SEESTADT BREMERHAVEN
Der Magistrat

Dezernat I
Magistratskanzlei
Herr Jacob, Tel. 3332
Bremerhaven, 18.11.2024

Vorlage Nr. I/ 275/2024 Anzahl Anlagen: 7
für den Magistrat

Grundsätze zur Gestaltung der Informationssicherheit beim Magistrat
hier: Rahmenrichtlinie zur Informationssicherheit

A Problem

Der Magistrat hat in seiner Sitzung am 21.12.2016 (Vorlage-Nr. I/ 345/2016) im Rahmen der Grundsätze zur Gestaltung der Informationssicherheit beim Magistrat die Dienstanweisung „Richtlinie zur Informationssicherheit für das Magistratsnetz“ beschlossen. Die Richtlinie orientierte sich an allgemeinen Sicherheitsstandards wie dem IT-Grundschutzkonzept des Bundesamts für Sicherheit in der Informationstechnik (BSI) bzw. der Norm ISO 27001. Soweit sich für einzelne Themenbereiche die Notwendigkeit ergab, wurden weitergehende Regelungen ergänzend beschlossen.

Die Verwaltungsabläufe in der Stadtverwaltung werden mittlerweile weitgehend durch den Einsatz von Informationstechnik (IT) unterstützt und sind somit hiervon abhängig. Durch diese verstärkte Abhängigkeit hat sich das Risiko der Beeinträchtigung von Informationsinfrastrukturen und deren IT-Infrastruktur-Komponenten durch vorsätzliche Angriffe von innen und außen, durch fahrlässiges Handeln, Unkenntnis oder technisches Versagen sowohl qualitativ als auch quantitativ deutlich erhöht. Mangelnde Informationssicherheit kann zu Störungen bei der Aufgabenerfüllung führen, die die Leistungsfähigkeit der Stadtverwaltung mindern und im Extremfall die Geschäftsprozesse zum Erliegen bringen.

Ein unzureichendes Sicherheitsniveau oder Sicherheitslücken können über die Netzinfrastrukturen wesentliche IT-Verfahren negativ beeinträchtigen. Es ist davon auszugehen, dass die gestellten Sicherheitsanforderungen im Bereich der Informations- und IT-Sicherheit künftig weiter steigen werden. Demzufolge ist die IT-Sicherheit die Voraussetzung für eine erfolgreiche Digitalisierung.

Vor diesem Hintergrund ist die Sicherstellung der Informationssicherheit für den Magistrat der Stadt Bremerhaven eine der zentralen Aufgaben, in deren Rahmen ein angemessenes Sicherheitsniveau in den Geschäftsprozessen organisiert werden muss. Aus diesem Grund hat sich der Betrieb für Informationstechnologie 2023 dazu entschlossen, eine Zertifizierung nach (C)ISIS12 und IT-Grundschutz-Profil Basis Absicherung Kommunalverwaltung anzustreben, die sämtliche Aspekte der Informationssicherheit berücksichtigt. Im Rahmen der ersten Auditierung wurden Regelungslücken aufgezeigt, die nunmehr zu schließen sind.

B Lösung

Der Betrieb für Informationstechnologie und die Magistratskanzlei haben die Hinweise der Zertifizierungsstelle aufgenommen und in einer Arbeitsgruppe wichtige Handlungsfelder identifiziert. Der Identifikation folgte ein Abgleich zu bislang gültigen Regelungen mit dem Ziel, die Resilienz der Informations- und Kommunikationstechnik der Stadtverwaltung zu erhöhen und sie dabei den aktuellen und zukünftigen Anforderungen anzupassen.

In einer neu entwickelten Übersicht der verschiedenen Handlungsfelder wurde deutlich, dass es zunächst eines klar definierten Rahmens bedarf, dem sich untergeordneten Einzelregelungen anzupassen haben.

Die den Hinweisen des Bundesamtes für Sicherheit in der Informationstechnik folgende neue Rahmenrichtlinie zur Informationssicherheit (Anlage 1) des Magistrats beschreibt allgemein, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der Stadtverwaltung hergestellt werden soll. Sie beinhaltet die angestrebten Informationssicherheitsziele sowie die verfolgte Sicherheitsstrategie und beschreibt die Sicherheitsorganisation.

In der IT-Sicherheitsrichtlinie, der Richtlinie Internetnutzung, der Richtlinie zum Umgang mit Passwörtern, der Richtlinie für die Nutzung der elektronischen Post (E-Mail-Richtlinie), der Richtlinie zum Umgang mit Software und der Richtlinie zum sicheren Umgang mit Daten und IT-Systemen (Anlagen 2-7) wird in einer einheitlichen Struktur Grundsätzliches zum jeweiligen Handlungsfeld beschrieben. Im Weiteren werden themenbezogene Anforderungen, rechtliche Aspekte, Zuständigkeiten und Verfahrensanweisungen beschrieben. Zudem wird sowohl in der Rahmenrichtlinie, als auch in allen untergeordneten Richtlinien eine regelmäßige Fortschreibung und Revision vorgeschrieben. Die im Rahmen der bereits erfolgreich durchgeführten Reauditierung vorgelegten Entwürfe der Richtlinien wurden seitens der zertifizierenden Stelle als positiv bewertet.

