Aufforderung zur Angebotsabgabe: Secure Access Service Edge (SASE) Plattform

Inhaltsübersicht

1. Einleitung und Hintergrund

[Name des Unternehmens] bittet um Angebote für eine umfassende Secure Access Service Edge (SASE)-Plattform zur Modernisierung unserer Netz- und Sicherheitsinfrastruktur. Diese Ausschreibung umreißt unsere Anforderungen an eine Cloud-native Lösung, die Netzwerkkonnektivität und Sicherheitsdienste zur Unterstützung unserer verteilten Belegschaft und unserer Cloud-first-Initiativen zusammenführt.

Organisation Hintergrund

- [Beschreiben Sie Ihr Unternehmen/Ihre Organisation]
- [Industrielle und gesetzliche Anforderungen]
- [Größe der Organisation und IT-Infrastruktur]

Aktuelles Umfeld

- [Aktuelle Netz- und Sicherheitsarchitektur]

-
- [Anzahl der Nutzer und Standorte]

Ziele des Projekts

- Implementierung einer einheitlichen, cloud-nativen SASE-Architektur
- Verbesserung des Sicherheitsniveaus durch integrierte Dienste
- Optimierung der Netzleistung und des Nutzererlebnisses
- Rationalisierte Verwaltung und Betrieb

2. Projektziele

1. Bereitstellung einer umfassenden SASE-Plattform, die integriert ist:
    - Software-definierte Weitverkehrsnetze (SD-WAN)
    - Security Service Edge (SSE)-Komponenten
    - Zero Trust Network Access (ZTNA)
    - Cloud-Sicherheitsdienste
2. Erzielen Sie die folgenden Ergebnisse:
    - Einheitliche Sicherheits- und Netzwerkinfrastruktur
    - Bessere Sichtbarkeit und Kontrolle
    - Verbesserte betriebliche Effizienz
    - Geringere Gesamtbetriebskosten
    - Skalierbare Cloud-native Architektur

3. Umfang der Arbeit

Erforderliche Komponenten

1. SD-WAN-Fähigkeiten
    - Optimierung des Netzes
    - Anwendungsorientiertes Routing

- Verwaltung der WAN-Verbindung
- QoS-Kontrollen

2. Sicherheitsdienstleiste (SSE)
    - Sicheres Web-Gateway (SWG)
    - Cloud Access Security Broker (CASB)
    - Zero Trust Network Access (ZTNA)
    - Firewall als Dienstleistung (FWaaS)
3. Erweiterte Sicherheitsfunktionen
    - Schutz vor Datenverlust (DLP)
    - Erweiterter Schutz vor Bedrohungen
    - Analyse des Benutzer- und Entitätsverhaltens
    - Integrierte Bedrohungsdaten
4. Verwaltung und Analytik
    - Einheitliche Verwaltungskonsole
    - Überwachung in Echtzeit
    - Erweiterte Analytik
    - Automatisierte Reaktion auf Vorfälle

Phasen der Umsetzung

1. Planung und Entwurf
    - Bewertung der Architektur
    - Entwicklung einer Migrationsstrategie
    - Gestaltung des politischen Rahmens
    - Bewertung der aktuellen Netz- und Sicherheitsinfrastruktur

- Planung von Schulungen und Änderungsmanagement für IT-Mitarbeiter und Endnutzer

2. Pilot-Einsatz
    - Erste Umsetzung
    - Prüfung und Validierung
    - Festlegung von Leistungsgrundlagen
    - Proof of Concept (PoC) Ausführung, einschließlich:
        - Klare Ziele und Erfolgskriterien
        - Testen der wichtigsten Anwendungsfälle
        - Leistungsvergleiche und Sicherheitsszenarien
        - Erforderliche Integrationstests
        - Bewertungsmaßstäbe und Berichtsanforderungen
3. Vollständiger Einsatz
    - Gestaffelte Markteinführung
    - Migration der Benutzer
    - Integration in bestehende Systeme
4. Optimierung
    - Leistungsoptimierung
    - Verfeinerung der Politik
    - Optimierung der Benutzerfreundlichkeit

