IT-Infrastrukturbeschreibung

Anlage zur Leistungsbeschreibung

Version: 1.18

Stand: 22.05.2024 / 21.01.2025

Inhaltsverzeichnis

Anhangverzeichnis

Abkürzungsverzeichnis

AD	Active Directory
ASP	Active Server Pages
CA	Certificate Authority
CN	Common Name
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
ECM	Enterprise Content Management
FMS	Formularmanagementsystem
IEEE	Institute of Electrical and Electronics Engineers
IEEE 802.3ae	10Gb/s Ethernet
IEEE 802.3z	heute IEEE 802.3 Clause 38 (Gigabit Ethernet auf Glasfaser und Twinax-Kabel)
IT-SRL	IT-Sicherheitsrichtlinie der LHH
IP	Internet Protocol
ISAPI	Internet Server API
LAN	Local Area Network
LHH	Landeshauptstadt Hannover
LWL	Lichtwellenleiter
MAPI	Messaging Application Programming Interface
MDM	Mobile Device Management
OMS	Output-Management-Server
OE	Organisationseinheit der LHH
PKI	Public Key Infrastructure
PKS	Public Key Service
SigG	Signaturgesetz
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
TCOS	TeleSec Chipcard Operating System
TCP	Transmission Control Protocol
USB	Universal Serial Bus
USV	Unterbrechungsfreie Stromversorgung
VPN	Virtual Private Network

1 Einleitung

Dieses Dokument enthält eine zusammenfassende Beschreibung der bei der Landeshauptstadt Hannover (LHH) eingesetzten IT-Infrastruktur. Die beschriebene IT-Infrastruktur bildet den Rahmen, in den sich sämtliche angebotenen Produkte voll kompatibel eingliedern müssen. Die vorhandene Infrastruktur muss mit den angebotenen Produkten voll nutzbar sein. Eine Überlagerung von bereits vorhandenen Funktionalitäten mit neuen Produkten ist nicht zulässig.

Kein angebotenes Produkt und keine angebotene Lösung darf einen ‚single Point of failure' enthalten, dessen Ausfall in der geplanten Endausbaustufe zu Funktionsstörungen der LHH führen würde, die mehr als 25% der unterstützten Arbeitsplätze beträfen.

Der IT-Betrieb der LHH ist zentral in einem Zwei-Standorte-Konzept organisiert. Alle angebotenen Produkte müssen geeignet sein, im Falle redundanter Auslegung in zwei räumlich getrennten Standorten betrieben zu werden.

2 Netzwerk

2.1 Physische Verbindung

Die grundsätzliche physikalische Verbindung erfolgt durch stadteigene oder angemietete Lichtwellenleiter (LWL). Seltener werden auch Kupferkabelwege verwendet. Kleinere Liegenschaften mit wenigen Arbeitsplätzen vor Ort (Schulen etc.) werden über Standard-DSLAnschlüsse unter Verwendung von verschlüsselten Zugangstechniken angebunden. Als Vermittlungsprotokoll wird vollständig auf TCP/IP v.4 gesetzt. Die Anbindung des städtischen Datennetzes an das Internet ist redundant über 5.000 Mbit/s ausgelegt und erfolgt abgesichert durch eine zentrale Firewall. Zusätzlich besteht eine redundante Verbindung mit 100 Mbit/s an das niedersächsische Landesnetz und damit mittelbar an das DOI-Netz. Externe Zugänge (bspw. für Ratsmitglieder, Telearbeit) zum städtischen Datennetz bestehen in großer Anzahl. Diese Anbindungen werden über private Internetanbindungen oder dienstlich bereitgestellte Mobilfunkverbindungen realisiert. Die Anbindung erfolgt unter Verwendung von verschlüsselten Zugangstechniken.

