Leistungsbeschreibung zum Vergabeantrag

Entwicklung einer OVGU-spezifischen Infrastruktur-Managementlösung

Das Universitätsrechenzentrum ist als Einrichtung der Otto-von-Guericke-Universität Magdeburg (OVGU) der zentrale IT-Dienstleister der Universität. Die zentralen Aufgaben des Universitätsrechenzentrums sind die Bereitstellung zentraler IT-Ressourcen und der Betrieb der Infrastruktur. Dies schließt natürlich auch die Server- und Storage-Ressourcen sowie die Netzwerkinfrastruktur der OVGU mit ein. Die moderne Infrastruktur erfordert eine stetige Weiterentwicklung, um den wachsenden Anforderungen an Verfügbarkeit, Sicherheit und Flexibilität gerecht zu werden. Insbesondere im Hochschulbereich, wo Forschungs- und Verwaltungsinfrastruktur effizient und sicher betrieben werden müssen, ist eine zentrale Herausforderung die zuverlässige Automatisierung und Verwaltung der komplexen Konfigurationen. Die zu entwickelnde Lösung soll nicht nur in der Lage sein, Konfigurationen zentral zu verwalten und zu automatisieren, sondern auch flexibel auf wechselnde Anforderungen reagieren können. Dabei liegt ein besonderer Fokus auf der Sicherheit der Infrastruktur, unterstützt durch eine umfassende Security Information and Event Management (SIEM)-Integration, um Bedrohungen frühzeitig zu erkennen und Angriffe zu verhindern. Zugleich sollen die Konfigurationsdaten herstellerübergreifend in einem automatisierten Prozess ausgerollt werden, ohne dabei auf manuelle Eingriffe angewiesen zu sein. Die Lösung sollte vollständig auf Open-Source basieren. Auch individuelle Anpassungen oder Neuentwicklungen sind als Open-Source zur Verfügung zu stellen.

Beschreibung des Ist-Zustands

Die grundlegenden Daten werden aktuell in unterschiedlichen Open-Source Systemen und Eigenentwicklungen gepflegt. Dazu kommen noch herstellerspezifische Management Anwendungen. Die Netzwerkkomponenten sind unterschiedlicher Bauart, unterschiedlichen Alters und von diversen Hardware-Herstellen (unter anderem: Arista, Cisco, Dell, HP PaloAlto, Ubiquiti) und Software-basierte Open-Source-Systemen (unter anderem: VyOS, PfSense, OPNSense). Zur Virtualisierung kommt VMware, Proxmox und Kubernetes zum Einsatz. Dazu kommen die unterschiedlichsten Dienste und Anwendungen auf Basis von Linux und Windows. Zurzeit ist nur ein kleiner Teil der aktuellen Infrastruktur automatisiert.

Beschreibung des Ziel-Zustands

Das Ziel dieser Ausschreibung ist die Beschaffung und Implementierung einer Lösung, die das Infrastrukturmanagement grundlegend transformiert. Weg von fragmentierten, herstellerabhängigen Systemen hin zu einer zentralisierten, herstellerunabhängigen Architektur, die es ermöglicht, sämtliche Netzwerkkomponenten konsistent und effizient zu steuern und die Server und Infrastruktur zu orchestrieren. Diese neue Lösung muss sowohl bestehende Anforderungen erfüllen als auch flexibel genug sein, um zukünftige Entwicklungen und Erweiterungen zu unterstützen.
Im Vordergrund steht dabei die nahtlose Integration aller relevanten Netzwerkkomponenten – von physischen und virtuellen Netzwerken über Container-Umgebungen bis hin zur Bereitstellung einer konsolidierten Sicherheitsarchitektur. Ein weiteres zentrales Anliegen ist die fortlaufende Überprüfung der Sicherheit nach den Maßstäben des IT-Grundschutzes. Hierbei soll die

Automatisierung nicht nur die Effizienz steigern, sondern auch zur Verbesserung der Sicherheit durch eine umfassende Überwachung und Prüfung beitragen.

