Inhalt

1 INCIDENT RESPONSE DIENSTLEISTUNGEN 2

2 ZIELSTELLUNG 2

3 LEISTUNGSBESCHREIBUNG 2

3.1 RAHMENBEDINGUNGEN ZUR LEISTUNGSERBRINGUNG 3

3.1.1 Infrastrukturelle Abhängigkeiten 4

3.2 MITWIRKUNGSPFLICHTEN DES AUFTRAGGEBERS 4

3.3 SERVICE- UND REAKTIONSZEITEN 5

3.4 AUFTRAGSVOLUMEN UND ABRECHNUNG 5

4 ZUSÄTZLICHE VERTRAGLICHE RAHMENBEDINGUNGEN 5

4.1 VERTRAGSLAUFZEIT UND KÜNDIGUNG 5

4.2 INFORMATIONSPFLICHTEN 6

4.3 NUTZUNGSRECHTE UND VERSCHWIEGENHEIT 6

4.4 INFORMATIONSSICHERHEIT, DATENSCHUTZ UND FERNZUGRIFF 6

4.5 AUSFÜLLUNG DES BEIGEFÜGTEN EVB-IT-VERTRAGSENTWURF 7

5 NACHWEIS DER EIGNUNG DES AUFTRAGNEHMERS 7

6 PRÜFUNG UND BEWERTUNG DER ANGEBOTE 8

6.1 PRÜFUNG DER EIGNUNGS- UND MUSS-KRITERIEN (ANLAGE B 4 – FRAGENKATALOG) 8

6.2 ZUSCHLAGSKRITERIUM 8

1 Incident Response Dienstleistungen

Leistungsverzeichnis für den Erwerb von Unterstützungsleistungen durch einen professionellen Dienstleister im Falle eines IT-Sicherheitsvorfalls.

2 Zielstellung

Die IKT-Ost AöR beabsichtigt im Rahmen der Notfallvorsorge, einen Incident-Response-Dienstleister vertraglich zu binden. Dieser soll operative Unterstützung durch Soforthilfe zur Bewältigung von IT-Sicherheitsvorfällen bieten, indem er insbesondere Experten aus den Bereichen IT-Forensik, Incident Response und Krisenmanagement bereitstellt.

Der Leistungsumfang für Incident-Response-Dienstleistungen umfasst unter anderem:

- Telefonische Soforthilfe (Incident-Response-Hotline zur Lagebeurteilung)
- Remote- und Vor-Ort-Unterstützung / Vorfallbehandlung (Eindämmung, Aufklärung, Wiederanlauf und Wiederherstellung)
- Forensik (Sicherungen und Analysen)
- Unterstützung beim Krisenmanagement

Das Ziel dieses Vergabeverfahrens ist der Abschluss eines EVB-IT-Dienstleistungsvertrages zwischen der IKT-Ost AöR (Auftraggeber AG) und einem externen Partner (Auftragnehmer AN) über die bedarfsgerechte Erbringung von Incident-Response-Dienstleistungen.

Die Leistungserbringung soll am 01.01.2027 beginnen.

3 Leistungsbeschreibung

Vom Incident-Response-Dienstleister wird erwartet, folgende Leistungen gemäß den Bedürfnissen der IKT-Ost AöR und ihren Trägerverwaltungen zu erbringen:

1. Telefonische Soforthilfe (Incident-Response-Hotline)

- Rund um die Uhr erreichbare Hotline an 365 Tagen im Jahr für die Meldung und Bewertung von IT-Sicherheitsvorfällen.
- Sofortige Beurteilung der Lage durch qualifiziertes Personal zur Einleitung angemessener Maßnahmen.

2. Remote- und Vor-Ort-Unterstützung / Vorfallbehandlung

- Bereitstellung von Fachexperten zur Unterstützung bei der Eindämmung, Aufklärung, Bereinigung, dem Wiederanlauf und der Wiederherstellung nach einem Sicherheitsvorfall.
- Die Unterstützung kann abhängig von Art und Umfang des Sicherheitsvorfalls remote oder vor Ort erfolgen.
- Analyse der betroffenen Systeme und Netzwerke, um Ursachen und Umfang des Sicherheitsvorfalls zu ermitteln und geeignete Maßnahmen abzuleiten.

3. Forensik und Beweissicherung

- Durchführung forensischer Analysen zur Sicherung relevanter Daten und Beweismittel.
- Sammlung und Analyse relevanter Informationen, um Ursprung, Ursache und Umfang des Sicherheitsvorfalls zu ermitteln.
- Durchführung von Malware-Analyse, Host-Forensik und Netzwerkforensik entsprechend der jeweiligen Vorfalllage.

