Telefon: 233 – 78 23 00

IT-Referat

Schutzschild gegen Cyberattacken erweitern

Schutzschild gegen Cyberattacken erweitern
Antrag Nr. 20-26 / A 02439 von der Herrn StR Manuel Pretzl
vom 24.02.2022, eingegangen am 24.02.2022

Sitzungsvorlage Nr. 20-26 / V 07397
2 Anlagen

- Stadtratsantrag
- Stellungnahmen

Beschluss des IT-Ausschusses vom 19.10.2022 (SB)

Öffentliche Sitzung

Inhaltsverzeichnis

I. Vortrag der Referentin

Zusammenfassung

Die Landeshauptstadt München (LHM) sieht sich stets neuen und unerwarteten Bedrohungen aus dem Cyberraum gegenüber, wie die aktuelle politische Situation mit Russland und die damit verbundenen potenziellen Cyberattacken zeigen.

Der Umgang mit eben dieser sich ständig ändernden Bedrohungslage ist ein wichtiger Aufgabenbereich im Informationssicherheitsmanagement (ISM) der LHM und wird sowohl aus strategischer wie auch operativer Sicht aktiv betrieben.

In diesem Rahmen wurden auch im Kontext des Kriegs in der Ukraine konkrete Sicherheitsmaßnahmen veranlasst, um potentielle Cyberangriffe mit diesem Hintergrund frühzeitig

detektieren zu können. In dieser Weise auf neue Bedrohungslagen zu reagieren und die Abwehrmechanismen der LHM zu stärken, erfolgt im ISM der LHM im Rahmen der regulären Tätigkeiten.

Im Antragstext wurden neben der Verwaltung auch weitere Betreiber*innen im Bereich kritischer Infrastrukturen im Stadtkonzern adressiert. Diese Stellen wurden zum Thema angefragt, ihre Darstellungen sind in Kapitel 4 aufgeführt.

1. Stadtratsantrag

Antragstext: „Die Landeshauptstadt München und die Stadtwerke München GmbH sowie weitere Betreiber kritischer Infrastrukturen werden aufgefordert, ihre Abwehrmechanismen gegen potenzielle Cyberattacken aus Russland zu prüfen und ggf. zu optimieren."

Begründung: „Aufgrund der eskalierenden Lage in der Ukraine und der bereits ausgesprochenen Kriegserklärung Russlands ist zu erwarten, dass weitere Sanktionen gegen Russland in Kraft treten, die auch für den Westen Auswirkungen haben können. In den Medien wird immer wieder darüber spekuliert, wie Russland auf die Sanktionen reagieren könnte. Genannt werden in diesem Zuge vermehrte Cyberattacken auf Behörden, Institutionen und Unternehmen. Betroffen davon könnten auch die Energieversorger sein. Deshalb ist es nötig, dass die Stadtwerke München GmbH, aber auch weitere Betreiber der kritischen Infrastruktur, ihre digitalen Schutzschilde gegen Cyberangriffe umfänglich prüft und alle Möglichkeiten ausschöpft, diese noch weiter zu optimieren. Eine enge Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik ist zu entwickeln bzw. auszubauen."

2. Aktuelle Situation im Informationssicherheitsmanagement der LHM

Kernaufgabe des ISM sind die Gewährleistung der Informationssicherheit und die damit verbundene Abwehr von Bedrohungen aus dem Cyberraum. Dies erfolgt anhand der Sicherheitsdisziplinen Prävention, Detektion, Reaktion und Adaption durch die zwei Säulen strategische Planung und operative Abwehr.

