Denis Royer und Martin Meints

Planung und Bewertung von Enterprise Identity Managementsystemen

Wie kann man Enterprise Identity Managementsysteme (EIdMS) in der Planung und im laufenden Betrieb bewerten? Der vorliegende Beitrag stellt einen Ansatz für ein auf der Balanced Scorecard basierendes Kennzahlensystem vor und entwickelt mögliche Kennzahlen für die Sicherheitsfunktionen von Enterprise Identity Management (EIdM) aus relevanten Normen und Standards.

1 Einleitung

Für die Umsetzung diverser betrieblicher Aktivitäten und Transaktionen greifen heutige Organisationen auf eine Vielzahl von parallel genutzten IT-Infrastrukturen und -Systeme zurück, die in die oftmals vielschichtigen (Geschäfts-)Prozesse einer Organisation integriert werden müssen. In diesem Kontext müssen sich Organisationen mit dem Thema der Nutzer- und Zugangsverwaltung, dem sogenannten Enterprise Identity Management (EIdM), auseinandersetzen. Ziel der Einführung von EIdM ist es u.a. bestehende IT-Infrastrukturen und Systeme vor unbefugten Zugriffen zu schützen, um Datenschutz- und Datensicherheitsanforderungen gerecht zu werden und um ggf. Kosteneinsparungspotentiale nutzen zu können.

Dipl.-Wirt.-Inf. Denis Royer

ist wiss. Mitarbeiter an der T-Mobile Stiftungsprofessur für Mobile Business und mehrseitige Sicher-heit an der Johann Wolfgang Goethe-Universität, Frank-furt am Main
E-Mail: Denis.Royer@M-Lehrstuhl.de

Dr. Martin Meints

ist Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) im Projekt FIDIS.
E-Mail:
ULD61@datenschutzzentrum.de

- **Die Einführung von Enterprise Identity Managementsystemen (EIdMS) stellt die Organisationen vor eine Reihe von Herausforderungen. Insbesondere in der Entscheidungs- und Planungsphase ist es wichtig, dass Organisationen ihre internen Dimensionen (z.B. Prozesse, Strukturen) und deren Wechselwirkungen untereinander berücksichtigen [Ro08].**

Um eine geeignete Entscheidungsgrundlage zu schaffen, müssen die aus der EIdM-Systemeinführung resultierenden Vor- und Nachteile mit Hilfe geeigneter Methoden identifiziert und bewertet werden, die über rein finanzielle Betrachtung hinausgehen und ganzheitlich alle relevanten Dimensionen einbeziehen. Eine solche Vorgehensweise wird in diesem Artikel auf Basis der Balanced Scorecard (BSC) von Kaplan und Norton [KaNo96] entwickelt und erörtert. Der vorgestellte Ansatz soll dabei vorrangig als Unterstützungsinstrument in der taktischen Planung mit einem Zeithorizont von einem bis drei Jahren dienen. Weiterhin werden Anknüpfungspunkte an etablierte IT-Sicherheitskriteriensysteme beleuchtet.

2 EIdM und seine Einsatzbereiche

Vor dem Hintergrund steigender Digitalisierung von Geschäfts- und zugehörigen Unterstützungsprozessen stellt das Thema EIdM eine zunehmende Herausforderung für Unternehmen und Organisationen dar [DeDe07]. Ein Grund hierfür ist u.a. die sich über den Zeitverlauf ändernden Nutzerberechtigungen (Rollen und Rechte), die bspw. aus einem Arbeitsstellenwechsel (z.B. Beförderungen) resultieren können. Die Änderungen in den (partiellen) Identitäten[1] der Nutzer müssen möglichst zeitnah und sicher angepasst werden [Wi05] und können dem sogenannten Identitätslebenszyklus zugeordnet werden, der aus den folgenden vier Prozessschritten besteht: Einschreibung (dem sog. Enrolement), Management, Unterstützung und letztlich der Löschung der Identitätsdaten [HaMe06] [Ro08] [Wi05].

