UNIVERSITÄT KOBLENZ · LANDAU
Institut für Wirtschafts- und Verwaltungsinformatik

Fachbereich 4 Informatik

IT-Sicherheitsanalyse von Geschäftsprozessen am Beispiel der Anwendungen “Kommunalwahlen” und “Geldauszahlung am Geldautomaten”

Rebecca Bindarra et al.

Nr. 4/2016

Arbeitsberichte aus dem Fachbereich Informatik

ausgelegt in:
Technische Informationsbibliothek Hannover, Bibliothek der Universität Köln, Deutsche Nationalbibliothek Frankfurt, Rheinische Landesbibliothek Koblenz, Universität Koblenz

Arbeitsberichte des Fachbereichs Informatik

ISSN (Print): 1864-0346
ISSN (Online): 1864-0850

Herausgeber / Edited by:

Der Dekan:
Prof. Dr. Lämmel

Kontaktdaten der Verfasser

Rebecca Bindarra, Lara Fiedler, Nico Merten, Sara West, Paulina Wojciechowska
Institut für Wirtschafts- und Verwaltungsinformatik
Fachbereich Informatik
Universität Koblenz-Landau
Universitätsstraße 1
D-56070 Koblenz
E-Mail:rbindarra@uni-koblenz.de, lfiedler@uni-koblenz.de, nmerten@uni-koblenz.de, swest@uni-koblenz.de, paulina.wojciechowska@uni-koblenz.de

IT-Sicherheitsanalyse von Geschäftsprozessen

am Beispiel der Anwendungen „Kommunalwahlen“ und „Geldauszahlung am Geldautomaten“

Forschungspraktikum

vorgelegt von

Rebecca Bindarra, Lara Fiedler, Nico Merten,
Sara West, Paulina Wojciechowska

Betreuung: Prof. Rüdiger Grimm; MSc. Daniela Simić-Draws, Forschungsgruppe IT-Risk-Management, Institut für Wirtschafts- und Verwaltungsinformatik, Fachbereich Informatik, Universität Koblenz-Landau

Koblenz, im September 2014

Vorwort

Die vorliegende Arbeit bildet den Abschluss eines Forschungspraktikums von Studierenden der Masterstudiengänge Informationsmanagement und Wirtschaftsinformatik unter Betreuung der wissenschaftlichen Mitarbeiterin Daniela Simić-Draws und von Prof. Dr. Rüdiger Grimm. Eine wesentliche Vorlage zu dieser Arbeit war ein Vorgehensmodell zur Sicherheitsanalyse von Geschäftsprozessen, das von D. Simić-Draws im Rahmen ihrer Dissertation erarbeitet wird und zu dessen laufender Verbesserung dieses studentische Forschungspraktikum wertvolle Hinweise liefern konnte. Als Anwendungsbeispiel wurden die sicherheitskritischen Prozesse „Kommunalwahl“ und „Geldauszahlung am Bankautomaten“ gewählt, weil die Arbeitsgruppe von Prof. Grimm in diesen beiden Anwendungen aus vorhergehender wissenschaftlicher Arbeit Erfahrung gesammelt hat. Insbesondere zum Anwendungsbeispiel „Kommunalwahl“ hatte sich dankenswerterweise das Ordnungsamt Koblenz, das für die Kommunalwahlen zuständig ist, unter aktiver Mithilfe ihres Leiters Dirk Urmersbach zur Zusammenarbeit angeboten, so dass dieser Geschäftsprozess wirklichkeitsnah untersucht werden konnte.

Naturgemäß sind studentische Arbeiten nicht auf demselben wissenschaftlichen Niveau wie Arbeiten erfahrener Wissenschaftler. Als Betreuer haben wir zwar darauf geachtet, dass die vorliegende Arbeit keine gravierenden Fehler enthält. Gleichwohl enthält sie noch einige Redundanzen und Lücken, die wir durch „Anmerkung der Betreuer“ in Fußnoten kenntlich gemacht haben. Wir sind dennoch der Meinung, dass es sich um eine nützliche Arbeit handelt, deren Ergebnisse aufgrund valider wissenschaftlicher Methoden als tragfähig angesehen werden kann. Wir hoffen, dass Anwender sie für ihre eigenen Prozessanalysen zur Stärkung der IT-Sicherheit nutzen können.

In diesem Sinne geben wir die Arbeit gerne an interessierte Kreise weiter und wünschen uns, dass sie einen guten Zweck zur Verminderung des IT-Risikos in sicherheitskritischen Anwendungen liefern wird. Rückmeldungen zur Arbeit nehmen wir gerne für die Verbesserung unserer Analysemethoden auf.

Koblenz, 22. November 2014

Daniela Simić-Draws und Prof. Dr. Rüdiger Grimm

Danksagung

Als Forschungsgruppe möchten wir uns für die Zusammenarbeit mit dem *Ordnungsamt* sowie der *Sparkasse Koblenz* bedanken. Durch das Bereitstellen von zum Teil internen Informationen konnten die Prozesse sehr viel genauer aufgenommen werden als wir das zu Anfang angenommen hatten. Mit diesem Wissen war es möglich die nachfolgende Analyse sehr viel detaillierter durchzuführen. Das Treffen Anfang Dezember im Ordnungsamt hat uns sehr geholfen, den doch sehr komplexen Wahlprozess nachzuvollziehen. Die Bereitschaft jederzeit Unklarheiten zu klären, haben wir sehr geschätzt. Vielen Dank noch einmal für Ihre Zusammenarbeit mit der Universität Koblenz-Landau.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

BPMN ..... Business Process Model and Notation

IKT ..... Informations- und Kommunikationstechnologie

JVA ..... Justizvollzugsanstalt

KGRZ ..... Kommunales Gebietsrechenzentrum

KWO ..... Kommunalwahlordnung

MAC ..... Message Authentification Code

MITM ..... Man-in-the-Middle

SW ..... Software

Glossar

Aktivität Eine Aktivität beschreibt eine Aufgabe innerhalb eines Geschäftsprozesses.

Arbeitsgruppe Zusammenschluss von mindestens vier Wahlhelfern, die gemeinsam einen Stimmbezirk auszählen.

Auszählungssoftware Die Auszählung der Stimmen sowie die Feststellung der Wahlergebnisse können mit der Unterstützung einer elektronischen Datenverarbeitung (elektronische Auszählungssoftware) erfolgen. Dies ist im Kommunalwahlgesetz verankert. Die Voraussetzungen für die Zulassung sowie die Verwendung der elektronischen Auszählungsgeräte regelt die Kommunalwahlordnung (KWO) in ihrem §§ 55 a und 55 b umfassend.

Black Box Die Aktivitäten eines Pools oder einer bestimmten Lane wurden nicht ausmodelliert und bleiben so dem Betrachter verborgen. Das Ziel einer Black Box ist es, das Zusammenspiel verschiedener Lanes zu verdeutlichen.

Kommunalwahlordnung Die KWO bildet die rechtliche Grundlage zur Durchführung der Kommunalwahl. Diese definiert Rollen- und Aufgabenverteilung innerhalb des Wahlprozesses.

Kontrolldatenblatt Ein Dokument, welches dem Abgleich der Daten dient.

Lane Lanes sind Modellierungskonstrukte in der BPMN, die eine Unterteilung eines Pools verschiedene Rollen erlauben.

Man-n-he-Middle-Angriff Bei diesem Angriff täuscht ein böswilliger Dritter, der die Kommunikationsflüsse zwischen zwei oder mehreren Kommunikationspartnern kontrolliert, zwei Kommunikationspartner, indem er

	ihnen jeweils die Identität des anderen vorspiegelt.
Mehr-Augen-Prinzip	Beim Mehr-Augen-Prinzip wird das Treffen einer Entscheidung bzw. die Durchführung einer Tätigkeit von mehreren Personen ausgeführt. Eine andere Form dessen ist die mehrfache Kontrolle einer Tätigkeit durch unabhängige Personen.
Message Authentification Code (MAC)	MAC ist ein Datensicherungscode. Er wird auf Schlüsseln angewendet um eine kryptografische Prüfsumme für die Integrität und Authentizität von Nachrichten zu bilden. Veränderungen der Nachricht werden dadurch direkt erkannt, wodurch der MAC-Code auch zur Fehlererkennung benutzt wird.
PC-Wahl	PC-Wahl ist ein modulares Softwarepaket für die Erfassung, Berechnung, grafische Präsentation, Meldung und statistische Nachbereitung von Wahlergebnissen. Die Software ist das meistgenutzte Wahlorganisationssystem in deutschen Verwaltungen.
Pool	Pools sind Modellierungskonstrukte in der BPMN. Hierbei repräsentiert ein Pool einen Benutzer, eine Benutzerrolle oder ein System im Modell.
Signatur	Die Signatur ist ein (strukturierter) Datensatz, der mit elektronischen Informationen verknüpft ist. Anhand dieses Datensatzes kann der Unterzeichner bzw. Ersteller der Signatur identifiziert und authentifiziert werden. Bildlich gesprochen handelt es sich um ein Siegel zu digital vorliegenden Daten, dass mit einem privaten Signaturschlüssel erzeugt wurde.
Stimmbezirk	In Koblenz darf ein Stimmbezirk nicht mehr als 2500 Einwohner umfassen. Die Abgrenzung der Stimmbezirke in einer Gemeinde ist so vorzunehmen, dass sie den Wahlberechtigten die Wahlteil-

nahme erleichtert. Größere Einrichtungen wie Altenheime oder auch Gefängnisse mit einer hohen Anzahl an Wahlberechtigten bilden Sonderstimmbezirke.

Use-Case Use-Case, auch Anwendungsfall genannt, ist die schematische Darstellung möglicher Szenarien. Es skizziert inhaltlich den Versuch einer bestimmten Zielerreichung, sowie mögliche Ergebnisse dieser Lösungswege.

Vier-Augen-Prinzip Ein Vier-Augen-Prinzip verhindert, dass kritische Tätigkeiten oder Entscheidungen von einer Person durchgeführt werden. Zwei Personen entscheiden bei einem Vier-Augen-Prinzip gemeinsam bzw. führen wichtige Tätigkeiten durch. Damit wird das Risiko von Fehlern bzw. Manipulationen reduziert. Das Vier-Augen-Prinzip ist eine Sonderform des Mehr-Augen-Prinzips.

Wahlausschuss Zu jeder Wahl erfolgt die Bildung eines Wahlausschusses. Dieser setzt sich aus 4 oder 6 Beisitzern, einem Schriftführer und dem Vorsitzenden zusammen. Den Vorsitz führt der Oberbürgermeister. Es sei denn, er steht selbst zur Wahl. In diesen Fällen führt den Vorsitz der Bürgermeister. Aufgabe des Wahlausschusses ist die Zulassung der eingereichten Wahlvorschläge, die Feststellung des amtlichen Endergebnisses und die evtl. notwendig werdende Festsetzung eines Wahltermins für eine Stichwahl.

Wählerverzeichnis Für jeden Stimmbezirk erstellt die Verwaltung ein Wählerverzeichnis. Darin aufgelistet sind die Wahlberechtigten mit Familienname, Vorname, Geburtstag und Anschrift. Als Grundlage dient das Wählerverzeichnis aus der vorangegangenen Wahl. Die vorzunehmenden Änderungen werden aus dem Melderegister bezogen. Die Erstellung des Wählerverzeichnisses erfolgt in der Software PC-Wahl. Nach Abschluss des Wählerverzeichnisses ist dieses auszudrucken, da es zur Überprüfung der Wahlberech-

tigten im Wahllokal benötigt wird.

1. Einleitung

Bei der vorliegenden Arbeit handelt es sich um einen Abschlussbericht des Forschungspraktikums Delta, welcher sich mit der Evaluierung des PrOSA-Vorgehensmodells[1] (Prozessorientierte Sicherheitsanalyse) anhand von zwei Geschäftsprozessen auseinandersetzt. Mithilfe des Vorgehensmodells, welches von Daniela Simić-Draws im Rahmen ihres Promotionsvorhabens entwickelt wurde, lassen sich IT-Sicherheitsanforderungen ermitteln. Die Grundlage dafür wird durch Geschäftsprozesse geschaffen, die in der Realität vorkommen (Simić-Draws, 2013, S.3).

