Leistungsverzeichnis

ALLGEMEINE HINWEISE

VORBEMERKUNG:
Das Helmholtz Zentrum München verfolgt als Deutsches Forschungszentrum für Gesundheit und Umwelt das Ziel, personalisierte Medizin für die Diagnose, Therapie und Prävention weit verbreiteter Volkskrankheiten zu entwickeln. Dafür untersucht es das Zusammenwirken von Genetik, Umweltfaktoren und Lebensstil. Der Hauptsitz des Zentrums liegt in Neuherberg im Norden Münchens. Das Helmholtz Zentrum München ist eine Forschungseinrichtung des Bundes und des Freistaats Bayern und ist Mitglied der Helmholtz-Gemeinschaft.

Die in den Vergabeunterlagen enthaltenen Angaben beziehen sich grundsätzlich auf Personen jeder Geschlechtsidentität. Lediglich der leichteren Lesbarkeit halber wird im Folgenden bei allen Bezeichnungen nur noch die grammatikalisch männliche Form verwendet.
Soweit in den Vergabeunterlagen nichts anderes angegeben ist, sind
- mit Auftraggeber die Mitglieder der Einkaufsgemeinschaft/die Bezugsberechtigten gemeint. Zur besseren Lesbarkeit im Folgenden kurz Auftraggeber bezeichnet.
- mit Bieter alle Unternehmen, die im Rahmen der Ausschreibung ein Angebot abgeben gemeint.
- mit Auftragnehmer alle Bewerber, denen der Auftraggeber den Zuschlag erteilt, gemeint.
- mit Hersteller der Hersteller der Geräte, bei Geräten, die aus mehreren Komponenten zusammengesetzt sind, alle Hersteller gemeint.

AUFTRAGGEBER:
Helmholtz Zentrum München
Deutsches Forschungszentrum für Gesundheit und Umwelt (GmbH)
vertreten durch die Geschäftsführung
Ingolstädter Landstr. 1
85764 Neuherberg - Deutschland

BEZUGSBERECHTIGUNG:
Das Helmholtz Zentrum München führt die Ausschreibung des Rahmenvertrags zur Deckung des eigenen Bedarfs sowie koordinierend für die folgenden weiteren Bezugsberechtigten durch:

(1) DESY:
Deutsches Elektronen-Synchrotron, Notkestr. 85, D-22607 Hamburg

(2) DKFZ:
Deutsches Krebsforschungszentrum (DKFZ), Im Neuenheimer Feld 280, 69120 Heidelberg

(3) FZJ:
Forschungszentrum Jülich GmbH, Wilhelm-Johnen-Straße, 52428 Jülich

(4) GEOMAR:
GEOMAR Helmholtz-Zentrum für Ozeanforschung Kiel, Wischhofstr. 1-3, 24148 Kiel

(5) GFZ:
GFZ Helmholtz-Zentrum für Geoforschung, Telegrafenberg, 14473 Potsdam

(6) HZI:
Helmholtz-Zentrum für Infektionsforschung GmbH, Inhoffenstraße 7, 38124 Braunschweig

(7) MPG:

Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V., Generalverwaltung, Hofgartenstraße 8 80539 München

(8) UFZ:
Helmholtz-Zentrum für Umweltforschung - UFZ, Permoserstraße 15, 04318 Leipzig

Die vorgenannte Institutionen decken ihren Bedarf eigenverantwortlich. Die Bestell-, Liefer- und Rechnungsabwicklung erfolgt direkt mit der abrufenden Stelle. Für jeden Einzelabruf gelten, sofern nicht ausdrücklich anderes vereinbart wird, die Bedingungen dieses Rahmenvertrages.

GEGENSTAND DER AUSSCHREIBUNG:
Beschafft wird ein Security Operations Center in Form eines Managed Detection and Response (MDR) Services. Dieser umfasst:
Managed Service for Incident Detection & Incident Response and Digital Forensics.

HINWEIS ZU DEN PREISPOSITIONEN:
ES SIND NUR DIE GEFORDERTEN PREISPOSITIONEN, WIE DIESE DEFINIERT SIND, ZU BEFÜLLEN. ES DÜRFEN KEINE SEPRATEN PREISBLÄTTER MIT ANDEREN KONDITIONEN ABGEGEBEN WERDEN! ALLE PREISPOSITIONEN MÜSSEN ANGEBOTEN UND BEFÜLLT WERDEN.
SOLLTE EINE ZU BEPREISENDE PREISPOSITION IN IHREM ANGEBOT KEINE GESONDERTEN KOSTEN VERURSACHEN, IST BEI DIESER PREISPOSITION 0,00 EURO EINZUTRAGEN!

HINWEIS MENGENANGABEN (Schätz- & Höchstmenge):
Eine verbindliche Mindestbestellmenge wird nicht festgelegt.

Bei den Mengenangaben handelt es sich um die Schätz- und Höchstmenge.

Diese geschätzte Abnahmemenge wurde unter Beachtung der Bedarfsmengen der letzten Jahre sowie den voraussichtlichen Bedarfsmengen festgelegt. Eine Abnahmeverpflichtung besteht nicht. Vergütet werden nur die tatsächlich bestellten und gelieferten Produkte bzw. die tatsächlich erbrachte Leistung.

Die Ermittlung der einzelnen Mengen erfolgte durch die jeweiligen Bezugsberechtigten. Die Mengen je Position des Helmholtz Zentrum Münchens und der weiteren Bezugsberechtigten entnehmen Sie bitte den nachfolgenden Preispositionen 1 bis 10.

Ausfüllhinweise: Sie müssen alle farblich unterlegten, unterstrichenen Felder ausfüllen. Optional können Sie Angaben in Feldern machen, die nur unterstrichen, aber nicht farblich unterlegt sind. Tragen Sie in der Spalte "Mengen- und Preisangaben" alle notwendigen, geforderten Angaben ein (Preise und Kosten jeweils ohne gesetzliche USt.). Ist eine Preiseinheit ungleich 1 vorgegeben (z.B. 1.000), so geben Sie bitte den Preis netto pro Einheit bezogen auf die Preiseinheit an (z.B. 10,00 EUR pro 1.000 Mengeneinheiten). Beziehen Sie in Rahmenvertragspositionen Ihren angebotenen Preis auf die angegebene geschätzte Menge. Geben Sie in der Spalte "Gesamtbetrag netto (EUR)" für jede Position den Betrag an, der für die Position aus den Einzelangaben zu kalkulieren ist. Beispiel für eine Position mit angegebener Menge und gefordertem Preis: Die Menge ist mit dem Preis netto pro Einheit in Euro zu multiplizieren.