2.2 Einordnung des EIdM

In Anlehnung an das Rahmenwerk von Bauer, Meints und Hansen [BaMeHa05] kann man EIdMS den sog. Typ 1-Identitätsmanagementsystemen zuordnen. Diese Art von Identitätsmanagementsystemen wird für die Zuweisung von Identitäten an einen Nutzer und zur zentralen Organisation und Verwaltung von Nutzerkonten eingesetzt und grenzt sich insofern von den sog. Profiling-Systemen (Typ 2 – Abstraktion/Ableitung von Identitäten) oder nutzergesteuerten Identitätsmanagementsystemen (Typ 3 – weitestgehende Kontrolle des Nutzers über seine eigenen Identitäten) ab.

Weiterhin kann bei den EIdMS hinsichtlich der organisatorischen und technischen Ebene differenziert werden. Auf der *organisatorischen Ebene* unterstützen

1 Partielle Identitäten sind Untermengen von Attributen einer vollständigen Identität (bspw. einer Person). Jede Identität einer Person besteht aus vielen partiellen Identitäten, wobei jede von ihnen eine Person in einer spezifischen Rolle oder einem spezifischen Kontext darstellt (basierend auf den Arbeiten von [HaMe06]).

EIdMS die einzelnen Prozessschritte des Identitätslebenszyklus, indem sie die Authentifizierung, die Autorisation, die Administration und das Audit/ Accounting (die sogenannten *4 As*) der zu verwaltenden Nutzerkonten ermöglichen.

Hinsichtlich der *technischen Ebene* lassen sich eine Vielzahl von Technikprodukten in den verschiedenen Bereiche (Nutzerdienste, Identitätsdienste, etc.) des EIdM unterscheiden. Beispiele sind Single-Sign-On (SSO)-Lösungen, Verzeichnisdienste, Public-Key-Infrastrukturen (PKI) und IAM-Systeme) [Fl07] [Wi05]. Das EIdM ist dabei als eine Unterstützungsfunktion anzusehen, die sich als zusätzliche Schicht in die bestehende IT-Infrastruktur einer Organisation als Schnittstelle zwischen Nutzern, Diensten und Applikationen integriert [Fl07].

- **Entgegen der von vielen (Technik-) Herstellern kommunizierten Meinung und publizierten Informationen handelt es sich beim EIdM um ein Technologierahmenwerk verschieden gearteter Technik und Funktionen statt um ein einzelnes Software-Produkt, das alle Unternehmensbereiche ohne Anpassungen abdecken könnte. Die Realität sieht oftmals eher so aus, dass bei der Einführung von EIdM-Lösungen in eine Organisation umfangreiche, unternehmensspezifische Konfigurationen notwendig sind (Customizing).**

2.2 Treiber für EIdM

Für die Einführung von EIdM in eine Organisation sprechen eine Vielzahl von Grün-den. So gehören IT-Risikomanagement-, Wertschöpfungs- und Compliance-Ziele zu den häufigsten Treibern für EIdM-Projekte. Die genannten Treiber stehen dabei nicht unbedingt in einem Zielkonflikt zueinander, sondern es lassen sich teilweise Synergien feststellen [Ro08].

Eine falsche oder fehlende Berücksichtigung dieser Aspekte und ein mangelhaftes oder fehlendes Management des Identitätslebenszyklus können erhebliche negative Konsequenzen für die Organisation nach sich ziehen. Dazu zählen unter anderen:

- Produktivitätseinbußen und erhöhte Kosten für das Management der Nutzerkonten,
- Risiken, die mit möglichen Sicherheitslücken einhergehen (resultierend aus schlecht verwalteten Nutzerkonten), und
- Sanktionen aufgrund der Nichteinhaltung von relevanten Gesetzen und Regelungen (Compliance) [Be05].

3 EIdM, ROI und ROSI

Die Bewertung von Investitionen im Bereich der IT-Sicherheit ist ein vielfach kontrovers diskutiertes Themengebiet (vgl. [CMR04], [MMZ07] und [SAS06]). Neben den verschiedenen Problemen von „klassischen" IT-Investitionen, wie dem IT-Produktivitäts-Paradoxon ([Br93], [WFW07]), steht auch die Bewertung von Investitionen im Bereich der IT-Sicherheit und insbesondere des EIdM vor einer Vielzahl von Herausforderungen [MMZ07] [SAS06].

Für die Bestimmung des Nutzens von EIdM werden oftmals Metriken mit limitiertem Geltungsbereich, wie bspw. die Kapitalverzinsung (ROI)[2], als Bewertungskriterium herangezogen, um die Treiber des EIdM und ihre Auswirkungen (z.B. das Maß der Prozessintegration oder die Einbeziehung aller relevanten Parteien) beurteilen zu können.