1.1. Problemstellung

In den letzten Jahren konnten viele Veränderungen in unserer Gesellschaft beobachtet werden. Unter anderem hat sie sich von einer Produktions- über Dienstleistungs- bis hin zu einer Informationsgesellschaft entwickelt (Hopf, 2009, S.1). Aus diesem Grund haben neue Aspekte, z.B. Informationen als ein zusätzlicher Produktionsfaktor, eine wichtige Rolle in vielen Bereichen des täglichen Lebens eingenommen. Dazu zählt z.B. die Informationstechnologie, die gegenwärtig sowohl die privaten als auch geschäftlichen Beziehungen dominiert (Eckert, 2013, S.3). Mit Hilfe von IT lassen sich beispielsweise innerbetriebliche sowie zwischenbetriebliche Kommunikation effizienter gestalten, wodurch unter anderem die Geschäftsabwicklung schneller erfolgen kann. Die Integration von solchen Technologien bringt aber auch viele Gefahren mit sich (Schmidt, 2009, S. 1) - die IT-Systeme werden immer komplexer, so dass sie anfälliger für Manipulationen und Fehler werden. Die Vernetzung von IT-Systemen untereinander sowie die Dynamik bei der IT-gestützten Bearbeitung von Geschäftsprozessen nehmen ständig zu. Diese beiden Aspekte zeigen Potenziale auf: Ein Beispiel hierfür ist die Umsetzung der Geschäftsprozesse. Diese erfolgen durch den Einsatz von IT schneller und effizienter. Dadurch können z.B. Kosten sowie Produktionszeiten gesenkt werden. Gleichzeitig entstehen jedoch mit diesen beiden Aspekten ein erhöhtes Fehlerpotenzial sowie ein Raum für Missbrauch (Simić-Draws, 2013, S.2). Unter anderem unterliegen die IT-Systeme in besonderer Weise unautorisierten, meist anonymen, Zugriffsversuchen. Die Angreifer (z.B. Cracker)

[1] Anm. der Betreuer: Das Vorgehensmodell beschreibt die Durchführung von Sicherheitsanalysen und die damit verbundene Herleitung von Sicherheitsanforderungen auf Basis von (Geschäfts-)Prozessen. Hierbei wird insbesondere der am Prozess beteiligte Mensch sowohl als Sicherheitsrisiko, als auch als Wissens- und Sicherheitsträger berücksichtigt. Das Vorgehensmodell ist Gegenstand der Dissertation von D. Simić-Draws und lag während des Forschungspraktikums in einer noch nicht finalisierten Version vor.

möchten sich durch die gelungene Zugriffsversuche rechtswidrige Vorteile verschaffen oder der Organisation, welche über das angegriffene IT-System verfügt, Schaden hinzufügen. Die gegenwärtigen Entwicklungen haben somit sowohl einen positiven als auch einen negativen Einfluss auf alle Lebensbereiche, z.B. viele Prozesse können schneller und effizienter abgewickelt werden. Gleichzeitig ist das Eintrittsrisiko wirtschaftlicher oder personeller Schäden, die durch Vertraulichkeitsverletzungen, Manipulationen oder auch Störungen der Verfügbarkeit von Diensten der Unternehmen verursacht werden können, sehr hoch (Simić-Draws, 2013, S.2). Die Höhe gegenwärtiger Risiken kann daher nicht mit der Vergangenheit verglichen werden (Eckert, 2013, S.3). Für die Risikominimierung bzw. -beseitigung wird der IT-Sicherheit eine Schlüsselrolle zugeschrieben (Grimm et al., 2014, S.1). Ihre Aufgabe besteht in dem Schutz der Organisationen und deren Werte vor Bedrohungen, die sich z. B. aus technischen Schwachstellen ergeben. Um das zu verwirklichen werden besondere Maßnahmen eingesetzt, durch welche die identifizierten Bedrohungen soweit ausgeschlossen sind, dass das verbleibende Risiko akzeptiert werden kann (Grimm et al., 2014, S.1). Durch diese Ausführung wird deutlich, dass keine hundertprozentige Sicherheit bestehen kann. Vielmehr verbleibt immer ein Restrisiko, welches jedoch geduldet werden kann.

Die IT-Sicherheit spielt darüber hinaus eine wichtige Rolle bei der Umsetzung rechtlicher Vorgaben. Die nachfolgenden Ausführungen beleuchten dies und zeigen, wie die IT-Sicherheit durch gesetzliche Regelungen in eine Organisation verankert wird. Vor ungefähr zwanzig Jahren agierten Unternehmen ohne Corporate-Governance-Richtlinien, d.h. es gab keine angemessene interne Kontrolle von organisatorischen Vorgängen. In einigen großen Unternehmen wurden somit bewusst wirtschaftliche Risiken akzeptiert. Dies hat zur Folge, dass Anleger mit großen Kapitalverlusten konfrontiert wurden. Unter anderem trat im Mai 1998 das Gesetz zur Kontrolle und Transparenz im Unternehmen (KonTraG) in Kraft, um eine bessere Überwachung der Unternehmensführung zu verschaffen (Martin, 2002, S. 14). Zudem wurden die Unternehmen verpflichtet ein Risikofrüherkennungssystem zur Erkennung von bestandsgefährdeten Risiken einzuführen. Des Weiteren wurde im Juli 2002 ein US-Bundesgesetz (Sarbanes-Oxley Act) erlassen, welches auch für Tochterunternehmen amerikanischer Gesellschaften im Ausland und nicht-amerikanische Firmen gelten, welche an amerikanischen Börsen gehandelt werden (Frugier, 2009, S. 3). Dabei wurde das Ziel verfolgt, verlorengegangenes Vertrauen der Anleger in die veröffentlichten Bilanzdaten von amerikanischen Unternehmen wiederherzustellen. Diese und weitere Richtlinien und Gesetze thematisieren den angemessenen Umgang mit technisch bedingten Risiken, wodurch auch die IT-

Sicherheit ins Spiel kommt. Als Beispiel kann folgende Situation genannt werden: Eine einwandfreie Berichterstattung ist nur durch erprobte und verlässliche IT-Prozesse und einen angebrachten Schutz der verwendeten Daten möglich, was durch die IT-Sicherheit und ihre Maßnahmen möglich ist (Hoffmann, 2010, S. 5). Somit wird deutlich, dass durch die IT-Sicherheit die Abläufe abgesichert werden können. Mit unternehmensinternen Corporate Governance-Richtlinien wird die IT-Sicherheit eines Unternehmens auf organisatorischer Ebene geregelt. Mit deren Hilfe soll das durch das Unternehmen geplante IT-Security-Management umgesetzt werden. Durch die nachhaltige Kontrolle des Unternehmens wird die Vertrauensbasis für Kunden, Mitarbeiter und andere Stakeholder verbessert. Aus diesem Grund nehmen unbeteiligte Dritte solch ein Unternehmen als seriös und vertrauenswürdig wahr. Die Fremdkapitalgeber können somit ermutigt werden, in das Unternehmen zu investieren.

Während sich die IT-Sicherheit auf die Absicherung der Abläufe konzentriert, befasst sich die IT-Sicherheitsanalyse mit Beschreibung eines Vorgehensmodells, welches zur Bewertung und Optimierung der Sicherheit von IT-Systemen geeignet ist (Simić-Draws, 2013, S.2). Diese Vorgehensmodelle werden in Kapitel 2 erläutert. Im Fokus dieser Modelle können konkrete IT-Systeme oder z.B. ein Teil von ihnen stehen. Die etablierten Vorgehensweisen betrachten jedoch nicht alle wichtigen Faktoren, die für eine Sicherheitsanalyse notwendig sind: Z.B. Interessenkonflikte zwischen Menschen, die miteinander sowie mit beteiligten IT-Systemen zusammenarbeiten (Simić-Draws, 2013, S.2). Zudem betrachten sie nicht die IT-Systeme in Bezug auf die Geschäftsprozesse, in denen sie eingesetzt werden. Es ist vor allem dann als Herausforderung anzusehen, wenn der gesamte Prozess vor Missbrauch und Angriffen abgesichert werden soll (Simić-Draws, 2013, S.2). Um diese Lücke zu schließen, wurde das PrOSA-Vorgehensmodell entwickelt (Simić-Draws, 2013, S.2). Eine genaue Beschreibung des Modells befindet sich in Kapitel 3. Bis jetzt wurde es jedoch noch nicht in der Praxis getestet.

Der vorliegende Abschlussbericht untersucht das entwickelte PrOSA-Vorgehensmodell, das Abläufe innerhalb von und zwischen IT-Systemen und beteiligten Anwendern abzusichern versucht (Simić-Draws, 2013, S.2). Dafür leitet es die IT-Sicherheitsanforderungen auf Grundlage von vorhandenen Geschäftsprozessen ab. Die Forschungsinhalte der Untersuchung konzentrieren sich auf die Betrachtung zweier Geschäftsprozesse, welche nach dem beschriebenen Ablauf des Vorgehensmodells bearbeitet werden. Ziel des Forschungspraktikums war es, eine erste Evaluation des Vorgehensmodells durchzuführen, damit es in einer weiteren Iteration verbessert werden kann.

1.2. Entstehung der Arbeit

Die vorliegende Arbeit entstand im Rahmen des *Forschungspraktikums Delta,* welches im WS 2013/2014 an der Universität Koblenz durchgeführt wurde. Im Vordergrund stand hier die praktische Überprüfung des PrOSA-Vorgehensmodells anhand zweier Geschäftsprozesse. Das Vorgehensmodell wurde im Rahmen des Promotionsvorhabens von Daniela Simić-Draws entwickelt. Es strebt die Ermittlung von IT-Sicherheitsanforderungen auf Basis von Geschäftsprozessen an. Das PrOSA-Vorgehensmodell untersucht und sichert die Abläufe innerhalb von und zwischen IT-Systemen (Protokolle, Daten) sowie den beteiligten Anwendern (Kommunikation, Datenaustausch) ab. Dabei spielen die Abbildung der Realität im IT-System sowie mögliche rückkoppelnde Effekte eine Schlüsselrolle (Simić-Draws, 2013, S.2). Um den IST-Zustand eines Geschäftsprozesses zu erfassen, wird der Top-Down-Ansatz verwendet (Schmidt, 2009, S.3). Davon ausgehend wird die Sicherheitsanalyse vorgenommen. Der Top-Down-Ansatz geht von abstrakten und allgemeinen Sachverhalten aus und geht hin zu speziellen untergeordneten Gegebenheiten (Sesselmann/Schmelzer, 2003, S.17). Als Ergebnis werden die Sicherheitsanforderungen formuliert sowie Maßnahmen implementiert, welche zu einem verbesserten, bezogen auf die IT-Sicherheit, Geschäftsprozess führen.

Die IT-Sicherheit, wie es im Rahmen dieser Arbeit verstanden wird, steht an der Schnittstelle zwischen Technik, Ökonomie und Recht. Der Abschlussbericht kann als Beitrag zu der Schließung bestehender Lücken von existierenden Methoden zur Anforderungserhebung verstanden werden. Das kann dadurch begründet werden, dass das PrOSA-Vorgehensmodell, welches im Rahmen dieser Arbeit das erste Mal evaluiert wird, auf die Schließung solcher Lücken abzielt. Einerseits werden in der Arbeit die Stärken und andererseits die Verbesserungspotenziale des Vorgehensmodells aufgezeigt. Daraus können Hinweise für die Weiterentwicklung bzw. Optimierung des Vorgehensmodells abgeleitet werden. Zudem wird ein Beitrag für die Praxis geleistet, da überprüft wird, ob das Vorgehensmodell sowohl von fachlicher als auch operativer Ebene einer Organisation verwendet werden kann.

