# Sicherer IT-Einsatz im kommunalen Bereich SAP R/3 beim LWL-Bau- und Liegenschaftsbetrieb

*Bertil Haack, Georg Fehlauer*

**Zusammenfassung**

Der Bau- und Liegenschaftsbetrieb LWL-BLB ist eine eigenbetriebsähnliche Einrichtung des Landschaftsverbandes Westfalen-Lippe (LWL) mit Betriebssitz in Münster, Nordrhein-Westfalen. Er führt den Immobilienbestand des LWL. Hierzu nutzt er das auf SAP R/3 basierende IT-System PROMOS.CITY der PROMOS consult GmbH, einem Kooperationspartner der TFH Wildau.

Ziel des vorliegenden Beitrages ist es, die von den Autoren initiierte und maßgeblich durchgeführte Entwicklung des IT-Sicherheits- und insbesondere des Berechtigungskonzeptes des LWL-BLB im Zusammenhang mit dem Einsatz von PROMOS.CITY zu skizzieren. Zunächst werden der LWL-BLB vorgestellt sowie die Rahmenbedingungen erklärt, denen das IT-Sicherheitskonzept genügen muss. Danach wird auf die Realisierung, Dokumentation und Einführung des Berechtigungskonzepts eingegangen. Abschließend werden notwendige weitere Schritte aufgezeigt, um das Sicherheitskonzept aktuell zu halten.

**Abstract**

The Bau- und Liegenschaftsbetrieb LWL-BLB, based in Münster, Nordrhein-Westfalen is an own establishment of the Landschaftsverband Westfalen-Lippe LWL. The LWL-BLB administrates the LWL real estate inventory using PROMOS-CITY. This is a SAP R/3 business solution developed by the PROMOS consult GmbH – a cooperation partner of the University of Applied Sciences Wildau.

The intention of this paper is to sketch the development of the LWL-BLB security and authorization concept concerning PROMOS.CITY initiated and significantly realized by the authors. At first we introduce the LWL-BLB and the general conditions with respect to the ict security concept. In the next step we describe the realization, documentation and implementation of the authorization concept. At least we discuss some steps which are necessary to keep the security concept up-to-date.

## 1 Ausgangssituation und Zielsetzung

### Der LWL-Bau- und Liegenschaftsbetrieb (LWL-BLB)

Der Landschaftsverband Westfalen-Lippe arbeitet als Kommunalverband mit 13.000 Beschäftigten für die 8,5 Millionen Menschen in der Region. Mit seinen 35 Förderschulen, 19 Krankenhäusern, 17 Museen und als einer der größten deutschen Hilfezahler für behinderte Menschen erfüllt der LWL Aufgaben im sozialen Bereich, in der Behinderten- und Jugendhilfe, in der Psychiatrie und in der Kultur, die sinnvollerweise westfalenweit wahrgenommen werden. Die neun kreisfreien Städte und 18 Kreise in Westfalen-Lippe sind die Mitglieder des LWL. Sie tragen und finanzieren den Landschaftsverband, den ein Parlament mit 100 Mitgliedern aus den Kommunen kontrolliert.

Der LWL-BLB mit Betriebssitz in Münster, Nordrhein-Westfalen, ist eine eigenbetriebsähnliche Einrichtung des LWL, arbeitet als Dienstleister für den Verband und bestimmt Standardvorgaben im Bau- und Liegenschaftsbereich für den LWL. Der LWL-BLB hat 125 Beschäftigte unterschiedlicher Berufssparten – Ingenieure/innen, Architekten/innen, Betriebswirte/innen, Juristen/innen, Immobilien- und Verwaltungsfachleute, die für die Immobilien des Verbandes planen, bauen und diese bewirtschaften.

Der Immobilienbestand des LWL ist nicht an einer Stelle konzentriert, sondern über das gesamte Verbandsgebiet mit einer Fläche von etwa 21.400 km² verteilt. Er wird im LWL-BLB als Sondervermögen geführt und an den LWL im Vermieter/Mieter-Modell vermietet. Hierbei handelt es sich u. a. um die Verwaltungsgebäude am Standort Münster, um Schulen und um Gebäude und Liegenschaften aus dem Kulturbereich im Verwaltungsgebiet. Nicht zum Sondervermögen des LWL-BLB gehört der Gebäude- und Liegenschaftsbe-

stand der Krankenhäuser im LWL. Dieser befindet sich im Sondervermögen des jeweiligen Krankenhauses. Gleichwohl plant und baut der LWL-BLB hierfür und hält diesen Gebäude- und Liegenschaftsbestand nach. Die zusätzliche Anmietung von Objekten für LWL-Aufgaben oder die Vermietung von Objekten, die nicht mehr zur Aufgabenerfüllung des LWL benötigt werden, werden ebenfalls durch den LWL-BLB vorgenommen.