Problematisch erweist sich häufig die Identifikation der potentiellen Ersparnisse bzw. nicht angefallenen Kosten, aufgrund der getätigten IT-Sicherheitsinvestitionen. So werden Investitionen in die IT-Sicherheit getätigt um Risiken abzuwenden und mögliche finanzielle und immaterielle Verluste zu verhindern [SAS06]. Die Abwendung dieser Verluste und Risiken macht es jedoch schwierig oder sogar unmöglich, die relevanten Kosten zu spezifizieren und zu bemessen, da unerwünschte Vorfälle aufgrund der präventiven Natur von Sicherheitstechnologien weitestgehend verhindert werden. Zusätzlich stellt die Bestimmung des optimalen Mitteleinsatzes für die gesamte IT-Sicherheit eine Herausforderung. In diesem Zusammenhang werden in der Literatur verschiedene Ansätze und Rahmenwerke zur Bewertung der ökonomischen Auswirkungen und Nutzen von IT-Sicherheitsinvestitionen diskutiert. Ein sehr verbreiteter Ansatz stellt dabei der sog. „Return on Security Investments (ROSI)" dar, der zur Monetarisierung von IT-Sicherheitsinvestitionen herangezogen werden kann [CMR04] [MMZ07] [SAS06]. Aufbauend auf den ROI ist der ROSI auf die Analyse und Monetarisierung von Produktivitätseinbußen oder potentiellen Verlusten durch Sicherheitslücken ausgerichtet. Neben dieser rein finanziell ausgerichteten Kennzahl bedarf es weiterreichender Metriken, die auch immaterielle und organisatorische Faktoren zum Zweck der ganzheitlichen Bewertung von EIdM-Investitionen mit in die Analyse einfließen lassen. Ein ganzheitlicher Ansatz wird im Folgenden vorgestellt.

2 Die Kapitalverzinsung oder auch „Return on Investment (ROI)" gibt den Effizienzgrad einer Investition basierend auf dem erwirtschafteten Profit an (vgl. [Pu04] oder [EFS04]).

4 Die BSC als Bewertungsansatz

Ein Kennzahlensystem ist in der betrieblichen Praxis ein nicht mehr wegzudenkendes Instrument zur Planung und Steuerung einer Vielzahl von Abläufen in Organisationen. Das Kennzahlensystem selbst ist eine geordnete Menge von Kennzahlen, die miteinander in Verbindung stehen können. Eine solche Vernetzung der Kennzahlen ermöglicht es, vollständige und komprimierte Informationen für die Planung und Kontrolle bereitstellen zu können. Kennzahlen wiederrum stellen Maßzahlen bzw. Indikatoren dar und werden zur Quantifizierung von Sachverhalten genutzt. Beispiele für Kennzahlen sind der Reifegrad von Geschäftsprozessen oder „*Key Performance Indicators*", wie sie z.B. beim IT-Service-Management auf Basis der IT Infrastructure Library (ITIL) verwendet werden.

Die klassische BSC wurde 1992 von Kaplan und Norton als ein *ausbalanciertes Kennzahlensystem* für Unternehmen und Organisationen entwickelt [KaNo96]. Die BSC ist in vier übergreifende Perspektiven aufgeteilt, die sich aus der „Vision und Strategie" einer Organisation ableiten. Die vier Perspektiven der BSC umfassen:

- die Finanzperspektive,
- die Prozessperspektive,
- die interne oder Potentialperspektive und
- die Kundenperspektive

Jede dieser genannten Perspektiven enthält jeweils spezifische, Organisations-abhängige Kennzahlen, die untereinander (kausale) Wirkungszusammenhänge und Vernetzungen aufweisen können.

