Prozesse und Sicherheitsaspekte am Beispiel e-Procurement

Lars Algermissen[1]
Sonja Hof[2]
Björn Niehaves[1]

1: Lehrstuhl für Wirtschaftsinformatik und Informationsmanagement, Universität Münster, Leonardo-Campus, 48149 Münster,
islaal@wi.uni-muenster.de
bjni@wi.uni-muenster.de

2: Universität Linz, Institut für Angewandte Informatik, Abteilung für Informatik in Wirtschaft, Verwaltung und Gesellschaft Altenbergerstrasse 69, 4040 Linz,
sonja.hof@ifs.uni-linz.ac.at

Schlagworte: e-Government Modellierungskonzept, Prozessmodellierung, Organisationsgestaltung, Multiperspektivische Modellierung, Sicherheit

Abstract: Im Zuge der Verwaltungsoptimierung, insbesondere im Rahmen des e-Government, ist die Analyse von Verwaltungsabläufen zusehends ins Zentrum wissenschaftlicher als auch praktischer Untersuchungen gerückt. Die aus dem betrieblichen Bereich entlehnten Methoden des Prozessmanagements diffundieren in zunehmendem Maße in den Bereich der öffentlichen Verwaltung. Dabei erfolgt eine domänenspezifische Adaption der Konzepte und Methoden jedoch häufig nicht in ausreichendem Maße. Die Integration von IT-Sicherheitsapekten in die Prozessdarstellung ist eine zentrale Anforderung der Praxis, hinreichende Berücksichtigung findet dies allerdings zumeist nicht. Im Folgenden wird daher eine Methode zur Modellierung von Verwaltungsprozessen vorgestellt, welche in besonderem Maße IT-Sicherheitsaspekte adressiert. Dabei wird die entwickelte Methode am Beispiel von eProcurement-Prozessen veranschaulicht.

1. Sicherheitsaspekte im e-Government

Die öffentliche Verwaltung steht seit Beginn der 90er Jahre einer Reihe von neuen Herausforderungen gegenüber. Die Gesellschaft wird nicht zuletzt durch den Einfluss neuer Technologien umgestaltet. Es ist ein Trend zu wachsender Individualisierung zu verzeichnen, wodurch der Anspruch des Einzelnen an den Staat als Problemlöser zunimmt. Es ist bis heute nicht

gelungen, parallel zu dem steigenden Aufgabenvolumen auch die Leistungsfähigkeit des Staates adäquat zu verbessern. Die erhöhten Anforderungen führten vielmehr zu einer stetigen Erhöhung der Staatsquote und des Schuldenstandes. Durch die Abweichung von Aufgabenvolumen und Leistungspotenzial ist eine Modernisierungs- und Leistungslücke entstanden.[1]

Als eine Möglichkeit, diese Lücke zu schließen, ist seit einigen Jahren der Begriff Electronic Government (e-Government) in aller Munde, der inzwischen dem Dunstkreis wissenschaftlicher Debatten entwachsen ist und zunehmend Gegenstand von Handlungsstrategien bei der Modernisierung der Verwaltung wird. Der Kern von e-Government besteht in der Abwicklung von Verwaltungsprozessen.[2] e-Government versteht sich als die Vereinfachung und Abwicklung von Informations, Kommunikations und Transaktionsprozessen zur Erbringung einer Verwaltungsdienstleistung durch den Einsatz von Informations- und Kommunikationstechnologien innerhalb und zwischen Behörden sowie zwischen Behörden und Privatpersonen bzw Unternehmen.[3]

Der Einsatz von Informations- und Kommunikationssystemen ist zentraler Bestandteil der Abwicklung von e-Government-Services. Jede technische Implementierung ist dabei entweder direkt oder indirekt durch Sicherheitsaspekte bestimmt. Sicherheitstechnologien sind bereits in diversen anderen Domänen umfassend angewendet worden,[4] wobei die Spezifikationen der Anwendungsdomäne zum Teil erheblichen Einfluss auf ihre konkrete Umsetzung ausüben.

Im Rahmen dieses Beitrags soll daher eine Methode zur fachkonzeptionellen Modellierung von e-Government-Prozessen vorgestellt werden, mit der IT-Sicherheitsaspekte explizit berücksichtigt werden.

