR-Systeme wurden vom Referat Security, Safety und Compliance der Magistratsabteilung 01 und in Zusammenarbeit mit dem CISO der Stadt Wien entsprechende SCADA- bzw. MSR-Systeme von Dienststellen für die ersten System- bzw. Sicherheitsprüfungen (Penetrationstest) ausgewählt.

Zur Durchführung solcher ersten Penetrationstests wurden externe Fachfirmen beauftragt. Die Beauftragung, Begleitung und Koordination dieser ersten Penetrationstests erfolgte durch das Referat Security, Safety und Compliance der Magistratsabteilung 01. Die anfallenden Kosten der ersten Penetrationstests wurden vom Zentralbudget der Magistratsabteilung 01 bedeckt und von der Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Prozessmanagement und IKT-Strategie entsprechend genehmigt.

Von der Magistratsabteilung 01 wurde angemerkt, dass - aufgrund von ungenügender Personalausstattung - nur in wenigen Fällen Prüfungen (Penetrationstests) durch das Referat Security, Safety und Compliance der Magistratsabteilung 01 selbst vorgenommen werden konnten. Gemäß der Magistratsabteilung 01 wurden diese Prüfungen (Penetrationstests) vorwiegend durch extern beauftragte Firmen durchgeführt.

Die Ergebnisse des Penetrationstests wurden an den CISO der Stadt Wien, an das Referat Security, Safety und Compliance der Magistratsabteilung 01 und an die betreffende Dienststelle übermittelt. In weiterer Folge wurden die Maßnahmen, die im Penetrationstest zur Umsetzung empfohlen wurden, gemeinsam mit der Dienststelle erläutert. Die Umsetzung der ausgewiesenen Maßnahmen des Penetrationstests ob-

lag aber letztendlich der jeweiligen Dienststelle, in deren Verantwortung der Betrieb des jeweiligen SCADA- bzw. MSR-System fällt.

4.7.2 Seitens des Referats Security, Safety und Compliance der Magistratsabteilung 01 wird eine eigenständige Nachverfolgung bzw. Überprüfung der effektiven Umsetzung in Dienststellen aufgrund der fehlenden organisatorischen Regelung mit einer festgelegten Befugnis nicht gesehen bzw. kann diese weiterführend nicht durchgeführt werden. Nur bei einer "freiwilligen" Rückmeldung der Dienststelle wird ein entsprechender neuer Penetrationstest zur Überprüfung der Umsetzung aus dem letzten Penetrationstest vom Referat Security, Safety und Compliance der Magistratsabteilung 01 weiter veranlasst.

Folgenden Aufgaben waren gemäß der im Intranet der Stadt Wien dargelegten Referatseinteilung des Referates Security, Safety und Compliance der Magistratsabteilung 01 angeführt:

Informationssicherheitsmanagement
- Zertifiziertes ISMS gemäß ISO/IEC 27001 und
- Umsetzung der Informationssicherheitsstrategie der Stadt Wien.

BCM
- Zertifiziertes BCM gemäß ISO 22301,
- Krisenmanagement und
- Zielvorgaben für das SCM und Notfallmanagement.

Compliance Management
- Risikomanagement für wesentliche Regelverstöße und
- Audit Management.

IKT-Sicherheitsbeauftragte bzw. IKT-Sicherheitsbeauftragter der Magistratsabteilung 01
- Ansprechperson für die bzw. den CISO der Stadt Wien und

- Unterstützung der Dienststellenleiterin bzw. des Dienststellenleiters der Magistratsabteilung 01 bei Fragen der Informationssicherheit.

WienCERT
- Ableitung der technischen Sicherheitsstrategie und Sicherheitsarchitektur aus der Informationssicherheitsstrategie der Stadt Wien,
- Beobachtung und Analyse von Risiken und Sicherheitsvorfällen,
- Lagebeurteilung,
- Vermeidung und Behandlung von Sicherheitsvorfällen und
- Zusammenarbeit und Abstimmung mit nationalen und internationalen Sicherheitsteams und Stadt Wien nahen Organisationen.