4. Technische Anforderungen

Netzwerk-Fähigkeiten

1. SD-WAN-Funktionen
    - Anwendungsorientiertes Routing

- Dynamische Pfadauswahl
- QoS- und Bandbreitenmanagement
- Link-Aggregation und Ausfallsicherung
- Traffic Shaping und Priorisierung

5. Funktionale Anforderungen

A. Funktionale Kernanforderungen

5.1 Cloud-native Architektur

Tipp: Eine Cloud-native Architektur ist die Voraussetzung für eine erfolgreiche SASE-Implementierung. Achten Sie auf Lösungen, die echte Cloud-first-Designprinzipien aufweisen, mit einer Microservices-basierten Architektur, die Skalierbarkeit, Flexibilität und einen stabilen Betrieb ermöglicht. Achten Sie darauf, wie die Architektur die verteilte Bereitstellung unterstützt und eine konsistente Leistung über verschiedene Cloud-Umgebungen hinweg gewährleistet.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Cloud-native Architektur	Cloud-first-Design mit Microservices-Architektur		
	Container-basierte Bereitstellungsfunktionen		
	Automatische Skalierung und elastische Ressourcenverwaltung		
	Unterstützung einer mandantenfähigen Architektur		
	Native Integration von Cloud-Anbietern		

5.2 Integrierte SD-WAN-Funktionen

Tipp: Eine effektive SD-WAN-Integration ist entscheidend für die Optimierung der Netzwerkleistung und die Gewährleistung einer zuverlässigen Konnektivität über verteilte Standorte hinweg. Konzentrieren Sie sich auf Lösungen, die umfassende

WAN-Optimierungsfunktionen und intelligente Traffic-Routing-Funktionen bieten und gleichzeitig eine konsistente Anwendungsleistung gewährleisten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
SD-WAN-Integration	Anwendungsspezifische Routing-Funktionen		
	Dynamische Pfadwahl und Optimierung		
	Lastausgleich und Aggregation von WAN-Verbindungen		
	Kontrollen der Dienstgüte (QoS)		
	Bandbreitenmanagement und -optimierung		

5.3 Umfassende Sicherheitsdienstleistungen

Tipp: Sicherheitsdienste bilden das Rückgrat der SASE-Architektur. Bewerten Sie Lösungen auf der Grundlage ihrer Fähigkeit, integrierte, aus der Cloud bereitgestellte Sicherheitskontrollen zu bieten, die alle Kanten des Netzwerks schützen und gleichzeitig eine einfache Verwaltung und Bereitstellung ermöglichen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Sicherheitsdienste	Firewall-Funktionen der nächsten Generation		
	Erweiterte Funktionen zur Abwehr von Bedrohungen		
	Funktionen zum Schutz vor Datenverlust (DLP)		
	Implementierung eines vertrauensfreien Netzwerkzugangs		
	Sichere Web-Gateway-Dienste		

5.4 Einheitliche Verwaltungsschnittstelle

Tipp: Eine zentrale Verwaltungsschnittstelle ist für einen effizienten SASE-Betrieb unerlässlich. Achten Sie auf Lösungen, die eine intuitive, umfassende Steuerung über eine einzige Oberfläche bieten, die eine einheitliche Richtlinienverwaltung, Überwachung und Berichterstellung ermöglicht und gleichzeitig verschiedene administrative Rollen und Zugriffsebenen berücksichtigt.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Management-Schnittstelle	Eine einzige Konsole für alle SASE-Funktionen		
	Rollenbasierte Zugangskontrollverwaltung		
	Anpassbare Dashboards und Berichte		
	Integrierte Politikverwaltung		
	Konfigurationsmöglichkeiten in Echtzeit		

5.5 Durchsetzung von Richtlinien

Tipp: Die konsistente Durchsetzung von Richtlinien über alle Netzwerkkanten und Sicherheitsfunktionen hinweg ist für die Aufrechterhaltung der Sicherheitslage von entscheidender Bedeutung. Bewerten Sie Lösungen anhand ihrer Fähigkeit, granulare Richtlinien einheitlich umzusetzen und gleichzeitig dynamische Anpassungen je nach Kontext und Risiko zu unterstützen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Durchsetzung der Politik	Detaillierte Erstellung und Kontrolle von Richtlinien		
	Benutzer- und gruppenbasierte Richtlinienverwaltung		
	Umsetzung standortbezogener Richtlinien		

