DB-embedded GIS – Mandantensichere, datenbankbasierte Webanwendungen am Beispiel eines bundesweiten Atlas für IT-Infrastrukturdaten

Ulf Binnemann, Kushtrim Krasniqi

GDV, Gesellschaft für geografische Datenverarbeitung mbH
Ingelheim am Rhein

Schlüsselworte

Oracle Application Express (APEX), Oracle MapViewer, Oracle WebLogic Server, Oracle 11G

Einleitung

Am 18.02.2009 wurde die Breitbandstrategie der Bundesregierung veröffentlicht. Deren Ziel ist die kurzfristige flächendeckende Versorgung mit leistungsfähigen Breitbandanschlüssen und langfristig der flächendeckende Aufbau von Hochleistungsnetzen. Für den Ausbau der Breitbandinfrastruktur ist eine Anbindung der zu versorgenden Regionen an das schnelle Netz erforderlich. Hierzu werden in der Regel Glasfaser- oder Funkstrecken eingesetzt. Die dabei entstehenden Kosten können gerade in ländlichen Regionen erheblich sein und haben damit entscheidenden Einfluss auf die Wirtschaftlichkeit von möglichen Ausbauplanungen. Gleichzeitig existieren Infrastrukturen, bei denen eine Mitnutzung aus technischer Sicht grundsätzlich möglich wäre und zu einer Reduktion der Ausbaukosten beitragen könnte.

Ein wesentlicher Bestandteil der Breibandstrategie ist daher die Nutzung von Synergien beim Infrastrukturausbau, da der Aufbau von Hochleistungsnetzen und die Anbindung unterversorgter Regionen an das Breitbandinternet umso schneller und kostengünstiger erfolgen kann, je effizienter bestehende Infrastrukturen mitgenutzt werden.

Die Bundesnetzagentur hat daher im Auftrag des Bundesministeriums für Wirtschaft und Technologie einen bundesweiten Infrastrukturatlas auf Basis eines Geographischen Informationssystems (GIS) erstellt, mit dem es möglich ist Auskünfte zu bestehenden Infrastrukturen und Infrastrukturbetreibern zu geben.

Bisher waren im Rahmen des **Infrastrukturatlas (ISA)** verschiedene Desktop-GIS-Fachanwendungen im Einsatz, mit deren Hilfe heterogene Daten von einer Vielzahl von Infrastrukturinhabern verarbeitet wurden.

Zielsetzung des Projektes „Infrastrukturatlas“ war die Entwicklung und Inbetriebnahme einer browserbasierten Software-Lösung für **Geodaten** (WebGIS-Viewer) basierend auf einem relationalen Datenbanksystem und einem Geografischen Informationssystem, welches die aktuell im Einsatz befindliche Desktop GIS-Fachanwendung ablösen sollte.

Das von der GDV mbH erstellte webbasierte Gesamtsystem „Infrastrukturatlas“ wurde zu großen Teilen mit Oracle Technologie umgesetzt: Zum Einsatz kamen u.a.:

- Oracle Database 11G inklusive Spatial, Virtual Private Database (VPD)
- Oracle WebLogic-Server
- Oracle MapViewer
- Oracle Application Express (APEX)

Die durchgeführte Schutzbedarfsanalyse für den Infrastrukturatlas ergab den Schutzbedarf „hoch“. Somit kam eine besondere Rolle der Absicherung des über das Inter- und Intranet verfügbaren Systems gegen unbefugten Zugriff zu.

Die Vorstellung des technischen Aufbaus, das Zusammenspiel der eingesetzten Komponenten. und die ergriffenen Maßnahmen zur Absicherung des Gesamtsystems „Infrastrukturatlas“, nach innen und außen, soll im Rahmen des Vortrags eine besondere Rolle zukommen.

Technischer Aufbau des „Infrastrukturatlas“

Der Infrastrukturatlas verfügt über eine Import-Datenbank die im internen Netz der BNetzA angesiedelt ist. In dieser Datenbank werden sämtliche **räumliche und attributive Daten eingespielt**, die von Unternehmen für den Infrastrukturatlas zur Verfügung gestellt werden.