Die strategische und planerische Ebene des ISM wird im IT-Referat (RIT-I) umgesetzt, betrieben und weiterentwickelt. Hierzu gehören unter anderem die Analyse der perspektivischen Bedrohungslage im Cyberraum sowie die langfristige Planung, um das ISM im Rahmen eines kontinuierlichen Verbesserungsprozesses weiterzuentwickeln. Unabhängig von der derzeitigen Ukrainekrise unterliegt die Verbesserung des ISM hierbei der ständigen Anpassung auf die sich ändernde Bedrohungslage. Zusätzlich besteht ein geeigneter Austausch mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie mit dem Landesamt für Sicherheit in der Informationstechnik Bayern (LSI) zur Steigerung der Informationssicherheit. Bezüglich der aktuellen Lage wurden beispielsweise bei der Prüfung des Einsatzes von Software aus Drittländern die Empfehlungen des BSI bzw. LSI berücksichtigt.

Die konkrete, operative Umsetzung der Erkennung und Abwehr von Cyberangriffen erfolgt durch das in Entwicklung befindliche Cyber Security Center (CSC), das bei it@M angesiedelt ist. In diesem Rahmen vollzieht das CSC kontinuierliche Analysen der aktuellen, konkreten Bedrohungslage und verbessert die technologischen Detektionsmechanismen entsprechend.

Auch in diesem operativen Tätigkeitsfeld bestehen Beziehungen zu anderen Sicherheitsbehörden auf Bundes- bzw. Landesebene. Im Kontext des Ukrainekriegs, der im Antrag referenziert wird, wurden beispielsweise Listen mit spezifischen technischen Angriffs-

mustern (Indicators of Compromise, IoC) durch das BSI bzw. LSI übermittelt, die in lokale Überwachungssysteme der LHM eingespeist wurden.

Zusammenfassend lässt sich festhalten, dass sowohl Prüfung wie auch Optimierung standardmäßig in den regulären Betriebsprozessen im ISM der LHM verankert sind. Dies umfasst sowohl planerische wie auch operative Aspekte im Rahmen der Detektion von Cyberangriffen sowie potentieller Reaktionen darauf.

3. Entwicklungen im Informationssicherheitsmanagement der LHM

Um die unterschiedlichen Bedrohungslagen für die Informationssicherheit angemessen adressieren zu können, ist eine kontinuierliche Entwicklung im ISM der LHM notwendig. Vor diesem Hintergrund wurden mit Beschlussfassung des Stadtrats im Dezember 2021 (Sitzungsvorlage Nr. 20-26 / V 03022) die folgenden strategischen Entwicklungsschwerpunkte im ISM festgelegt.

- Sichere Authentisierung und digitale Prozesse
- Risikomanagement IT-Sicherheit
- IT-Sicherheitsarchitektur und Offensive Security
- Security Orchestration Automation and Response (SOAR)
- Endpoint Protection
- ISM Governance
- Cloud Security Management

Die hierbei aufgezeigten Handlungsfelder sind nicht spezifisch für die besondere Bedrohungslage durch den Krieg in der Ukraine, sondern ermöglichen die notwendige Steigerung der generellen Informationssicherheits-Resilienz der LHM.

Mit Beginn der Umsetzung entsprechender Maßnahmen in diesem Jahr werden somit wichtige Elemente im Informationssicherheitsmanagement entwickelt, um die LHM in die Lage zu versetzen, auf dynamische Entwicklungen im Cyberraum, wie zum Beispiel durch den Krieg in der Ukraine, angemessen reagieren zu können.

4. Rückmeldungen im Kontext kritischer Infrastrukturen der LHM

Die Fragestellungen des Antrags wurden insbesondere auch an die Betreiber*innen kritischer Infrastrukturen im Stadtkonzern gerichtet. Im Folgenden sind die entsprechenden Darstellungen der SWM, des Baureferats sowie der MSE und des AWM aufgeführt.

Stadtwerke München GmbH

Die SWM/MVG nehmen das Thema Informationssicherheit als Betreiberin kritischer Infrastrukturen (KRITIS) sehr erst. Hierfür setzen wir seit vielen Jahren einerseits auf ein Informationssicherheitsmanagementsystem (ISMS) in dem wir u. a. kontinuierlich die relevanten Risiken, die sich durch interne oder externe Einflüsse ergeben, systematisch erfassen und minimieren.