Allgemeine Anforderungen:

Zentralisierte, herstellerneutrale Verwaltung und Automatisierung:
Die Lösung muss in der Lage sein, die Konfigurationen verschiedener Hersteller und Typen in einer einzigen, zentralisierten Plattform zu konsolidieren. Diese Plattform soll es ermöglichen, Änderungen an der Infrastrukturkonfigurationen effizient und konsistent über alle Komponenten hinweg umzusetzen. Unabhängig davon, ob es sich um die Konfiguration eines Servers, Dienstes, Routers, Switches, einer Firewall oder eines Access Points handelt – alle Konfigurationen müssen zentral definiert und ohne manuelle Eingriffe ausgerollt werden können. Dabei soll eine maximale Automatisierung gewährleistet werden, um das Risiko menschlicher Fehler zu minimieren. Gleichzeitig soll die Lösung sicherstellen, dass durch die zentrale Steuerung keine herstellerspezifischen Abhängigkeiten entstehen. Grundlage sind die bestehenden Datenbanken der einzelnen bestehenden Systeme. Diese müssen zentralisiert werden. Durch die Nutzung offener Standards und Protokolle sollen die Konfigurationen für alle eingesetzten Geräte und Systeme gültig sein und unabhängig vom spezifischen Hersteller automatisiert angewendet werden können.

Modularität und Erweiterbarkeit:
Die vorgeschlagene Lösung muss modular aufgebaut sein, um flexibel auf sich ändernde Anforderungen reagieren zu können. Diese Modularität soll es ermöglichen, neue Komponenten ohne größeren Aufwand in die bestehende Infrastruktur zu integrieren. Ein besonderes Augenmerk liegt dabei auf der Fähigkeit, Policies zentral zu definieren und diese über die Infrastruktur hinweg konsistent durchzusetzen. Durch diese Flexibilität soll gewährleistet werden, dass das System nicht nur den aktuellen, sondern auch zukünftigen Herausforderungen gewachsen ist.

Automatisierung des Deployments und Konfigurationsmanagements:
Ein weiteres zentrales Element der Lösung ist die Fähigkeit, automatisierte Deployments und Konfigurationsanpassungen effizient und zuverlässig durchzuführen. Hierbei geht es nicht nur darum, einzelne Netzwerkelemente, Dienste oder Server zu konfigurieren, sondern eine ganzheitliche und integrierte Lösung zu schaffen, bei der Änderungen zentral definiert und automatisch auf alle relevanten Systeme verteilt werden. Dabei müssen die Konfigurationen versioniert und im Bedarfsfall jederzeit zurückgesetzt werden können, um eine maximale Flexibilität und Kontrolle über die Infrastruktur zu gewährleisten. Ein Inventar- und Flottenmanagement soll integriert werden. Dies beinhaltet auch die Unterstützung im Bereich Patch- und Konfigurationsmanagement.

Integrierte Sicherheitsprüfungen und IT-Grundschutz-Check:
In Zeiten wachsender Cyberbedrohungen ist die Sicherheit der Infrastruktur von zentraler Bedeutung. Die zu entwickelnde Lösung muss daher in der Lage sein, die Konfigurationen kontinuierlich gegen die Anforderungen des IT-Grundschutzes zu prüfen. Eine ML/KI-gestützte Komponente soll sicherstellen, dass zum Beispiel alle Netzwerkelemente und Serverkonfigurationen den festgelegten Sicherheitsstandards entsprechen und Abweichungen von den vorgegebenen Schutzniveaus (Basis-, Standard- oder Kernabsicherung) frühzeitig erkannt werden.
Die Lösung soll darüber hinaus automatisierte Vorschläge für die Anpassung der Konfigurationen bieten, um sicherzustellen, dass das gewünschte Sicherheitsniveau stets eingehalten wird. Diese Funktionalität ist insbesondere im Hinblick auf die zentrale Verwaltung von Policies und Konfigurationen von entscheidender Bedeutung, um die Infrastruktur kontinuierlich und dynamisch an die geltenden Sicherheitsstandards anzupassen.