Nr.	Bezeichnung	Mengen- und Preisangaben	Gesamtbetrag netto (EUR)
1	Geschätztes Log-Volumen in TB / Monat (1) HMGU: 720 Stück für 4 Jahre (2) DESY: 48 Stück für 4 Jahre (3) DKFZ: 624 Stück für 4 Jahre (4) FZJ: 0 Stück für 4 Jahre (5) GEOMAR: 168 Stück für 4 Jahre (6) GFZ: 96 Stück für 4 Jahre (7) HZI: 768 Stück für 4 Jahre (8) MPG: 178 Stück für 4 Jahre (9) UFZ: 240 Stück für 4 Jahre HINWEIS: Die genannten Stückzahlen werden nur abgerufen, wenn Kriterium A 12 Proof-of-Concept erfolgreich abgeschlossen wurde.	**Menge:** 2.842 Stück **Preiseinheit:** 1 Stück **Nettopreis in Euro** _____ **USt.:** 19 %, falls abweichend _____ %	_____
2	Pauschale Implementierungsaufwand Wird je Teilnehmer 1 x abgerufen. AUSNAHME: Teilnehmer FJZ: Hier wird nur die reinge Beratung (Incident Response and Digital Forensics) in Anspruch genommen.	**Menge:** 8 Pauschale **Preiseinheit:** 1 Pauschale **Nettopreis in Euro** _____ **USt.:** 19 %, falls abweichend _____ %	_____

Nr.	Bezeichnung	Mengen- und Preisangaben	Gesamtbetrag netto (EUR)
3	Pauschale benötigter PoC im Vorfeld (1) HMGU: nein (2) DESY: ja (3) DKFZ: ja (4) FZJ: nein (5) GEOMAR: ja (6) GFZ: nein (7) HZI: ja (8) MPG: nein (9) UFZ: nein	**Menge:** 4 Pauschalen **Preiseinheit:** 1 Pauschalen **Nettopreis in Euro** _____ **USt.:** 19 %, falls abweichend _____ %	_____
4	Pauschale Anzahl Incident Response & Digital Forensik pro Jahr Retainer mit 40 Stunden pro Jahr 160 Stunden für 4 Jahre Insgesamt 8 Pauschalen für 1 Jahr / 32 Pauschalen für 4 Jahre (1) HMGU: ja (2) DESY: nein (3) DKFZ: ja (4) FZJ: ja (5) GEOMAR: ja (6) GFZ: ja (7) HZI: ja (8) MPG: ja (9) UFZ: ja	**Menge:** 32 Pauschalen **Preiseinheit:** 1 Pauschalen **Nettopreis in Euro** _____ **USt.:** 19 %, falls abweichend _____ %	_____

Nr.	Bezeichnung	Mengen- und Preisangaben	Gesamtbetrag netto (EUR)
5	Pauschale Tagessatz Security Analyst Geben Sie die Pauschale für einen Personentag an. Ein Personentag (PT) entspricht 8 Stunden, 1 Stunde entspricht 60 Minuten. Mit diesem pauschalen Tagessatz sind der zeitliche Aufwand auf der Verrechnungsgrundlage von 8 Arbeitsstunden pro Tag, alle Reisekosten und Reisezeiten sowie Übernachtungs- und Verpflegungskosten abgegolten. Eventuelle Mehrstunden pro Arbeitstag werden nicht gesondert vergütet. Anzahl der geplanten Tage für die Laufzeit von 4 Jahren je Teilnehmer: (1) HMGU: 0 (2) DESY: 0 (3) DKFZ: 20 (4) FZJ: 0 (5) GEOMAR: 1 (6) GFZ: 8 (7) HZI: 10 (8) MPG: 8 (9) UFZ: 1	**Menge:** 48 Tage **Preiseinheit:** 1 Tage **Nettopreis in Euro** _____ **USt.:** 19 %, falls abweichend _____ %	_____

Nr.	Bezeichnung	Mengen- und Preisangaben	Gesamtbetrag netto (EUR)
6	Pauschale Tagessatz Senior Security Analyst Geben Sie die Pauschale für einen Personentag an. Ein Personentag (PT) entspricht 8 Stunden, 1 Stunde entspricht 60 Minuten. Mit diesem pauschalen Tagessatz sind der zeitliche Aufwand auf der Verrechnungsgrundlage von 8 Arbeitsstunden pro Tag, alle Reisekosten und Reisezeiten sowie Übernachtungs- und Verpflegungskosten abgegolten. Eventuelle Mehrstunden pro Arbeitstag werden nicht gesondert vergütet. Anzahl der geplanten Tage für die Laufzeit von 4 Jahren je Teilnehmer: (1) HMGU: 40 (2) DESY: 0 (3) DKFZ: 12 (4) FZJ: 0 (5) GEOMAR: 1 (6) GFZ: 12 (7) HZI: 20 (8) MPG: 14 (9) UFZ: 1	**Menge:** 100 Tage **Preiseinheit:** 1 Tage **Nettopreis in Euro** _____ **USt.:** 19 %, falls abweichend _____ %	_____

Nr.	Bezeichnung	Mengen- und Preisangaben	Gesamtbetrag netto (EUR)
7	Pauschale Tagessatz Cyber Security Advisor Geben Sie die Pauschale für einen Personentag an. Ein Personentag (PT) entspricht 8 Stunden, 1 Stunde entspricht 60 Minuten. Mit diesem pauschalen Tagessatz sind der zeitliche Aufwand auf der Verrechnungsgrundlage von 8 Arbeitsstunden pro Tag, alle Reisekosten und Reisezeiten sowie Übernachtungs- und Verpflegungskosten abgegolten. Eventuelle Mehrstunden pro Arbeitstag werden nicht gesondert vergütet. Anzahl der geplanten Tage für die Laufzeit von 4 Jahren je Teilnehmer: (1) HMGU: 80 (2) DESY: 0 (3) DKFZ: 16 (4) FZJ: 0 (5) GEOMAR: 1 (6) GFZ: 12 (7) HZI: 30 (8) MPG: 12 (9) UFZ: 1	**Menge:** 152 Tage **Preiseinheit:** 1 Tage **Nettopreis in Euro** _____ **USt.:** 19 %, falls abweichend _____ %	_____

