Anforderungskatalog

Implementierung von IT-Lösungen

in die IT-Infrastruktur & Cybersicherheit der BGK IT Services GmbH

Systemanforderungen

Inhalt

1. Einleitung 3
   1.1 Rahmenbedingungen zur Bereitstellung von IT-Lösungen 3
2. Grundsätzliches zur zentralen Bereitstellung 3
   2.1 Bereitstellung von Server und Storage 3
      2.1.1 Serverplattform 3
      2.1.2 Basis Infrastruktur 3
      2.1.2.1 Verfügbarkeit & Ausfallsicherheit 4
      2.1.2.2 Mandantentrennung & Isolation 4
      2.1.2.3 Namenskonventionen 4
      2.1.2.4 Monitoring & Betrieb 4
      2.1.2.5 Patch- & Lifecycle-Management 4
      2.1.2.6 Backup, Restore & Wiederanlauf 4
   2.2 IT-Netzwerk und Netzwerk-Sicherheit 5
      2.2.1 Grundvoraussetzung im Netzwerk 5
      2.2.2 WAN Fähigkeit 5
   2.3 Zugriffe 5
      2.3.1 Authentifizierung 6
      2.3.2 Public Key Infrastructure (PKI) 6
      2.3.3 Administrative Zugriffe 7
      2.3.4 Protokollierung & Nachvollziehbarkeit 7
      2.3.5 Sitzungs- & Zugriffskontrolle 7
      2.3.6 Sonderfälle & Ausnahmen 7
   2.4 Datenbank Cluster 7
   2.5 Client Zugriff 8
   2.6 IT Sicherheit 8
   2.7 IT-Service 9

1. Einleitung

Zentrale Anwendungen, die im Kontext der BG Kliniken betrieben werden sollen, sind durch die zentrale IT der BG Kliniken (BGK IT Services GmbH) bereitzustellen. Hierbei gelten Rahmenbedingungen und Systemanforderungen, die es einzuhalten gilt

1.1 Rahmenbedingungen zur Bereitstellung von IT-Lösungen

2. Grundsätzliches zur zentralen Bereitstellung

Die BG Kliniken betreiben ein BG-weites Netzwerk mit zentralen und dezentralen Rechenzentren. Anwendungen werden grundsätzlich in den zentralen Rechenzentren bereitgestellt, aus denen die Standorte versorgt werden. Lokale an den Standorten vorhandene Systeme unterstützen die Bereitstellung.

- Georedundante Bereitstellung, möglicherweise über große Entfernungen
- Zentrale Hauptkomponenten und dezentrale Caching-Systeme
- Backup- und Restore- Mechanismen werden zur Verfügung gestellt und im Rahmen der Installation getestet und dokumentiert (Wirtschaftsprüferfest)
- Hochverfügbarkeit der Lösung ist gegeben und Produktbestandteil bzw. kann in vorhandene Lösung integriert werden (z.B. Citrix Netscaler, HAProxy, MSSQL Server Cluster)
- Mandantentrennung
    - Die einzelnen BG Kliniken sind wirtschaftlich selbständige Tochtergesellschaften der BG Kliniken Holding.
    - Daher kann bei einer zentralen Bereitstellung einer klinikweiten Anwendung eine durchgängige Trennung der Mandanten zur Gewährleistung einer Datentrennung im Sinne des Datenschutzes sein.
    - Die Anwendung muss demnach in der Lage sein, Datenbestände in geeigneter Weise nach Mandanten zu trennen.
    - Eine zentrale Anwendung ist nicht Mandantenfähig, wenn sie mehrfach bereitgestellt wird.

2.1 Bereitstellung von Server und Storage

IT-Anwendungssysteme werden grundsätzlich auf IT-Ressourcen der BG Kliniken bereitgestellt. Dabei gelten folgende Rahmenbedingungen, sofern keine begründete Ausnahmeanforderung vorliegt.