2.2 Backbone

Das zentrale Verteilernetz besteht aus mehreren Standorten (Backbone-Knoten), die überwiegend mit 10 Gbit/s (IEEE 802.3ae, LWL, SingleModeFibre) angebunden sind. Einzelne Strecken wurden auf 40 Gbit/s (IEEE 802.3ba bzw. 802.3bm) umgestellt. Der Backbone ist in einer hierarchischen Struktur aufgebaut. Das Rechenzentrum ist direkt mit zentralen Core-Switchen verbunden, an welchen die Switche der Distributionsebene mit zwei redundanten 10Gbit/s (LWL) angebunden sind.

Die Netzsegmentierung erfolgt durch Routing in den Layer-3-Switches. Alle Netzknoten sind durch eine USV mit Notstromversorgung abgesichert. Die Anbindung der ca. 450 Standorte im Stadtgebiet erfolgt mit min. 2 Mbit/s (Kupfer) oder 1000 Mbit/s (LWL) an der Distributionsebene oder alternativ über eine VPN-Verbindung mit mindestens DSL 10 Mbit/s.

2.3 Arbeitsplätze

Die ca. 12.200 Arbeitsplätze sind entweder direkt per LWL (Fiber to the Desktop) oder in zunehmendem Maße per Kupfer über einen Büro- bzw. Kabelkanalswitch (Fiber to the Office) mit dem Backbone verbunden. In neuen Gebäuden kommt eine strukturierte Verkabelung (Kupfer) mit Etagenverteilern und einem Übergabepunkt zur Anbindung an den Backbone zum Einsatz. Die Arbeitsplätze sind in der Regel mit jeweils 100 Mbit/s (Full Duplex) angebunden, vereinzelt erfolgt eine Vernetzung mit 1 Gbit/s (Full Duplex).

Es sind ca. 90% der IT-Arbeitsplätze mit min. 100 Mbit/s (Full Duplex) am LHH LAN angebunden. Die verbleibenden 10% sind entweder mit 2 Mbit/s, 10Mbit/s oder mit 1Gbit/s angeschlossen. Ca. 200 kleine Standorte mit je 2 oder 3 Arbeitsplätzen sind per DSL erschlossen.

2.4 Netzwerkprotokolle

Als Netzwerkprotokoll wird TCP/IP v4 eingesetzt. Die Adressierung erfolgt über einen zentralen DHCP-Server unter Nutzung privater TCP/IP-Adressen nach RFC 1918. Weitere Netzwerkparameter werden über DHCP-Optionen konfiguriert.

Im Zuge der Migration zu IPv6 wird ein IPv4/IPv6-Dual-Stack-Betrieb eingeführt. Dabei muss die Betriebsart „Stateful Autoconfiguration“ unterstützt werden. Die Betriebsart wird von zentraler Stelle durch Setzen des M-Flag (Managed address configuration) und O-Flag (Other stateful configuration) auf den beteiligten IPv6-Routern gesteuert. Nutzt der Client IPv6 Privacy Extensions, müssen diese dauerhaft deaktiviert werden können.

2.5 WLAN-Infrastruktur

In verschiedenen Dienstgebäuden werden WLAN-Zugangsmöglichkeiten über eine zentral gesteuerte WLAN-Infrastruktur bereitgestellt. Die WLAN-Standards IEEE802.11 a/n/ac (5 GHz) und IEEE802.11 b/g/n (2,4 GHz) werden unterstützt. Die Authentifizierung im Mitarbeitenden-WLAN (= internes WLAN) erfolgt mit Hilfe von Maschinen- bzw. Benutzerzertifikaten
(IEEE802.1x-Methode). Der Anmeldung im Gast-WLAN erfolgt über „Gast-Tickets“ (WebAuth). Ein direkter Intranet-Zugang ist über das WLAN nicht möglich; es müssen vorhandene Gateways genutzt werden. Auf Anforderung wird in einzelnen Dienstgebäuden ein offenes WLAN zur Verfügung gestellt.

2.6 Verschlüsselte Zugangstechnik – Always-On

Arbeitsplätze, die über externe Zugänge angebunden sind, benutzen die Technik Microsoft „Always-On“. Es handelt sich dabei um eine transparente VPN-Technik. Sämtlicher Datenverkehr wird hierbei zum LHH-LAN geleitet (kein Split-Tunneling). Eine direkte Kommunikation mit dem Internet findet nicht statt (außer zur Always-On-Gegenstelle). Über Mechanismen des Betriebssystems wird basierend auf DNS-Abfragen der IP-Datenverkehr durch einen Tunnel geroutet. Bei Always-On wird der Datenverkehr durchgängig über IPv4 abgewickelt.