Die klassische BSC hat das Bestreben, die zurückliegenden Erfolge aufzuzeigen und zukünftige Trends abzubilden, indem

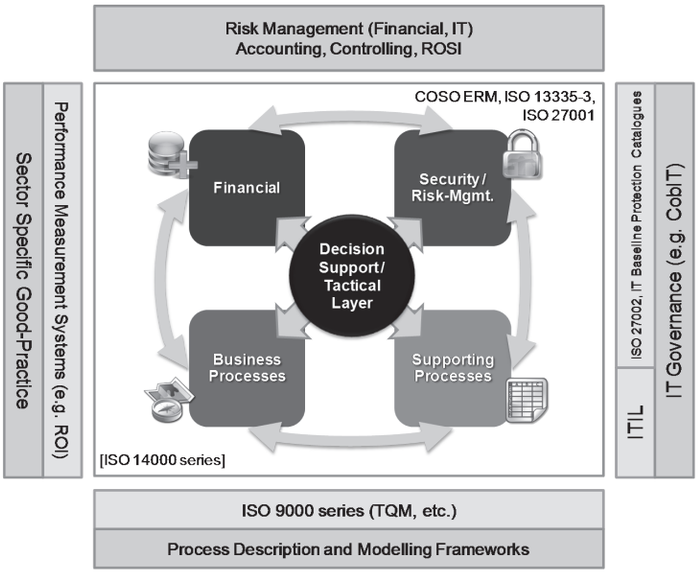
die einzelnen Perspektiven mit der *Vision und Strategie* einer Organisation verknüpft werden. Die BSC erweitert dabei aufgrund des ganzheitlichen Ansatzes die klassischen, finanzwirtschaftlichen Kennzahlen um immaterielle Kennzahlen, wie bspw. die Kundenzufriedenheit. Damit lassen sich umfassendere Erkenntnisse über die Organisation gewinnen und ein nachhaltigeres Handeln im Interesse der Organisation ableiten. Um die Zusammenhänge und Verknüpfungen zwischen den einzelnen Perspektiven und den darin enthaltenen Kennzahlen aufzeigen zu können, werden Kausalketten und kausale Netzwerke für deren Analyse verwendet [JLM04].

5 Die taktische EIdM-BSC

Im Gegensatz zur klassischen, strategischen BSC hat die hier präsentierte BSC eher einen taktischen Fokus mit einem Zeithorizont von ein bis drei Jahren. Innerhalb dieses Zeitraums werden die strategischen Vorgaben einer Organisation in Projekten umgesetzt. Hier kann die BSC als Entscheidungsunterstützungsinstrument für die Einführung von EIdMS genutzt werden oder im Weiteren als Steuerungsinstrument im Rahmen des Projektcontrollings (z.B. Messung der Zielerreichung). Die hier vorgeschlagene BSC umfasst die folgenden vier Perspektiven [Ro08]:

- ***Finanz-Perspektive:*** Diese Perspektive enthält die klassischen finanzwirtschaftlichen Kennzahlen. Dazu gehören bspw. die generellen Finanzinformationen und die Kosten, die mit einem EIdM-Projekt einhergehen (basierend auf TCO, LCC, etc.). Dies hilft eine Übersicht über die potentiellen Zahlungsflüsse zu erhalten.
- ***Geschäftsprozess-Perspektive:*** Hier werden die Kernprozesse einer Organisation betrachtet und analysiert. Relevante Kennzahlen sind bspw. der aktuelle und gewünschte Grad der Integration der Informationssysteme und der EIdMS in die Geschäftsprozesse einer Organisation oder potentiellen Effizienzsteigerungen innerhalb der Organisation, bestimmen [JLM04].
- ***Risikomanagements- und Sicherheits-Perspektive:*** In diesem Bereich werden die potentiellen Risiken (z.B. Projektrisiken, Sicherheitsrisiken) und das Sicherheitsmanagement analysiert, die im Rahmen eines EIdM-Projektes auftreten können. Hierbei lassen sich schwerpunktmäßig Kennzahlen aus den Bereichen Compliance (z.B. Basel II, KonTraG oder SOX), Best-Practice (ITIL, etc.) oder generellen Standards zur Informationssicherheit (ISO/IEC 27000-Normenreihe, etc.) ableiten.
- ***Unterstützungsprozess-Perspektive:*** Die letztgenannte Perspektive untersucht die Unterstützungsprozesse in einer Organisation (Personalwirtschaft, IT, Management, etc.), die indirekt an der Wertschöpfung des Unternehmens beteiligt sind. Im Zusammenhang mit dem EIdM erlaubt diese Perspektive eine weitergehende Analyse der Prozessreife zwischen den Geschäfts- und Unterstützungsprozessen.