### Randbedingungen für das Projekt »IT-Sicherheitskonzept«

Der LWL-BLB stand vor der Aufgabe, innerhalb von drei Monaten Liegenschaften mit rund 250 Gebäuden (Bürogebäude, Schulen, Museen) verteilt in Westfalen-Lippe in sein Sondervermögen zu übernehmen, im Rahmen eines Vermieter/Mietermodells zu bewirtschaften, ein kaufmännisches Rechnungswesen zu implementieren und den Beschäftigten den Weg von der Behörde zu einem kommunalen Dienstleister zu ebnen. All diese Forderungen wurden Schritt für Schritt realisiert. Zu einem festgelegten Stichtag waren dabei der Finanzfluss für die Soll- und Habenseite des Betriebes zu gewährleisten, die Immobilien in den Geschäftsverkehr (Mietverhältnis) zu bringen und die Beschäftigten für die neue Aufgabe fit zu machen.

Zur Unterstützung dieser Aufgaben des LWL-BLB wurde auf Grundlage eines Vergabeverfahrens die SAP R/3-basierte immobilienwirtschaftliche Anwendung PROMOS.CITY des IT-Unternehmens PROMOS consult aus Berlin eingeführt. Die Software liegt auf einem Server außerhalb des LWL-BLB und wird extern betreut. Hierfür war ein maßgeschneidertes Sicherheitskonzept zu realisieren, wobei zu jeder Zeit im Projekt die erforderliche Sicherheit der Finanz- und Mietbuchhaltung zu gewährleisten war. Dazu wurde zeitnah zur Softwareeinführung ein Projekt »IT-Sicherheitskonzept« aufgesetzt. Dessen Idee bestand darin, das bereits existierende IT-Sicherheitskonzept des LWL-BLB schrittweise zu optimieren und am Einführungsstand von PROMOS.CITY auszurichten. Somit konnte und kann in jedem Moment die bestmögliche IT-Sicherheit gewährleistet werden.

### Ziel und Aufbau des Beitrages

Ziel des vorliegenden Beitrages ist es, die von den Autoren initiierte und maßgeblich durchgeführte Entwicklung des IT-Sicherheits- und insbesondere des Berechtigungskonzeptes des LWL-BLB im Zusammenhang mit der Nutzung von PROMOS.CITY zu skizzieren. Im Einzelnen werden dazu der LWL-BLB vorgestellt sowie die Rahmenbedingungen erklärt, denen das IT-Sicherheitskonzept genügen muss (Kapitel 2). Danach werden die Arbeitsschritte (Projektstufen) erörtert und es wird auf die Realisierung, Dokumentation und Einführung des endgültigen Berechtigungskonzepts eingegangen (Kapitel 3). Kapitel 4 fasst die wesentlichen Überlegungen dieses Papiers kurz zusammen und zeigt notwendige weitere Schritte auf, um das Sicherheitskonzept aktuell zu halten.

## 2 Das Projekt »IT-Sicherheitskonzept«

### Grundüberlegungen zu IT-Sicherheitsstandards

Für jeden Betrieb oder jede öffentliche Einrichtung stellt es eine Herausforderung dar, einen passenden Sicherheitsstandard für die Abwicklung datentechnisch gestützter zahlungs- und betriebsrelevanter Vorgänge zu finden. Kommt dieser Betrieb aus dem öffentlichen Bereich, sind zudem besondere haushalts- und kassenrechtliche Vorschriften zu berücksichtigen. Ziel ist es unbestritten, hier ein Höchstmaß an Sicherheit gegen Manipulationen und kriminelle Handlungen zu erreichen. Jedoch ergeben sich aus der Praxis vielfältige Fragen. Werden optimierte betriebliche Abläufe durch überhöhte Sicherheitsvorgaben gehemmt? Wie viel Sicherheit ist gefordert? Wie sinnvoll sind die getroffenen Maßnahmen? Welche Kosten entstehen? Wohl nicht umsonst gibt es wegen dieser Fragestellungen eine Menge an Sicherheitsempfehlungen und viele theoretische Abhandlungen zu verschiedenen Teilbereichen. – Wie gestaltet sich aber die Praxis? Einen einheitlichen, umfassenden Sicherheitsstandard zu definieren ist schwierig, weil z. B. für einen kaufmännisch orientierten Betrieb, in dem der monetäre Zahlvorgang im Vordergrund steht, ein zu erarbeitendes Sicherheitskonzept anders ausgerichtet sein muss als z. B. für ein Unternehmen aus dem Gesundheitsbereich, bei dem es beispielsweise um schutzwürdige Patientendaten geht. Entsprechende Sicherheitskonzepte und auch die dafür notwendigen Kontrollen und Prüfungen sind daran anzupassen. Zudem ist immer die Eigenart des Betriebes mit zu berücksichtigen. Aufgaben, Organisation und das eingesetzte Personal sind zusätzliche Faktoren, die ein Sicherheitskonzept beeinflussen.

