Gefährdung der Ordnungsmäßigkeit rechnungslegungsrelevanter SAP-Systeme durch irreguläre Quellcode-Transfers

Christoph Wildensee, DBA, CISM, CRISC [1]

Abstract

Es ist u.a. Aufgabe der Internen Revision, die Wirksamkeit der definierten Kontrollen in den eingesetzten rechnungslegungsrelevanten ERP-Systemen zu prüfen und möglichst zu bestätigen. Es droht der Verlust der Ordnungsmäßigkeit der Buchführung, wenn im IT-System Programme vorhanden sind, die es ermöglichen, dass nach Belieben sowohl Daten als auch Programmcode und Abrechnungslogik ohne Nachvollzug der Aktivitäten und Verursacher manipuliert werden können. Der nachfolgende Artikel stellt die Ergebnisse einer limitierten Untersuchung dar, in wie vielen Unternehmen in produktiven SAP-Systemen derartige Programme vorkommen und wer sie üblicherweise in die Umgebungen implementiert. Dieses Thema tangiert die Grenzen des Systemeinsatzes und kann bis zur Ordnungswidrigkeit des IT-Systemeinsatzes führen. Obwohl der deutsche Rechtsrahmen spezifisch ist, wird dieses Thema auch in anderen Ländern von Interesse sein, denn SAP ist ein über die Landesgrenze hinweg tätiges Unternehmen, dessen Produkte weltweit und konsolidierend im Einsatz sind. Es sollte gleichsam auch im Interesse von Wirtschaftsprüfungsunternehmen sein.

1. Einleitung

Das eingesetzte ERP-System beinhaltet alle notwendigen Daten, Programme, Prozessdefinitionen und Schnittstellen zur Abbildung der Geschäftstätigkeit des jeweiligen Unternehmens. Es werden auch Details der Steuerbemessung berücksichtigt. Solche IT-Systeme unterliegen der landesspezifischen Gesetzgebung zur Nachweisführung der Geschäftstätigkeit und der stichtagsbezogenen Bemessung des Erfolges und Unternehmenswertes. Eine Manipulation von Daten und Programmcode darf es dabei nur geben, wenn dies unter Beachtung der gesetzlichen Nachweispflichten erfolgt, also z.B. Änderungsbelege entstehen, temporale Datenabgrenzungen und Historisierungen durchgeführt werden, Versionsverwaltung betrieben wird usw. Nicht dokumentierte und irregulär stattfindende Manipulationen im IT-System gefährden die Integrität des Systems, des rollenbasierten Zugriffsschutzes und der so abgesicherten Business-Daten, so dass Vertrauen in die Aussagekraft der Daten, ggf. sogar in das Management selbst, verlorengehen kann. SAP offeriert Möglichkeiten der gesicherten Daten- und Programmmanipulation. Beschränkt sich die Eigenentwicklung auf diese Standardfunktionen, kann das Access Management funktional und gesetzeskonform ausgestaltet werden. SAP bietet auch Befehle, die in Quellcode eingefügt die Integrität wie zuvor beschrieben terminieren. Ein Programm aus nur wenigen Zeilen bestehend, wie es letztlich auch Kempf (2014, S. 14) beschreibt, kann ein rechnungslegungsrelevantes Produktionssystem vollständig destabilisieren.

[1] Verantwortet die IV-Revision mit Schwerpunkt SAP-Systemprüfung (Ordnungsmäßigkeit, Sicherheit) bei einem Energieversorger in Hannover (D).

2. Verlust der Daten- und Programmintegrität

Chuprunov (2013, S. 154) stellt fest: “As far as application security is concerned, the first important thing to understand is that the risk comes not from specific transactions but from special ABAP commands. […] From a technical perspective, ABAP code is not created through transactions SE38 and SE80 but by the command INSERT REPORT. However, this command neither performs an authorization check nor checks whether it is run on a live system. These checks do take place explicitly in the source code of the transactions SE38 and SE80.” Das Kommando „INSERT REPORT“ ist bereits seit geraumer Zeit als kritischer Befehl in SAP-Systemen in der Diskussion. Nicht erst Wiegenstein (2012, S. 12) und Kempf (2014, S. 14) haben die Problematik publiziert, zuletzt Wiegenstein (2014, S. 14) sogar für das „Bundesamt für Sicherheit in der Informationstechnik“ (BSI), Bonn. Bereits vor ihnen haben andere Fachautoren die Diskussion angeheizt, z.B. Vera (2008), Wulff (2009) und SAPITTOOLBOX (2003). SAP (2015) selbst hat zuletzt festgestellt, dass drei Befehle „als kritische ABAP-Anweisungen“ gelten: „INSERT REPORT“, „EDITOR-CALL“ und „GENERATE SUBROUTINE POOL.“ In 2009 wurden in einem ABAP-Tech-Blog “…two illegal methods to modify the system program…” von SDYUGUANG (2009) dargestellt, eine der Methoden entspricht der Kombination der ABAP-Befehle „INSERT REPORT“ und „EDITOR-CALL“ zur irregulären Anpassung des Systems. Hiermit ist es möglich, an definierten Implementations- / Transport- und Genehmigungswegen vorbei ohne Möglichkeit des Nachvollzugs der Aktivitäten, die mithilfe einer so gearteten Funktionalität angestoßen werden, und ohne dass weitere Entwicklerrechte vergeben sind, dynamisch Quellcode einzufügen.