1.3. Ziele der Arbeit

Die vorliegende Arbeit bietet einen Einblick in die Dokumentation des *Forschungspraktikums Delta,* das sich mit der Evaluierung des PrOSA-Vorgehensmodells befasst hat. Es soll untersucht werden, ob das Vorgehensmodell auch in der Praxis angewendet werden kann bzw. ob es zu dem gewünschten Endergebnis führt. Dies umfasst die Ermittlung von IT-Sicherheitsanforderungen auf Basis ausgewählter und untersuchter Geschäftsprozesse. Zudem

soll festgestellt werden, ob Verbesserungspotenziale für das Vorgehensmodell bestehen. Die durch das Vorgehensmodell vorgegebene geschäftsprozessorientierte Sicht ermöglicht die Untersuchung der menschlichen Akteure, die an dem Prozess beteiligt sind. Diese Untersuchung bezieht sich auf mögliche Angriffsmotive und den daraus resultierenden Angriffsmöglichkeiten. Zur Durchführung der Untersuchung wurden zwei Prozesse ausgewählt. Hierbei handelt es sich zum einen um die *Kommunalwahlen in Koblenz* und zum anderen um die *Auszahlung von Geld am Geldautomaten.*

Bei dem ersten Prozess handelt es sich um die Vorbereitung und Durchführung der Kommunalwahlen am 25.05.2014 in Koblenz. Die Erhebung des Prozesses wurde in enger Zusammenarbeit mit dem Ordnungsamt Koblenz – Abteilung Wahlen – vorgenommen. Motivation zur Kooperation bestand von beiden Seiten: Das Ordnungsamt erhoffte sich durch die Prozesserhebung eine transparentere Darstellung des Wahlablaufs. Für die Arbeitsgruppe IT-Risk-Management – die das Forschungspraktikum betreute – ist die Untersuchung eines Wahlprozesses aufgrund des Forschungsschwerpunkts eVoting von Interesse gewesen. Darüber hinaus sprechen noch einige andere Faktoren für die Untersuchung des Wahlprozesses: Des Weiteren ist die IT-Unterstützung in diesem Prozess zunächst (für der Wähler) nicht ersichtlich. Außerdem sind an dem Prozess viele Akteure beteiligt, wodurch die Gefahr der Manipulation des Prozesses entsteht.

Der zweite Prozess, der im Rahmen des Forschungspraktikums untersucht wird, ist die Auszahlung von Geld am Geldautomaten. Hierfür wurde der Geldautomat am Campusgelände untersucht. Der Prozess wurde als Untersuchungsgegenstand herangezogen, weil hier eine umfassende elektronische Unterstützung vorhanden ist. Zudem ist eine direkte Partizipation am Prozess möglich, d.h. die Teammitglieder konnten an dem Prozess persönlich beteiligt sein. Des Weiteren ist die Motivation für Betrug seitens des Anwenders hoch: Dieser fühlt sich nicht beobachtet und kann durch den Betrug an das Geld aus dem Automaten gelangen.

Vor dem Hintergrund dieser Zielsetzung wendet sich die vorliegende Arbeit an Leser aus dem wissenschaftlichen Umfeld, die sich mit der IT-Sicherheitsanalyse von Organisationen befassen. Die folgenden Fragen werden in dem Abschlussbericht beantwortet:

- Inwiefern kann das PrOSA-Vorgehensmodell für die Ermittlung von IT-Sicherheitsanforderungen in der Praxis eingesetzt werden?
- Welche Verbesserungsvorschläge können für PrOSA- Vorgehensmodells aufgrund der Evaluierung gemacht werden?

Der Abschlussbericht liefert den Wissenschaftlern erste Erkenntnisse und erste Antworten auf die vorgestellten Fragen.

1.4. Vorgehen und Aufbau

Die vorliegende Arbeit orientiert sich hauptsächlich an den Schritten des PrOSA-Vorgehensmodells. Das zweite Kapitel befasst sich mit den bekannten Vorgehensweisen, welche für die IT-Sicherheitsanalyse geeignet sind. Des Weiteren wird in Kapitel 3 ein Überblick über die Struktur und Inhalte des PrOSA-Vorgehensmodells gegeben. In Kapitel 4 wird die Notationssprache BPMN näher beschrieben, d.h. es wird erläutert, wie die Spezifikationssprache funktioniert und wie Geschäftsprozesse und Arbeitsabläufe mit deren Hilfe modelliert und dokumentiert werden können. Wie schon in Kapitel 1.1 erläutert wurde, spielen die IT-Systeme in allen Bereichen der Informationsgesellschaft eine wichtige Rolle. Neben steigenden Anforderungen nach Leistungsfähigkeit dieser Systeme steigen auch die Forderungen nach Sicherheit und Vertrauenswürdigkeit. Das Kapitel 5 setzt sich mit den Sicherheitsanforderungen auseinander, wobei diese ausführlich erläutert werden. Nach diesen Kapiteln wird der theoretische Teil der Arbeit abgeschlossen, welcher dem Leser grundlegende Informationen vermittelt, die zum Verständnis der Arbeit wichtig sind. Im Anschluss daran folgt der praktische Teil der Arbeit. Der Schwerpunkt im Kapitel 6 liegt auf dem ersten, untersuchten Geschäftsprozess, d.h. die Durchführung der Kommunalwahl in Koblenz. Aufgrund des Prozessumfangs, fand eine Zerlegung in die vier Teilprozesse der Wahlvorbereitung, der Stimmabgabe, der Stimmauszählung sowie der Wahlnachbereitung statt, welche in Form von BPMN-Diagrammen dargestellt wurden. Um an die Prozesserfassung systematisch herangehen zu können, werden die Use-Case-Beschreibungen eingesetzt, welche dazu dienen, alle Rollen und Anwendungsfälle sichtbar zu machen und detailliert zu beschreiben. Dadurch wird es möglich, einen genauen Einblick in den Prozess zu gewinnen und somit ein Verständnis für die Thematik des Wahlprozesses und die damit verbundene Komplexität zu gewinnen. Jeder Unterprozess besteht aus einer Reihe zusammenhängender Aktivitäten. Ausgehend von den einzelnen Aktivitäten werden Sicherheitsanforderungen abgeleitet. Hierbei besteht die Notwendigkeit zu überprüfen, ob die ermittelten Sicherheitsanforderungen widerspruchsfrei sind. Des Weiteren wird eine Analyse der Interessenkonflikte durchgeführt, welche als Ausgangspunkt für mögliche Bedrohungen gelten. Als nächstes findet die Konsistenzprüfung statt. Um das Vorgehen kurz zusammenfassen zu können, kann folgendes festgehalten werden: In der vorliegenden Arbeit ermöglicht PrOSA-Vorgehen eine Sicherheitsanalyse ausgehend von

Geschäftsprozessmodellen (BPMN). Die Geschäftsprozesse werden zerlegt, damit einzelne Handlungsabläufe sichtbar werden. Wenn die atomaren Elemente (Aktivitäten) vorliegen, wird die eigentliche Analyse durchgeführt. Dabei werden die verschiedenen Interessenlagen berücksichtigt, da sie als Grundlage für mögliche Interessenkonflikte gelten. Hierbei werden Sicherheitsanforderungen abgeleitet, die beim Wiederzusammensetzen des Prozesses auf Widerspruchsfreiheit geprüft werden. Kapitel 7 schließt mit einem kurzen Zwischenfazit die Fertigstellung des ersten Geschäftsprozesses ab. Hierbei wird das Vorgehen kritisch betrachtet und festgelegt, ob der zweite Prozess nach dem gleichen Vorgehensschema untersucht wird. In Kapitel 8 wird der zweite zu untersuchende Prozess behandelt: Auszahlung von Bargeld an einem EC-Kartenautomaten. Zunächst wurden Use-Cases und ein BPMN Modell erstellt. Nachdem das geschehen ist und die einzelnen Aktivitäten ersichtlich wurden, konnte die eigentliche Analyse durchgeführt werden. Anhand der Erkenntnisse aus Prozess 1 wurde das Vorgehensmodell für Prozess 2 geändert. Da dieser Prozess weniger umfangreich ist, war es nicht notwendig diesen in mehrere Teilprozesse zu unterteilen. Kapitel 9 schließt mit einem Fazit ab, in welchem auf die Ergebnisse sowie auf weitere Implikationen für Forschung und Praxis eingegangen wird.

2. Related Work[2]

In diesem Kapitel werden verschiedene Vorgehensmodelle vorgestellt, die für die Durchführung einer IT-Sicherheitsanalyse geeignet sind. Die Sicherheitsanalyse bezieht sich dagegen auf ein Vorgehensmodell, welches sich mit der Bewertung und Optimierung der Sicherheit eines IT-Systems befasst (Grimm et al., 2014, S.2). Wann die einzelnen Vorgehensmodelle zum Einsatz kommen, hängt im Wesentlichen von dem Fokus der Analyse ab. Die Analyse kann sich beispielsweise auf ein konkretes IT-System oder aber nur auf einen Teil davon beziehen. Die etablierten Verfahren nehmen dabei verschiedene Sichten auf die IT-Sicherheitsanalyse ein:

- organisatorische Sicht
- produktorientierte Sicht
- rechtliche Sicht

[2] Anm. der Betreuer: Dieses Kapitel ist methodisch nicht so rigoros ausgeführt, wie es die Wissenschaft verlangt. Einerseits fehlen einige Quellenverweise, andererseits werden Internetquellen verwendet, ohne dass ihre Qualität festgestellt wurde. URLs sind nicht mit dem Datum ihrer letzten Prüfung versehen (gilt als formaler Zitierfehler).

Nachfolgend werden die drei Sichten und die dazugehörige Verfahren, welche am weitesten verbreitet sind, vorgestellt.

2.1. Organisatorische Sicht

Die organisatorische Sicht liefert eine umfassende Untersuchung der IT-Sicherheit (Simić-Draws, 2013, S. 2). Dies wird sichergestellt, indem die in einem Unternehmen verwendeten IT-Systeme und deren Infrastruktur sowie beteiligten Akteure analysiert werden. Nachfolgend werden zwei Verfahren beschrieben, welche dieser Sicht zugeordnet werden können.

ISO 27001

ISO 27001 ist ein internationaler Standard innerhalb der Informationstechnik. Diese Norm spezifiziert die Anforderungen eines Informationssicherheits-Managementsystems und beschreibt wie Informationssicherheit im gesamten Unternehmen gewährleistet werden kann. Die letzte Revision dieser Norm wurde 2013 veröffentlicht. Die vollständige Beschreibung des Standards lautet ISO/IEC 27001:2013.

Der Standard dient zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der Informationen. Der grobe Vorgang innerhalb einer Organisation zur Einhaltung des Standards ist die Definition potentieller Probleme im Zusammenhang mit Informationen, wie z.B. eine Risikoeinschätzung. Des Weiteren wird festgestellt, welche Maßnahmen im Unternehmen zur Vermeidung der möglichen Probleme unternommen werden müssen. Ein Beispiel hierfür ist eine Risikominderung oder Risikobehandlung. Generell bestehen die Sicherheitsmaßnahmen innerhalb ISO 27001 aus Richtlinien, Verfahren und technischen Umsetzungen. Durch die Umsetzung des Standards werden in der Regel organisatorische Regeln im Unternehmen festgelegt, um Sicherheitslücken zu vermeiden[3].

Die Vorteile für ein Unternehmen sind, dass

- Gesetzliche Vorschriften einfacher eingehalten werden. Insbesondere durch den Zuwachs von Vorschriften werden diese automatisch mit Hilfe von ISO 27001 umgesetzt.
- Ein Wettbewerbsvorteil gegenüber anderer Unternehmen vorherrscht. Durch eine Zertifizierung fühlen sich Kunden sicherer.

[3] Quelle: http://www.iso27001standard.com/de/was-ist-iso-27001/

- Niedrigere Kosten vorhanden sind. Störanfälle innerhalb der Organisation werden vermieden.
- Eine bessere Organisation vorherrscht. Prozesse werden schriftlich festgehalten und dadurch Leerlaufzeiten der Mitarbeiter vermieden.

Diese Vorgehensweise wird ausführlich vom Bundesamt für Sicherheit in der Informationstechnik zu ISO 27001 Zertifizierung auf Basis von IT-Grundschutz beschrieben[4]. Als weiterführende Literatur bzw. Quellen wäre die Internetseite des TÜV Süd[5] zu nennen.