Die Aufgaben und Befugnisse des Referates Security, Safety und Compliance und des WienCERT der Magistratsabteilung 01 leiten sich ferner aus dem Erlass MD-OS 51600-2013-1 Sicherheit in der "Informations- und Kommunikationstechnologie" ab.

Aus Sicht des Stadtrechnungshofes Wien wird im genannten Erlass unter Punkt *"4.3. Verantwortlichkeiten der IKT-Dienststelle(n)"* eine mögliche aber nicht eindeutige Zuständigkeit bzw. Verantwortlichkeit im Zusammenhang mit der Thematik von SCADA- bzw. MSR-Systemen dargelegt.

Für den Stadtrechnungshof Wien begründet sich dies im Wesentlichen über eine unklare bzw. fehlende Abgrenzung der Begriffsbestimmungen "IKT-Einrichtungen", "IKT-Infrastruktur" und "OT" (s. Punkt 2.5).

Unter Punkt *"5. Abweichende Verantwortlichkeiten"* des genannten Erlasses besteht die Möglichkeit, abweichende Vorgehensweise und Verantwortlichkeiten festzulegen. Derartige abweichende Verantwortlichkeiten im Bezug zur vorliegenden Thematik im Zusammenhang zu SCADA- bzw. MSR-Systemen waren für den Stadtrechnungshof Wien bei der Magistratsabteilung 01 nicht erkennbar.

4.7.3 Seitens des CISO der Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Prozessmanagement und IKT-Strategie ist langfristig die Strategie derartige Penetrationstests nicht durch die Magistratsabteilung 01 bzw. der Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Prozessmanagement und IKT-Strategie zu beauftragen, zu koordinieren und zu finanzieren. Es sollte vielmehr damit ein erster Anstoß zur Schaffung eines Sicherheits- und Aufgabenbewusstseins in der für das jeweilige SCADA- bzw. MSR-System zuständigen Dienststellen iniziiert werden.

Langfristig ist es das Ziel, das derartige Penetrationstests und die Umsetzung der daraus abgeleiteten Maßnahmen im Rahmen der Betriebsführung des jeweiligen SCADA- bzw. MSR-System von den jeweils betriebsführenden Dienststellen berücksichtigt und eigenständig durchgeführt werden.

4.7.4 Von der Magistratsabteilung 01 wurde beispielhaft der zeitliche Ablauf eines Penetrationstests bzw. Rechecks (s. Punkt 4.7.1) dargelegt. Folgender zeitlicher Rahmen war in der Abwicklung gegeben. Innerhalb von rd. acht Monaten wurde das Startgespräch, die Beauftragung und Durchführung eines Penetrationstests sowie der Endbericht abgewickelt. Nach rd. zwei Jahren und vier Monaten wurde vom WienCERT eine Rückmeldung der getroffenen Maßnahmen von der Dienststelle erbeten, um einen neuen Penetrationstest zur Überprüfung der Umsetzung veranlassen zu können. Nach rd. zwei Jahren und drei Monaten bestätigte die Dienststelle nach mehrmaligem Schriftverkehr die Überprüfung durch einen neuen Penetrationstest (Grund war der Umbau der Anlage) an das WienCERT. Innerhalb von rd. fünf Monaten erfolgte ein weiterer Penetrationstest mit der Übermittlung eines Berichtsentwurfes.

Der Stadtrechnungshof Wien anerkannte die bereits gesetzten Anstrengungen und schloss aus den voran dargelegten Informationen, dass noch weitere klarere bzw. ausreichend organisatorische und verpflichtende Regelungen, Befugnisse und Ressourcen notwendig sind, um eine effizientere und effektivere Koordination der The-

matiken in Zusammenhang mit Automatisierungssystemen in der Stadt Wien (SCADA- bzw. MSR-Systeme sowie von OT) bewerkstelligen zu können.