Wenn unternehmensinterne SAP-Entwickler diese Möglichkeiten ausnutzen, obwohl im Unternehmen definierte Wege für den regulären Quellcodeimport vorhanden sind, ist folglich die Backdoor-Implementierung bei Kenntnis des Rechtsrahmens als arbeitsvertragliche Sorgfalts- und Obhutspflichtverletzung des Arbeitnehmers zu sehen. Der Arbeitgeber kann arbeitsrechtlich sanktionieren. Externe Entwickler sind häufig versierte Experten, ohne deren Fachwissen anspruchsvolle Projekte im Unternehmen nicht realisiert werden können. Tatsächlich ist es ambitioniert, dass eigene Entwickler in einem so dynamischen Umfeld versuchen, ihre Kompetenz umfassend und dauerhaft auf höchstem Niveau aufrecht zu erhalten. Es ist üblich, auftretende Know-how- und Kapazitätsdefizite durch qualifizierte externe Dienstleister ausgleichen zu lassen. Es liegt dann ein dezidierter Vertrag vor, der auf dem Handelsrecht beruht. Es ist davon auszugehen, dass Dienstleistungsunternehmen im IT-Umfeld die jeweils zentralen rechtlichen Grundlagen kennen und ihre Beschäftigten auf die Einhaltung verpflichten. Kempf (2014) zeigt, dass dieses Bewusstsein sehr wohl vorhanden ist.

3. Umfrage

Entsprechend kann die Frage gestellt werden, wie weit verbreitet Programme und sonstige Funktionalitäten wie zuvor dargestellt in SAP-Systemen sind? Ein vorweggenommenes Ergebnis ist die Erkenntnis, dass sicherheitskritische Programme in rechnungslegungsrelevanten SAP-Systemen durchaus zu finden sind. Sie werden sowohl durch interne SAP-Entwickler als auch durch Beschäftigte externer Dienstleister in die produktiven Umgebungen eingefügt. Der Verlust von Daten durch unzureichenden Schutz führt in Deutschland nach GOBD.7(103) und (104) ggf. zur Zuerkennung des Status‘ „**formell nicht mehr ordnungsmäßig**“. Werden Systemfunktionen oder **Manipulationsprogramme** nach GOBD.8(112) verwendet, die die Umsetzungen der Schutzanforderungen nach GOBD.8(111) terminieren bzw. diesen entgegenstehen, führt dies zur „**Ordnungswidrigkeit der elektronischen Bücher** […]“, GOBD (2014*) für steuerliche Veranlagungszeiträume ab 2015*.

Bereits die Möglichkeit der irregulären Nutzung ist hinsichtlich der Ordnungsmäßigkeit hinreichend bedenklich. Wie Thelen (2015, S. 142) feststellt, findet ein Unternehmen, aber auch der Wirtschaftsprüfer an dieser Stelle eine Eindeutigkeit vor, die bisher so klar nicht formuliert war.

Von März bis Juli 2015 wurden insgesamt **14** Revisionsabteilungen (Internal Audit Departments) aus Unternehmen der Energieversorgungsbranche in Deutschland, die SAP einsetzen, befragt, ob Programme oder Funktionen in produktiven SAP-Systemen (HCM, Core, IS-U) vorhanden sind (Analyse über SAP-Report AFX_CODE_SCANNER), die folgende Bedingungen erfüllen:

- ausführbares Programm (Typ 1) oder nutzbarer Funktionsbaustein oder nutzbare Methode oder anderes Objekt, aus ABAP-Programmen referenzierbar, Funktionalität bisher dort dauerhaft verbleibend (temporäre Programm-, FuBa-, Include-, Modulpool-, Methoden-Implementierungen sind nicht erfasst)
- Befehl „GENERATE SUBROUTINE POOL“ oder
- Befehl „INSERT REPORT“ oder
- „INSERT REPORT“ in Kombination mit dem Befehl “EDITOR-CALL”.

