Ein Maßnahmenkatalog für die Datensicherheit in der ERP Anwendungsentwicklung am Beispiel von SAP ERP

Holger Wittges, Sonja Hecht, Helmut Krcmar

Lehrstuhl für Wirtschaftsinformatik,
Technische Universität München

1 Einleitung

Durch die Etablierung von Enterprise Resource Planning (ERP) Systemen können Unternehmensdaten aus verschiedenen internen und externen Quellen integriert, korreliert und ausgewertet werden. Dadurch steigen die Möglichkeiten zur Nutzung der Daten, zugleich aber auch die Gefahr des Datenmissbrauchs. Vor diesem Hintergrund ist das Management von Unternehmen gefordert, Sicherheitskonzepte zu entwickeln und umzusetzen, um sensible Unternehmensdaten vor einem unberechtigten Zugriff durch Dritte zu schützen. Hierbei sollten insbesondere auch die Gefahren aus dem Inneren des Unternehmens berücksichtigt werden. Gerade bei schwerwiegenden Fällen von Datendiebstahl sind häufig Mitarbeiter oder Partner des betroffenen Unternehmens in den Datendiebstahl verwickelt. Prominente Beispiele sind die Liechtenstein-Affäre, ausgelöst durch den Verkauf von gestohlenen Kundendaten durch einen ehemaligen Mitarbeiter einer Tochtergesellschaft der betroffenen LGT Bank (Financial Times Deutschland 2009), oder der Datenskandal bei T-Mobil, ausgelöst durch das Ausspähen von Verbindungsdaten durch Mitarbeiter der Sicherheitsabteilung (Louven 2008).

Gemessen an der Anzahl der Angriffe überwiegen in den letzten Jahren zwar die Angriffe von außen (Baker et al. 2008, S. 9-10; Richardson 2008, S. 14), jedoch entsteht durch Angriffe aus dem Inneren ein wesentlich größerer Schaden. In einer von Verisign durchgeführten Studie (Baker et al. 2008, S. 10-13) waren in 73 % der Fälle Angreifer außerhalb des Unternehmens beteiligt, gemessen an der Anzahl der entwendeten Datensätze war der Schaden durch Angriffe aus dem Inneren der Organisation sowie durch Partner aber fast 19 mal größer. Bei den Angriffen aus dem Inneren oder durch Partner ging ein wesentlicher Anteil der Angriffe direkt von Personen aus, die mit der Administration von IT-Lösungen betraut waren. Ein Angriff von dieser Personengruppe kann aufgrund deren Zugriffsmöglichkeiten

sowie deren Wissen über die Schwachstellen der Informationssysteme zu schwerwiegenden Schäden führen (Magklaras und Furnell 2002, S. 64-65).

Aufgrund der geschilderten Entwicklungen fokussiert sich dieser Beitrag auf Sicherheitsaspekte im Rahmen der Anwendungsentwicklung für ERP Systeme. Während für ERP Systeme der unberechtigte Datenzugriff durch Endanwender durch ein Rollenkonzept weitgehend unterbunden werden kann, sind die Datenzugriffsmöglichkeiten für die Personengruppe der Anwendungsentwickler aufgrund ihres Aufgabenspektrums häufig weit gefasst.

Ziel dieses Beitrags ist, Schwachstellen in der Datensicherheit für die ERP Anwendungsentwicklung zu identifizieren und einen umfassenden Maßnahmenkatalog zu entwickeln, um einen unberechtigten Datenzugriff durch die Personengruppe der Anwendungsentwickler so weit wie möglich zu unterbinden.

Der Beitrag gliedert sich hierbei wie folgt: Zuerst werden hierfür geeignete Maßnahmen aus dem IT-Grundschutz Maßnahmenkatalog des Bundesamt für Sicherheit in der Informationstechnik (BSI 2008) identifiziert. Diese Maßnahmen werden im Rahmen eines Fallbeispiels auf deren Anwendbarkeit im praktischen Einsatz untersucht. Abschließend wird ein Maßnahmenkatalog für die Datensicherheit in der ERP Anwendungsentwicklung vorgeschlagen, der die Maßnahmen des IT-Grundschutz aufgreift, weiter detailliert und ergänzt.