Über eine Datenbanksynchronisation kann der importierte Datenbestand mit einer zweiten Datenbank in der Demilitarisierten Zone (DMZ) synchronisiert werden. Diese zweite „Produktiv“-Datenbank liefert Daten an das Web-Front-End, das dem Endbenutzer über das Internet zur Verfügung steht.

Eine manuell vom Administrator auszulösende Synchronisation über eine Administrationsanwendung stellt dabei sicher, dass nur Daten im Web-Front-End zur Verfügung stehen, die auch vom Administrator explizit dafür freigegeben wurden. Die Einschränkung der zu synchronisierenden Daten ergibt sich dabei

- benutzer- / rollen-,(Einschränkung der verfügbaren Werkzeuge)
- gebiets- (Einschränkung auf bestimmte Gebiete), und
- fachsichtsbezogen (Einschränkung der angezeigten Infrastrukturarten).

Über das Administrationswerkzeug stehen auch eine Benutzerverwaltung, ein Kontakt/-Adressmanagementsystem zur Verfügung.

Bei den über den jeweiligen Application–Server zur Verfügung gestellten browserbasierten Anwendungen handelt es sich um Oracle Application Express (APEX) Anwendungen, die über. „https“ zur Verfügung stehen.

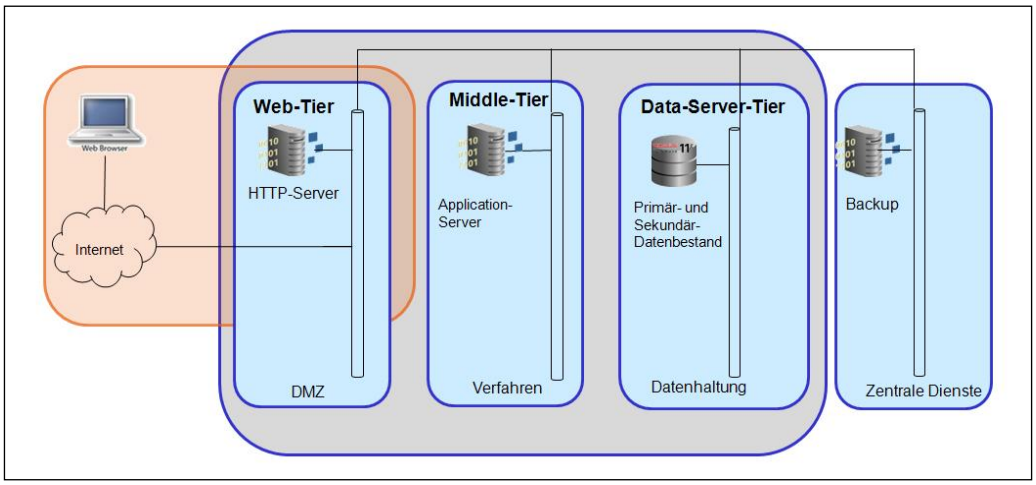

Abbildung 1: Grobarchitektur und Datenhaltung für den Infrastrukturatlas

Datenhaltung und –Erfassung, Kartenbereitstellung

Import von Daten

Eine besondere Herausforderung besteht im Infrastrukturatlas bei der Anpassung und dem Import von Geodaten, die in unterschiedlichsten Datenformaten von TK-Unternehmen zur Verfügung gestellt werden. Die aus verschiedenen GI- und CAD-System stammenden Daten werden mit Hilfe der Extract, Transform, Load (ETL) –Software FME direkt in die Oracle-Datenbank übertragen.