Dies gilt insbesondere unter dem Paradigma der entsprechend gesetzlichen Vorgaben (NISG) und einer zu bewertenden Kritikalität (kritische Infrastruktur) der jeweilig sich im Einsatz befindlichen Automatisierungssystemen in der Stadt Wien (SCADA- bzw. MSR-Systeme sowie von OT).

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 01 alle Maßnahmen einzuleiten, um alle erforderlichen Schritte für eine ganzheitliche strukturierte und nachvollziehbare Koordination von Automatisierungssystemen in der Stadt Wien (SCADA- bzw. MSR-Systeme sowie von OT) in Abstimmung mit den weiteren verantwortlichen Stellen und Funktionen zu veranlassen. Dabei wären die Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Prozessmanagement und IKT-Strategie mit dem CISO der Stadt Wien einzubinden.

5. Stichprobenweise Überprüfung eines Supervisory Control and Data Acquisition- bzw. Mess-, Steuer- und Regelungssystems

Auf Basis der ersten durchgeführten Penetrationstests wurde die Umsetzung der in einem Ergebnisbericht ausgewiesenen Maßnahmen eines ausgewählten SCADA- bzw. MSR-System bei einer Dienststelle der Stadt Wien stichprobenartig durch den Stadtrechnungshof Wien überprüft.

Diese Überprüfung erfolgte durch eine zeitknappe Ankündigung in der betreffenden Dienststellenleitung, dem Leiter des Referats Security, Safety und Compliance bzw. des WienCERT der Magistratsabteilung 01, dem CISO der Stadt Wien sowie dem Leiter der Internen Revision der Magistratsabteilung 01.

Vor Ort wurde unter Beiziehung eines Vertreters des Referates Security, Safety und Compliance bzw. des WienCERT der Magistratsabteilung 01 sowie die für das SCADA- bzw. MSR-System zuständigen Mitarbeitenden der betreffenden Dienststel-

le die entsprechenden Überprüfungen am diesbezüglichen SCADA- bzw. MSR-System vorgenommen.

Dabei wurden aus dem Ergebnisbericht des durchgeführten Penetrationstests stichprobenartig einige - unter einer wirtschaftlichen und technisch möglichen Vorgehensweise - dokumentierte Schwachstellen auf die Umsetzung der vorgeschlagenen Maßnahmen überprüft.

Die Überprüfung ergab, dass die aus dem Ergebnisbericht des durchgeführten Penetrationstests ausgewählten Maßnahmen zum Prüfungszeitpunkt nicht erkennbar umgesetzt waren.

Seitens der zuständigen Mitarbeitenden der betreffenden Dienststelle wurde angegeben, dass entsprechende Veranlassungen zur Umsetzung der vorgeschlagenen Maßnahmen aus dem Ergebnisbericht des Penetrationstests bei der zuständigen Firma grundsätzlich veranlasst wurden. Ferner wurde mitgeteilt, dass aufgrund des Ausscheidens eines Mitarbeitenden entsprechendes Wissen im Zusammenhang mit dem betreffenden System nicht mehr zur Verfügung stand.

Der Stadtrechnungshof Wien wies darauf hin, das genauere Daten und Informationen zu dem dargelegten Ergebnis der stichprobenartigen Überprüfung der Informationssicherheit unterliegen und nicht durch die Veröffentlichung im vorliegenden Prüfungsbericht dargelegt werden dürfen. Bei einer Veröffentlichung der Informationen würde ein inhärentes Risiko der Ausnutzung dieser veröffentlichten Schwachstelle durch einen entsprechenden versierten Angreifer ("Hacker") gegeben sein.

Das Ergebnis der voran dargelegten vor Ort Überprüfung bestätigte all jene im Prüfungsbericht bereits dargelegten Gegebenheiten, Feststellungen und Erkenntnisse und den dadurch ausgesprochenen Empfehlungen.

