Europäische Strukturfonds Sachsen-Anhalt 2007 - 2013

Machbarkeitsstudie Geodaten

Projekt-Nr. EFRE16.01.4.13.00056

Betriebskonzept

SACHSEN-ANHALT

Europäische Kommission
Europäischer Fonds
für regionale Entwicklung
INVESTITION IN IHRE ZUKUNFT

Autoren der Studie

Stefan Blume	con terra
Sören Dupke	con terra
Dr. Udo Einspanier	con terra
Marc Kleemann	con terra
Antje Kügeler	con terra
Sarah Walter	con terra
Martin Plenk	Capgemini
Marc Akkermann	Capgemini

Version 1.0

Magdeburg, 22.11.2013

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abkürzung	Beschreibung
BDSG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
CPU	Central Processing Unit. Prozessor eines Computers.
DBMS	Datenbankmanagementsystem
DMZ	Demilitarisierte Zone. Geschütztes Netzsegment zwischen vertrauenswürdigen und weniger vertrauenswürdigen Netzen.
ETL	Extract Transform Load
GDI	Geodateninfrastruktur
GIS	Geoinformationssystem
GML	Geography Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
INSPIRE	INfrastructure for SPatial InfoRmation in Europe
IT	Informationstechnik
ITIL	IT Infrastructure Library. Sammlung von Best zur Umsetzung eines IT-Service-Managements (ITSM). Gilt inzwischen international als De-facto-Standard.
ITN-LSA	Informationstechnisches Netz. Das Landesnetz von Sachsen Anhalt
ITN-XT	Neues Landesnetz von Sachsen Anhalt (vorgesehen ab 2015)
KomNet	Verwaltungsnetz der Kommunen und Landkreise in Sachsen Anhalt
LSA	Land Sachsen-Anhalt
LRZ	Landesrechenzentrum Sachsen-Anhalt
Mbit	Megabit. Wird als Maß für die Bandbreite von Netzwerkverbindungen verwendet (Mbit/Sekunde).
NAS	Network Attached Storage
MLU	Ministerium für Landwirtschaft und Umwelt Sachsen-Anhalt
MLV	Ministerium für Landesentwicklung und Verkehr Sachsen-Anhalt
OGC	Open Geospatial Consortium
OLA	Operational Level Agreement. Vereinbarung, die üblicherweise innerhalb einer Organisation zwischen unterschiedlichen Organisationseinheiten getroffen wird und der Absicherung eines übergeordneten Service Level Agreements (SLA) der Organisation gegenüber einem Dritten dient.

Abkürzung	Beschreibung
RAC	Real Application Cluster. Produkt der Firma Oracle zum Betrieb von Datenbank-clustern.
RZ	Rechenzentrum
SAN	Storage Area Network
SLA	Service Level Agreement. Vereinbarung bzw. die Schnittstelle zwischen Auftraggeber und Dienstleister für wiederkehrende Dienstleistungen.
SMS	Short Message Service
SNMP	Simple Network Management Protocol. Ein Protokoll zur Kommunikation zwischen der Überwachungskomponente und überwachten Netzwerkelementen.
SSL	Secure Sockets Layer
UHD	User Help Desk
WAN	Wide Area Network, Weitverkehrsnetz, z.B. Internet oder ITN-LSA
WCS	Web Coverage Service
WFS	Web Feature Service
WFS-G	Web Feature Service - Gazetteer
WMS	Web Map Service
WMTS	Web Map Tile Service
x86	Mikroprozessor-Architektur und damit verbundene Befehlssätze, welche unter Anderem von den Chip-Herstellern Intel und AMD entwickelt werden.

1 Einführung

1.1 Management Zusammenfassung

Für den Betrieb des zentralen Knotens ist es unbedingt notwendig, dass technischer und fachlicher Betrieb Hand in Hand arbeiten. Nur ein kombiniertes technisches und fachliches Monitoring kann sicherstellen, dass die Geodienste des zentralen Knotens eine entsprechende Qualität bezüglich Performance und Verfügbarkeit erreichen. Außerdem muss auch eine enge Abstimmung bei allen weiteren Aspekten des Betriebs erfolgen, wie z.B. die Wartung der Hardware und das Aufspielen von Software-Updates.