2 Die IT-Grundschutz-Kataloge

Die IT-Grundschutz-Kataloge empfehlen Sicherheitsmaßnahmen für typische Geschäftsprozesse, Anwendungen und IT-Systeme. Die vorgeschlagenen Maßnahmen decken hierbei organisatorische, personelle, infrastrukturelle als auch technische Aspekte ab (BSI 2008, S. 14). Im Rahmen des IT-Grundschutz werden auch IT-Sicherheitsaspekte für ERP Systeme am Beispiel von Systemen des Anbieters SAP AG betrachtet. Um einen Überblick über vorhandene Maßnahmen in diesem Bereich zu schaffen, werden in
Tabelle 1 IT-Grundschutz Maßnahmen für den IT-Grundschutz Baustein *SAP Systeme* betrachtet, die im Rahmen der ERP Anwendungsentwicklung eingesetzt werden können, um das Risiko eines unberechtigten Datenzugriffs durch die betrachtete Personengruppe der Anwendungsentwickler zu verringern. Es werden hierbei Maßnahmen betrachtet, die in diesem Zusammenhang geeignet erscheinen oder direkt für diesen Kontext empfohlen werden.

Tabelle 1: Maßnahmen für die Sicherheit in der ERP Anwendungsentwicklung am Beispiel von SAP Systemen

Maßnahme	Behandelte Aspekte
M 2.341 Planung des SAP Einsatzes	Benutzerverwaltung/Berechtigungskonzept Planung der SAP Systemlandschaft Audit- und Logging-Konzept Änderungsmanagement-Konzept
M 2.347 Sicherheitsprüfung für SAP Systeme	Auswertung des Security Audit Logs Regelmäßige Prüfung von Benutzerrechten auf kritische Berechtigungen
M 2.349 Sicherheit bei der Software-Entwicklung für SAP Systeme	Berechtigungskonzept für Anwendungsentwickler Berechtigungsprüfung für erstellte Programme Einspielen von Software unter Einsatz eines mehrstufigen Software-Freigabe-Konzepts
M 4.262 Konfiguration zusätzlicher SAP Berechtigungsprüfungen	Sperren von Transaktionen für die Ausführung beliebiger Programme Bereitstellung von Programmen ausschließlich über Transaktionscodes
M 4.270 SAP Protokollierung	Einschränkung des Zugriffs auf Protokolldaten Protokollierung kritischer oder schwerwiegender Systemereignisse
M 4.272 Sichere Nutzung des SAP Transportsystems	Einschränkung des Zugriffs auf das SAP Transportsystem durch Entwickler

Aus Tabelle 1 wird ersichtlich, dass die IT-Grundschutz-Kataloge bereits ein breites Spektrum an Maßnahmen anbieten. Anhand des folgenden Fallbeispiels soll nun betrachtet werden, wie diese Maßnahmen in der Praxis in ERP Systemen umgesetzt werden können und welche Schwierigkeiten sich im Rahmen der Umsetzung ergeben.

3 Fallbeispiel SAP ERP Entwicklung

Da in den Maßnahmenkatalogen des IT-Grundschutz die Systeme der SAP AG exemplarisch für die Beschreibung von Maßnahmen verwendet wurden und diese eine hohe Verbreitung haben, nutzt das folgende Fallbespiel mit SAP ERP ebenfalls ein System der SAP AG. Das ERP System SAP ERP unterstützt Prozesse in den Bereichen Finanzwesen, Personalwirtschaft, Logistik und Corporate Services und nutzt als technologische Plattform den SAP Netweaver Application Server.
Anhand des Fallbeispiels soll untersucht werden, wie Maßnahmen für die Datensicherheit in der ERP Anwendungsentwicklung umgesetzt werden können und welche Schwierigkeiten in der Umsetzung auftreten können. Der Vergleich der Sicherheitskonzepte von SAP ERP mit den Sicherheitskonzepten anderer ERP Systeme ist nicht Teil dieses Beitrags.