### Risikopotenziale

Risikopotenziale und damit Ansatzpunkte für das IT-Sicherheitskonzept sind insbesondere in den Regelungen, ihrer Dokumentation und transparenten Durchfüh-

rung zu nachfolgenden Themen der IT-Arbeitsabwicklung zu sehen:

- Zugriffsberechtigungen,
- Customizing,
- Programmentwicklungen und -änderungen,
- Test- und Freigabeverfahren,
- Releasewechsel.

Diese Komplexe können in zwei Gruppen zusammengefasst werden: Einerseits betreffen sie die Nutzung einer vorhandenen IT-Lösung, andererseits deren Veränderung. Entsprechend muss das Sicherheitskonzept zwei wesentliche Bausteine umfassen: zum einen ein Zugriffsberechtigungskonzept sowie zum anderen ein Change Management-Konzept mit den verbleibenden Teilbereichen Customizing, Programmentwicklungen und -änderungen, Test- und Freigabeverfahren und Releasewechsel.

Aus dem zeitlichen Ablauf der Implementierung einer IT-Anwendung in einem Unternehmen ergibt sich, dass Fragen der Zugriffsberechtigung in der Regel zunächst eine höhere zeitliche Priorität besitzen als Fragen der Änderung dieser Software. Im ersten Schritt geht es ja genau darum, die vorhandene Anwendung betriebsbereit zur Verfügung zu stellen und diese tatsächlich zu nutzen. Aus dem täglichen Umgang mit der Software, aufgrund gesetzlicher oder technischer Anforderungen oder aber auch weil die Anwendung seitens des Herstellers weiterentwickelt wurde, können sich dann zu späteren Zeitpunkten Änderungsanforderungen ergeben, die ein angemessenes Change Management erfordern.

Der LWL-BLB hat hierauf reagiert, indem die Erarbeitung und Einführung des Sicherheitskonzeptes in zwei Projektstufen vorgesehen wurden:

- Stufe I zur Entwicklung und Einführung des Zugriffs-Berechtigungskonzepts,
- Stufe II zur Entwicklung und Einführung des Change Management-Konzepts.

### Projektphasen in Stufe I »Zugriffsberechtigungskonzept«

Allen Beteiligten war bewusst, dass die kurze Zeit zur Einführung einer Finanz- und Mietbuchhaltung (s. o.) ein Vorgehen in geeigneten Phasen auf Basis geeigneter grundlegender Regelungen erforderte. Der LWL-BLB hat sich für ein Vorgehen in drei Phasen entschieden: Einführungsphase, Feinabstimmung und Optimierung. Die Sicherheitseinstellungen der Finanz- und Mietbuchhaltung wurden jeweils an die bestehenden Notwendigkeiten zum jeweiligen Einführungsstand der Software angepasst.

In der **Einführungsphase (Phase 1)** wurde von folgenden Basiskomponenten ausgegangen:

- ein am Einführungsstand orientiertes, mitwachsendes Berechtigungs- und Rollenkonzept (in einer Excel-Datei geführt),
- eine personifizierte Rechnerstruktur (pro PC-Kennung eine Userzuweisung),
- eine durchgängige automatisierte Zugriffsdokumentation (jeder Tastendruck wird automatisiert und nachvollziehbar dokumentiert) und
- eine laufende Dokumentation der einzuführenden Software.

Das Zusammenspiel dieser Basiskomponenten erlaubt im Rahmen einer Einführungsphase ein prüfungsfestes Sicherheitskonzept. Zudem war es notwendig, dass wegen der kurzen Einführungsphase die Zugriffsmöglichkeiten weiter gefasst sein mussten, ohne einen ausreichenden Sicherheitsanspruch zu vernachlässigen.

