Landeshauptstadt
München
IT-Referat

Landeshauptstadt München, Referat für Informations- und Telekommunikationstechnik, 80335 München

Dr. Laura Dornheim
Berufsmäßige Stadträtin

I. CSU-FW-Fraktion

Rathaus

Datum:
12.12.2022

Können die IT-Systeme der LHM lahmgelegt werden und besteht ein ausreichender Schutz?

Schriftliche Anfrage gemäß § 68 GeschO
Anfrage Nr. 20-26 / F 00545 von Herrn StR Rudolf Schabl, Herrn StR Hans-Peter Mehling vom 21.09.2022, eingegangen am 21.09.2022

Sehr geehrter Herr Stadtrat Schabl,
sehr geehrter Herr Stadtrat Mehling,

in Ihrer Anfrage haben Sie folgenden Sachverhalt vorausgeschickt:

Cyberangriffe auf Informationstechnologie-Systeme u. a. auf Kommunen und Firmen nehmen signifikant zu. Dies geschieht auf verschiedene Art, wie beispielsweise durch gefälschte E-Mails oder eingeschleuste Virensoftware.

Zu den von Ihnen gestellten Fragen kann ich Ihnen Folgendes mitteilen:

Frage 1:
Hat die Landeshauptstadt München einen ausreichenden finanziellen Schutz durch eine Cyberversicherung, die diese Angriffe auf die IT-Systeme entstehenden Schäden entsprechend abgedeckt?

Agnes-Pockels-Bogen 21
80992 München
Telefon: 089 233 – 767777

Antwort:
Die Landeshauptstadt München verfügt über keine Cyberversicherung und es bestehen aktuell auch keine diesbezüglichen Planungen. Aus Sicht des Informationssicherheitsmanagements der LHM hierzu nachfolgende Begründung.

Cyberversicherung werden durch Versicherungsunternehmen in verschiedenen Leistungsstufen angeboten. In der Regel sind sie so gelagert, dass sie Eigen- und zum Teil auch Drittschäden abdecken, die durch Cyberkriminalität entstehen. Gerade für Organisationen (im Vergleich zu Privatpersonen) handelt es sich hierbei jedoch um kein standardisiertes Versicherungsprodukt, so dass sich angebotene Schadensfallleistungen sowie die entsprechenden Tarife zum Teil erheblich unterscheiden. Insbesondere für große Organisationen wie die LHM gilt hierbei, dass sowohl Leistungsstufen wie auch Tarife erst nach eingehenden Prüfungen durch Versicherungsunternehmen angeboten werden.

In diesem Zusammenhang besteht häufig ein direkter Zusammenhang zwischen zu erfüllenden Mindestanforderungen im Bereich der Informationssicherheit einer Organisation und der Möglichkeit, überhaupt eine Versicherung abschließen zu können. Versicherungsanbieter prüfen im Vorfeld somit, ob ausreichende Standards bei möglichen Kunden*innen etabliert sind, bevor ein entsprechendes Angebot (Tarif, Bausteine) ausgesprochen wird. Solche Prüfungen sind bei Organisationen unserer Größenordnung sehr zeit- und kapazitätsintensiv und je nach Versicherungsanbieter an unterschiedlichen Normen ausgerichtet. Sie müssten somit anbieterspezifisch und damit mehrmals in unterschiedlicher Ausprägung durchlaufen werden.

Ein weiterer Aspekt in der Betrachtung ist natürlich der Schadensfall und die damit einhergehende Diskussion, wann er eintritt und wann die Versicherung auch leistet. Cyberversicherungen sind normalerweise als Vermögensschadenversicherung ausgebracht und schließen Schäden durch terroristische oder kriegerische Akte in der Regel aus. Die aktuelle geopolitische Lage mit dem Krieg in der Ukraine zeigt jedoch, dass ein solcher Ausschluss in der aktuellen Zeit, gerade was die Gefährdungslage im Cyberraum angeht, für Versicherungsnehmer als nachteilig zu werten ist.

Zusammenfassend lässt sich festhalten, dass für die LHM hohe Aufwände im Rahmen der Anforderungsprüfungen (bzw. im Nachgang zur Erfüllung der Anforderungen) sowie für eine Organisation dieser Größenordnung entsprechend hohe jährliche Tarifkosten zu erwarten wären. Diese sind gepaart mit einer aus Sicht des Versicherungsnehmers nicht unerheblichen Unsicherheit, ob im Schadensfall auch tatsächlich eine zufriedenstellende Regulierung stattfinden kann. Diese Position wird gestützt durch Erkenntnisse, die aus einer internen Befassung mit dem Themengebiet in 2019 hervorgeht. Das Ergebnis war damals wie heute, dass eine Cyberversicherung, nach Abwägung aller Vor- und Nachteile sowie von Kosten und Nutzen, zum aktuellen Zeitpunkt nicht zielführend für die LHM ist. Sollten sich Änderungen an dieser grundlegenden Situation ergeben, wird das Thema erneut im Rahmen des Informationssicherheitsmanagements geprüft.

Vor diesem Hintergrund wurde die Frage nach Cyberversicherungen auch auf Ebene des bayerischen Städtetags (Arbeitskreis IuK) diskutiert. Eine informelle Abfrage zum Einsatz von Cyberversicherungen zeigte, dass vor allem im Bereich von größeren Städten eine solche Versicherung, ebenso wie bei der Landeshauptstadt München, nicht zum Einsatz kommt.

Frage 2:
Werden die Arbeitnehmerinnen und Arbeitnehmer der LHM entsprechend sensibilisiert durch zielgerichtete Schulungen?

Antwort:
Im Hinblick auf die Sensibilisierung von Mitarbeitenden der LHM bzgl. Cyberrisiken sind zwei Bereiche zu unterscheiden.