Im Folgenden werden zuerst grundlegende Aspekte der Authentifizierung und Autorisierung für die Entwicklung und Ausführung von Programmen in SAP ERP und beleuchtet. Darauf folgt ein Überblick über die Gestaltungsmöglichkeiten der Systemlandschaft und deren Rolle für die Datensicherheit bei der Entwicklung und Anpassung von Programmen des ERP Systems. Abschließend werden die IT-Grundschutz Maßnahmen für die Datensicherheit in der ERP Anwendungsentwicklung unter dem Aspekt der Praktikabilität kritisch betrachtet und mögliche Sicherheitslücken in der praktischen Umsetzung identifiziert.

3.1 Authentifizierung und Autorisierung in SAP ERP

Für den Zugriff auf ein SAP ERP System und dessen Programme und Datenobjekte ist eine Authentifizierung und Autorisierung des Benutzers erforderlich. Die Authentifizierung des Benutzers erfolgt durch die Eingabe von Mandant ID, Benutzer ID und Passwort bei der Anmeldung am System. Die Prüfung der Autorisierung des Benutzers hingegen erfolgt auf Basis der dem Benutzer zugeordneten Rollen in den jeweiligen Anwendungsprogrammen. Auf Ebene der Datenbank erfolgt keine benutzerindividuelle Autorisierungsprüfung, da für alle SQL Zugriffe derselbe Standardbenutzer verwendet wird (Bögelsack et al. 2008, S. 58). Hat ein Benutzer selbst Entwicklerberechtigungen, kann dieser eigene Anwendungsprogramme anlegen, ohne zwingend eine Autorisierungsprüfung in diesen Programmen zu implementieren. Somit hat dieser Benutzer Zugriff auf alle Tabellen eines SAP Systems.

3.2 Systemlandschaft

In der Regel setzt ein Unternehmen eine mehrstufige Systemlandschaft für ERP Systeme ein, wobei verschiedene Systeme unterschiedliche Aufgaben abdecken. Die SAP AG (2005, S. 57-59) schlägt hier eine 3-stufige Systemlandschaft vor. In dieser idealtypischen Systemlandschaft werden sämtliche Entwicklungen in einem

Entwicklungssystem durchgeführt, das keine Echtdaten enthält. Nach Fertigstellung werden die neu entwickelten Objekte in ein Transportverzeichnis exportiert und von dort aus in das *Qualitätssicherungssystem* importiert. Der Import kann hierbei automatisch erfolgen. Das Qualitätssicherungssystem dient der Durchführung von Tests im Rahmen der Qualitätssicherung. Falls produktive Daten für diese Tests erforderlich sind, kann eine Datenkopie aus dem *Produktivsystem* in das Qualitätssicherungssystem eingespielt werden. Nachdem der Test mit Erfolg durchgeführt wurde, werden die Objekte manuell durch einen Systemadministrator in das Produktivsystem importiert. Der Export und Import von Entwicklungsobjekten wird als *Transport* bezeichnet und durch das *Transportsystem* gesteuert.

