Landeshauptstadt
München
IT-Referat

Landeshauptstadt München, IT-Referat
Marienplatz 8, 80331 München

Dr. Laura Dornheim
Berufsmäßige Stadträtin

An die Fraktion ÖDP/München-Liste

Im Rathaus

Webex-Skandal bei der Bundeswehr:
Welche Konsequenzen zieht die Landeshauptstadt München?

Schriftliche Anfrage gemäß § 68 GeschO
Anfrage Nr. 20-26 / F 00887 von der Fraktion ÖDP/München-Liste
vom 04.03.2024, eingegangen am 04.03.2024

Sehr geehrte Damen und Herren,

in Ihrer Anfrage haben Sie folgenden Sachverhalt vorausgeschickt:

„Die deutsche Bundeswehr ist Opfer eines Abhörskandals geworden. Das Gespräch, das von Russland abgehört wurde, wurde offenbar die amerikanische Kommunikationsplattform Webex geführt. Diese schien bisher recht sicher zu sein, da sie eine Ende-zu-Ende-Verschlüsselung ermöglicht. Diese Verschlüsselung muss jedoch manuell aktiviert werden und funktioniert nicht, wenn Teilnehmer sich per Telefon einwählen.
Die Landeshauptstadt München setzt seit dem Ausbruch der Corona-Pandemie bei ihren Videokonferenzen auf die Plattform Webex. Auch auf kommunaler Ebene werden Themen besprochen, die vertraulich sind und bleiben sollen."

Im Vorfeld der nachfolgenden Ausführungen zu Ihren Fragestellungen darf ich folgenden Sachverhalt zum Thema Webex vorausschicken.

Das Bundesministerium der Verteidigung (BMVg) sieht es im Rahmen der laufenden Untersuchungen als erwiesen an, dass ein individueller Anwendungsfehler dazu führte, dass vertrauliche Gesprächsinhalte aus der von Ihnen angesprochenen Webex-Konferenz an die Öffentlichkeit gelangten. Laut BMVg waren zu keiner Zeit unautorisierte Dritte in die Konferenz eingewählt. Allem Anschein nach erfolgte die Kompromittierung der Gesprächsinhalte damit unabhängig von der Kommunikationsplattform Webex, da sich nicht alle Teilnehmer*innen an die Vorgaben des BMVg zur sicheren Konferenzeinwahl gehalten hatten. Ein konkreter Anlass, die

grundsätzlichen Sicherheitseigenschaften von Webex in Frage zu stellen, ist demzufolge aus Sicht des Informationssicherheitsmanagements der Landeshauptstadt München nicht gegeben.

Zu den im Einzelnen gestellten Fragen kann ich Ihnen Folgendes mitteilen:

Frage 1:
Wird die Landeshauptstadt München auch künftig Webex für Video- und Telefonkonferenzen nutzen?

Antwort:
Der aktuell durch die LHM abgeschlossene Lizensierungsrahmen für Webex läuft bis Anfang 2026.

Die Bewertung einer Lizensierungsverlängerung oder aber einer alternativen Neubeschaffung einer anderen Softwarelösung erfolgt im Rahmen der IT-Prozesse der LHM standardmäßig in Form eines IT-Projekts. In diesem Rahmen erfolgt dann auch die Evaluierung weiterer Anbieter und Lösungen.

Im Hinblick auf Webex wird dieses Thema bereits in einem aktuell laufenden IT-Projekt adressiert, das zum Ziel hat, die Funktionsbereiche Telefonie, Videokonferenzen und Teamkollaboration zu integrieren. In diesem Rahmen wird somit auch eine Entscheidungsgrundlage bzgl. des weiteren Einsatzes von Webex bei der LHM erarbeitet.

Um entsprechenden Projektergebnissen nicht vorzugreifen, können zum aktuellen Zeitpunkt daher noch keine Aussagen dazu getroffen werden, ob Webex auch über 2026 hinaus bei der LHM zum Einsatz kommen wird.

Frage 2:
Welche Alternativen zu Webex wurden in Betracht gezogen und wie schneiden sie in Bezug auf Daten- und Zugriffs-Sicherheit ab?

Antwort:
Im Rahmen des Einführungsprojekts von Cisco Webex bei der LHM wurden standardmäßig verschiedene Produkte im Rahmen einer Marktsondierung evaluiert. Zu den betrachteten Produkten gehörten sowohl proprietäre Produkte von Avaya, Cisco, Microsoft, MiTel und Unify als auch Open Source Lösungen wie z. B. Matrix, Bria, BigBlueButton, Mattermost, Rocket.Chat, Jitsi, Wire oder Wickr.

Im Rahmen dieser Evaluationen zur Produktauswahl stehen primär fachliche und technische Aspekte im Vordergrund. Geprüft wird z. B. der Funktionsumfang einer Lösung, ihre Integrationsmöglichkeiten in die IT-Infrastruktur der LHM oder auch Skalierungs- und Performanceaspekte. Neben diesen zentralen Themen werden auch weitere Faktoren beleuchtet, wie etwa die Wirtschaftlichkeit oder auch Aspekte der Informationssicherheit und des Datenschutzes.