SIEM-Integration:
Ein integraler Bestandteil der Lösung muss die Echtzeitüberwachung und -analyse sicherheitsrelevanter Ereignisse sein. Hierzu ist eine SIEM-Lösung (Security Information and Event Management) zu integrieren, die sicherstellt, dass Bedrohungen und Sicherheitsvorfälle in Echtzeit erkannt und analysiert werden. Diese Komponente soll in der Lage sein, sicherheitsrelevante Daten zu sammeln, zu korrelieren und entsprechend zu reagieren. Die Lösung muss außerdem gewährleisten, dass sicherheitsrelevante Protokolle und Ereignisse langfristig dokumentiert und analysiert werden können, um potenzielle Bedrohungen frühzeitig zu erkennen und Gegenmaßnahmen zu ergreifen.

Infrastrukturübergreifende Automatisierung und Management:
Die Lösung muss in der Lage sein, die Infrastruktur ganzheitlich zu verwalten. Dies umfasst sowohl physische Server- und Netzwerkkomponenten als auch virtuelle Netzwerke (z.B. Proxmox, KVM, VMware) sowie Container-basierte Netzwerke (z.B. Kubernetes). Diese verschiedenen Netzwerktypen müssen nahtlos integriert und über eine zentrale Steuerung verwaltet werden können, um eine einheitliche Verwaltung und Überwachung zu ermöglichen. Das Ausrollen von Systemen und virtuellen Server muss unabhängig von der Virtualisierung möglich sein.

Benutzerfreundliches Interface:
Für die Verwaltung der Infrastruktur soll ein benutzerfreundliches Interface bereitgestellt werden, das es den Administratoren ermöglicht, alle relevanten Informationen und Konfigurationen zentral einzusehen und zu steuern. Dieses Interface muss nicht nur die Konfiguration vereinfachen, sondern auch die Automatisierung von Standardaufgaben ermöglichen, um den Verwaltungsaufwand zu minimieren. Durch ein Rechte und Rollen System muss es möglich sein, Teile der Infrastruktur dezentral verwalten zu lassen ohne negative Einflüsse auf das Hauptsystem.

Monitoring und Analyse-Tools:
Die Lösung soll bestehende Monitoring-Lösungen wie Zabbix unterstützen und erweitern, um eine umfassende Überwachung der Infrastruktur zu ermöglichen. Durch die Integration von Echtzeit-Überwachungstools und die Analyse von sicherheitsrelevanten Daten soll die Lösung sicherstellen, dass potenzielle Probleme frühzeitig erkannt und behoben werden.

Inventar und Raum Management:
Die zu entwickelnde Lösung soll als Teil der IT-Dokumentation die vorhandenen Informationen zusammenfassen. Es sind die räumlichen und technischen Gegebenheiten der einzelnen Räume zu erfassen. Einzubeziehen ist der Aufbau der Racks und die Versorgung mit Strom und Kälte. Der zweite Teil ist das Kabelmanagement auf der einen Seite als Patch Management im Raum und auf der anderen Seite als LWL- und Spleißdokumentation im Raum bzw. über das Gebäude hinweg. Dies sollte grafisch darstellbar sein und eine Kapazitätsbetrachtung sowie den Aus- und Umbau von Standorten unterstützen.

Zusammenfassung:
Ziel dieser Ausschreibung ist die Beschaffung einer Lösung, die es ermöglicht, die Infrastrukturkonfiguration einer komplexen und heterogenen Landschaft zentral und automatisiert zu verwalten, ohne dabei auf herstellerspezifische Lösungen angewiesen zu sein. Gleichzeitig wird ein umfassendes Monitoring und Sicherheitsaudit nach IT-Grundschutz-Standards integriert, um ein langfristiges und zukunftssicheres Management der Infrastruktur zu gewährleisten.

Konkrete Anforderungen

Anforderungen und Architektur des SDN:

- Entwicklung einer offenen SDN-Architektur, die auf existierenden Open-Source-Technologien wie OpenDaylight, ONOS, oder Tungsten Fabric basiert.
- Unterstützung einer „Fabric“-Architektur (EVPN-VXLAN), die eine zentrale Steuerung aller Netzwerkkomponenten ermöglicht.
- Implementierung eines „Controllers“, der verschiedene Netzwerkgeräte und Hersteller über offene Standards wie Netconf, OpenFlow und gNMI verwaltet.
- Integration Ansible und Netbox
- Sicherstellung, dass das System nach den Anforderungen des IT-Grundschutzes konzipiert ist, insbesondere in Bezug auf die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit.

