

346326-2026 - Hange

Saksamaa – Turvatarkvarapakett – Einführung und der Betrieb EDR/XDR & Managed Security Operations Center (SOC)

OJ S 96/2026 20/05/2026

Hanketeade või kontsessiooniteade – üldkord - Paranduse teade

Asjad

1. Hankija

1.1. Hankija

Ametlik nimi: Landkreis Rotenburg (Wümme)

E-posti aadress: vergabe@lk-row.de

Hankija õiguslik vorm: Kohalik omavalitsus

Hankija tegevus: Üldised avalikud teenused

2. Menetlus

2.1. Menetlus

Pealkiri: Einführung und der Betrieb EDR/XDR & Managed Security Operations Center (SOC)
Kirjeldus: Der Landkreis Rotenburg (Wümme) beabsichtigt, seine Kapazitäten zur Erkennung, Analyse und Abwehr von komplexen Cyberangriffen signifikant zu stärken.

Auftragsgegenstand ist die Einführung und der Betrieb einer modernen, integrierten Sicherheitslösung, die aus einer Technologieplattform und darauf aufbauenden Managed Services besteht, der zusätzlich einen „Incident Response“-Service samt eventuell nötiger Forensik beinhaltet.

Menetluse tunnus: 56e1e745-f763-4964-9429-ed95cadf99a3

Sisemine tunnus: 65/26/12

Menetluse liik: Väljakuulutamisega läbirääkimistega hankemenetlus / konkurentsipõhine läbirääkimistega hankemenetlus

Kiirendatud menetlus: ei

2.1.1. Eesmärk

Lepingu olemus: Asjad

Peamine liigitus (cpv): 48730000 Turvatarkvarapakett

Täiendav liigitus (cpv): 72000000 IT-teenused: nõuande-, tarkvaraarendus-, Interneti- ja tugiteenused

2.1.2. Lepingu täitmise koht

Linn: Rotenburg (Wümme)

Sihtnumber: 27356

Riik – jaotus (NUTS): Rotenburg (Wümme) (DE937)

Riik: Saksamaa

2.1.3. Maksumus

Eeldatav maksumus käibemaksuta: 840 000,00 EUR

2.1.4. Üldine teave

Õiguslik alus:

Direktiiv 2014/24/EL

2.1.6. Kõrvaldamise alused

Väljajätmise aluste allikad: Teade

Ainult siseriiklikest kõrvalejätmise alustest tulenevate kohustuste rikkumine: Gemäß § 123, 124 GWB, § 57, 42 Abs. 1 VgV und § 16 VOB/A

5. Osa

5.1. Osa: LOT-0001

Pealkiri: Einführung und der Betrieb EDR/XDR & Managed Security Operations Center (SOC)
Kirjeldus: Der Landkreis Rotenburg (Wümme) beabsichtigt, seine Kapazitäten zur Erkennung, Analyse und Abwehr von komplexen Cyberangriffen signifikant zu stärken.

Auftragsgegenstand ist die Einführung und der Betrieb einer modernen, integrierten Sicherheitslösung, die aus einer Technologieplattform und darauf aufbauenden Managed Services besteht, der zusätzlich einen „Incident Response“-Service samt eventuell nötiger Forensik beinhaltet.

Sisemine tunnus: 3c04df01-3767-4609-9fb3-a220e6dedbdf

5.1.1. Eesmärk

Lepingu olemus: Asjad

Peamine liigitus (cpv): 48730000 Turvatarkvarapakett

Täiendav liigitus (cpv): 72000000 IT-teenused: nõuande-, tarkvaraarendus-, Interneti- ja tugiteenused

5.1.2. Lepingu täitmise koht

Linn: Rotenburg (Wümme)

Sihtnumber: 27356

Riik – jaotus (NUTS): Rotenburg (Wümme) (DE937)

Riik: Saksamaa

5.1.3. Eeldatav kestus

Muu kestus: Teadmata

5.1.4. Uuendamine

Maksimaalne lepingu uuendamiste arv: 1

Muu informatsioon uuendamise kohta: Mit Beginn der Betriebsphase läuft der Vertrag 36 Monate ("Grundlaufzeit") und endet ohne weiteres mit Ablauf des letzten Tages der Grundlaufzeit bzw. der Verlängerungszeit. Der Auftraggeber hat das einmalige Recht, die Grundlaufzeit um ein Jahr zu verlängern ("Verlängerungszeit"). Von diesem Recht muss er spätestens drei Monate vor Ablauf der Grundlaufzeit in Textform gegenüber dem Auftragnehmer Gebrauch machen.

5.1.6. Üldine teave

Reserveeritud osalemine:

Osalemine ei ole reserveeritud.