C Alternativen
Der Verzicht auf den Erlass der Rahmenrichtlinie zur Informationssicherheit und der untergeordneten Richtlinien ist in Kenntnis der Abhängigkeit von den Informations- und Kommunikationstechniken und unter Berücksichtigung der allgemeinen Bedrohungslage keine vertretbare Alternative.

D Auswirkungen des Beschlussvorschlags
Der Beschlussvorschlag hat keine unmittelbaren finanziellen Auswirkungen. Im Rahmen der Bereitstellung der insgesamt notwendigen Haushaltsmittel im Kapitel 6024 – Informations- und Kommunikationstechniken – sind auch weiterhin die Aufwendungen zur Gewährleistung der Sicherheit der Informations- und Kommunikationstechniken zu berücksichtigen. Der Beschlussvorschlag hat keine unmittelbaren personalwirtschaftlichen Auswirkungen.

Zudem hat der Beschlussvorschlag keine klimaschutzzielrelevanten Auswirkungen und für eine Genderrelevanz gibt es keine Anhaltspunkte. Ferner sind weder ausländische Mitbürgerinnen und Mitbürger noch die besonderen Belange der Menschen mit Behinderung und des Sports betroffen. Eine örtliche Betroffenheit eines Stadtteils ist ebenfalls nicht erkennbar.

E Beteiligung / Abstimmung
Die Vorlage ist mit dem Betrieb für Informationstechnologie abgestimmt.

Die Mitbestimmungsgremien (Schwerbehindertenvertretung, Sprecherin der Frauen- und Gleichstellungsbeauftragen sowie der Gesamtpersonalrat) waren an der Erstellung der Dienstanweisung beteiligt und haben den vorliegenden Fassungen zugestimmt.

F Öffentlichkeitsarbeit / Veröffentlichung nach dem BremIFG
Keine. Eine Veröffentlichung gemäß des Bremischen Informationsfreiheitsgesetzes wird gewährleistet.

G Beschlussvorschlag
Der Magistrat beschließt die als Anlagen beigefügte Rahmenrichtlinie zur Informationssicherheit sowie die daraus resultierenden IT-Sicherheitsrichtlinie, die Richtlinie Internetnutzung, die Richtlinie zum Umgang mit Passwörtern, die Richtlinie für die Nutzung der elektronischen Post (E-Mail-Richtlinie), die Richtlinie zum Umgang mit Software sowie der Richtlinie zum

sicheren Umgang mit Daten und IT-Systemen. Die Regelungen werden zum 01.01.2025 wirksam.

Die Magistratskanzlei wird gebeten, Hinweise auf eine einheitliche E-Mail-Signatur im Intranet bereitzustellen und im Rahmen einer Mitteilung für die Verwaltung zu veröffentlichen. Der Betrieb für Informationstechnologie wird gebeten, technische Voraussetzungen für eine zentral einheitliche E-Mail-Signatur zu prüfen und in Abstimmung mit der Magistratskanzlei einzuführen.

Die mit der IT-Sicherheit beauftragten Personen werden gebeten, in regelmäßigen Informationsveranstaltungen und in angemessener Weise die Beschäftigten des Magistrats für das Thema IT-Sicherheit zu sensibilisieren.

Die Entsorgungsbetriebe Bremerhaven (Anstalt des öffentlichen Rechts) wird gebeten, die Anwendbarkeit der Rahmenrichtlinie sowie aller untergeordneten Richtlinien durch ihre zuständigen Organe erklären zu lassen.

Die Bereiche, die nicht zum Verwaltungsnetz des Magistrats gehören (pädagogisches Netz der Schulen, das Netz der Ortspolizeibehörde, das Schulungsnetz der Volkshochschule sowie das Netz der Integrierten Regionalleitstelle Unterweser-Elbe) werden aufgefordert, spätestens im zweiten Quartal 2025 eigene Richtlinien mit gleichermaßen beschriebenen Schutzzielen zu erlassen.

Grantz
Oberbürgermeister

Anlage 1: Rahmenrichtlinie zur Informationssicherheit
Anlage 2: IT-Sicherheitsrichtlinie
Anlage 3: Richtlinie Internetnutzung
Anlage 4: Richtlinie zum Umgang mit Passwörtern
Anlage 5: Richtlinie für die Nutzung der elektronischen Post (E-Mail-Richtlinie)
Anlage 6: Richtlinie zum Umgang mit Software
Anlage 7: Richtlinie zum sicheren Umgang mit Daten und IT-Systemen