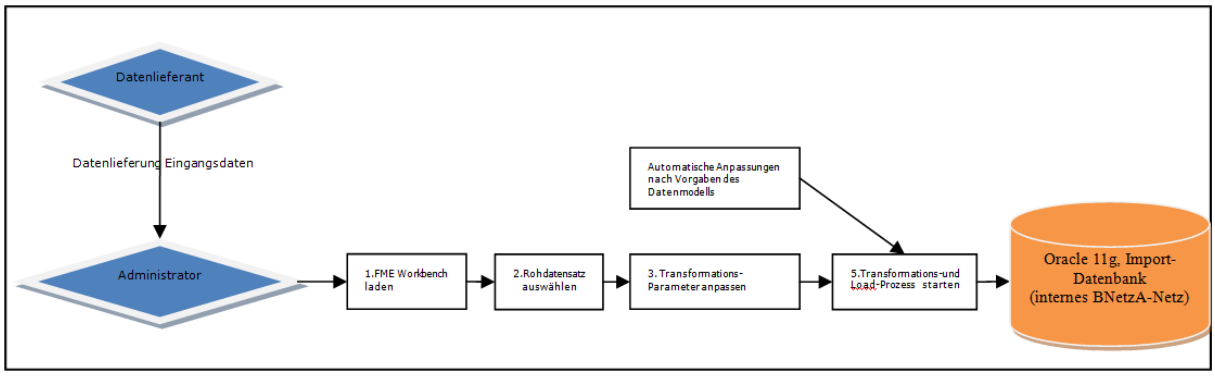

Abbildung 2: Datenaufbereitung der Rohdaten und Datenbankimport, Infrastrukturatlas

Einsatz von Oracle MapViewer

Als technische Plattform zur Karten- und Datenvisualisierung wird für den Infrastrukturatlas Oracle MapViewer Oracle eingesetzt. Die clientseitige Programmierung erfolgt dabei über HTML und JavaScript. Oracle MapViewer ist kostenfrei in allen Oracle Application Server Editionen enthalten ist.

Oracle MapViewer bietet als Basisfunktionalität die Visualisierung von Geo-Daten und einen Reporting Service. Das Java-basierte Visualisierungstool wird in einer JEE Umgebung verwendet und bietet standardmäßige Routinen für das Rendern/Erzeugen von Karten auf Basis in Oracle gespeicherter, räumlicher Daten. MapViewer nutzt grundlegenden Funktionen für die Verarbeitung

der geografischen Kartendaten, die mit Oracle 10g oder höher mitgeliefert werden (bereitgestellt durch Oracle Locator oder Oracle Spatial).

MapViewer ist als JEE-Applikation realisiert. Die Komponente wird auf Basis des Oracle Application Servers WebLogic betrieben und ist als Lizenz in diesem enthalten.

Die Definition einer Kartendarstellung erfolgt mittels Metadaten in der Oracle Datenbank, der Funktionsumfang der Kartenanwendung wird mittels JavaScript festgelegt.

Zur Definition der Kartenmetadaten kommt das Werkzeug Oracle MapBuilder aus dem Lieferumfang von MapViewer zum Einsatz.

Oracle Maps (Kartenclient von Oracle MapViewer) stellt sich dem Anwender als moderne AJAX-basierte Webanwendung dar. Der Zugriff auf Hintergrunddaten erfolgt über einen Tileserver (Map Cache Server), der in der Lage ist, die benötigten Kacheln zur berechnen und zwischenzuspeichern. Damit ist ein hoch performanter Zugriff auf die raster- oder vektorbasierten Hintergrunddaten gewährleistet. Zusätzlich werden die Fachdaten als direkte Geometrieobjekte (Feature of Interest, FOI) eingebunden. Dies ermöglicht beispielsweise den direkten Zugriff auf Attribute (Maptipps) und das Bearbeiten der Features.

Erfassung von Infrastrukturen über die WebGIS-Komponente durch Benutzer

Über die WebGIS-Komponente des Infrastrukturatlas ist es berechtigten Benutzern möglich selbst Infrastrukturen zu erfassen und diese an das System zu übermitteln. Die Daten können nach Überprüfung durch den Administrator direkt im Infrastrukturatlas zur Verfügung stehen.

APEX-Anwendungen / WebFrontends

Den Administratoren steht als APEX Anwendung ein Autoriserungs- und Administrationswerkzeug zur Verfügung. Diese Anwendung steht berechtigten Personen nur über das Intranet zur Verfügung. Über die Anwendung kann gesteuert werden, wie und für welche Personen Daten im Internet über die eigentliche Infrastrukturatlas WebGIS-Komponente zur Verfügung stehen.