Hankeprojekt, mida ei rahastata ELi vahenditest

Hanke suhtes kohaldatakse riigihankelepingut (GPA): jah

See hange sobib ka väikestele ja keskmise suurusega ettevõtjatele (VKEd): ei

5.1.7. Strateegilised hanked

Strateegilise hanke eesmärk: Ei kohaldata strateegilist hanget

5.1.9. Kvalifitseerimistingimused

Valikukriteeriumide allikad: Teade

Kriteerium: Viited määratud teenustele

Valikukriteeriumi kirjeldus: Der Bewerber hat mindestens zwei Referenzen über Leistungen nachzuweisen, die mit der zu vergebenden Leistung vergleichbar sind (Implementierung und Betrieb eines MSOC-Dienstes als EDR (Endpoint Detection and Response) bzw. XDR (Extended Detection and Response) unter Nutzung eines System zur Sicherheitsinformations- und Ereignisüberwachung mit Vorfallreaktion und Incident Response-Unterstützung. Die Leistungserbringung muss in den letzten vier Jahren erfolgt sein. Der Auftrag muss nicht abgeschlossen sein, sondern kann zum Zeitpunkt der Antragsabgabe fort dauern. Die Leistung muss für die Anerkennung der zum Zeitpunkt der Antragabgabe bereits seit mindestens 12 Monate erbracht worden sein. Zusätzlich sollen die Bewerber mit dem Teilnahmeantrag weitere Referenzen einreichen, die als Auswahlkriterium der Bieter dienen können. Je Referenz sind mindestens anzugeben (bei Bewerbungsgemeinschaften von jedem Mitglied): Auftraggeber, Leistungsgegenstand, Leistungszeitraum, Leistungsart sowie ein ungefähres Auftragsvolumen. Der Bewerber soll je Referenz einen fachlichen Ansprechpartner des Auftraggebers benennen. Sofern die Benennung eines Ansprechpartners zum Zeitpunkt der Angebots- bzw. Teilnahmeantragsabgabe nicht möglich ist, ist dieser auf Anforderung des Auftraggebers im weiteren Verfahren nachzureichen. Erfolgt dies trotz Aufforderung nicht, kann der Bewerber vom Verfahren ausgeschlossen werden. Datenschutzrechtlicher Hinweis: Für die übermittelten Daten zu den Ansprechpartnern werden vertrauliche Behandlung und die Verwendung nur im Rahmen dieser Ausschreibung seitens des Auftraggebers zugesichert. Die Details finden sich in den Blättern zu den Referenzen. Der Auftraggeber behält sich vor, die angegebenen Referenzen zu verifizieren. Zum Nachweis verwenden Sie bitte das "Formblatt Kunden-Referenzen.xlsx". Die Bewerber erhalten je Referenz maximal 1.000 Punkte. Das genaue Bewertungsschema entnehmen Sie bitte dem entsprechenden Abschnitt der Ausschreibungsunterlagen zum Teilnahmewettbewerb. Maximal erhalten die Bewerber für alle Referenzen 5.000 Punkte. Sollte ein Bewerber mehr als fünf Referenzen einreichen, bewertet der Auftraggeber nur die besten fünf Referenzen. Eine Referenz wird als gültig erachtet, wenn alle formalen Mindestanforderungen erfüllt sind und mindestens 650 von 1.000 Punkten erreicht werden.

Kriteeriume kasutatakse menetluse teise etappi kutsutavate taotlejate väljavalimiseks

Kaal (punktid, täpne): 500,00

Kriteerium: Keskmise aastane tööjõud

Valikukriteeriumi kirjeldus: Der Bewerber muss mitteilen, wie viele MSOC-Analysten dem Auftragnehmer für die Leistungserbringung zur Verfügung stehen. Die Definition von MSOC-Analysten entnehmen Sie bitte der Leistungsbeschreibung. Der Bieter weist nach, dass alle genannten MSOC-Analysten mindestens über eines der nachfolgend aufgeführten Personenzertifizierungen oder über vergleichbare Zertifikate mit Schwerpunkt Security Incident Management verfügen: Certified Information Systems Security Professional (CISSP) Certified Information Security Manager (CISM) Certified Ethical Hacker (CEH) TeleTrust Information Security Professional (T.I.S.P.) Cyber Security Expert (CSE) Cyber Security Professional (CSP) Datenschutzrechtlicher Hinweis: Für die übermittelten Daten zu den Ansprechpartnern werden vertrauliche Behandlung und die Verwendung nur im Rahmen dieser Ausschreibung seitens des Auftraggebers zugesichert. Zum Nachweis verwenden Sie bitte das ""Formblatt Mitarbeiter-Referenzen.xlsx"". Für jeden MSOC-Analysten, über den der Bewerber verfügt (Vollzeitäquivalent/FTE) und für den er eine der genannten Personenzertifizierungen oder vergleichbaren Zertifikate nachweist, erhält der Bewerber 50

Punkte. Maximal erhält ein Bewerber in diesem Auswahlkriterium 500 Punkte (bei 10 MSOC-Analysten, die über eine der genannten Personenzertifizierungen oder vergleichbaren Zertifikaten verfügen).

Kriteeriume kasutatakse menetluse teise etappi kutsutavate taotlejate väljavalimiseks
Kaal (punktid, täpne): 500,00

Kriteerium: Viited määratud teenustele

Valikukriteeriumi kirjeldus: "Der Bewerber hat mindestens zwei Referenzen über Leistungen nachzuweisen (bei Bewerbergemeinschaften von mindestens einem Mitglied), die mit der zu vergebenden Leistung hinsichtlich Implementierung und/oder Betrieb eines EDR/XDR-gestützten Security Monitorings bzw. eines System zur Sicherheitsinformations- und Ereignisüberwachung mit Vorfallreaktion mit Managed-SOC-Services und Incident-Response-Unterstützung vergleichbar sind. Die angegebenen Referenzen sollen hinsichtlich Umfang, Komplexität und Leistungsinhalt mit der ausgeschriebenen Leistung vergleichbar sein. Die Leistungserbringung muss nach dem 01.01.2022 erfolgt sein. Der Auftrag muss nicht abgeschlossen sein, sondern kann zum Zeitpunkt der Antragsabgabe fort dauern. Die Leistung muss für die Anerkennung der zum Zeitpunkt der Antragabgabe bereits seit mindestens 12 Monate erbracht worden sein. Je Referenz sind mindestens anzugeben: Auftraggeber, Leistungsgegenstand, Leistungszeitraum, Leistungsart sowie ein ungefähres Auftragsvolumen. Der Bewerber soll je Referenz einen fachlichen Ansprechpartner des Auftraggebers benennen. Sofern die Benennung eines Ansprechpartners zum Zeitpunkt der Angebots- bzw. Teilnahmeantragsabgabe nicht möglich ist, ist dieser auf Anforderung des Auftraggebers im weiteren Verfahren nachzureichen. Erfolgt dies trotz Aufforderung nicht, kann der Bewerber vom Verfahren ausgeschlossen werden. Datenschutzrechtlicher Hinweis: Für die übermittelten Daten zu den Ansprechpartnern werden vertrauliche Behandlung und die Verwendung nur im Rahmen dieser Ausschreibung seitens des Auftraggebers zugesichert. Der Auftraggeber behält sich vor, die angegebenen Referenzen zu verifizieren. Eine Referenz muss als Auftraggeber einen öffentliche Auftraggeber i.S.d. §99 GWB ausweisen. Nachzuweisen sind mindestens zwei vergleichbare Aufträge. Für den Fall, dass ein Bewerber einzelne Unternehmen als Nachunternehmer einsetzen möchte, wird auf die Möglichkeit der Eignungsleihe und die in § 47 VgV genannten Voraussetzungen hingewiesen. Wenn und soweit sich der Bewerber auf die Eignung eines anderen Unternehmens beruft, ist mit dem Angebot insbesondere eine Verpflichtungserklärung des anderen Unternehmens einzureichen, dass dieses seine Ressourcen und Kapazitäten dem Bewerber im Auftragsfall zur Verfügung stellt. Bei der Eignungsprüfung werden Bewerbergemeinschaften als Ganzes betrachtet. Bewerber sollen die auf der Vergabeplattform hinterlegten Vordrucke verwenden. Der Auftraggeber behält sich vor, Unterlagen im Rahmen des § 56 Abs. 2 VgV nachzufordern. Hierauf besteht kein Rechtsanspruch."