	Anwendungsspezifische Regeldurchsetzung		
	Automatisierte Bereitstellung von Richtlinien		

5.6 Optimierung des Verkehrs

Tipp: Funktionen zur Verkehrsoptimierung wirken sich direkt auf die Benutzerfreundlichkeit und die Anwendungsleistung aus. Konzentrieren Sie sich auf Lösungen, die umfassende Optimierungsfunktionen bieten und gleichzeitig Sicherheit und Transparenz über alle Verkehrsströme hinweg gewährleisten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Optimierung des Verkehrs	Optimierung des WAN-Verkehrs		
	Beschleunigung der Anwendungsleistung		
	Kontrolle der Bandbreitenzuweisung		
	Mechanismen zur Priorisierung des Verkehrs		
	Fähigkeiten zur QoS-Implementierung		

5.7 Skalierbarkeit

Tipp: Die Skalierbarkeit stellt sicher, dass Ihre SASE-Lösung mit Ihrem Unternehmen wachsen kann. Achten Sie auf horizontale und vertikale Skalierbarkeit und auf die Fähigkeit, die Leistung auch bei einer Erweiterung der Bereitstellung aufrechtzuerhalten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Skalierbarkeit	Unterstützung der horizontalen Skalierung		

	Elastische Ressourcenverwaltung		
	Leistungsoptimierung im großen Maßstab		
	Automatisierte Kapazitätsplanung		
	Dynamischer Lastausgleich		

5.8 Integrationsfähigkeiten

Tipp: Die Integrationsmöglichkeiten bestimmen, wie gut die SASE-Lösung mit Ihrer bestehenden Infrastruktur zusammenarbeitet. Beurteilen Sie die Breite und Tiefe der Integrationsmöglichkeiten und konzentrieren Sie sich dabei auf APIs und vorgefertigte Konnektoren für gängige Unternehmenssysteme.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Integration	API-Verfügbarkeit und Dokumentation		
	SIEM-Systemintegration		
	Konnektivität der Identitätsanbieter		
	Integration von Sicherheitstools von Drittanbietern		
	Individuelle Integrationsmöglichkeiten		

5.9 Erweiterter Schutz vor Bedrohungen

Tipp: Fortschrittlicher Schutz vor Bedrohungen ist in der heutigen, sich ständig weiterentwickelnden Bedrohungslandschaft von entscheidender Bedeutung. Suchen Sie nach Lösungen, die mehrere Erkennungsmethoden mit automatisierten Reaktionsmöglichkeiten kombinieren, um einen umfassenden Schutz vor komplexen Angriffen zu bieten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Schutz vor Bedrohungen	Schutz vor Zero-Day-Bedrohungen		

	Erweiterte Sandboxing-Funktionen		
	Integration von Bedrohungsdaten		
	Merkmale der Verhaltensanalyse		
	Automatisierte Reaktion auf Bedrohungen		

5.10 Identitäts- und Zugangsmanagement

Tipp: Identitätsbasierte Zugriffskontrolle ist die Grundlage für Zero-Trust-Sicherheit. Evaluieren Sie Lösungen auf der Grundlage ihrer Fähigkeit, sich in bestehende Identitätssysteme zu integrieren und gleichzeitig robuste Authentifizierungs- und Autorisierungsfunktionen zu bieten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
IAM	Unterstützung der Multi-Faktor-Authentifizierung		
	Single Sign-On-Funktionen		
	Integration von Verzeichnisdiensten		
	Verwaltung des privilegierten Zugangs		
	Mechanismen zur Identitätsüberprüfung		

5.11 Überwachung und Analyse in Echtzeit

Tipp: Effektive Überwachungs- und Analysefunktionen bieten Einblick in die Sicherheit und Leistung. Konzentrieren Sie sich auf Lösungen, die umfassende Echtzeit-Überwachungsfunktionen mit umsetzbaren Erkenntnissen und anpassbaren Berichten bieten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Überwachung und Analyse	Leistungsüberwachung in Echtzeit		