Nach der Einführungsphase folgte die **Feinabstimmung (Phase 2)**. Hier wurden die organisatorischen und betrieblichen Abläufe auf die immobilienbewirtschaftende Software detailliert angepasst. In vielen Fällen war es einfacher und wirtschaftlicher, die Organisation auf die Software abzustimmen als umgekehrt. Die Verantwortlichkeit wurde sukzessiv auf mehrere so genannte Key User mit klar abgegrenzten Bereichen und an der abgestimmten Aufgabe orientiert verlagert. An dieser Stelle wurde vom LWL-BLB eine unabhängige Prüfung des IT-Verfahrens durch eine Wirtschaftsprüfungsgesellschaft beauftragt. Ziel war es, die nunmehr abgestimmten Prozesse und das für die Einführung vorhandene Sicherheitskonzept durch die Prüfungsergebnisse für den Betrieb zu optimieren und an Abläufe zu koppeln. Die Prüfung schloss mit einem Maßnahmenkatalog der Wirtschaftsprüfungsgesellschaft ab, der für den Betrieb vorhandene gesetzliche Regelungen und Vorschriften mit abdeckt.

Dieser Maßnahmenkatalog wurde zum Zweck der **Optimierung (Phase 3)** in zwei Aufgabenbündel geteilt, die im laufenden Betrieb neben dem Tagesgeschäft umgesetzt werden konnten. Das erste Paket befasst sich mit der Optimierung des Zugriffs- und Berechtigungskonzepts und den damit verbundenen Abläufen (Stufe I des Projektes). Das zweite Paket beschäftigt sich mit der Dokumentation für das Änderungsmanagement im Softwarebetrieb und des Verfahrens des Gesamtbetriebes (Stufe II des Projektes). Das Gesamte

soll zudem nicht statisch aufgebaut sein, sondern sich dynamisch an Änderungen im Betrieb entwickeln lassen. Darüber hinaus ist die Forderung gestellt worden, eine möglichst allgemein verständliche Beschreibung zum Verfahren zu erhalten. Hintergrund dessen war das unter wirtschaftlichen Gesichtspunkten sinnvolle Outsourcen von sehr fachspezifischen DV-gestützten Betriebsabläufen. Es muss hierbei jedoch die Kontrolle der Verfahren beim LWL-BLB sichergestellt sein, ohne dass dafür tiefgehendes Spezial-Know-how seitens des LWL-BLB erforderlich ist.

### Projektstufe II »Change Management-Konzept«

Veränderungen am beim LWL-BLB eingesetzten IT-System PROMOS.CITY können vier verschiedene Ausprägungen haben:

1. Änderungen in den Zugriffsberechtigungen,
2. Realisierung von Änderungsanforderungen an PROMOS.CITY,
3. Releasewechsel,
4. Einspielen von Support Packages.

Die Regelungen, Verfahrensweisen und Hilfsmittel zu 1. sind Resultate der Stufe I des Projektes »IT-Sicherheitskonzept« LWL-BLB und als solche im Berechtigungskonzept dokumentiert (s. o.).

Demgegenüber liefert Projektstufe II alle Regelungen, Verfahrensweisen und Hilfsmittel zur Bearbeitung von Veränderungen des IT-Systems PROMOS.CITY gemäß 2. bis 4. Diese sind im Change Management-Konzept des LWL-BLB dokumentiert. Hierauf soll im vorliegenden Beitrag nicht detailliert eingegangen werden.

## 3 Überblick über das Zugriffsberechtigungskonzept

### Anforderungen an ein Berechtigungskonzept im kommunalen Umfeld

Das Berechtigungskonzept ist ein wesentliches Merkmal der Betriebssicherheit. Es regelt die Handlungen von Personen mit der Software. Es erlaubt Handlungen und schränkt diese ein und ist auf die Organisation des Betriebes abzustimmen. Für ein Berechtigungskonzept im kommunalen Bereich sind zudem nicht nur sicherheitsrelevante Vorgaben zu berücksichtigen, sondern auch interne Regelungen, Vereinbarungen mit anderen Abteilungen der kommunalen Einrichtung und der Personalvertretung. So erfolgt z. B. in diesem die eigentliche Zahlung nicht beim LWL-BLB, sondern nach den Rahmenregelungen des Verbandes in der LWL-Finanzabteilung. Hierfür musste ein eigenständiges Verfahren entwickelt werden, welches ebenfalls im Berechtigungskonzept einzuarbeiten war. Im öffentlichen Bereich ist zudem nicht nur die eigentliche originäre Sicherheit des Systems gefordert, sondern in erhöhtem Maße auch eine im öffentlichen Blickfeld stehende nachvollziehbare Korruptionsprävention. Der LWL-BLB hat hierfür eine strukturierte Verfahrens- und Ablaufdokumentation erarbeitet. Es wurde Wert darauf gelegt, dass nicht nur eine einmal aufgestellte statische Verfahrensdokumentation erarbeitet, sondern eine modifizierbare und handhabbare Dokumentation konzipiert wurde. Einzelne Dokumentationsbausteine wurden personifiziert. Das bedeutet, Personen sind verantwortlich mit der Weiterentwicklung der Dokumentation betraut. So wird sichergestellt, dass die Dokumentation bei Systemerweiterungen und -änderungen immer auf dem aktuellen Stand bleibt.