Kriteeriume kasutatakse menetluse teise etappi kutsutavate taotlejate väljavalimiseks
Tähtsuse järjekord: 0,00

Kriteerium: Muud majanduslikud või finantsnõuded

Valikukriteeriumi kirjeldus: Die Bewerber / Bewerbergemeinschaften müssen ihre wirtschaftliche und finanzielle Leistungsfähigkeit nachweisen. Dabei müssen die folgenden genannten Anforderungen im Falle einer Bewerbergemeinschaft durch die Bewerbergemeinschaft insgesamt erfüllt sein. Für die Beurteilung der wirtschaftlichen und finanziellen Leistungsfähigkeit einer Bewerbergemeinschaft wird die Bewerbergemeinschaft als Ganzes beurteilt. Es ist daher ausreichend, wenn mindestens ein Mitglied der Bewerbergemeinschaft die geforderten Erklärungen und Nachweise erbringt. Der Bewerber hat seinen Gesamtumsatz sowie den Umsatz mit Leistungen, die mit der ausgeschriebenen

Leistung vergleichbar sind, für die letzten drei abgeschlossenen Geschäftsjahre anzugeben. Der Auftraggeber behält sich vor, zum Nachweis Jahresabschlüsse oder vergleichbare Unterlagen nachzufordern. Der Auftragnehmer bestätigt, dass der Umsatz in den letzten drei Geschäftsjahren mindestens einen durchschnittlichen Umsatz im Bereich MDR/SOC Dienstleistungen in Höhe von 1 Mio. € netto erreicht hat. Der Auftragnehmer muss die Unternehmensstruktur, dabei mindestens die folgenden Kriterien, transparent nachweisen: Unternehmensbeschreibung gegliedert nach: a) Geschäftsstruktur b) Gründungsjahr c) Hauptgeschäftsbereich d) Hauptsitz e) Anzahl Mitarbeiter gesamt
Kriteriume kasutatakse menetluse teise etappi kutsutavate taotlejate väljavalimiseks
Tähtsuse järjekord: 0,00

Kriteerium: Turvalisus klassifitseeritud teabe töötlemiseks, salvestamiseks ja edastamiseks
Valikukriteeriumi kirjeldus: "Der Sitz der Gesellschaft des Bewerbers und gegebenenfalls von Subunternehmern ist und bleibt während der gesamten Vertragslaufzeit innerhalb der EWR, der Schweiz oder Großbritannien. Die angebotenen Managed-SOC-Services einschließlich Analyse, Eskalation und operativer Kommunikation werden aus dem EWR, der Schweiz oder Großbritannien erbracht. Der Bewerber muss in der Lage sein, im Bedarfsfall Vor-Ort-Leistungen am Standort des AG zu erbringen. Sämtliche im Rahmen der Leistungserbringung verarbeiteten sicherheitsrelevanten Daten sind ausschließlich innerhalb des EWRs, der Schweiz oder Großbritannien zu speichern und zu verarbeiten. Dies gilt auch für sämtliche Unterauftragnehmer und sonstige Dritte, die Zugriff auf diese Daten erhalten. Der Bewerber stellt während der gesamten Vertragslaufzeit feste, deutschsprachige Ansprechpartner für die Rollen Projektleitung sowie Service Delivery Management bereit. Für die Implementierungsphase ist ein verantwortlicher Projektleiter zu benennen. Für den Regelbetrieb ist ein fester Service Delivery Manager zu benennen. Beide verfügen über ein Sprachniveau entsprechend dem Level C2 nach dem Gemeinsamen Europäischen Referenzrahmen. Darüber hinaus muss gewährleistet sein, dass die Kommunikation in Incident-, Eskalations- und Betriebsfällen in deutscher Sprache auf dem Level C1 erfolgen kann. Der Bewerber erklärt, dass er als AN über die gesamte Vertragslaufzeit ausschließlich Mitarbeiter im Analyseteam einsetzen wird, die in der deutschen Sprache über ein Sprachniveau entsprechend dem Level C1 oder höher nach dem Gemeinsamen Europäischen Referenzrahmen verfügen. Der Bewerber muss einen Managed Service für EDR/XDR-System zur Sicherheitsinformations- und Ereignisüberwachung mit Vorfallreaktion und SOC-Leistungen entsprechend der Leistungsbeschreibung bereitstellen. Dies umfasst den Betrieb notwendiger Systeme sowie die kontinuierliche Überwachung und Bearbeitung sicherheitsrelevanter Ereignisse im 24/7-Betrieb anhand abgestimmter Kommunikations-, Ticket- und Eskalationsprozesse.
Kriteriume kasutatakse menetluse teise etappi kutsutavate taotlejate väljavalimiseks
Tähtsuse järjekord: 0,00