2.1.1 Serverplattform

- Bereitstellung von virtuellen Anwendungsservern
- VMware vSphere Hypervisor, Version 8 - Stand Januar 2026 oder höher
- 2 vCPU, 8GB RAM, 80GB Systempartition Thin Provisionierung
- Unterstützte Betriebssysteme / OS:
    - Microsoft Windows Server ab Version 2022 (oder höher)
    - Ubuntu Linux ab Version 24.04 LTS (oder höher)

2.1.2 Basis Infrastruktur

- Zentrale Bereitstellung in den BGK IT Rechenzentren
- Hyperconverged Infrastructure (HCI) Server mit vSAN Storage Plattform
- SAN Storage möglich
- Deduplizierung auf Storage

- Standard-Backup der Server durch BGK IT
- Tägliches Veeam Backup der Server (Crach-Konsistent)
- Individuelle RTO (Recovery Time Objective) und RPO (Recovery Point Objective) möglich, Standard 6 Wochen
- Agentenbasierte Datenbanksicherung möglich

2.1.2.1 Verfügbarkeit & Ausfallsicherheit

- Die Infrastruktur ist hochverfügbar ausgelegt (z. B. Clusterbetrieb).
- Kritische Komponenten sind redundant ausgeführt, um Single Points of Failure zu vermeiden.

2.1.2.2 Mandantentrennung & Isolation

- Systeme sind logisch voneinander getrennt (z. B. durch Netzwerk- und Ressourcenisolation).
- Die Trennung von Produktiv-, Test- und Entwicklungsumgebungen ist sichergestellt.

2.1.2.3 Namenskonventionen

Für alle Infrastruktur-, System- und Anwendungsobjekte gelten einheitliche Namenskonventionen, um eine eindeutige Identifikation, einen sicheren Betrieb sowie eine nachvollziehbare Administration sicherzustellen.

Die Namenskonventionen werden zentral durch die BGK IT definiert und dokumentiert und gelten insbesondere für:

- Server und virtuelle Maschinen
- Datenbanken, Datenbankinstanzen und Aliase
- Anwendungen und Applikationskomponenten
- Benutzer-, Gruppen- und Servicekonten
- Netzwerkobjekte (z. B. VLANs, Subnetze, Load Balancer)

2.1.2.4 Monitoring & Betrieb

- Zentrales Monitoring für Systemverfügbarkeit, Ressourcenverbrauch und Fehlerzustände ist implementiert.
- Kritische Ereignisse werden automatisiert erkannt und entsprechend eskaliert.

2.1.2.5 Patch- & Lifecycle-Management

- Betriebssysteme, Hypervisor und Infrastrukturkomponenten unterliegen einem regelmäßigen Patch- und Update-Prozess.
- Nicht mehr unterstützte Versionen (End of Life) werden nicht betrieben.

2.1.2.6 Backup, Restore & Wiederanlauf

- Backups werden regelmäßig auf Integrität geprüft.
- Wiederherstellungstests (Restore-Tests) werden in definierten Intervallen durchgeführt und dokumentiert.
- Backup-Daten sind vor unbefugtem Zugriff geschützt.

2.2 IT-Netzwerk und Netzwerk-Sicherheit

Es gelten höchste IT-Sicherheitsanforderungen, insbesondere die Mikrosegmentierung von Netzwerken zwischen IT-Systemen mit unterschiedlichen Nutzungsszenarien. Die Kommunikation zwischen den Netzwerken (VLANs) erfolgt daher ausschließlich über dedizierte Portfreigaben.

Die Standardkommunikation findet über IPv4 und DNS statt.

2.2.1 Grundvoraussetzung im Netzwerk

Der Netzwerkflow sowie das Systemschaubild stellen die Kommunikationsbeziehungen zwischen den einzelnen Systemkomponenten dar und visualisieren die Datenflüsse innerhalb der Gesamtarchitektur. Sie dienen als Grundlage für die sicherheitstechnische Bewertung, insbesondere zur Definition von Firewall-Regeln, Zonenübergängen und Abhängigkeiten zwischen den Systemen.

Zusätzlich ist eine Kommunikationsmatrix erforderlich, in der die zulässigen Kommunikationsbeziehungen (Quell-/Zielsysteme, Protokolle, Ports und Richtungen) eindeutig dokumentiert sind.