IT-Grundschutz

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) geht von der Annahme aus, dass Informationen als schützenswerte Güter für Unternehmen und Behörden anzusehen sind. Der angemessene Umgang mit Informationen wird genauso wichtig wie die Sicherheit und Zuverlässigkeit der Informations- und Kommunikationstechnik (IKT) erachtet. Die Wichtigkeit des letzten Punktes liegt vor allem daran, dass IKT immer wichtiger z.B. für die Informationsvermittlung ist. Wenn diese beiden Aspekte vernachlässigt werden, können sie zu einem Risikofaktor für die Existenz der Organisation werden. Aus diesem Grund verweist das BSI auf Verstärkung des Informationsschutzes sowie der Sicherung der IT.

Dafür wird seit einigen Jahren das Vorgehen nach IT-Grundschutz zusammen mit IT-Grundschutz-Katalogen des BSI angeboten, welches sich mittlerweile als Standard etabliert hat. Es kann als ganzheitliches Konzept für Informationssicherheit angesehen werden. Diese etablierte Methode hilft bei dem Aufbau von einer Sicherheitsorganisation und dient als Grundlage für Bewertung von ermittelten Risiken. Darüber hinaus lässt sich damit das vorhandene Sicherheitsniveau feststellen sowie die geeignete Informationssicherheit umsetzen. Die genannten IT-Grundschutz-Kataloge sind für viele Organisationen Vorbilder für ihre eigenen zu entwickelnden Maßnahmenkataloge. Mithilfe des IT-Grundschutzes lassen sich die möglichen Schäden verhindern und das Risiko minimieren. Hierfür werden organisatorische, personelle, infrastrukturelle und technische Standard-Sicherheitsmaßnahmen miteinander kombiniert. Das dadurch erreichte Sicherheitsniveau ist für den normalen Schutzbedarf angemessen und ausreichend, um die relevante Informationen zu schützen. Um das Gebiet der

[4] Quelle: https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Uebersicht/uebersicht_node.html
[5] Quelle: http://www.tuev-sued.de/management-systeme/it-dienstleistungen/iso-27001

IT besser aufgliedern und aufbereiten zu können, folgt der IT-Grundschutz einem Baukastenprinzip: Die Teilbereiche (z.B. Notfall-Management, Client-Server-Netze) bilden die täglichen Abläufe und Einsatzorte der IT ab. In jedem Teilbereich wird zunächst die aktuelle Lage hinsichtlich der Bedrohungen beschrieben (Risikoanalyse). Dieser Schritt gilt als Grundlage für die Ableitung spezifischer Sicherheitsmaßnahmen. Anschließend wird das verbleibende Restrisiko evaluiert. Der IT-Grundschutz kann als ein Soll-Ist-Vergleich zwischen den bereits umgesetzten Sicherheitsmaßnahmen und den von den IT-Grundschutz-Katalogen vorgeschlagenen Maßnahmen verstanden werden. Defizite werden aufgezeigt, indem die noch nicht realisierten, aber empfohlenen Maßnahmen identifiziert werden. Diese sollen auch schnellstmöglich verwirklicht werden. Der IT-Grundschutz macht es für jede Organisation möglich, ein geeignetes Sicherheitskonzept einfach auszuarbeiten.

Diese Vorgehensweise wurde ausführlich in einem Leitfaden zu Informationssicherheit des Bundesamts für Sicherheit in der Informationstechnik beschrieben (BSI, 2012).

2.2.Produktorientierte Sicht

Die produktorientierte Sicht bezieht sich auf ein konkretes IT-Produkt (Simić-Draws, 2013, S. 2). Durch Verfahren wie z.B. Common Criteria, Pentesting sowie spezifische Standards für einzelne Kryptographie-Verfahren ist eine vollständige Untersuchung der betrachteten IT-Produkte möglich. Nachfolgend werden die genannten Vorgehensweisen erläutert.

Common Criteria

Common Criteria for Information Technology Security Evaluation (kurz CC) ist ein internationaler Standard der Bewertung und Zertifizierung der Sicherheit von Computersystemen. Der Schwerpunkt hierbei liegt insbesondere bei der Datensicherheit[6]. CC setzt sich aus standardisierten Kriterien für skalierbare, unabhängige und weltweit anerkannte Sicherheitsprüfungen für IT Produkte zusammen. Evaluiert werden dabei beispielsweise Betriebssysteme, Rechnernetze, verteilte Systeme oder Anwendungen, aber auch Hardware wie Kartenleser.

Insgesamt besteht die CC aus drei Teilen:

Teil eins ist die Einführung in die Vorgehensweise nach CC und beschreibt das allgemeine Modell: Die Grundlagen der IT-Sicherheitsevaluierung und der allgemeine Gültigkeitsbereich

[6] Quelle: https://www.tuvit.de/de/produkte/common-criteria-447.htm

wird erläutert. Ergänzend werden auch Schutzprofile (Protection Profile) und Sicherheitsvorgaben (Security Target) vorgestellt. Teil zweienthält einen umfangreichen Katalog von Funktionalitätsanforderungen. Als Teil drei werden die Anforderungen an die Vertrauenswürdigkeit aufgezählt. Das Evaluierungsergebnis basiert am Ende auf einer Vertrauenswürdigkeitsstufe (EAL). Diese setzt sich aus sieben hierarchischen Stufen zusammen. Je höher die Stufe, desto vertrauenswürdiger ist das System[7].

Diese Vorgehensweise mit ihren verschiedenen Vertrauenswürdigkeitsstufen wird ausführlich vom Bundesamt für Sicherheit in der Informationstechnik vorgestellt. Als weiterführende Literatur ist das Buch von Debra S. Herrmann (2003) zu nennen.

Kryptographie

Kryptographie bedeutet das Verschlüsseln von Daten bzw. Botschaften jeglicher Art durch ein sogenanntes kryptographisches Verfahren. Im Allgemeinen wird die Kryptographie mit dem Ziel angewendet Vertraulichkeit, Integrität und Authentizität zu schützen. Um das kryptographische Verfahren anzuwenden, werden mathematische Algorithmen zur Verschlüsselung genutzt.

Generell wird zwischen der symmetrischen Verschlüsselung, wie z.B. AES, DES und Blowfish[8] unterschieden. Hierbei verwenden sowohl der Versender, als auch der Empfänger den gleichen Schlüssel. Als zweite Methode gibt es die asymmetrische Verschlüsselung, wie z.B. RSA und Rabin. Ein Schlüsselpaar wird bei diesem Verfahren verwendet, wobei ein Schlüssel verdeckt vom Versender genutzt wird und der zweite öffentlich bereitgestellt wird. Dieses Verfahren kommt insbesondere bei den digitalen Signaturen zum Einsatz[9].

Des Weiteren wird in der Kryptographie zwischen schwacher und starker Verschlüsselung unterschieden. Diese ist abhängig von den folgenden Faktoren:

- Der Kryptographie-Anwendung und die verwendeten Verschlüsselungsalgorithmen
- Dem Übertragungsmedium
- Dem Schlüssel; wie z.B. der Schlüssellänge, Schlüsselentropie und dem Schutz des Schlüssels.

[7] Quelle: http://www.secupedia.info/wiki/Common_Criteria_/_ISO15408
[8] Anm. der Betreuer: Hier fehlen die Verweise zu den entsprechenden Standards: diese bilden in mehrerer Hinsicht die Grundlage bei einer Analyse, z. B. bei ihren Vorgaben zur Schlüssellänge.
[9] Quelle: http://www.kryptowissen.de/kryptographie.html

- Dem Computer und seinem Benutzer[10]

Diese Vorgehensweise wird ausführlich vom Bundesamt für Sicherheit in der Informationstechnik über kryptographische Verfahren: Empfehlungen und Schlüssellängen vorgestellt [BSI TR-02102-1]. Als weiterführende Literatur wäre das Konferenzprotokoll der Datenschutzbeauftragten des Bundes und der Länder zu nennen (Arbeitskreis Technik, 2003).

Penetrationstest (kurz: Pentesting)

IT-Systeme, welche über Verbindungen zu öffentlichen Netzen verfügen, sind Angriffen sowie unautorisierten und meist anonymen Zugriffsversuchen ausgesetzt. Solche Situationen stellen vermehrt eine Bedrohung für Unternehmen und öffentliche Einrichtungen dar. Sie verfügen meist über komplexe Kommunikationsstrukturen, die sich nur teilweise beeinflussen lassen und die sich oft den einzelnen Organisationen nicht mehr ganzheitlich erschließen. Durch den Anschluss z.B. an das Internet wird ein Teil ihrer Verantwortung (z.B. Verfügbarkeit fremder Server und Netze) abgegeben. Zusätzlich müssen diese mit neuen Bedrohungen rechnen, auf die sie in geeigneter Form reagieren müssen. Als Beispiele können hierbei Angriffe von Hackern (befassen sich mit Sicherheitslücken aufgrund des technischen Interesse) bzw. Crackern (verfolgen kriminelle Interessen) genannt werden.

Um den Bedrohungen im Voraus entgegenwirken zu können, existieren viele praktische Vorgehensweisen. Eine Lösung sind Penetrationstests. Durch einen Penetrationstest kann untersucht werden, inwieweit die Sicherheit der IT-Systeme durch die Angreifer gefährdet ist bzw. ob die IT-Sicherheit durch die eingesetzten Sicherheitsmaßnahmen gewährleistet wird. Dabei wird die gesamte Situation aus dem Blickwinkel des Angreifers analysiert. Es wird versucht, die Attacken des Angreifers (an Computersystem bzw. -netzwerk) praktisch nachzustellen und somit die vorhandenen Schwachstellen zu identifizieren. Typische Angriffspunkte für einen Penetrationstest sind Firewalls, Webserver sowie Modems und Funknetzwerke. Bei dem Test wird darauf geachtet, dass ähnliche Techniken eingesetzt werden, die auch bei einem realen Angriff verwendet werden. Die ermittelten Schwachstellen können durch geeignete Maßnahmen eliminiert werden. So kann vermieden werden, dass diese Lücke von unautorisierten Dritten genutzt wird. Die Penetrationstests können mithilfe verschiedener Programme durchgeführt werden. Mittlerweile existieren unterschiedliche Schwachstellen-Scanner, wel-

[10] Quelle: http://www.netplanet.org/kryptografie/einfuehrung.shtml

che entweder frei erhältlich sind oder kommerziell erworben werden können. Mithilfe dieser Tools können die Schwachstellen der zu überprüfenden Systeme ermittelt werden. Somit können Aussagen zu deren Gefährdungen getroffen werden. Die Qualität sowie der Nutzen eines Penetrationstests sind von der Betrachtung der individuellen Situation des Auftraggebers (Organisation) abhängig. Der Erfolg des Penetrationstest ist abhängig von der Kreativität des Testers, den ermittelten Schwachstellen und von der investierten Zeit und Geld.

Diese Vorgehensweise wurde ausführlich in einer Studie des Bundesamts für Sicherheit in der Informatik über Durchführungskonzept für Penetrationstests beschrieben (BSI, 2003). Als weiterführende Literatur bzw. Quellen wären die Internetseite des HvS-Consulting[11] und der Artikel „Kosten und Nutzen von Penetrationstest“ (Schreiber, 2006) zu nennen.

2.3.Rechtliche Sicht

Die rechtliche Sicht befasst sich mit Gesetzen und Vorschriften, die sich auf IT-Sicherheit beziehen und das Risikomanagement eines Unternehmens unterstützen (Simić-Draws, 2013, S. 2). Diese müssen unbedingt eingehalten werden. An dieser Stelle können verschiedene Vorgehensweisen wie Konkretisierung rechtlicher Anforderungen (kurz: KORA) oder das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) eingesetzt werden. Nachfolgend werden diese beiden Verfahren erläutert.