Kriteerium: Kvaliteedi tagamise meetmed
Valikukriteeriumi kirjeldus: Fully-Managed Betriebsmodell 1. Der Bewerber erklärt, die operative Verantwortung für die Erkennung, Analyse und Reaktion auf Sicherheitsvorfälle an den externen Dienstleister (MSOC-Anbieter) zu übernehmen. 2. Der Bewerber erklärt als ausgelagertes, hochspezialisiertes Sicherheitsteam zu agieren, das die technologische Plattform (EDR/XDR) nicht nur überwacht, sondern auch proaktiv managt und im Ernstfall direkt eingreift. Das Ziel ist es, den AG maximal zu entlasten, sodass sich dessen interne IT-Ressourcen auf ihre Kernaufgaben und strategische Projekte konzentrieren können. 3. Der Bewerber erklärt, dass er als AN den AG über die gesamte Vertragslaufzeit im Rahmen des MSOC-Service bei der Weiterentwicklung, Optimierung und Migration von Use-Cases

unterstützt. Der Bewerber erklärt sich damit einverstanden, dass die maximale Reaktionszeit des AN auf Alarmer der Priorität ""P1 – kritisch"" rund um die Uhr (24/7) maximal 60 Minuten beträgt, mit einer initialen Antwortzeit innerhalb dieser einen Stunde ab Eingang des Alarms oder ab Meldung durch den Auftraggeber. Kritische Alarmer betreffen einen potentiell schwerwiegenden Sicherheitsvorfall. Als ""schwerwiegend"" wird ein IKT-bezogener Vorfall mit potenziell weitreichenden negativen Auswirkungen auf die Schutzziele von Netz- und Informationssystemen, die kritische Funktionen oder Geschäftsprozesse der ILB unterstützen, oder auf die Fähigkeit des LK-RoW, aufsichtsrechtliche Anforderungen zu erfüllen, bezeichnet. Hierzu zählen auch Datenverluste, die besonders schutzwürdige Daten im Sinne der DSGVO (Art. 9) betreffen. Die Reaktionszeit beginnt mit der automatischen Erstellung eines Alarms oder durch eine Meldung seitens des AG. Sie umfasst eine qualifizierte Bewertung des Incidents durch einen MSOC-Analysten sowie die Einleitung geeigneter Maßnahmen, einschließlich der Benachrichtigung des AG innerhalb der ersten Stunde über die im Onboarding definierten Meldewege. Ergänzung: Üblicherweise gehen wir von 4 Tiers oder Stufen für die Beschreibung von Erfahrung, Kompetenz und Verantwortung von Analysten aus. Sollten Sie intern eine andere Stufung haben, so bitten wir um Darstellung der Zuordnungen ihrer Ebenen zu den Tiers 1-4 unter Beachtung der weiterhin gültigen Reaktionszeit von 1 h für kritische Alarmer - P1. Entscheidend und vertraglich bindend ist die Einhaltung der für die Prioritätsstufen des Auftraggebers geforderten Service Level Agreements und Maßnahmen. Direkte aktive Maßnahmen dürfen ausschließlich im vorab vereinbarten Umfang erfolgen. Der Bewerber muss in der Lage sein, Maßnahmen zur Eindämmung und Reaktion auf Sicherheitsvorfälle umzusetzen. Die Umsetzung aktiver Maßnahmen hat auf Basis abgestimmter Prozesse, Playbooks und Freigaben zu erfolgen. Der Bewerber muss in der Lage sein, weitergehende Incident-Response-Leistungen, einschließlich Post-Breach-Forensik, sowohl remote als auch vor Ort beim AG zu erbringen. On-prem bzw. kundenseitig betriebene Komponenten des angebotenen Service müssen in einem sicheren und abgestimmten Betriebsmodell durch den Bewerber aus der Ferne überwacht und administrativ betreut werden können. Der hierfür erforderliche Zugriff ist sicher, nachvollziehbar und rollenbasiert auszugestalten. Kundenspezifisch für den Auftraggeber erstellte Use Cases, Playbooks, Regelwerke, Konfigurationen, Dokumentationen und sonstige individuell entwickelte Artefakte verbleiben im Eigentum bzw. im uneingeschränkten Nutzungsrecht des Auftraggebers und sind diesem spätestens bei Vertragsende in nutzbarer und nachvollziehbarer Form zu übergeben. Der Bewerber muss mit dem Angebot einen realistischen Implementierungs- und Onboarding-Plan vorlegen, der Projektstart, Wellenmodell, Abhängigkeiten, Testphase, Übergang in den Regelbetrieb sowie AG-seitige Mitwirkungen transparent darstellt. Der Bewerber muss in der Lage sein, die gemeinsam priorisierten Welle-1-Quellen innerhalb eines mit AG abgestimmten Zielzeitraums produktiv zu überführen und entsprechend dem Betriebsmodell zu überwachen.

Kriteeriume kasutatakse menetluse teise etappi kutsutavate taotlejate väljavalimiseks

Tähtsuse järjekord: 0,00

Kriteerium: Teabe turvalisus

Valikukriteeriumi kirjeldus: Der Bewerber hat den Nachweis zu erbringen, dass für die zur Leistungserbringung eingesetzten Organisationseinheiten ein Informationssicherheitsmanagementsystem nach ISO/IEC 27001:2022 bzw. ISO/IEC 27001:2019 oder nach ISO27001 auf Basis IT-Grundschutz BSI und/oder BSI C5:2020 eingerichtet ist und betrieben wird. Der Geltungsbereich des Informationssicherheitsmanagementsystems (ISMS) des AN schließt alle Prozesse und IT-Assets des SOC-Dienstes mit ein. Der Nachweis kann durch ein gültiges Zertifikat oder gleichwertige Unterlagen erbracht werden. Der Bewerber erklärt, sich als AN zu verpflichten, dass seine Mitarbeiter die IS-Richtlinien,

Prozesse und Protokolle des AG zur Informations- und IKT-Sicherheit einhalten. "Der Bewerber erklärt, dass er als AN gewährleistet, die Datenspeicherungsanforderungen des AG zu erfüllen, indem die für Detection, Analyse, Nachvollziehbarkeit und forensische Rückverfolgung erforderlichen sicherheitsrelevanten Daten für einen Zeitraum von mindestens 180 Tagen verfügbar und zugreifbar sind. Diese Anforderung bezieht sich auch auf durch den Bewerber selbst betriebene Systeme zur Erbringung des MSOC Service. Der Bewerber muss erklären, in den letzten drei abgeschlossenen Geschäftsjahren durchschnittlich mindestens 10 Mitarbeiter (Vollzeitäquivalent) im Managed Security Operations Center (MSOC) zu beschäftigen. Diese müssen im Bereich SOC Analyse tätig sein (Level 1 - Monitoring und /oder Level 2 - Analyse). Der Bewerber erklärt sich damit einverstanden, dass die Anzahl an Incidents pro Monat ebenso unbegrenzt ist wie der Aufwand pro Incident.