---

[1] *Budäus, D. & Schwiering, K.* (1999) Die Rolle der Informations- und Kommunikationstechnologien im Modernisierungsprozeß öffentlicher Verwaltungen. In: Electronic Business und Knowledge Management, *A.-W. Scheer* (Ed), 143–165, Heidelberg.

[2] *von Lucke, J. & Reinermann, H.* (2003) Speyerer Definition von Electronic Government. http://foev.dhv-speyer.de/ruvii/Sp-EGov.pdf (2002-01-02).

[3] *Becker, J., Algermissen, L. & Niehaves, B.* (2003) E-Government – State of the art and development perspectives. Muenster.

[4] *Desmedt, Y. & King, B.* (2002) Verifiable Democracy: a Protocol to secure e-Government. In: Proceedings of the 1st International Conference on E-Government 2002; *Fleck, K.* (2003) Portal Austria Service – der sichere Zugang zu Verwaltungs-Services. In: Proceedings of the 2nd e-Gov-Day 2003, 183–190, Österreichische Computer Gesellschaft.

2. Prozesse im Fokus des e-Government

Prozessorientierung ist seit Beginn der 90er Jahre als eine Maxime der Unternehmensgestaltung akzeptiert. In den letzten Jahren wurde im Zuge der Verbreitung von e-Government auch in der öffentlichen Verwaltung begonnen, die Strukturen an den Geschäftsprozessen auszurichten. Da jede Organisationsstruktur ihren eigenen Wirkungszusammenhang besitzt, müssen bei der Modellierung von Verwaltungsprozessen die Eigenschaften der Domäne detailliert untersucht und die sich daraus ergebenden Anforderungen berücksichtigt werden. Zu den wichtigsten Eigenschaften von Verwaltungsprozessen gehören:

1. *Repetitivität:* Abläufe in Verwaltungen weisen hohe Fallzahlen auf.
2. *Linearität:* für Verwaltungsprozesse existieren verschiedene Ablaufmöglichkeiten, die durch zahlreiche Entscheidungssituationen bedingt sind. Betrachtet man die Entscheidungssituationen jedoch in Relation zur Länge der Prozesse, so lassen sich Verwaltungsprozesse im Vergleich zu anderen betrieblichen Domänen als linear charakterisieren.
3. *Gesetzesbindung:* das Verwaltungshandeln ist entweder gesetzlich geregelt oder zumindest von gesetzlichen Regelungen abhängig.
4. *Bilateralität:* eine Vielzahl von Verwaltungsprozessen kennzeichnet sich durch eine starke Einbindung des Kunden (Bürger/Unternehmen).
5. *Dezentralität:* viele Verwaltungsprozesse sind charakterisiert durch stark fragmentiertes, verteiltes Arbeiten,[5] das aus der Beteiligung diverser Organisationseinheiten innerhalb und außerhalb der einzelnen Verwaltungen resultiert.

3. Sicherheitstechnologien

Wichtig bei der Integration von Sicherheitsanforderungen ist es diese bereits bei der ersten Phase, beim Entwurf von Prozessen zu berücksichtigen. Sicherheitsrelevante Anforderungen sind nicht nur technischer Art sondern zB auch rechtlicher Natur. Jeder Prozess, kann entsprechend seiner Sicherheitsanforderungen klassifiziert werden[6], was sich in Folge bei den Umsetzungen auf entsprechende technische Maßnahmen positiv auswirkt. In der konzeptionellen Phase der Prozessmodellierung ist der De-

[5] *Lenk, K.* (1995) Business Process Reengineering. Sind die Ansätze der Privatwirtschaft auf die öffentliche Verwaltung übertragbar? In: Geschäftsprozesse in der öffentlichen Verwaltung. Neugestaltung mit Informationstechnik, *R. Traunmüller* (Ed), 27–43, Heidelberg.

[6] *Hof, S.* (2003) Security Aspects within e-Government. In: Proceedings of the DEXA 2003. 266–271, *R. Traunmüller* (Ed), Springer.

taillierungsgrad der notwendigen Sicherheitsmassnahmen nicht so groß wie im Implementierungsprozess. Entsprechende Sicherheitsdesigns sind erst in der Implementierungsphase relevant.