3 Hardware Infrastruktur

3.1 Client System

Im Folgenden werden für Neubeschaffungen verwendete Standard-PCs, Notebooks und Server mit deren Hardwareausstattung aufgelistet.

3.1.1 Desktop Computer (PC / Mini-PC / Grafikworkstation)

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

3.1.2 Mobile Computer (Notebook / Subnotebook)

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

3.1.3 Smartphones/Tablets

Es werden iPhones ab Version XR/XS mit der jeweils aktuellen Version des Betriebssystems eingesetzt. Die Geräte werden über ein vorhandenes MDM-System verwaltet, es kommen Mobilfunkverträge verschiedener Anbieter zum Einsatz. Die Geräte werden nicht über VPN in das LHH-LAN eingekoppelt. Neben den Smartphones werden das iPad (ab 6), iPad Air (ab 3), iPad Pro und iPad mini (ab 5) betrieben. Hierfür gelten die gleichen Rahmenbedingungen.

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

3.2 Server System

3.2.1 Rackserver

Die Beschaffung der Server erfolgt i.d.R. über Rahmenverträge.
Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

3.3 Storage System

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

4 Software Infrastruktur

4.1 Client Systeme

4.1.1 Allgemein

Als Standardbrowser werden Microsoft Edge und der Mozilla Firefox aus dem Extended Support Release (64-Bit) in der aktuellen Herstellerversion eingesetzt. Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

4.1.2 Desktop PC

Als Betriebssystem wird Windows 10 Enterprise in den Versionen 2021 LTSC (x64) und auslaufend 2019 LTSC (x64) eingesetzt. Windows 11 Enterprise ist in Vorbereitung. Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

4.1.3 Notebook / Subnotebook

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

4.1.4 Mini-PC

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

4.1.5 Smartphones

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

4.2 Server Systeme

4.2.1 Serverbetriebssystem

Als Betriebssysteme werden Microsoft Windows Server und Linux verwendet. Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

4.2.2 E-Mail

Das Emailsystem basiert auf Microsoft Exchange Server.

E-Mailpostfächer stehen für Personen und Gruppen sowie zur Organisation von Raumbelegungen zur Verfügung. Es stehen weder öffentliche Ordner noch Active-Directory integrierte Kontakte für externe Benutzer zur Verfügung.

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

4.2.3 Virtualisierung

Als Virtualisierungslösung wird VMware vSphere verwendet.

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

4.2.4 Datenbanken

Folgende relationale Datenbanken sind in aktuellen Versionen im Einsatz:

- MySQL
- MariaDB
- MS SQL Server Standard Edition
- PostgreSQL

Datenbankspezifische Anforderungen sind dem Anhang 2 *„DB-Anforderungen an Verfahrenssoftware*“ zu entnehmen.

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

4.2.5 Terminal Server Based Computing

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

4.2.6 Domino Server

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

4.2.7 Softwareverteilung

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

4.2.8 WebServer

Es werden Webserver verschiedener Hersteller verwendet. Folgende Konfigurationen sind gegeben:

- Microsoft IIS
  - ASP.NET
  - ISAPI Extensions möglich
  - Adobe Coldfusion – Standard Edition

- Apache Webserver
  - PHP und Perl Unterstützung in den aktuellen Versionen
  - auf Windows oder Linux basierend

- NGINX Webserver
  - auf Windows oder Linux basierend

- Apache Tomcat Standalone und Cluster

Webanwendungen, die aus dem Internet erreichbar sind (E-Government), werden durch einen Reverse-Proxy adressiert. Die Installation von Webanwendungen kann in Test-, QS- und Produktionsumgebungen auch mithilfe von gepflegten Docker-Containern realisiert werden:

- Docker
  - auf Linux basierend

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

4.2.9 Fax-Gateway

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

4.2.10 Scan-Server

Es wird Kofax Capture als Scan-Server verwendet.