2.2.2 WAN Fähigkeit

Die Applikation sollte für den Betrieb über Wide Area Networks (WAN) ausgelegt und unterstützt den Zugriff aus verteilten Netzen und Standorten. Die Kommunikation zwischen Clients, Anwendungsservern und weiteren Systemkomponenten erfolgt netzwerkunabhängig und ist für höhere Latenzen sowie schwankende Bandbreiten ausgelegt.

Die Applikation wird zentral in den Rechenzentren der BGK IT betrieben. Der Zugriff auf die Applikation erfolgt ausschließlich über das WAN. Die WAN-Fähigkeit der Applikation stellt somit eine zentrale Abhängigkeit für den ordnungsgemäßen Betrieb dar.

Die Applikation nutzt ausschließlich definierte und dokumentierte Kommunikationsbeziehungen. Netzwerk Latenzen oder temporäre Verbindungsunterbrechungen führen nicht zu inkonsistenten Datenzuständen. Wiederholungsmechanismen und Timeouts sind angemessen konfiguriert.

Alle WAN-Verbindungen erfolgen über das MPLS - Corporate Network der BG Kliniken (CN-BGK) verschlüsselt und unter Berücksichtigung der geltenden Sicherheitsvorgaben der BGK IT.

Die Performance der Applikation ist so ausgelegt, dass sie auch bei WAN-Zugriffen einen stabilen und nutzbaren Betrieb ermöglicht. Bandbreiten- und Latenzanforderungen sind dokumentiert und werden bei der Auslegung der Infrastruktur berücksichtigt.

Die WAN-Fähigkeit ist Bestandteil der Architektur- und Sicherheitsbewertung und wird bei Änderungen an der Netz- oder Systemarchitektur erneut geprüft.

2.3 Zugriffe

Die Infrastruktur wird gemäß einem 3-Tier-Modell (Tier 0–2) betrieben.

- Tier 0 stellt die höchste Sicherheitszone dar und umfasst sicherheitskritische Infrastrukturkomponenten.

- Tier 1 bildet die Anwendungs- und Serverebene.
- Tier 2 stellt die Client- und Benutzerebene dar.

Zugriffe zwischen den Tier-Ebenen erfolgen ausschließlich von höherem zu niedrigerem Tier und maximal über eine Tier-Grenze hinweg. Direkte Zugriffe über mehrere Tier-Ebenen hinweg sind nicht zulässig.

Anwendungen auf der Clientschicht (Tier 2) greifen ausschließlich auf Anwendungen der Anwendungsschicht (Tier 1) zu.

Benutzer arbeiten ausschließlich im Tier 2 und haben keinen direkten Zugriff auf Systeme der Tier-Ebenen 0 und 1.

Administrative Konten und Berechtigungen sind tierübergreifend strikt getrennt. Administratoren dürfen jeweils nur innerhalb des ihnen zugeordneten Tier-Levels tätig sein. Eine Vermischung von administrativen Rechten über mehrere Tier-Ebenen hinweg ist nicht zulässig.

2.3.1 Authentifizierung

Die Authentifizierung erfolgt auf Basis von Active Directory (Kerberos) und innerhalb der Anwendung erfolgt rollenbasiert (RBAC) nach dem Least-Privilege-Prinzip. Rollen und Berechtigungen werden zentral verwaltet und regelmäßig überprüft. Änderungen an Berechtigungen sind zu dokumentieren und nachvollziehbar zu genehmigen.

Eine Synchronisation von Benutzerkonten und Attributen in die Anwendung ist möglich. Dabei muss sichergestellt sein, dass Änderungen an Konten und Attributen unverzüglich übernommen werden, insbesondere bei Sperrung oder Entzug von Berechtigungen.

Identitäten / Benutzerobjekte können über folgende Mechanismen bereitgestellt werden:

- Active Directory Domain Services (AD DS)
  - LDAPS
  - Kerberos
- Microsoft Entra ID
  - SAML
  - OAuth 2.0
  - SCIM
- 802.1X
- X.509 Zertifikatsbasierte Authentifizierung

2.3.2 Public Key Infrastructure (PKI)

Die Absicherung der Kommunikation sowie die Authentifizierung technischer Komponenten erfolgt über eine zentrale Public Key Infrastructure (PKI) der BGK IT. Die Kommunikation erfolgt grundsätzlich verschlüsselt.

