Landeshauptstadt
München
Oberbürgermeister

Landeshauptstadt München, Oberbürgermeister, 80313 München

Dieter Reiter

Stadtratsfraktion
Freiheitsrechte, Transparenz und
Bürgerbeteiligung
Rathaus
Marienplatz 8
80331 München

26.08.2016

Wie gut sind Münchens kritische Infrastrukturen gesichert?

Schriftliche Anfrage nach § 68 GeschO
Anfrage Nr. 14-20 / F 00662 von Herrn StR Dr. Michael Mattar, Frau StRin Gabriele Neff, Herrn StR Dr. Wolfgang Heubisch, Herrn StR Wolfgang Zeilnhofer, Herrn StR Thomas Ranft vom 10.08.2016, eingegangen am 10.08.2016

Az. D-HA II/V1 0471-1-0060

Sehr geehrte Kollegin, sehr geehrte Kollegen,

ich nehme Bezug auf Ihr Schreiben vom 10.08.2016, in dem Sie eine Anfrage zum Thema der Sicherheit von Münchens kritischen Infrastrukturen stellen. In Ihrer Anfrage führen Sie aus:

„Durch das Internet wurde die Administration vieler Infrakstrukturenanlagen vereinfacht. Meist werden die Anlagen über sogenannte Scada-Systeme (Supervisory Control and Data Acquisition) gesteuert, ein Teil davon sind Human Machine Interfaces (HMI).
Obwohl diese auf keinen Fall im Internet auffindbar sein sollten, geschieht es immer wieder, dass auf Grund zum Beispiel falscher Standardeinstellungen der Anbietersoftware, solche Anlagen doch gefunden und auch manipuliert werden können. Eine Manipulation wäre für eine Großstadt wie München fatal, zehntausende Bürgerinnen und Bürger wären davon betroffen. Diese Anlagen sind beliebte Ziele bei Hackern und könnten auch von anderen Gruppen als Schwachstelle genutzt werden.“

Vor der Beantwortung der im Einzelnen gestellten Fragen möchte ich eine kurze Klärung bzw. Präzisierung des Begriffs "Kritische Infrastruktur" für die Landeshauptstadt München (LHM) voranstellen. Dies soll in erster Linie dazu dienen, die Differenzierung in den weiter unten stehenden Antworten auf Ihre Fragen zu erläutern.

Rathaus, Marienplatz 8
80331 München
Telefon: (089) 233 - 82300
Telefax: (089) 233 - 98982300

Ich gehe davon aus, dass Sie den Begriff "Kritische Infrastruktur" auf der Grundlage des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz, IT-SiG) vom 17.06.2016 interpretieren. Demnach sind unter Kritischen Infrastrukturen Einrichtungen oder Anlagen zu verstehen, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, da durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Da diese Definition sehr allgemein gehalten ist, werden kritische Infrastrukturen in die Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen unterteilt. Das IT-Sicherheitsgesetz sieht weiterhin vor, dass kritische Infrastrukturen in den einzelnen Sektoren durch Rechtsverordnungen des Bundesministeriums des Inneren näher bestimmt werden (vgl. Art. 1 Abs. 2 IT-SiG).

Seit dem 3. Mai dieses Jahres ist die diesbezüglich erste "Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz" (BSI-KritisV) in Kraft getreten, die sich auf die Sektoren Energie, Informationstechnik und Telekommunikation, Wasser sowie Ernährung bezieht. In dieser Verordnung wird pro Sektor anhand von angegebenen Kategorien, Bemessungskriterien und Schwellwerten definiert, welche Art von Anlagen als kritische Infrastruktur zu werten sind.
Aus diesen Vorgaben lassen sich im Kern fünf Bereiche identifizieren, in denen Einheiten oder Unternehmen der LHM durch die Rechtsverordnung betroffen sind. Zum einen sind dies die Stadtwerke München (SWM), die im Sektor Energie in den Bereichen Stromversorgung, Gasversorgung und Fernwärmeversorgung sowie im Sektor Wasser im Bereich der Trinkwasserversorgung kritische Infrastrukturen betreiben. Zum anderen ist die Münchner Stadtentwässerung (MSE) im Sektor Wasser im Bereich der Abwasserentsorgung als Betreiber kritischer Infrastrukturen zu werten.
Aus Sicht des von Ihnen angesprochenen Bereichs der IT-Sicherheit sind somit in der Beantwortung ihrer Fragen zwei unterschiedliche Perspektiven zu berücksichtigen. Die Gründe hierfür liegen auch in den unterschiedlichen Rahmenbedingungen, unter denen die IT-Sicherheit in den beiden Organisationen sichergestellt wird.