4. Unterstützung beim Krisenmanagement

- Beratung und Unterstützung des durch die IKT-Ost AöR eingesetzten Krisen- oder Koordinationsteams bei der Bewältigung eines IT-Sicherheitsvorfalls.
- Bereitstellung von Fachwissen zur Koordination erforderlicher technischer und organisatorischer Maßnahmen.
- Unterstützung bei erforderlichen Melde- und Informationsprozessen sowie bei der Abstimmung mit zuständigen Behörden, CERT-Stellen und weiteren Beteiligten, soweit dies durch die IKT-Ost AöR beauftragt wird.

5. Schadensbegrenzung und Wiederherstellung

- Eindämmung von Sicherheitsverletzungen, um den Schaden zu begrenzen und die weitere Ausbreitung des Vorfalls zu stoppen.
- Unterstützung bei Bereinigung, Wiederanlauf und Wiederherstellung betroffener Systeme, Daten und Dienste.
- Empfehlung geeigneter technischer und organisatorischer Maßnahmen zur Wiederherstellung eines sicheren Betriebszustandes.

6. Kommunikation und Koordination

- Unterstützung bei der Kommunikation mit internen und externen Beteiligten sowie bei der Koordination der erforderlichen Maßnahmen.
- Bereitstellung fachlicher Informationen und unterstützender Materialien für die interne Kommunikation während eines Sicherheitsvorfalls.

7. Nachbereitung und Berichterstattung

- Durchführung einer Nachbereitung des Sicherheitsvorfalls, um daraus Erkenntnisse zu gewinnen und Maßnahmen zur Verbesserung der Sicherheit zu identifizieren.
- Erstellung eines Abschlussberichts über den Sicherheitsvorfall, insbesondere mit Ursachenanalyse, wesentlichen Feststellungen, durchgeführten Maßnahmen und Empfehlungen für zukünftige Präventions- und Reaktionsmaßnahmen.

3.1 Rahmenbedingungen zur Leistungserbringung

Nach Zuschlagserteilung erfolgt eine operative Abstimmung zwischen Auftraggeber und Auftragnehmer. Dabei sind insbesondere Ansprechpartner, Melde- und Eskalationswege, Erreichbarkeiten, sichere Kommunikationswege sowie die für eine Vorfallbehandlung notwendigen organisatorischen und technischen Zugangswege abzustimmen.

3.1.1 Infrastrukturelle Abhängigkeiten

Die Landkreise Vorpommern-Greifswald und Mecklenburgische Seenplatte sowie die Vier-Tore-Stadt Neubrandenburg haben den Betrieb ihrer Informations- und Kommunikationstechnik auf die IKT-Ost AöR ausgelagert.

Die Incident-Response-Dienstleistungen beziehen sich daher auf PC-Arbeitsplätze, die im Verantwortungsbereich der IKT-Ost AöR liegen und schließen damit die Endgeräte in Schulen und Verwaltung ein.

Die IKT-Ost AöR nutzt dabei Leistungen der neu-itec GmbH als Infrastrukturdienstleister für IT-Infrastrukturleistungen, insbesondere für Rechenzentrumsbetrieb und Netzwerkleistungen. Für die von neu-itec GmbH verantworteten Infrastrukturanteile bestehen eigene Incident-Response-Strukturen bzw. vertraglich gebundene Incident-Response-Dienstleister.

Der Auftragnehmer erbringt die in diesem Leistungsverzeichnis beschriebenen Incident-Response-Dienstleistungen für die IKT-Ost AöR und ihre drei Trägerverwaltungen. Soweit ein IT-Sicherheitsvorfall mehrere Verantwortungsbereiche betrifft oder die Zuständigkeit zu Beginn der Vorfallbehandlung noch nicht eindeutig festgestellt werden kann, ist eine Zusammenarbeit und Abstimmung mit den durch die IKT-Ost AöR benannten Ansprechpartnern sowie den beteiligten Incident-Response-Dienstleistern erforderlich.

3.2 Mitwirkungspflichten des Auftraggebers

1. Bereitstellung von Informationen

Der Auftraggeber stellt dem Auftragnehmer im Rahmen der Vorfallbehandlung relevante Informationen über seine IT-Infrastruktur, seine Geschäftsprozesse und gegebenenfalls frühere Sicherheitsvorfälle zur Verfügung, soweit diese für die Analyse und Behandlung des jeweiligen Sicherheitsvorfalls erforderlich sind.