Nr.	Bezeichnung	Mengen- und Preisangaben	Gesamtbetrag netto (EUR)
8	Pauschale Tagessatz Digital Forensic & Incident Response Consultant Geben Sie die Pauschale für einen Personentag an. Ein Personentag (PT) entspricht 8 Stunden, 1 Stunde entspricht 60 Minuten. Mit diesem pauschalen Tagessatz sind der zeitliche Aufwand auf der Verrechnungsgrundlage von 8 Arbeitsstunden pro Tag, alle Reisekosten und Reisezeiten sowie Übernachtungs- und Verpflegungskosten abgegolten. Eventuelle Mehrstunden pro Arbeitstag werden nicht gesondert vergütet. Anzahl der geplanten Tage für die Laufzeit von 4 Jahren je Teilnehmer: (1) HMGU: 0 (2) DESY: 0 (3) DKFZ: 12 (4) FZJ: 0 (5) GEOMAR: 1 (6) GFZ: 12 (7) HZI: 10 (8) MPG: 8 (9) UFZ: 1	**Menge:** 44 Tage **Preiseinheit:** 1 Tage **Nettopreis in Euro** _____ **USt.:** 19 %, falls abweichend _____ %	_____

Nr.	Bezeichnung	Mengen- und Preisangaben	Gesamtbetrag netto (EUR)
9	Pauschale Tagessatz Recovery Engineer Geben Sie die Pauschale für einen Personentag an. Ein Personentag (PT) entspricht 8 Stunden, 1 Stunde entspricht 60 Minuten. Mit diesem pauschalen Tagessatz sind der zeitliche Aufwand auf der Verrechnungsgrundlage von 8 Arbeitsstunden pro Tag, alle Reisekosten und Reisezeiten sowie Übernachtungs- und Verpflegungskosten abgegolten. Eventuelle Mehrstunden pro Arbeitstag werden nicht gesondert vergütet. Anzahl der geplanten Tage für die Laufzeit von 4 Jahren je Teilnehmer: (1) HMGU: 0 (2) DESY: 0 (3) DKFZ: 12 (4) FZJ: 0 (5) GEOMAR: 1 (6) GFZ: 8 (7) HZI: 5 (8) MPG: 4 (9) UFZ: 1	**Menge:** 31 Tage **Preiseinheit:** 1 Tage **Nettopreis in Euro** _____ **USt.:** 19 %, falls abweichend _____ %	_____

Nr.	Bezeichnung	Mengen- und Preisangaben	Gesamtbetrag netto (EUR)
10	Pauschale Tagessatz Krisenmanager Geben Sie die Pauschale für einen Personentag an. Ein Personentag (PT) entspricht 8 Stunden, 1 Stunde entspricht 60 Minuten. Mit diesem pauschalen Tagessatz sind der zeitliche Aufwand auf der Verrechnungsgrundlage von 8 Arbeitsstunden pro Tag, alle Reisekosten und Reisezeiten sowie Übernachtungs- und Verpflegungskosten abgegolten. Eventuelle Mehrstunden pro Arbeitstag werden nicht gesondert vergütet. Anzahl der geplanten Tage für die Laufzeit von 4 Jahren je Teilnehmer: (1) HMGU: 0 (2) DESY: 0 (3) DKFZ: 8 (4) FZJ: 0 (5) GEOMAR: 1 (6) GFZ: 14 (7) HZI: 10 (8) MPG: 1 (9) UFZ: 1	**Menge:** 34 Tage **Preiseinheit:** 1 Tage **Nettopreis in Euro** _____ **USt.:** 19 %, falls abweichend _____ %	_____

Wertungsschema

LEISTUNGSVERZEICHNIS

Die Wertung erfolgt nach der einfachen Richtwertmethode nach UfAB 2018 (abrufbar unter http://www.cio.bund.de). Für die Bestimmung des wirtschaftlichsten Angebotes wird das Leistungs-Preis-Verhältnis herangezogen. Es wird jeweils der Quotient aus Leistungspunkten und Preis berechnet. Die so ermittelte Kennzahl wird mit dem Skalierungsfaktor 100000 multipliziert. Das Angebot mit dem höchsten Ergebnis wird als das wirtschaftlichste angesehen; bei mehreren Angeboten mit absolut gleichen Ergebnissen erhält das preisgünstigste den Zuschlag.

Summe der Gewichtungspunkte (GP): 100 Gewichtungspunkte (GP)

Geltungsbereich
Dieses Dokument legt die Anforderungen für die Bereitstellung eines Security Operation Centers in der Form eines "Gemanagter Service für die Erkennung und Reaktion auf Sicherheitsvorfälle" fest, einschließlich der Leistungsbeschreibung, der Schnittstellen und der Berichterstattung sowie der Service Level Agreements.

Definitionen/Akronyme/Abkürzungen:
Bedrohungsüberwachung: umfasst die kontinuierliche Überwachung und Analyse potenzieller Sicherheitsbedrohungen für das Netzwerk, IT-Systeme und Daten. Dazu gehört die Identifizierung verdächtiger Aktivitäten, unbefugter Zugriffe und potenzieller Sicherheitsverletzungen.

Threat Intelligence: ist eine evidenzbasierte, detaillierte und anwendbare strategische Informationsquelle zu Bedrohungen, die auf einer flexiblen, dynamischen Technologie basiert, die Datensammlungen und -analysen nutzt, um Bedrohungen, die auf eine Organisation abzielen, zu verhindern und zu beseitigen.

Threat Hunting: aktiver, von Menschen (z.B. SOC Team) gesteuerter Prozess, der Bedrohungsinformationen zusammen mit anderen Datenquellen und Tools nutzt, um proaktiv nach potenziellen Bedrohungen im Netzwerk oder in den Systemen eines Unternehmens zu suchen und Aktivitäten wie Persistenzmechanismen, ungewöhnliche Anwendungsverwendung, Netzwerkaktivitäten oder Taktiken, Techniken und Verfahren ("TTPs") von Bedrohungsakteuren zu erkennen,
Bedrohungserkennung: umfasst die Identifizierung, Meldung und Eindämmung von Cyberangriffen. BSI: Bundesamt für Sicherheit in der Informationstechnik
ISO: International Organization for Standardization
MDR: Managed Detection and Response URL: Uniform Resource Locator

Hinweis:
Die im Leistungsverzeichnis festgelegten Ausschlusskriterien(A-Kriterien) definieren den Leistungsumfang des zu vergebenden Auftrags. Ein Angebot, welches diese Anforderungen nicht erfüllt - bei dem also im Leistungsverzeichnis die Option "Nein" angekreuzt wird - weicht von den Vergabeunterlagen ab und ist daher zwingend vom Verfahren auszuschließen.