Der geringe Umfang der Teilnehmerzahl als Grundgesamtheit ist geschuldet an die Erwartung, dass aufgrund des vorhandenen und zuletzt konkretisierten Rechtsrahmens nur wenige bis keine Trefferzahlen erreicht werden. Es lässt sich in Umfragen kaum verhindern, dass befragte Unternehmen trotz Anonymitätszusagen keine verwertbaren Angaben bereitstellen. Der Autor hat ihm namentlich bekannte Ansprechpartner aus Revisionsabteilungen der Energieversorgungsbranche ausgewählt. Eine persönliche Ansprache erhöht üblicherweise die Rücklaufquote. Befragt wurden mittelgroße bis große Unternehmen mit in 2014 im gestutzten Mittel ca. 2.760 Beschäftigten im Konzernverbund (Gas- und / oder Stromversorger, auch Wasser, Wärme, vereinzelt sogar mit öffentlichem Nahverkehr, Bäderbetrieb, Entsorgung, Telekommunikationsbereitstellung), bei denen mit SAP die Kernprozesse abgebildet und unterstützt werden. Dabei ist relevant, ob in einem der SAP-Systeme ein Treffer vorhanden ist, nicht in wie vielen Systemen. Von den 14 angefragten Revisionsabteilungen haben sich **12** an der Umfrage beteiligt (Rücklaufquote 86%).

Es wurden Elemente in SAP IS-U-Systemen in **sieben** der **12 Unternehmen (58%)** gefunden.

4. Ergebnisse der Analyse

Es kann anhand des Ergebnisses festgestellt werden, dass es ein Problem in den Unternehmen gibt: Kritische Objekte sind gängig in den Systemen vorhanden und sie werden sowohl durch interne als auch externe Fachkräfte eingeschleust.

Folgende zusammenfassende Ergebnisse können dargestellt werden:

	Σ	INSERT REPORT	EDITOR-CALL	GENERATE SUBROUTINE POOL	TYP 1 kritisch	FuBa	INCLUDE oder Modul Pool	Methode
Mit Ergebnis	7	7	5	1	6	1	3	2
Ohne Fund	5	(Kein Fund [oder ohne Interesse oder Möglichkeit an einer Identifizierung. Dies ist nicht verifizierbar.])						
Gesamt	**12**							

Details ID	Quelle	INSERT REPORT	EDITOR-CALL	GENERATE SUBROUTINE POOL	TYP 1 kritisch	FuBa	INCLUDE oder Modul Pool	Methode
@E 1	intern	X	X		X			
@E 2	extern	X	X		X		X	
@E 3	intern	X*[1]		X	X			X
@E 4	extern	X*[2]	X*[2]			X	X	X
@E 5	extern	X	X		X			
@E 6	extern	X	X		X		X	
@E 7	nicht ermittelbar	X*[1]			X			
Σ		**7**	**5**	**1**	**6**	**1**	**3**	**2**

[x[1] : Upload aus Datei; x[2] :„INSERT REPORT“ und „EDITOR-CALL“ nicht gemeinsam in einem ABAP-Code. Somit vier Unternehmen mit dieser Kombination.]

Tabelle 1: Details der Untersuchung.

Es ist möglich, analog bereits SAPFANS (2003), per „INSERT REPORT“ in Kombination mit dem File-Upload von Code in eine interne SAP-Tabelle Programme in das System einzufügen. Diese kritische Kombination wurde in der Untersuchung zweifach vorgefunden (E3, E7). Als besonders kritisch gelten Programme, die eine Kombination aus „INSERT REPORT“ und „EDITOR-CALL“ aufweisen. Diese wurde vierfach vorgefunden (E1, E2, E5, E6). Gesicherte Erkenntnis ist, dass in zwei Fällen SAP-Betreuer des Unternehmens die Objekte in die Produktivumgebung einbrachten, und in drei Fällen Entwickler von externen Unternehmen diejenigen waren, die als Entwickler / technischer Integrator die Objekte einschleusten. Es gibt folglich in **sechs** Unternehmen (E1-E3, E5-E7) kritische (zumeist sy-uname-aufrufbeschränkte) ausführbare Programme, wobei in **drei** Unternehmen die externe Unterstützung Auslöser war. In einem Fall konnte der Verursacher nicht mehr festgestellt werden. Auch der siebente Fall (E4) ist im kritischen Bereich zu sehen, wird hier doch ein durch externe Unterstützung bereitgestellter – wenn auch wie häufig üblich über sy-uname aufrufbeschränkter – Funktionsbaustein im Kundennamensraum mit „INSERT REPORT“ offeriert. Er kann z.B. über Transaktion SE37 (Testmodus ausreichend) von diesen Personen genutzt oder von diesen in Programme eingefügt werden. Insoweit beträgt die **durch Externe** verursachte Implementierungsquote kritischen Codes in diesen sieben Fällen belegt **57%**. Der Nachweis, welche Aktivitäten durch wen mit den jeweiligen Programmen / Funktionen ausgeführt wurden, konnte in keinem Fall erbracht werden.