	Analyse von Sicherheitsereignissen		
	Verfolgung der Benutzererfahrung		
	Analyse der Netzleistung		
	Anpassbare Berichtswerkzeuge		

5.12 Multi-Cloud-Unterstützung

Tipp: Multi-Cloud-Unterstützung ist für moderne verteilte Architekturen unerlässlich. Evaluieren Sie Lösungen auf der Grundlage ihrer Fähigkeit, konsistente Sicherheit und Konnektivität über verschiedene Cloud-Anbieter hinweg zu bieten und gleichzeitig eine einheitliche Verwaltung zu gewährleisten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Multi-Cloud	Cloud-übergreifende Konnektivität		
	Cloud-to-Cloud-Sicherheit		
	Sicherheit beim Cloud-Zugang		
	Schutz von Cloud-Workloads		
	Multi-Cloud-Verwaltungstools		

5.13 Unterstützung von Edge Computing

Tipp: Edge-Computing-Unterstützung ermöglicht die Verarbeitung näher an den Datenquellen. Suchen Sie nach Lösungen, die Sicherheits- und Netzwerkfunktionen auf Edge-Standorte ausdehnen können, ohne die zentrale Kontrolle zu verlieren.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Edge Computing	Bereitstellung von Edge-Diensten		
	Unterstützung der lokalen Datenverarbeitung		

	Sicherheitskontrollen am Rande		
	Optimierung der Kantenleistung		
	Funktionen für verteiltes Rechnen		

5.14 Automatisierte Reaktion auf Vorfälle

Tipp: Automatisierte Funktionen für die Reaktion auf Sicherheitsvorfälle verkürzen die durchschnittliche Reaktions- und Wiederherstellungszeit bei Sicherheitsvorfällen. Konzentrieren Sie sich auf Lösungen, die eine umfassende Automatisierung bieten und gleichzeitig eine angemessene menschliche Aufsicht gewährleisten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Reaktion auf Vorfälle	Automatisierte Bedrohungsabwehr		
	Automatisierung von Arbeitsabläufen bei Vorfällen		
	Antwort-Orchestrierung		
	Automatisierte Wiederherstellungsverfahren		
	Instrumente für die Analyse nach einem Vorfall		

5.15 Verwaltung der Einhaltung der Vorschriften

Tipp: Compliance-Management-Funktionen helfen bei der Einhaltung von Vorschriften. Bewerten Sie die Lösungen anhand ihrer Fähigkeit, Compliance-Richtlinien durchzusetzen und die erforderliche Dokumentation und Berichte zu erstellen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Einhaltung der Vorschriften	Instrumente zur Überwachung der Einhaltung der Vorschriften		

	Merkmale der aufsichtsrechtlichen Berichterstattung		
	Pflege des Prüfpfads		
	Überprüfung der Einhaltung von Richtlinien		
	Funktionalität des Dashboards zur Einhaltung der Vorschriften		

B. Anforderungen an KI und maschinelles Lernen

5.16 KI-gestützte Sicherheit

Tipp: KI-gestützte Sicherheit verbessert die Fähigkeiten zur Erkennung von und Reaktion auf Bedrohungen. Suchen Sie nach Lösungen, die KI effektiv nutzen und gleichzeitig Transparenz in ihre Entscheidungsprozesse bringen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
AI-Sicherheit	KI-basierte Erkennung von Bedrohungen		
	Automatisierte Sicherheitsreaktionen		
	KI-gesteuerte Risikobewertung		
	Analytik des maschinellen Lernens		
	Analyse von Verhaltensmustern		

5.17 Generative KI-Integration

Tipp: Generative KI-Funktionen verbessern die Automatisierungs- und Entscheidungsprozesse. Konzentrieren Sie sich auf Lösungen, die generative KI nutzen, um Konfiguration, Fehlerbehebung und Richtlinienverwaltung zu verbessern und gleichzeitig Sicherheit und Genauigkeit zu gewährleisten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Generative KI	KI-gestützte Politikgestaltung		

	Automatisierte Unterstützung bei der Konfiguration		
	Intelligente Dokumentationserstellung		
	KI-unterstützte Fehlersuche		
	Fähigkeiten zur Verarbeitung natürlicher Sprache		