Kriteeriume kasutatakse menetluse teise etappi kutsutavate taotlejate väljavalimiseks

Tähtsuse järjekord: 0,00

Kriteerium: Alltöövõtu osakaal

Valikukriteeriumi kirjeldus: Der Landkreis Rotenburg (Wümme) unterliegt als Körperschaft des öffentlichen Rechts besonderen regulatorischen Anforderungen. In der Folge muss der Landkreis Rotenburg (Wümme) stets eine hohe Verlässlichkeit ihrer IT-Sicherheitsinfrastruktur und des IKT-Risikomanagements gewährleisten. Der AG muss stets eine hohe Verlässlichkeit seiner IT-Systeme und IT-Sicherheitsinfrastruktur gewährleisten. Gemäß der regulatorischen Vorgaben und in Anlehnung an §47 VgV hat der Bewerber zu erklären, dass er die ausgeschriebenen Leistungen zu mindestens 50 % als Eigenleistung erbringt. Die Eigenleistungsquote bemisst sich nach dem Anteil der durch den Auftragnehmer selbst bearbeiteten Alarme an der Gesamtzahl der Alarme innerhalb des Leistungszeitraums und umfasst alle Stufen der Alarm- und Vorfallsbearbeitung (Tier1-4). Eine Weitergabe von mehr als 50 % der Leistungen an Subunternehmer ist unzulässig. Der Bewerber bestätigt diese Anforderung durch Unterzeichnung der beigefügten Eigenerklärung. Soweit sich der Bewerber zum Nachweis seiner Eignung auf Kapazitäten anderer Unternehmen stützt, hat er mit dem Teilnahmeantrag die hierfür erforderlichen Nachweise und Verpflichtungserklärungen vorzulegen, aus denen hervorgeht, dass ihm die entsprechenden Mittel im Auftragsfall tatsächlich zur Verfügung stehen.

Kriteeriume kasutatakse menetluse teise etappi kutsutavate taotlejate väljavalimiseks

Tähtsuse järjekord: 0,00

Kriteerium: Kvaliteedi tagamise meetmed

Valikukriteeriumi kirjeldus: Der Landkreis Rotenburg (Wümme) unterliegt als Körperschaft des öffentlichen Rechts besonderen regulatorischen Anforderungen. In der Folge muss der Landkreis Rotenburg (Wümme) stets eine hohe Verlässlichkeit ihrer IT-Sicherheitsinfrastruktur und des IKT-Risikomanagements gewährleisten. Der AG muss stets eine hohe Verlässlichkeit seiner IT-Systeme und IT-Sicherheitsinfrastruktur gewährleisten. Als Eignungsnachweis hat der Bewerber sicherzustellen, dass zum Zeitpunkt des Vertragsabschlusses für sämtliche im Rahmen dieses Auftrags eingesetzte Schlüsselpersonen und Analysten ein gültiges Führungszeugnis vorliegt. Das Führungszeugnis muss mindestens dem einfachen Führungszeugnis (§ 30 BZRG) entsprechen, vergleichbar bzw. höherwertig sein. Durch eine Eigenerklärung sichert der Bewerber zu, dass er einen Prozess zur Überprüfung der personellen Zuverlässigkeit für das gesamte eingesetzte Personal etabliert hat und für die gesamte Vertragslaufzeit aufrecht erhält. Die Führungszeugnisse müssen nicht vorgelegt werden. Der Bewerber erklärt, dass er über Systeme zur verschlüsselten E-Mail-Kommunikation verfügt, die PGP (Pretty Good Privacy) oder alternativ S/MIME (Secure /Multipurpose Internet Mail Extensions) unterstützen und diese während der

Auftragserbringung einsetzt. Alternative technische Lösungen zur E-Mail-Verschlüsselung mittels PGP oder S/MIME werden als technisch gleichwertig akzeptiert, sofern sie dieses Schutzziel nachweislich erfüllen (z.B. TLS gesicherte Serviceportale oder Ticketsysteme mit starker Authentifizierung). Die Verfügbarkeit ist durch eine Eigenerklärung oder ein technisches Konzept nachzuweisen, das den Einsatz solcher Systeme beim Bewerber beschreibt. Der Bewerber erklärt, dass er als AN gewährleistet, den angebotenen Managed Security Operations Center (MSOC)-Dienst an 7 Tagen pro Woche, 24 Stunden pro Tag, ganzjährig (24/7/365) ohne Einschränkung bereitzustellen. Die Betriebszeit umfasst die kontinuierliche Überwachung, Analyse sicherheitsrelevanter Ereignisse, Übergabe an den Incident Response Prozess, sowie die Kommunikation mit dem Auftraggeber gemäß den vereinbarten Eskalations- und Reaktionszeiten. Der Bewerber hat mit dem Angebot eine Eigenerklärung abzugeben, aus der hervorgeht, dass der angebotene Dienst uneingeschränkt im 24/7/365-Modus erbracht wird. Der Bewerber weist für den angebotenen MSOC-Dienst eine durchschnittliche Jahresverfügbarkeit von mindestens 99% nach. Die Verfügbarkeit berechnet sich auf Basis des gesamten Kalenderjahres (8760 Stunden) und bezieht sich auf die Betriebszeiten des Dienstes gemäß der in den Angebotsunterlagen beschriebenen Leistung. Berechnung: $((\text{Gesamte Serviceminuten}) - (\text{Gesamte Ausfallminuten})) / \text{Gesamte Serviceminuten}$. Die vollumfängliche Verfügbarkeit des SOC Services umfasst dabei auch alle technischen Komponenten, die für die Erbringung notwendig sind, insb. alle vom AN genutzten und bereitgestellten Systemkomponenten wie z.B. SIEM, NIDS, Threat Intelligence Feeds etc. Mit welchen technologischen Mitteln der AN alle geforderten Schutzziele vollumfänglich erfüllt, obliegt dem AN. Die maximale Ausfallzeit bis zur Wiederherstellung der vollumfänglichen SOC Services inkl. aller dafür vom AN bereitgestellten und genutzten Systemkomponenten wie z.B. SIEM, OT NIDS oder Threat Intelligence Feeds darf 24 Stunden nicht überschreiten. Der Nachweis ist durch geeignete Unterlagen zu erbringen, z.B.: eine Eigenerklärung zur durchschnittlichen Verfügbarkeit auf Basis von Betriebsdaten der letzten 12 Monate, oder durch Referenznachweise aus vergleichbaren Projekten, aus denen die Einhaltung dieser Verfügbarkeit hervorgeht.