2. Gewährung von Zugang zur IT-Infrastruktur

Der Auftraggeber gewährt dem Auftragnehmer die für die Vorfallbehandlung erforderlichen Zugänge zu Systemen, Netzwerken, Daten und sonstigen relevanten Informationsquellen, soweit dies technisch, organisatorisch und rechtlich zulässig ist.

3. Kommunikation und Koordination

Der Auftraggeber stellt eine geeignete Kommunikationsstruktur sicher und benennt die für die Zusammenarbeit mit dem Auftragnehmer erforderlichen fachlichen und organisatorischen Ansprechpartner. Bei Bedarf wird ein Koordinator für die Vorfallbehandlung benannt.

4. Unterstützung bei der Umsetzung von Maßnahmen

Der Auftraggeber unterstützt den Auftragnehmer bei der Umsetzung der im Rahmen der Vorfallbehandlung abgestimmten Maßnahmen und stellt die hierfür erforderliche interne Koordination sicher.

Diese Mitwirkungspflichten dienen dazu, eine effektive und effiziente Vorfallbehandlung durch den Incident-Response-Dienstleister zu ermöglichen.

3.3 Service- und Reaktionszeiten

Die folgenden Service- und Reaktionszeiten sind durch den Auftragnehmer verbindlich einzuhalten. Die Reaktionszeiten gelten ab Eingang der Meldung über die vereinbarte Incident-Response-Hotline.

Leistung	Anforderung	Zeitvorgabe
Hotline	Erreichbarkeit	24/7/365
Erstreaktion	Bestätigung der Übernahme und Beginn der Bearbeitung	max. 30 Minuten
Erstbewertung	Qualifizierte erste Lageeinschätzung und Handlungsempfehlung	max. 4 Stunden
Vor-Ort-Unterstützung	Bereitstellung qualifizierten Personals am vereinbarten Einsatzort	max. 24 Stunden

3.4 Auftragsvolumen und Abrechnung

Die Vergütung setzt sich aus einer monatlichen Bereitstellungspauschale für die 24/7-Rufbereitschaft sowie der Vergütung tatsächlich abgerufener Incident-Response-Leistungen zusammen.

Für die Bedarfs- und Auftragswertplanung wurde mit einem unverbindlichen Planungswert von 15 Personentagen Incident-Response-Leistung pro Jahr gearbeitet.

Zur Herstung der preislichen Vergleichbarkeit im Preisblatt wird mit einem unverbindlichen, fiktiven Ansatz von jeweils 10 Personentagen pro Jahr für Remote- sowie für Vor-Ort-Leistungen gerechnet. Dieser fiktive Ansatz dient ausschließlich der kalkulatorischen Preisbewertung und begründet keine Verpflichtung des Auftraggebers zur Abnahme einer bestimmten Mindestmenge. Die tatsächliche Inanspruchnahme richtet sich nach Art, Anzahl und Umfang der auftretenden IT-Sicherheitsvorfälle.

Der Anteil der remote und vor Ort zu erbringenden Leistungen kann nicht im Voraus bestimmt werden und richtet sich nach der jeweiligen Vorfalllage. Remote- und Vor-Ort-Leistungen sind im Preisblatt getrennt auszuweisen.

Bei Vor-Ort-Leistungen sind sämtliche erforderlichen Reise-, Übernachtungs- und Nebenkosten in der angebotenen Preisposition zu berücksichtigen und werden nicht gesondert vergütet.

4 Zusätzliche vertragliche Rahmenbedingungen

Der Abschluss eines EVB-IT-Dienstleistungsvertrages ist vorgesehen und den Vergabeunterlagen beigefügt. Dieses Leistungsverzeichnis wird Bestandteil der vertraglichen Vereinbarungen. Daneben ist vom Bieter ein Auftragsverarbeitungsvertrag (AV-Vertrag) bei Angebotsabgabe beizufügen. Der Auftraggeber behält sich vor, diesen Entwurf vor Zuschlagserteilung datenschutzrechtlich zu prüfen. Erforderliche redaktionelle oder rechtliche Anpassungen werden im Rahmen der Angebotsaufklärung einvernehmlich zwischen Auftraggeber und Bieter abgestimmt und vor Zuschlagserteilung abgestimmt. Der Bieter verpflichtet sich, an einer finalen, beiderseits zustimmungsfähigen Fassung des Auftragsverarbeitungsvertrags (AVV) mitzuwirken und diesen mit Zuschlagserteilung einzugehen.

