Christoph Wildensee

Der Zugriff auf wirtschaftlich sensible Kundendaten im SAP®

Ein Prüfungsansatz für die Interne Revision und den Datenschutz

„Datenskandale“ gab es in der letzten Zeit mehr als genug. Nicht nur die Verhaltensüberwachungen von Mitarbeiterinnen und Mitarbeitern per (verdeckter) Videoanlage und Detektiveinsatz, E-Mail-Analysen der Mitarbeiter-Accounts durch den Arbeitgeber oder undifferenzierte Massendatenanalysen mit Personaldatenbezug zur vorgeblichen Korruptionsprävention sind hier zu nennen, sondern auch die Möglichkeit des Zugangs externer Beratungs- und Dienstleistungsunternehmen auf **Kunden-Echtdaten** (vor Ort ggf. mit ungesicherten Systemen oder per Remote-Access) oder der „Verlust“ von Kundendaten mit Informationen wie Vertragslaufzeiten und monetären Ablaufleistungen.

Dabei blieb in den Medien unbeachtet, ob Datenlieferungen an Externe im Rahmen von Auftragsdatenverarbeitungsverhältnissen nach § 11 Bundesdatenschutzgesetz möglicherweise korrekt abliefen und die externen Dienstleister ggf. rechtswidrig ihrer Pflicht zur Datenlöschung nicht nachkamen. Der vermeintliche Schaden des Vertrauens- und Integritätsverlustes diktierte den angeschlagenen Ton.

Ich möchte aber nicht die weitere Diskussion um Massendatenanalysen mit Personenbezug und deren mögliche rechtliche Zulässigkeitsbedingungen – wie häufig in aktueller Literatur zu finden – befeuern, sondern vielmehr beispielhaft den Gefährdungsaspekt von Persönlichkeitsrechten durch die Nutzung gespeicherter Kundendaten außerhalb der eigenen Systeme bzw. des eigenen Hauses beleuchten.

Dabei rücken Zahlungsdaten immer mehr in den Fokus der Betrachtung. Nach Recherchen der „Wirtschaftswoche“ sind auf dem Schwarzmarkt Bankverbindungen von mehr als 21 Millionen Bundesbürgern illegal im Umlauf [1]. Inwieweit diese Bankdaten aktuell sind, wird zwar nicht erläutert, wenn aber nur ein Bruchteil davon nutzbar ist, kann dies zu erheblichen Schäden für den Einzelnen und die Banken führen. Über Internet-Kriminalität (z.B. „Phishing“) und auch über Abbuchungen aus dem Ausland oder aber Geldtransfers in das Ausland über lokale „Finanzagenten“ wurde bereits häufig berichtet.

1 siehe WIWO2008

Mit zunehmender Intensität werden Kontoinformationen dazu verwendet, Abbuchungen ohne vertragliche Grundlage zu generieren – in der Hoffnung, dass der Kontoinhaber die Kontobewegung nicht moniert und sie daher nicht rückgängig macht innerhalb gesetzter möglicher Frist [2]. Dass also Kontoinformationen en bloc nicht nur sensible Daten darstellen, sondern insbesondere wirtschaftlich verwertbar sind, ist schnell ersichtlich.

Interessant ist aber, woher solche Kundendaten stammen? Wer hat in Unternehmen – wenn doch die Erkenntnis vorhanden ist, dass es sich um sensible Daten handelt – Zugriff auf die Rohdaten der Kunden, aber auch auf spezifische Auswertungen oder Datenbank-Views ? Kann ein Unternehmen diese Daten(kategorien) überhaupt vor strukturierter Auswertung und Download schützen ?

Der nachfolgende Artikel soll ausgesuchte Grundlagen speziell am Beispiel von SAP® IS-U und BI/BW darstellen – dem Vertragsverwaltungs- und -abrechungssystem der Energieversorgung und dem Datenanalyse- und Reportingwerkzeug von SAP®. Daten hieraus können aufgrund der hohen Qualität und Aktualität grundsätzlich auch missbräuchlich genutzt werden. Unbeachtet bleibt bei der folgenden Betrachtung, dass ein System wie IS-U auch weitere Schnittstellen – z.B. zu einem Portal- oder CRM-System – aufweist, die ebenfalls häufig diese Daten beinhalten.