### Aufbau des Berechtigungskonzeptes

Das Berechtigungskonzept setzt sich aus technischen, die Parameter der Software betreffenden Festlegungen sowie aus organisatorischen, die Arbeitsprozesse betreffenden Regelungen zusammen. Die technischen Festlegungen spiegeln sich in den Standard-Mechanismen von SAP R/3 zur Berechtigungsvergabe und in den speziellen Features von PROMOS.CITY wider. Die organisatorischen Regelungen führen zu spezifischen Arbeitsprozessen und spezifischen Werkzeugen wie etwa Formulare und Checklisten.

Seitens der Software R/3 steht eine Vielzahl von **Standard-SAP-Mechanismen zur Berechtigungsvergabe** und damit zur IT-konformen Absicherung der Betriebsplattform SAP zur Verfügung. Da dieser Beitrag im Wesentlichen die *spezielle* Nutzung von Standard-SAP-Mechanismen im Kontext des kommunalen Bereichs darstellen soll, wird auf eine umfangreiche Wiedergabe von *generellen* Aspekten des SAP-Berechtigungskonzepts verzichtet. Hierzu sei auf die umfangreiche Literatur zu SAP-Berechtigungsthemen verwiesen (s. Literaturverzeichnis). Exemplarisch seien die folgenden Berechtigungsthemen genannt:

- Benutzerverwaltung (Kennwortrichtlinie, Usertypen etc.),
- Berechtigungskonzept mit Rollen/Profilen.

Die Benutzerverwaltung der SAP ERP Central Component (SAP ERP ECC) verwendet die durch den SAP NetWeaver Application Server für ABAP angebotenen

Mechanismen wie Benutzertypen und Kennwortkonzept. Die SAP ERP Central Component verwendet das Berechtigungskonzept des SAP NetWeaver Application Servers. Daher gelten für SAP ECC die Sicherheitsempfehlungen und -richtlinien für Berechtigungen, wie sie im Sicherheitsleitfaden des SAP NetWeaver Application Servers für ABAP beschrieben sind.

Mit Hilfe von Berechtigungen können Sie den Zugriff der Benutzer auf das System einschränken und somit Transaktionen und Programme vor unberechtigtem Zugriff schützen.

Grundlegend für die Berechtigungsmechanismen in einem SAP-System sind folgende Bausteine, die konkret festzulegen sind:

- Rollen,
- Berechtigungen,
- Berechtigungsobjekte,
- Berechtigungsprofile.

Neben diesen Berechtigungsmechanismen besteht für Administratoren im System die Möglichkeit, über eine Vielzahl von Mandanten-, Parameter- und Systemeinstellungen den Zugriff und die Veränderung von DB-Tabellen zu protokollieren. Diese Protokollierung kann auf Einzeltabellen, wie z. B. buchhalterischen Tabellen, festgelegt und über Audit-Reports ausgewertet werden. Damit kann vom Administrator jederzeit der Zugriff auf sensible Bereiche eines SAP-Systems protokolliert oder sogar gänzlich eingeschränkt werden.

Die immobilienwirtschaftliche Anwendung PROMOS.CITY ist eine branchenspezifische Lösung auf Basis SAP R/3. Sie setzt auf den angesprochenen Standard-SAP-Mechanismen zu Berechtigungen auf und bietet ein revisionssicheres Berechtigungskonzept. Die wesentlichen **PROMOS.CITY-Mechanismen zu Berechtigungen** sind:

- SAP-Systemparameter,
- Mandanteneinstellungen,
- Repository/Tabellen,
- Benutzerverwaltung,
- Rollen und Berechtigungen,
- Berechtigungsvergabe,
- Notfallkonzept,
- System-Dokumentation.

Generell erfolgte die konkrete Ausprägung dieser Komponenten – beispielsweise die Einstellung der SAP-Systemparameter für den LWL-BLB – bei der Umsetzung des Projektes. Durch eine zentrale Protokollierung während der Einführungsphase wurden alle Einstellungen zusammengefasst und dokumentiert.