3.3 Sicherheitsmaßnahmen im praktischen Einsatz

Aus der Tätigkeit der Autoren in verschiedenen SAP Projekten hat sich gezeigt, dass Unternehmen die Empfehlungen des IT-Grundschutz zur Datensicherheit grundsätzlich umsetzen möchten, eine Umsetzung aller vorgeschlagenen Maßnahmen jedoch häufig nicht praktikabel ist, was folgende Beispiele verdeutlichen:

a) Nach IT-Grundschutz Maßnahmen M 2.341 sowie M 2.349 soll eine *Aufgabentrennung bei der Durchführung von Transporten* realisiert werden, es dürfen keine direkten Transporte durch Entwickler von dem Entwicklungssystem in das Qualitätssicherungs- oder Produktivsystem möglich sein. In der Praxis ist eine strikte Aufgabentrennung zwischen Entwicklung, Transport und Test von Anwendungen jedoch oft nur unter erheblichem personellem Aufwand möglich.

b) Nach IT-Grundschutz Maßnahme M 2.341 sollten *produktive Daten nicht unverändert in das Qualitätssicherungssystem übernommen werden*, falls die Vertraulichkeit der Daten in diesem System nicht gewährleistet werden kann. Für technische Programmtests sind jedoch häufig realitätsnahe Daten erforderlich, um alle Datenkonstellationen überprüfen zu können. Bestätigt wird diese Annahme durch eine Studie von Freeform Dynamics (Atherton et al. 2008, S. 3). Entsprechend dieser Studie nutzen über 70 % der befragten Unternehmen produktive Daten für Softwaretests, davon knapp ein Drittel in unveränderter Form.

c) Nach IT-Grundschutz Maßnahme M 2.349 sind Eigenentwicklungen immer mit einer Berechtigungsprüfung auszustatten. Durch Dritte entwickelte Software sollte einem *Abnahmeprozess* unterliegen, der insbesondere auch die *Erfüllung von im vorab definierten Sicherheitsanforderungen prüft.* Auch diese Forderung kann in der Praxis gerade bei kleineren Unternehmen häufig nicht voll umgesetzt werden, da die Qualitätssicherung von Programmen hinsichtlich Sicherheitsaspekte zeitintensiv ist und spezielles Fachwissen von einer unabhängigen Person erfordert.

d) Nach IT-Grundschutz Maßnahme M 2.349 wird empfohlen, den *Zugang zum Produktivsystem für Entwickler* so weit wie möglich zu sperren. Dies ist in der Praxis oftmals nicht realisierbar, z. B. wenn der Entwickler Programmfehler analysieren muss, die nur in der produktiven Umgebung auftreten.

Für die identifizierten Schwachstellen in der Umsetzung von Sicherheitsmaßnahmen wurde analysiert, (1) ob diese für alle Systemtypen zutreffen, und (2) ob diese Abhängigkeiten zu anderen Schwachstellen aufweisen, welche die Gefahr des unberechtigten Datenzugriffs erhöhen oder verringern. Tabelle 2 zeigt die Analyse beispielhaft für Schwachstelle *Transport durch Entwickler*.

Tabelle 2: Analyse von Schwachstelle *Transport durch Entwickler*

Schwachstelle	(1) Systemtyp	(2) Abhängigkeit zu anderen Schwachstellen
Transport durch Entwickler	Qualitätssicherung	- Gefahr nur dann vorhanden, wenn reale Daten im Qualitätssicherungssystem - Gefahr steigt, wenn keine Qualitätssicherung der Programme
	Produktiv	- Gefahr steigt, wenn keine Qualitätssicherung der Programme

Ergebnisse der Analyse zeigen, dass die Gefahr, die von einer bestimmten Schwachstelle ausgeht, sowohl vom Systemtyp als auch von der Existenz weiterer Sicherheitsmaßnahmen abhängt. Zugleich bedeutet dies auch, dass eine Gefahr durch bestehende Schwachstellen durch weitere Maßnahmen abgemildert werden kann. Hier wird der Bedarf nach einem Maßnahmenkatalog deutlich, der bei der Wahl alternativer Maßnahmen unterstützt und Unternehmen ein breites Maßnahmenspektrum aufzeigt.