Kriteriume kasutatakse menetluse teise etappi kutsutavate taotlejate väljavalimiseks
Tähtsuse järjekord: 0,00

Kriteerium: Professionaalne riski hüvitis kindlustus

Valikukriteeriumi kirjeldus: "Der Bewerber hat eine Betriebshaftpflichtversicherung mit einer angemessenen Deckungssumme für Personen-, Sach- und Vermögensschäden nachzuweisen. Die Deckungssumme soll in der Regel mindestens 3 Mio. EUR für Sachschäden und mindestens 0,5 Mio. EUR für Personenschäden betragen. Die Zusicherung der Haftpflichtversicherung in der geforderten Höhe muss im Teilnehmerwettbewerb erfolgen. Der Versicherungsnachweis muss spätestens vor der Beauftragung vorliegen. Der Auftraggeber behält sich vor, im Einzelfall höhere Deckungssummen zu verlangen, sofern dies durch das Risikoprofil der Leistung gerechtfertigt ist."

Kriteriume kasutatakse menetluse teise etappi kutsutavate taotlejate väljavalimiseks
Tähtsuse järjekord: 0,00

Kriteerium: Teabe turvalisus

Valikukriteeriumi kirjeldus: Der Bewerber erklärt sich bereit, als AN das ITSM-Tool des AG (OTRS community edition) für die Bearbeitung von Security Incident Tickets mit zuverwenden (z.B über eine API), sobald der AG zu involvieren ist, neben den sonstigen Kommunikationswegen, die im Implementierungsprojekt zwischen AN und AG noch anhand der Incident-Kritikalitäten zu erarbeiten. Der Bewerber erklärt sich bereit, als AN an den regelmäßig stattfindenden Notfalltests bzw. Cyberübungen (im Sinne eines simulierten

Angriffs) im Rahmen der Leistungserbringung des Managed Service teilzunehmen. In der Regel werden diese Tests 1 (ein) mal im Jahr durchgeführt. Der AN weist mindestens einen Mitarbeitenden in der Rolle aus, für den ein Skill-Level Senior Analyst Level 3 (Tier-3) oder Senior Threat Hunting Expert zutrifft. Die personelle Besetzung dieser Rolle ist über die gesamte Vertragslaufzeit durch den AN zu gewährleisten. Der Mitarbeitende ist der Deutschsprachig (mind. C1 Niveau). Der AN ist als APT-Response Dienstleister zusätzlich zu A17 gemäß BSI zertifiziert. Sofern die Erfüllung dieses Kriteriums über eine Eignungsleihe abgedeckt wird, sind hierfür im Angebot die entsprechenden Nachweise (Zertifikat des Nachunternehmers) und eine Verpflichtungserklärung bei Abgabe der Unterlagen für den Teilnehmerwettbewerb vorzulegen. Aus der Erklärung muss unzweideutig hervorgehen, dass der zertifizierte Dritte sich verpflichtet, dem Auftraggeber im Auftragsfall seine zertifizierte Dienstleistung vollumfänglich zur Verfügung zu stellen. Dabei ist auch hier das Mindestkriterium A23 zu beachten ("Eignungsleihe insgesamt kleiner 50%"). Das Mindestkriterium stellt keine funktionale Anforderung dar, kann nicht durch eine gleichwertige technische Umsetzung wie z.B. über eine Software erfüllt werden und wird keiner Gleichwertigkeitsprüfung unterzogen.

Kriteeriume kasutatakse menetluse teise etapi kutsutavate taotlejate väljalimiseks
Tähtsuse järjekord: 0,00

Kriteerium: Muud majanduslikud või finantsnõuded

Valikukriteeriumi kirjeldus: "Der Bewerber sichert zu, dass er sich und etwaige Subunternehmer vertraglich verpflichtet, dass personenbezogene Daten ausschließlich und vollständig innerhalb des EWR, der Schweiz oder Großbritanniens verarbeitet und gespeichert werden und alle Datenverarbeitungsvorgänge DSGVO-konform sind. Der Bewerber bestätigt, dass er die Anforderungen an Auftragsverarbeiter gemäß Art. 28 DSGVO erfüllt und geeignete technische und organisatorische Maßnahmen (TOM) implementiert hat. Die Beibringung der AVVs für alle Bestandteile der Dienstleistung wird nach Zuschlag und vor Vertragsabschluss fällig. Abweichungen von den vorgegebenen Datenschutzregelungen sind gesondert darzustellen und bedürfen der ausdrücklichen Zustimmung des Auftraggebers." "Der Bewerber stellt sicher, dass der angebotene Managed-SOC- und Incident-Response-Service den Auftraggeber bei der Einhaltung der gesetzlichen Meldepflichten gemäß der Richtlinie (EU) 2022/2555 (NIS2) unterstützt. Hierzu gehören insbesondere: - die Fähigkeit zur strukturierten Erfassung, Klassifizierung und Bewertung von Sicherheitsvorfällen im Hinblick auf deren Meldepflichtigkeit, - die Bereitstellung von Informationen und Auswertungen, die eine fristgerechte Meldung an zuständige Behörden ermöglichen (z. B. Erstmeldung, Zwischenmeldung, Abschlussbericht), - die Unterstützung bei der zeitlichen Einordnung von Vorfällen (z. B. Erkennung, Eskalation, Beginn des Vorfalls), - die Bereitstellung relevanter technischer und organisatorischer Informationen zur Vorfallsanalyse. Das entsprechende Vorgehen ist im Angebot nachvollziehbar zu beschreiben. Sofern der Bewerber diese Unterstützung nicht nachweisen kann, führt dies zum Ausschluss aus dem Vergabeverfahren."