Der Stadtrechnungshof Wien empfahl der Magistratsabteilung 01, alle Maßnahmen einzuleiten, um bei der Einleitung der erforderlichen Schritte bzw. der Evaluierung

von Automatisierungssystemen für eine ganzheitlich strukturierte und nachvollziehbare Koordination innerhalb der Stadt Wien (SCADA- bzw. MSR-Systeme sowie von OT) zu sorgen. Die Überprüfbarkeit bzw. die Nachverfolgung von umzusetzenden Maßnahmen im Sinn eines entsprechenden Risikomanagements bzw. eines auszugestaltenden IKS wäre mitzubetrachten.

6. Zusammenfassung der Empfehlungen

Empfehlung Nr. 1:

Alle notwendigen Schritte zu einer Evaluierung der Geschäftseinteilung für den Magistrat der Stadt Wien hinsichtlich der eindeutigen Zuständigkeiten von IKT-Sicherheit (Informationssicherheit) bei SCADA- bzw. MSR-Systemen sind einzuleiten. Bei einer diesbezüglichen Evaluierung sollte eine mögliche Umsetzung im Rahmen eines "Compliance Management Systems" in der Stadt Wien nicht unbeachtet bleiben (s. Punkt 4.1).

Stellungnahme der Magistratsabteilung 01:

Die organisatorischen Verantwortungen in der Stadt Wien zur IKT-Sicherheit werden nicht alleine durch die Geschäftseinteilung für den Magistrat der Stadt Wien geregelt, sondern auch durch die weiteren Bestimmungen des Erlasses "Sicherheit in der Informations- und Kommunikationstechnologie, Zl. MD-OS 51600-2013-1" vom 28. Jänner 2013.

Dessen Punkt 4.2 bestimmt zu den Verantwortlichkeiten der Leiterinnen bzw. Leiter der (auftraggebenden) verantwortlichen Stellen: "Jede Leiterin und jeder Leiter einer (auftraggebenden) verantwortlichen Stelle hat die zur Gewährleistung der IKT-Sicherheit (im eigenen Bereich) erforderlichen organisatorischen, personellen, technischen und baulichen Maßnahmen zu veranlassen." Die Begriffe "auftraggebende" bzw. "verantwortliche Stellen" sind dabei im datenschutzrechtlichen Sinn zu ver-

stehen, gemeint sind damit Dienststellen gemäß § 3 der Geschäftsordnung für den Magistrat der Stadt Wien oder Unternehmungen gemäß § 71 der Wiener Stadtverfassung.

Hingegen bestimmt Punkt 4.3 zu den Verantwortlichkeiten der IKT-Dienststelle(n):

"Sie sind für die zur Gewährleistung der IKT-Sicherheit (im eigenen Bereich sowie für die von der jeweiligen IKT-Dienststelle betriebene IKT-Infrastruktur) erforderlichen organisatorischen, personellen, technischen und baulichen Maßnahmen verantwortlich."

Somit ist eindeutig klargelegt, dass die IKT-Sicherheit von SCADA- bzw. MSR-Systemen, die durch die Dienststellen selbst betrieben werden, auch in deren Verantwortungsbereich liegt. Damit ist aus Sicht der Magistratsabteilung 01 auch kein Bedarf gegeben, die Geschäftsordnung für den Magistrat der Stadt Wien zu ändern.

Empfehlung Nr. 2:
Gemäß den Vorgaben des Erlasses MDK-168759-1/12 Büroordnung für den Magistrat der Stadt Wien wäre eine Dokumentation im Hinblick auf das Thema Sicherheit bei SCADA- bzw. MSR-Systemen sicherzustellen (s. Punkt 4.3).

Stellungnahme der Magistratsabteilung 01:
Die Magistratsabteilung 01 wird bei von ihr initiierten Besprechungen die vorgeschlagene Empfehlung in Form einer geeigneten Dokumentation umsetzen.

Empfehlung Nr. 3:
Die vorliegenden Inhalte und Linkverknüpfungen der Intranetseite "Security für SCADA-Systeme" des WienCERT - Security Informationen Blog wären zu überprüfen (s. Punkt 4.3.2).

Stellungnahme der Magistratsabteilung 01:
Die Empfehlung wurde für diesen einen Blog-Artikel bereits umgesetzt.