Abbildung 1 | Zuordnung von relevanten Standards und Best-Practice-Rahmenwerke auf die vorgestellte EIdM-Balanced Scorecard (eigene Darstellung basierend auf [Ro08]).



Die für den Anwendungsbereich von EIdM abgeleitete BSC ist in Abbildung 1 dargestellt (eigene Darstellung basierend auf [Ro08]). Im Weiteren lassen sich die vier Perspektiven den Geschäftszielen (Finanz- und Geschäftsprozesse) oder den Compliance-Zielen (Risikomanagement und Sicherheit und Unterstützungsprozesse) zuordnen. Durch den Einsatz der hier skizzierten EIdM-BSC lassen sich diese zwei Zielsetzungen übergreifend gegenüberstellen. Weiterhin können die so gewonnen Informationen für den weiteren Entscheidungsprozess genutzt werden.

- **Wie auch bei der klassischen BSC gilt es zu bedenken, dass die in den vier Perspektiven enthaltenen Kennzahlen kausale Vernetzungen aufweisen können. Hier besteht weiterer Forschungsbedarf, um die Wechselwirkungen der in der EIdM-BSC enthaltenen materiellen und immateriellen Kennzahlen in der Praxis besser verstehen und in die Ausgestaltung einbeziehen zu können.**

Weiterhin können die einzelnen Perspektiven und deren Kombinationen auf taktischer Ebene größtenteils mit bereits existierenden Best-Practice-Ansätzen (CobiT, ITIL, etc.) und relevanten Standards (z.B. in den Normenreihen ISO/IEC 9000, ISO/IEC 27000, ISO/IEC 15408) abdeckt oder verknüpft werden, wodurch eine integrierte und detaillierte Analyse der einzelnen Perspektiven ermöglicht werden kann (vgl. Abbildung 1). Auch lassen sich im Weiteren verbundene Steuerungskonzepte für ein übergreifendes Management des EIdM schaffen, das die Aspekte Risikomanagement („Risk-Management“), Erfolgsmessung („Performance Measurement“), Organisation der IT („IT-Governance“) und Prozessbeschreibungen („Process Description Frameworks“) zusammenführt (vgl. Abbildung 1). Auf die übergreifenden Bereiche IT-Governance und Risk-Management soll im Folgenden weiter eingegangen.

6 Normen zur Informationssicherheit

Im Folgenden werden nun die ISO/IEC 27000-Normenreihe und die Common Criteria (CC)[3] analysiert. Beide Normen sind etabliert und werden in Europa verbreitet eingesetzt. Sie sind daher als besonders relevant einzustufen.

6.1 ISO 27000 Normenreihe

Die Normenreihe ISO/IEC 27000 behandelt Informationssicherheitsmanagement-Systeme (ISMS). Sie sind für die Umsetzung in Organisationen konzipiert. Für die Zertifizierung von ISMS beschreibt die ISO/IEC 27001:2005 die geltenden Anforderungen im *Annex A* in Form von in generelle „Control Objectives" (Sicherheitsziele) und zugehörige „Controls" (Prüfpunkte, auch als Maßnahmen übersetzt). Diese sind nur sehr knapp, oft mit nur einem Satz, ausgeführt. In der Norm ISO/IEC 27002:2005 (vormals ISO/IEC 17799:2005) werden diese Anforderungen dann mit spezifischeren Umsetzungsempfehlungen versehen.[4]

Die infrastrukturelle Bedeutung von EIdM spiegelt sich in sofern in der ISO/IEC 27000-Normenreihe wider, als eine ganze Reihe von „Control Objectives" und „Controls" ganz oder in wesentlichen Teilen unter Nutzung des EIdM umgesetzt werden können. Relevant sind in diesem Umfeld unmittelbar:

- A.8 (Human resource security), insbesondere die Punkte:
  - A.8.1.1 ([Definition of] roles and responsibilities [prior to employment])
  - A8.2.1 (Management responsibilities [during employment])
  - A.8.3.1 (Termination responsibilities)
- A.9 (Physical and environmental security), insbesondere
  - A.9.1.2 (Physical entry control), ggfs. bei integrierten Lösungen noch
  - A.9.1.3 (Securing offices, rooms and facilities)
- A.10.10 (Monitoring) mit den "Controls"
  - A.10.10.1 (Audit logging)
  - A.10.10.3 (Protection of log information)
  - A.10.10.4 (Administrator and operator logs)
  - A.10.10.5 (Fault logs)
  - A.10.10.6 (Clock synchronization)
- A.11 (Access control), insbesondere
  - A.11.2.1 (User registration)
  - A.11.2.2 (Privilege management)
  - A.11.2.3 (User password management)
  - A.11.2.4 (Review of user access rights)
  - A.11.3.1 (Password use)
  - A.11.4.2 (User authentication for external [network] connections)
  - A.11.5.1 (Secure log-on procedures [for operating systems])
  - A.11.5.2. (User identification and authentication)
  - A.11.5.3 (Password management system)
  - A.11.5.5 (Session time-out)
  - A.11.5.6 (Limitation of connection time)
  - A.11.6.1 (Information access restriction [in applications])
- A.12 (Information systems acquisition, development and maintenance), insbesondere
  - A.12.4.3 (Access control to program source code)

Darüber hinaus kann das EIdM eingesetzt werden, um die Umsetzung weiterer „Control Objectives" und „Controls" zu unterstützen. Dies betrifft insbesondere:

- A.10.9.1 (Electronic commerce)
- A.15.1.4 (Data protection and privacy of personal information), da Schutz von Zutritt, Zugang und Zugriff unter Datenschutzgesichtspunkten relevante Sicherheitsziele sind (siehe z.B. Anlage zu §9 Satz 1 BDSG)

6.2 Common Criteria

Die CC sind in der Version 2.3 als ISO/IEC 15408 normiert und stellen eine international standardisierte Methode zur Evaluation und Zertifizierung von Produkten unter Sicherheitsgesichtspunkten dar. Die aktuelle Version 3.1 der CC, auf die sich die folgenden Ausführungen beziehen, befindet sich derzeit im Normierungsverfahren bei der ISO (International Organization for Standardization). Da EIdMS ebenfalls im Sinne der ISO/IEC 15408 einen Produktkern haben, lassen sich wesentliche der ggfs. benötigten Sicherheitsfunktionen z.B. im Vorfeld einer Beschaffung aus den CC ableiten.

Im Teil 2 beschreiben die CC eine Reihe von Klassen und darin in Familien organisiert die zugehörigen Sicherheitsfunktionen für zu zertifizierende Produkte. Wie schon bei der ISO/IEC 27000-Normenreihe zeigt sich, dass zahlreiche Sicherheitsfunktionen Relevanz haben. Diese Funktionen beziehen sich sowohl auf das EIdM selber als auch auf Anwendungen, die sich bei Authentifizierung, Autorisierung und – in Abhängigkeit von der Ausbaustufe – möglicherweise weiteren Funktionen auf das EIdM stützen. Ein Beispiel für ein ausgebautes EIdM kann ein System sein, das bspw. durch eine PKI erweitert ist, so dass spezielle Sicherheitsfunktionalitäten der Nichtabstreitbarkeit von Nachrichten realisiert werden können.

Unmittelbar betroffen ist die Klasse „*Authentication and Authorisation*" (FIA). Alle darin enthaltenen Familien und Funktionalitäten betreffen den Kern der EIdMS:

- Reaktionen des Systems auf Fehlauthentisierung (Familie FIA_AFL)
- Definition von Attributen der Benutzer (Familie FIA_ATD)
- Spezifikation eines Geheimnisses (Familie FIA_SOS; diese bezieht sich u.a. auf die Qualität von Kennwörtern)
- Authentisierung der Benutzer (Familie FIA_UAU; diese behandelt u.a. relevante Sicherheitsaspekte wie den Zeitpunkt und die Angemessenheit der Stärke der Authentisierung)
- Identifizierung von Benutzern (Familie FIA_UID)
- Korrekte Bindung der Sicherheitsattribute an den Benutzer (Familie FIA_USB)

In zahlreichen anderen Klassen kann das EIdMS unterstützende Funktionen wahrnehmen. Diese Klassen sind vor allem:

- Auditierung (Klasse FAU), insbesondere Aspekte der Protokollierung (siehe auch [MeTh07]
- Kommunikation (Klasse FCO), Funktional erfüllbar insbesondere durch Signaturen und PKI
- Schutz der Daten der Benutzer (Klasse FDP)
- Sicherheitsmanagement (Klasse FMT), hier insbesondere durch Verwaltung von Attributen
- Privatsphäre und Recht auf informationelle Selbstbestimmung (Klasse FPR), in der sich Funktionalitäten wie Anony-