4.1 Vertragslaufzeit und Kündigung

Der Vertrag beginnt am 01.01.2027 und wird auf unbestimmte Zeit geschlossen.

Der Vertrag kann von beiden Vertragsparteien mit einer Frist von drei Monaten zum Monatsende ordentlich gekündigt werden, frühestens zum Ablauf der Mindestvertragsdauer von 12 Monaten, d.h. zum 31.12.2027.

Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

Die Führung in der aktuellen Liste der qualifizierten APT-Response-Dienstleister des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist während der gesamten Vertragslaufzeit aufrechtzuerhalten. Der Auftragnehmer informiert den Auftraggeber unverzüglich in Textform, wenn die Listung entfällt oder ruht oder ihm ein Verfahren zur Aussetzung oder Streichung der Listung bekannt wird.

Entfällt die Listung während der Vertragslaufzeit, stellt dies einen wichtigen Grund dar, der den Auftraggeber zur außerordentlichen Kündigung des Vertrages berechtigt. Der Auftraggeber kann dem Auftragnehmer zuvor eine angemessene Frist zur Wiederherstellung der Listung einräumen.

4.2 Informationspflichten

Die Informationspflichten umfassen, dass der Auftragnehmer und der Auftraggeber sich unverzüglich informieren, wenn die Erbringung der Leistungen aus zeitlichen, personellen oder technischen Gründen nicht im vereinbarten Zeitrahmen oder zu den vereinbarten Terminen möglich ist.

4.3 Nutzungsrechte und Verschwiegenheit

Die Nutzungs- und Verbreitungsrechte an den erbrachten Leistungen liegen ausschließlich beim Auftraggeber.

Der Auftragnehmer verpflichtet sich zur Verschwiegenheit und Geheimhaltung hinsichtlich der Leistungserbringung sowie der dabei gewonnenen Erkenntnisse, Daten, Informationen und Strukturen.

Nach Beendigung des Auftrages bzw. des Vertragsverhältnisses übergibt der Auftragnehmer alle überlassenen Unterlagen und Ergebnisse an den Auftraggeber und löscht lokale Kopien, soweit keine gesetzlichen oder vertraglichen Aufbewahrungspflichten entgegenstehen.

Der Auftraggeber behält sich vor, vom Auftragnehmer den Nachweis eines polizeilichen Führungszeugnisses für die an der Leistungserbringung beteiligten Personen zu verlangen. Dieser Nachweis ist vor der Leistungserbringung durch diese Personen zu erbringen. Der Auftragnehmer sichert zu, dass für das eingesetzte Personal ein Führungszeugnis ohne einschlägige Eintragungen vorliegt und auf Anforderung unverzüglich vorgelegt werden kann.

4.4 Informationssicherheit, Datenschutz und Fernzugriff

Der Auftragnehmer erhält im Rahmen der Leistungserbringung gegebenenfalls Zugriff auf vertrauliche technische Informationen, Protokolldaten, Systemkonfigurationen und personenbezogene Daten. Sämtliche Informationen sind vertraulich zu behandeln und ausschließlich zur Erfüllung des jeweiligen Auftrags zu verwenden.

- Fernzugriffe auf Systeme der IKT-Ost AöR dürfen nur nach vorheriger Freigabe durch die IKT-Ost AöR und über abgestimmte sichere Zugangsverfahren erfolgen.

- Für Fernzugriffe sind sichere Authentisierungsverfahren und nachvollziehbare Protokollierungen einzusetzen.
- Der Auftragnehmer stellt sicher, dass die für die Leistungserbringung eingesetzten Systeme und Werkzeuge angemessen abgesichert und aktuell gehalten werden.
- Soweit personenbezogene Daten im Auftrag verarbeitet werden, sind vor Beginn der entsprechenden Verarbeitung die erforderlichen Vereinbarungen gemäß Art. 28 DSGVO zu treffen.
- Unterauftragnehmer dürfen nur im Rahmen der vertraglich und vergaberechtlich vorgesehenen Regelungen eingesetzt werden.