Nr.	Bezeichnung	**Antwort**	**Kriteriengewichtung**
KHG A	**ANFORDERUNGEN - Ausschlusskriterium (A-Kriterien)**		**0,00 GP**
A 1	**Leistungsumfang** (Ist Ausschlusskriterium) (Ist Ja-oder-Nein-Kriterium) (1) Der Auftragnehmer muss eine MDR-Dienstleistung erbringen, die die folgenden zwei Dienstleistungskomponenten umfasst: (a) Managed Service for Incident Detection - im Folgenden als Incident Detection Dienst bezeichnet (b) Support for Incident Response and Digital Forensics - im Folgenden als Incident Response und Digitale Forensik Dienst bezeichnet (2) Die Rechenzentren, Standorte und Mitarbeiter, die für die Bereitstellung der in Kriterium A 1 / Punkt (1) aufgeführten Dienste eingesetzt werden, müssen sich im Europäischen Wirtschaftsraum befinden. (3) Der Auftragnehmer muss nach Zuschlagserteilung ein kleines Team von 2-3 Personen ernennen, das als zentraler Ansprechpartner für alle dienstleistungsbezogenen Aufgaben und Maßnahmen zuständig ist.	☐ **Ja** ☐ **Nein**	

Nr.	Bezeichnung	Antwort	Kriteriengewichtung
	(4) Der Auftragnehmer muss die Dienstleistung remote erbringen. Vor-Ort-Aktivitäten auf Räumlichkeiten des Auftraggebers sind nicht erwünscht, es sei denn, sie werden ausdrücklich von beiden Parteien angefordert und vereinbart.		
A 2	**Incident Detection Dienst - Dienstmerkmale** (Ist Ausschlusskriterium) (Ist Ja-oder-Nein-Kriterium) (1) Der Auftragnehmer muss den Incident Detection Dienst als betreuten Dienst bereitstellen, alle erforderlichen Maßnahmen durchführen inklusiv die Anbindung von unterschiedlichen Logquellen, und die erforderliche Infrastruktur, Anwendungen und Werkzeuge bereitstellen. (2) Der Incident Detection Dienst muss mindestens folgende Leistungen umfassen: (a) Echtzeit Bedrohungsüberwachung (b) Threat Hunting (c) Bedrohungserkennung (d) Threat Intelligence einschließlich Dark Web Monitoring (3) Der Auftragnehmer muss alle vom Auftraggeber bereitgestellten Protokolldateien verarbeiten und alle Protokollereignisse auf Sicherheitsvorfälle analysieren. (4) Der Auftragnehmer muss die Protokolldaten mindestens 1 Jahr lang und höchstens bis zum Ablauf des Vertrags speichern. (5) Der Incident Detection Service muss die folgenden Protokollquellen unterstützen: SIEHE DOKUMENT "VgV_2025-005 Anlage zum LV". HINWEIS: DIESES DOKUMENT WIRD ERST NACH VORLAGE DER GEFORDERTEN GEHEIMHALTUNGSVEREINBARUNG ÜBERMITTELT! (6) Der Auftragnehmer muss soweit erforderlich die APIs der in Kriterium A 2 / Punkt (5) aufgeführten Systeme verwenden, um zusätzliche Nachweise oder Kontextdaten zu sammeln, die nicht im Syslog-Feed	☐ **Ja** ☐ **Nein**	

Nr.	Bezeichnung	Antwort	Kriteriengewichtung
	dieser Systeme enthalten sind. (7) Der Incident Detection Dienst muss eine unbegrenzte Anzahl von Log-Quellen basierend auf den in Kriterium A 2 / Punkt (5) definierten Log-Quellentypen unterstützen. (8) Der Auftragnehmer muss innerhalb von 10 Werktagen nach der Anfrage des Kunden Unterstützung für neue Arten von syslog-basierten Protokollquellen bereitstellen, die derzeit nicht in Kriterium A 2 / Punkt (5) enthalten sind. (9) Der Auftragnehmer muss dem Auftraggeber Mechanismen - wie z. B. lokale Log-Kollektoren - zur Verfügung stellen, die es ermöglichen, die in Kriterium A 2 / Punkt (5) definierten Log-Quellen auf sichere und zuverlässige Weise an den Incident Detection Dienst zu senden. (10) Der Auftragnehmer muss Dokumentation und Unterstützung für die Konfiguration der in Kriterium A 2 / Punkt (5) definierten Protokollquellen bereitstellen, um Protokolle an den Incident Detection Dienst zu senden. Der Auftraggeber wird seine Protokollquellen gemäß dieser Dokumentation konfigurieren. (11) Der Auftragnehmer muss den Incident Detection Dienst 24 Stunden am Tag und 365 Tage im Jahr anbieten. (12) Der Auftragnehmer muss Bedrohungen wie schädliches Verhalten, Netzwerkaktivität, Kontroll- und Steuerungskommunikation sowie Anwendungsnutzung, nach dem Sinne des MITRE ATT&CK Frameworks identifizieren. (13) Der Auftragnehmer muss fortschrittliche Technologien für die Erkennung komplexer Cyberbedrohungen nutzen, einschließlich unbekannter und fortschrittlicher Angriffsvektoren. (14) Im Rahmen der Threat Hunting Leistung, muss der Auftragnehmer kontinuierlich und proaktiv nach verborgenen oder sich entwickelnden Bedrohungen innerhalb des Netzwerks des Auftraggebers suchen.		