- Alle eingesetzten Zertifikate werden durch eine vertrauenswürdige, von der BGK IT betriebene Zertifizierungsstelle (CA) ausgestellt.
- Die PKI dient zur:
  - Absicherung der Transportverschlüsselung (z. B. TLS),
  - gegenseitigen Authentifizierung von Systemen und Diensten,
  - optionalen Zertifikatsauthentifizierung von Benutzern oder Maschinen.

- Zertifikate sind eindeutig einem System, Dienst oder Benutzer zugeordnet.
- Die Verwendung von Wildcard-Zertifikaten ist ausgeschlossen.
- Private Schlüssel sind vor unbefugtem Zugriff zu schützen und dürfen das jeweilige Zielsystem nicht verlassen.
- Die Gültigkeitsdauer, Erneuerung und Sperrung (CRL/OCSP) von Zertifikaten wird zentral durch die BGK IT gesteuert.
- Abgelaufene oder kompromittierte Zertifikate sind unverzüglich zu sperren und zu ersetzen.
- Die eingesetzten kryptographischen Verfahren und Schlüssellängen entsprechen den jeweils aktuellen Sicherheitsvorgaben der BGK IT.

2.3.3 Administrative Zugriffe

- Administrative Zugriffe auf Anwendungs-, Datenbank- und Betriebssystemebene sind auf einen definierten Personenkreis beschränkt.
- Administratoranmeldungen erfolgen ausschließlich mit personengebundenen Konten; Sammel- oder Funktionskonten sind unzulässig (Ausnahme: technisch zwingend erforderlich, dann gesondert dokumentiert).
- Administrativer Zugriff erfolgt nur über gesicherte Management-Zugänge (z. B. Jump Hosts).

2.3.4 Protokollierung & Nachvollziehbarkeit

- Erfolgreiche und fehlgeschlagene Anmeldeversuche sowie sicherheitsrelevante Aktionen (z. B. Rollenänderungen) werden vollständig protokolliert.
- Protokolldaten sind vor Manipulation geschützt und werden gemäß den geltenden Aufbewahrungsfristen gespeichert.
- Eine Auswertung der Logs zu Sicherheitszwecken ist möglich.

2.3.5 Sitzungs- & Zugriffskontrolle

- Sitzungen werden nach definierter Inaktivität automatisch beendet.
- Gleichzeitige Mehrfachanmeldungen können eingeschränkt oder unterbunden werden.
- Zugriffe aus nicht vertrauenswürdigen Netzen können eingeschränkt oder zusätzlichen Prüfungen unterliegen.

2.3.6 Sonderfälle & Ausnahmen

- Temporäre Zugriffe (z. B. für Wartung oder Support) sind zeitlich begrenzt und nach Abschluss zu deaktivieren.
- Abweichungen von diesen Regelungen bedürfen einer dokumentierten Freigabe durch die BGK IT.

2.4 Datenbank Cluster

- Datenbanken werden in vorhandene MS SQL 2022 Datenbank Cluster integriert
- Named Instances sowie SQL-Aliase werden unterstützt.
- Es erfolgt eine strikte Trennung zwischen Datenbank- und Applikationsservern.
- Die Kommunikation erfolgt über definierte Ports; eine Nutzung der Standardinstanz (TCP 1433) ist nicht zulässig.
- Ggf. erforderliche zusätzliche SQL-Server-Komponenten (z. B. Reporting Services) sind zu beschreiben und deren technische Anforderungen klar zu definieren.
- Berechtigungen werden ausschließlich anwendungsbezogen und maximal bis zur Rolle „db_owner“ vergeben. Weitergehende Berechtigungen sind nicht zulässig.

2.5 Client Zugriff

Zentrale Anwendungen werden grundsätzlich auf Basis von Citrix Terminalservern als veröffentlichte Anwendung oder Desktop bzw. als VDI bereitgestellt. Die jeweilige Anwendung muss eine Bereitstellung über Terminalserver unterstützen.