Kriteeriume kasutatakse menetluse teise etapi kutsutavate taotlejate väljalimiseks
Tähtsuse järjekord: 0,00

Teave kaheetapilise menetluse teise etapi kohta:

Menetluse teise etapi kutsutavate taotlejate miinimumarv: 3

Menetluse teise etapi kutsutavate taotlejate maksimumarv: 5

Menetlus toimub järjestikuste etappidena. Igas etapis võidakse mõni osaleja kõrvaldada. Hankija jätab endale õiguse sõlmida leping esialgsete pakumuste alusel ilma edasiste läbirääkimisteta.

5.1.10. Pakkumuste hindamise kriteeriumid

Kriteerium:

Liik: Hind

Nimi: Preis

Kirjeldus: Maßgeblich ist das bewertungsrelevante Gesamt-Entgelt (netto) über drei Jahre für alle vertraglich zu erbringenden Leistungen. Das Angebot mit dem günstigsten bewertungsrelevanten Gesamt-Entgelt (netto) erhält 500 Punkte. Bieter mit einem Angebotspreis, der zumindest 200% über dem niedrigsten Angebotspreis liegt, erhalten 0 Punkte. Die Punktevergabe für alle anderen Bieter erfolgt durch lineare Interpolation zwischen dem niedrigsten Angebotspreis und einem um 100 % höheren Angebotspreis (doppelter Angebotspreis). Die Punkteanzahl der übrigen Angebote berechnet sich wie folgt: $\text{Punkte}(P) = 500 * (1 - ((P - P_{\min}) / (2 * P_{\min})))$ Beispiel: Günstigstes bewertungsrelevantes Gesamt-Entgelt Bestbieter A = 10000, Bewertungsrelevantes Gesamt-Entgelt Bieter B = 15000. Punktbewertung für bewertungsrelevantes Entgelt Bieter B: $500 * (1 - ((15000 - 10000) / (2 * 10000))) = 375$ Punkte (wo nötig, wird auf die zweite Nachkommastelle gerundet) Eine Punktzahl von weniger als 50% in einem der Wertungsbereiche führt zum Ausschluss des Anbieters.

Hindamise kaalukriteeriumi kategooria: Kaal (protsentides, täpne)

Hindamiskriteerium – arv: 50

Hindamise fikseeritud väärtusega kriteeriumi kategooria: Fikseeritud väärtus (kokku)

Hindamiskriteerium – arv: 500

Kriteerium:

Liik: Kvaliteet

Nimi: Leistungsbewertung gemäß Kriterienkatalog

Kirjeldus: Bewertung der Bereiche Technik, MSOC-Service, Incident Response-Service anhand der im Kriterienkatalog festgelegten Maßstäbe. Details sind den Vergabeunterlagen zu entnehmen. Ein Anbieter wird ausgeschlossen, wenn er in einem der Wertungsbereiche weniger als 50% der Punktzahl erreicht.

Hindamise kaalukriteeriumi kategooria: Kaal (protsentides, täpne)

Hindamiskriteerium – arv: 50

Hindamise fikseeritud väärtusega kriteeriumi kategooria: Fikseeritud väärtus (kokku)

Hindamiskriteerium – arv: 500

5.1.11. Hankedokumendid

Keeled, milles hankedokumendid on ametlikult kättesaadavad: saksa keel

Lisateabe taotlemise tähtaeg: 08/06/2026 10:00:00 (UTC+02:00) Ida-Euroopa aeg, Kesk-Euroopa suveaeg

Hankedokumentide aadress: <https://bieterzugang.deutsche-evergabe.de/evergabe.bieter/api/supplier/external/deeplink/subproject/aa143b10-ac56-48da-8c26-6de21d882846>

5.1.12. Hanke tingimused**Menetluse tingimused:**

Eeldatav kuupäev, millal saadetakse pakkumuste esitamise ettepanek: 03/07/2026

Esitamise tingimused:

Elektrooniline esitamine: Nõutav

Esitamise aadress: <https://bieterzugang.deutsche-evergabe.de/evergabe.bieter/api/supplier/external/deeplink/subproject/aa143b10-ac56-48da-8c26-6de21d882846>

Keeled, milles võib pakkumusi või osalemistaotlusi esitada: saksa keel

Elektrooniline kataloog: Ei ole lubatud

Variandid: Ei ole lubatud

Pakkujad võivad esitada rohkem kui ühe pakkumuse: Ei ole lubatud

Osalemistaotluste esitamise tähtaeg: 15/06/2026 10:00:00 (UTC+02:00) Ida-Euroopa aeg, Kesk-Euroopa suveaeg

Teave, mida saab pärast esitamise tähtaega täiendada:

Ostja äranägemisel võib kõik puuduvad pakujaga seotud dokumendid esitada hiljem.

Lisateave: Gemäß § 56 Abs. 2 VgV, § 51 Abs. 2 SektVO, § 16a Abs. 1 VOB/A-EU. Mögliche Hinweise des Auftraggebers in den Vergabeunterlagen sind zu beachten.

Lepingutingimused:

Lepingu täitmine peab toimuma kaitstud tööhõive programmide raames: Ei

Vajalik on konfidentsiaalsuskokkulepe: jah

Lisateave konfidentsiaalsuskokkuleppe kohta: Der vollständige Kriterienkatalog mit den Zuschlagskriterien für die Angebotsphase wird mit der Aufforderung zur Abgabe eines Erstangebotes unter Berücksichtigung der einzureichenden Verschwiegenheitserklärung zur Verfügung gestellt. Auf Anfrage wird dieser bereits vorab im Teilnahmewettbewerb zur Verfügung gestellt. Hierzu ist gemäß § 41 Abs. 3 VgV zum Schutz der Vertraulichkeit von Informationen die Abgabe der anliegenden Verschwiegenheitserklärung erforderlich. Diese ist über die Bieterkommunikation mit der Bitte um Übersendung des vollständigen Kriterienkataloges einzureichen.