Nr.	Bezeichnung	Antwort	Kriteriengewichtung
	(15) Der Auftragnehmer muss sicherstellen, dass der Prozentsatz, der dem Auftraggeber mitgeteilten falsch positiven Erkennungen von Bedrohungen unter 5% liegt. (16) Im Rahmen der Threat Intelligence Leistung, muss der Auftragnehmer einen Sicherheitsinformations-Feed bereitstellen, um IP-Adressen, Domainnamen und URLs zu blockieren. Dieser Sicherheitsinformations-Feed muss so bereitgestellt werden, dass er automatisch und regelmäßig in Next-Generation-Firewalls und Internet-Proxys des Auftraggebers importiert werden kann. (17) Der Auftragnehmer muss ein webbasiertes Portal für den Auftraggeber bereitstellen, das Zugriff auf - alle vom Auftraggeber gesendeten Protokollereignisse und Warnmeldungen, - statistische Informationen zu den Protokollereignisdaten und zu den Incidents, - Berichterstellungsfunktion, mit der auf Abruf Berichte mit einer Zusammenfassung des Incident Detection-Dienstes erstellt werden können. - Sicherheitsvorfallberichte und Sicherheitsvorfallmanagement, und - die Möglichkeit zur Interaktion mit dem Auftragnehmer bei Anfragen oder Problemen bietet. - die Möglichkeit bietet, Bilder oder andere Dateien für den Auftragnehmer hochzuladen, die sich auf Vorfälle oder Anfragen beziehen. - Newsfeed mit Updates des Auftragnehmers zu Service, Portal und anderen Themen, die der Auftragnehmer für relevant hält. (18) Das unter Kriterium A 2 / Ziffer (17) definiertes Webportal muss den Auftraggeber Mitarbeitern die Möglichkeit bieten, mit einer Abfragesprache (z. B. SQL, KQL) Abfragen für alle gesammelten und geparsten Daten durchzuführen, die zur Erkennung von Bedrohungen verwendet werden. (19) Das unter Kriterium A 2 / Ziffer (17) definierte Webportal muss zusätzlich zu der		

Nr.	Bezeichnung	Antwort	Kriteriengewichtung
	in Kriterium A 2 / Ziffer (18) definierten Funktionalität auch eine Bibliothek nützlicher Queries bereitstellen, die regelmäßig aktualisiert wird, um die Mitarbeiter des Auftraggebers bei der Erkennung von Bedrohungen zu unterstützen. (20) Das in Kriterium A 2 / Ziffer (17) definierte webbasierte Portal muss eine Zwei-Faktor-Authentifizierung (2FA) unterstützen.		
A 3	**Incident Detection Dienst - Liefergegenstände** (Ist Ausschlusskriterium) (Ist Ja-oder-Nein-Kriterium) (1) Der Auftragnehmer muss den Auftraggeber unverzüglich über jede festgestellte Bedrohung per Telefon und/ oder E-Mail gemäß dem in der Einführungsphase abegehaltenen Workshop (vgl. Kriterium A 6) vereinbarten Ablauf, informieren. (2) Der Auftragnehmer muss für jede festgestellte Bedrohung einen klaren, detaillierten Sicherheitsvorfallbericht vorlegen, der mindestens Einzelheiten über den Vorfall, Beobachtungen, Empfehlungen zur Eindämmung des Vorfalls und zur Behebung enthält. (3) Der Auftragnehmer muss vierteljährlich mit dem Auftraggeber Bedrohungsüberprüfungen durchführen. Bedrohungsüberprüfungen sind virtuelle Besprechungen, in denen der Auftragnehmer Folgendes präsentiert und bespricht: - den Status des Dienstes, - die Überprüfung von Sicherheitsvorfällen, - Informationen über die Sicherheitslage und Angriffsfläche des Auftraggebers und - Empfehlungen an den Auftraggeber zu Sicherheitsverbesserungen. (4) Der Auftragnehmer muss sicherstellen, dass ein Senior-Analyst aus dem Analystenteam, das den Incident-Detection-Service bereitstellt, für relevante Teile der in Kriterium A 3/ Ziffer (3) definierten Bedrohungsprüfungen verantwortlich ist und diese Prüfungen leitet.	☐ **Ja** ☐ **Nein**	

Nr.	Bezeichnung	Antwort	Kriteriengewichtung
A 4	**Incident Response und Digitale Forensik Dienst - Leistungsmerkmale** (Ist Ausschlusskriterium) (Ist Ja-oder-Nein-Kriterium) (1) Der Incident Response und digitale Forensik Dienst muss mindestens Folgendes bereitstellen: - Incident-Management - Incident-Eindämmungsempfehlungen - Ursachenanalyse - Beweissicherung - Forensische Analyse - Malware-Analyse - Netzwerkverkehrsanalyse - Bedrohungsanalyse (2) Der Auftragnehmer muss täglich 24 Stunden, 7 Tage die Woche und 365 Tage im Jahr auf Abruf und für den Vorfallsreaktions- und Digitalforensikdienst verfügbar sein. (3) Nach der Beauftragung durch den Auftraggeber muss der Auftragnehmer innerhalb von 2 Stunden reagieren und innerhalb von 4 Stunden die Arbeit aufnehmen. (4) Der Auftragnehmer muss für jeden Vorfall eine dedizierte zentrale Anlaufstelle benennen - gem. Kriterium A 4 / Ziffer (3). (5) Der Auftragnehmer muss den Vorfallsreaktions- und digitalen Forensikdienst remote erbringen, unter Verwendung von Tools oder Ressourcen, die vom Auftragnehmer oder vom Auftraggeber bereitgestellt werden. Vor-Ort-Aktivitäten auf Räumlichkeiten des Auftraggebers sind nicht erforderlich, es sei denn, sie werden ausdrücklich von beiden Parteien angefordert und vereinbart. (6) Der Auftragnehmer muss einen jährlichen Mindestanspruch von 40 Stunden für den Vorfallsreaktions- und Digitalforensikdienst bereitstellen. Sollte dieses Kontigent im aktuellen Jahr nicht aufgebraucht werden, müssen bis zu 50% der zu übertragenden Stunden in die in Kriterium A 13 beschriebenen Dienstleistungen für das Folgejahr umgewandelt werden können. (7) Der Auftragnehmer muss dem	☐ **Ja** ☐ **Nein**	