SAP IS-U und die Aktualität der Grunddaten

SAP IS-U ist ein geschäftsprozessorientiertes Vertriebs- und Informationssystem, das alle Versorgungsarten, Sparten und Serviceleistungen eines Energiedienstleistungsunternehmens abdecken kann. Es dient gleichermaßen zur Verwaltung und Abrechnung von Tarif-, Sondervertrags- und Dienstleistungskunden. Durch Integration der Standardkomponenten Kundenservice (CS), Vertrieb (SD) und Instandhaltung (PM) können auch Serviceaufträge u.Ä. abgewickelt werden. Aufgrund der großen Anzahl von Buchungen aus Abrechnungen und Abschlagsforderungen (bisher im Tarifbereich zumeist monatlich als Abschlag mit jährlicher Ist-Abrechnung, zukünftig bspw. im Rahmen von Smart Meter auch andere Modalitäten) werden diese in einer eigenen Nebenbuchhaltungskomponente Vertragskontokorrent (FI-CA) verarbeitet.

Es ist naheliegend, dass Kundendaten eines solchen Unternehmens besonders interessant für eine missbräuchliche Nutzung sind, denn für eine abusive Verwendung ist die Aktualität von hoher Bedeutung. Kundendaten nicht oder erst vor kurzer Zeit gekündigter Vertragsverhältnisse von Energieversorgern können kaum attraktiver sein, wenn sie mit einer gültigen Bankverbindung ausgestattet sind. Energie bezieht fast jede Person. Entsprechende Zugriffe auf den Kundendatenbestand ermöglichen somit die Versorgung mit „frischen“ / nutzbaren Grunddaten für Akquise und Abbuchung.

2 SUEDBADEN2009: „Eine Flut von Beschwerden über unerlaubte Telefonwerbung, untergeschobene Verträge und unerlaubte Kontoabbuchungen erhält die Verbraucherzentrale Baden-Württemberg zurzeit. Dreist rufen Gewinnspielfirmen und Lottospielgemeinschaften Verbraucher zu allen Tageszeiten an, konfrontieren sie mit angeblichen Vertragsabschlüssen sowie ihren Kunden- und Kontodaten und buchen illegal Beträge von ihren Konten ab.“.

Ausgesuchte Grundzüge des Berechtigungskonzeptes

Die Berechtigungsverwaltung im SAP IS-U-System erfolgt rollenbasiert. Die Mitarbeiterinnen und Mitarbeiter erhalten nur Zugriff auf relevanten Content entsprechend der Arbeitsplatzrolle. Allerdings ist leicht ersichtlich, dass die Anzahl der Rollen im Unternehmen begrenzt werden muss, da ansonsten die Administration für beinahe jede Person eine eigene Rolle entwerfen / ausprägen kann. So werden Mitarbeiter/-innen aufgabenbezogen gebündelt. Es entstehen Rollen, unter denen sich mehrere Personen finden, deren Aufgabenumfang zumeist nicht vollständig übereinstimmt, aber sehr ähnlich ist (Standard-Arbeitsplätze). Die Summe der notwendigen Berechtigungen der Gruppenmitglieder definiert das Zugriffsspektrum der jeweiligen Rolle. Zusätzlich werden Delta-Berechtigungen, sog. Add-Ons, bereitgestellt, die ausgesuchten Key-Usern zugewiesen werden, die beispielsweise über langjährige Erfahrung verfügen und analog Sonderfälle bearbeiten oder zur Fallbearbeitung spezielles Know-how beitragen können. Diese Berechtigungen werden dann aus den Standardrollen herausgehalten. In nachstehender Tabelle Tab. 1 werden einige Rollen aufgeführt.

Eine Vielzahl von umfangreich berechtigten Personen arbeitet in der Sachbearbeitung der „Customer-Shared-Service"-Bereiche. Diese kümmern sich übergeordnet um Kundendaten im weitesten Sinne, z.B. als zentraler First-Level-Ansprechpartner der Kunden, um einen großen Prozentsatz der Kundenanfragen bereits hier abzudecken *(ggf. auch über Call-Center-Strukturen: Entweder werden die Kunden bereits in den Standardaufgaben wie Einzug, Auszug u.Ä. im Call-Center betreut und lediglich bei den komplexeren Aufgaben in das Back-Office des Hauses verwiesen, oder die Call-Center-Agents nehmen lediglich die Fälle auf und reichen sie an autorisierte Mitarbeiter/-innen des Unternehmens weiter)* oder als Spezialist für Sonderfälle im Kunden-Back-Office-Bereich. So ist es nicht abwegig, dass neben den System-, Schnittstellen-, Modulbetreuungs- und Administrationsusern des IS-U allein über die (erweiterte) Sachbearbeitung ggf. um die 100 Personen oder auch mehr mit jeweils partiellen Änderungs- und weitreichenden Sichtrechten ausgestattet sind. Hinzu kommen die zentrale Kundenabrechung, analysierende Bereiche wie ein ggf. zentrales Datenreporting usw. Hierbei einzubeziehen ist ebenfalls, dass sowohl ein produktives Vertriebssystem als auch ein System der Netzgesellschaft vorhanden ist, in denen die Kundenstammdaten gleich lauten. Die „Shared-Service"-Bereiche haben üblicherweise auf alle produktiven Kundendaten Zugriff.