Anwendungsorientierte Netzwerkverwaltung:

- Patch- und Port-Management der Vorhanden und neuen Infrastruktur
  - Integration der vorhandenen Datenbanken
  - Integration ins neue Frontend
- Bereitstellung einer Schnittstelle für die Definition von Netzwerkrichtlinien basierend auf den Anforderungen der Anwendungen.
- Unterstützung von Mikrosegmentierung und Sicherheitsrichtlinien auf Anwendungsebene, basierend auf den Sicherheitsanforderungen des IT-Grundschutzes.
- Integration von virtualisierten Netzwerken und hybriden Cloud-Umgebungen (Multi-Cloud-Support).
- Inventur und Patch-Management

Container-Verwaltung:

- Unterstützung der Verwaltung von Container-basierten Anwendungen durch Integration mit Container-Orchestrierungssystemen wie Kubernetes.
- Verwendung von CNI-Plugins wie Calico, Flannel oder Weave, um Container-Netzwerke über das SDN-Framework zu steuern.
- Sicherstellung, dass Netzwerkrichtlinien auch auf Container-basierte Umgebungen angewendet werden, einschließlich Mikrosegmentierung, QoS und Bandbreitensteuerung.
- Inventur und Patch-Management

Virtualisierungsumgebungen:

- Unterstützung von Open-Source-Virtualisierungsumgebungen wie Proxmox VE, KVM oder VMware zur Verwaltung von virtualisierten Maschinen.
- Integration von Netzwerkrichtlinien und Sicherheitsfunktionen in die virtuellen Maschinen und Netzwerkverbindungen.
- Nahtlose Verwaltung von virtuellen Maschinen über das Framework und das zentrale Kundeninterface.
- Unterstützung der dynamischen Migration und Skalierung von virtuellen Maschinen basierend auf Netzwerkauslastung und Anwendungsanforderungen.
- Integration Ansible und Netbox
- Inventur und Patch-Management

Server und Speicherumgebung:

- Unterstützung vom Erzeugen, Administrieren und Inventarisieren vom Linux/Windows Server aller Art
- Inventur und Patch-Management
- Automatische Softwareverteilung
- Software und Lizenzerfassung mit Schnittelle zum Asset Management Spider
- Bereitstellung und Monitoring von verteiltem Speicher (Ceph)
- Integration Ansible und Netbox

Herstellerneutrale Unterstützung:

- Interoperabilität mit unterschiedlichen Herstellern durch den Einsatz von offenen Protokollen und Standards.
- Sicherstellung, dass die Lösung auf kommerziellen und Open-Source-Netzwerkgeräten gleichermaßen funktioniert.

Kundeninterface:

- Entwicklung einer benutzerfreundlichen, anwendungszentrierten Verwaltungsoberfläche, die als zentrales Interface zur Steuerung der gesamten Infrastruktur dient.
- Das Interface muss unabhängig von der zugrunde liegenden Hardware oder den Backend-Systemen funktionieren und die nahtlose Konfiguration, Überwachung und Verwaltung ermöglichen.
- Unterstützung von Drag-and-Drop-Konfigurationen sowie automatisierten Arbeitsabläufen über das Interface.
- Eine ausgeprägte Mandanten-/Rollenfähigkeit zur Verwaltung von Teilbereichen muss gegeben sein.
- Client System unabhängiges Webinterface basierend auf Linux Server Diensten
- Möglichst ohne Java
- Offene APIs zur Integration des Interfaces in bestehende Systeme und externe Tools.

Künstliche Intelligenz (KI) und Automatisierung:

- Integration von KI-basierten Algorithmen zur automatischen Optimierung des Netzwerkbetriebs, wie z.B.:
  - Verkehrsmanagement und Bandbreitenoptimierung.
  - Proaktive Fehlererkennung und Selbstheilung.
  - Automatische Skalierung und Lastverteilung basierend auf Netzwerkauslastung und Anwendungsanforderungen.
- IT-Grundschutz-Check: Die KI muss in der Lage sein, die Konfiguration der gesamten Infrastruktur gegen den IT-Grundschutz zu prüfen.
  - Die KI führt einen klassischen IT-Grundschutz-Check durch und identifiziert Abweichungen zu den verschiedenen Schutzniveaus: Basisabsicherung, Standardabsicherung oder Kernabsicherung.
  - Vorschläge zur Behebung der Abweichungen und zur Erreichung des gewünschten Schutzniveaus werden automatisch generiert.
  - Möglichkeit, das Sicherheitsniveau flexibel einzustellen (Basis, Standard oder Kern), und Anpassungen der Konfiguration gemäß den Vorschlägen durchzuführen.