Die Notwendigkeit eines fachlichen und technisches Betriebs gibt es auch bei den dezentralen Knoten, daher sollte das LVermGeo für die dezentralen Knoten Beratungsleistungen zur Aufstellung des Betriebs etablieren. Dies sichert eine gute Qualität der Geodatendienste der dezentralen Knoten.

Das Thema Dienste-Sicherheit ist für die Web Feature Service (WFS) der dezentralen Knoten relevant, falls die darüber bereitgestellten Daten nicht öffentlich verfügbar gemacht werden sollen, sondern nur vom zentralen Knoten gelesen werden dürfen. Damit die Realisierung der Geodienste an den dezentralen Knoten und des Clients am zentralen Knoten (d.h. der Transformationsdienst) mit Standardkomponenten erfolgen kann, sollten hier einfache und weit verbreitete Schutzmechanismen verwendet werden. Im vorliegenden Dokument wird hierzu ein Verfahren beschrieben.

Ganz besondere organisatorische Aspekte kommen auf den zentralen aber auch die dezentralen Knoten zu, wenn eine Aktualisierung der Geodaten ansteht. Hier ist ein genauer Prozess, der auch die Mitwirkung dezentralen Anbieter fordert, zu definieren. Dieser Prozess ermöglicht die Aktualisierung von den Geodaten und Geodiensten auf dem zentralen Knoten und definiert auch für Fehler/Probleme mögliche Lösungswege.

Ebenfalls ist es wichtig einen einheitlichen Ansprechpartner am zentralen Knoten bei Fragen oder Problemen zu schaffen. Es bietet sich an, hierzu beim LVermGeo einen User Help Desk für den Geo-Bereich (Geo-UHD) einzurichten, der den sogenannten First Level Support für alle Nutzer per Telefon und E-Mail sicherstellt.

1.2 Zielsetzung dieses Dokuments

Dieses Dokument enthält Empfehlungen für den Betrieb des zentralen und der dezentralen Knoten. Es wird dabei besonders auf das fachliche und technische Monitoring und die Ausfallsicherheit eingegangen. Außerdem werden die organisatorischen Aspekte, die eine Aktualisierung von Geodiensten mit sich führen, dargelegt.

1.3 Aufbau dieses Dokuments

In diesem Dokument werden in Kapitel 2 Empfehlungen für den Betrieb des zentralen und der dezentralen Knoten ausgesprochen. Des Weiteren werden in Kapitel 3 die Verfügbarkeitsaspekte für diese näher beleuchtet. Dabei spielt sowohl das technische als auch fachliche Monitoring eine wichtige Rolle. Der Schwerpunkt von Kapitel 4 liegt auf der Beschreibung der Dienste-Sicherheit. In Kapitel 5 wird im Detail auf die organisatorischen Aspekte, die im Zusammenhang mit einer Aktualisierung von Diensten bedacht werden müssen, eingegangen.

Das vorliegende Dokument gehört zu einer Reihe von anderen Dokumenten, die im Rahmen der „Machbarkeitsstudie Geodaten“ erstellt wurden. Im Einzelnen sind dies

- Machbarkeitsstudie
- IT-Konzept zur Machbarkeitsstudie
- Maßnahmenplan zentraler Knoten
- Maßnahmenplan dezentrale Knoten
- **Betriebskonzept** (dieses Dokument)
- Umsetzungskonzept

Für das Verständnis des vorliegenden Betriebskonzepts wird empfohlen, dass im Vorfeld die folgenden Dokumente gelesen werden:

- Machbarkeitsstudie (Kapitel 4, 6 und 7)
- IT-Konzept zur Machbarkeitsstudie
- Umsetzungskonzept (Kapitel 3)

1.4 Zielgruppe dieses Dokuments

Dieses Dokument richtet sich an:

- fachliche und technische Entscheider für den Auf- bzw. Ausbau des zentralen Knotens
- fachliche und technische Entscheider für die dezentralen Knoten bei Kommunen, Landkreisen, kreisfreien Städten und sonstigen geodatenhaltenden Stellen.

2 Empfehlungen für den Betrieb der Geodateninfrastrukturknoten

In diesem Kapitel werden die Tätigkeiten, die im Rahmen des Betriebes der Geodateninfrastrukturknoten notwendig sind, genauer erläutert. Es wird der direkte Bezug zum Organisationsmodell im IT-Konzept (Kapitel 6) hergestellt und im Schwerpunkt die Phase „Service Operation“ beschrieben.