KORA

KORA beschreibt eine Methode zur **Ko**nkretisierung **r**echtlicher **A**nforderungen, um abstrakte rechtliche Vorgaben in entsprechend konkrete technische Anforderungen umzuwandeln (Hammer et. al., 1993, S.21). Dabei gliedert sich die Methode in vier Schritte. Im ersten Schritt werden die rechtlichen Anforderungen abgebildet. Dabei dient meistens das Grundgesetz als erste Grundlage, woraus dann für die Funktionen des zu betrachtenden Techniksystems, passende rechtliche Vorgaben abgeleitet werden. Im zweiten Schritt werden die vorher gewonnenen Anforderungen zu Kriterien konkretisiert, wobei diese technische, rechtliche und soziale Aspekte aufweisen. Daraus werden im dritten Schritt technische Gestaltungsziele formuliert, die als “Soll-Anforderungen” verstanden werden können. Im abschließenden vierten

[11] Quelle: http://www.hvs-consulting.de/penetrationstests.aspx

Schritt werden aus diesen Zielen technische Gestaltungsvorschläge entwickelt, wobei diese noch keinen endgültigen Systementwurf beschreiben (Hoffmann et. al., 2011, S.77).

Die KORA-Methode wurde zuerst in einem Paper von Hammer et al. (1993) vorgestellt. Als weiter erklärende Texte sind das Buch von Hoffmann et. al. (2011) zur Integration rechtlicher Anforderungen an soziotechnischen Systemen in frühe Phasen der Systementwicklung und der Internetauftritt von P23R Methodenleitfaden[12] zu nennen, wobei auf der Internetseite der Universität Kassel[13] eine beispielhafte Anwendung von KORA beschrieben ist.

IT-Governance

Unter IT-Governance (kurz ITG) werden verschiedene Grundsätze oder Richtlinien verstanden, die ein Zusammenspiel von IT und Unternehmungsführung (auch *Corporate Governance*, kurz CG) regeln sollen. Dabei soll sichergestellt werden, dass bei einem Unternehmen die eingesetzte IT die definierten Geschäftsziele abdeckt und unterstützt, eingesetzte Ressourcen verantwortungsvoll im Sinne einer langfristigen Wertschöpfung verwendet, eventuelle Risiken angemessen überwacht und entgegengewirkt und qualitative Leistungsbeurteilungen wie Messungen durchgeführt werden (Meyer et al., 2003, S.445). Für eine praktische Umsetzung bietet beispielsweise COBIT (*Control Objectives for Information and Related Technology*) ein etabliertes Referenzmodell, welches Methoden zu den genannten Grundsätzen und Richtlinien beschreibt[14]. Andere Modelle sind beispielsweise die internationale ISO/IEC 20000 Norm[15] oder die *IT Infrastructure Library* (kurz ITIL)[16]. Zudem hat der deutsche Gesetzgeber im Jahr 1998 das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (kurz KonTraG[17]) verabschiedet, das mitunter Vorstand und Aufsichtsrat eines Unternehmens zur Einrichtung eines *Risikofrüherkennungssystems* verpflichtet[14,18]. Dieses Gesetz schreibt nicht nur die Fortentwicklung und Verbesserung der CG in deutschen Unternehmen vor, sondern beeinflusst damit auch Teile der ITG, beispielsweise den Aspekt des Risikomanagements. Die Begründung hierfür ist nach Meyer et. al. (2003, S. 446) die Untrennbarkeit von

[12] Quelle: http://mlf.p23r.de/module/modul16-kora/
[13] Quelle: http://www.uni-kassel.de/eecs/fileadmin/datas/fb16/iteg/subico/Schulz-Vorschl%C3%A4ge_zur_rechtskonformen_Gestaltung_selbst-adaptiver_Anwendungen.pdf
[14] Quelle: http://www.itgi.org/
[15] Quelle: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=4133
[16] Quelle: http://www.itil-officialsite.com/
[17] Quelle: https://beck-online.beck.de/default.aspx?bcid=Y-100-G-KonTraG
[18] Quelle: http://wirtschaftslexikon.gabler.de/Definition/gesetz-zur-kontrolle-und-transparenz-im-unternehmensbereich-kontrag.html

ITG und CG, da die Verwendung von IT Systemen und die Einhaltung von Geschäftszielen gleichermaßen relevant für den Unternehmenserfolg sind[11].

Das *IT Governance Institute*, welches den Begriff *ITG* definiert hat, wurde im Jahre 1998 von der *Information Systems Audit and Control Association* (kurz *ISACA*[19]) gegründet (Meyer et. al., 2003, S.446)[11]. Weiter Informationen zu COBIT können auf der Internetseite des IT Governance Institute[11] entnommen werden. Im Paper zum IT-Governance-Modell von Rohloff et. al. (2003) findet sich eine praktischere Interpretation des ITG Begriffs.

Im Rahmen der IT-Sicherheitsanalyse wird ein Vorgehensmodell beschrieben, das zur Bewertung und Optimierung der Sicherheit eines IT-System dient. Abhängig von dem Gegenstand der IT-Sicherheitsanalyse (konkretes IT-System, ein Teil davon oder zusätzlich die einsetzende Umgebung) können Vorgehensmodelle mit unterschiedlichem Fokus verwendet werden (Simić-Draws, 2013). Die IT-Sicherheitsanalyse kann sich z.B. auf ein spezifisches IT-Produkt begrenzen oder direkt ein ganzes Unternehmen untersuchen. Die zuvor vorgestellten Analyseverfahren berücksichtigen kaum weitere wichtige Faktoren. Beispielsweise betrachtet keines der Vorgehensmodelle die Interessenkonflikte, welche zwischen Menschen entstehen können, wenn diese miteinander kommunizieren. Auch die IT-Systeme, welche verwendet werden, dürfen bei dieser Betrachtung nicht vergessen werden. Zusätzlich wird die Sicherheitsanalyse von IT-Systemen in deren Anwendungskontexten (also in Geschäftsprozessen) ebenfalls vernachlässigt. Aus diesem Grund fehlt diesen Vorgehensmodellen der Bezug zur Realität. Ein Problem, welches dabei besonders deutlich ist, tritt bei der Untersuchung des gesamten Prozesses auf, v.a. wenn dieser vor Missbrauch geschützt werden soll. Die Schwachstellen der vorhandenen Vorgehensmodelle sollen durch das PrOSA-Vorgehensmodell überwunden werden.

[19]https://www.isaca.org/Pages/default.aspx

3. Das PrOSA-Vorgehensmodell (Prozessorientierte Sicherheitsanalyse)

In diesem Kapitel wird das PrOSA-Vorgehensmodell beschrieben. Dabei handelt es sich um eine prozessorientierte Sicherheitsanalyse, welche teilweise die organisatorische Sicht mit der produktorientierten Sicht vereinbart. Die nachfolgenden Ausführungen basieren überwiegend auf dem Paper von (Simić-Draws, 2013).

Wie schon in Kapitel 2 erwähnt, fehlt allen dort beschriebenen Analyseverfahren der Bezug zur Realität. Innerhalb von den drei genannten Sichten kann ein IT-System nicht in seinem Anwendungskontext untersucht werden. Dieser Umstand kann durch eine prozessorientierte Sicht geliefert werden, welche sich auf die Abbildung der Geschäftsprozesse einer Organisation konzentriert. Da Geschäftsprozesse als Folgen bestimmter zusammenhängender Zustandsänderungen bzw. Aktivitäten des betrachteten Systems „Unternehmen“ verstanden werden können, ist durch die Modellierung solcher Geschäftsprozesse eine Abbildung der Realität möglich (Kölsch, 2004, S.3). Folglich kann die prozessorientierte Sicht die Wirklichkeit mit einem abstrakten IT-System verbinden. Durch die Realität wird der Anwendungskontext (Menschen, Ressourcen, Konflikte, Abläufe) bestimmt und das IT-System kann mit seinen architektonischen Komponenten (Protokolle, Daten, Module) beschrieben werden (Simić-Draws, 2013, S.3).

3.1. Vierte Sicht auf IT-Sicherheitsanalyse

Das PrOSA-Vorgehensmodell schlägt eine vierte Sichtweise, die primär prozessorientiert ist, vor. Dabei werden in erster Linie die Geschäftsprozesse einer oder mehrerer Organisationen betrachtet. Somit können die Teilmengen vereint werden, die in der organisatorischen und produktorientierten Sicht betrachtet werden[20]. Zudem wird die Geschäftsprozessmodellierung vorgenommen, um so den Realitätsbezug darzustellen. Somit gelingt es, die Realität mit dem abstrakten IT-System zu verbinden.

[20] Über die Betrachtung von Prozessen wird eine nachvollziehbare Abgrenzung des Untersuchungsgegenstandes möglich. Es werden also nur diejenigen IT-Systeme und organisatorischen Komponenten (z.B. Geschäftsregeln) betrachtet, die den untersuchten Prozess unterstützen

Dies wird vor allem durch folgende Formulierung deutlich:

„*(...) Die Realität bestimmt den Anwendungskontext mit den beteiligten Menschen, Ressourcen, Konflikten, organisatorischen und rechtlichen Rahmenbedingungen sowie Kommunikations- und Arbeitsabläufe. Das statische IT-System hingegen wird mit seinen architektonischen Komponenten wie Protokolle, Daten, Module oder Schnittstellen beschrieben. Für die systemrelevanten Komponenten stellen die Common Criteria und das Grundschutzhandbuch das entsprechende Anforderungsvokabular zur Verfügung. (...)"* (Simić-Draws, 2013, S.3).

Durch das Vorgehensmodell werden die Abläufe in und zwischen verschiedenen IT-Systemen und den beteiligten Akteuren realitätsnah abgebildet. Die Untersuchung und Absicherung erfolgt systematisch. Aus diesem Grund spielt der Realitätsbezug eine Schlüsselrolle in dem Vorgehensmodell. Die IST-Aufnahme eines Geschäftsprozesses erfolgt mithilfe des Top-Down-Ansatzes. Auf dieser Grundlage erfolgt die Sicherheitsanalyse. Die aus der Sicherheitsanalyse gewonnenen Ergebnisse dienen als Fundament für die Implementierung von Maßnahmen, welche den Geschäftsprozess sicher und optimal gestalten. Es gibt eine Reihe von Beispielen für potenziell zu untersuchende Prozesse (z.B. Homebanking-Transaktionen oder Prozesse im Bereich des eCommerce). Im Rahmen des Forschungspraktikums wurden zwei Geschäftsprozesse ausgewählt und anschließend untersucht: Vorbereitung und Durchführung der Kommunalwahlen am 25.05.2014 in Koblenz sowie Auszahlung von Geld am Geldautomaten am Campusgelände (Sparkasse). Im nächsten Abschnitt werden die genauen Analyseschritte des PrOSA-Vorgehensmodells beschrieben.

3.2. Vorstellung des Vorgehensmodells

Das PrOSA-Vorgehensmodell (siehe Abbildung 1), welches im Rahmen des Forschungspraktikums zum Einsatz gekommen ist, besteht aus insgesamt fünf Schritten (Simić-Draws, 2013, S. 3 ff.):

1. Problemstellung
2. Zusammenfassung der ermittelten Informationen in einem Use-Case-Diagramm
3. Durchführung der Sicherheitsanalyse aufgrund der zerteilten und wieder zusammengefügten Geschäftsprozesse
4. Ergebnisse der Sicherheitsanalyse

5. Implementierung der vorgeschlagenen Maßnahmen

Nachfolgend werden die einzelnen Schritte des PrOSA-Vorgehensmodells beschrieben.

1. Schritt: Problemstellung

In diesem Schritt wird eine konkrete Problemstellung bearbeitet. Daraus geht eine Fragestellung hervor, an welcher sich das weitere Vorgehen orientieren wird, um somit diese am Ende beantworten zu können. Des Weiteren ist es hierbei wichtig, dass die Problemstellung informell erfolgt und einen konkreten Geschäftsprozess betrachtet wird. Dadurch wird ein Bereich eingegrenzt, auf welchen sich das weitere Vorgehen beschränkt. In dieser Phase sollen allgemeine Überlegungen festgehalten werden, welche einen Bezug zu der Problemstellung haben. Dabei kann reflektiert werden, welche IT-Systeme und Akteure an dem Prozess beteiligt sind. Des Weiteren kann überlegt werden, welche möglichen Use-Cases existieren können und welche Interessen die identifizierten Akteure verfolgen. Durch diesen Schritt wird der zu untersuchende Prozess verständlich und nachvollziehbar (Simić-Draws, 2013, S. 3).