1. *Verschlüsselung:* die Verschlüsselung sollte, entsprechend der Klassifizierung der Daten, mit einem entsprechenden Standards geschützt werden.
2. *Authentifikation:* bei diesem Schritt werden Personen identifiziert zB mit Benutzername und Passwort oder mit Zwei-Faktoren-Authentifikation.
3. *Autorisierung:* die Autorisierung wird typischerweise nach der Phase der Authentifikation ausgeführt. Abhängig von den Benutzerberechtigungen der angemeldeten Personen, wird in diesem Mechanismus sichergestellt, dass ein Benutzer Zugang zu entsprechenden Applikationen erhält zB Rollenkonzepte.
4. *Zugriffskontrolle:* in Ableitung des Datenschutzes (zB einer Verschlüsselung) gibt es unterschiedliche Möglichkeiten die Zugriffskontrolle umzusetzen. Ist kein entsprechender Sicherheitsmechanismus implementiert, ist die Zugriffskontrolle einer der wichtigsten Mechanismen im Bereich Datensicherheit.
5. *Archivierung:* für die korrekte Durchführung der Archivierung ist es vor allem wichtig, dass auf lange Sicht Daten wiederhergestellt werden können.
6. *Backup:* anders als bei der Archivierung bezieht man sich beim Backup auf zeitliche relativ kurze Intervalle. Das Backup soll die Wiederherstellung der Daten im Falle eines Systemausfalles garantieren.

Die Integration sicherheitsnotwendiger Maßnahmen ist bis zu einem bestimmten Detaillierungsgrad für Prozessmodelle anwendbar. Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit sind nur die Basis auf der Sicherheitskonzepte aufbauen. Deshalb sollten schon bei der Modellierung auf fachkonzeptioneller Ebene bestimmte sicherheitstechnische Bereiche formuliert werden, ohne dabei bis im Detail festzulegen, wie sie in späterer Folge umgesetzt werden müssen. Gerade der Bereich der Verschlüsselung kann, ohne Berücksichtigung auf verwendeten Algorithmen oder Verfahrensweisen, schon bei der Prozessmodellierung einfließen. Die Prozessanalyse ist eine Möglichkeit ein besseres Verständnis für laufende Prozesse zu entwickeln und diese als zusätzlichen Punkt zB als Grundstein einer Sicherheitsbeurteilung nutzen. Die Analyse beinhaltet notwendige Fakten, die es den zuständigen Personen vereinfachen, ein bestimmtes Basiswissen für eine genaue Analyse der Sicherheitsaspekte der beschriebenen Prozesse zu erhalten[7].

[7] *Hübner, M.* (2001) Sicherheitsarchitekturen für elektronische Geschäftsprozesse. In: Elektronische Geschäftsprozesse, *P. Horster* (Ed), 64–74.

Aus Sicht der Sicherheit ist Interaktion genauso wichtig wie die Systemkomponenten selbst. Deshalb ist es nie ganz eindeutig. ob eine neu hinzugefügt Komponente nur sicherheitsrelevant oder auch (abhängig von ihren Verbindungen) andere Einflüsse auf das System in sich birgt.

Mit Hilfe anpassbarer Bemessungsgrundlagen des Sicherheitsdesigns ist es möglich, komplexe Sicherheitsstrukturen und Ansätze in eine gutes technisches Niveau abzubilden. So wird bei verschiedenen Teilen die Komplexität reduziert und die dadurch gewonnene geringer Komplexität lässt sich leichter abarbeiten. Mit der Kombination solcher Komponenten kann man ein holistisches Sicherheitsmodell aufspannen, das beliebig weiter kombinierbar ist. Ein so ausgeweitetes Sicherheitsschema verbindet die Prozessentwicklungsphase mit den entsprechenden Sicherheitsmechanismen.

4. Anforderungen an eine Modellierungsmethode im e-Government

Aus den domänenspezifischen Eigenschaften und den Eigenschaften der Modelladressaten lassen sich Anforderungen an Modellierungsmethoden im e-Government ableiten. Dies sind zunächst generelle Anforderungen, die auch außerhalb der Domäne e-Government Gültigkeit entfalten. Hierzu gehören die Faktoren *Einfachheit, hoher Formalisierungsgrad, Standardisierung des Modellinhalts, ganzheitliche Perspektive, Prozess-Controlling, Unterstützung von Prozess-Simulationen und Werkzeugunterstützung.*