Autorisierungs- und Administrationswerkzeug

Das Autorsierungs- und Administrationswerkzeug ist eine APEX Anwendung zur Administration des Gesamtsystems ISA

Das Werkzeug bietet browserbasierte Funktionalitäten zur:

- Benutzerverwaltung und Rollenzuweisung
- Synchronisation der beiden Datenbanken
- Kontaktmanagement von Ansprechpartnern
- Adress- und Kontaktmanagement von TK-Unternehmen

Funktionalitäten der WebGIS-Komponente des Infrastrukturatlas

Als Web-Frontend dient eine APEX Anwendung mit Oracle Maps, die um spezielle Funktionalitäten per JavaScript erweitert wurde. Benutzern stehen nur die Daten und Werkzeuge zur Ansicht zur Verfügung die über das Autorsierungs- und Administrationswerkzeug vom Administrator freigegeben wurden.

Die WebGIS-Komponente besteht aus der eigentlichen Kartenansicht und verschiedenen Toolbars, die sich aus der Oberfläche frei verschieben lassen und je nach Benutzer in unterschiedlicher Ausprägung zur Verfügung stehen.

Sicherheitsmaßnahmen zum Schutz der Daten

Dem Schutz von unternehmensbezogen Daten wird im Infrastrukturatlas besondere Priorität eingeräumt. Eine Schutzbedarfsanalyse hat einen hohen Schutz der eingesetzten Daten ergeben. Dem muss mit erweiterten Maßnahmen zum Schutz begegnet werden Zu den ergriffenen Maßnahmen zum Schutz der sensiblen Daten zählen ein erweiterter Loginmechanismus mit PIN-Verfahren und der Einsatz der Oracle Virtual-Private Database (VPD).

PIN-Verfahren: ISA- Authentifikation

Der in APEX-Anwendungen bereits nutzbare Loginmechanismus wurde um ein sog. PIN Verfahren erweitert. Hierzu wurde eine JSP-Anwendung (ISA-Authentifikation) entwickelt, die dem Standard-Loginmechanismus vorgeschaltet ist. In einem separatem Verfahren werden Benutzername, Passwort und PIN überprüft und an die Anwendung übergeben. Die Anwendung wird bei bestimmten Aktionen, wie bspw., einer dreimaligen falschen Eingabe von Benutzerdaten automatisch für Benutzer gesperrt.

Einsatz der Virtual Private Database (VPD)