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

4.2.11 Dokumentenmanagementsystem

Folgendes Dokumentenmanagementsystem ist im Einsatz:

- D.velop d.3

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

4.2.12 Jobscheduling-Server

Für die Automation von Prozessen auf Scheduling-Servern, wird die Automation Engine von der Firma Broadcom (ehem. ca technologies Automic) eingesetzt.

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

4.2.13 Output-Management-Server (OMS)

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

4.2.14 Docker

Für die Bereitstellung von Docker-Containern wird die jeweils aktuelle Docker Version auf den unterstützen Linux-Distributionen von RedHat/Rocky Linux oder Debian eingesetzt. Das Docker-Image, für die Erstellung des Docker-Containers, muss vom Entwickler aktuell und gepflegt bereitgestellt werden, damit dieses zum Einsatz kommen kann. Dies beinhaltet auch weitere Softwarekomponenten, die sich ggfs. im Docker-Image befinden oder weitere DockerImages, die für den Betrieb des ursprünglichen Docker-Containers notwendig sind. Der Einsatz von nicht vertrauenswürdigen und unsicheren Docker-Images ist nicht zulässig. Weiterhin werden Docker-Images abgelehnt, die Software oder Teile hiervon enthalten, die für den Einsatz in der LHH nicht freigegeben sind. Der Abruf von Docker-Images ist nur aus vertrauenswürdigen Repositories/Quellen möglich.
Es stehen Test-, QS- und Produktionsumgebungen für den Einsatz von Docker zur Verfügung.

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

4.2.15 Druckserver

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

Landeshauptstadt Hannover

5 Unternehmensanwendung

5.1 SAP

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

5.2 ECM Module

5.2.1 Portal

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

5.2.2 Formularservice (FMS)

Es sind folgenden Softwarekomponenten im Einsatz:

- cit intelliForm Server
- Webserver Apache
- JBOSS EAP
- OPEN JAVA SDK
- cit ServiceProxy/Camunda
- cit Folders

Als Betriebssystem wird Windows Server eingesetzt.

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

5.2.3 CMS

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

6 Security Infrastruktur

6.1 Online / offline Authentifizierungsmethoden

6.1.1 Authentifizierung am Windows Client

Die Standardanmeldung erfolgt über Microsoft Active Directory Domaincontroller.

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

6.2 PKI (Elektronische Signatur)

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

6.3 IT Sicherheitsrichtlinien

Grundsätzlich muss die Einhaltung der IT-Sicherheitsrichtlinien (IT-SRL) der LHH analog gewährleistet werden. Bei der Nutzung von Anwendungen und deren Betrieb ist diesbezüglich die Passwortsicherheit von Bedeutung. Eingesetzte Verfahren Dritter müssen folg. Vorgaben erfüllen:

6.3.1 Gestaltung von Kennwörtern

Kennwörter müssen gehasht und gesalzen sein und dürfen im Datenbestand des Verfahrens bzw. in Systemen von Dritten nicht als Klartext geführt werden. Plausibilitätskontrollfunktionen zur Verhinderung unerlaubter Kennwörter müssen vorhanden sein.

Kennwörter sind durch das eingesetzte Verfahren mindestens 8-stellig alphanumerisch zu gewährleisten. Dabei sind Ziffern, Sonderzeichen und Groß- wie Kleinbuchstaben einzusetzen.

Kennwörter dürfen nicht mit dem Benutzernamen identisch sein und auch nicht aus dem Benutzernamen ableitbar sein (z.B. durch Auswechseln eines führenden Buchstabens o.ä.).

Die Verwendung vorheriger Kennwörter von Benutzer*innen zum wiederholten Mal soll Verfahrens- bzw. Systemseitig vermieden werden.

6.3.2 Initialkennwörter

Vom Hersteller gesetzte Standardkennwörter sind im Rahmen der Inbetriebnahme unverzüglich zu ändern bzw. der/die Anwender*in ist bei Erstanmeldung zur Änderung durch das Verfahren aufzufordern.