Für den Betrieb der Geodateninfrastrukturknoten sind grundsätzlich folgende Bereiche zu betrachten:

- technischer Betrieb
- fachlicher Betrieb
- Support
- Geodatenmanagement

Die ersten drei Punkte werden im aktuellen Kapitel betrachtet. Der Bereich des Geodatenmanagements wird in Kapitel 5 sowie im Maßnahmenplan zentraler Knoten (Kapitel 2.2) näher erläutert.

2.1 Zentraler Knoten

Der zentrale Knoten soll unter Federführung des LVermGeo betrieben werden. Hierbei sind klare Aufteilungen der einzelnen Betriebsaufgaben zu sehen:

2.1.1 Technischer Betrieb

Die Technik wird zentral durch einen IT-Dienstleister (Dataport AöR) betrieben. Dafür sind explizite und detaillierte Vorgaben (ein Service Level Agreement – SLA) im Rahmen des Service Level Managements zu erarbeiten (siehe IT-Konzept, Organisationsmodell, Service Design).

Innerhalb des technischen Betriebes sind die folgenden Punkte sicherzustellen:

- Monitoring der Hardware und der Systemdienste (siehe auch Kapitel 3.1)
  Hierbei kommt es darauf an, nicht nur Ausfälle sofort zu registrieren und zu melden, sondern den „Gesundheitszustand“ des Systems zu überwachen. Ein Beispiel hierfür ist das Steigen der Fehlerrate bei Lese-/Schreibzugriffen auf einer Festplatte im SAN. Hier kann ein Austausch erfolgen, ohne dass es zum Ausfall kommt.

  In der Regel sind für den technischen Betrieb bei professionellen IT-Dienstleistern Standardverfahren und –werkzeuge implementiert.

- Installation von im Rahmen des fachlichen QS-Prozesses (freigegebenen) Updates/Patches und von neuer Software
  Aktualisierungen und Fehlerbehebungen bezüglich systemnaher Software erfolgt in der Regel autark durch den IT-Dienstleister. Hierzu werden die Auswirkungen auf den Betrieb zunächst in Entwicklungs- und Integrationsumgebung geprüft, um dann nach vorgegebenen Verfahren ausgerollt zu werden. Für die fachliche Software ist dieser Prüfungsprozess vorab durch Spezialisten des LVermGeo in Zusammenarbeit mit dem IT-Dienstleister durchzuführen (siehe IT-Konzept, Organisationsmodell, Service Transition). Im Anschluss erfolgt die Installation durch den IT-Dienstleister.

Daneben ist auch die Regeneration der Systemkomponenten rechtzeitig zu planen, um den Betrieb des Geodateninfrastrukturknotens auch über die Lebensdauer der Gerätegeneration hinweg sicherzustellen.

2.1.2 Fachlicher Betrieb

Der fachliche Betrieb für den zentralen Knoten ist durch das LVermGeo sicherzustellen. Hierzu ist eine enge Zusammenarbeit mit dem IT-Dienstleister auf der Administrationsebene erforderlich.

Die folgenden zwei Tätigkeitsbereiche sind abzudecken:

- Monitoring der Geodienste
  Über die Funktionalität der technischen Komponenten (Hardware und systemnahe Dienste) hinaus muss eine kontinuierliche Überwachung der Dienst-/Applikationsebene sichergestellt werden. Dies erfordert den Einsatz von Spezialisten (siehe Kapitel 0 und IT-Konzept, Organisationsmodell, Service Operation).
- Fachadministration
  Die Komponenten der Zielarchitektur, die „oberhalb“ der Systemebene liegen (z.B. Geodiensteserver, Geodatenbank, Transformationsserver etc.) müssen aus fachlicher Sicht administriert werden. Hierzu ist durchgehend ein entsprechend ausgebildeter Fachadministrator erforderlich (siehe IT-Konzept, Organisationsmodell, Service Operation).

2.1.3 Support

Für die Nutzer der Zielarchitektur ist ein einheitlicher Ansprechpartner bei Fragen und/oder Problemen zu schaffen. Es bietet sich an, hierzu beim LVermGeo einen User Help Desk für den Geo-Bereich (Geo-UHD) einzurichten, der den sogenannten First Level Support (einfache Anfragen zur Bedienung, kleinerer Fehler, Berechtigungsverwaltung etc.) für alle Nutzer per Telefon und E-Mail sicherstellt.