3 Ein unentgeltlicher Download der benannten Versionen ist unter www.bsi.de/cc/ möglich.

4 Die genannten Normen können über die International Organization for Standardization (ISO, www.iso.org) oder einschlägige Fachverlage (z.B. den Beuth Verlag, www.beuth.de) bezogen werden.

mität, Pseudonymität, Unverkettbarkeit und Unbeobachtbarkeit finden, und
- Zugang zum Evaluationsgegenstand (Klasse FTA), insbesondere Aspekte der Kontrolle über Sitzungen der Benutzer.

6.3 Kennzahlen

Aus den in den genannten Normen (ISO 27000 Normenreihe und CC) aufgeführten Anforderungen an EIdMS lassen sich nun mögliche Kennzahlen für die EIdM-BSC ableiten – speziell die Perspektiven Risikomanagement und Sicherheit und Unterstützungsprozesse. Kennzahlen können auf absoluten oder relativen, quantitativ messbaren Werten, wie etwa die prozentuale Umsetzung, oder qualitativen Werten im Sinne von Stufen eines Reifegradmodells[5] basieren. Im Folgenden sind nun einige Beispiele für Kennzahlen genannt, die in Abhängigkeit von der bestehenden oder den Zielen der geplanten Implementierung (siehe Lastenheft) des EIdMS organisationsabhängig genutzt werden können:

- Zutrittszonen erfasst im Verhältnis zu vorhandenen Zutrittszonen
- In das EIdMS integrierte Mitarbeiter im Verhältnis zu Mitarbeiter gesamt
- Mittels EIdMS verwaltete Benutzerkonten mit Sonderrechten im Verhältnis zu vorhandenen Benutzerkonten mit Sonderrechten
- Unter Verwendung des EIdMS verwaltete und qualitätsgesicherte Passwörter im Verhältnis zu Kennwörtern insgesamt
- Betriebssystem-, Anwendungs- und Netzverbindungen von Benutzern, die durch das EIdMS einer Zeitbeschränkung unterliegen, im Verhältnis zu Betriebssystem-, Anwendungs- und Netzverbindungen insgesamt

Erreichte/erreichbare Stufen der Authentifizierungsstärke im Verhältnis zu erreichter/benötigter Stufe der Authentifizierungsstärke [Reifegrad]

- Erreichte/erreichbare Stufe der Qualität (Inhalt, Umfang, Auswertbarkeit z.B. unter Tooleinsatz) der Protokollierung im Verhältnis zu erreichter/benötigter Stufe der Qualität der Protokollierung [Reifegrad]
- Erreichte/erreichbare Stufe der Revisionssicherheit der Protokollierung im Verhältnis zu erreichter/benötigter Stufe der Revisionssicherheit der Protokollierung [Reifegrad]

Unter Nutzung des EIdMS verwaltete Informationsquellen wie Anwendungen, Verzeichnisse etc. im Verhältnis zu Informationsquellen insgesamt [Kennzahl für Integration, die aber auch die Reichweite der Sicherheitsfunktionen in der Organisation beschreibt]

Qualität der verfügbaren Nutzerdaten in den einzelnen Anwendungssystemen als übergreifende Kennzahl für die Integration verschiedener Datenquellen für Identitätsinformationen [Reifegrad].

Die hier zusammengestellte Übersicht an Kennzahlen ist weder vollständig noch universell für jeden Zweck geeignet und bedarf projektabhängiger Anpassungen, um im Weiteren kausale Abhängigkeitsnetze modellieren zu können [KaNo96].