5.18 KI-gestütztes Netzwerkmanagement

Tipp: KI-gestütztes Netzwerkmanagement verbessert die betriebliche Effizienz und die Netzwerkleistung. Bewerten Sie Lösungen anhand ihrer Fähigkeit, Routineaufgaben zu automatisieren und intelligente Optimierungsempfehlungen zu geben.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
AI-Netzwerk-Management	Automatisierte Netzwerkoptimierung		
	Intelligente Fehlersuche		
	Leistungsvorhersage		
	Intelligentes Konfigurationsmanagement		
	Fähigkeiten zur Netzwerkautomatisierung		

5.19 Autonomes digitales Erlebnismanagement (ADEM)

Tipp: ADEM sorgt durch automatische Überwachung und Optimierung für ein optimales Nutzererlebnis. Suchen Sie nach Lösungen, die einen umfassenden Einblick in die Benutzererfahrung und automatische Abhilfemöglichkeiten bieten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
ADEM	Überwachung der Erfahrungen in Echtzeit		

	Verfolgung der Anwendungsleistung		
	Bewertung der Benutzererfahrung		
	Automatisierte Problembehebung		
	Tools zur Erlebnisoptimierung		

5.20 KI-Betrieb (AIOps)

Tipp: AIOps-Funktionen rationalisieren den IT-Betrieb durch intelligente Automatisierung. Konzentrieren Sie sich auf Lösungen, die Betriebsdaten effektiv mit KI kombinieren, um die Effizienz zu steigern und manuelle Eingriffe zu reduzieren.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
AIOps	Automatisierte operative Aufgaben		
	Merkmale der vorausschauenden Wartung		
	Optimierung der Ressourcen		
	Intelligentes Alarmierungssystem		
	Optimierung der Leistung		

5.21 Verbesserte Erkennung von Bedrohungen durch KI

Tipp: KI-gestützte Bedrohungserkennung ermöglicht eine genauere und schnellere Identifizierung von Sicherheitsbedrohungen. Evaluieren Sie Lösungen anhand ihrer Fähigkeit, KI für eine verbesserte Bedrohungserkennung zu nutzen und gleichzeitig Fehlalarme zu minimieren.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
AI-Bedrohungserkennung	Erweiterte Bedrohungsanalyse		
	Fähigkeiten zur Mustererkennung		

	Erkennung von Anomalien		
	Vorausschauende Identifizierung von Bedrohungen		
	Bedrohungsanalyse in Echtzeit		

5.22 KI-gestützte Entscheidungsfindung

Tipp: KI-gesteuerte Entscheidungsfindung verbessert Reaktionszeiten und Genauigkeit. Suchen Sie nach Lösungen, die transparente, erklärbare KI-Entscheidungen bieten und gleichzeitig eine angemessene menschliche Aufsicht gewährleisten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
AI-Entscheidungsfindung	Automatisierte politische Entscheidungen		
	Intelligente Risikobewertung		
	Optimierung der Ressourcenzuweisung		
	Leistungsbezogene Entscheidungen		
	Prüfpfade für Entscheidungen		

5.23 Natürliche Sprachschnittstellen

Tipp: Natürlichsprachliche Schnittstellen verbessern die Benutzerinteraktion und die Verwaltungseffizienz. Konzentrieren Sie sich auf Lösungen, die eine intuitive und präzise Verarbeitung natürlicher Sprache bieten und gleichzeitig die Sicherheitskontrollen beibehalten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Natürliche Sprache	Interpretation der Befehle		
	Abfragen in natürlicher Sprache		

	Konversationsfähige Schnittstelle		
	Unterstützung mehrerer Sprachen		
	Bewusstsein für den Kontext		

5.24 Prädiktive KI-Fähigkeiten

Tipp: Prädiktive KI ermöglicht proaktives Management und Optimierung. Bewerten Sie Lösungen auf der Grundlage ihrer Fähigkeit, Trends und potenzielle Probleme genau vorherzusagen und gleichzeitig verwertbare Erkenntnisse zu liefern.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Prädiktive KI	Vorhersage der Kapazität		
	Leistungsprognose		
	Vorhersage der Bedrohung		
	Vorhersage des Ressourcenverbrauchs		
	Trendanalyse		