Für den weitergehenden Support (Second und Third Level Support) sind beim Geo-UHD die jeweiligen Ansprechpartner für die technischen Komponenten (Service Desk des IT-Dienstleisters) und fachlichen Komponenten (Service Desk des Fachanbieters) zu hinterlegen, so dass eine effektive und effiziente Störungsbeseitigung sichergestellt werden kann.

In jedem Fall sollte der Geo-UHD alle Informationen zu laufenden Meldungen/Problemen zentral sammeln und jederzeit auskunftsfähig zum Bearbeitungsstand sein.

2.2 Dezentrale Knoten

Grundsätzlich gelten die Angaben aus Kapitel 2.1 auch für die dezentralen Knoten. Anstelle des LVermGeo steht dann die geodatenhaltende Stelle (z.B. Kommune).

Im Einzelfall ist zu betrachten, in wie weit auch fachliche Aspekte des Betriebes an einen IT-Dienstleister ausgelagert werden können, wenn im eigenen Bereich entweder die Kapazitäten oder auch Kompetenzen zur Wahrnehmung der fachlichen Betriebsaufgaben eingeschränkt sind.

Grundsätzlich sollte hier auch eine Beratungsleistung zur Gestaltung einer passenden technischen und organisatorischen Umsetzung des dezentralen Knotens seitens des LVermGeo für die geodatenhaltenden Stellen etabliert werden.

3 Verfügbarkeitsaspekte

Dieses Kapitel stellt das erforderliche technische und fachliche Monitoring zur Sicherung der Verfügbarkeit der Geodienste vor.

3.1 Technisches Monitoring und Ausfallsicherheit

Das in Kapitel 0 beschriebene fachliche Monitoring prüft die Funktion der Anwendungen auf fachlicher Ebene, kann aber den Ausfall von redundanten Komponenten in der Regel nicht erkennen. Daher ist zusätzlich ein technisches Monitoring auf Ebene der einzelnen Komponenten erforderlich.

Da am zentralen Knoten eine Speicherung der aufbereiteten Daten aus den dezentralen Knoten vorgesehen ist, ist eine Verfügbarkeit der dezentralen Knoten für die Abrufbarkeit der Daten am zentralen Knoten nicht erforderlich. Entsprechend muss die Verfügbarkeit der dezentralen Knoten nicht ständig überwacht werden. Aus Sicht des zentralen Knotens genügt es, Fehlermeldungen für die dezentralen Knoten auszugeben, die beim Datenabruf nicht verfügbar waren. Für diese Knoten ist dann ein erneuter Datenabruf zu veranlassen. Entsprechend konzentriert sich dieses Kapitel auf den zentralen Knoten, ein vergleichbares Monitoring wird aber auch den Betreibern der dezentralen Knoten empfohlen.

Es wird davon ausgegangen, dass für das technische Monitoring die beim IT-Dienstleister vorhandenen Monitoringsysteme (z.B. IBM Tivoli, HP OpenView, Nagios) verwendet werden können. An dieser Stelle kann keine Darstellung des gesamten Monitorings im Rechenzentrum erfolgen, es werden lediglich die für den zentralen Knoten wesentlichen Punkte dargestellt.

Da sowohl physische als auch virtuelle Komponenten mindestens mehrheitlich redundant ausgelegt sind, führt der Ausfall einer einzelnen Komponente in der Regel nicht zum Ausfall der Anwendung. Werden die Einzelkomponenten nicht überwacht, kann somit ein Ausfall so lange unbemerkt bleiben, bis die redundante Komponente ebenfalls ausfällt. Zur Gewährleistung der Ausfallsicherheit ist daher eine Überwachung aller Einzelkomponenten erforderlich.

Neben der Überwachung der physischen Komponenten ist auch eine Überwachung der virtuellen Komponenten erforderlich. Dabei ist sowohl zu überwachen, ob die virtuellen Server gestartet sind, als auch, ob die jeweils vorgesehenen Anwendungen gestartet wurden (Prozessüberwachung).

Abgestürzte Anwendungen führen entweder direkt auf dem betroffenen Server zu erhöhter Prozessorlast oder aber die Last auf dem redundanten Server steigt aufgrund der wegfallenden Lastverteilung. Daher ist die Überwachung der Auslastung von CPU und Arbeitsspeicher unabdingbar.

Da vollgeschriebene Storagebereiche häufig zu Inkonsistenzen in den Datenbanken und zu fehlerhaften Dateien führen, muss die Auslastung des Storage überwacht werden.