Nr.	Bezeichnung	Antwort	Kriteriengewichtung
	Auftraggeber bei der Bewältigung eines Vorfalls unterstützen, wobei die Unterstützung mindestens Folgendes umfasst: - Eindämmung der Bedrohung - Beseitigung von Kompromittierungen und Infektionen - Wiederherstellung kompromittierter Systeme (8) Der Auftragnehmer muss mindestens eine Möglichkeit anbieten, Systeme im Falle eines kritischen Vorfalls eigenständig zu blockieren (z.B. über einen Zugriff auf EDR).		
A 5	**Incident Response und Digitale Forensik Dienst - Liefergegenstände** (Ist Ausschlusskriterium) (Ist Ja-oder-Nein-Kriterium) (1) Der Auftragnehmer muss für jeden Sicherheitsvorfall einen Bericht vorlegen, der mindestens Folgendes enthält: - Zusammenfassung - Zeitplan der Aktivitäten - Einzelheiten zu den Ergebnissen und Nachweisen - Empfehlungen (2) Der Auftragnehmer muss den Sicherheitsvorfallbericht bei kritischen Sicherheitsvorfällen innerhalb von 30 Minuten und ansonsten innerhalb von 120 Minuten nach Feststellung des Schweregrads des Sicherheitsvorfalls einreichen.	☐ **Ja** ☐ **Nein**	
A 6	**Einführungsphase** (Ist Ausschlusskriterium) (Ist Ja-oder-Nein-Kriterium) Der Auftragnehmer muss den Dienst zu Beginn des Vertrags während der Einführungsphase mit entsprechenden Workshops einrichten, die nicht länger als zwei Wochen dauern dürfen. Zielsetzung der Workshops ist die Abstimmung der Prozesse und Schnittstellen zwischen dem Dienstleister und dem lokalen Ansprechpartner zur Optimierung der Zusammenarbeit. Folgende Anforderungen sind in den Workshops in der Einführungsphase zu erfüllen: - Meldestrukturen: Der Dienstleister hat ein	☐ **Ja** ☐ **Nein**	

Nr.	Bezeichnung	Antwort	Kriteriengewichtung
	Meldeschema zu entwickeln, das definiert, wer für die Meldung von Vorfällen verantwortlich ist, welche Informationen erforderlich sind und an wen diese übermittelt werden müssen. - Klassifikation von Risiken: Der Dienstleister muss Kriterien und Methoden zur Identifizierung, Klassifikation und Priorisierung von Risiken bereitstellen. Der Auftraggeber muss in der Lage sein, angemessene Reaktionen auf identifizierte Risiken zu formulieren. - Rückmeldungsprozesse: Es ist sicherzustellen, dass klare Abläufe zur Rückmeldung von Informationen definiert sind. Der Dienstleister hat einen transparenten Feedback-Mechanismus zu implementieren, der die Verantwortlichkeiten für die Kommunikation von Ergebnissen und Maßnahmen festlegt. - Richtlinien zur Datenspeicherung: Der Dienstleister hat die geltenden gesetzlichen und internen Vorgaben zur Speicherung von Daten zu berücksichtigen, einschließlich der maximalen Speicherdauer und der Maßnahmen zur Datensicherheit. Alle Beteiligten müssen über die entsprechenden Richtlinien informiert werden. - Dokumentation: Der Dienstleister hat die Ergebnisse der Workshops in einem schriftlichen Bericht zu dokumentieren, der die erarbeiteten Prozesse, Schnittstellen und Vereinbarungen festhält. Die Einführungsphase ist abgeschlossen, wenn: - alle in Kriterium A 2 / Punkt (5) definierten Protokollquellen mit dem Incident Detection Dienst verbunden sind, - die Ansprechpartner für den Dienst gem. Kriterium A 6 definiert sind, - die erforderlichen Prozesse definiert, dokumentiert und gegenseitig vereinbart sind, und - der Auftragnehmer den Dienst starten kann.		
A 7	**Anpassungsphase** (Ist Ausschlusskriterium) (Ist Ja-oder-Nein-Kriterium) Es ist nicht ausreichend, lediglich Protokollquellen anzubinden; vielmehr ist es unerlässlich, diese kontinuierlich zu überwachen und anzupassen. Ziel ist es,	☐ **Ja** ☐ **Nein**	

Nr.	Bezeichnung	Antwort	Kriteriengewichtung
	sicherzustellen, dass ausschließlich die tatsächlich benötigten Informationen an den Dienstleister übertragen werden. Diese Vorgehensweise ist aus wirtschaftlichen und datenschutzrechtlichen Gründen von großer Bedeutung. Die Übertragung aller Daten ohne gezielte Filterung kann zu einem signifikanten Anstieg des Protokollvolumens führen. Ein erhöhtes Protokollvolumen hat direkte Auswirkungen auf die Betriebskosten, da mehr Speicherplatz benötigt wird und höhere Anforderungen an die Netzwerkbandbreite entstehen. Dies kann die Effizienz der Systeme beeinträchtigen und zu zusätzlichen Kosten bei der Datenverarbeitung und -speicherung führen. Durch eine gezielte Auswahl der zu übertragenden Daten können Unternehmen Kosten sparen und ihre Ressourcen effizienter nutzen. Die Übertragung sensibler oder irrelevanter Informationen kann auch datenschutzrechtliche Risiken bergen. Gemäß den geltenden Datenschutzgesetzen müssen Unternehmen sicherstellen, dass nur die notwendigen Daten verarbeitet und übertragen werden. Eine übermäßige Datenübertragung kann nicht nur gegen Datenschutzbestimmungen verstoßen, sondern auch das Risiko von Datenlecks und Missbrauch erhöhen. Indem sie die Übertragung auf relevante Informationen beschränken, können Unternehmen ihre Compliance mit Datenschutzrichtlinien sicherstellen und das Vertrauen ihrer Kunden und Partner stärken. Insgesamt ist es daher von entscheidender Bedeutung, die Protokollquellen regelmäßig zu überprüfen und anzupassen, um sicherzustellen, dass nur die benötigten Informationen an den Dienstleister weitergegeben werden. Dies trägt sowohl zur Kostenkontrolle als auch zum Schutz der personenbezogenen Daten bei. Der Dienstleister muss die eingesetzten Technologien, Softwarelösungen und Schnittstellen zwischen den Systemen analysieren und optimieren, um eine effiziente Integration und Datenübertragung		