Die MSE, als Eigenbetrieb der LHM, ist mit ihren lokalen IT-Sicherheitsbeauftragten in die IT-Sicherheitsorganisation der LHM eingebunden. In diesem Rahmen gelten entsprechende IT-Sicherheitsvorgaben und -prozesse sowohl für die Nutzung als auch für die Bereitstellung und den Betrieb von IT-Lösungen, die aus stadtweiter Sicht durch das bei D-III (STRAC) angesiedelte zentrale IT-Sicherheitsmanagement definiert und fortgeschrieben werden. Der grundlegende Ansatz in diesem Bereich baut auf dem Konzept der Risikoorientierung in der IT-Sicherheit auf und ist mit der Implementierung eines Informationssicherheits-Managementsystems (ISMS) bei der LHM an den Normen des ISO/IEC Standards 27001 ausgerichtet.

Die SWM, als eigenständiges Unternehmen, verfügt hingegen über einen von der LHM unabhängigen Ansatz für den Schutz kritischer Infrastrukturen, der sich auf den Konzernbereich der SWM bezieht. Dieser basiert auf bestehenden und zertifizierten Managementsystemen für Qualitätsmanagement (ISO9001) und IT-Servicemanagement (ISO20000), dem Technischen Sicherheitsmanagement, TÜV-Überprüfungen sowie weiterer diverser Normen und Branchenstandards. Ein ISMS auf Basis des ISO/IEC Standards 27001 befindet sich im Aufbau.

Es wird deutlich, dass in beiden Organisationen ähnlich ausgerichtete Ansätze im Bereich des IT-Sicherheitsmanagements bestehen, deren Wirkungsbereiche jedoch auf die jeweiligen Organisationsgrenzen beschränkt sind. Dies kann zu unterschiedlichen Ausprägungen, Gegebenheiten und auch IT-Sicherheitsmaßnahmen führen, wenn es um die Absicherung von Münchens kritischen Infrastrukturen geht. Vor diesem Hintergrund erfolgt die Beantwortung Ihrer gestellten Fragen jeweils einzeln aus Sicht der jeweiligen Organisation.

Die Münchner Stadtentwässerung (MSE) nimmt zur oben genannten Anfrage wie folgt Stellung:

Die Münchner Stadtentwässerung setzt sich als öffentliches Unternehmen aktiv für den Gewässerschutz ein. Fünf übergeordnete Unternehmensziele prägen unsere Arbeit:

- Umwelt- und Gesundheitsschutz
- Nachhaltigkeit
- Wirtschaftlichkeit
- Kundenorientierung
- Sicherheit

Unsere zwei Großklärwerke im Münchner Norden mit insgesamt drei Millionen Einwohnerwerten reinigen täglich 560.000 Kubikmeter Abwasser aus Haushalt und Industrie. Somit ist die Münchner Stadtentwässerung im Sinne des "IT-Sicherheitsgesetzes" und der daraus resultierenden BSI-KritisV über den Sektor Wasser (Vgl. §3 BSI-kritisV) und dem Schwellenwert (500.000 Einwohnerwerten) nach Anhang 2 Teil 3 Spalte D eine sog. "kritische Infrastruktur". Zu den betroffenen Anlagen gehören die dem Prozess Siedlungsentwässerung zugeordnete Anlage Kanalisation sowie dem Prozess Abwasserbehandlung und Gewässereinleitung zugeordnete Anlagen Kläranlage und Leitzentrale.

Frage 1
Durch welche Maßnahmen werden Münchens kritische Infrastrukturen gesichert?

Antwort
Bei der Münchner Stadtentwässerung werden die Maßnahmen aus den IT-Sicherheitsvorgaben der Landeshauptstadt München umgesetzt. Des Weiteren orientieren sich sämtliche getroffene Maßnahmen an den branchenüblichen Standards, wie die Einführung eines Informationssicherheitsmanagementsystems (ISMS) nach DIN ISO/IEC27001:2013, den Maßnahmen des IT-Grundschutzkataloges und des ICS-Kompendiums des Bundesamtes für Sicherheit in der Informationstechnik.
Im Zuge des IT-Sicherheitsgesetzes überprüft die Münchner Stadtentwässerung derzeit sämtliche bereits getroffenen Maßnahmen und strebt hierzu bis zum Jahr 2018 eine Zertifizierung nach DIN ISO/IEC27001:2013 an. Des Weiteren hat die Münchner Stadtentwässerung bereits die folgenden Zertifizierungen mit Auswirkungen auf die Sicherheit von Anlagen vorzuweisen:

- Qualitätsmanagementsystem nach DIN EN ISO 9001
- Umweltmanagementsystem nach DIN EN ISO 14001
- Arbeits- und Gesundheitsschutzmanagementsystem nach BS OHSAS 18001

Frage 2
Gibt es Human Machine Interfaces (HMI) die über das Internet zugänglich sind?
Durch welche Maßnahmen sind diese geschützt? Sind diese im Internet auffindbar?

Antwort
Über das Internet sind keine Human Machine Interfaces (HMI) der Münchner Stadtentwässerung erreichbar.

Frage 3
Sind die Anlagen vor DoS oder DDos-Attacken geschützt?

Antwort
Wir verweisen hierzu im Wesentlichen auf die Antwort zu Frage 2. Der Verwaltungsbereich wird durch den zentralen Dienstleister it@M geschützt.

Frage 4
Wurden von den Münchner Versorgungsgesellschaften alle Sicherheitsrelevanten Einstellungen genau überprüft? Wurden die Firewalls richtig konfiguriert, wurden die Anlagen durch transportverschlüsselte Verbindungen (mittels SSL/TLS/https) gesichert?

Antwort
Alle sicherheitsrelevanten Einstellungen werden regelmäßig und bei Bedarf überprüft und den aktuellen Anforderungen sowie der technischen Machbarkeit angepasst.

Frage 5
Wie werden die gängigen IT-Sicherheitsstandards bei den Versorgungsunternehmen umgesetzt?

Antwort
Wir verweisen hierzu auf die Antwort zu Frage 1.

Des Weiteren nehmen die SWM zu Ihren Fragen wie folgt Stellung:

Die Anlagen zur Erzeugung und Verteilung von Energie und Trinkwasser gelten bei SWM von Beginn an als für die Versorgungssicherheit der Landeshauptstadt München essentielle Anlagen. Aus diesen Gründen unterliegt Planung, Errichtung und Betrieb der Anlagen ganz besonderen Anforderungen. Dies gilt insbesondere z. B. für Objektschutz, Basisschutz (Sicherung der Funktionsfähigkeit) und auch in den letzten Jahren zunehmend der IT-Sicherheit.

Zwischenzeitlich wurden diese Anlagen auch per Gesetz zu „kritischen Infrastruktur-Anlagen“ erklärt, die entsprechende gesetzliche Mindeststandards erfüllen müssen. So werden durch den Gesetzgeber im IT-Sicherheitsgesetz z. B. angemessene organisatorische und technische Vorkehrungen nach dem Stand der Technik gefordert, um die IT-Sicherheit kritischer Infrastrukturen zu gewährleisten. Diesbezüglich wird derzeit ein Informationssicherheits-Managementsystem nach ISO/IEC 27001 bei SWM eingeführt, mit dem sichergestellt ist, dass Schulungen, Anweisungen, Prozessabläufe und IT-Sicherheitsmaßnahmen den aktuell geltenden Anforderungen entsprechen. Eine aus Sicht des Gesetzgebers fristgerechte Zertifizierung wird durch externe Auditoren erfolgen.

Aus der Gesamtverantwortung für die Versorgungssicherheit der Landeshauptstadt München mit Energie und Trinkwasser, damit wesentlichen Teilen der kritischen Infrastrukturen der SWM, verzichten wir auf eine ausführliche Beantwortung der sehr detaillierten Fragen. SWM sind all diese Themenfelder bekannt und es sind wirkungsvolle Schutzsysteme aufgebaut. Diese werden ständig gepflegt und weiterentwickelt um so ein Höchstmaß an Sicherheit für die kritischen Infrastrukturen zu gewährleisten.

Zusammenfassend bleibt festzustellen, dass die Betreiber kritischer Infrastrukturen der Landeshauptstadt München mit den dargestellten Maßnahmen die aktuell bestehenden Anforderungen durch die Gesetzgeber vollumfänglich adressieren.

Von den vorstehenden Ausführungen bitte ich Kenntnis zu nehmen und gehe davon aus, dass die Angelegenheit damit abgeschlossen ist.

Mit freundlichen Grüßen

gez.

Dieter Reiter