4 Maßnahmen für die Datensicherheit in der ERP Anwendungsentwicklung

Ziel des zu entwickelnden Maßnahmenkatalogs ist, Maßnahmen für die Datensicherheit in der ERP Anwendungsentwicklung aufzuzeigen, zu strukturieren und bezüglich ihrer Umsetzbarkeit in ERP Systemen zu bewerten. Der Maßnahmenkatalog kann als Grundlage für die Entwicklung und die Analyse von Sicherheitskonzepten für die ERP Anwendungsentwicklung herangezogen werden.

4.1 Literaturreview

Um ein möglichst breites Spektrum an Maßnahmen aufzuzeigen, wurden im ersten Schritt auf Basis eines Literaturreviews geeignete Theorien für die Ableitung und Strukturierung von Maßnahmen zur Reduzierung von IT-Sicherheitsrisiken aus dem Inneren identifiziert, die hier kurz vorgestellt werden.

Die *General Deterrence Theory* basiert auf der abschreckenden Wirkung von Sanktionen, um kriminelle Aktionen zu verhindern. Entsprechend dieser Theorie werden potentielle Angreifer in der Durchführung krimineller Aktionen gehindert, wenn das Risiko ertappt zu werden hoch ist und mit schweren Sanktionen verbunden ist (Straub 1990, S. 258). Basierend auf dieser Theorie können nach Straub und Welke (1998, S. 445) Maßnahmen zur Reduzierung von IT-Sicherheitsrisiken den vier sequenziell aufeinander folgenden Aktivitäten *Abschreckung* (Deterrence), *Prävention* (Prevention), *Entdeckung* (Detection) und *Behebung/Bestrafung* (Remedies) zugeordnet werden. Für eine Operationalisierung dieser Aktivitäten durch konkrete Maßnahmen liefert die Literatur eine Fülle von Hinweisen: Eine abschreckende Wirkung haben bspw. eine offene Kommunikation und Bestrafung von kriminellen Handlungen, Investitionen in Sicherheitssysteme, Verschwiegenheitserklärungen und Richtlinien für die Systemnutzung (Lee und Lee 2002, S. 60; Straub 1990, S. 272-273; Straub und Welke 1998, S. 445). Zu den präventiven Maßnahmen zählen u.a. eine physische Zugriffskontrolle von Serverräumen, eine logische Zugriffskontrolle (Straub und Welke 1998, S. 445) und eine Aufgabentrennung in sicherheitskritischen Bereichen (Theoharidou et al. 2005, S. 479). Maßnahmen zur Entdeckung von Angriffen fokussieren sich vor allem auf eine Auswertung von Logdateien (Straub und Welke 1998, S. 446). Nachdem der Angreifer identifiziert wurde ist eine Bestrafung des Angreifers, z.B. durch Entlassung oder Anzeige, erforderlich, was einen abschwächenden Effekt auf zukünftige kriminelle Handlungen hat (Straub und Welke 1998, S. 446).

Neben kriminologischen Theorien können jedoch auch Theorien aus den Sozialwissenschaften genutzt werden, um ein kriminelles Verhalten von Mitarbeiter wie z.B. Datendiebstahl zu erklären und entsprechende Maßnahmen abzuleiten, um diese Handlungen zu vermeiden (Lee und Lee 2002, S. 57-58; Theoharidou et al. 2005, S. 475-476). Nach der *Social Bond Theory* sind beispielsweise Personen mit schwach ausgeprägten sozialen Beziehungen eher gefährdet, kriminelle Aktionen durchzuführen, als Personen mit einem stabilen sozialen Umfeld (Theoharidou et al. 2005, S. 475). Die *Social Learning Theory* nimmt an, dass die Möglichkeit einer kriminellen Handlung durch eine Person zunimmt, wenn diese Kontakt zu anderen Personen mit kriminellem Verhalten hat (Lee und Lee 2002, S. 59).