6.4 Netzwerktopologie

6.4.1 Übersicht

Die in den einzelnen Punkten erwähnten Komponenten werden nochmal zusammenfassend in der folgenden Übersicht der Netzwerktopologie zusammengefasst.

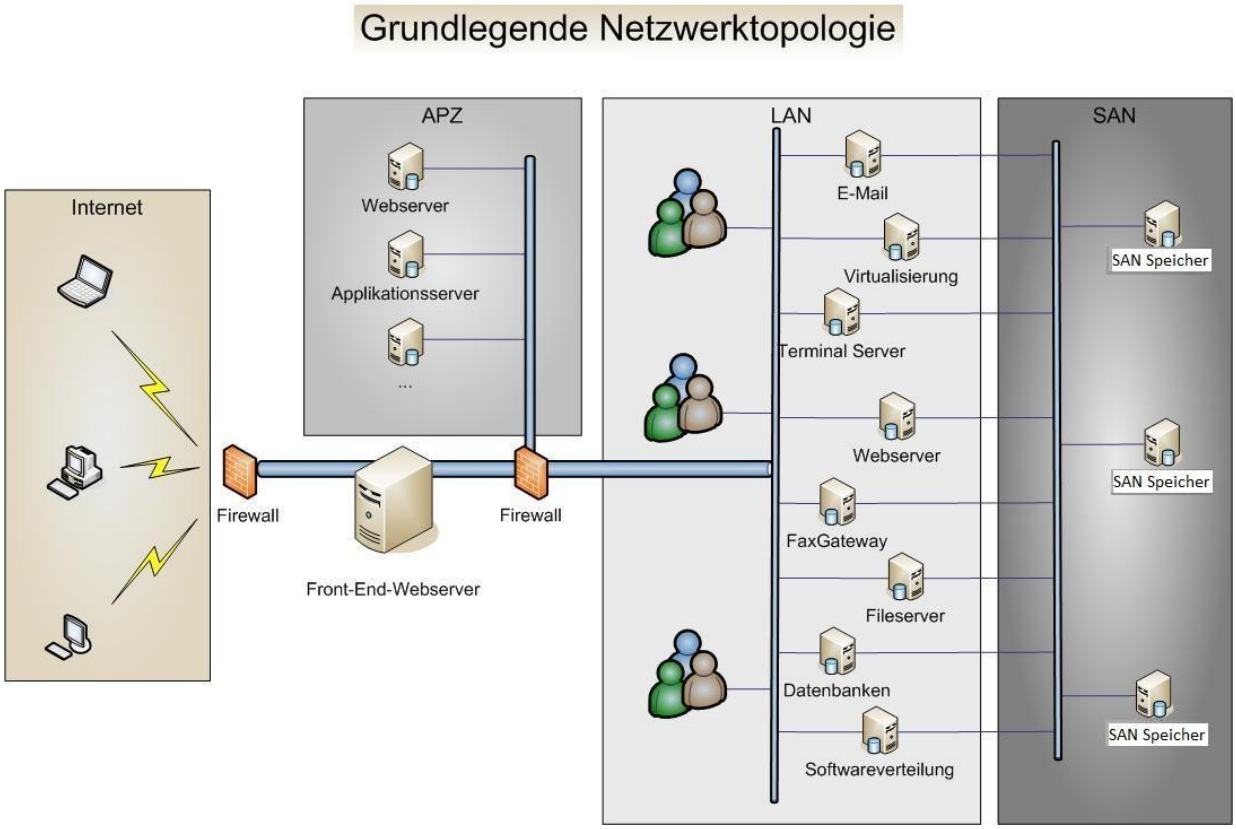

Abbildung 1: Übersicht der Netzwerktopologie

6.4.2 Security Systeme der Intranet-Zone

Alle Clients im Intranet sind mit einem Virenscanner und der Windows Firewall ausgestattet. Ergänzend kommt eine zentrale Firewall-Lösung zum Einsatz.