Rolle / Aktivitätsgruppe
ADDON_ENERGIEDATENMANAGEMENT
ADDON_INKASSODIENST
ADDON_MAHNUNGSBEARBEITUNG
ARBPL_AUSSENDIENST
ARBPL_GERAETE_PRUEFUNG
ARBPL_GERAETE_STAMMBEARBEITUNG
ARBPL_KUNDENDATENREPORTING
ARBPL_ABRECHNUNG
ARBPL_SONDERVERTRAG
ARBPL_FORDERUNGSMANAGEMENT
ARBPL_SACHBEARBEITUNG
ARBPL_ZAHLUNGSEINGANG
[...]

Tab. 1: Beispielrollen im IS-U

Tabellenzugriffe

Die Kundenverwaltung wird in einer größeren Anzahl von Tabellen gehalten. Der nachfolgende Ausschnitt zeigt einen wesentlichen Teil hieraus:

BUT000	Business Partner (BP): Partnernummer, Kategorie, Name usw. (KeyField: PARTNER)
BUT020	BP: Adressen-Index, Gültigkeit (KeyField: PARTNER, ADDRNUMBER)
BUT021_FS	BP: Zeitabhängige (aktuelle) Adressverwendung (KeyField: PARTNER, ADDRNUMBER)
ADRC	tatsächliche Adressdaten (KeyField: ADDRNUMBER)
ADR2	BP: Telefonnummern (KeyField: ADDRNUMBER)
ADR6	BP: Email-Adressen (KeyField: ADDRNUMBER)
BUT0BK	BP: Bankdaten (KeyField: PARTNER; relevante Felder mind. BANKL, BANKN, KOINH)
BUT050	BP: Beziehungen / Rollenfindungen – Index Allg. Daten (KeyField: PARTNER1, PARTNER2)
BUT051	BP: Beziehungen – Index Ansprechpartner (KeyField: PARTNER1, PARTNER2)
DPAYH	Zahlungsprogramm – Daten zur Zahlung (KeyField: GPA1R, ACC1R, ZBNKL, ZBNKN)
FKKVKP	Vertragskonten (KeyField: GPART, VKONT)
EEIN	Einzugsbeleg Vertragskontoebene (KeyField: EINZBELEG, KUNDE, VKONT)
EAUS	Auszugsbeleg Vertragskontoebene (KeyField: AUSZBELEG, KUNDE, VKONT)
EVER	IS-U-Vertrag (KeyField: VERTRAG, VKONT, ANLAGE)
ERDK	Druckbeleg / Kopfdaten Rechnung (KeyField: OPBEL, PARTNER, VKONT)

Tab. 2: Ausschnitt relevanter Tabellen

Aus diesen Tabellen lassen sich bereits Listen mit den wesentlichen Kundenstamminformationen einschließlich der kritischen Inhalte E-Mail, Telefonnummer und Bankverbindung entwerfen, die zwar nicht immer, aber doch in einer nicht unbeträchtlichen Anzahl gepflegt sind.

Interessant ist zunächst, zu welchen Berechtigungsgruppen diese Tabellen gehören. Hierüber lässt sich ermitteln, wer über die allgemeine Tabellenanzeige wie z.B. SE16, SE16N, SE17 usw. Zugriff auf diese Daten erhält.

Die Tabelle TDDAT zeigt für die hier genannten Tabellen vornehmlich die Gruppe **SA** an.

Da das Sichtrecht zumeist als weniger sensibel angesehen wird als das Recht zur Änderung, wird der Zugriff häufig weit gestreut. Wenn die Berechtigungen sogar nur dahingehend eingeschränkt werden, dass der Zugriff über die zutreffende oder verweigerte Transaktionsberechtigung gesteuert wird und alle Benutzerstammsätze eine Vielzahl von Berechtigungsobjekten mit höherer Ausprägung – z.B. mit Berechtigungsgruppe * – aufweisen, steht hier möglicherweise eine weitreichende Sicht- und ggf. Download-Berechtigung zur Verfügung.

Für eine Tabellensicht auf diese Tabellen ist folgende Berechtigungsobjektausprägung notwendig:

Tabellenzugriff:

S_TABU_DIS
ACTVT 03 (Anzeigen)
DICBERCLS **SA**

Transaktionscode:

S_TCODE		
	TCODE	SE16 oder
		SE16N oder
		SE17 o.Ä.