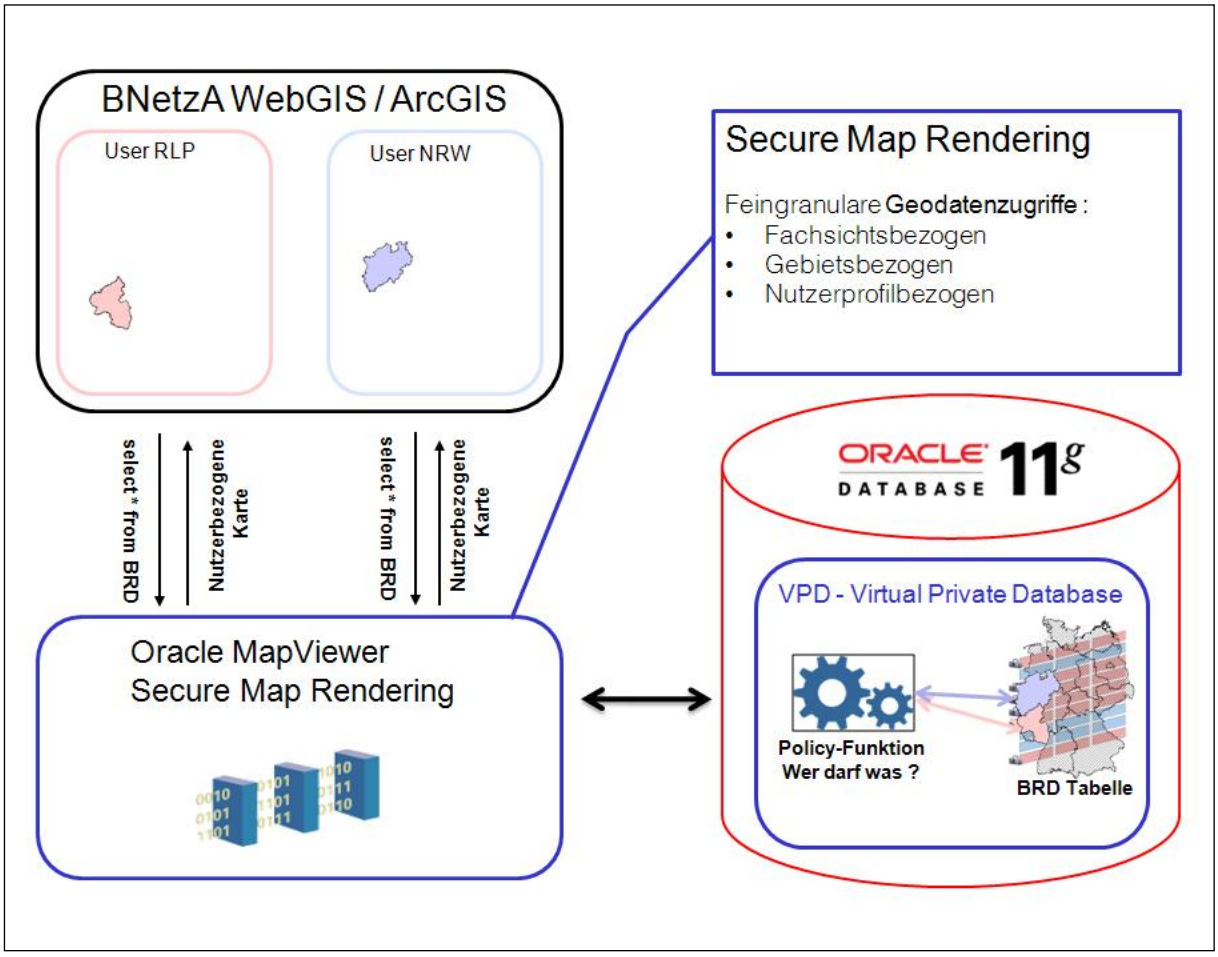

Abbildung 3: Datensicherheit mit Virtual Private Database (VPD) und Secure Map Rendering

Mit Hilfe der Oracle Datenbanktechnologie „Virtual Private Database“ können Datensätze hinsichtlich Benutzern (benutzerbezogen), Rollen (fachsichtsbezogen) und Raum (gebietsbezogen) autorisiert bzw. eingeschränkt werden.

Mit dieser Datenbank ist es möglich Datenbank- View ähnliche Abfragen zu erstellen, die direkt über dem jeweiligen Objekt, d.h. der Tabelle oder einer anderen View liegen. Während bei der Verwendung von bekannten Views, zumindest die Datenbankentwickler den wahren Inhalt der Tabelle, des zugrunde liegenden Objekts sehen können, ist dies bei der Verwendung einer VPD nicht möglich. Die Sicherheitsmaßnahmen greifen aus dem Blickwinkel der Datenbankbenutzer direkt auf View- bzw. Tabellenebene. D.h., dass selbst die Entwickler eine eingeschränkte Sicht auf die Inhalte von Tabellen und Views haben. Dies ist vor allem wichtig wenn besonders sensible Daten, wie im Falle des Infrastrukturatlas, in einer Tabelle abgelegt sind.

Die Policy- Funktionen werden meist durch die Datenbankadministratoren an- und in einem bestimmten Schema für Sicherheitsrichtlinien abgelegt.

Verbesserter Schutz für Internetanwendungen mit Virtual Private Database (VPD)

Der mit VPD verbundene Schutz ist u.a. für den Applikationskontext „Internet“ von großer Bedeutung. Greifen Anwender über das Internet auf eine Datenbank zu, so kann es ohne VPD unter Umständen mittels „SQL–Injection“ dazu kommen, dass die Datenbank angegriffen wird um Daten auszulesen. Wird nun eine Sicherheitsmaßnahme der Applikationen über der Datensicht, z.B. die Internetanbindung oder die PL/SQL –Prozedur, die auf die Tabelle oder die View zugreift, ausgehebelt, so kann der Angreifer die gewünschten Daten nicht auslesen, da die Sicherung direkt mit dem Objekt, also der Tabelle bzw. View verknüpft ist.

Kontaktadresse:

Ulf Binnemann, Kushtrim Krasniqi
GDV, Gesellschaft für geografische Datenverarbeitung mbH
Neisser Straße 4
D-55218 Ingelheim
Telefon: +49 (0) 6132-71480
Fax: +49 (0) 6132-712828
E-Mail info@gdv.com
Internet: www.gdv.com