4.5 Ausfüllung des beigefügten EVB-IT-Vertragsentwurf

Der den Vergabeunterlagen beiliegende Entwurf des EVB-IT Dienstleistungsvertrages ist vom Bieter im Rahmen seiner Angebotserstellung durchzusehen, in den nachfolgenden Kapiteln zu befüllen sowie dem Angebot ausgefüllt beizufügen:

- Ziffer 4.1.1 (Kategorien / Vergütungssätze): Befüllung der Tabelle zu den prozentualen Zuschlägen.
- Ziffer 6 (Ansprechpartner): Angabe der fachlichen und organisatorischen Ansprechpartner des Bieters / Auftragnehmers (Name, Kontaktdaten).
- Ziffer 13.3 (Teleservice): Angabe des vom Bieter eingesetzten Verfahrens bzw. der Remote-Zugangsverfahren.

5 Nachweis der Eignung des Auftragnehmers

Der Auftragnehmer weist die grundlegende fachliche Eignung des für die Leistungserbringung vorgesehenen Personals durch entsprechende Personenzertifikate – wobei das Vorhandensein von mindestens einem der nachfolgenden Zertifikate oder eines gleichwertigen Qualifikationsnachweises ausreicht - wie Cyber Security Incident Manager (ZSICM), Certified Incident Handler (ECIH), Vorfall-Experte (BSI), Lead Incident Manager (ISO) nach. Diese Nachweise belegen das grundlegende Fachwissen des eingesetzten Personals im Bereich Incident Response.

Der Auftragnehmer verfügt über Fähigkeiten in den Bereichen Malware-Analyse, Host-Forensik und Netzwerkforensik.

Darüber hinaus weist der Auftragnehmer die Kompetenz nach, im Falle eines IT-Sicherheitsvorfalls umfassende Unterstützungsleistungen vor Ort beim Auftraggeber und dessen Trägerverwaltungen zu erbringen. Hierzu verfügt der Auftragnehmer über eine mobil einsetzbare technische Ausstattung, um forensische Untersuchungen beim Auftraggeber vor Ort durchzuführen.

Der Auftragnehmer muss über ausreichende personelle Kapazitäten verfügen, um die vereinbarten Service- und Reaktionszeiten auch bei parallelen Kundenereignissen einhalten zu können.

Die Kommunikation zwischen Auftraggeber und Auftragnehmer erfolgt ausschließlich in deutscher Sprache. Dies gilt auch für wesentliche Dokumentationen und Berichte. Das für die Vorfallbehandlung eingesetzte Personal muss die deutsche Sprache fließend beherrschen.

Angesichts der besonderen Anforderungen bei gezielten und komplexen Cyberangriffen ist es zwingend erforderlich, dass der Auftragnehmer zum Zeitpunkt der Angebotsabgabe in der aktuellen Liste der qualifizierten APT-Response-Dienstleister des Bundesamtes für Sicherheit in der Informationstechnik (BSI) geführt wird.

6 Prüfung und Bewertung der Angebote

6.1 Prüfung der Eignungs- und Muss-Kriterien (Anlage B 4 – Fragenkatalog)

Zur strukturierten und vergleichbaren Überprüfung der fachlichen Eignung und der geforderten Mindestanforderungen dient der als „Anlage B 4 Fragenkatalog“ beigefügte Fragenkatalog, der durch den Bieter vollständig auszufüllen und einzureichen ist.

Sämtliche an „Anlage B 4 Fragenkatalog“ aufgeführten Kriterien sowie in diesem Leistungsverzeichnis definierten Vorgaben sind zwingende Muss-Anforderungen, die von jedem Bieter vollständig erfüllt werden müssen. Unabhängig von den Angaben in „Anlage B 4 Katalog“ bleiben alle Bestimmungen dieses Leistungsverzeichnisses in vollem Umfang verbindlich.

6.2 Zuschlagskriterium

Unter den Angeboten, welche die formalen Anforderungen sowie sämtliche geforderten Eignungs- und Muss-Kriterien erfüllen, erfolgt die Zuschlagswertung ausschließlich anhand des Preises.

Zuschlagskriterium: Preis 100 %

Der für die Zuschlagswertung maßgebliche Vergleichspreis setzt sich aus folgenden Preisbestandteilen zusammen:

- monatliche Bereitstellungspauschale für die 24/7-Rufbereitschaft,
- Kosten für Remote- und Vor-Ort-Leistungen auf Grundlage der im Preisblatt vorgegebenen Vergleichsmengen,

Die für die Preiswertung zugrunde gelegten Mengen und Berechnungsparameter werden im Preisblatt verbindlich vorgegeben. Die dort angegebenen Vergleichsmengen dienen ausschließlich der Herstellung der Vergleichbarkeit der Angebote und begründen keine Mindestabnahme.

Zur Ermittlung eines vergleichbaren Angebotspreises ist das vorgegebene Preisblatt vollständig auszufüllen.