Download-Berechtigung:

S_GUI		
	ACTVT	61 (Exportieren)

oder obiger Tabellenzugriff i.V.m. RFC-Berechtigung (siehe beispielsweise externes Tool ‚Extract On Demand for SAP'):

S_RFC		
	ACTVT	16 (Ausführen)
	RFC_TYPE:	FUGR (Funktionsgruppe)
	RFC_NAME:	(SYSE, SYST, SYSU, SRFC) und (SDTX oder SRTT oder BDCH [Zugriff beispielsweise auf den Funktionsbaustein RFC_READ_TABLE über die Gruppe SDTX])

Zusätzlich ergeben sich ggf. Zugriffsrechte durch Tabellenänderungs- und -anzeigetransaktionen im Kundennamensraum (z.B. ZTAB* o.Ä.), die ebenfalls in eine Berechtigungsanalyse einzubeziehen sind. Wenn also ggf. abgestufte Änderungs- oder Anzeigetransaktionen für die Sachbearbeitung bereitgestellt werden, um eben nicht die Standardtransaktionen und notwendigen Berechtigungsobjekte ausprägen zu müssen, kann sich ein weites Feld öffnen.

Besonderheit der Tabelle DPAYH

Die Tabelle DPAYH (Berechtigungsgruppe &NC&) ist die zentrale Datei des Zahlungsstroms in Richtung Geschäftspartner / Kunde. Gleichsam kann sie angesehen werden als Historie verifizierter Kontoverbindungen. Enthalten sind hier Geschäftspartnernummern, Vertragskonten, Adress- und Zahlungsinformationen, d.h. Kontoverbindung, Zahlungsempfänger, Ausgleichsbetrag und Ausführungsdatum je Ausgleichsposten. Wer hier zugriffsberechtigt ist, hält ebenfalls maßgeblichen Content in der Hand – nicht nur Grunddaten der Vertragspartner, sondern auch eine individualisierte Abschätzungsmöglichkeit des Vertragsvolumens oder -verhaltens. Zu beachten ist die Zugehörigkeit zur Berechtigungsgruppe &NC&. Sie ist die ursprüngliche Berechtigung zum Anzeigen aller nicht geschützten / klassifizierten Tabellen (ohne Eintrag in der Tabelle TDDAT). Auch solche Tabellen können somit problematisch wirken. Dies ist in den Analysen ebenfalls einzubeziehen.

Analysemethodik analog oben mit Tabellenzugriff:

S_TABU_DIS		
	ACTVT	03 (Anzeigen)
	DICBERCLS	&NC&

Häufig liegen die Berechtigungen in der dargestellten Form vor, allerdings ist dies wie oben angedeutet nicht die einzige Möglichkeit, Zugriff auf sensible Kundendaten zu nehmen. Vielmehr existieren beispielsweise noch Views, die ebenfalls eine Einsichtnahme ermöglichen und in Kombination mit der Download-Berechtigung kritisch sind.

View-Zugriffe

Views (engl. Sicht) sind logische Relationen auf vorhandene Tabellen zur Abbildung thematisch nahestehender Felderkonstellationen oder in der Sicht verkürzter Tabellendarstellungen. Meist bestehen Views aber aus Zugriffen auf mehrere logisch abhängige Tabellen. Der aufrufende Benutzer kann eine Sicht wie eine Tabelle abfragen, muss sich aber keine Gedanken darüber machen, welche hierarchischen Abhängigkeiten / Fremdschlüsselbeziehungen ggf. zu beachten sind, wenn die Originaltabellen herangezogen werden. Insofern stellt die Nutzung solcher Views technisch einen erleichterten und Performance-optimierten Zugriff auf relevanten Content dar.

Häufig werden lediglich die direkten Tabellensichten eingeschränkt, weil hier die originären SAP®-Tabellen angegeben und zur weiteren Nutzung bereitgestellt werden können. Tatsächlich stellen aber auch Views eine unproblematische Datenbereitstellung dar, die es im Rahmen einer Risikobetrachtung zu minimieren gilt. Zugriffe auf gespeicherte Inhalte in Tabellenform via View-Aufruf kann man beispielsweise erhalten über die Transaktionen SA38 (ABAP-Programmausführung), SE38 (ABAP-Editor), SE84 (Repository-Infosystem), SE15 (Object-Navigator) u.Ä.