Andererseits orientieren wir bzgl. Bau und Betrieb der IT-Anteile unserer Betriebsanlagen natürlich an einschlägigen Normen z. B. bezogen auf die verwendeten Komponenten sowie den IT-Architekturen, in denen diese eingesetzt werden.

Abgerundet wird dies durch Systeme, die Angriffe automatisiert erkennen und eine geeignete Reaktion ermöglichen, so wie es zwischenzeitlich für KRITIS-Betreiber auch vom

Gesetzgeber gefordert wird. Mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) stehen wir dazu natürlich im kontinuierlichen Austausch.

Baureferat

Bei Bau-T3 Straßenbeleuchtung und Verkehrsleittechnik werden informationstechnische Anlagen der Verkehrsleittechnik, die aufgrund ihrer Anwendung/Funktion und Ausprägung einer kritischen Infrastruktur im Sinne des IT-Sicherheitsgesetzes zugeordnet sind, in einem sogenannten „Verkehrsleittechniknetzwerk“ betrieben.

Das Verkehrsleittechniknetzwerk ist autark und besitzt keine direkte Verbindung in das Internet. Somit ist es gegen Cyberattacken von außerhalb geschützt. Zum internen und externen Datenaustausch besitzt das Netzwerk einen Netzübergang in das IT-Netzwerk der Landeshauptstadt München. Die Sicherung dieses Netzübergangs erfolgt durch den städtischen IT-Dienstleister it@M.

Gemäß Kritisverordnung des BSI ist Bau-T3 verpflichtet, im zweijährigen Turnus für das Verkehrsleittechniknetzwerk ein externes Sicherheitsaudit durchführen zu lassen. Die bisher durchgeführten Audits (2019 und 2021) ergaben keine Sicherheitsmängel und wurden erfolgreich bestanden.

Münchner Stadtentwässerung

Die Münchner Stadtentwässerung betreibt die beiden Münchner Großklärwerke und das zugehörige Kanalnetz. Zur Steuerung und Überwachung der Ableitung und Reinigung des Abwassers sind in den Klärwerken Gut Großlappen und Gut Marienhof zentrale Leitwarten im 24h Betrieb etabliert. Die Klärwerke, das Kanalnetz und die zugehörigen zentralen Leitwarten sind beim BSI als kritische Infrastruktur registriert und unterliegen somit einem zweijährigen Prüfzyklus. Das Ergebnis der Prüfung ist dem BSI zu übermitteln und soll nachweisen, dass alle organisatorischen und technischen Maßnahmen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ergriffen wurden.

Die Münchner Stadtentwässerung wurde in 2019 und 2021 bereits erfolgreich geprüft. Die nächste Prüfung ist für Februar 2023 terminiert.

Aufgrund der zyklisch wiederkehrenden Prüfungen ist die Münchner Stadtentwässerung dazu verpflichtet, alle Maßnahmen zu ergreifen, um mögliche Risiken, wie z. B. Cyberattacken auf die kritische Infrastruktur zu vermeiden. Zur Umsetzung und Unterstützung wird den Betreibern kritischer Infrastrukturen vom BSI und dem CAZ (Cyber-Allianz-Zentrum Bayern) Informationen bzgl. der aktuellen Bedrohungslagen per Mail mitgeteilt. Hierzu werden z. B. tgl. Tageslageberichte versandt, die auf mögliche Gefährdungen hindeuten. Diese werden ausgewertet und bei Bedarf Maßnahmen ergriffen, um diese Gefährdungen auszuschließen, oder zu minimieren.

Aus technischer Sicht sind die vorgenannten Bereiche der kritischen Infrastruktur in einem vom Verwaltungsnetz der Landeshauptstadt München getrennten, autarken Netzwerk angesiedelt. Das Netzwerk der kritischen Infrastruktur wird durch eine demilitarisierte Zone (gestaffelte Firewalls) geschützt. In dieser Zone sind Systeme zur Angriffserkennung und Schwachstellenanalyse situiert.

