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

Maßnahmenbekanntgabe zu

MA 01, Prüfung von Steuerungssystemen

INHALTSVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

Blog	Weblog
bzw.	beziehungsweise
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
ELAK	Elektronischer Akt
https	Hypertext Transfer Protocol Secure
ICS	Industrial Control System
IEC	International Electrotechnical Commission
IKS	Internes Kontrollsystem

IKT	Informations- und Kommunikationstechnologie
IT	Informationstechnologie
lt.	laut
MDK	Magistratsdirektor - Gruppe Koordination
MD-OS	Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit
MSR-System	Mess-, Steuer- und Regelungssystem
NIS	Netz- und Informationssystemsicherheit
NISG	Netz- und Informationssystemsicherheitsgesetz
NIST SP	National Institute of Standards and Technology Special Publication
Nr.	Nummer
OT	Operational Technology
Rev. 2	Revision 2
SCADA	Supervisory Control and Data Acquisition
URL	Uniform Resource Locator
usw.	und so weiter
WEB	Kurzform Internet
www	World Wide Web
z.B.	zum Beispiel
Zl.	Zahl

Erledigung des Prüfungsberichtes

Der Stadtrechnungshof Wien unterzog die Magistratsabteilung 01 hinsichtlich der IKT-Sicherheit bei verwendeten Steuerungssystemen der Stadt Wien einer Prüfung. Der diesbezügliche Bericht des Stadtrechnungshofes Wien wurde am 10. März 2020 veröffentlicht und im Rahmen der Sitzung des Stadtrechnungshofausschusses vom 13. Mai 2020, Ausschusszahl 24/20 mit Beschluss zur Kenntnis genommen.

Kurzfassung des Prüfungsberichtes

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 Automatisie-

rungssystemen (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.

Bericht der Magistratsabteilung 01 zum Stand der Umsetzung der Empfehlungen

Im Rahmen der Äußerung der geprüften Stelle wurde folgender Umsetzungsstand in Bezug auf die ergangenen 10 Empfehlungen bekannt gegeben:

Stand der Umsetzung der Empfehlungen	Anzahl	Anteil in %
umgesetzt	8	80,0
in Umsetzung	1	10,0
geplant/in Bearbeitung	-	-
nicht geplant	1	10,0

Umsetzungsstand im Einzelnen

Begründung bzw. Erläuterung der Maßnahmenbekanntgabe seitens der geprüften Stelle unter Zuordnung zu den im oben genannten Bericht des Stadtrechnungshofes Wien erfolgten Empfehlungen, der jeweiligen Stellungnahme zu diesen Empfehlungen seitens der geprüften Stelle und allfälliger Gegenäußerung des Stadtrechnungshofes Wien:

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.

Stellungnahme der geprüften Stelle:

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.

Maßnahmenbekanntgabe der geprüften Stelle:
Die Umsetzung der Empfehlung ist nicht geplant.

Für die IKT-Sicherheit bzw. Informationssicherheit sind alle Dienststellen und Bediensteten der Stadt Wien verantwortlich, für Regelung von Zuständigkeiten im Detail scheint die Geschäftseinteilung nicht das geeignete Instrument zu sein. Vielmehr soll die Abgrenzung der einzelnen Verantwortlichkeiten zwischen der Magistratsdirektion Gruppe Prozessmanagement und IKT-Strategie des Geschäftsbereichs Organisation und Sicherheit, den IKT-Dienststellen, den sonstigen Dienststellen und den Benutzerinnen bzw. Benutzern in Abstimmung mit der Magistratsdirektion Gruppe Prozessmanagement und IKT-Strategie im IKT-Sicherheitserlass in kompakt zusammengefasster Form erfolgen. Der derzeit geltende Erlass "Sicherheit in der

Informations- und Kommunikationstechnologie", MD-OS 51600-2013-1 vom 28. Jänner 2013 befindet sich in Überarbeitung. Die Verantwortung für die IKT-Sicherheit von SCADA- bzw. MSR-Systemen soll dabei durch die ausdrückliche Erwähnung des "sicheren Betriebs von IKT-Services und IKT-Infrastruktur in dienststelleneigener Verantwortung" eindeutig klargestellt werden. Dafür ist vorgesehen, dass die Dienststellen ein Informationssicherheitsmanagement mit speziellen Vorgaben je Klassifikation umsetzen müssen. Die Spezifizierung dieser Vorgaben wird 2021 in einem Projekt erarbeitet.

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.

Stellungnahme der geprüften Stelle:

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

Maßnahmenbekanntgabe der geprüften Stelle:

Die Empfehlung wurde umgesetzt.

Seitens der Magistratsabteilung 01 wird der Nachweis über die Kommunikation mit den Dienststellen, betreffend der in ihrem eigenen Wirkungsbereich betriebenen SCADA- bzw. MSR-Systemen, künftig im ELAK dokumentiert werden.

Empfehlung Nr. 3

Die vorliegenden Inhalte und Linkverknüpfungen der Intranetseite "Security für SCADA-Systeme" des WienCERT - Security Informationen Blog wären zu überprüfen.