Sicherheit gemäß IT-Grundschutz:

- Integration eines XDR-Systems wie Wazuh zur Erkennung und Analyse von Sicherheitsvorfällen.
- Wazuh soll in die Infrastruktur integriert werden, um in Echtzeit Bedrohungen zu erkennen und darauf zu reagieren.
- Die Sicherheitslösung muss die Sicherheitsanforderungen des BSI IT-Grundschutzes erfüllen, insbesondere in den Bereichen Erkennung und Reaktion auf Sicherheitsvorfälle, Sicherheitsüberwachung und Protokollierung.
- Implementierung eines Sicherheitsmoduls, das die Mikrosegmentierung auf Anwendungsebene unterstützt und die Anforderungen des IT-Grundschutzes an Schutzmaßnahmen in Netzwerken, Servern und Diensten (z.B. Schutz vor unbefugtem Zugriff, Angriffserkennung) berücksichtigt.
- Patch-, Software- und Schwachstellenmanagement

- Unterstützung von End-to-End-Verschlüsselung und Netzwerksicherheitsrichtlinien auf allen Ebenen.

Skalierbarkeit und Leistung:

- Die Lösung muss skalierbar sein und Infrastrukturen unterschiedlicher Größe und Komplexität unterstützen, von Edge Niederlassungen bis hin zu großen, verteilten Umgebungen
- Hohe Leistung bei minimaler Latenz und hoher Ausfallsicherheit
- Implementierung der Anforderungen des IT-Grundschutzes für Ausfallsicherheit und Redundanz
- Das System muss die Funktion eines Configuration Management Database (CMDB**)** und Change-Managements abbilden oder integrieren

Raum und Kabelmanagement

- Integration der Raumpläne
- Abbildung des Aufbaus der IT-Systemen (Rackmanagement)
- Erfassung von Versorgungsleistungen und Versorgungswegen der Strom- und der Kälteversorgung
- Kapazitätsplanungen und Reports
- Planung vom Um- und Ausbau ist möglich
- Patch und Verkabelungsverwaltung im Raum/Schrank
- Kabelwege, Verteilungen sowie Faser und Spleißmanagement (Raumübergreifend)

Aufgaben im Projektumfeld:

- Bereitstellung umfassender Dokumentation für die Installation, Konfiguration und Wartung des Systems, unter Berücksichtigung der Anforderungen des IT-Grundschutzes.
- Durchführung von Schulungen für Administratoren und Entwickler, um den Einsatz und die Weiterentwicklung des Systems zu unterstützen, sowie spezifische Schulungen zum IT-Grundschutz.
- Framework soll vollkommen auf Linux basieren
- Integration ins ISMS System

Die Lösung muss vollständig auf Open-Source basieren. Auch individuelle Anpassungen oder Neuentwicklungen sind als Open-Source zur Verfügung zu stellen. Die unbefristete Nutzung, Weitereinwicklung und Erweiterung durch den Auftraggeber oder dessen Beauftragen ist zu ermöglichen. Der vollständige Code und die vollständige Dokumentation inkl. Build-Anweisungen und -skripte für die zu entwickelnde Lösung ist zur Verfügung zu stellen. Die OVGU stellt ein zu nutzendes Quellcodeverwaltungssystem zur Verfügung (Zugang zu Gitlab). Nach Ermittlung des Bedarfs und Abstimmung der Arbeiten werden die benötigen Systeme und IT-Ressourcen dem Bieter durch den AG installiert und bereitgestellt.

Alle Anwendungen und Funktionen müssen ausschließlich auf den Systemen der OVGU laufen (on-premises). Es dürfen keine Funktionalitäten von Externen abhängig sein. Darüber hinaus dürfen keine Daten außerhalb der OVGU verarbeitet werden.