Die **organisatorischen Abläufe** zur Umsetzung des LWL-BLB-Berechtigungskonzepts wurden in fünf Etappen entwickelt:

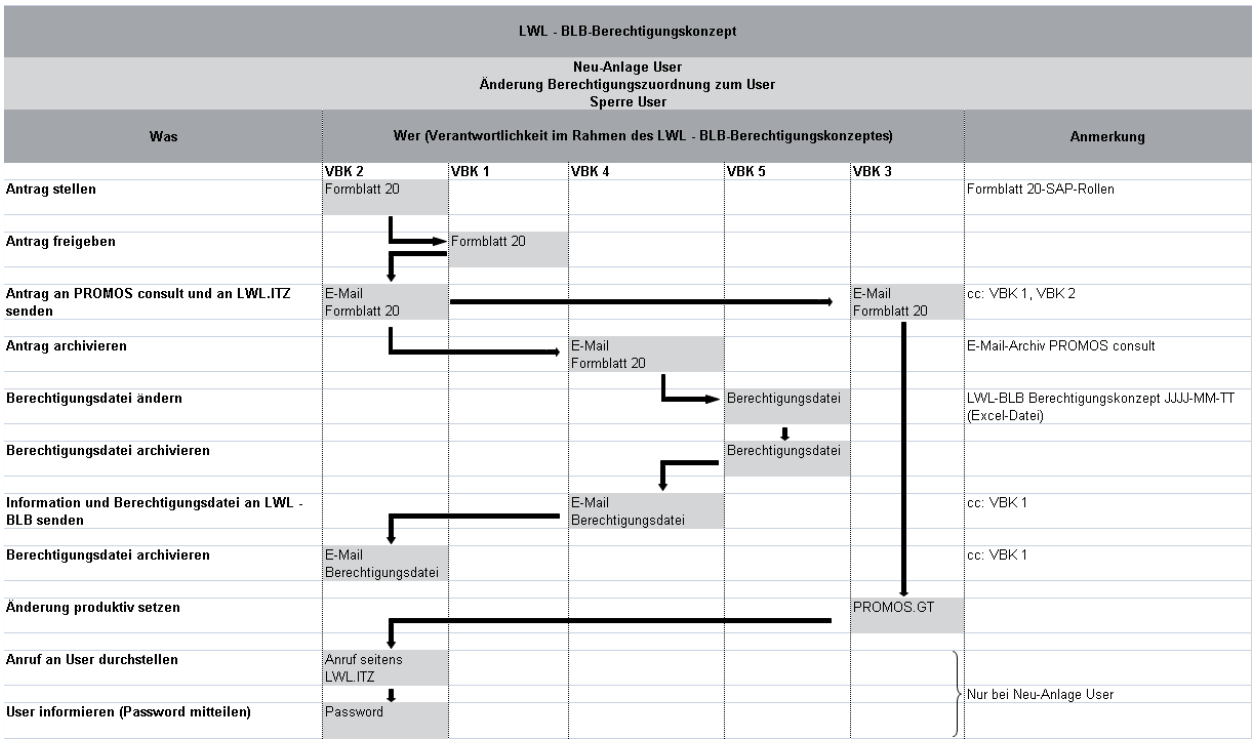


Abb. 1: Ausgewählte Prozesse im Berechtigungskonzept

- Analyse der Ist-Situation und Aufbereitung der Ergebnisse,
- Beschreibung der zukünftigen Arbeitsprozesse im Rahmen des Berechtigungswesens des LWL-BLB,
- Abstimmung und Überarbeitung der Arbeitsprozesse,
- Freigabe der Arbeitsprozesse,
- Einweisung der Mitarbeiter in das Berechtigungswesen (speziell: in die Arbeitsprozesse).

Am Ende des Projektes stand eine vollständige Beschreibung aller Aufgaben im Rahmen des LWL-BLB-Berechtigungswesens zur Verfügung. Es war damit festgelegt, wer wann welche Aufgabe im Berechtigungswesen wahrzunehmen hat.