Stellungnahme der geprüften Stelle:
Die Empfehlung wurde für diesen einen Blog-Artikel bereits umgesetzt.

Maßnahmenbekanntgabe der geprüften Stelle:
Die Empfehlung wurde umgesetzt.

Im konkreten Blog-Artikel wurde die entsprechende "Linkverknüpfung" (URL) auf die aktuell gültige geändert.

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.

Stellungnahme der geprüften Stelle:
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.

<u>Maßnahmenbekanntgabe der geprüften Stelle:</u>
Die Empfehlung wurde umgesetzt.

Das angesprochene Dokument wird im Rahmen eines Informationssicherheitsportals publiziert. Seitens der Magistratsabteilung 01 kann sichergestellt werden, dass Verlinkungen aus dem Portal auf das Dokument funktionieren. Eine Verlinkung durch Autorinnen bzw. Autoren, die außerhalb dieses Informationssicherheitsportals ihren WEB - Content mit diesen Dokumenten in Form sogenannter "deep links" verbinden, kann nicht verhindert werden und liegt außerhalb des Einflusses und der Möglichkeiten des Informationssicherheitsportals, sodass für deren Funktionieren keine Garantie übernommen werden kann.

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.

Stellungnahme der geprüften Stelle:

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

Maßnahmenbekanntgabe der geprüften Stelle:

Die Empfehlung wurde umgesetzt.

Sobald die überarbeitete Sicherheitsvorgabe gemäß der Empfehlung Nr. 6 des Berichtes des Stadtrechnungshofes Wien vorliegt, wird diese von der Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Prozessmanagement und IKT-Strategie gegenüber den Abteilungen für verbindlich erklärt werden.

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.

Stellungnahme der geprüften Stelle:
Eine Überarbeitung der bestehenden Unterlagen unter Berücksichtigung der IEC 62443 wird erfolgen.

Maßnahmenbekanntgabe der geprüften Stelle:
Die Empfehlung befindet sich in Umsetzung.

Es wurden "Security-Vorgaben für OT-Systeme für auftraggebende Stellen" und "Security-Vorgaben für OT-Systeme (Lastenheft für Auftragnehmerinnen bzw. Auftragnehmer)" ausgearbeitet. Die Anforderungen und Grundsätze beider Dokumente sind aus branchenweit anerkannten Wissensbeständen wie IEC 62443-2-1, IEC 62443-3-3, IEC 62443-4-2, NIS Fact Sheet 8/2019, NIST SP 800-82 Rev. 2 und dem ICS-Sicherheitskompendium des Bundesamtes für Informationssicherheit (BSI) abgeleitet. Nach einer letzten Abstimmung mit dem Betrieb der Magistratsabteilung 01 und der CISO der Magistratsdirektion sollen diese im Laufe des 1. Quartals 2021 verbindlich in Kraft gesetzt werden.

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.

Stellungnahme der geprüften Stelle:
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.

Maßnahmenbekanntgabe der geprüften Stelle:
Die Empfehlung wurde umgesetzt.

Zur detaillierten und vollständigen Erfassung von SCADA- bzw. MSR-Systemen wurde von der Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Prozessmanagement und IKT-Strategie ein Erhebungsbogen an die Dienststellen ausgesendet. Die eingelangten Rückmeldungen wurden seitens der Magistratsabteilung 01 erfasst und kategorisiert und an die Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Prozessmanagement und IKT-Strategie übermittelt.

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.

Stellungnahme der geprüften Stelle:
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.

Maßnahmenbekanntgabe der geprüften Stelle:
Die Empfehlung wurde umgesetzt.

Anhang der Gesamtliste erfolgt eine Risikobewertung durch die Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Prozessmanagement und IKT-Strategie in Abstimmung mit den Abteilungen und infolge eine Einstufung der Systeme nach kritischer Abstufung bezogen auf die Stadt Wien.

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.

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

Maßnahmenbekanntgabe der geprüften Stelle:
Die Empfehlung wurde umgesetzt.

Es wird von der Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Prozessmanagement und IKT-Strategie ein Sicherheitskonzept für OT (Operational IT) erstellt, welches - abhängig von der Einstufung der Systeme - auch Nachweise über Sicherheitsüberprüfungen bzw. Audits sowie das Monitoring der Umsetzung der sich daraus ergebenden Maßnahmen vorsehen soll.

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.

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

Maßnahmenbekanntgabe der geprüften Stelle:
Die Empfehlung wurde umgesetzt.

Das Monitoring der Maßnahmen wird Teil des Konzeptes der Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Prozessmanagement und IKT-Strategie lt. Empfehlung Nr. 9 sein. Weder die Magistratsdirektion - Geschäftsbereich Organisation und Sicherheit, Gruppe Prozessmanagement und IKT-Strategie noch die Magistratsabteilung 01 werden ein IKS im Verantwortungsbereich der Abteilungen erstellen können.

Für den Stadtrechnungshofdirektor:
Mag. Manfred Jordan
Wien, im Februar 2021