4.2 Maßnahmenkatalog

Aufbauend auf dieser Theoriebasis ist der Maßnahmenkatalog entsprechend der folgenden fünf Kategorien strukturiert:

- Kategorie 1: Abschreckende Maßnahmen
- Kategorie 2: Präventive Maßnahmen
- Kategorie 3: Maßnahmen zur Aufdeckung von Angriffen
- Kategorie 4: Maßnahmen zur Behebung/Bestrafung
- Kategorie 5: Maßnahmen in Personalmanagement und –führung

Tabelle 3: Überblick Maßnahmenkatalog

Maßnahme	Im IT Grundschutz		Umsetzung der Maßnahme in SAP ERP (3)
	thematisiert (1)	Empfehlungen zur Umsetzung (2)	
Kategorie 1: Abschreckende Maßnahmen			
Sicherheitsvorgaben für die Systemnutzung	Ja	●	Nicht Teil der Untersuchung
Vertraulichkeitsvereinbarung für Anwendungsentwickler	Ja	●	
Kategorie 2: Präventive Maßnahmen			
Logische Zugriffskontrolle für die Systemnutzung	Ja	◔	●
Aufgabentrennung bei Transporten/Qualitätssicherung	Ja	◔	●
Betrieb von mehreren ERP Systemen	Nein	○	●
Verschlüsselung von sensiblen Daten	Nein	○	◔
Anonymisierung von Testdaten	Nein	○	◔
Kategorie 3: Maßnahmen zu Aufdeckung von Angriffen			
Audit- / Logging-Konzept	Ja	◐	◐
Kategorie 4: Maßnahmen zur Behebung/Bestrafung			
Bestrafung / Kommunikation	Nein	○	Nicht Teil der Untersuchung
Kategorie 5: Maßnahmen in Personalmanagement und -führung			
Einhaltung von Gesetzen, Vorschriften, Regelungen	Ja	●	Nicht Teil der Untersuchung
Positive Gestaltung des Betriebsklimas	Ja	●	
Anlaufstelle bei persönlichen Problemen	Ja	●	
Sicherheitsüberprüfung von Mitarbeitern	Ja	●	

Tabelle 4: Legende zur Bewertung des Maßnahmenkatalogs

Bewertung	Empfehlungen zur Umsetzung im IT-Grundschutz	Umsetzung der Maßnahme in SAP ERP
	Umfangreiche Empfehlungen	Voll unterstützt, umfangreiche Gestaltungsmöglichkeiten
	Umfangreiche Empfehlungen, die aber eine Konkretisierung erfordern	Voll unterstützt, durchschnittliche Gestaltungsmöglichkeiten
	Empfehlungen enthalten, aber wesentliche Ergänzungen erforderlich	Unterstützt, aber weitere Funktionen wünschenswert
	Empfehlungen ansatzweise enthalten	Umsetzung nur in Teilbereichen/ durch Eigenentwicklung möglich
	Keine Empfehlungen enthalten	Keine Umsetzung möglich

Als Quellen für die Ableitung von Maßnahmen sowie deren Bewertung wurde die untersuchte Literatur, der Maßnahmenkatalog des IT Grundschutz, Dokumente der SAP AG und anderer Anbieter, sowie eine Analyse von sicherheitsrelevanten Systemeinstellungen von SAP ERP und der zugrundeliegenden Technologieplattform herangezogen. Für jede der aufgeführten Maßnahmen wurde untersucht, ob die Maßnahme

1. im IT-Grundschutz thematisiert wird,
2. im IT-Grundschutz konkrete Empfehlungen zur Umsetzung enthalten sind, bspw. durch Checklisten oder Beispiele zur Umsetzung,
3. mit Standardfunktionen von SAP ERP und der zugrundeliegenden Technologieplattform umsetzbar ist.

Tabelle 3 zeigt einen Überblick über den entwickelten Maßnahmenkatalog.