Im Rahmen der Implementierungskonzepte sind für CPU, Arbeitsspeicher und Storage Schwellwerte für Warnungen und Alarme zu definieren.

Um rechtzeitig auf zunehmende Systemauslastung reagieren zu können, sind mit dem IT-Dienstleister Berichte über die Auslastungsspitzen (mindestens CPU und Arbeitsspeicher) und die mittlere Auslastung der Stunden mit der höchsten Auslastung zu vereinbaren.

Die meisten Ausfälle haben ihre Ursache in Konfigurationsänderungen der Soft- oder Hardware. Um dieses Risiko zu minimieren, darf ein Einspielen von Soft- und Hardwareupdates und –upgrades erst nach Erprobung derselben in der Integrationsumgebung erfolgen.

Da eine Verfügbarkeit von 99% identifiziert wurde (siehe IT-Konzept, Kapitel 2.3), ist eine absolute Ausfallsicherheit im Sinne einer Hochverfügbarkeitslösung nicht erforderlich. Dennoch ist die Dauer von Ausfällen zu minimieren.

Häufig gestaltet sich der Wiederanlauf komplexer Verfahren als schwierig. Werden hier Fehler gemacht, gelingt der Neustart nicht, obwohl das den Ausfall verursachende Problem bereits behoben wurde. Um dies zu vermeiden, sind im Rahmen der Erstellung der Betriebshandbücher die Identifizierung von Abhängigkeiten zwischen den Komponenten inklusive der Anwendungen und die Definition von Restart-Prozeduren erforderlich.

Um zu vermeiden, dass im Falle der Notwendigkeit eines Einspielens von Backups alle Änderungen seit dem letzten Backup verloren gehen, ist, wie beim Betrieb professioneller produktiver Datenbanken üblich, ein Transaktionslog auf Datenbankebene zu führen.

Das Wiedereinspielen von Datenbankbackups und Transaktionslogs, der Rollback von Datenbanktransaktionen sowie der Neustart des Gesamtverfahrens sind regelmäßig, mindestens einmal jährlich zu testen. Die dafür benötigte Zeit ist zu dokumentieren.

3.2 Fachliches Monitoring

Das fachliche Monitoring von zentralen Diensten erweitert die Aspekte des technischen Monitorings um den konkreten Bezug zur Fachlichkeit des Systems (hier die gesamte Fachlichkeit des zentralen Knotens).

Folgende Messwerte können im Rahmen eines Monitorings auf den fachlichen Kontext des aktuellen Anwendungsfalls bezogen werden.

- Dauer einer Kartenanfrage bezogen auf den Erwartungswert für die Generierung eines Kartenbildes (Darstellungsdienst)
- Dauer einer Anfrage nach Geoobjekten bezogen auf den Erwartungswert für die Auslieferung eines geographischen Objektes (Downloaddienst)
- fachliche Konsistenz der Antwort einer Capabilities-, Karten- oder Geoobjekt-Anfrage

3.2.1 Dauer einer Kartenanfrage

Die Dauer einer Kartenanfrage bestimmt in erheblicher Weise die Zufriedenheit der Nutzer bei der Verwendung eines Kartendienstes. Es besteht bei dynamischen Kartendiensten eine starke Relation zu der Anzahl der zu zeichnenden Geoobjekte und der definierten kartographischen Ausgestaltung zur Dauer der Kartenanfrage, so dass keine pauschalen Mess- und Grenzwerte für dieses Monitoring definiert werden können. Einen Richtwert bieten hier die INSPIRE Anforderungen (siehe IT-Konzept, Kapitel 2.1). Für jeden Geodienst sollte aber auch individuell ein Richtwert definiert werden können, der zu einem fachlichen Monitoring herangezogen wird.

3.2.2 Dauer einer Geoobjekt-Anfrage

Die oben gemachten Angaben zur Kartenanfrage lassen sich hinsichtlich der Komplexität des zugrunde liegenden Datenmodells auf die Dauer von Geoobjekt-Anfragen übertragen.

Für jeden Geodienst bzw. jeden Datentyp des Dienstes ist daher individuell ein Richtwert zu definieren, der zu einem fachlichen Monitoring herangezogen werden kann.