Neben diesen generellen Anforderungen ergeben sich zum Zwecke der adäquaten Abbildung der domänenspezifischen Problemstruktur spezielle Anforderungen:

1. *Abbildung von Interaktionspunkten:* die Explikation des bilateralen Prozesses zwischen dem Kunden (Bürger/Unternehmen) und der Verwaltung sowie die Darstellung von Interaktionspunkten (in punkto Häufigkeit, Dauer etc) zwischen den Prozessbeteiligten dient der Analyse der Qualitätswahrnehmung der Verwaltungsdienstleistung durch den Kunden.
2. *Explikation der fragmentierten, dezentralen Prozessbearbeitung:* durch die Darstellung der Dezentralität der Arbeitsabläufe können im Rahmen eines Schnittstellenmanagements Prozessübergaben (in punkto Häufigkeit, Inhalt etc) gezielt analysiert und Optimierungspotenziale erschlossen werden.
3. *Multiperspektivische Darstellung:* es existiert eine Vielfalt von Modellnutzern (Bürgermeister, Bürger, Organisationsabteilung, Sachbearbeiter etc), welche die Prozessmodelle zu unterschiedlichen Zwecken

(Controlling, Organisations- oder Anwendungssystemgestaltung etc) und Befugnissen (Bürgermeister, Bürger etc) verwenden. Zur Reduzierung der Komplexität des dargestellten Sachverhalts sind durch die Modellierungsmethode Konfigurationsmechanismen zu unterstützen, die eine multiperspektivische Modelldarstellung ermöglichen.

Sicherheitsmechanismen einzuführen und einen bestimmten Grad an Sicherheit zu bewahren ist nicht einfach. Obwohl wir uns hauptsächlich auf die interne, administrative Sicht beschränken, ist die Anzahl der zu berücksichtigenden Probleme vielfältig. Zusätzlich erschwerend kommt hinzu, dass die inhärente Struktur im Bereich e-Government spezifische Risiken in sich birgt, die sowohl im Bereich der Technik als auch im sozialen Bereich zu finden sind:

1. *Multiple Sicherheitsstufen:* die verschiedenen Aufgaben von e-Government-Prozessen stellen verschiedene Anforderungen an den Grad, mit dem sie gesichert werden müssen. Neben Teilprozessen welche keine oder kaum sicherheitsrelevante Abläufe enthalten, gibt es andere Prozesse die im höchsten Masse sicherheitsrelevant sind.
2. *Perspektivenabhängige Sicherheitsmodellierung:* e-Government-Prozesse kennen verschiedene Nutzertypen. Diese verwenden die Prozessmodelle nicht zwangsweise für verschiedene Prozesse. Gewisse (Teil-) Prozesse werden von verschiedenen Nutzern geteilt. Dabei kann die notwendige Sicherheitsrelevanz in Abhängigkeit des Benutzers stark schwanken.
3. *Sicherheitsmechanismen:* e-Government-Umgebungen benötigen eine Vielzahl von technischen Sicherheitsmechanismen (Authentisierung, digitale Signatur, Verschlüsselung etc) sowie soziale und organisatorische Sicherheitsmassnahmen (Sicherheitsbewusstsein, Schulungen und Wiederherstellungsprozeduren).

All angeführten Mechanismen und Maßnahmen sollten vom Modell abgebildet werden können. Wenn man die entsprechenden Prozessbeschreibungen analysiert, wird deutlich, dass man die diversen Sicherheitsaspekte um so sorgfältiger in Augenschein nehmen sollte, je komplexer ein Prozess ist.[8] Basierend auf einer Prozessbeschreibung und den Interaktionen innerhalb der Administration kann man ein Schema der technischen Prozesskomponenten aufbauen. Einzig ein Prozessmodell, dass die entsprechenden Kriterien erfüllt, kann für Sicherheitsmodelle herangezogen werden.

[8] *Götz, B.* (2003) E-Governement mit der el. Signatur im Land Berlin, proc. of the D-A-CH Security 2003; *Hof, S.* (2003) E-Portals and Security. 251–258, In: Proceedings of the IDIMT 2003, *G. Chroust & C. Hofer* (Eds), Verlag R. Trauner.