Für Maßnahmen, die keine IT-Unterstützung erfordern (Kategorie 1, 4 und 5), sind im IT-Grundschutz umfangreiche Empfehlungen für die Umsetzung enthalten. Eine Ausnahme bildet Kategorie 4, die im IT-Grundschutz nicht thematisiert wird. Maßnahmen, die in der Regel eine IT-Unterstützung erfordern (Kategorie 2 und 3), werden zwar thematisiert, für eine Auswahl und Umsetzung der Maßnahmen sollten jedoch weitere Informationsquellen herangezogen werden. Dies ist durchaus verständlich, da der IT-Grundschutz auch eine Allgemeingültigkeit und Anwendbarkeit für Systeme verschiedener Hersteller aufweisen sollte.

Für die Analyse der Umsetzbarkeit von Maßnahmen durch SAP ERP Standardfunktionen wurden lediglich Maßnahmen der Kategorien 2 und 3 betrachtet, da Maßnahmen der anderen Kategorien zwar durch Informationstechnologie unterstützt werden können, dies aber nicht unbedingt erforderlich ist. Bei der Ana-

lyse von Maßnahmen der Kategorie 2 hat sich gezeigt, dass ein großer Teil der Maßnahmen überdurchschnittlich gut unterstützt wird. Ausnahmen stellen die Verschlüsselung von Daten und die Anonymisierung von Testdaten dar. Hierfür stehen zwar Werkzeuge zur Verfügung, diese decken jedoch nur Teilbereiche von SAP ERP ab oder erfordern zusätzlichen Entwicklungsaufwand. Auch für die Umsetzung von Audit- und Logging-Konzepten (Kategorie 3) stehen Werkzeuge zur Verfügung, weitere Funktionalitäten, wie z. B. eine flexiblere Definition sicherheitsrelevanter Systemereignisse, wären aber hilfreich.

Der Maßnahmenkatalog umfasst die aus Sicht der Autoren wichtigsten Maßnahmen, erhebt aber nicht den Anspruch auf Vollständigkeit. Eine Erweiterung des Maßnahmenkatalogs in allen fünf Kategorien ist durchaus sinnvoll und kann einen wesentlichen Beitrag zur Datensicherheit in der ERP Anwendungsentwicklung liefern. Letztlich müssen aber alle Maßnahmen einen Realitätstest bestehen. Ob eine konkrete Maßnahme umgesetzt wird, hängt dann neben der technischen Realisierbarkeit und der organisatorischen Durchsetzbarkeit auch von ihrer Angemessenheit im Nutzungskontext der Anwendung ab. Diese Angemessenheit könnte zum Beispiel durch die Unterscheidung von Schutzklassen erfolgen. Dabei können sicherheitskritische Module einer ERP Anwendung, zum Beispiel die Personalverwaltung, in eine höhere Schutzklasse eingeordnet werden als weniger sicherheitskritische Module, wie z. B. die Lagerverwaltung. Der Nutzen des vorgeschlagenen Maßnahmenkatalogs würde dadurch weiter steigen, da im Vorfeld zusätzlich anhand der Schutzklasse die grundsätzliche Angemessenheit einer Maßnahme bestimmt werden kann.

5 Ausblick und weiterer Forschungsbedarf

Die IT-Grundschutz-Kataloge bieten eine fundierte Grundlage für die Erhöhung der Datensicherheit in der ERP Anwendungsentwicklung, dennoch bestehen häufig Schwierigkeiten in der praktischen Umsetzung. Neben der Entwicklung eines breitgefächerten Maßnahmenkatalogs zielt dieser Beitrag auch darauf ab, ein grundlegendes Verständnis und eine Sensibilität für das Thema Sicherheit in der ERP Anwendungsentwicklung zu schaffen, um erforderliche Maßnahmen in einem Unternehmen umsetzen zu können.