Nr.	Bezeichnung	Antwort	Kriteriengewichtung
	zu gewährleisten.		
A 8	**Außerbetriebnahme** (Ist Ausschlusskriterium) (Ist Ja-oder-Nein-Kriterium) Der Auftragnehmer muss alle Daten, die sich auf den Auftraggeber oder sein Personal beziehen und sich in seinem Besitz befinden, am Ende des Vertrags löschen.	☐ **Ja** ☐ **Nein**	
A 9	**Sicherheit** (Ist Ausschlusskriterium) (Ist Ja-oder-Nein-Kriterium) (1) Der Auftragnehmer muss die geltenden nationalen und internationalen IT-Sicherheitsempfehlungen einhalten. (2) Der Auftragnehmer muss nachweisen können, dass die von ihm erbrachte Dienstleistung mindestens einem Standard entspricht, der dazu dient, Dritten zu versichern, dass bei den Entwicklungs-, Management- und Betriebsaktivitäten im Zusammenhang mit dem verwendeten Tool gute Praktiken des Informationssicherheitsmanagements angewendet wurden (d. h. ISO 27001, BSI IT-Grundschutz oder ein vergleichbares nationales Äquivalent).	☐ **Ja** ☐ **Nein**	
A 10	**Datenschutz** (Ist Ausschlusskriterium) (Ist Ja-oder-Nein-Kriterium) (1) Der Auftraggeber ist dem Schutz personenbezogener Daten verpflichtet. Der Auftraggeber verarbeitet personenbezogene Daten in Übereinstimmung mit seinen internen Rechtsvorschriften, die auf den Grundsätzen intern festgelegter bewährter Verfahren, insbesondere den Datenschutzvorschriften der Europäischen Union, aufbaut. Der Auftragnehmer stellt sicher, dass die Verarbeitung personenbezogener Daten durch den Auftragnehmer und die Unterauftragsverarbeiter für den Dienst an den Auftraggeber in Übereinstimmung mit allen anwendbaren Gesetzen und Vorschriften erfolgt, insbesondere mit der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), wobei	☐ **Ja** ☐ **Nein**	

Nr.	Bezeichnung	Antwort	Kriteriengewichtung
	gleichzeitig sichergestellt wird, dass die DSGVO nicht direkt auf den Auftraggeber anwendbar ist. (2) Der Auftragnehmer stellt sicher, dass der Standort des/der Server(s), der/die für die Speicherung und/oder Verarbeitung von im Zusammenhang mit dem Auftraggeber stehenden personenbezogenen Daten verwendet wird/werden, auf diejenigen beschränkt ist/sind, die innerhalb der geografischen Grenzen der EU-Mitgliedstaaten, der Schweiz oder Großbritannien gehostet werden.		
A 11	**Sprache** (Ist Ausschlusskriterium) (Ist Ja-oder-Nein-Kriterium) Der Auftragnehmer verwendet für den Dienst, für die Kommunikation mit dem Auftraggeber und für alle zu erbringenden Leistungen Englisch oder Deutsch.	☐ **Ja** ☐ **Nein**	
A 12	**Proof-of-Concept-Phase** (Ist Ausschlusskriterium) (Ist Ja-oder-Nein-Kriterium) Der Auftragnehmer muss die Möglichkeit bieten den Dienst im Rahmen eines Proof of Concepts dem Auftraggeber zu Testzwecken bereitzustellen. Diese Leistung ist nur auf gesonderten Abruf hin zu erbringen. Ein Anspruch auf Beauftragung der Leistung besteht nicht. Der Proof of Concept ist abgeschlossen, wenn: - maximal fünf der in Kriterium A 2 / Punkt (5) definierten Protokollquellen mit dem Incident Detection Dienst verbunden sind, - die Ansprechpartner für den Dienst definiert sind, - die erforderlichen Prozesse definiert sind und - der Auftraggeber den Dienst für drei Monate testen konnte.	☐ **Ja** ☐ **Nein**	
A 13	**Dienstleistungen** (Ist Ausschlusskriterium) (Ist Ja-oder-Nein-Kriterium) Während der Dauer des Rahmenvertrags kann der Auftraggeber Unterstützungsleistungen für Beratung und Unterstützung in technischen und strategischen Fragen der IT-Sicherheit anfordern. Die Leistungserbringung der Dienstleistungen erfolgt primär Vor-Ort	☐ **Ja** ☐ **Nein**	

Nr.	Bezeichnung	Antwort	Kriteriengewichtung
	beim Auftraggeber, kann in Abstimmung mit dem Auftraggeber aber auch remote erbracht werden. Die technischen Vorrausetzungen dafür werden vom Auftraggeber bereitgestellt. Damit dies bedarfsbezogen vom Auftraggeber abgerufen werden kann, sind 6 Kategorien an Kompetenzprofilen anzubieten. Skill-Profile der Mitarbeiter sind dem Angebot beizulegen (pseudonymisiert). Es muss sich um tatsächliche Mitarbeiter des Auftragnehmers handeln. Folgende Leistungen sind über die Vertragslaufzeit zu erwarten: - Durchführung von IT-Security Audits - Erarbeitung von Optimierungsstrategien für IT-Security-Themen - Beratung IT-Security-Architektur - Beratung bei Digital Forensic & Incident Response - Krisenmanagement - Unterstützung bei der Wiederherstellung nach einem Security Vorfall Dafür hat der Auftragnehmer qualifiziertes und auch zertifiziertes Personal vorzuhalten. Es sind folgende Skill-Level zur Verfügung zu stellen. (1) Security Analyst (a) 1-3 Jahre Erfahrung im IT-Sicherheitsumfeld (b) Beispielhafte Aufgaben: Überwachung der MDR-Quellen auf Sicherheitsvorfälle, Durchführung von Schwachstellenanalysen, Implementierung von Sicherheitsmaßnahmen (Aufzählung nicht abschließend). (2) Senior Security Analyst (a) Mindestens 3-5 Jahre Erfahrung im IT-Sicherheitsumfeld (b) Beispielhafte Aufgaben: Entwicklung von Sicherheitsstrategien, Beratung in Sicherheitsfragen, Monitoring und Analyse von Sicherheitsmeldungen, Dokumentation und Reporting der Security Vorfälle, Threat Hunting (Aufzählung nicht abschließend). (3) Cyber Security Advisor (a) Mindestens 5 Jahre Erfahrung im IT-Sicherheitsumfeld		