Die Rollenausprägungen der Fachbereichsarbeitsplätze sollten somit möglichst keine Funktionalitäten beinhalten, die einen Direktaufruf von Views zulassen. Solche Transaktionen aus dem Basis-Bereich sollten weitestgehend eine Ausnahme für die Sachbearbeitung darstellen, da sie aus nachvollziehbaren Gründen für die Administration, ggf. Revision u.Ä. zu reservieren sind. Der Kundennamensraum ist selbstverständlich auch hier einzubeziehen.

Die nachfolgende Tabelle zeigt Beispiel-Views mit Referenz zu Bank- und Adressdaten, die in Kombination o.g. wirtschaftlich sensible Daten darstellen.

View-Name	Bezeichnung
INV_BP_BANK_DATA	Bankdaten zum Geschäftspartner
V_BUT000	Help-View Business Part. Bank Account
V_BUT020	Help-View Part. Bank Account: Search by address
V_BUT0BK_BW	GP: Bankverbindungen
V_FVKPBA	Vertragskonten =›Bankverbindungen selektieren
V_FVKPG	Selektion von GPs zum Konto (Adressen)
U_11131	Geschäftspartner-Bankverbindung

Tab. 3: Beispiel-Views mit Kundenbankdaten- und -adressbezug

Reporting

Übliche Wege für einen Zugriff auf Kundendaten für die Sachbearbeitung stellen die Standard-Transaktionen und -Reports / ABAPs bereit. Allerdings sind im IS-U keine vorhanden, die in Listform z.B. Kundendaten mit Bezug zu den Datenfeldern BUT0BK-BANKL (BLZ), BUT0BK-BANKN (Kontonummer) und ggf. BUT0BK-KOINH (Kontoinhaber) darstellen. Zumeist werden die Daten zu einem Kunden zur Einzelsatzbearbeitung /

-ansicht als Bearbeitungsblatt bereitgestellt, was nebenbei als Hemmschwelle einer missbräuchlichen Massendatennutzung gesehen werden kann, denn eine große Anzahl von Kunden bereitzustellen, bedarf einer intensiven manuellen Bearbeitung. Beispiele hierfür sind die Darstellung über CIC-Profile oder die Transaktion EC20 (IS-U Front Office).

Zur flexiblen Datenaufbereitung in Listform kann allerdings das **SAP BI/BW** bzw. der **BEx Analyser** eingesetzt werden (z.B. Transaktion RRMX [Analyser] und RSA1 [Administration Workbench: Modellierung]). Die ausgewählten InfoProvider (Datencontainer) können über Queries abgefragt und den Fachbereichen als Query-View zugeordnet werden. Die Daten werden adäquat zur weiteren Bearbeitung in Excel dargestellt.

InfoProvider können auch als Datenlieferant verstanden werden, die als strukturierte Datencontainer mit IS-U-Daten beladen werden (Basis-InfoCubes, transaktionaler InfoCube usw.). Hierunter fallen aber auch Objekte, die keine physische Datenablage, sondern eine logische Sicht auf Daten darstellen (RemoteCubes, MultiProvider usw.). Alle Typen von InfoCubes sind InfoProvider; sie unterscheiden sich lediglich in der Art der Datenbeschaffung, dem Detaillierungsgrad und der Nähe zum Quelldatensystem.

