Bezirksamt Reinickendorf von Berlin
Abteilung Finanzen, Personal und Bürgerdienste
Serviceeinheit Finanzen

Bezirksamt Reinickendorf von Berlin, Eichborndamm 215, 13437 Berlin

BERLIN

3033

Geschäftszeichen (bitte angeben)
Haush L (k)

Herr Seidel
Tel. +49 30 90294-2292
Fax +49 30 90294-2225
Alexander.Seidel
@reinickendorf.berlin.de
Elektronische Zugangseröffnung:
post@reinickendorf.berlin.de
Eichborndamm 215, 13437 Berlin
Raum 334 A

15.Juli.2026

An den
Vorsitzenden des Hauptausschusses

über
die Präsidentin des Abgeordnetenhauses
von Berlin

über
Senatskanzlei - G Sen -

Investitionen der Bezirke aus dem Kapitel 2980 - Infrastrukturinvestitionen aus dem Sondervermögen des Bundes - Zustimmung zur Aufnahme folgender Maßnahme
Titel 88342 - Sonstige Investitionen aus dem Sondervermögen des Bundes für den Bezirk Reinickendorf
Hier: Security Operations Center - SOC (Ukt. 357)

Hinweis zum haushaltstechnischen Vollzug: Die Senatsverwaltung für Finanzen wird den Sammeltitel 2980/88342 neu einrichten. Da die Ausgaben durch Einnahmen aus dem Sondervermögen des Bundes vollständig gegenfinanziert sind, handelt es sich nicht um außerplanmäßige Ausgaben (vgl. § 37 Abs. 6 LHO).

Rote Nummer: 2400

Vorgang: 94. Sitzung des Hauptausschusses vom 10.12.2025

Geschätzte Gesamtausgaben: 600.000 €

Vorbemerkung:

Gem. Ziffer 1 des Rundschreibens der Senatsverwaltung für Finanzen vom 19.05.2026 über Infrastrukturinvestitionen aus dem Sondervermögen des Bundes (Kapitel 2980) stehen die bezirklichen Projekte unter Zustimmungsvorbehalt des Hauptausschusses. Vor der Inangriffnahme von Planungen ist daher die Zustimmung des Hauptausschusses zu den beabsichtigen Projekten einzuholen.

Beschlussvorschlag:

Der Hauptausschuss stimmt zu, die folgende Maßnahme aus dem Sondervermögen des Bundes in Kapitel 2980, Sammeltitel 88342 realisieren zu können. Im Übrigen wird der nachfolgende Bericht zur Kenntnis genommen.

Hierzu wird berichtet:

1. Kurzbeschreibung der Maßnahme

Einführung eines Managed Security Operations Center (SOC) zur kontinuierlichen Überwachung der kommunalen IT-Infrastruktur durch einen externen spezialisierten Dienstleister. Das SOC überwacht sicherheitsrelevante Ereignisse rund um die Uhr, erkennt potenzielle Cyberangriffe, Datenabflüsse und sonstige Anomalien frühzeitig und unterstützt bei der Einleitung geeigneter Gegenmaßnahmen. Ergänzend werden regelmäßige Angriffssimulationen (Red-Teaming) durchgeführt, um technische, organisatorische und personelle Schwachstellen zu identifizieren und die Wirksamkeit bestehender Sicherheitsmaßnahmen zu überprüfen. Ziel der Maßnahme ist die nachhaltige Erhöhung der Informationssicherheit und Resilienz der Verwaltung, die Sicherstellung der Verfügbarkeit kritischer IT-Systeme und Fachverfahren sowie die Unterstützung bei der Einhaltung gesetzlicher und regulatorischer Anforderungen, insbesondere aus DSGVO, BSI-Grundschutz und NIS2.