5. Zusammenfassung

Wenn Experten externer Dienstleister neue Objekte anlegen oder ändern, also Entwicklung betreiben, sollten auch für sie die Beschränkungen gelten, die für die eigenen Entwickler bestehen und die Tiede (2014, S. 644) wie folgt erläutert: „Das Durchführen von Transporten darf nicht in der Hand derjenigen liegen, die im Entwicklungssystem entwickeln oder Customizing-Einstellungen vornehmen. Transporte sind der Administration vorbehalten.“ Diese strikte Aufgabentrennung impliziert, dass die Entwickler – auch die externe Unterstützung – keine Entwickler-

schlüssel im Produktionssystem aufweisen. Tiede (2014, S. 591) stellt fest: „Anwendungsentwicklung wird ausschließlich im Entwicklungssystem durchgeführt.“ Es ist nicht zu erwarten, dass SAP die beschriebenen Möglichkeiten des Befehls „INSERT REPORT“ in selbsterstellten Programmen einschränkt. Entsprechend müssen die Ergebnisse von Eigenentwicklungen vor dem Transport in die Produktivumgebung vollumfänglich auf Verwendung problematischen Codes untersucht werden, denn andernfalls würde blindes Vertrauen gegenüber den Entwicklern dazu führen, dass die Kontrollfunktion versagt. In einem Produktionssystem dürfen keine Manipulationsmöglichkeiten bestehen, die undokumentiert Daten oder Programmlogik manipulieren können. Daten, Source Code und Abrechnungslogik dürfen keiner nachweislosen Manipulation unterworfen sein.

In einer nicht repräsentativen Umfrage wurde festgestellt, dass es neben Entwicklern des eigenen Hauses auch solche externer Unternehmen gibt, die den Ruf des Dienstleisters dadurch schädigen, dass sie durch Implementieren von kritischem Code, der die definierten Genehmigungs- und Transportwege beim Kunden ohne Nachweisführung für Quellcode umgeht, die Ordnungsmäßigkeit des IT-Systems negativ beeinträchtigen. Eine Erweiterung der Datenbasis ist zumindest an dieser Stelle nicht notwendig, um trotz der zu geringen Datenbasis für allgemeingültige Aussagen plausibel zu erkennen, dass Unternehmen im Bereich möglicher Programm-, Logik- und Datenmanipulationen Angriffspunkte bieten und dass das Vertrauen in externe Unterstützung trotz ggf. erfolgreicher Projektumsetzungen nicht immer gerechtfertigt ist. Über die Motivlage der Personen, die irregulär Funktionalität implementieren, kann nur spekuliert werden. Dies wäre ein wichtiger weiterer Untersuchungsgegenstand. Einen vorsätzlichen Import von Instrumenten zur Wirtschaftsspionage / Sabotage sollte man nicht unterstellen, doch beinhaltet ein solcher Code-Transfer zumindest auch diese Möglichkeit. Die dargestellte Problematik ist m.E. keine zu vernachlässigende Randerscheinung.

Aus Sicht des Unternehmens wird der Wirtschaftsprüfer im schlimmsten Fall auf solche Code-Konstrukte aufmerksam. Dies kann folgend zu von der Geschäftsleitung unerwünschten und öffentlichkeitswirksamen Testat-Formulierungen führen. Entsprechend sollten sich zum Schutz der Unternehmensdaten und Infrastruktur zumindest die Unternehmensbereiche Finanz- und Rechnungswesen, SAP-Entwicklung und Interne Revision gemeinsam einem unsachgemäßen Fahren der produktiven rechnungslegungsrelevanten SAP ERP-Systeme entgegenstellen.

