STADT NAUMBURG (Saale)

Vorlagen-Nr.:	137/24
Vorlagentyp:	Entscheidung
Einreicher:	Oberbürgermeister
Prüfung:	☒ Barrierefreiheit
	☒ Gleichstellung
	☒ Finanzen
Eingang am:	15.10.2024
Version	1

Teilnahme:	intern:	Herr Ehrhardt
	extern:	

TOP:	14

☒ öffentlich	☐ nicht öffentlich

Beratungsfolge:

Gremium	Datum	TOP	Liste	Art*	Ergebnis
Hauptausschuss	04.12.2024	7.	A	V	einstimmige Annahme
Gemeinderat	11.12.2024	14.	A	V	

Art* I=Information V=Vorberatung A=Anhörung B=Beschlussfassung

Betreff:
Verabschiedung einer Informationssicherheitsrichtlinie zur Erfüllung der Anforderungen der EU-Richtlinie NIS-2

Beschlussvorschlag:
1. Der Gemeinderat verabschiedet die Leitlinie zur Informationssicherheit der Stadtverwaltung Naumburg (Saale).

2. Die Verwaltung wird beauftragt, die notwendigen Schritte zur Umsetzung der Richtlinie einzuleiten.

3. Die dafür notwendigen Finanzmittel werden zur Verfügung gestellt und sind im Haushalt einzustellen.

Finanzielle Auswirkung:

☐ nein ☒ ja, in folg. Höhe: 50.000 Euro ggfs. Sonderbedarf pro Jahr

Deckungsvorschlag: ☒ Haushaltsplan : 25 TEuro über 5431200, 25 TEuro über
☐ über-/außerplanmäßig

Buchungsstelle:

Begründung:

I. Ausgangslage

Die NIS-2-Richtlinie (Netz-und Informationssicherheit) ist eine EU-weite Vorschrift, die darauf abzielt, die Cybersicherheit in Europa zu stärken. Sie wurde 2022 beschlossen und ist eine überarbeitete Version der ursprünglichen-Richtlinie von 2016. Das Ziel ist es, durch strengere Sicherheitsvorschriften und einheitliche Standards die Resilienz der kritischen Infrastrukturen zu verbessern und auf seine Bedrohung koordinierter zu reagieren. Kernpunkte der NIS-2-Richtlinie sind:

1. erweiterter Geltungsbereich
Die Richtlinie betrifft mehr Sektoren als die ursprüngliche Fassung. Neben kritischen Infrastrukturen wie Energie, Verkehr und Gesundheitswesen werden nun auch kommunale Bereiche wie Abfallwirtschaft, öffentliche Verwaltung und digitale Dienstleistung einbezogen.

2. Verstärkte Sicherheitsanforderungen
Unternehmen und Kommunen müssen striktere Maßnahmen für Netz-und Informationssicherheit einhalten, was die IT-Sicherheit, Risikobewertung und-management sowie den Schutz sensibler Daten betrifft.

3. Meldepflichten
Organisationen müssen Cybervorfälle innerhalb kurzer Fristen an die zuständigen Behörden melden. Diese Meldepflichten helfen, Bedrohung schneller zu erkennen und auf europäischer Ebene besser koordiniert darauf zu reagieren.

4. Sanktionsmechanismen
Die NIS-2-Richtlinie sieht höhere Strafen bei Nichteinhaltung vor. Die soll Unternehmen zur Einhaltung der Vorschriften anhalten und den Anreiz für Investitionen in Cybersicherheit erhöhen.

II. Konsequenzen für die Kommunen

Durch die NIS-2-Richtlinie werden Kommunen erstmals spezifisch in den Geltungsbereich der Richtlinie mit einbezogen. Sie gehören nun zur kritischen Infrastruktur, die besonders zu schützen ist. Die wichtigsten Anforderungen sind:

1.Sicherheitsmaßnahmen und Risikomanagement
Kommunen müssen Maßnahmen zur Netz und Informationssicherheit implementieren. Dazu gehören technische und organisatorische Maßnahmen, um die IT-Infrastruktur abzusichern, wie zum Beispiel regelmäßige Sicherheitsupdates, Zugangsverwaltung, Firewalls und Verschlüsselung. Ein umfassendes Risikomanagementsystem muss entwickelt werden, das potentielle Cyberrisiken regelmäßig evaluiert und präventive Maßnahmen bereitstellt.