Die Umsetzung bzw. die Auswahl von Maßnahmen ist häufig jedoch auch an technische Restriktionen gebunden, denn für einige der identifizierten Maßnahmen besteht noch ein großer Bedarf an entsprechenden Hilfsmittel für die Umsetzung, der Raum für weitere Forschungsaktivitäten lässt. Ein Beispiel hierfür ist eine Verbesserung der Audit- und Logging-Funktionalitäten, um unberechtigte Datenzugriffe oder Systemänderungen schnell und pro-aktiv erkennen zu können. Darüber hinaus fehlen Audit- und Logging-Konzepte unter Berücksichtigung gesetzlicher Vorgaben. Ein weiteres Beispiel stellt die Anonymisierung von Testdaten dar. Trotz verschiedener am Markt verfügbarer Lösungen für die Anonymisierung von

Daten verwenden viele Unternehmen für Testzwecke unveränderte Daten aus dem Produktivsystem. Hier scheint es eine Lücke zwischen den gesetzlichen Vorgaben und der Realität zu geben. Die Datenschutzgesetze beschränken die Nutzung von Echtdaten stark, so dass für Entwicklung und Test in vielen Fällen anonymisierte Testdaten verwendet werden müssten. Auf der anderen Seite sind aber keine Werkzeuge verfügbar, die die entsprechenden Testdaten mit vertretbarem Aufwand in einer mit Echtdaten vergleichbaren Qualität bereitstellen. Eine detaillierte Betrachtung der Gründe hierfür, sowie die Ermittlung des Verbesserungspotentials, könnten einen wesentlichen Beitrag für die Datensicherheit in der ERP Anwendungsentwicklung liefern.

Literatur

Atherton M, Collins J, Vile D (2008) Data governance in the software lifecycle: Assuring the security of sensitive information. http://www.freeformdynamics.com/fullarticle_subscribe.asp?aid=336. Abruf am 2009-11-25.

Baker WH, Hylender CD, Valentine JA (2008) Data Breach Investigations Report. http://www.verizonbusiness.com/resources/security/databreachreport.pdf. Abruf am 2009-11-25.

Bögelsack A, Gradl S, Mayer M, Krcmar H (2008) SAP MaxDB-Administration. Galileo, Bonn.

BSI (2008) IT Grundschutz-Kataloge - 10. Ergänzungslieferung. https://www.bsi.bund.de/cln_174/ContentBSI/grundschutz/kataloge/katalo ge.html. Abruf am 2009-11-25.

Financial Times Deutschland (2009) Streit um Steuerdatenklau: Berlin düpiert Liechtensteins Ermittler. http://www.ftd.de/politik/europa/:Streit-um-Steuerdatenklau-Berlin-d%FCpiert-Liechtensteins-Ermittler/491628.html?mode=print. Abruf am 30.04.2009.

Lee J, Lee Y (2002) A holistic model of computer abuse within organisations. IMCS 10(2):57-63.

Louven S (2008) Konzern zieht personelle Konsequenzen aus den Datenskandalen: Telekom beurlaubt Mitarbeiter. http://www.handelsblatt.com/unternehmen/it-medien/telekom-beurlaubt-mitarbeiter;2074054. Abruf am 2009-11-25.

Magklaras GB, Furnell SM (2002) Insider threat prediction tool: Evaluating the probability of IT misuse. Computer & Security 21(1):62-73.

Richardson R (2008) CSI Computer Crime and Security Survey. http://www.gocsi.com/forms/csi_survey.jhtml. Abruf am 2009-11-25.

SAP AG (2005) SAP NetWeaver Application Server ABAP Security Guide. https://websmp208.sap-ag.de/~form/sapnet?_SHORTKEY=01100035870000401180. Abruf am 2009-11-25.

Straub DW (1990) Effective IS security. Information Systems Research 1(3):255-276.

Straub DW, Welke RJ (1998) Coping with systems risk: Security planning models for management decision-making. MIS Quarterly 22(4):441-469.

Theoharidou M, Kokolakis S, Karyda M, Kiountouzis E (2005) The insider threat to information systems and the effectiveness of ISO17799. Computers & Security 24(6):472-484.