2. Begründung der Notwendigkeit gem. § 6 LHO und der Wirtschaftlichkeit gem. § 7 LHO

Die fortschreitende Digitalisierung der Verwaltungsleistungen und die zunehmende Vernetzung der IT-Systeme führen zu einer erheblich gestiegenen Gefährdungslage durch Cyberangriffe. Zur Sicherstellung der Informationssicherheit ist die Einführung einer zentralen technischen Sicherheitsplattform erforderlich, welche sicherheitsrelevante Ereignisse automatisiert sammelt, analysiert und bewertet. Mit der Maßnahme wird eine bislang nicht vorhandene technische Infrastruktur geschaffen, die eine zentrale Sicherheitsüberwachung der gesamten bezirklichen IT-Landschaft ermöglicht. Die Plattform unterstützt die frühzeitige Erkennung von Angriffen, die Analyse komplexer Sicherheitsvorfälle sowie die schnelle Einleitung geeigneter Gegenmaßnahmen. Dadurch werden kritische Fachverfahren, digitale Verwaltungsleistungen

und personenbezogene Daten nachhaltig geschützt. Die Einführung einer vergleichbaren Infrastruktur in Eigenregie würde erhebliche Investitionen in Hard- und Software sowie den dauerhaften Aufbau hochqualifizierter Spezialistenteams erfordern. Für den wirtschaftlichen Betrieb einer eigenen Security-Operations-Umgebung wären umfangreiche personelle Ressourcen sowie ein dauerhaftes Lizenz-, Wartungs- und Betriebsmanagement notwendig. Durch die Beschaffung einer integrierten Sicherheitsplattform einschließlich der erforderlichen Einführungs-, Integrations- und Betriebsleistungen können etablierte Marktstandards genutzt werden. Dies vermeidet hohe Investitions- und Personalkosten, reduziert Projektrisiken und gewährleistet gleichzeitig den Aufbau einer modernen Sicherheitsinfrastruktur nach aktuellem Stand der Technik. Die Maßnahme entspricht damit den Grundsätzen der Wirtschaftlichkeit und Sparsamkeit gemäß § 7 LHO und stellt einen wesentlichen Baustein zur nachhaltigen Stärkung der digitalen Resilienz der Berliner Verwaltung dar.

3. Finanzierung der Maßnahmen

Die Finanzierung erfolgt vollständig im Rahmen des Sondervermögens Infrastruktur des Bundes (Kapitel 2980). Die Gesamtkosten in Höhe von 600.000 € sind entsprechend der Maßnahmenplanung im Haushaltsjahr 2027 geplant.
Die Mittel dienen der Einführung einer zentralen Security-Operations-Plattform einschließlich der erforderlichen Softwarekomponenten, Sicherheitsanalysewerkzeuge, Sensorik, technischen Integration, Implementierung und Inbetriebnahme sowie der projektbezogenen Unterstützungsleistungen. Darüber hinaus umfasst die Finanzierung die für den Betrieb der Plattform erforderlichen technischen Unterstützungsleistungen einschließlich Sicherheitsmonitoring, Incident-Analyse und kontinuierlicher Optimierung der Sicherheitskonfiguration. Diese Leistungen dienen der Sicherstellung der Funktionsfähigkeit und Wirksamkeit der eingeführten Sicherheitsinfrastruktur. Nach Abschluss der Maßnahme steht dem Bezirksamt eine moderne technische Plattform zur zentralen Sicherheitsüberwachung der IT-Infrastruktur zur Verfügung, welche die Grundlage für eine dauerhaft erhöhte Cyberresilienz bildet.
Etwaige spätere Betriebs-, Wartungs-, Lizenz-, Support- oder Anpassungskosten wären nach Abschluss aus zukünftigen Haushaltsmitteln des Bezirks zu tragen.

4. Nachteile für Berlin bei Maßnahmenverzicht

Ohne die Einführung der Security-Operations-Plattform kann keine zentrale technische Sicherheitsinfrastruktur zur automatisierten Erkennung und Bewertung von Cyberbedrohungen aufgebaut werden. Die bestehenden IT-Systeme könnten sicherheitsrelevante Ereignisse weiterhin nur eingeschränkt oder zeitverzögert erkennen. Cyberangriffe, Schadsoftware oder Datenabflüsse würden mit höherer Wahrscheinlichkeit zu erheblichen Betriebsunterbrechungen, Datenverlusten oder Beeinträchtigungen kritischer Verwaltungsverfahren führen. Zudem könnten wesentliche Anforderungen aus dem IT-Grundschutz des BSI, der NIS2-Richtlinie sowie

weiterer regulatorischer Vorgaben nur mit erheblichem Mehraufwand erfüllt werden. Die Widerstandsfähigkeit der bezirklichen IT gegenüber aktuellen und zukünftigen Bedrohungslagen würde dauerhaft hinter dem erforderlichen Sicherheitsniveau zurückbleiben.

Mit freundlichen Grüßen

Emine Demirbüken-Wegner
Bezirksbürgermeisterin