Der Ablauf der Sondierungen ist gestuft. Im Rahmen von Vorauswahlen werden aus Sicht der Informationssicherheit nur grundlegende Aspekte abgeprüft, in weiteren Runden nimmt die Prüftiefe zu. Eine vollständige Prüfung im Rahmen der Informationssicherheitsprozesse und -vorgaben der LHM erfolgt nur für Lösungen, die auf Grundlage der fachlichen Evaluierungsergebnisse für eine Beschaffung vorgesehen sind.

Im Rahmen des Vorauswahlprozesses wurde somit eine grobe Überprüfung von Informationssicherheitsanforderungen für alle potentiell geeigneten Lösungen durchgeführt. Ein vollständige Detailprüfung aller bei der LHM relevanten Anforderungen im Rahmen des Risikomanagements Informationssicherheit erfolgte nur für Webex.

Vor diesem Hintergrund sind die Prüfergebnisse der Alternativlösungen aus Informationssicherheitssicht nicht mit den Ergebnissen zu Webex vergleichbar, da unterschiedliche Prüftiefen vorliegen. Grundsätzlich kann hierzu jedoch festgehalten werden, dass die analysierten Lösungen im Hinblick auf die Informationssicherheit grundsätzlich zwar ähnlich gelagerte Schutzkonzepte und Sicherheitsfunktionen aufwiesen, ihre konkrete Ausgestaltung und vor allem auch die resultierenden Integrationsmöglichkeiten in die IT-Sicherheitsarchitektur der LHM stark differierten.

Für Webex gilt in diesem Zusammenhang, dass es neben den etablierten Zertifizierungen im Bereich der Informationssicherheit mit dem C5-Testat des Bundesamts für Sicherheit in der Informationstechnik (BSI) über die notwendigen Security-Standards im Bereich Cloud Computing verfügt. Weiterhin besteht für die LHM im Rahmen der Lizensierung die Möglichkeit, Codereviews von Webex bei der Herstellerfirma Cisco durchzuführen.

Frage 3:
Welche Maßnahmen ergreift die Landeshauptstadt München, um vertrauliche Daten zu schützen (z. B. Schulungen für Mitarbeiter, Sicherheitsrichtlinien oder regelmäßige Audits)?

Antwort:
Der Schutz von Informationen, die von der Stadtverwaltung verarbeitet werden, fällt in den Aufgabenbereich des Informationssicherheitsmanagements der Landeshauptstadt München (ISM).

Das ISM ist über die Informationssicherheitsleitlinie der LHM verbindlich in der Stadtverwaltung verankert. Organisatorisch ist es unter der Leitung des Informationssicherheitsbeauftragten der LHM im IT-Referat sowie bei it@M angesiedelt. Der Verantwortungsbereich des ISM umfasst die Referate und Eigenbetriebe der Stadtverwaltung sowie im besonderen it@M als zentralen IT-Serviceprovider der LHM.

Das Aufgabenspektrum im ISM orientiert sich an nationalen und internationalen Standards und umfasst alle relevanten Aktivitäten und Maßnahmen zur Prävention, Detektion und Reaktion im Hinblick auf Cyberangriffe und andere Bedrohungen für die Informationssicherheit der Stadtverwaltung.

Die Wirkungsbereiche des ISM beziehen sich dabei auf technologische, organisatorische, prozessuale und regulatorische Aspekte der Informationssicherheit. Beispielhaft können in diesem Zusammenhang im ISM etablierte Aufgabenbereiche benannt werden, wie etwa Risikomanagement (Prävention), Monitoring and Detection (Detektion), Vulnerability Management (Prävention, Detektion) oder Event- und Incident Management (Reaktion). Im Hinblick auf die Absicherung der städtischen IT-Infrastruktur ist weiterhin der Bereich des IT-Security Architecture Managements von zentraler Bedeutung, über den die Konzeption und der Aufbau sicherheitsrelevanter Technologien bei it@M zentral vorangetrieben wird.

Mit Blick auf die in der Fragestellung exemplarisch angeführten Tätigkeiten kann abschließend festgehalten werden, dass diese ebenfalls im Aufgabenbereich des ISM verankert sind und im Rahmen der Entwicklung des Informationssicherheitsniveaus der LHM bedarfsgerecht ausgeprägt werden.

Frage 4:
Wie wird sichergestellt, dass nur autorisierte Benutzer an Webex-Meetings teilnehmen können und dass keine unbefugten Zugriffe erfolgen?