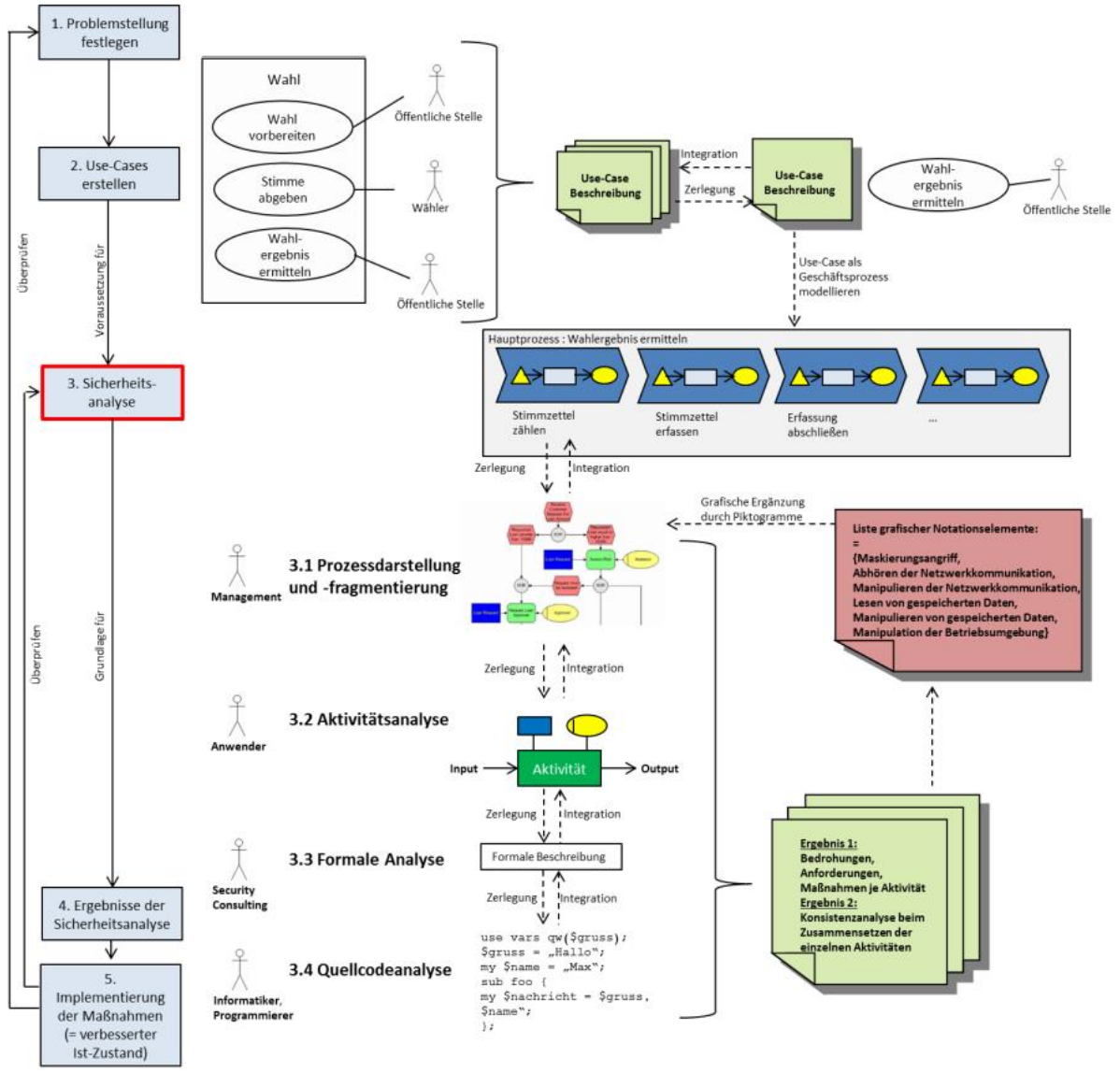

Abbildung 1: Grafische Darstellung des PrOSA-Vorgehensmodells [Simić-Draws, 2013][21]

[21] Anm. der Betreuer: Die hier dargestellte und im Rahmen des Forschungspraktikums verwendete Version des Vorgehensmodells wurde inzwischen in der weiteren Entwicklung ihrer Dissertation von D. Simić-Draws umfassend überarbeitet und ist daher nicht mehr aktuell. Gleichwohl taugt sie noch gut zur Analyse, wie sie im Forschungspraktikum durchgeführt wurde, Die nachfolgenden Ausführungen beziehen sich auf die veraltete Version. Irrelevante, aber unschädliche Bestandteile der Beschreibung haben wir im Text unkommentiert belassen.

2. Schritt: Zusammenfassung der ermittelten Informationen in einem Use-Case-Diagramm

Die Informationen, welche in dem ersten Schritt ermittelt werden, werden hier zusammengefasst und in Form von Use-Case-Diagrammen vorgestellt. Dadurch lassen sich die Ergebnisse aus dem ersten Schritt strukturiert und nachvollziehbar darstellen. Um dies zu vertiefen, werden die Diagramme zusätzlich textuell erläutert. Dadurch werden mögliche Fehlinterpretationen der Diagramme vermieden und ihr Inhalt wird ausführlich beschrieben. Damit alle Use-Case-Diagramme, welche für einen Prozess erstellt werden, einheitlich dargestellt werden, wird von der Autorin des PrOSA-Vorgehensmodells die Nutzung einer Schablone empfohlen (Simić-Draws, 2013, S. 4). Dadurch wird ein standardisiertes Vorgehen ermöglicht.

3. Schritt: Durchführung der Sicherheitsanalyse aufgrund der zerteilten und wieder zusammengefügten Geschäftsprozesse

Dieser Schritt bildet den Schwerpunkt des gesamten Vorgehensmodells (Simić-Draws, 2013, S. 4.). Zunächst wird ein Use-Case ausgewählt, welcher als Grundlage für das weitere Vorgehen dient. Es wird empfohlen, dass die Use-Cases mithilfe eines anderen Notationsmodells (EPK oder BPMN) dargestellt wird, da die Aktivitätsdiagramme nicht über genügend Umfang an Darstellungsmöglichkeiten verfügen (Simić-Draws, 2013, S. 4). Das liegt daran, dass hierbei wesentliche Modellierungselemente fehlen, welche die Variabilität in Use-Cases ausdrücken könnten (von der Maßen/Lichter, 2003, S.4). Das Projektteam hat sich während der Bearbeitung des Forschungspraktikums für BPMN entschieden. Die Gründe dafür und die Beschreibung der Spezifikationssprache werden im weiteren Verlauf der Arbeit beschrieben. Durch die Modellierung lassen sich die Geschäftsprozesse grafisch abbilden und aufteilen, damit die einzelnen Elemente ersichtlich werden. Dieser Schritt ist besonders für die tatsächliche Analyse wichtig. Wenn er nicht vorgenommen wird, besteht die Gefahr, dass z.B. einzelne Sicherheitsanforderungen, aufgrund der Komplexität des Geschäftsprozesses, nicht ersichtlich werden (Simić-Draws, 2013, S. 5). Wenn dieser Schritt durchgeführt wird, ist es möglich den Prozess soweit aufzugliedern, bis seine einzelnen Aktivitäten sichtbar werden. Nach diesem Schritt, kann die eigentliche Analyse beginnen, wobei die einzelnen Aktivitäten

getrennt voneinander betrachtet werden. Es wird unter anderem untersucht, welche IT-Systeme an jeder Aktivität beteiligt sind.

Durch die Aufteilung des Gesamtprozesses auf die unterste Ebene (Aktivitäten) werden die teilnehmenden Akteure ersichtlich (Simić-Draws, 2013, S. 5). So können verschiedene Interessen identifiziert werden, welche von diesen Akteuren verfolgt werden und aus welchen mögliche Konflikte entstehen können (Simić-Draws, 2013, S. 5). Durch diesen Schritt werden mögliche Bedrohungen sichtbar. Des Weiteren werden in dieser Phase vorhandene Sicherheitsanforderungen sowie Maßnahmen ermittelt, welche für die Gewährleistung dieser Anforderungen sorgen. Zusätzlich können Sicherheitsanforderungen identifiziert werden, welche zur Optimierung des IST-Zustandes führen können und möglicherweise durch weitere Sicherheitsmaßnahmen unterstützt werden können. Als Ergebnis dieser Phase können Bedrohungen, Sicherheitsanforderungen sowie Sicherheitsmaßnahmen **pro Aktivität** festgehalten werden. Im Rahmen des Forschungspraktikums wurde die Quellcodeanalyse nicht durchgeführt, weil das dafür notwendige Expertenwissen (z.B. vertiefte Programmierkenntnisse) gefehlt hat bzw. die Quellcodes auch nicht einsehbar waren.

4. Schritt: Ergebnisse der Sicherheitsanalyse

Für einzelne Aktivitäten konnten, in den früheren Phasen, Sicherheitsanforderungen, Sicherheitsmaßnahmen und spezifische Bedrohungen identifiziert werden. Diese werden im vierten Schritt erfasst.

5. Schritt: Implementierung der vorgeschlagenen Maßnahmen

Für das weitere Vorgehen des PrOSA-Vorgehensmodells ist es wichtig, dass der vorerst aufgeteilte Prozess wieder zusammengesetzt wird. Die ermittelten Ergebnisse müssen dabei auf Widerspruchsfreiheit untersucht werden, denn bei diesem Schritt besteht die Gefahr von Inkonsistenzen. Es könnte beispielsweise passieren, dass sich die für Aktivität B ermittelte Sicherheitsanforderung mit der vorhandenen Sicherheitsmaßnahme der Aktivität A ausschließt. Dies muss durchgeführt werden, bevor die Ergebnisse der Sicherheitsanalyse implementiert werden. Dadurch wird sichergestellt, dass die Umsetzung widerspruchsfrei ist und zur Optimierung des aktuellen IST-Zustandes führt. Abschließend werden die ermittelten Maßnahmen umgesetzt.

4. Prozessmodellierung mit BPMN 2.0

Der folgende Abschnitt beschäftigt sich mit der Beschreibung und der Dokumentation der beiden gewählten Geschäftsprozesse. Für die Notation der beiden Geschäftsprozesse wurde auf BPMN[22] in der Version 2.0 zurückgegriffen. Hierbei wurden die beiden Geschäftsprozesse in der Cloud-basierten Plattform von *Signavio*[23] modelliert. Der *Signavio Process Editor* für akademische Institutionen eignet sich besonders gut für ein gemeinschaftliches Arbeiten, da alle Mitglieder über ihren Account auf die modellierten Prozessmodelle zugreifen sowie diese kommentieren können.

Bei der Prozessnotation in BPMN *2.0* können insgesamt 116 grafische Elemente verwendet werden (Schöpp, 2014, S. 51). Um eine Einheitlichkeit der Prozessdokumentation zu erlangen sowie die Komplexität zu reduzieren, wurden jedoch nicht alle verfügbaren Elemente zur Modellierung der beiden Geschäftsprozesse genutzt, sondern lediglich einige Kernelemente, auf welche im weiteren Verlauf dieses Abschnittes kurz eingegangen wird.

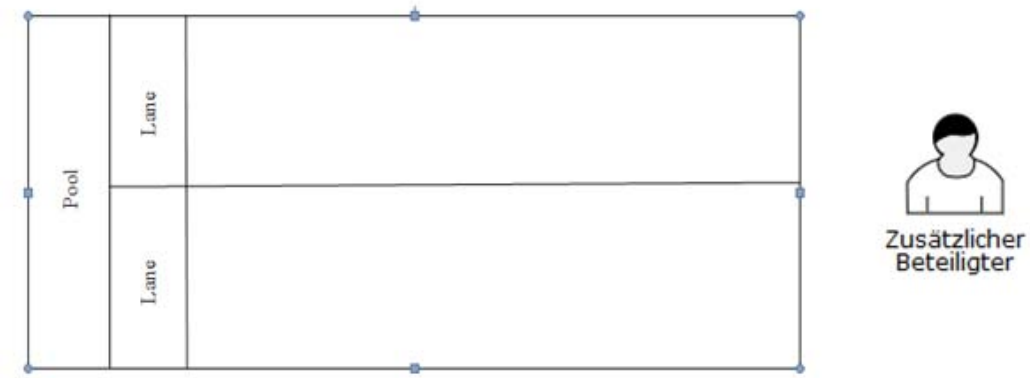

Abbildung 2: Angewandte Rollen-Symbole zur Geschäftsprozessmodellierung [eigene Darstellung in Anlehnung an Allweyer, 2009 S. 23; BPM Offensive Berlin, 2011]

Um zunächst die Systeme und die Akteure in den Systemen darzustellen, wurden in der Notation sogenannte Pools und Swimlanes dafür vorgesehen (siehe Abbildung 2). Pools werden dazu verwendet, um einen ganzheitlichen und abgeschlossenen Prozess in einer Einheit darzustellen. Hierbei kann ein Pool mit dem Namen des Prozesses oder auch mit dem Namen der

[22] Anm. der Betreuer: Die Verwendung von BPMN wurde vorgegeben
[23] Quelle: http://www.signavio.com/de/

auszuführenden Organisationseinheiten des Prozesses bezeichnet werden (Allweyer, 2009, S. 17). Zusätzliche Beteiligte werden verwendet, wenn diese nur bei einzelnen Aktivitäten beteiligt sind.