Empfehlung Nr. 4:
Der Prozess der Bereitstellung bzw. Aktualisierung der Informationen der Intranetseite "Security für SCADA-Systeme" des WienCERT - Security Informationen Blog mit dem Link auf das Dokument "Securityvorgaben für Regelungs-, Steuerungs- und Messsysteme; Vergabe, Implementierung, Betrieb" wäre aufgrund der Bedeutung der Thematik zu evaluieren. Dabei wiederkehrend Prüfungen der einwandfreien Funktion bzw. Abrufbarkeit dieser Intranetseite wären in Betracht zu ziehen (s. Punkt 4.3.2).

Stellungnahme der Magistratsabteilung 01:
Die von der Magistratsabteilung 01 betreute Intranet-Seite mit Security-relevanten Informationen wurde Jahre nach Veröffentlichung des zitierten Blog-Artikels - wie auch viele andere Intranet-Auftritte - auf eine neue Technologie migriert. Dadurch änderten sich zwangsläufig auch die Adressen einzelner Unterlagen. Es wurde jedoch zu jedem Zeitpunkt sichergestellt, dass die Verlinkung aus der aktuellen Security-Homepage heraus funktioniert. Das einwandfreie Funktionieren von Verlinkungen, die außerhalb des Einflusses der Magistratsabteilung 01 erfolgen, oder Verlinkungen in alten Blog-Artikeln (Tagebucheinträge sind nicht dafür gedacht, beliebig im Nachhinein geändert zu werden) kann bei Änderungen der zugrunde liegenden Techno-

logie leider nicht gewährleistet werden. Dies ist kein Einzelphänomen, sondern betrifft das gesamte World Wide Web.

In der Zwischenzeit gibt es das Informationssicherheitsportal mit allen relevanten Informationen. Dieses kann im Intranet (www.intern.magwien.gv.at) unter "Technische Hilfe|Security" aufgerufen werden und hat - Stand heute - den URL https://www.intern.magwien.gv.at/web/informationssicherheit/. Das angesprochene Dokument wird im Rahmen dieses Informationssicherheitsportals publiziert. Seitens der Magistratsabteilung 01 kann sichergestellt werden, dass Verlinkungen aus dem Portal auf das Dokument funktionieren. Bei außerhalb des Informationssicherheitsportals vorgenommenen Verlinkungen kann es auch künftig zu "broken links" kommen, da das Informationssicherheitsportal als Einheit gesehen wird und eine Verlinkung von außen auf einzelne Inhalte ("deep links") nicht vorgesehen und nicht unterstützt ist, technisch aber nicht verhindert werden kann. Qualitätsgesicherte Dokumente müssen zumindest jährlich auf Aktualität überprüft und gegebenenfalls angepasst werden. Blog-Einträge zählen nicht dazu.

Empfehlung Nr. 5:
Alle Maßnahmen zu einer Evaluierung einer verbindlichen Anwendung der Policy bzw. Richtlinie "Securityvorgaben für Regelungs-, Steuerungs- und Messsysteme; Vergabe, Implementierung, Betrieb" für SCADA- bzw. MSR-Systeme im Magistrat der Stadt Wien wären vorzunehmen (s. Punkt 4.4).

Stellungnahme der Magistratsabteilung 01:
Bereits während der Prüfung fanden Gespräche mit der Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Prozessmanagement und IKT-Strategie zur Überarbeitung des IKT-Sicherheitserlasses statt. Die Magistratsabtei-

lung 01 wird in diesem Zusammenhang die Evaluierung der Verbindlichkeit der Policy bzw. Richtlinie "Securityvorgaben für Regelungs-, Steuerungs- und Messsysteme; Vergabe, Implementierung, Betrieb" thematisieren.

Empfehlung Nr. 6:
Das bereits gesetzte Ziel einer Einbindung bzw. Berücksichtigung der Normenreihe IEC 62443 in der Policy bzw. Richtlinie "Securityvorgaben für Regelungs-, Steuerungs- und Messsysteme; Vergabe, Implementierung, Betrieb" wäre verstärkt zu verfolgen bzw. voranzutreiben (s. Punkt 4.4).