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

6.4.3 Internetzugriff für Systeme/Anwendungen

Der Zugriff auf Internetressourcen erfolgt ausschließlich über einen expliziten Proxy-Server.

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

6.5 Datensicherheit

6.5.1 Sicherung

Commvault Backup & Recovery wird zur Image- und Dateisicherung eingesetzt.

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

6.5.2 Integrität

Eine Datensicherung wird gemäß den geltenden Rechtsvorschriften angewandt.

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

6.5.3 Vertraulichkeit

Die Verschlüsselung personenbezogener Daten beim Transport erfolgt gemäß den geltenden Rechtsvorschriften.
Eine Rechtestruktur mit Zugriffschutz, Gruppen- und Rollenkonzept ist vorhanden.

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

7 System & Service Management Infrastruktur

7.1 Serverzentralisierung

Der gesamte technische Rechenzentrumsbetrieb wird in seinen wesentlichen Teilen zentralisiert durch den Bereich Informations- und Kommunikationssysteme (OE 18.5) ausgeführt. Die technische Administration ist örtlich und organisatorisch fast vollständig zentralisiert. Der Rechenzentrums-Betrieb verteilt sich auf 2 Standorte.

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

7.2 Nutzerverwaltung

Für die Administration der Windows-Benutzer- und Computerkonten existiert ein zentrales verwaltungsweites Active Directory auf Basis von Microsoft Windows.

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

7.3 IT-Servicemanagement

ITSM-Tool „ky2help“ von der Firma Kyberna AG

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

8 Anhang

Anhang 1: ky2help Schnittstellen

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.

Anhang 2: DB-Anforderungen an Verfahrenssoftware

Bei der LHH werden zentrale, standardisierte Datenbankserver eingesetzt, d.h. es werden bis zu 50 unterschiedliche Datenbanken / Datenbank-Instanzen auf einem Server gehosted. Daraus ergeben sich folgende Muss- und Sollkriterien:

I. Musskriterien:
1. Auf den zentralen Datenbankservern wird keinerlei applikationsbezogene Software installiert.
2. Auf zentralen Datenbankservern findet kein direkter Fernwartungszugriff statt. Im Ausnahmefall kann mit dem Client-PC des DB-Administrators eine Remote-Sitzung hergestellt werden, um einen kontrollierten Zugriff auf die Datenbank gewährleisten zu können.
3. Ein direkter ODBC-Zugriff der Benutzer auf die Datenbank muss ausgeschlossen sein (mangels Nachvollziehbarkeit/Protokollierung), d.h. der Zugriff auf die Datenbank erfolgt ausschließlich über die Applikation (Masteruser bzw. eigene Kennwortverwaltung).
4. Die Benutzer- bzw. Rechteverwaltung erfolgt verfahrensintern und obliegt dem Fachbereich - im Datenbankmanagementsystem werden keine Endbenutzerrechte gepflegt.
5. Individuelle serverweite Konfigurationsvorgaben werden nicht berücksichtigt. Die Konfiguration der Datenbankserver entspricht im Wesentlichen den Vorgaben der Datenbankmanagementsystem-Hersteller. Bei Bedarf können diese bei der OE 18.52.4 erfragt werden (18.52.4@hannover-stadt.de).
6. Eine Applikationsbezogene Protokollierung erfolgt nicht mit Datenbankmitteln (Tracing). Auch die vom Datenbankmanagementsystem erzeugten Transaktionslogs ersetzen keine Protokollierung von Zugriffen, sondern dienen ausschließlich der Wiederherstellung (Recovery) bzw. der Fehleranalyse.