3.2.3 Fachliche Konsistenz einer Antwort

Für beide Dienst-Typen (WMS und WFS) kann es sinnvoll sein, die fachliche Konsistenz einer Antwort automatisiert überwachen zu lassen. Diese Prüfung kann erfolgen, indem geprüft wird, ob bei der Anfrage das erwartete Ergebnis oder eine Fehlermeldung zurückgegeben wird. Die OGC-Dienste geben jeweils definierte Exceptions zurück, gegen die geprüft werden kann. Ein Geodienst, der fehlerhaft ist, wird in vielen Fällen eine solche Exception zurückgeben, die aber beim technischen Monitoring nicht als Fehler erkannt werden würde.

Weitergehende Prüfungen könnten erfolgen, indem

- die absolute Anzahl der gelieferten Geoobjekte gezählt wird (WFS),
- Werte bestimmter Geoobjekte geprüft werden,
- das erzeugte Kartenbild auf Größe geprüft wird und
- Bildanalysen auf dem Kartenbild durchgeführt werden.

Da die meisten Probleme mit Geodiensten schon mit der Prüfung der Rückgabewerte auf Exceptions erfasst werden können, wurden die weitergehenden Prüfungen nicht als konkrete Anforderungen für das Geodienstemonitoring am zentralen Knoten aufgenommen (siehe Umsetzungskonzept, Kapitel 3).

4 Dienste-Sicherheit und Digital Rights Management

Dieses Kapitel beschreibt die Mechanismen, die in diesem Projekt zur Absicherung von Geodiensten bzw. der von diesen Diensten bereitgestellten Geodaten eingesetzt werden sollten. Ein Schutz von Geodiensten ist in den folgenden Fällen erforderlich:

- Bestimmte Informationen dürfen aus datenschutzrechtlichen Gründen nicht an alle potenziellen Clients abgegeben werden.
- Die Abgabe bestimmter Informationen soll zum Beispiel in der Form reglementiert werden, dass sie nur an Nutzer erfolgt, die eine entsprechende Lizenz zur Nutzung der Informationen erworben haben.

Zur Absicherung von Diensten werden generell zwei Verfahren eingesetzt:

1. Authentifizierung und Autorisierung: Über Authentifizierung wird sichergestellt, dass der zugreifende Client dem Server bekannt ist und seine „Echtheit“ bestätigt wird. Authentifizierung kann z.B. über die Eingabe von Nutzernamen und Passwort oder über die IP-Adresse des zugreifenden Clients erfolgen. Autorisierung bezeichnet das Einräumen bestimmter Berechtigungen an einen vorher authentifizierten Client.
2. Verschlüsselung: Durch Verschlüsselung werden Daten durch ein Verschlüsselungssystem in eine unlesbare Darstellung umgewandelt. Um die Daten wieder lesbar zu machen, muss das passende Entschlüsselungsverfahren angewendet werden. Verschlüsselung ist erforderlich, falls Daten über ein Netzwerk übertragen werden, zu dem auch Nutzer Zugang haben, die diese Daten nicht lesen dürfen. Verschlüsselung kann auf Anwendungs- und auf Transportebene erfolgen.

Für den zentralen Knoten wurden keine Anwendungsfälle identifiziert, die einen Zugriffsschutz für die Geodienste erforderlich machen. Alle Daten, die von den Geodiensten im zentralen Knoten bereitgestellt werden, sind öffentlich. Ein personalisierter Zugang zu den Geodiensten ist ebenfalls nicht erforderlich, d.h. alle Nutzer sehen die gleichen Informationen. Dies vereinfacht die Architektur des

zentralen Knotens, da der Zugriff auf die Geodienste direkt über die jeweilige Standardschnittstelle ohne Protokollzusätze zur Durchsetzung eines Zugriffschutzes erfolgen kann.

Für die Downloaddienste der dezentralen Knoten gibt es dagegen einen Schutzbedarf. Die bereitgestellten Web Feature Service (WFS) Schnittstellen müssen abgesichert werden, falls die darüber bereitgestellten Daten nicht öffentlich verfügbar gemacht werden sollen, sondern nur vom zentralen Knoten gelesen werden dürfen.

Ob Daten vom dezentralen Knoten als öffentlich zu betrachten sind, hängt auch vom Netzwerk ab, über das der zentrale Knoten angebunden ist. Erfolgt die Anbindung über das Internet, sind nur solche Daten öffentlich, die auch von jedem eingesehen werden dürfen. Innerhalb der Verwaltungsnetze ITN-LSA/KomNet sind dagegen nur solche Daten nicht öffentlich, die nicht von anderen Behörden oder Kommunen eingesehen werden sollen.