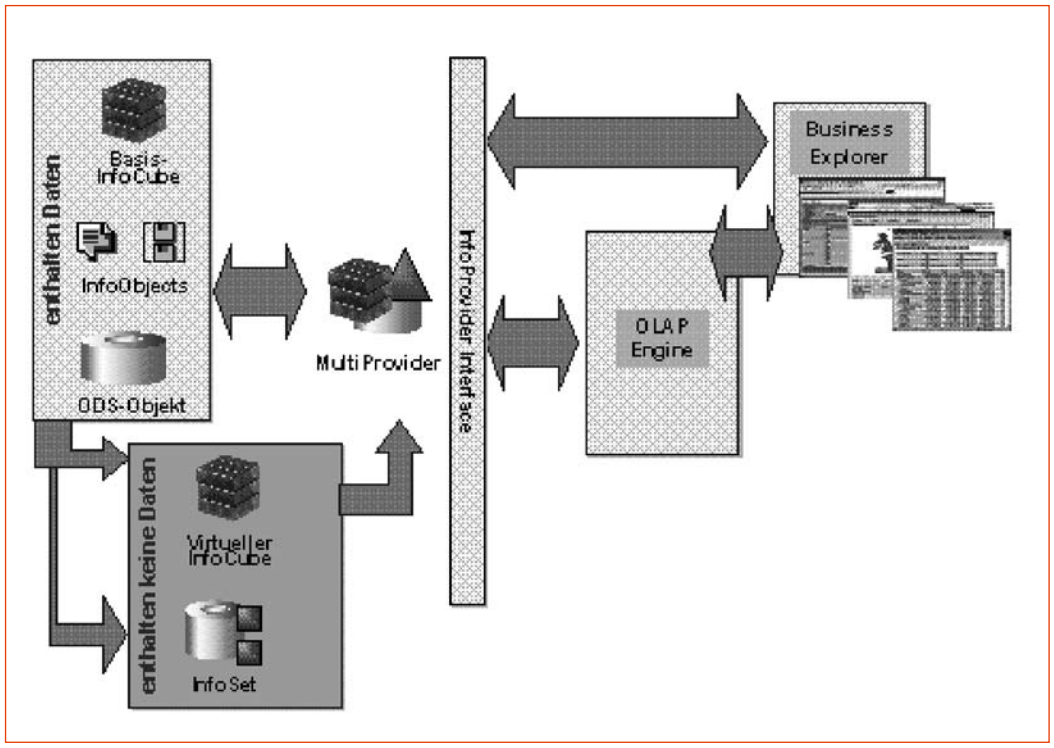

Abb. 1: Überblick über verfügbare Objekte des SAP BI/BW (Quelle: SAP® AG)

Datencontainer bieten definierte Datenbereiche, die über Queries angesteuert werden können. Dabei werden betriebswirtschaftlich gruppierte Strukturen in Relation gesetzt, so dass würfelähnliche Analysewege eingeschlagen werden können. Beispielsweise können Verkaufszahlen zum einen über mehrere Jahre betrachtet werden, aber auch über unterschiedliche Verkaufsregionen, Sparten- oder Kundengruppen. Die Provider/InfoCubes werden abgebildet in Datengruppierungen mit Attributen bzw. Merkmalen, die dann in den Queries ausgewählt werden können. InfoCubes sind somit die zentralen Objekte, auf denen Analysen basieren und einen aus Reportingsicht in sich geschlossenen Datenbestand beschreiben. Sie bestehen aus verschiedenen InfoObjects, die sich in Attribute/Merkmale, Kennzahlen, Einheiten usw. aufgliedern. Das InfoObject Geschäftspartner wird beispielsweise attributiert mit GP-Nummer, Vorname, Nachname, Adresse und Hausnummer, PLZ und Wohnort usw. InfoObjects als strukturierte Darstellung von zusammenhängenden Informationen sind die kleinsten Einheiten des BI/BW.

Wird nun beispielsweise ein InfoObject wie der Geschäftspartner um bestimmte Inhalte ergänzt, können alle hierauf fußenden Queries diese neuen Inhalte abfragen. Voraussetzung ist, dass ein Mapping zwischen Quell- (IS-U) und Zieldatenbestand (BI/BW) existiert. SAP BI/BW bietet eine Vielzahl von Standard-Datenquellen, die allerdings längst nicht alle IS-U-Datenfelder beinhalten. Entsprechend kann es vorkommen, dass Erweiterungen entwickelt werden müssen. Für die Revision und den Datenschutz ist es wichtig, InfoObjects (als kleinste vorhandene Einheit) zu identifizieren, die beispielsweise eine Referenz auf die IS-U-Felder der Tabelle DPAYH oder auf die Felder BUT0BK-BANKL, BUT0BK-BANKN und ggf. BUT0BK-KOINH (ggf. in Verbindung mit der Tabelle BUT000 - evtl. auch mit dem Feld Geburtsdatum BIRTHDT) aufweisen. Diese InfoObjects sollten nur restriktiv in den Queries Verwendung finden.