Um zeitnah Änderungen berücksichtigen zu können und Missverständnissen entgegenzuwirken, ist ein Entwicklungsprozess auf Basis inkrementeller agiler Softwareentwicklung erforderlich. Ein Entwicklungs-/Anpassungszyklus mit kurzen Iterationen (ca. 4 Wochen pro Zyklus) ist zu nutzen, um die Risiken und Fehlentwicklungen im Entwicklungsprozess zu minimieren.

Da von hohem Entwicklungs- oder Konfigurationsbedarf auszugehen ist, wird eine Gesamtprojektzeit von 5 Jahren angestrebt.

Das gemeinsame Anforderungsmanagement ist Teil der zu erbringenden Leistung. Die sollte im Rahmen eines Workshops beim Projektstart erfolgen und sich in regelmäßigen Zeiträumen wiederholen.

Auftragnehmerprofil:

Um sicherstellen zu können, dass der Auftragnehmer den hohen Anforderungen gerecht wird, die durch das heterogene Umfeld des AG entsteht, muss die Eignung des Auftragnehmers nachgewiesen werden. Die Kriterien sind zwingend anzugeben und nachzuweisen. Der Nachweis ist durch geeignete Unterlagen zu erbringen, die dem Angebot beizufügen sind. Bewerber, die dieses Kriterium nicht erfüllen, können bei der Vergabe nicht berücksichtigt werden. Durch das breite fachliche Spektrum und die zentrale Bedeutung des Projektes ist der Bieter verpflichtet, 10 Mitarbeiter nachzuweisen, die in dem Projekt mitarbeiten, um die Anforderungen in technischer und organisatorischer Hinsicht sicher erfüllen zu können.

Folgende fachliche Expertise wird an den Bieter zwingend gestellt:

1. Expertise in Netzwerkmanagement und Automatisierung

- Erfahrung mit Netzwerktechnologien: Der Anbieter muss tiefgehende Kenntnisse in der Konfiguration, Verwaltung und Automatisierung von Netzwerkinfrastrukturen verschiedener Hersteller (z.B. Arista, Cisco, Dell etc.) haben.
- Netzwerkautomatisierung: Der Anbieter muss in der Lage sein, Netzwerkkonfigurationsänderungen über Automatisierungstechnologien (z.B. Ansible, Netconf, REST APIs) effizient zu verwalten und diese automatisiert auf verschiedene Netzwerkgeräte auszurollen.
- Herstellerunabhängige Lösungen: Erfahrungen in der Implementierung herstellerneutraler, standardbasierter Netzwerkautomatisierungslösungen (z.B. OpenFlow, NetBox) sind erforderlich.

2. Erfahrung mit Software Defined Networking (SDN)

- SDN-Technologien und -Protokolle: Der Anbieter muss Erfahrung in der Implementierung von SDN-Architekturen haben, einschließlich der Anwendung von SDN-Controllern wie OpenDaylight, ONOS, oder ähnlichen Plattformen.
- Netzwerkvirtualisierung: Expertise in der Verwaltung und Implementierung von virtuellen Netzwerken (z.B. VXLAN, EVPN, VRF) und die Fähigkeit, SDN-basierte Richtlinien zur Netzwerksicherheit und Verkehrssteuerung zu implementieren.
- Expertise in Künstlicher Intelligenz und/oder Machine Learning im Bereich Netzwerke

3. Erfahrung mit Security Information and Event Management (SIEM)

- SIEM-Systeme: Der Anbieter muss über umfassende Kenntnisse in der Implementierung von SIEM-Lösungen, auf Basis von Open-Source-Technologien wie Wazuh oder ELK-Stack, verfügen.
- Erkennung von Bedrohungen: Die Fähigkeit, Sicherheitsprotokolle zu analysieren und Bedrohungen in Echtzeit zu erkennen und darauf zu reagieren, ist unerlässlich. Kenntnisse in der Ereigniskorrelation, Mustererkennung und Forensik sind ebenfalls erforderlich.