5.25 Relationship Mapping für UEBA

Tipp: Die Abbildung von UEBA-Beziehungen bietet tiefere Einblicke in die Verhaltensmuster der Nutzer. Suchen Sie nach Lösungen, die Beziehungen effektiv abbilden und analysieren und gleichzeitig die Anforderungen an Datenschutz und Compliance erfüllen.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
UEBA-Zuordnung	Analyse des Nutzerverhaltens		
	Abbildung von Entitätsbeziehungen		
	Mustererkennung		
	Korrelation der Anomalien		
	Verhaltensanalytik		

5.26 Erklärbare KI zur Erkennung von Anomalien

Tipp: Erklärbare KI sorgt für Transparenz bei Anomalieerkennungsprozessen. Konzentrieren Sie sich auf Lösungen, die klare Erklärungen für die von KI erkannten Anomalien liefern und gleichzeitig die Erkennungsgenauigkeit beibehalten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Erklärbare AI	Transparente Entscheidungslogik		
	Merkmale zur Erklärung von Anomalien		
	Argumentation bei der Erkennung		
	Erstellung von Prüfprotokollen		
	Unterstützung bei Ermittlungen		

6. Qualifikationen des Anbieters

Erforderliche Qualifikationen

1. Überblick über das Unternehmen
    - Jahre auf dem SASE-Markt
    - Marktstellung
    - Finanzielle Stabilität
    - Kundenstamm
2. Technisches Fachwissen
    - Erfahrung mit der SASE-Architektur
    - Sicherheitszertifizierungen
    - Fähigkeiten zur Umsetzung
    - Unterstützung der Infrastruktur
3. Dienstabdeckung
    - Globale Präsenz

- Metriken zur Dienstverfügbarkeit
- Geografische Abdeckung
- Punkte der Präsenz

4. Zertifizierungen und Normen
    - Sicherheitszertifizierungen
    - Konformitätsbescheinigungen
    - Angleichung an Industriestandards
    - Rahmenwerke für bewährte Verfahren
5. Zukünftige Entwicklung
    - Produkt-Fahrplan
    - Innovationsstrategie
    - Geplante Erweiterungen
    - Technologie-Partnerschaften

7. Kriterien für die Bewertung

Die Vorschläge werden nach folgenden Kriterien bewertet:

1. Technische Fähigkeiten (30%)
    - Vollständigkeit der Merkmale
    - Architekturentwurf
    - Leistungsmetriken
    - Sicherheitsfunktionen
2. Umsetzungskonzept (20%)
    - Methodik des Einsatzes
    - Migrationsstrategie
    - Risikomanagement

- Zeitplan - Machbarkeit

3. Qualifikationen des Anbieters (20%)
    - Erleben Sie
    - Referenzen
    - Unterstützungsmöglichkeiten
    - Finanzielle Stabilität
4. Kostenstruktur (30%)
    - Gesamtbetriebskosten
    - Preismodell
    - Zusätzliche Kosten
    - Gutes Preis-Leistungs-Verhältnis

8. Einreichungsrichtlinien

Die Vorschläge müssen Folgendes enthalten:

1. Zusammenfassung
2. Beschreibung der technischen Lösung
3. Ansatz für die Umsetzung
4. Zeitplan des Projekts
5. Details zur Preisgestaltung
6. Qualifikationen des Unternehmens
7. Kundenreferenzen
8. Unterstützungsmodell
9. Muster-SLAs
10. Zusätzliche Dokumentation
11. Fallstudien und Referenzen

- Ähnliche Beispiele für die Umsetzung
- Branchenspezifische Einsätze
- Erfolgsmetriken
- Erfahrungsberichte von Kunden

9. Zeitleiste

- RFP-Freigabedatum: [Datum]
- Einsendeschluss: [Datum]
- Fälligkeitsdatum des Vorschlags: [Datum]
- Präsentationen des Anbieters: [Datumsbereich]
- Auswahlentscheidung: [Datum]
- Projektbeginn: [Datum]
- Geplante Fertigstellung: [Datum]

Vorschläge einreichen bei: [Kontaktinformationen]