Zum einen der Bereich der IT-Nutzenden, die als Anwender*innen die IT-Services der LHM im Rahmen ihres Dienstgeschäfts verwenden. Diese Zielgruppe wird durch regelmäßige Beiträge und praktische Verhaltenshinweise im Intranet der LHM für Themen der Informationssicherheit (nicht nur bzgl. Cyberrisiken) informiert und sensibilisiert. Dedizierte Schulungen in diesem Bereich finden nicht statt, da sie auf Grund der Zielgruppengröße (> 25.000) weder wirtschaftlich noch fachlich zielführend sind.

Der zweite Bereich umfasst sogenannte IT-Schaffende, somit die Mitarbeitenden, die die IT-Infrastrukturen und -Services der LHM verantworten, betreiben und entwickeln. In diesem Bereich werden fachspezifische Schulungen und auch Weiterbildungen durchgeführt, jedoch nicht großflächig sondern bedarfsorientiert.

Für beide Bereiche gleichermaßen stehen in jedem Referat und jedem Eigenbetrieb dedizierte Informationssicherheitsbeauftragte zur Verfügung, die als Ansprechpartner*in fungieren und auch bei konkreten Sicherheitsereignissen entsprechende Sensibilisierungen durchführen.

Frage 3:
Wie wird die IT derzeit vor Cyberangriffen geschützt?

Antwort:
Die Landeshauptstadt München verfügt über ein etabliertes Informationssicherheitsmanagement (ISM), das über die Informationssicherheitsleitlinie in der Organisation verankert ist.

Über das ISM werden alle relevanten Tätigkeiten und Maßnahmen zur Prävention, Detektion und Reaktion im Hinblick auf Cyberangriffe geplant, gesteuert und weiterentwickelt. Der Verantwortungsbereich des ISM umfasst dabei sowohl die Referate und Eigenbetriebe der LHM wie auch it@M als zentralen IT-Dienstleister für die Stadt München. Die Wirkungsbereiche des ISM beziehen sich dabei auf technologische, organisatorische, prozessuale und regulatorische Aspekte der Informationssicherheit bei der LHM.

Im Hinblick auf die Weiterentwicklung des ISM, und damit auch auf die Weiterentwicklung der Schutzmaßnahmen vor Cyberangriffen, sei auf die Beschlussfassung des Stadtrats Ende 2021 (Sitzungsvorlage Nr. 20-26 / V 03022: „Für ein sicheres digitales München – Ausbau des Informationssicherheitsmanagements der LHM“) verwiesen, in der konkrete Handlungsfelder zur Fragestellung ausgewiesen sind. Weiterhin wurden diesbezügliche Informationen auch im Stadtratsbeschluss „Schutzschild gegen Cyberattacken erweitern“ (Sitzungsvorlage Nr. 20-26 / V 07397) dargestellt.

Frage 4:
Wie viele Cyberangriffe wurden bislang ermittelt und wie wird dagegen vorgegangen?

Antwort:
Der Begriff des „Cyberangriffs“ ist sowohl im alltäglichen wie auch im fachspezifischen Gebrauch nicht unbedingt trennscharf definiert und kann je nach Interpretation ein weites Feld umspannen.

Würde zum Beispiel jeder Scanversuch über unsere Infrastrukturen, immerhin fester Bestandteil jeder Cyber Kill Chain, als Angriffsversuch gewertet werden, so wären die entsprechenden Zahlen unseriös hoch. Gleiches gilt im Übrigen auch für eingehende SPAM- bzw. Schadmails. Würde jede dieser Mails als Angriff gewertet werden, so wäre die LHM im Durchschnitt pro Monat ca. 4 Mio. Angriffen ausgesetzt – denn dies ist die ungefähre Anzahl der externen E-Mails, die an den eingehenden Mailsystemen pro Monat geblockt werden.

Es wird somit deutlich, dass eine exakte numerische Antwort zu dieser Frage wenig informationellen Mehrwert bieten kann. Um trotzdem eine gewisse Indikation zu geben, kann festgehalten werden, dass durch die Informationssicherheitsorganisation der LHM in der Regel über 500 sicherheitsrelevante Vorgänge pro Jahr aktiv im Rahmen einer Security Event- und Incident-Response behandelt werden.

Im Hinblick auf die Reaktionsweise auf Cyberangriffe als zweiter Teil der Fragestellung sei auf die Antwort zu Frage 3 und die dortigen Verweise auf frühere Stadtratsbefassungen zum Thema verwiesen.

Frage 5:
Welche Schäden finanzieller und sachlicher Art wurden bereits verursacht?

Antwort:
Durch Cyberangriffe wurden bisher keine größeren Schäden bei der Landeshaupt München verursacht. Die finanziell wie auch sachlich negativen Effekte, die sich in der Vergangenheit im Rahmen einer Security Event- und Incident-Response ergeben haben, lagen alle in einem Bereich, der über bestehende Kapazitäten im Rahmen des allgemeinen IT-Betriebs abgebildet werden konnten.

In Bezug auf die titelgebende Leitfrage der vorliegenden Stadtratsanfrage lässt sich zusammenfassend festhalten, dass Schäden durch Cyberangriffe sicherlich eintreten können, da es keine 100 %ige Informationssicherheit geben kann. Daher arbeitet das Informationssicherheitsmanagement der LHM im IT-Referat und bei it@M stetig daran, die entsprechend notwendigen Fähigkeiten zur Cyberabwehr in unserer Organisation zu etablieren und kontinuierlich an die sich ändernde Gefährdungslage im Cyberraum anzupassen.

Mit freundlichen Grüßen

gez.
Dr. Laura Dornheim
IT-Referentin