E-arveldamine: Nõutav

Kasutatakse elektroonilisi tellimusi: jah

Kasutatakse elektroonilisi makseid: jah

Rahastamiskord: EVB-IT- Vertrag, VOL/B

5.1.15. Vahendid

Raamleping:

Ei kohaldata raamlepingut

Teave dünaamilise hankesüsteemi kohta:

Ei kohaldata dünaamilist hankesüsteemi

5.1.16. Lisateave, lepitus ja vaidlustus

Vaidlustusorgan: Vergabekammer Niedersachsen beim Nds. Ministerium für Wirtschaft, Verkehr, Bauen und Digitalisierung

Teave vaidlustamise tähtaegade kohta: Gemäß § 160 Abs. 1 GWB leitet die Vergabekammer ein Nachprüfungsverfahren nur auf Antrag ein. Der Antrag ist unzulässig, soweit der Antragsteller den geltend gemachten Verstoß gegen Vergabevorschriften vor Einreichen des Nachprüfungsantrags erkannt und gegenüber dem Auftraggeber nicht innerhalb einer Frist von 10 Kalendertagen gerügt hat; der Ablauf der Frist nach § 134 Absatz 2 bleibt unberührt (§ 160 Abs. 3 Nr.1GWB). Der Nachprüfungsantrag ist gemäß § 160 Abs. 3 Nr. 2 GWB ebenfalls unzulässig, soweit Verstöße gegen Vergabevorschriften, die aufgrund der Bekanntmachung erkennbar sind, nicht spätestens bis zum Ablauf der in der Bekanntmachung benannten Frist zur Bewerbung oder zur Angebotsabgabe gegenüber dem Auftraggeber gerügt werden. Der Vergabenachprüfungsantrag ist ferner nach § 160 Abs. 3 Nr. 3 GWB unzulässig, soweit Verstöße gegen Vergabevorschriften, die erst in den Vergabeunterlagen erkennbar sind, nicht spätestens bis zum Ablauf der Frist zur Bewerbung oder zur Angebotsabgabe gegenüber dem Auftraggeber gerügt werden. Der Nachprüfungsantrag ist gemäß § 160 Abs. 3 Nr. 4 GWB schließlich dann unzulässig, soweit mehr als 15 Kalendertage nach Eingang der Mitteilung des Auftraggebers, einer Rüge nicht abhelfen zu wollen, vergangen sind. Für die weiteren Voraussetzungen der Zulässigkeit wird auf §§ 160 und 161 GWB verwiesen.

Organisatsioon, mis annab lisateavet hankemenetluse kohta: Landkreis Rotenburg - Zentrale Vergabestelle

8. Organisatsioonid

8.1. ORG-0001

Ametlik nimi: Landkreis Rotenburg (Wümme)
Registreerimisnumber: 4182c8b8-8884-4fb2-90cc-b7fbbdf4bde5
Postiaadress: Hopfengarten 2
Linn: Rotenburg (Wümme)
Sihtnumber: 27356
Riik – jaotus (NUTS): Rotenburg (Wümme) (DE937)
Riik: Saksamaa
E-posti aadress: vergabe@lk-row.de
Telefon: +49 4261983-0
Faks: +49 4261983-2199
Internetiaadress: <http://www.lk-row.de>
Selle organisatsiooni rollid:
Hankija

8.1. ORG-0002

Ametlik nimi: Vergabekammer Niedersachsen beim Nds. Ministerium für Wirtschaft, Verkehr,
Bauen und Digitalisierung
Registreerimisnumber: 7018baaf-0131-4475-b6fa-4ada30549563
Postiaadress: Auf der Hude 2
Linn: Lüneburg
Sihtnumber: 21339
Riik – jaotus (NUTS): Lüneburg, Landkreis (DE935)
Riik: Saksamaa
E-posti aadress: vergabekammer@mw.niedersachsen.de
Telefon: +49 4131153308
Faks: +49 4131152943
Internetiaadress: <http://www.mw.niedersachsen.de>
Selle organisatsiooni rollid:
Vaidlustusorgan
Organisatsioon, mis annab lisateavet vaidlustamise kohta

8.1. ORG-0003

Ametlik nimi: Landkreis Rotenburg - Zentrale Vergabestelle
Registreerimisnumber: ac12f6e2-87ba-4113-8d09-b4a39c8c69f1
Postiaadress: Hopfengarten 2
Linn: Rotenburg (Wümme)
Sihtnumber: 27356
Riik – jaotus (NUTS): Rotenburg (Wümme) (DE937)
Riik: Saksamaa
E-posti aadress: vergabe@lk-row.de
Telefon: +49 4261983-0
Faks: +49 4261983-2199
Selle organisatsiooni rollid:
Organisatsioon, mis annab lisateavet hankemenetluse kohta

8.1. ORG-0004

Ametlik nimi: Datenservice Öffentlicher Einkauf (in Verantwortung des Beschaffungsamts des BMI)

Registreerimisnumber: 0204:994-DOEVD-83

Linn: Bonn

Sihtnumber: 53119

Riik – jaotus (NUTS): Bonn, Kreisfreie Stadt (DEA22)

Riik: Saksamaa

E-posti aadress: noreply.esender_hub@bescha.bund.de

Telefon: +49228996100

Selle organisatsiooni rollid:

TED eSender

10. Muudatus

Eelmise teate versioon, mida muudetakse

:

90a294f2-dafb-46ec-a942-f6926e042328-01

Muudatuse peamine põhjus

:

Hankija vea parandamine

Kirjeldus

:

Austausch der Datei "Anlage 1 Kriterienkatalog TNW"

Teave teate kohta

Teate tunnus/versioon: 558af8e0-42f9-4317-bb5d-121ff8a0517e - 01

Vormi liik: Hange

Teate liik: Hanketeade või kontsessiooniteade – üldkord

Teate alaliik: 16

Teate saatmise kuupäev: 19/05/2026 09:36:37 (UTC+02:00) Ida-Euroopa aeg, Kesk-Euroopa suveaeg

Keeled, milles käesolev teade on ametlikult kättesaadav: saksa keel

Teate avaldamise number: 346326-2026

ELT S väljaande number: 96/2026

Avaldamise kuupäev: 20/05/2026