Damit die Realisierung der Geodienste an den dezentralen Knoten und des Clients am zentralen Knoten (d.h. der Transformationsdienst) mit Standardkomponenten erfolgen kann, sollten einfache und weit verbreitete Schutzmechanismen verwendet werden.

Die Verschlüsselung nicht öffentlicher Daten sollte daher auf Transportebene über Secure Socket Layer (SSL) erfolgen, d.h. für alle Dienstaufrufe wird das Hypertext Transfer Protocol Secure (HTTPS) Protokoll verwendet. HTTPS wird von den meisten gängigen Hypertext Transfer Protocol (HTTP) Clients und Web Servern unterstützt und erfordert somit keine zusätzlichen Systemanpassungen.

Für Authentifizierung/Autorisierung bieten sich zwei gängige Möglichkeiten:

1. HTTP Basic Authentication: Hierbei werden in dem Header einer HTTP Anfrage Nutzername und Passwort übertragen und können vom Server ausgewertet werden. Da Name und Passwort nicht verschlüsselt sind, sollte dieses Verfahren nur zusammen mit HTTPS verwendet werden. Basic Authentication wird von allen verbreiteten Web Servern unterstützt.
2. Zugriffsschutz über Internetprotokoll (IP) Adresse: Hierbei wird die Quelladresse aus den Kopfdaten der ankommenden IP-Pakete vom Server ausgewertet. Nur vorkonfigurierte IP-Adressen erhalten Zugriff auf eine bestimmte Ressource (hier: den WFS). Der IP-Filter kann innerhalb eines Web Servers oder einer Firewall implementiert werden.

Für nicht öffentliche Geodaten wird empfohlen, zumindest für Zugänge aus dem Internet beide Möglichkeiten zu kombinieren. Für Zugänge aus internen und Verwaltungsnetzen (ITN-LSA/KomNet) sollte für die Server-to-Server Kommunikation mindestens der Zugriffschutz über IP-Adresse, für die Server-to-Client Kommunikation mindestens der Zugriffschutz mittels HTTP Basic Authentication implementiert werden.

Absprachen zwischen dem LVermGeo und den geodatenhaltenden Stellen zur generellen Nutzung der Daten im zentralen Knoten müssen außerhalb des Systems getroffen werden (d.h. es ist keine Unterstützung mit Software des Zielsystems geplant). Hierzu gibt es – außerhalb des Kontextes der Machbarkeitsstudie – beim LVermGeo die zentrale Komponente zur Lizensierung, die bei Bedarf genutzt werden kann (siehe Machbarkeitsstudie, Kapitel 7.4).

5 Organisatorische Aspekte bei der Aktualisierung von Geodiensten

In diesem Kapitel werden die organisatorischen Aspekte bei der Aktualisierung der zentralen Geodienste beschrieben.

Bei der Aktualisierung eines Geodienstes am zentralen Knoten sind diverse organisatorische Aspekte zu bedenken und im Vorfeld Vereinbarungen zwischen den Akteuren des zentralen und der dezentralen Knoten zu treffen. Diese Vereinbarungen sollten schriftlich, z.B. in Form eines standardisierten SLA, festgehalten werden.

Unter der Annahme, dass es bereits einen produktiv laufenden Geodienst mit dazugehörigem Transaktionsdienst am zentralen Knoten gibt, kann der Aktualisierungsprozess wie nachfolgend beschrieben ablaufen:

Der Extract Transform Load (ETL-) Experte hat bereits bei der Einrichtung des Transformationsdienstes eine zeitgesteuerte Ausführung des ETL-Prozesses für die Aktualisierung auf dem Transformationsdienst eingerichtet. Der Aktualisierungszyklus kann für jeden Transformationsdienst einzeln eingestellt werden. Zum jetzigen Zeitpunkt geht man von einer Aktualisierung einmal pro Monat aus.

Mit der zeitgesteuerten Ausführung können die Geodaten von den einzelnen dezentralen WFS nacheinander abgeholt und verarbeitet werden. Nachdem der Prozess ausgeführt wurde, erfolgt eine automatische E-Mail-Benachrichtigung des ETL-Experten des zentralen Knotens. Es sollte das Ziel sein, dass später – wenn die Prozesse eingespielt sind – auch die GIS-Koordinatoren der dezentralen Knoten automatisiert eine E-Mail bekommen, wenn die Transformation erfolgreich war. Im Fehlerfall sollte nur der ETL-Experte informiert werden.