Nr.	Bezeichnung	Antwort	Kriteriengewichtung
	(b) Beispielhafte Aufgaben: Beratung IT-Security-Architektur, Durchführung von Risikoanalysen, Erarbeitung von Optimierungsstrategien für IT-Security-Themen (Aufzählung nicht abschließend). (4) Digital Forensic & Incident Response Consultant (a) Mindestens 5 Jahre Erfahrung im IT-Sicherheitsumfeld (b) Beispielhafte Aufgaben: Untersuchung von IT-Sicherheitsvorfällen und bei der Ergreifung von Gegenmaßnahmen, Durchführung von Analysen im Incident-Response-Bereich sowie forensische Untersuchungen (Clients, Server, Network, Mobile und Cloud), Durchführung von Compromise Assessments, Konzeptionelle und technische Beratung in den Bereichen: IT Forensic Readiness, DFIR-Prozesse, Angriffserkennung und Verteidigung. Effiziente Vorbereitung von Systemen, um schnell auf Angriffe zu reagieren; Vermittlung von Techniken zur frühzeitigen Identifizierung von Bedrohungen, einschließlich der Analyse von Protokollen und der Nutzung von SIEM-Systemen; Angriffsanalyse und effektive Abwehrmaßnahmen; Darstellung von gängigen Musterangriffen und Entwicklung realistischer Reaktionsstrategien; Penetrationstests auf ein System, Netzwerk oder eine Anwendung, um Sicherheitslücken und Schwachstellen zu identifizieren; Durchführung von Tabletop-Übungen in simulierten Szenarien um die Reaktionsstrategien auf Sicherheitsvorfälle testen und Verbesserungsmöglichkeiten zu identifizieren (Aufzählung nicht abschließend). (5) Recovery Engineer (a) Mindestens 3-5 Jahre Erfahrung im IT-Sicherheitsumfeld (b) Beispielhafte Aufgaben: Unterstützung bei der Wiederherstellung von Systemen nach einem Security Vorfall, Entwicklung von Notfallwiederherstellungsplänen (Aufzählung nicht abschließend). (6) Krisenmanager (a) Mindestens 5 Jahre Erfahrung im IT-Krisenmanagement (b) Beispielhafte Aufgaben: Krisenreaktion,		

Nr.	Bezeichnung	Antwort	Kriteriengewichtung
	Entwicklung des Krisenmanagementplans, Koordination der Reaktions- und Wiederherstellungsmaßnahmen, Kommunikation mit Stakeholdern, Evaluation des Krisenumgangs (Aufzählung nicht abschließend).		
A 14	**Bereitstellung von Ressourcen** (Ist Ausschlusskriterium) (Ist Ja-oder-Nein-Kriterium) Der Auftraggeber stellt Folgendes bereit: (1) Ressourcen für den Betrieb lokaler Log-Kollektoren (2) VPN-Fernzugriffseinrichtungen (3) zentrale Ansprechpartner für die Verwaltung des Dienstes (4) technische Kontakte, die der Auftragnehmer für den Dienst benötigt (5) Kontakte für die Meldung von Vorfällen	☐ **Ja** ☐ **Nein**	
A 15	**Servicegleitklausel** (Ist Ausschlusskriterium) (Ist Ja-oder-Nein-Kriterium) Während der Laufzeit der Rahmenvereinbarung werden kontinuierlich Erweiterungen und Modernisierungen aktuellen Sicherheitstechnologien stattfinden. Bedingt durch Technologieveränderungen und Weiterentwicklungen, unterliegt das Sortiment an angefragten Services kontinuierlichen Veränderungen. Der Auftraggeber ist berechtigt, die Aufnahme von zusätzlichen IT-Sicherheitsservices zu verlangen, sofern sich diese im aktuellen Sortiment des Auftragnehmers befinden und das Sicherheitsniveau der Systemumgebung des Auftraggebers sinnvoll ergänzen und begründbar (z.B. durch Sicherheitsvorfälle oder andere drängende Änderungen der Sicherheitsarchitektur) benötigt werden.	☐ **Ja** ☐ **Nein**	
KHG B	**KONZEPT(E) - Bewertungskriterium (B-Kriterium)**		**100,00 GP**
B 16	**Konzept** HINWEIS: Maximaler Umfang von 10 DIN A4 Seiten (inkl. Deckblatt, Inhaltsverzeichnis, Grafiken und Bilder). Seiten, die über diesen Umfang (Deckblatt+ Inhaltsverzeichnis + Grafiken + Bilder) hinausgehen, werden nicht bewertet. Schriftgröße mindestens 12 pt.. KEINE POWERPOINT!		100 GP

Nr.	Bezeichnung	Antwort	Kriteriengewichtung
	DAS KONZEPT DARF KEINE PREISANGABEN ENTHALTEN! Dieses Konzept wird ebenfalls Vertragsbestandteil. AUFGABENSTELLUNG: Der Auftragnehmer muss ein Konzept für einen Incident-Management Use Case zur Vorgehensweise bei der Identifizierung eines mit Ransomware kompromittierten Gerätes vorlegen, einschließlich der Beweissicherung, der rechtssicheren Begutachtung und der Dokumentation der gesicherten Beweise. BEWERTUNG: 10 Punkte: Hervorragende Darstellung bzw. Beantwortung, in der auf die Frage präzise und ausführlich eingegangen wurde; in der Antwort wurden nachprüfbare und verbindliche Angaben gemacht, die als Vertragsbestandteil ein Erreichen der genannten Ziele des Auftraggebers in einem besonders hohen Maße gewährleisten und später im Projekt überprüfbar sind. 8 Punkte: Gute Darstellung bzw. Beantwortung, in der auf die Frage eingegangen wurde und im hohen Maße unter Angabe von nachprüfbaren und vertraglich verbindlichen Fakten geantwortet wurde. Eine Überprüfung im Projekt ist später möglich. 6 Punkte: Befriedigende Darstellung bzw. Beantwortung, in der auf die Frage eingegangen wurde und überwiegend unter Angabe von nachprüfbaren und vertraglich verbindlichen Fakten geantwortet wurde. Eine Überprüfung im Projekt ist später teilweise möglich. 4 Punkte: Unzureichende Darstellung bzw. Beantwortung, in der auf die Frage nur teilweise eingegangen wurde bzw. in wesentlichen Teilen nur unverbindlich oder ohne Fakten zu benennen beantwortet wurde. Eine Prüfung der Fakten ist kaum möglich. Eine Überprüfung im Projekt ist kaum möglich.		

Nr.	Bezeichnung	Antwort	Kriteriengewichtung
	2 Punkte: Mangelhafte Darstellung bzw. Beantwortung, in der auf die Frage nur kaum bis gar nicht eingegangen wurde bzw. im Großteil der wesentlichen Teile nur unverbindlich oder ohne Fakten zu benennen beantwortet wurde. Eine Prüfung der Fakten ist nicht möglich. Eine Überprüfung im Projekt ist nicht möglich. 0 Punkte: Es liegt kein Konzept vor oder unzureichende Beantwortung bzw. fehlende Konzeptbestandteile.		

Angebot

Mit Unterzeichnung des Angebotes erkennt der Bieter die Forderungen und Angaben des Leistungsverzeichnisses an und bestätigt die Richtigkeit der von ihm gemachten Angaben.	Beschreibung	Betrag
	Gesamtangebotssumme ohne USt. (EUR):	
	Gesamtangebotssumme inkl. USt. (EUR):	