STADT BOCHUM

Auswahl und Einführung eines
Identity & Access Management Tools
Az. StBo_ZVS1_2026_00542_OV_IT

Leistungsbeschreibung **(Anhang 01)**

Inhaltsverzeichnis

1. Leistungsbeschreibung 2
2. Nutzen des Projekts 2
   2.1 Joiner 2
   2.2 Mover 2
   2.3 Leaver 3
   2.4 Rollenbasiertes Zugriffsmanagement 3
3. Leistungspakete 3
   3.1 Lizenzen (Subscriptions) 3
   3.2 Durchführung des Projektes zur Implementierung des IAM Systems 3
      3.2.1 Projektorganisation 3
      3.2.2 Anforderungsanalyse 3
      3.2.3 Erarbeitung Projektziele / Nicht-Ziele 4
      3.2.4 Ermittlung der Aufwände 4
      3.2.5 Kommunikation (integrierte 360 Grad Kommunikation) 4
   3.3 Implementierung des IAM-Systems 4
   3.4 Unterstützungsleistungen nach Beendigung der Implementierungsphase 5
4. Rahmenbedingungen 6

1. Leistungsbeschreibung

Die Stadt Bochum benötigt eine moderne Lösung im Bereich Identity & Access Management, um optimierte, ökonomische und sichere digitale Arbeitsweisen für die Mitarbeitenden zu gewährleisten.

Es handelt sich hier um ein zweistufiges Projekt, welches sowohl aus der Abbildung von Organisationsstrukturen und Optimierung von Prozessen (u.a. Joiner/Mover/Leaver Prozess, Workflows, De-/Provisionierung von Usern, Self Services, Single-Sign-On, Multifaktor Authentifizierung, Clearing Center) als auch der Implementierung des Systems mit anschließendem Betrieb und Support besteht. Zu Beginn der Inbetriebnahme ist insbesondere eine Hypercare-Phase vorgesehen.

Aktuell hat die Stadt Bochum hier Handlungsbedarf, da ein verwaltungsweites Konzept zur Administration von Identitäten und Zugriffsrechten sowie die passende technische Umsetzung fehlt. Das bestehende On-Prem System erfüllt die Anforderungen nur zu einem geringen Teil. Es ermöglicht weder eine ausreichende Automatisierung der Prozesse bei Authentifizierung und Berechtigung noch eine Anbindung der wichtigsten eingesetzten Verzeichnisdienste und Fachverfahren.

2. Nutzen des Projekts

Das Projekt soll zur Stärkung und Optimierung der IT-Prozesse (Joiner/Mover/Leaver) bei der Stadt Bochum beitragen und somit die IT-Sicherheit verwaltungsweit deutlich erhöhen.

Insbesondere soll auch durch die Einführung eines rollenbasierten Berechtigungskonzept nach dem Least-Privilege-Prinzip die Resilienz der IT-Umgebung gegenüber Cyberangriffen u. Ä. deutlich erhöht werden.

Strukturelle Schwächen der bestehenden Prozesse und Systeme sollen im Rahmen des Projektes beseitigt werden.

2.1 Joiner

Bei der Stadt Bochum gibt es zurzeit keinen definierten und dokumentierten Prozess für das Onboarding neuer Mitarbeitenden. Benutzerkennungen und Berechtigungen werden zum Teil „auf Zuruf“ eingerichtet. Im Rahmen des Projektes soll ein effizienter Prozess auf Basis der beteiligten Stellen bei der Stadt Bochum erarbeitet werden.

2.2 Mover

Die Arbeitsplatzumgebung in einer großen Organisation wie der Stadtverwaltung unterliegt ständigen Veränderungen. Bei einem internen Wechsel der Mitarbeitenden ist es erforderlich, dass die Berechtigungsstrukturen möglichst automatisiert angepasst werden.

Derzeit wird davon ausgegangen, dass sowohl für Nutzerkonten als auch für Berechtigungen ein Clearing Prozess benötigt wird.