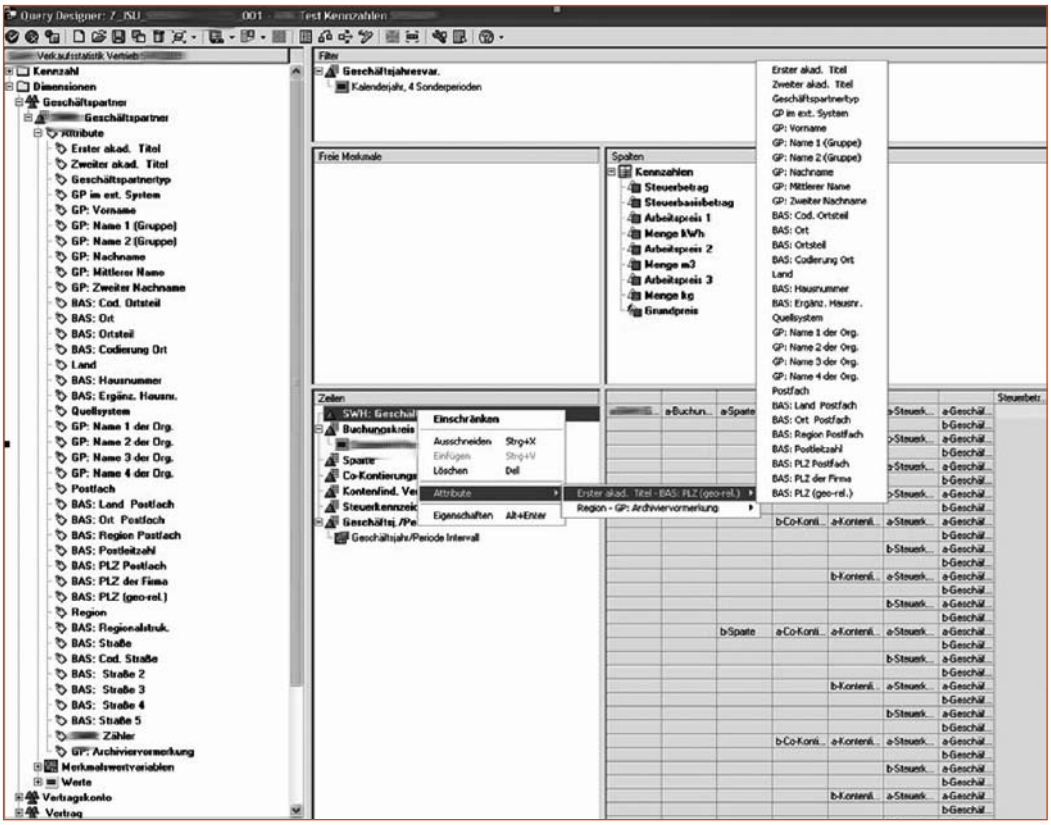

Abb. 2: Query-Designer mit Referenz zu InfoCube und Beispiel-InfoObject Geschäftspartner

Grundsätzlich sollte gelten, dass ausschließlich die Administration / Modulbetreuung Datencontainer modelliert und InfoObjects erweitert. Die Berechtigungen der Fachbereiche sollten wiederum so differenziert werden, dass nur ein zentraler Bereich als Dienstleister Queries anlegen und ändern kann, während alle anderen Bereiche Queries ausschließlich ausführen dürfen. Ggf. ist es sinnvoll, dass der Datenschutzbeauftragte informiert wird, wenn obige Tabellen in Erweiterungen einbezogen werden.

Download

SAP kann nur über die Ausprägung der Rollen im Berechtigungskonzept selbst, d.h. über das Gewähren oder Verwehren von Berechtigungen via Steuerungsfelder wie z.B. organisatorische Abgrenzungen, Aktivitäten und Gruppenzugehörigkeiten o.Ä. innerhalb der unterschiedlichen Rollen, Funktionen bereitstellen oder sie verhindern. Grundsätzlich gilt: Ist ein Benutzerstammsatz berechtigt, beispielsweise Inhalte aus tabellarischen Datendarstellungen (siehe ALV-Grid / List-Viewer) in Dateien auf den Rechner zu transferie-

ren, kann er dies aus den Auswertungen und Datendarstellungen heraus, die dies ermöglichen, durchführen. Es ist nicht möglich, bei vorhandener Zuweisung der Funktion diese zusätzlich an eine Bedingung zu knüpfen. Beispielsweise wäre es hilfreich, die Download-Funktion daran zu koppeln, dass sie in bestimmten unkritischen Auswertungen zur Verfügung steht, bei der direkten Tabelleneinsicht und besonders sensiblen Analysen aber nicht. Dies würde die Definition kritischer Inhalte und Funktionen mit gewisser Verbindlichkeit bzw. Allgemeingültigkeit und eine adäquate Erweiterung der Berechtigungssteuerung in SAP® voraussetzen.

Konsequenterweise ist hier nur eine nahezu vollständige Entziehung der Download-Berechtigung für eine große Anzahl von Arbeitsplätzen denkbar, was allerdings an den Erfordernissen des praktischen Einsatzes scheitert. Aber auch bei weit reichendem Entzug der Download-Berechtigung blieben genügend Arbeitsplätze und Benutzerstammsätze, die diese Funktion beinhalten (müssen).