Die Transformation wird zunächst nur in der Integrationsumgebung ausgeführt. Das System liefert einen Statusbericht, anhand dessen der ETL-Experte erkennen kann, ob die Transformation erfolgreich oder fehlerhaft war. Bei einem bereits produktiv laufenden Geodienst mit eingespieltem Transformationsprozess sollten nur wenige Fehler auftreten. Dennoch muss der Statusbericht immer auf Fehler kontrolliert werden. War die Transformation fehlerhaft und liegt der Fehler bei den Ausgangsdaten, muss der ETL-Experte an den Service-Administrator des liefernden dezentralen Knoten herantreten und um die Behebung des Fehlers in den Ausgangsdaten bitten. Meldet der Service-Administrator des dezentralen Knotens, dass der Fehler in den Ausgangsdaten behoben wurde, führt der ETL-Experte erneut die testweise Transformation der korrigierten Geodaten in einen Testdatenbestand aus. Liefert das System weiterhin Transformationsfehler aufgrund der Ausgangsdaten, muss die zuvor beschriebene Prozedur erneut durchgeführt werden. Transformationsfehler, die nicht aufgrund der Ausgangsdaten auftreten, muss der ETL-Experte selber oder mit Hilfe des Supports der Herstellerfirma der Software lösen.

Verläuft die Transformation in den Testdatenbestand auf dem Integrationsserver erfolgreich, informiert der ETL-Experte den Service-Administrator über die Aktualisierung des Datenbestands in der Integrationsumgebung. Dieser aktualisiert den Geodienst in der Integrationsumgebung, der auf diesen Daten aufsetzt. Anschließend informiert er den ETL-Experten und alle GIS-Koordinatoren der dezentralen Knoten, deren Daten in diesem Geodienst eingebunden sind und bittet um Prüfung auf Korrektheit für ihre Daten im Geodienst. Für die Benachrichtigung sollten E-Mail-Verteiler angelegt werden.

Für die Prüfung wird den GIS-Koordinatoren eine vorher vereinbarte Frist gesetzt (beispielsweise eine Woche), in der sie Probleme melden können, die sie an den transformierten Geodaten entdeckt haben. Falls Probleme erst später gemeldet werden, werden sie mit dem nächsten Aktualisierungszyklus behoben.

Solange es Fehler gibt, müssen diese in enger Absprache der Akteure (ETL-Experte, Service-Administrator und GIS-Koordinatoren) gelöst werden. In schwierigen Fällen kann Support von den Herstellern der genutzten Softwarekomponenten angefordert werden.

Nach Ablauf der Frist für die Prüfung kann der ETL-Experte die Transformation der Geodaten in den zentralen Geodatenbestand der Produktionsumgebung durchführen. Anschließend muss der Service-Administrator informiert werden, damit dieser den produktiven zentralen Geodienst auf dem aktualisierten zentralen Geodatenbestand aktualisieren kann.

Wenn der Geodienst erfolgreich im Produktivsystem aufgesetzt wurde, informiert der Service-Administrator den ETL-Experten und die GIS-Koordinatoren, dass die Aktualisierung durchgeführt wurde.

Alternativ zu einem festgelegten Aktualisierungszyklus, wie z.B. einmal pro Monat, ist auch eine Aktualisierung auf Anforderung der geodatenhaltenden Stelle denkbar. Dies ist vor Allem bei Geodatenbeständen sinnvoll, die sich selten ändern. Der Vorteil bei diesem Vorgehen ist, dass nur bei Bedarf und dann auch nur die Geodaten aktualisiert werden, die tatsächlich verändert wurden.

Im Rahmen der Abstimmung des gemeinsamen Datenmodells (siehe Maßnahmenplan zentraler Knoten, Kapitel 2.2) sollte geprüft werden, ob es möglich ist, eine einheitliche Beschreibung einzuführen, wann die Geodaten zuletzt aktualisiert wurden (beispielsweise über eine Vorgabe in den Dienste-Capabilities).

Machbarkeitsstudie Geodaten

Betriebskonzept

SACHSEN-ANHALT

Europäische Kommission
Europäischer Fonds
für regionale Entwicklung
INVESTITION IN IHRE ZUKUNFT