2.3 Leaver

Es gibt derzeit einen großen Bestand an inaktiven Nutzerkonten, die ein hohes Sicherheitsrisiko darstellen. Ein Teil der inaktiven Nutzerkonten ist Mitarbeitenden zuzuordnen, die temporär abwesend sind. Der andere Teil der Nutzerkonten ist ausgeschiedenen Mitarbeitenden zuzuordnen und deaktiviert.

Im Zuge des Projekts wird definiert, wie mit inaktiven Nutzerkonten umzugehen ist und wann deaktivierte Nutzerkonten bzw. deren Daten gelöscht werden.

Durch einen solchen Prozess können die Angriffsvektoren reduziert werden.

2.4 Rollenbasiertes Zugriffsmanagement

Rechte und Rollen von Anwendenden sollen nur von deren Aufgaben abhängig sein, nicht von der hierarchischen Einordnung. Pseudo-Rollen (eine Rolle nur für Zuweisung eines Rechtes) sind zu vermeiden. Dieser Ansatz verfolgt den Nutzen, die De-/ Provisionierung zu standardisieren.

Mit den derzeitigen Systemen können keine vergangenen Hierarchien abgebildet werden (z.B. "Wer war Projektmanager in Projekt XY? Wer hat dort das Controlling gemacht? ...“).

Im Rahmen des Projekts ist zu ermitteln, ob die Veränderungshistorie mit Hilfe eines Systems und Prozesses ökonomisch nachvollzogen werden kann.

3. Leistungspakete

3.1 Lizenzen (Subscriptions)

- Bereitstellung von Lizenzen (Subscriptions) für die implementierte, eingerichtete und eingeführte IAM-Lösung entsprechend den Vorgaben der Stadt Bochum

3.2 Durchführung des Projektes zur Implementierung des IAM Systems

3.2.1 Projektorganisation

- Übernahme der Gesamtprojektleitung
- Erstellung eines Projektzeitplans
- Umfangreiche Projektdokumentation
- Regelmäßige Abstimmungsmeetings
- Unterstützung bei der Entwicklung und dem Controlling des Projektplans

3.2.2 Anforderungsanalyse

- Ist-Analyse / Soll-Analyse
- Prozessdefinition

3.2.3 Erarbeitung Projektziele / Nicht-Ziele

- Erkennen und Beschreiben von Projektzielen / Nicht-Zielen (Scoping/ Outscoping)
- Priorisierung der Projektziele
- Risikomanagement

3.2.4 Ermittlung der Aufwände

- Ressourcenschätzung für die Implementierung (Zeit, Kosten, Personal)

3.2.5 Kommunikation (integrierte 360 Grad Kommunikation)

- Entwerfen einer nachhaltigen Kommunikationsstrategie
- Ausarbeitung und Vorstellung der Projekt-Mehrwerte
- Erstellung eines Schulungskonzeptes für die Administratoren & Anwendenden

3.3 Implementierung des IAM-Systems

Am Ende des Projekts sollen die folgenden Produkte/Ergebnisse vorliegen bzw. implementiert sein:

- Eindeutige Objektdefinition (autoritative Ablageorte, Verantwortlichkeiten und Objektstrukturen) für Rollen, Rechte, Anwender und Systeme (Life Cycle Management)
- Definition der Zuständigkeiten/Verantwortlichkeiten im operativen Betrieb und der Prozesse inkl. Service Level Agreements (SLAs)
- Optimierte Provisionierung u. Deprovisionierung von Usern
- Optimierter und definierter Joiner/Mover/Leaver Prozess
- Workflows (synchronisierte Verteilungsprozesse von Software und Usern) mit einem eindeutig führenden Merkmal
- Definition von Clearing Prozessen sowie deren operativer Umsetzung
- Standardisierte Schnittstellen, die Multifaktor-Authentifizierung (MFA) für alle Plattformen und Systeme anbieten
- Self-Service, der so umfassend wie möglich für alle definierten Prozesse angeboten wird
- Dokumentierte Berechtigungskonzepte inkl. Berechtigungshistorie
- Anbindung von Applikationsanwendungen (siehe Abschnitt BOC-IAM-200 Integrationen im Dokument Anforderungskatalog Ausschlusskriterien)
- Eindeutige Definition der Single-Sign-On-Wege (SSO)
- Berücksichtigung der Empfehlungen aus dem BSI-Grundschutz