Um die Prozesse in den jeweiligen Pools und Lanes modellieren zu können, werden die anfallenden Aufgaben, welche der Geschäftsprozess umfasst, mit Flussobjekten dargestellt. Bei Flussobjekten handelt es sich um die Knoten in den jeweiligen Geschäftsprozessen. Diese Knoten können entweder als Aktivität, als Gateway oder als Ereignis beschrieben werden (White & Miers, 2008, S. 28).

Wird ein Ereignis verwendet, besagt dieses, dass sich im Verlauf des Prozesses etwas ausgelöst wird. Dabei können Ereignisse zeitlich unterschieden werden in die Kategorien der Startereignisse, der Zwischenereignisse und der Endereignisse. Bei Zwischenereignissen kann zusätzlich in „catching“ und „throwing“ unterschieden werden. „Catching“ wird Ereignissen zugeordnet, die etwas empfangen. Gegensätzlich hierzu, fungieren „throwing“-Ereignisse als Auslöser, welche dazu dienen, etwas für den weiteren Prozessverlauf zu senden (Möhring & Vogel, 2013, S. 55). Des Weiteren werden Ereignisse in verschiedene Arten unterteilt, welche im Inneren des Kreises als Symbol angezeigt wird (Göpfert & Lindenbach, 2012, S. 51). Bei der Modellierung der beiden Geschäftsprozesse wurden hierfür Zeit-, Nachrichten- und Bedingungsereignisse benötigt.

Abbildung 3: Angewandte Ereignis-Symbole zur Geschäftsprozessmodellierung [eigene Darstellung in Anlehnung an BPM Offensive Berlin, 2011]

Als Startereignisse für die Modellierung der beiden Geschäftsprozesse wurden einfache, Zeit-, Nachrichten- und Bedingungs-Startereignisse verwendet. Zeit-Startereignisse werden verwendet, wenn der Prozess zu einem bestimmten Zeitpunkt startet. Nachrichten-Startereignisse kommen zum Einsatz, wenn der Prozess nach dem Erhalt einer Nachricht beginnen soll. Bedingungs-Startereignisse wurden gebraucht, wenn der Prozess startet soll, wenn eine Bedingung vorliegt, wie z.B. das Benötigen von Geld. Einfache Startereignisse wurden verwendet, wenn keines der zuvor beschriebenen Startereignisse zutraf. Wie in Abbildung drei zu erkennen, wurden die gleichen Arten ebenfalls für die Modellierung der Zwischenereignisse eingesetzt. Lediglich für die End-Ereignisse wurden die zwei Arten des einfachen Endereignisses sowie des Nachrichten-Endereignis herangezogen (siehe Abbildung 3).

Tritt ein Gateway in einem Geschäftsprozess auf, ist an dieser Stelle eine Verzweigung oder eine Zusammenführung des Sequenzflusses festzustellen (Allweyer, 2009, S. 25). Für die Erstellung der beiden Geschäftsprozesse wurden drei unterschiedliche Arten von Gateways für die Darstellung benötigt (siehe Abbildung 4). Gateways zeigen auf, dass bestimmte Ereignisse in einem Prozess nur unter bestimmten Bedingungen auftreten (Freund & Rücker, 2012, S. 21).

Abbildung 4: Angewandte Gateway-Symbole zur Geschäftsprozessmodellierung [eigene Darstellung in Anlehnung an Freund & Rücker, 2012 S. 26 ff.]

Häufig wurde hierfür ein datenbasiertes exklusives Gateway verwendet. Hierbei gibt es verschiedene Alternativen die eintreten können. Bei diesem Gateway ist es also nicht möglich, dass mehrere Aktivitäten auf einmal eintreten können, sondern lediglich nur eine. Folglich schließen sich die existierenden Alternativen gegenseitig aus (Freund & Rücker, 2012, S. 28).

Zusätzlich wurden bei dem Modellierungsvorgang ebenfalls parallele Gateways verwendet. Bei diesem Gateway gibt es verschiedene Eintrittsalternativen im Prozessfluss. Diese schließen sich allerding nicht gegenseitig aus, sondern können parallel zueinander eintreten. (Allweyer, 2009, S. 28).

Bei der letzten Gateway-Art handelt es sich um ein inklusives Gateway, welches dazu genutzt wird, einen oder mehrere Pfade zusammenzuführen. Hierbei gibt es ebenfalls verschiedene

Eintrittsalternativen, die für eine Möglichkeit eintreffen können. Dabei muss mindestens eine der existierenden Alternativen eintreten. Hierbei werden also die Möglichkeiten der beiden vorangegangenen Gatewayarten kombiniert, da mindestens eine Aktivität nach dem Gateway eintritt, aber auch mehrere parallel zueinander eintreffen können. (Allweyer, 2009, S. 32).

Abbildung 5: Angewandte Aktivitäts-Symbole zur Geschäftsprozessmodellierung [eigene Darstellung in Anlehnung an Bartsch, 2010 S. 124; BPM Offensive Berlin, 2011]

Jeder Prozess sieht eine Reihe von Dingen vor die erledigt werden müssen, damit ein Prozessfluss stattfinden kann. Für diese Aufgaben oder Tätigkeiten werden bei BPMN 2.0 die sogenannten Flussobjekte gebraucht. Als Flussobjekte in den modellierten Geschäftsprozessen wurden Aktivitäten, zugeklappte Unterprozesse sowie Ereignisunterprozesse verwendet, welche in Abbildung 5 zu sehen sind. Aktivitäten haben die Aufgabe atomare oder komplexe Aufgaben eines Prozessflusses zu beschreiben und abzubilden (Bartsch, 2010, S. 124). Um die im Prozess anfallenden Aufgaben (Tasks) festzulegen, wurde auf den unspezifizierten Typ zurückgegriffen. Dies bedeutet, dass alle Aufgaben allgemeiner dargestellt wurden ohne den Aufgabentyp näher festzulegen oder zu gruppieren (Göpfert & Lindenbach, 2012, S. 13). Ziel der Modellierung in BPMN ist es, eine vereinfachte Darstellung zu erarbeiten und somit einen schnellen Einblick in die Prozessabläufe zu erhalten (Göpfert & Lindenbach, 2012, S. 23). Um die Komplexität der beiden Geschäftsprozesse zu reduzieren, wurden bei den untersuchten Prozessen zwei Arten von Unterprozessen bei der Modellierung verwendet. Der zugeklappte Unterprozess dient dazu, die Details zu verbergen und somit den Prozessüberblick einfacher zu gestalten (Göpfert & Lindenbach, 2012, S.23). Wird die Notation der Aktivitäten betrachtet, so unterscheiden sich die Aktivitäten innerhalb eines Unterprozesses durch ein „Plus-Zeichen“ gegenüber einfachen Aktivitäten (White & Miers, 2008, S. 67). Ein Ereignis-Unterprozess wird stets in einem Prozess oder einem Unterprozess platziert. Dieser wird durch ein Ereignis gestartet und bestimmt wie der Gesamtprozess fortgesetzt wird. Zudem kann dieser Unterprozess beliebig oft ausgeführt werden, bevor der Prozessfluss fortgesetzt wird (Göpfert & Lindenbach, 2012, S. 31).

Abbildung 6: Angewandte Konnektoren-Symbole zur Geschäftsprozessmodellierung [eigene Darstellung in Anlehnung an Göpfert & Lindenbach, 2012 S.100; Bartsch, 2010 S. 125; BPM Offensive Berlin, 2011]

Um Flussobjekte miteinander verbinden zu können werden sogenannte Konnektoren benötigt, wie in Abbildung 6 zu sehen sind. Diesen kommt die Aufgabe zu, einzelne Objekte anhand ihrer Kanten miteinander zu verbinden. Am meisten verwendet wird hierbei der Sequenzfluss, welcher Aktivitäten, Gateways und Ereignisse innerhalb eines Pools bzw. einer Lane miteinander verbindet. Er zeigt dabei auf in welcher Reihenfolge diese Objekte miteinander verbunden werden. In den beiden Geschäftsprozessen werden, neben den Sequenzflüssen, außerdem Nachrichtenflüsse verwendet. Diese verbinden Pools, Lanes oder Flussobjekte in einem Geschäftsprozessdiagramm miteinander. Ziel ist es anzuzeigen, dass Pools, Lanes, Flussobjekte oder deren einzelne Elemente miteinander in Kontakt stehen und Informationen austauschen (Bartsch, 2010, S. 125). Zur weiteren Anwendung im Rahmen des Forschungspraktikums kamen des Weiteren alle Assoziations-Arten, welche dazu genutzt werden Informationen oder Artefakte mit den einzelnen Flusselementen zu verknüpfen. Hierbei zeigt die Pfeilspitze ebenfalls die Flussrichtung an (Bartsch, 2010, S. 125; Göpfert & Lindenbach, 2012, S. 118).

Abbildung 7: Angewandte Datenobjekt-Symbole zur Geschäftsprozessmodellierung [eigene Darstellung in Anlehnung an BPM Offensive Berlin, 2011]

In den beiden bearbeiteten Geschäftsprozessen haben Aktivitäten Dateninput sowie Output erhalten. Um den Prozessfluss korrekt darstellen zu können, müssen diese ebenfalls modelliert werden. Dies umfasst die Darstellung der Übergabe aller Datenobjekte (siehe Abbildung 7), die als Input in den Prozess eingebunden sind. Des Weiteren müssen ebenfalls die resultierenden Datenobjekte als Output wiedergespiegelt werden. Dies kann dazu dienen, dass eine

bestimmte Aktivität in einem Prozess erst gestartet werden darf, wenn der notwendige Dateninput vorliegt (Allweyer, 2009, S. 137). Die Daten können in beliebiger Form sowie beliebiger Beschaffenheit vorliegen und werden mit Hilfe von Daten-Assoziationen an die jeweilige Aufgabe oder Sequenzfluss gebunden (Göpfert & Lindenbach, 2012, S. 119). Datenspeicher werden verwendet, wenn Daten in einem permanenten Speicher aktualisiert oder abgerufen werden sollen. Der Datenspeicher muss nicht notwendigerweise aus einer Datenbank bestehen, sondern es kann sich auch um einen physisch greifbaren Aufbewahrungsort wie beispielsweise einen Aktenschrank oder ähnliches handeln (Göpfert & Lindenbach, 2012, S. 120).

Wird ein Nachrichten-Symbol verwendet, wird angezeigt dass dieses Nachricht eingeht und damit das dazugehörige Ereignis ausgelöst werden kann (Allweyer, 2009, S. 132).

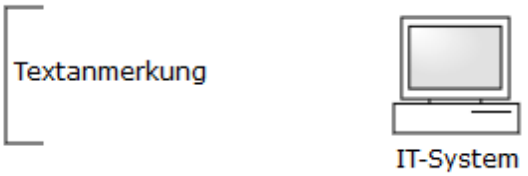

Abbildung 8: Angewandte Artefakt-Symbole zur Geschäftsprozessmodellierung [eigene Darstellung in Anlehnung an Bartsch, 2010 S. 124; BPM Offensive Berlin, 2011]

Artefakten kommt die Aufgabe zu, ergänzende Informationen über den Prozess zu liefern (siehe Abbildung 8). Bei den beiden bearbeiteten Geschäftsprozessen, geschah dies zum einen in Form von Textanmerkungen, welche an der spezifischen Stelle Anmerkungen zu der Modellierung machen. Zum anderen wurden die im Prozessablauf involvierten IT-Systeme als Artefakte abgebildet (Bartsch, 2010, S. 125).