Als Beispiel sei der Prozess in Abbildung 1 genannt. Er beschreibt, in welcher Weise die Aktionen

- Neuanlage User,
- Änderung Berechtigungszuordnung zum User,
- Sperre User

durchzuführen sind. Anhand dieses Beispiels wird deutlich, dass die **Verantwortlichkeiten** für die einzelnen Prozessschritte durch ein auf Rollenkonzept geregelt werden, d. h. dass das Berechtigungskonzept auf Rollen basiert, die von den jeweils zuständigen Mitarbeitern/innen wahrgenommen werden müssen. Im vorliegenden Fall sind dies insgesamt fünf Rollen, VBK1 bis VBK5 (VBK = Verantwortliche/r für das Berechtigungskonzept):

- VBK1 besitzt die Gesamtverantwortung für das Zugriffsberechtigungskonzept (Beispiel: Antrag Neuanlage User freigeben).
- VBK2 besitzt die fachliche Verantwortung für das Zugriffsberechtigungskonzept (Beispiel: Antrag Neuanlage User stellen).
- VBK 3 besitzt die Verantwortung seitens LWL.ITZ für die Durchführung von Berechtigungszuweisungen (Neuanlage User im System durchführen).
- VBK 4 besitzt die Gesamtverantwortung für das Zugriffsberechtigungskonzept seitens PROMOS consult (Beispiel: Änderungen Berechtigungsdatei bei Neu-Anlage User initiieren).
- VBK 5 besitzt die technische Verantwortung für das Zugriffsberechtigungskonzept seitens PROMOS consult (Beispiel: Änderung Berechtigungsdatei bei Neu-Anlage User durchführen).

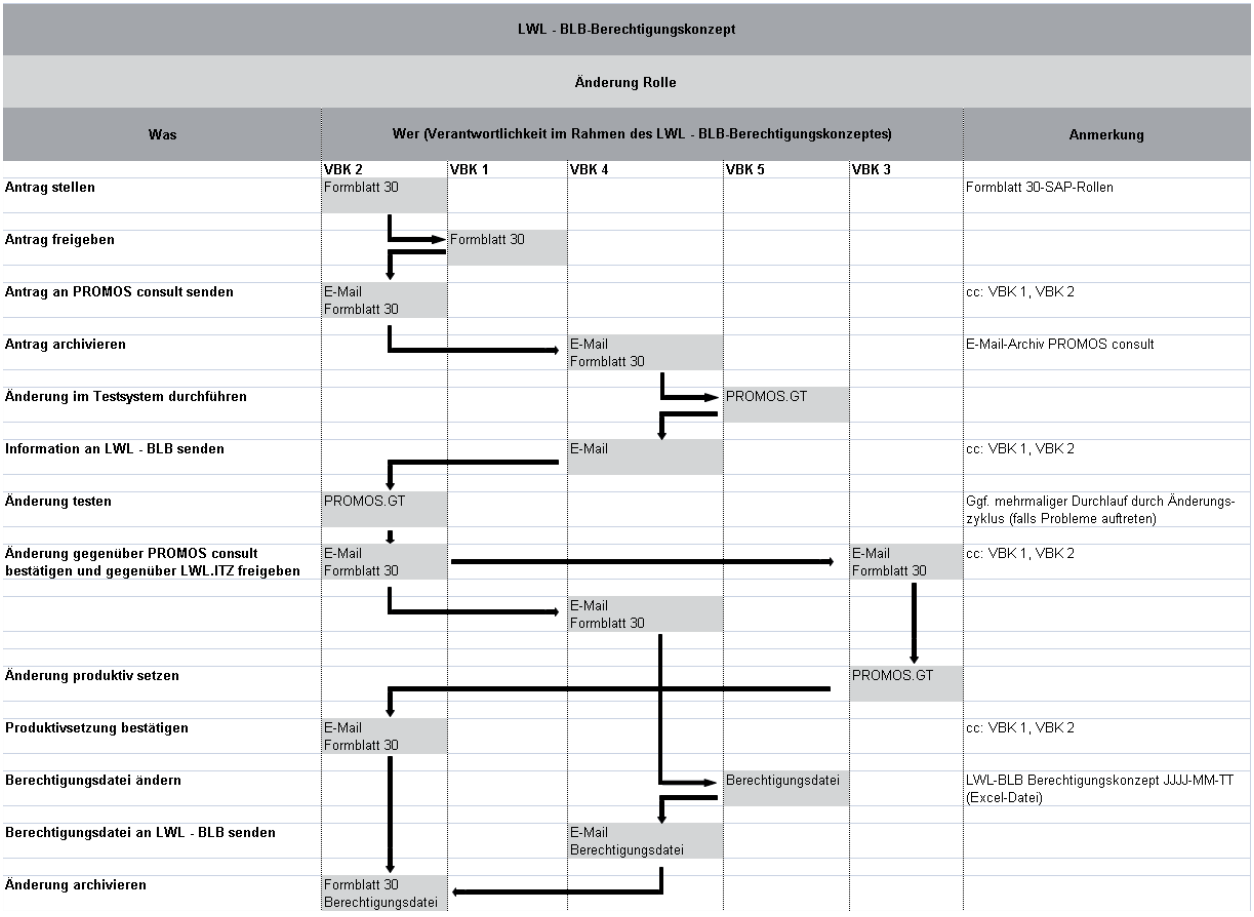


Abb. 2: Änderung von Rollen im SAP-System

Diese Verantwortlichkeiten kommen auch im Prozess in Abbildung 2 zum Tragen. Dieser legt fest, wie Änderungen an den im SAP-System gültigen Rollen (z. B. Mietbuchhalter) durchzuführen sind.