Clientzugriffe erfolgen verschlüsselt auf den Anwendungsserver bzw. das Anwendungssystem in der jeweiligen Bereitstellungsebene (On-Premise, Cloud oder Hybrid).

Installations- und Update-Mechanismen der Client-Software (inkl. Abhängigkeiten) sollen automatisiert sein bzw. als non-interaktives Setup zentral verteilt werden können.

Bei Updates muss ein Self-Update der Anwendung ohne administrative bzw. erhöhte Rechte möglich sein, z. B. über einen lokalen Update-Dienst.

Erforderliche Lizenzen für Support und Wartung von Abhängigkeiten (z. B. Java) sind in der Lizenzierung enthalten oder es ist auf Java zu verzichten. Webanwendungen müssen mit dem „MS Edge (Chromium)“ kompatibel sein.

Updates von Abhängigkeiten, insbesondere Security-Updates (z. B. .NET, Java, Python, Perl), müssen zeitnah möglich sein.

2.6 IT Sicherheit

IT-Sicherheit ist bei den BG Kliniken ein kontinuierlicher Prozess. Zum Schutz der Unternehmenswerte gelten verbindliche und unumstößliche Sicherheitsregeln:

- IT-Systeme und deren Zugriffe werden grundsätzlich nach dem Zero-Trust-Designprinzip etabliert.
- Der Zugriff auf Webseiten sowie die gesamte Kommunikation erfolgt ausschließlich verschlüsselt. Die erforderlichen Zertifikate werden über die PKI des Auftraggebers bereitgestellt.
- Endpoint-Security ist auf jedem Client verpflichtend vorhanden und wird vom Auftraggeber vorgeben.
- Mikrosegmentierung der Anwendungsserver ist umzusetzen.
- Kommunikationsbeziehungen sind vollständig darzustellen, inklusive schematischer Darstellung sowie einer Firewall- / Kommunikationsmatrix (insbesondere Ost-West-Traffic).
- Berechtigungen werden nach dem Prinzip des „Least Privilege“ konzipiert und vergeben.
- Die Benutzerverwaltung kann an ein zentrales Active Directory oder an mehrere dezentrale Active Directories angebunden werden.
- Die Gruppenverwaltung kann ebenfalls an ein oder mehrere Active Directories angebunden werden.
- Single-Sign-On-Verfahren (SSO) werden unterstützt.
- Remote-Zugriffe erfolgen ausschließlich über die vom Auftraggeber bereitgestellten Mechanismen.
- Backups können verschlüsselt und mandantenfähig abgelegt werden.
- Logfiles müssen am zentralen SIEM angebunden werden.
- Die Anbindung am Vulnerability- / IT Schwachstellen Management muss gewährleistet sein.

2.7 IT-Service

Zur Bereitstellung der zentralen Anwendungen gehören vollständige Dokumentationen, die das IT-Service-Management (ITSM) unterstützen. Die relevanten ITSM-Prozesse sind klar zu dokumentieren und transparent zu kommunizieren.

Für Wartungszwecke kann ein Fernwartungszugriff eingerichtet werden. Dabei gelten ausschließlich die Regelungen der BGK IT Services GmbH. Der Fernwartungszugriff unterliegt folgenden Rahmenbedingungen:

- Privilegierter Zugriff auf IT-Systeme der BG Kliniken ist nur auf Basis eines vorliegenden Auftragsverarbeitungsvertrags (AV-Vertrag) zulässig.
- Der technische Zugriff erfolgt ausschließlich über die von den BG Kliniken bereitgestellte sichere Lösung.
- Vor jedem technischen Zugriff ist ein Freigabe-Workflow zwingend erforderlich.
- Zugriff:
    - ist zeitlich begrenzt (Zeitraum und Dauer),
    - wird vollständig protokolliert und die Session aufgezeichnet,
    - erlaubt keinen direkten Datentransfer (Inbound oder Outbound). Der Datentransfer erfolgt ausschließlich über eine zentrale Datensicherheitsschleuse.