Technische Architekturprinzipien der Nürnberger Cloud Strategie (NCS)

Autor: Amt für Informationstechnologie

Version: 1.01

Stand: 14.04.2025

1 Dokumenteninformation 3
1.1 Versionshistorie 3
2 Technische Architekturprinzipien 4
2.1 Integration in die zentrale Identitäts- und Berechtigungsverwaltung 4
2.2 Verfügbarkeit von Datenverschlüsselung und Schlüsselverwaltung 4
2.3 Dokumentation von Schnittstellen & Integrationsmöglichkeiten 4
2.4 Backup- und Restore 5
2.5 Betriebskritikalität und Definition der Verfügbarkeitsziele 5

1 Dokumenteninformation

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

1.1 Versionshistorie

Version	Datum	Autor	Änderungsgrund	Beschreibung
1.01	14.04.2025	Amt für Informations-technologie		Aktuelle Version

2 Technische Architekturprinzipien

Technischen Architekturprinzipien definieren technische Anforderungen und ermöglichen dadurch ressourcenschonenden Einsatz von Cloud-Diensten sowie die reibungslose Integration in die städtische IT.

2.1 Integration in die zentrale Identitäts- und Berechtigungsverwaltung

Basis einer funktionierenden Cloud-Strategie ist eine zentrale, abgesicherte digitale Identität der IT-Anwender für alle Zugriffe auf Dienste und Ressourcen der Stadt Nürnberg. Unabhängig vom Ort eines Dienstes/ einer Ressource im eigenen Rechenzentrum oder in der Cloud ist der Zugriff auf Basis dieser zentralen Identität sicherzustellen.

LEITLINIE: Das zentrale Management von Benutzerkonten (Identitäten) und -berechtigungen von Cloud-Diensten muss in die zentrale Identitätsverwaltung der Stadt Nürnberg integriert werden können.

2.2 Verfügbarkeit von Datenverschlüsselung und Schlüsselverwaltung

Die Datenverschlüsselung und Schlüsselverwaltung sind entscheidend, um die Sicherheit sensibler Informationen in einer kommunalen Verwaltung zu gewährleisten.

Das Schlüsselmanagement bezieht sich auf den Prozess der Verwaltung und des Schutzes von Schlüsseln, die für die Verschlüsselung und Entschlüsselung von Daten verwendet werden. Effizientes Schlüsselmanagement stellt sicher, dass nur autorisierte Benutzer auf verschlüsselte Informationen zugreifen können und die Schlüssel selbst vor Missbrauch geschützt sind.

Für die Verschlüsselung in der Cloud ist zum einen die Transportverschlüsselung sicherzustellen, d.h. alle Daten zwischen Ihrer Organisation und dem Cloud-Anbieter müssen während der Übertragung verschlüsselt sein. Zum anderen stellt die Speicherverschlüsselung sicher, dass die Daten auch im Ruhezustand (Speicherung oder „at rest“) verschlüsselt sind. Dies ist anzustreben bzw. je nach Schutzbedarf der in der Cloud verarbeiteten Daten und der genauen technischen Ausgestaltung des Cloud-Dienstes ggf. sogar zwingend.

Die DIN Norm ISO 27001 und die NIST SP 800-57 geben Empfehlungen und definieren die best practices für die Schlüsselverwaltung und die Anwendung kryptographischer Maßnahmen.

LEITLINIE: Beim Einsatz von Cloud-Diensten sind eine Transportverschlüsselung nach Stand der Technik sicherzustellen und eine Speicherverschlüsselung, sowie ein Schlüsselmanagement in Händen der Stadt anzustreben bzw. sicherzustellen. Die einschlägigen Normen sind zu beachten.

2.3 Dokumentation von Schnittstellen & Integrationsmöglichkeiten

Beim Einsatz von Cloud-Diensten ist die Dokumentation von Schnittstellen und Integrationsmöglichkeiten wichtig, um Transparenz, Sicherheit und die effiziente Zusammenarbeit mit den IT-Systemen der kommunalen IT zu gewährleisten.

Eine Übersicht der verfügbaren Schnittstellen eines Cloud-Dienstes umfasst APIs, Webhooks, Datenbankverbindungen und andere Kommunikationswege. Die Beschreibung der

Schnittstellen beinhaltet welche Funktionen die Schnittstelle bietet und welche Daten übertragen werden. Die Dokumentation der Sicherheitsaspekte umfasst die Authentifizierungsmethoden (z. B. OAuth, API-Schlüssel), die Verschlüsselung für den Transport und eventuelle Zugriffsbeschränkungen der Schnittstelle.

Datenfluss-Diagramme visualisieren den Datenfluss zwischen den Systemen und zeigen, wie Daten über Schnittstelle ausgetauscht werden.

Für das Monitoring, die Fehlerbehebung und das Änderungsmanagement wird dokumentiert, wie der Zustand der Schnittstellen überwacht wird (welche Metriken relevant sind) und wie die Versionierung bei Änderungen erfolgt.

LEITLINIE: Beim Einsatz von Schnittstellen zu Cloud-Diensten ist zu dokumentieren, welche Systeme oder Dienste über diese Schnittstellen miteinander interagieren. Dabei sind sowohl konzeptionelle, betriebstechnische als auch Sicherheitsaspekte aussagekräftig niederzulegen.

2.4 Backup- und Restore

Backup- und Restore-Mechanismen gewährleisten die Wiederherstellbarkeit und Integrität kritischer Daten und Anwendungen. Durch regelmäßige Backups und entsprechende Restorepläne können Wiederherstellungen ermöglicht und damit Datenverluste und Ausfallzeiten reduziert werden. Dies gilt für den on-premises Betrieb im eigenen Rechenzentrum, aber ebenso für den Einsatz von Cloud-Diensten.

LEITLINIE: Für den Einsatz von Cloud-Diensten sind grundsätzlich Backup- und Restore-Mechanismen und Notfallwiederherstellungspläne mit dem Cloud Dienstleister vertraglich zu vereinbaren, zu dokumentieren und turnusmäßig hinsichtlich Ihrer Funktion zu überprüfen.

2.5 Betriebskritikalität und Definition der Verfügbarkeitsziele

Die Betriebskritikalität von Fachverfahren bezieht sich auf die Bedeutung und Dringlichkeit, mit der bestimmte Anwendungen und Dienste für den täglichen Betrieb der Stadt verfügbar sein müssen. Kritische Fachverfahren erfordern eine besonders hohe Verfügbarkeit und Zuverlässigkeit. Die Definition von Verfügbarkeitszielen stellt sicher, dass diese Dienste auch bei technischen Störungen oder Ausfällen kontinuierlich zugänglich bleiben.

LEITLINIE: Beim Einsatz von Cloud-Diensten sind entsprechend der Betriebskritikalität gewählte Ziele/KPIs (Verfügbarkeit, Antwortzeitverhalten, …) vertraglich mit dem Cloud-Dienstleister zu vereinbaren. Der Cloud-Dienstleister ist weiterhin zu verpflichten, die Einhaltung der vereinbarten Ziele zu dokumentieren und nachzuweisen. Dies gilt auch deshalb, weil eine (längerfristige) Nichtverfügbarkeit von Systemen einen meldepflichtigen Datenschutzverstoß darstellen kann.