## 4 Fazit und weitere Schritte

Im vorliegenden Beitrag werden zentrale Überlegungen hinsichtlich des IT-Sicherheitskonzepts eines kommunalen Eigenbetriebes beschrieben. Ausgangssituation für die hier dargestellte Arbeit ist die Einführung der Software für die Immobilienbewirtschaftung PROMOS.CITY im LWL-Bau- und Liegenschaftsbetrieb. Im Zusammenhang damit wurde ein IT-Maßnahmenkatalog für den LWL-BLB entwickelt. Dieser kann als Basisdokument im Rahmen der IT-Sicherheitskonzeption des LWL-BLB betrachtet werden. Aus ihm wurde das IT-Sicherheitskonzept des LWL-BLB mit den Komponenten Berechtigungskonzept und Change Management-Konzept abgeleitet. Die einzelnen Positionen des Maßnahmenkataloges wurden hierfür im Verlauf der hier dargestellten Arbeitsschritte erledigt und damit das IT-Sicherheitskonzept in der gewünschten Weise realisiert.

Indem anschließend alle Positionen des Maßnahmenkataloges daraufhin betrachtet wurden, ob es sich um einmalige oder regelmäßig zu wiederholende Aufgaben handelt, wurde aus dem Maßnahmenkatalog zu guter Letzt eine To Do-Liste mit Verantwortlichkeiten und Terminvorgaben der Aktivitäten hergeleitet, die in Zukunft nachgehalten werden müssen, um das IT-Sicherheitskonzept und damit PROMOS.CITY jederzeit auf dem notwendigen aktuellen Stand zu halten. Maßgabe dabei ist, dass der LWL und der LWL-BLB jederzeit alle Grundlagen der ordnungsgemäßen Buchhaltung (GoB) erfüllen und damit insbesondere den Anforderungen des Wirtschaftsprüfers genügen müssen und wollen.

Das skizzierte Vorgehen kann und soll keine Allgemeingültigkeit für sich beanspruchen. Dessen ungeachtet liefert es Anregungen und gleichsam Rezepte für Unternehmen speziell im kommunalen Umfeld, die ebenfalls vor der Frage stehen, ein passendes Sicherheitskonzept für IT-gestützte zahlungs- und betriebsrelevante Vorgänge zu erarbeiten und sicherzustellen. Die einzelnen Vorschläge stammen aus der Praxis für die Praxis und zeichnen sich daher durch ihre Einfachheit, Effektivität und Effizienz aus. Zwischenzeitlich sind sie in ergänzter Fassung als Buch erschienen (s. Literatur).

### Literatur

Fehlauer, G./Haack, B./Schulz, V./Wollenhaupt, H. (2008): IT-Sicherheitsstandards im kommunalen Bereich – Das Sicherheitskonzept des LWL – Bau- und Liegenschaftsbetriebes, Berlin: PROMOS press.

IBM Business Consulting Services (2006): SAP-Berechtigungswesen – Design und Realisierung von Berechtigungskonzepten für SAP R/3 und SAP Enterprise Portal, Bonn: Galileo Press (3. Nachdruck).

Linkies, M./Off, F. (2006): Sicherheit und Berechtigungen in SAP-Systemen, Bonn: Galileo Press.

Kösegi, A./Nerding, R. (2005): SAP-Änderungs- und Transportmanagement, Bonn: Galileo Press (2. aktualisierte und erweiterte Auflage).

### Autoren

**Dipl.-Ing. Georg Fehlauer**
Projektverantwortlicher beim Landschaftsverband Westfalen-Lippe (LWL) – Bau- und Liegenschaftsbetrieb (BLB)
georg.fehlauer@lwl.org

**Prof. Dr. Bertil Haack**
Technische Fachhochschule Wildau
Dekan des Fachbereichs Wirtschaft, Verwaltung und Recht
bertil.haack@tfh-wildau.de
www.goals-strategies.com/haack