4. Kenntnisse im IT-Grundschutz und Sicherheitsstandards

- IT-Grundschutz: Der Anbieter muss mit den BSI IT-Grundschutz-Katalogen vertraut sein und die Anforderungen der verschiedenen Sicherheitsniveaus (Basis-, Standard- und Kernabsicherung) verstehen und umsetzen können.
- Automatisierte Sicherheitsprüfungen: Erfahrung mit der Implementierung von KI-basierten Systemen zur Überprüfung von Sicherheitskonfigurationen gegen die BSI IT-Grundschutz-Standards.
- Compliance: Kenntnisse im Bereich der ISO 27001 nach BSI Grundschutz und deren praktische Anwendung.

5. Expertise in Virtualisierung, Container-Technologien und Server Betrieb

- Virtualisierung: Der Anbieter muss umfassende Kenntnisse über Virtualisierungsplattformen wie Proxmox und KVM haben und in der Lage sein, Netzwerke und Ressourcen für virtuelle Maschinen effizient zu verwalten und zu automatisieren.
- Container-Orchestrierung: Erfahrung mit Kubernetes und der Integration von Container-Netzwerken über CNI-Plugins (z.B. Calico, Flannel) ist notwendig, um Container-Netzwerke zu konfigurieren und zu verwalten.
- Server Automatisierung per Ansible
- Erfahrungen in heterogenen Linux- und Windows-Umgebungen

6. Erfahrung mit Monitoring- und Analyse-Tools

- Monitoring-Systeme: Der Anbieter muss Erfahrung mit der Implementierung und Verwaltung von Monitoring-Tools wie Zabbix haben und in der Lage sein, Netzwerke kontinuierlich zu überwachen und Probleme frühzeitig zu erkennen.
- Analyse von Netzwerkdaten: Expertise in der Analyse von Netzwerkverkehr und Protokollen zur Identifikation von Leistungs- und Sicherheitsproblemen.

7. Entwicklung von benutzerfreundlichen Interfaces

- Web-basierte Interfaces: Erfahrung in der Entwicklung von benutzerfreundlichen und mandantenfähigen Weboberflächen, die es Administratoren ermöglichen, Konfigurationsänderungen und Monitoring-Aufgaben durchzuführen.
- Self-Service-Schnittstellen: Der Anbieter muss in der Lage sein, Self-Service-Interfaces für verschiedene Benutzerrollen zu entwickeln, um die Konfiguration zu vereinfachen.

8. Modulare Softwareentwicklung und Open-Source-Expertise

- Modulare Architektur: Der Anbieter muss in der Lage sein, modulare und skalierbare Lösungen zu entwickeln, die sich an die spezifischen Bedürfnisse der Infrastruktur anpassen lassen.
- Open-Source-Erfahrung: Der Anbieter muss über umfassende Erfahrung in der Implementierung und Anpassung von Open-Source-Lösungen verfügen, inklusive der Bereitstellung von Quellcode, Dokumentation und Lizenzanforderungen.

10. Projektmanagement und agile Entwicklungsansätze

- Agile Methoden: Erfahrung mit agilen Methoden wie Scrum oder Kanban ist notwendig, um iterative Entwicklungszyklen mit kurzen Feedback-Schleifen umzusetzen.
- Anforderungsmanagement: Der Anbieter muss in der Lage sein, ein effektives Anforderungsmanagement durchzuführen und gemeinsam mit dem Auftraggeber die Workflows und Funktionalitäten kontinuierlich anzupassen und zu optimieren.

Ein Nachweis über die geforderten fachlichen Kompetenzen kann über Zertifikate oder Projektreferenzen der letzten 5 Jahre erfolgen. Referenzen für ähnliche Projekte, idealerweise auch im Hochschulumfeld oder im öffentlichen Sektor.

Ansprechpartner

Der Auftragnehmer definiert für den AG einen Ansprechpartner, um eine kundengerechte Beratung und Betreuung sicherzustellen. Dies gilt für die gesamte Vertragslaufzeit. Eine erste Benennung des Ansprechpartners genügt bei der Auftragserteilung. Bei einer Änderung der Ansprechpartnerin/des Ansprechpartners während der Vertragslaufzeit ist die/der neue Ansprechpartnerin/Ansprechpartner umgehend zu nennen.

Zugriff

Der AG stellt den Auftragnehmer einen gesicherten Zugang zu den Systemen zur Verfügung. Dieser wird bei Bedarf freigeschaltet und steht für die Dauer der Arbeiten zur Verfügung. Alle Aktionen sind mit dem AG abzustimmen und zu dokumentieren.