2. Meldung von Sicherheitsvorfällen
Kommunen müssen ihre Mitarbeiter regelmäßig zur Cybersicherheit schulen und sensibilisieren. Dazu gehören Schulungen zur Erkennung von Phishing-Angriffen, sicherem Umgang mit Passwörtern und anderen grundlegenden Sicherheitsmaßnahmen.

3. Notfallpläne
Die Entwicklung von Notfallplänen zur schnellen Reaktion auf Cyberangriffe wird verpflichtend. Hierbei soll definiert werden, wie die Kommunen im Ernstfall die wichtigsten Dienstleistungen aufrechterhalten kann. Regelmäßige Übungen und Simulationen werden gefordert, um die Krisenreaktionsfähigkeit sicherzustellen bestehende Pläne auf Effektivität zu prüfen.

4. Zusammenarbeit und Informationsaustausch
Kommunen sollen sich mit anderen Behörden und relevanten Organisation vernetzen, um Information über Bedrohung und Best-Practice auszutauschen.

5. Berufung eines Sicherheitsbeauftragten
Viele Kommunen müssen einen eigenen Sicherheitsbeauftragten benennen, der für die Implementierung und Überwachung der Cybersicherheitsstrategien verantwortlich ist. Dieser ist auch Ansprechpartner für externe Behörden und für die Einhaltung der NIS-2-Vorgaben.

III. Konkreter Regelungsumfang der Sicherheitsrichtlinie

Die Stadtverwaltung beabsichtigt deshalb die beigefügte Richtlinie zur Informationssicherheit zu verabschieden. Diese legt einen verbindlichen Rahmen fest, der definiert, wie die Stadtverwaltung ihre sensiblen Daten, IT Systeme und Informationsflüsse schützt. Sie beschreibt klare Regeln, Maßnahmen und Verantwortlichkeiten für den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationssystemen, um Risiken wie Datenverlust, Cyberangriffe oder Insider-Bedrohungen zu minimieren.

Die Stadtverwaltung wird dazu ein Managementsystem für Informationssicherheit (ISMS), das dem Regelwerk „IT Grundschutz“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI) genügen soll, einrichten. Ein Informationsmanagementsystem ist eine Aufstellung von Verfahren und Regeln, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren und fortlaufend zu verbessern.

Mit dieser Richtlinie bekennt sich die Stadtverwaltung zur Informationssicherheit. Auf dieser Grundlage sollen dann detaillierte Regelungen für die einzelnen Teilbereiche per Dienstanweisungen, Dienstvereinbarungen, Konzepte, Pläne und Regelung für die einzelnen Bereiche verabschiedet werden.

Die Umsetzung der NIS-2-Richtlinie erfordert von der Stadtverwaltung erhebliche Investitionen in die IT-Sicherheit sowie die Einrichtung von Prozessen zur Risikoerkennung und-bewältigung.

Die Informationssicherheitsrichtlinie soll regelmäßig überprüft und an neue Bedrohungen oder Änderungen angepasst werden. Sie bildet die Grundlage für ein effektives Informationssicherheitsmanagement und kann durch detaillierte Verfahrensanweisungen oder Sicherheitsstandards ergänzt werden.

Für die Informationssicherheit hat die Stadtverwwaltung bereits 2019 eine Cyberversicherung abgeschlossen (Kosten 10.056,00 Euro/Jahr). Die Stadt wird diese weiter aufrechterhalten. Ferner wurde die sehr renommierte Fa. Robin Data GmbH aus Merseburg gebunden, die die Stadtverwaltung in Sachen Datenschutz und Informationssicherheit berät (Kosten 833,00 Euro/Monat zzgl. Sonderaufwand. Die Kosten hierfür sind im Haushalt eingeplant.

Es könnten aber Kosten für technische Investitionen entstehen, die noch nicht absehbar sind. Hierfür werden 50.000 € eingeplant (jeweils 25.000 € über 54312000 und 78310100).

Armin Müller
Oberbürgermeister