3.4 Unterstützungsleistungen nach Beendigung der Implementierungsphase

- Service Desk und Störungsannahme
  - Zentrale Rufnummer und E-Mail-Adresse für Störungsmeldungen.
  - Erreichbarkeit während definierter Servicezeiten.
  - Ticket-System bzw. Self-Service-Portal ist wünschenswert.
  - Deutschsprachiger Support.
  - Fernwartung über die von der Stadt vorgegebenen Werkzeuge (aktuell Microsoft Teams).
- Service Level Agreements (SLA)
  - Reaktionszeiten
  - Bearbeitungszeiten
  - Eskalationsverfahren
  - Prioritätsklassen
  - Verfügbarkeitsanforderungen
  - Reporting und Service-Reviews
- Betriebsunterstützung
  - Unterstützung des Regelbetriebs
  - Proaktive Überwachung der Lösung
  - Erstellung von Betriebs- und Statusberichten
  - Unterstützung bei Konfigurationsänderungen
  - Incident-, Problem- und Request-Management
- Wartung und Patchmanagement
  - Durchführung notwendiger Updates und Patches
  - Frühzeitige Ankündigung von Wartungsfenstern
  - Sicherheitsupdates zeitnah nach Verfügbarkeit
  - Information der Stadt über Änderungen und Auswirkungen
- Dokumentation
  - Betriebshandbuch
  - Administrationshandbuch
  - Technische Dokumentation
  - Notfall- und Supportprozesse
  - Installations- und Updateanleitungen
  - Dokumentation von Berechtigungskonzepten und Schnittstellen
- Wissenstransfer und Schulungen
  - Administratorenschulungen
  - Übergabe in den Regelbetrieb
  - Begleitung einer Hypercare-Phase nach Go-Live

4. Rahmenbedingungen

- Die Stadt Bochum beschäftigt rund 7.000 Mitarbeitende. Auf den Client PCs wird durchgängig Windows 11 eingesetzt, mobile Endgeräte basieren auf Apple iOS/iPadOS.
- Seitens der Stadtverwaltung Bochum arbeitet ein Kernteam aus mehreren Personen für das Projekt, für einige Dienste muss auf weitere Mitarbeitende aus dem Regelbetrieb zurückgegriffen werden.
- Der Auftragnehmer kann die Leistung auch mit unterschiedlichen Personen erbringen, hat in diesem Fall aber dafür zu sorgen, dass alle eingesetzten Mitarbeitenden immer über den gleichen Projektkenntnisstand verfügen.
- Das Projekt muss unmittelbar nach Zuschlagserteilung starten und die vollständige Implementierung und Ersteinrichtung nach 12 Monaten abgeschlossen sein.
- Die Erbringung der Leistung wird im Regelfall remote per Webkonferenz erfolgen. Wird ein Vor-Ort-Einsatz nötig, ist dieser unter folgender Adresse zu erbringen: Hans-Böckler-Straße 19, 44787 Bochum.
- Die Kommunikationssprache ist Deutsch. Die entwickelten Dokumente sind ebenfalls in Deutsch zu erstellen, in Ausnahmefällen ist auch nach vorheriger Absprache Englisch zugelassen.
- Es ist ein einheitlicher Stundennachweis für alle eingesetzten Mitarbeitenden zu führen, dieser muss der Abrechnung beigefügt werden. Als kleinste Abrechnungseinheit gilt eine halbe Stunde.
- Der Auftragnehmer verpflichtet sich, Rechnungen in elektronischer Form der Stadt Bochum (Leitweg-ID: 05911-31001-89) im Format der XRechnung über das Bereitstellungsportal NRW (Adresse: https://erechnung.nrw) zur Verfügung zu stellen.