▸ **In jedem Fall zeigen diese Beispiele jedoch, welche geeigneten Kennzahlen anhand der vorgestellten Sicherheitsanforderungen an EIdMS für unterschiedliche Organisationen genutzt werden können,. Damit wird eine objektivierte und vergleichbare Bewertung bestehender oder geplanter Implementierungen von EIdMS ermöglicht.**

7 Fazit und Ausblick

▸ **Die EIdM-BSC unterstützt den Entscheidungsprozess in einer Organisation auf der taktischen Managementebene. Jedoch besteht weiterer Forschungsbedarf, um die Wechselwirkungen der in der EIdM-BSC enthaltenen materiellen und immateriellen Kennzahlen in der Praxis besser verstehen zu können. Der Nutzen des vorgestellten Ansatzes für die taktische Entscheidungsfindung in Organisationen soll zukünftig in der Praxis weiter analysiert und evaluiert werden. Die hier gewonnenen Erkenntnisse sollen dabei in die Weiterentwicklung eines Rahmenwerkes für die Erstellung einer EIdM-BSC einfließen.**

5 Wie z.B. das *Capability Maturity Model*, entwickelt Mitte der 1990er Jahre an der Carnegie Mellon University (Pittsburgh, USA) für Prozesse zur Entwicklung von Software; siehe www.sei.cmu.edu/cmm/.

Literatur

BaMeHa05 Bauer, M., Meints, M., Hansen, M. (Hrsg.), FIDIS Deliverable D3.1 – Structured Overview on Prototypes and Concepts of Identity Management Sys-tems, Frankfurt a.M. 2005.

Be05 Berghel, H.: The Two Sides of ROI: Return on Investment vs. Risk of Incarceration. Communications of the ACM, Nr. 4 (48), 2005; S. 15-20.

Br93 Brynjolfsson, E.: The Productivity Paradox of Information Technology. Communications of the ACM, Nr. 12 (36), 1993; S. 67-77.

CMR04 Cavusoglu, H.; Mishra, B.; Raghunathan, S.: A Model for Evaluating IT Security Investments. Communications of the ACM, Nr. 7 (47), 2004; S. 87-92.

DeDe07 Dewey, B.I.; DeBlois, P.B.: Current Issues Survey Report 2007. EDUCAUSE Quarterly, Nr. 2 (30), 2007; S. 12-31.

EFS04 Erdogmus, H.; Favaro, J.; Strigel, W.: Return on Investment. IEEE Software, Nr. 3 (21), 2004; S. 18-22.

Fl07 Flynn, M.J.: Enterprise Identity Services. http://360tek.blogspot.com/2006/07/enterprise-identity-services.html, 2007.

HaMe06 Hansen, M.; Meints, M.: Digitale Identitäten – Überblick und aktuelle Trends. Datenschutz und Datensicherheit (DuD), Nr. 9 (30), 2006; S. 571-575.

JLM04 Jonen, A. et al.: Balanced IT-Decision-Card, Ein Instrument für das Investitionscontrolling von IT-Projekten. Wirtschaftsinformatik, Nr. 3 (46), 2004; S. 196-203.

KaNo96 Kaplan, R.S.; Norton, D.P.: The Balanced Scorecard. Translating Strategy into Action, Random House, 1996.

MeTh07 Meints, M., Thomsen, S., Protokollierung in Sicherheitsstandards. Datenschutz und Datensicherheit (DuD), Nr. 10 (31), 2007; S. 749-751.

MMZ07 Magnusson, C.; Molvidsson, J.; Zetterqvist, S.: Value Creation and Return On Security Investmensts (ROSI). In (Venter, H. et al. Hrsg.): IFIP SEC 2007: New Approaches for Security, Privacy and Trust in Complex Environments, Springer, Boston, 2007; S. 25-35.

Pu04 Purser, S.A.: Improving the ROI of the security management process. Nr. 6 (23), 2004; S. 542-546.

Ro08 Royer, D.: Assessing the Value of Enterprise Identity Management (EIdM) – Towards a Generic Evaluation Approach. Proceedings of the 3rd International Conference on Availability, Reliability and Security („ARES 2008 – The International Dependability Conference"), IEEE Press, Barcelona, 2008.

SAS06 Sonnenreich, W.; Albanese, J.; Stout, B.: Return On Security Investment (ROSI) – A Practical Quantitative Model. Journal of Research and Practice in Information Technology, Nr. 1 (38), 2006; S. 45-56.

WFW07 Wan, Z.; Fang, Y.; Wade, M.: A Ten-Year Odyssey of the "IS Productivity Paradox" – A Citation Analysis (1996-2006). In (AIS Hrsg.): Proceedings of the 13th Americas Conference on Information Systems (AMCIS), Keystone, Colorado, 2007.

Wi05 Windley, P.J.: Digital Identity. O'Reilly, Sebastopol et al., 2005.