1. Hintergrund und Zielsetzung

Im Rahmen der Befassung mit IT-Projekten und Vorhaben der Digitalisierung sowie der Absicherung kritischer IT-Infrastrukturen beabsichtigt die Polizei Brandenburg (nachfolgend Auftraggeber) die Beauftragung externer Unterstützungsleistungen im Bereich Informationssicherheit.
Ziel ist die fachliche und operative Unterstützung bei der Planung, Umsetzung und Überwachung von Sicherheitsmaßnahmen in IT-Vorhaben nach Maßgabe des BSI-Grundschutzes (Edition 2024) sowie weiterer einschlägiger Sicherheitsrichtlinien des Landes Brandenburg.
Die zu erbringende Leistung dient der Stärkung der Cyber-Resilienz, insbesondere im Hinblick auf genereller Prävention, sowie Erkennung, Analyse und Reaktion auf hochentwickelte Cyber-Angriffe (Advanced Persistent Threats – APT).

2. Leistungsgegenstand

Der Auftragnehmer erbringt Dienstleistungen im Bereich Informationssicherheit mit Schwerpunkt auf folgenden Tätigkeitsfeldern:

- Durchführung von Risikoanalysen, Schutzbedarfsfeststellungen und Sicherheitsbewertungen nach BSI-Grundschutz (Edition 2024)
- Erstellung und Fortschreibung von Sicherheitskonzepten, Notfallkonzepten und Sicherheitsdokumentationen unter Nutzung des ISMS-Tools verinice
- Begleitung und Qualitätssicherung von Sicherheitsmaßnahmen in IT-Entwicklungs-, Migrations- und Betriebsprojekten
- Beratung und operative Unterstützung bei der Umsetzung von Sicherheitsanforderungen in IT-Projekten des Auftraggebers
- Analyse und Reaktion auf sicherheitsrelevante Vorfälle (Incident Response) mit Schwerpunkt auf APT-Angriffsszenarien
- Unterstützung bei Audits, Penetrationstests und Schwachstellenanalysen
- Beratung zu organisatorischen und technischen Maßnahmen im Sinne von § 8a BSIG und relevanten BSI-Empfehlungen

Der Einsatz erfolgt in enger Abstimmung mit dem internen Informationssicherheitspersonal, Projektleitungen und weiteren Verantwortlichen des Auftraggebers.

3. Kontingent

Für die zu erbringende Unterstützungsleistung wird von einem Kontingent in Höhe von 600 Personentagen (PT) verteilt über 3 Jahre ausgegangen. Davon wird eine Abnahme von insgesamt 150 PT garantiert. Ein Mindestabnahmemenge von 50 PT jährlich ist sicherzustellen.

4. Qualifikationsanforderungen

Zur Erbringung der Leistungen wird ein nachweislich qualifizierter Dienstleister gesucht, der folgende Mindestanforderungen erfüllt:

- Nachgewiesene Erfahrung in der Befassung mit Informationssicherheit für öffentliche Auftraggeber
  - hierzu Vorlage von drei Referenzen innerhalb der zurückliegenden fünf Jahre bei Auftraggebern der öffentlichen Verwaltung (Bund/Land) in Deutschland
- Nachgewiesene Kenntnisse und praktische Erfahrung mit
  - BSI-Grundschutz (Edition 2024), IT-Grundschutz++ (ab 2026), sowie Community und Final Drafts
  - IT-Notfallmanagement nach BSI-Standard 200-4
  - ISO 22301 Business Continuity Management (BCM)
  - ISO/IEC 27001-zertifizierten Managementsystemen
  - Landes- und bundesweiten Sicherheitsvorgaben (z. B. IT-Sicherheitsrichtlinien des Landes Brandenburg, BSI-Maßnahmenkataloge)
- Zertifizierung der einzusetzenden Mitarbeiter/-innen gemäß BSI-Grundschutz
  - Für jedes Projekt / IT-Vorhaben beim Auftraggeber ist mindestens ein zertifizierter IT-Grundschutz-Berater erforderlich
- Nachweis von nachhaltiger und tiefgreifender Erfahrung in
  - Überprüfung von IT-Sicherheitsprodukten bzw. Hard- und Software (Nachweis mittels akkreditierter CC / ITSEC Prüfstellen des BSI)
  - Durchführung von Revision und Penetrationstests von IT-Systemen (gemäß „Liste zertifizierter IT-Sicherheitsdienstleister in den Geltungsbereichen IS-Revision und IS-Penetrationstests“ des BSI)
  - Vorfallbearbeitung (gem. „Liste zertifizierter IT-Sicherheitsdienstleister in dem Geltungsbereich Vorfallbearbeitung“ des BSI)
- Nachweis von nachhaltiger Absicherung zum Datenschutz (mittels Zertifikat gem. ISO 27701)
- Zertifizierung oder Qualifizierung gemäß BSI-Anforderung für APT-Response-Dienstleister (gemäß BSI C5/APT Response Service Provider – Mindeststandards und Nachweisverfahren)
- Fähigkeit zur schnellen Einsatzbereitschaft und APT-Response-Koordination im Falle sicherheitsrelevanter Vorfälle, mit flexibel skalierbarer Kapazität

- Nachweis der Mitwirkung in IT- und Cybersicherheitsspezifischen Informationsverbünden (mittels Mitgliedschaft und akkreditiertem „trusted introducer status“ im CERT Verbund

5. Rahmenbedingungen

- Einsatzort: Polizei Brandenburg (virtuell und vor Ort in Einrichtungen des Auftraggebers)
- Leistungszeitraum: Nach Zuschlagserteilung, zunächst befristet auf 36 Monate mit Option auf Verlängerung
- Bewertung: Die Vergabeentscheidung erfolgt ausschließlich auf Grundlage der A-Kriterien (Eignungskriterien). Wirtschaftliche oder qualitative B-Kriterien sind nicht vorgesehen.
- Leistungsabruf: Im Bedarfsfall nach Anforderung einzelner IT-Vorhaben über Einzelabrufe oder definierte Arbeitspakete

6. Vertraulichkeit und Sicherheitsvorgaben

Der Dienstleister verpflichtet sich zur Einhaltung aller relevanten Sicherheitsbestimmungen der öffentlichen Verwaltung des Landes Brandenburg, speziell der für die Polizei Brandenburg geltenden Bestimmungen, einschließlich:

- Sicherheitsüberprüfung nach SÜG für eingesetztes Personal
- Vertraulichkeitsvereinbarungen gemäß § 2 BSIG
- Einhaltung der Verschlusssachenanweisung (VSA), soweit anwendbar

7. Erwartetes Ergebnis

Bereitstellung einer BSI-qualifizierten, reaktionsschnellen und fachlich versierten Informationssicherheitsunterstützung, die zur Erhöhung der Sicherheit und Resilienz von IT-Systemen der Polizei Brandenburg beiträgt. Die zu erbringende Dienstleistung entspricht sowohl präventiver Maßnahmen in aktuellen IT-Projekten und Vorhaben, die eine Grundlage für die Freigabe zur Einführung neuer IuK-Services darstellen, als auch analytischer Tätigkeiten zur Unterstützung bei der Identifikation von Auffälligkeiten in bestehenden IT-Systemen. Die erforderliche Dokumentation hat unter Vorgabe des Auftraggebers und mittels dessen ISMS Tool bzw. Vorlagen zu erfolgen.