Notwendig sind neben Schulungen der eigenen Entwicklerteams zu den Security- und Rechtsgrundlagen verpflichtende Vorgaben für das Vertragswerk bei Entwicklungsausschreibungen (verbindliche Programmierrichtlinie für interne und externe Entwickler) und regelmäßig wiederkehrende Kontrollen im Bereich der Eigenentwicklungen und von SAP-Fremdobjekten, z.B. per Transaktion CODE_SCANNER und dem Code-Inspector (Transaktion SCI). Wirtschaftsprüfer wiederum sollten dies zum Anlass nehmen, im Rahmen der Jahresabschluss-IT-Vorprüfung die dargestellten Inhalte in allen hier relevanten SAP-Produktivsystemen zu überprüfen.

Literatur

CHUPRUNOV (2013), Auditing and GRC Automation in SAP, Berlin, Heidelberg 2013.

GOBD (2014), Schreiben des Bundesministeriums der Finanzen vom 14.11.2014, IV A 4 - S 0316/13/10003, http://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/Datenzugriff_GDPdU/2014-11-14-GoBD.pdf?__blob=publicationFile&v=1 .

GOBS (1995), Schreiben des Bundesministeriums der Finanzen vom 7.11.1995, IV A 8 - S 0316 - 52/95 - BStBl 1995 I S. 738, http://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Betriebspruefung/ 015.pdf?__blob=publicationFile&v=3 .

GDPDU (2001), Schreiben des Bundesministeriums der Finanzen vom 16.7.2001, IV D 2 - S 0316 - 136/01 - BStBl I S. 415, http://www.baron-consult.de/Archiv/GDPdU.pdf .

GDPDU (2012), Änderung des BMF-Schreibens „Grundsätze zum Datenzugriff und zur Prüfung digitaler Unterlagen (GDPdU)“ IV A4 - S 0316/12/10001, http://www.cdh.de/user/eesy.de/cdh.de/dwn/bmf_13_datenzugriff.pdf .

KEMPF (2014), SAP Systeme absichern: Gut gemeint ist nicht gut gemacht, http://www.akquinet.de/SAP/Flyer-Praesentationen/Vortrag_DSAG_2014_Gut_gemeint_ist_nicht_gut_gemacht.pdf .

SDYUGUANG (2009), ABAP two illegal methods to modify the system program…, http://www.cprogramdevelop.com/4949209/ .

SAP (2015), CHAPBC_0CRTABAP - CHAPBC 0CRTABAP, ABAP Short Reference, https://www.consolut.com/s/sap-ides-zugriff/d/e/doc/YX-CHAPBC_0CRTABAP .

SAPFANS (2003), http://www.sapfans.com/forums/viewtopic.php?f=13&t=79176&start=0 ; smurf 25.11.2003 .

SAPITTOOLBOX (2003), Blog, http://sap.ittoolbox.com/groups/technical-functional/sap-dev/function-module-that-creates-an-abap-program-222024 .

THELEN (2015), GoBD - Die Büchse der Pandora? in: PRev Revisionspraxis, 3/2015, S. 140-144.

TIEDE (2014), SAP R/3 - Ordnungsmäßigkeit und Prüfung des SAP-Systems (OPSAP), 3. Auflage, Hamburg 2014.

VERA (2008), Blog, Edit program in PROD/QA, http://myabapdocumentation.blogspot.de/2008/10/edit-program-in-prod-qa.html .

WIEGENSTEIN (2012), (3)…(2)…(1)…(SAP_ALL), Vortrag auf der Jahresfachtagung 2012 der IBS Schreiber GmbH, September 2012, https://www.virtualforge.com/tl_files/web/content/archiv-public/20120913_Praesentation_3_2_1_SAP_ALL_Wiegenstein_Jia.pdf .

WIEGENSTEIN (2014), Top 20 Sicherheitsrisiken in ABAP Anwendungen, Detail-Level-Ausarbeitung, Version 0.5, Oktober 2014, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Extern/TOP-20_Sicherheitsrisiken-in-ABAP-Anwendungen.pdf?__blob=publicationFile .

WULFF (2009), Includes / Programme generieren, http://www.tricktresor.de/blog/includes-programme-generieren/ .

Abkürzungen

ABAP	Advances Business Application Programming (proprietäre Programmiersprache von SAP)
ERP	Enterprise Resource Planning
FuBa	Funktionsbaustein
GOBD	„Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff“
HCM	Human Capital Management
IS-U	Industrial Solution - Utilities

Autor

Dipl.-Betriebswirt Christoph Wildensee, DBA, CISM, CRISC, ist seit 1993 als IV-Revisor bei der Stadtwerke Hannover AG (SWH) tätig. Zusätzlich war er von 2008 bis 2012 auch Datenschutzbeauftragter der SWH und der entsprechenden Netzgesellschaft.