Fazit

Die Berechtigungen in SAP IS-U sind aus praktischen Erwägungen heraus nur unzureichend in der Form eingrenzbar, wie dies aufgrund der sensiblen Daten notwendig ist. Selbst wenn die kritisch-manipulativen Sachbearbeitungsfunktionen in der Rollenverteilung begrenzt sind, womit zumindest eine gewisse Sicherheit einhergeht, dass Daten nicht unkontrolliert und ohne entsprechendes Fachwissen manipuliert werden, existieren doch Zugangswege und Datendarstellungen, die die grundlegenden Daten umfassend (im Sichtmodus) ohne aussagekräftige Protokollierung bereitstellen und zumeist auch mit Download-Funktion offerieren – wesentliche Pfade wurden aufgezeigt. Dies sind systembedingte Unzulänglichkeiten mit entsprechender Wirkung. Sie können nur durch Sensibilisierungen, regelmäßigen Analysen und (im Rahmen des „lebenden Berechtigungswesens“) Rollenreduktionen auf ein notwendiges Maß angegangen werden.

Inwieweit ein Unternehmen im Rahmen der Praxiserfordernis adäquat ausgestatteter und vernetzter Arbeitsplätze einer missbräuchlichen Nutzung effektiv entgegentreten kann, ist trotz zunehmender Öffentlichkeitswirkung fraglich. Es geht jedoch um das Bemühen, bei einem sich berechtigungsseitig stetig verändernden und mit anderen Systemen korrespondierenden IT-System Eingrenzungen vorzunehmen und den Risiken proaktiv zu begegnen. Dies gilt nachvollziehbar nicht nur für Produktivsysteme, sondern auch für Test-/Integrations-/Entwicklungs- und Migrationssysteme.

Beispielhafter Fragenkatalog

- Wer darf über SAP-Standardtabellentransaktionen auf die Tabellen der Kundenverwaltung incl. Bankverbindungen zugreifen (lesend oder manipulierend) ?
- Existieren im Kundennamensraum abgestufte Transaktionen, Reports oder ABAPs, die einen entsprechenden Zugriff ermöglichen ?
- Wer darf hierüber auf die Tabellen der Kundenverwaltung incl. Bankverbindungen zugreifen ?
- Wer darf über RFC auf die Tabellen der Kundenverwaltung incl. Bankverbindungen zugreifen ?

- Wer darf über definierte Views (Standard, Kundennamensraum) auf Inhalte der Kundenverwaltung incl. Bankverbindungen zugreifen ?
- Wer darf über Transaktionen, Reports oder ABAPs im Kundennamensraum in Listform auf die Kundenverwaltung incl. Bankverbindungen zugreifen ?
- Wer hat die Berechtigung zum Download im SAP IS-U ?
- Wer darf über die oben genannten Wege auf die Tabelle DPAYH zugreifen ?
- Wer hat die Berechtigung, über weitere Zugriffsmechanismen auf obige Inhalte Zugriff zu nehmen (SAP Queries o.Ä.) ?
- Wer darf in BI/BW InfoObjects mit Kundendaten – speziell mit Bankverbindungen – definieren oder anpassen ?
- Wer darf InfoCubes modellieren ?
- Wer darf Queries mit Bezug zu problematischen InfoCubes / InfoObjects anlegen ?
- Wer kann auf vorhandene Queries mit Inhalten der Kundenverwaltung incl. Bankverbindungen Zugriff nehmen ?
- Existieren Berechtigungseinschränkungen in BI/BW mit Bezug zu Kundenbankverbindungen ?

Literatur / Links:

SAPBIBWGLOSSAR: http://www.bi-co.de/knowhow/glossarbw/index.html

SAP IS-U-Berechtigungskonzept: http://www.auditplan-xp.de/veroeff.html

SAP IS-U-Tabellendarstellung: http://kkrumi.googlepages.com/isu_tables.ppt

SUEDBADEN2009: http://suedbaden.business-on.de/illegale-kontoabbuchungen-von-lotto-und-gewinnspielfirmen-sowie-untergeschobene-vertraege_id4531.html vom 22.04.2009.

WIWO2008: http://www.wiwo.de/unternehmen-maerkte/kontonummern-von-21-millionen-buergern-illegal-im-umlauf-380382/ vom 06.12.2008.

Dipl.-Betriebswirt **Christoph Wildensee**, CISM, ist seit 1994 als IV-Revisor bei der Stadtwerke Hannover AG (enercity), einem großen kommunalen Energiedienstleister mit beinahe 3 Mrd. EUR Umsatz (2009), tätig und verfügt somit über eine langjährige Erfahrung im Bereich der Revision. Er arbeitete 2001 und 2002 projektbezogen auch für die IBS-Gruppe aus Hamburg in der SAP-Beratung und ist Verfasser verschiedener Fachartikel – insbesondere zum Thema SAP-Prüfung. Seit 2008 ist er in Personalunion auch Datenschutzbeauftragter der Stadtwerke Hannover AG und mehrerer Beteiligungen. Mehr zu ihm: http://www.auditplan-xp.de/leben.html .