II. Sollkriterien:
1. Vor Produktionsaufnahme sollte eine Testinstallation auf einem zentralen städt. Testserver obligatorisch sein, damit die Einhaltung aller Vorgaben vor Produktionsaufnahme überprüft werden kann.
2. Im Filesystem des Datenbankservers sollen weder temporäre, noch permanente Daten abgelegt werden. Im Einzelfall werden auf separaten Partitionen entsprechende Freigaben geschaffen, um die Funktionsfähigkeit der Datenbank nicht zu gefährden.
3. Für die auf produktiven Datenbankinstanzen eingerichteten Datenbankbenutzer sollen weder serverweite Berechtigungen(Systemadministrator-Rechte) vergeben, noch seitens der Administration Skripte ausgeführt werden, welche serverweite Berechtigungen erfordern. Bei Unabdingbarkeit ist die Anwendung auf separaten DB-Instanzen zu betreiben, welches zu erheblich höherem administrativen Aufwand bzw. Kosten im Bereich Systeminfrastruktur führt. Darüber hinaus kann aufgrund der unerwünschten Rechtestruktur ein fehlerfreier Datenbankbetrieb insbesondere hinsichtlich der Datenbanksicherung nicht gewährleistet werden.
4. Für die auf Test-Datenbankinstanzen eingerichteten Datenbankbenutzer können vorübergehend (z.B. zum Zwecke der Ersteinrichtung) diese serverweiten Berechtigungen vergeben werden oder seitens der Administration Skripte ausgeführt werden, sofern eine Beeinträchtigung anderer Testdatenbanken ausgeschlossen werden kann.

Verfahren, welche diesen o.g. Musskriterien nicht entsprechen, werden nicht auf der zentralen Datenbankserver-Infrastruktur betrieben. Die Einhaltung der Soll-Kriterien wird bei der Bewertung der Anwendung Berücksichtigung finden.

Anhang 3: Standards für Webanwendungen

Im Folgenden werden Anforderungen an Webverfahren und Webservices dargestellt, die bei der LHH zum Einsatz kommen sollen.

Grundsätzlich werden Webanwendungen auf Shared-Server Plattformen implementiert, d.h. sie teilen sich die Ressourcen mit anderen Anwendungen. Exklusivinstallationen sind aus datenschutzrechtlichen und Performancegründen nach Absprache möglich.

Die Installation von anwendungsbezogenen Programmkomponenten und Diensten auf Shared-Servern wird nicht unterstützt.

Die Installation von lokalen Datenbanken auf Webservern wird nicht unterstützt, dafür stehen entsprechende Infrastrukturdienste (DB-Server) zur Verfügung.

Für alle Produktivinstallationen kann eine Entwicklungs-/Qualitätssicherungsinstallation zur Verfügung gestellt werden.

Installationen von Webanwendungen die vom Internet aus erreichbar sind, unterliegen möglicherweise Einschränkungen durch Härtung von Serversystemen in der DMZ oder die Firewall-Infrastruktur der LHH (Webapplikation Firewall, Frontend-Server).

Alle Verfahren werden durch eine SSL-/TLS-Verschlüsselung mit aktueller Cipher-Konfiguration nach Stand der Technik geschützt. Bei diesen Verfahren sollen Javascripts (JS) und Stylesheets (CSS) **nicht** inline im Quellcode eingebettet sein, sondern als lokale Dateiquellen geladen werden. z.B. <script type="text/javascript" src="js/1234/asdf.js">

Neue Webanwendungen müssen vor dem Produktivstart und nach Updates sowie in regelmäßigen Abständen Sicherheitsüberprüfungen durchlaufen (Penetration-Tests), die intern und/oder von externen Dienstleistern durchgeführt werden.

Vor Produktauswahl, Installation und Produktionsaufnahme ist in jedem Fall ein Architekturgespräch mit den beteiligten Arbeitsgruppen in der OE 18.52 und eine Testinstallation durchzuführen, in deren Rahmen auch ein Sizing der Serverressourcen erfolgt.

<u>Übersicht der Webserver Plattformen</u>

Windows	Windows Linux RedHat Rocky Linux	Windows Linux RedHat Rocky Linux	Windows Linux RedHat Rocky Linux
IIS	Apache	Tomcat	Nginx
Coldfusion	PHP		PHP

Infrastrukturdienste: Datenbanken // Verzeichnisdienste // Mail // PKI

Genaue Spezifikationen wurden aus Sicherheitsgründen entfernt und können bei begründetem Bedarf erfragt werden.