5. Modellierung von Sicherheitsaspekten in e-Government-Prozessen

Die im Folgenden vorgestellte Modellierungsmethode soll den in Kapitel 4 formulierten Anforderungen genügen. Ihre Basis bildet die so genannte erweiterte ereignisgesteuerte Prozesskette (eEPK). Diese besteht aus zwei elementaren Komponenten: Ereignisse und Funktionen, dargestellt durch Sechsecke bzw durch abgerundete Rechtecke.[9] Eine eEPK beschreibt, welche Ereignisse welche Funktionen auslösen und welche Ereignisse von welchen Funktionen erzeugt werden. Ereignisse haben einen passiven Charakter und besitzen keine Entscheidungskompetenz. Sie stellen Zustände dar, auf die mit bestimmten Funktionen reagiert werden kann. Funktionen sind die aktive Komponente in einer eEPK. Sie führen die Transformation von Daten durch und haben Entscheidungskompetenz, dh in einer Funktion kann entschieden werden, welches Ereignis als Resultat eintritt. Verknüpft werden diese beide Elemente mit Konnektoren, die das „logische UND", das „logische ODER" oder das „logische disjunkte ODER" (entweder oder) darstellen können. Die eEPK ist Bestandteil der Architektur Integrierter Informationssysteme (ARIS). Diese Architektur bietet einen Bezugsrahmen zur Beschreibung von Geschäftsprozessen. Dabei wird ein hoher Strukturierungsgrad durch die unterschiedlichen Sichtweisen der Organisations, Daten, Funktions und Steuerungssicht erreicht. Die eEPK wird zur Modellierung der Steuerungssicht verwendet, mit welcher alle Sichtweisen vereinigt werden. Durch entsprechende Elemente/Symbole integriert die eEPK beispielsweise Informationen der Datensicht (zB durch das Dokumentsymbol) und der Organisationssicht (zB durch das Symbol der organisatorischen Einheit).

Unter Berücksichtigung der oben formulierten domänenspezifischen Anforderungen an eine Methode zur Geschäftsprozessmodellierung sind weitere Elemente zu ergänzen (vgl Tabelle A).

[9] *Becker, J. & Schütte, R.* (1996) Handelsinformationssysteme, Landsberg/Lech.

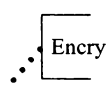
Name	Symbol	Definition
Interaktionspunkt		Interaktionspunkte beschreiben den Teil eines Prozesses, an dem eine Prozessübergabe zwischen Bürger und Verwaltung stattfindet oder an dem beide Parteien involviert sind.
Sicherheitslevel		Sicherheitslevel werden numerisch differenziert (1: niedrig, 2: mittel, 3: hoch). Sowohl Funktionen, Dokumente, Informationssysteme als auch Interaktionspunkte können in ihrem Sicherheitslevel beschrieben werden.
Sicherheitsmechanismus		Sicherheitsmechanismen können zur Gewährleistung eines bestimmten Sicherheitslevels angewendet werden.

Tabelle A: Informationsobjekterweiterungen

6. Fazit und Ausblick

Das Geschäftsprozessmanagement rückt zunehmend in den Fokus von e-Government-Projekten. Die im privaten Sektor entwickelten Methoden des Prozessmanagements sind jedoch häufig nicht direkt im Bereich der öffentlichen Verwaltung anwendbar, da die Spezifikationen der Domäne nur unzureichend berücksichtigt werden. Vor allem die Sicherheitsaspekte werden in der besonders wichtigen frühen Phase der Organisations- und Anwendungssystementwicklung nur unzureichend adressiert. Die im Kapitel 5 dargestellte Modellierungsmethode ist in der Lage, den formulierten Anforderungen zu begegnen.

Im Rahmen weiterer praktischer Projekte soll die präsentierte Modellierungsmethode angewendet und empirisch validiert werden. Derzeit erfährt sie im Rahmen eines e-Government Projekts auf kommunaler Ebene Anwendung, an dem zwei Kreisverwaltungen und fünf Stadt- und Gemeindeverwaltungen beteiligt sind. Die durch die umfassende Modellierung von sowohl verwaltungsinternen als auch verwaltungsübergreifenden Prozessen gewonnenen Erfahrungen werden als Feedback zur weiteren Verbesserung der Methode verwendet. Darüber hinaus werden derzeit Mechanismen zur Konfiguration von Prozessmodellen erarbeitet, welche die Tool-gestützte multi-perspektivische Darstellung unterstützen.