Stellungnahme der Magistratsabteilung 01:
Eine Überarbeitung der bestehenden Unterlagen unter Berücksichtigung der IEC 62443 wird erfolgen.

Empfehlung Nr. 7:
Alle Maßnahmen für eine detaillierte und vollständige Erfassung von SCADA- bzw. MSR-Systemen sowohl der im Magistrat der Stadt Wien, als auch in den von der Magistratsabteilung 01 mit 1. Juli 2018 übernommenen Bereichen bzw. allenfalls weiteren betreuten Stellen in Abstimmung mit den weiteren verantwortlichen Stellen und Funktionen wären zu veranlassen (s. Punkt 4.5).

Stellungnahme der Magistratsabteilung 01:
Die Magistratsabteilung 01 wird im Zuge der Überarbeitung des IKT-Sicherheitserlasses anregen, dass der Betrieb derartiger Systeme durch Dienststellen in ihrem eigenen Bereich an die Magistratsabteilung 01 gemeldet werden muss. Dadurch würde eine Möglichkeit geschaffen, eine Gesamtübersicht über die im Magistrat der Stadt Wien betriebenen Systeme zu führen und diese regelmäßig zu aktualisieren.

Empfehlung Nr. 8:
Alle Maßnahmen wären einzuleiten, um auf Basis der rechtlichen Vorgaben bzw. weiterer relevanter Regelwerke (z.B. NISG, IEC 62443 usw.) und den Erfordernissen der Verwaltung (Management) und des Betriebes von SCADA- bzw. MSR-Systemen gemäß dem Aufgabengebiet der Magistratsabteilung 01 eine entsprechende Aufstellung über die Kategorisierung bzw. Priorisierung in Verbindung mit dem jeweiligen SCADA- bzw. MSR-System mit den jeweils notwendigen Informationen in Abstimmung mit den weiteren verantwortlichen Stellen und Funktionen zu veranlassen (s. Punkt 4.6).

Stellungnahme der Magistratsabteilung 01:
Eine Kategorisierung der Systeme mit den aus Sicht der Informationssicherheit erforderlichen Informationen wird im Zuge der Erstellung der Aufstellung gemäß Empfehlung Nr. 6 vorgenommen werden. Der Eintrag der Priorisierung erfolgt über Beauftragung der gegenüber der Magistratsabteilung 01 weisungsberechtigten Stellen.

Empfehlung Nr. 9:
Alle Maßnahmen wären einzuleiten, um alle erforderlichen Schritte für eine ganzheitliche strukturierte und nachvollziehbare Koordination von Automatisierungssystemen in der Stadt Wien (SCADA- bzw. MSR-Systeme sowie von OT) in Abstimmung mit den weiteren verantwortlichen Stellen und Funktionen zu veranlassen (s. Punkt 4.7.4).

Stellungnahme der Magistratsabteilung 01:
Die Magistratsabteilung 01 wird im Zuge der Überarbeitung des IKT-Sicherheitserlasses dieses Thema einbringen.

Empfehlung Nr. 10:
Alle Maßnahmen wären einzuleiten, um bei der Einleitung der erforderlichen Schritte bzw. der Evaluierung von Automatisierungssystemen für eine ganzheitlich strukturierte und nachvollziehbare Koordination innerhalb der Stadt Wien (SCADA- bzw. MSR-Systeme sowie von OT) zu sorgen. Die Überprüfbarkeit bzw. die Nachverfolgung von umzusetzenden Maßnahmen im Sinn eines entsprechenden Risikomanagements bzw. eines auszugestaltenden IKS wäre mitzubetrachten (s. Punkt 5.).

Stellungnahme der Magistratsabteilung 01:
Die Magistratsabteilung 01 wird im Zuge der Überarbeitung des IKT-Sicherheitserlasses dieses Thema einbringen.

Der Stadtrechnungshofdirektor:
Dr. Peter Pollak, MBA
Wien, im März 2020