Diese Absicherung und Vorgehensweise ist nicht den möglichen Cyberattacken aus Russland geschuldet, sondern stellt den Standard für kritische Infrastrukturen dar.

Entsprechend der stadtweiten Vorgaben nutzt die MSE für die IT-Anwendungen, die außerhalb des Prozessleittechnik-Netzes betrieben werden, die städtische Infrastruktur des

IT-Verwaltungsnetzes mit den zentral betriebenen IT-Services der LHM. Aufbauend auf dem städtischen ISM strebt die MSE hier im Rahmen eines gemeinsamen Projektes eine weitere Erhöhung des Sicherheitsniveaus an.

Abfallwirtschaftsbetrieb München

Der Abfallwirtschaftsbetrieb München betreibt seine Cyberabwehr zusammen mit dem etabliertem ISM des IT-Referat der Stadt München.

Das ISM bildet ein Rahmenwerk von IT-sicherheitsrelevanten Prozessen beziehungsweise Maßnahmen um IT-Infrastrukturen, Dienste und digital verarbeiteten Informationen zu schützen. Wichtige Aspekte der Maßnahmen sind die Netzwerksicherheit (Virenschutz, Firewall, Security Operation Center) und die Sensibilisierung der Mitarbeiter auf die Informationssicherheit.

Der AWM führt zusätzlich eine jährliche TÜV-Süd-Prüfung seiner Anlagen, der Organisation und der personelle Ausstattung, des Versicherungsschutzes und der Sachkunde seiner Mitarbeiter*innen durch.

Seit der Sektor Entsorgung 2021 durch das IT-Sicherheitsgesetz 2.0 als kritische Infrastruktur definiert worden ist, verstärkt der AWM seine Cyberabwehr mit der Umsetzung von weiteren Maßnahmen, wie einem Business Continuity Management (BCM) und einem IT-Notfallmanagement System, sowie mit Technologie zur Angriffserkennung, um auf Vorfälle schnell reagieren zu können.

5. Beteiligungen / Stellungnahmen der Referate

Die Beschlussvorlage wurde mit dem Baureferat, der MSE, dem RAW, dem AWM und dem Gesamtpersonalrat abgestimmt.

Anhörung des Bezirksausschusses

In dieser Beratungsangelegenheit ist die Anhörung des Bezirksausschusses nicht vorgesehen (vgl. Anlage 1 der BA-Satzung).

Korreferentin und Verwaltungsbeiräte

Die Korreferentin des IT-Referats, Frau Stadträtin Sabine Bär, der zuständige Verwaltungsbeirat von RIT-I, Herr Stadtrat Lars Mentrup, und die Verwaltungsbeirätin von it@M, Frau Stadträtin Judith Greif, haben einen Abdruck der Sitzungsvorlage erhalten.

II. Antrag der Referentin

1. Der Stadtrat nimmt den Vortrag der Referentin zur Cybersicherheit der IT der LHM, der SWM sowie der weiteren Betreiber*innen kritischer Infrastrukturen zur Kenntnis.
2. Mit diesem Beschluss wird der Stadtratsantrag Nr. 20-26 / A 02439 „Schutzschild gegen Cyberattacken erweitern“ von der CSU vom 24.02.2022 geschäftsordnungsmäßig erledigt.
3. Der Beschluss unterliegt nicht der Beschlussvollzugskontrolle.

III. Beschluss

nach Antrag.

Der Stadtrat der Landeshauptstadt München

Der / Die Vorsitzende — Die Referentin

Ober-/Bürgermeister/-in
ea. Stadtrat / ea. Stadträtin

Dr. Laura Dornheim
Berufsm. Stadträtin

IV. Abdruck von I. mit III.

über die Stadtratsprotokolle

an das Direktorium - Dokumentationsstelle
an die Stadtkämmerei
an das Revisionsamt

z. K.

V. Wv. - RIT-Beschlusswesen