Antwort:
Termine zu Webex-Meetings können in der Webex-Anwendung selbst sowie innerhalb von Microsoft Outlook als Standard-E-Mail-Client bei der LHM vereinbart werden. Auf diese Weise werden Termine erstellt, zu denen Einladungen mit entsprechenden Zugriffsinformationen (z. B. Meeting-Link, Telefonnummer und PIN für Telefoneinwahl) lediglich an die eingeladenen Personen versandt werden.

Für einen konkreten Termin können durch die Terminersteller*innen weitere Sicherheitsfunktionen aktiviert werden. Dies sind z. B. eine automatische Sperrfunktion nach Meetingstart, eine Lobbyfunktion oder auch die Unterbindung der telefonischen Einwahl.
Über die Sperrfunktion kann ein ungesteuerter Zutritt Dritter zu Terminen nach einer konfigurierbaren Zeitspanne unterbunden werden. Die Lobbyfunktion ermöglicht es, dass Personen, die nicht zum Meeting eingeladen wurden, jedoch Kenntnis des Meeting-Links erhalten haben, zunächst in einer Lobby warten und durch die Terminersteller*innen aktiv zugelassen werden müssen.

Diese Sicherheitsfunktionen sind organisationsweit nicht standardmäßig aktiviert, da die Anforderungen an Webex-Meetings im gesamtstädtischen Nutzungskontext unterschiedlich ausgeprägt sind und je nach Anwendungsfall variieren. Nutzende können die entsprechenden Sicherheitseinstellungen jedoch in ihren persönlichen Profilen hinterlegen und somit für die von ihnen erstellten Webex-Meetings standardmäßig aktivieren.

Im Hinblick auf die im Rahmen von Webex-Meetings übertragenen Informationen greifen zudem weitere Sicherheitsfunktionen. In der organisationsweit definierten Standardeinstellung werden z. B. alle Chatverläufe oder geteilten Dateien verschlüsselt übertragen und sind auch durch den Hersteller Cisco nicht zugreifbar. Sogenannte Echtzeitdaten hingegen, wie z. B. Audio- und Videostreams, werden zwar verschlüsselt übertragen, sind jedoch durch Cisco einsehbar. Diese Standardeinstellung ist aktiviert, um Mehrwertfunktionen, wie z. B. die automatische Untertitelung von Meetings, nutzen zu können.

Auch diesbezüglich haben Nutzende Einfluss auf die jeweilige Einstellung und können durch die Auswahl anderer Meetingtypen eine vollständige „Ende-zu-Ende-Verschlüsselung“ aktivieren. Hierbei ist jedoch zu berücksichtigen, dass bei Aktivierung der Ende-zu-Ende-Verschlüsselung Funktionseinbußen in Kauf zu nehmen sind. Eine telefonische Meeting-Einwahl, eine Meeting-Teilnahme per Webbrowser oder auch eine automatische Untertitelung werden in diesem Fall nicht mehr unterstützt

Neben den im Hinblick auf die Fragestellung dargestellten technischen Lösungen obliegt es schlussendlich auch den Nutzenden selbst, analog zu anderen Kommunikationsmitteln, dafür Sorge zu tragen, dass nur befugte Personen Kenntnis von Meetinginhalten erlangen können. Im Fall von Webex bedeutet dies beispielsweise, aktiv darauf zu achten, dass sich nur autorisierte Personen in einer Konferenz befinden.

Frage 5:
Gibt es spezielle Sicherheitsrichtlinien oder Best Practices, die von der Landeshauptstadt München für die Nutzung von Webex und anderen Programmen festgelegt wurden?

Antwort:
Webex ist als Standardplattform für Videokonferenzen und Teamkollaboration durch das Informationssicherheitsmanagement der LHM freigegeben. Diese Freigabe erfolgte im Rahmen der üblichen Vorgehensweisen im Risikomanagement Informationssicherheit, in dessen Rahmen relevante Sicherheitsanforderungen an Webex definiert und umgesetzt wurden. Eine Webex-spezifische Sicherheitsrichtlinie ist gemäß den Standards im Informationssicherheitsmanagement der LHM daher nicht erforderlich.

Mit Blick auf den stadtweiten Einführungsprozess von Webex kann festgehalten werden, dass umfangreiche Aktivitäten in den Bereichen Kommunikation und Information von Nutzenden stattgefunden haben. So wurden z. B. vielfältige Postings im stadtweiten Intranet der LHM publiziert, Hilfeartikel, FAQs und Einführungsfilme zu Webex veröffentlicht sowie auch weiterführende Informationen zur Nutzung von Webex bereitgestellt.

In diesem Zusammenhang wird durch it@M ein sogenannter Arbeitsraum im Intranet der LHM aktiv betrieben, in dem zusätzlich zu den genannten Inhalten auch Kontakt- und Austauschmöglichkeiten bei Fragen oder Problemen angeboten werden. Dieser Arbeitsraum wird aktuell von über 5.000 Mitarbeitenden der LHM im Intranet abonniert.

Mit freundlichen Grüßen

gez.
Dr. Laura Dornheim
IT-Referentin