Datenschutz

Dem Angebot muss eine Beschreibung der technischen und organisatorischen Maßnahmen (TOMs) nach Art. 32 Datenschutz-Grundverordnung (DS-GVO) vom Bieter beiliegen.

Verschwiegenheitserklärung

Durch die Dienstleistungen erhält der Auftragnehmer Zugang zu erheblichen Informationen über die systemkritische Infrastruktur der OVGU. Um die Vertraulichkeit und Sicherheit dieser sensiblen Informationen zu gewährleisten, wird eine Verschwiegenheitserklärung verlangt. Diese Erklärung dient dazu, die Verpflichtungen des Auftragnehmers hinsichtlich des Schutzes vertraulicher Informationen festzulegen.

Vertragslaufzeit

Durch die Größe und Komplexität des Projektes muss ein Abruf der vereinbarten Leistung in den nächsten 5 Jahren möglich sein.

Es werden monatlich die Aufwendungen und die Projektziele besprochen und dementsprechend von den beiden Parteien abgezeichnet. Die Abrechnung erfolgt vierteljährlich auf Basis von Stundenzetteln die sich aus den vereinbarten Arbeiten und Zielen ergeben. Der AN stellt auf deren Basis den AG die Leistung vierteljährlich rückwirkend in Rechnung.

Bei Nichterfüllung, eklatanter Abweichung oder nicht nachkommen von Anforderungen aus dem Rahmen der Beauftragung kann der Vertrag vierteljährlich fristlos gekündigt werden.

Leistungsumfang

Pos	Bezeichnung/Beschreibung	Geschätzter Aufwand
1	**Projekt- und Servicemanagement / Consulting und Weiterbildung** • Abstimmung der Anforderung/Lösungen • Analyse der Anforderungen • Bedarfsanalyse • Diskussion und Abstimmung der Änderungen • Workshops zur Abstimmung/Wissenstransfer	2400 Personen Stunden

2 Software Entwicklungsleistung / Anpassung 6400 Personen Stunden

- jegliche Entwicklungsleitung
- Software-Entwicklung muss bis Ende des 3. Jahres abgeschlossen sein

3 Integration in unsere Infrastruktur Als Bestandteil o.g. Stunden

- fortlaufend, bis spätestens Ende des 5. Jahres

1 Personentag entspricht 8 Personen Stunden

Leistungsabruf
Die Erbringung der Gesamtleistung ist auf 5 Jahre angelegt. Die Verteilung der Leistung über die Jahre wird wie folgt geschätzt.

Jahr	Prozentualer Anteil
1.	20 %
2.	40 %
3.	20 %
4.	10 %
5.	10 %

Die Software-/Produktentwicklung muss bis zum Ende des 3. Jahres abgeschlossen sein.
Die Integration in unsere Infrastruktur muss spätestens bis Ende des 5. Jahres erfolgt sein.

Bewertung

Neben den für die formale Zulassung zu Ausschreibung zu erbringen Dokumente sind wie im Text beschreiben noch folgende Dokumente/Nachweise zu erbringen.

- Unternehmensprofil mit Mitarbeiterverteilung (Plausibilität der Aufgabenverteilung bzw. Zuordnung zum Thema, für das die jeweilige Expertise siehe ab S. 7 (1.-10.) erforderlich ist)
- Nachweise zur Befähigung einer erfolgreichen Umsetzung des Projektes (z. B. als Mitarbeit in abgeschlossenen Projekten oder über Zertifikate)
- Referenzen für vergleichbare ähnliche Projekte, idealerweise im Hochschulumfeld oder im öffentlichen Sektor (letzte 5 Jahre)
- kurze Beschreibung des Projektablaufes in fachlicher und zeitlicher Hinsicht (Umsetzungskonzept)

Wenn alle Nachweise und Beschreibungen der Referenzen vollständig vorliegen und den Anforderungen entsprechen, wird anschließend das Angebot auf Übereinstimmung mit den Vorgaben geprüft. Wenn alle diese Bedingungen erfüllt sind, wird der Zuschlag auf der Grundlage des Preises erteilt.