Durch die Eingrenzung der zu verwendenden Notationselemente ist es uns nun möglich, unabhängig voneinander zu modellieren. Gerade für den komplexeren Wahlprozess in Kapitel 6 sollte das helfen.

5. Sicherheitsanforderungen

Damit alle Mitglieder des Forschungspraktikums die gleiche Auffassung von Sicherheitsanforderungen haben und auf einer gemeinsamen Menge gearbeitet wird, wurden diese zu Anfang definiert. Dies ist notwendig, da unterschiedliche Mengen oder auch Definitionen von Sicherheitsanforderungen bzw. Sichtweisen bestehen. Dabei wurde sich an den vom Bundesamt für Informationstechnik definierten Sicherheitsanforderungen orientiert[24]. Sicherheitsanforderungen beziehen sich auf Personen, Informationen, IT-Komponenten und Kommunikation.

- Authentizität (Originalität + Integrität)

  Diese Sicherheitsanforderung gewährleistet, dass eine Person auch diejenige ist, die sie vorgibt zu sein. Dies lässt sich ebenso auf IT-Komponenten anwenden. Von authentischen Informationen wird gesprochen, wenn die angegebene Quelle der Erstellung sichergestellt werden kann (Originalität) und die Informationen unverändert vorliegen (Integrität).
- Integrität

  Integrität stellt die Unversehrtheit von Daten sicher, d.h. dass diese vollständig und unverändert sind. Bezogen auf Systeme, stellt Integrität deren korrekte Funktionsweise sicher.
- Verfügbarkeit

  Die Sicherheitsanforderung gewährleistet, dass Funktionen von IT-Komponenten oder auch Informationen zugänglich sind, wenn der Anwender diese nutzen möchte.
- Vertraulichkeit

  Vertraulichkeit bedeutet, dass Informationen nur für einen bestimmten Personenkreis vorgesehen sind. In den meisten Fällen ist der Personenkreis vom Sender frei wählbar. Ausnahmen sind vorgeschriebene Empfänger wie z.B. das Militär.
- Nichtabstreitbarkeit

  Durch diese Sicherheitsanforderung ist der Versand und Empfang von Informationen gegenüber Dritten nachweisbar. Somit kann der Versand bzw. Empfang nicht mehr geleugnet werden.

[24] Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html

- Verbindlichkeit (Authentizität + Nichtabstreitbarkeit)

  Verbindlichkeit fasst die beiden Sicherheitsziele Authentizität und Nichtabstreitbarkeit zusammen. Bezogen auf die Übertragung von Informationen bedeutet diese, dass zum einen die Identität der Informationsquelle bewiesen wurde, zum anderen der Nachrichtenempfang nicht abgestritten werden kann.

Des Weiteren wurden der Liste der Sicherheitsanforderungen noch zwei weitere hinzugefügt, die auf der Präsentation von A. Pfitzmann 2008 in seiner Vorlesung 2008 (Pfitzmann 2008) basieren.

- Anonymität

  Anonymität gewährleistet, dass die Person oder die Herkunft der Information nicht identifizierbar ist. Eine Zuordnung kann somit nicht erfolgen. Bezogen auf Kommunikation bedeutet Anonymität das Gegenteil zu Nichtabstreitbarkeit.
- Korrektheit

  Es wird unterschieden zwischen partieller und totaler Korrektheit. Partielle Korrektheit wird synonym zu Integrität verwendet. Totale Korrektheit setzt sich aus partieller Korrektheit, sprich Integrität, und Verfügbarkeit zusammen. Bezogen auf Information bedeutet das, dass diese unverändert und verfügbar sein muss. In der nachfolgenden Ausarbeitung meint Korrektheit immer die totale Korrektheit.

6. Prozess 1: Kommunalwahlen 2014 in Koblenz

6.1. Überblick über den Prozess verschaffen

In diesem Kapitel wird die Erstellung des Wahlprozesses als BPMN-Diagramm beschrieben. Es wird erklärt, wie es zu den einzelnen Schritten, Namensgebung der Lanes usw. gekommen ist. Der Prozess ist insofern interessant, weil er sehr komplex ist. An den Prozess werden viele rechtliche Anforderungen gestellt, die es zu erfüllen gilt. An ihm sind sehr viele menschliche Akteure beteiligt, wodurch es zu Fehlern in der Prozessbearbeitung kommen kann. Zusätzlich können die Akteure verschiedene Interessen verfolgen, wodurch es zu Konfliktsituationen kommen kann. Zudem ist die IT-Unterstützung in dem Prozess nicht auf den ersten Blick für den Wähler erkennbar, was für Schaffung der Transparenz in dem Prozess spricht. „Wahlen“ sind auch Forschungsschwerpunkt der AG Grimm, von der das durchgeführte Forschungs-

praktikum Delta betreut wurde. Für den Wahlprozess wurden die Kommunalwahlen in Koblenz als Untersuchungsgegenstand angenommen. Für diesen Prozess sind umfangreiche Rechtsgrundsätze vorhanden, die erfüllt sein müssen und die zur Komplexität des Prozesses beitragen. Da an dem Prozess eine Vielzahl unterschiedlicher Personen partizipiert, geschieht eine Absicherung insbesondere durch organisatorische Maßnahmen. Durch die Teilnahme der vielen menschlichen Akteure treffen, wie schon angedeutet, unterschiedliche Interessen aufeinander. So können diese durch die Modellierung des Prozesses veranschaulicht werden und Manipulationsversuche sowie Schwachstellen innerhalb des Prozesses identifiziert werden.

Um einen Einstieg und Überblick über das Thema zu bekommen, wurde zuerst ein Referenzprozess gewählt. Dabei handelt es sich um den Prozess „Kommunalwahlen in Zossen“. Durch die Auseinandersetzung mit dem Referenzprozess, musste der Anwendungsfall aus Koblenz nicht direkt ins kleinste Detail ermittelt werden. Nachfolgend wird das hier angewendete Vorgehen detailliert beschrieben.

6.1.1. Referenzprozess in BPMN

Um einen Überblick über den Aufbau von Wahlabläufen zu erhalten und die Modellierungsmöglichkeiten innerhalb BPMN festzustellen, wurde im ersten Schritt ein Referenzprozess erstellt. Als Grundlage diente hierfür die Kommunalwahl 2008 in Zossen / Brandenburg. Hierbei liegt der Fokus im Inhalt des Prozesses und nicht auf der syntaktischen und semantischen Richtigkeit.
In der Abbildung 9 ist die grobe Struktur des Referenzprozesses abgebildet.

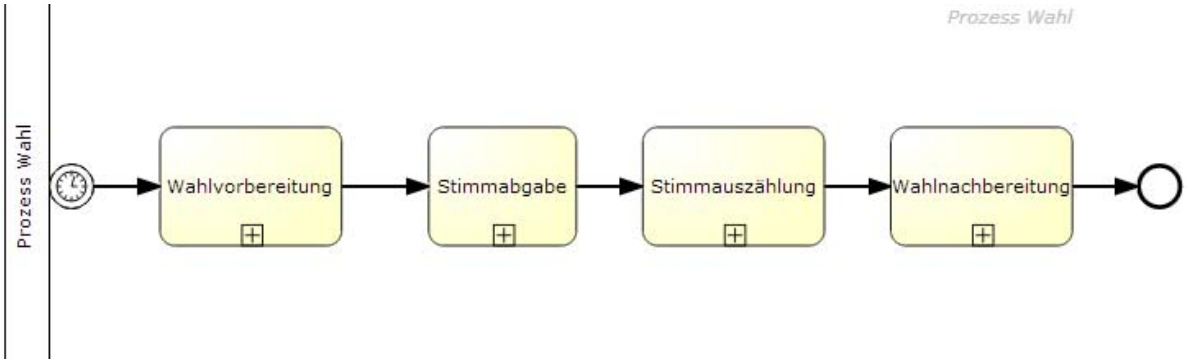

Abbildung 9: Übersicht des gesamten Prozesses Wahl

Innerhalb des Wahlprozesses Zossen, wurden acht beteiligte Personengruppen identifiziert. Diese setzen sich aus den verschiedenen Rollen und Aufgabenverteilungen innerhalb des

Wahlprozesses zusammen. Anschließend wird für jede Gruppe eine einzelne Lane abgebildet, die wie folgt zusammengesetzt sind:

- Kreiswahlleiter
- Wahlberechtigte
- Parteien, Listenvereinigungen, politische Vereinigung, Wählergruppen oder Einzelbewerber
- Vertrauensperson
- Wahlausschuss
- Gemeindewahlbehörde
- Landeswahlausschuss
- Wahlvorstand

In den späteren Prozessen werden die Lanes *„Kreiswahlleiter“* und *„Gemeindewahlbehörde“* als *„Verwaltung“* zusammengefasst.

Der Wahlprozess startet mit einem zugeklappten Unterprozess mit der Wahlvorbereitung. Die dazu gehörende Aktivität sind die „Bekanntmachungen“. Des Weiteren setzt sich die Wahlvorbereitung aus dem Vorgang „Empfangen und Prüfen der Wahlvorschläge“, sowie „Beschwerde über abgelehnte Wahlvorschläge einreichen und bearbeiten“ zusammen.

Insgesamt wird die Wahlvorbereitung innerhalb des Prozesses bereits im Referenzprozess aufgrund der bestehenden Informationen sehr detailliert dargestellt, während die „Stimmabgabe“, „Stimmauszählung“ und „Wahlnachbereitung“ nur sehr kurz gefasst werden.

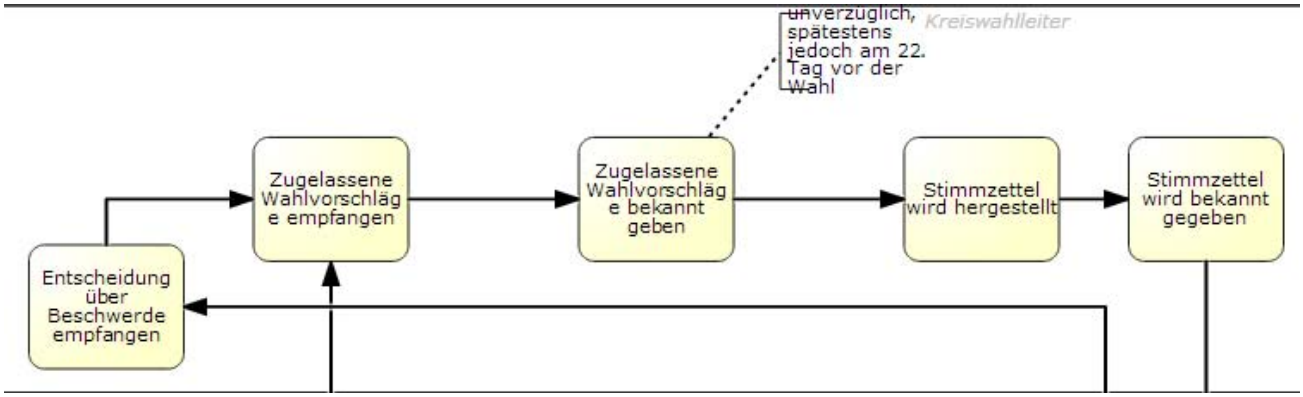

Abbildung 10: Ende der Wahlvorbereitung

Wie in Abbildung 10 und 11 zu entnehmen ist, endet der Abschnitt der „Wahlvorbereitung“ mit der Aktivität „Stimmzettel wird bekannt gegeben“ und geht direkt weiter zum Vorgang

„Stimmabgabe“ mit der Aktivität „mit Personalausweis oder Reisepass ausweisen“. Dadurch gibt es kein direktes Endereignis für den Abschnitt Wahlvorbereitung und kein Startereignis für den Teilprozess Stimmabgabe.

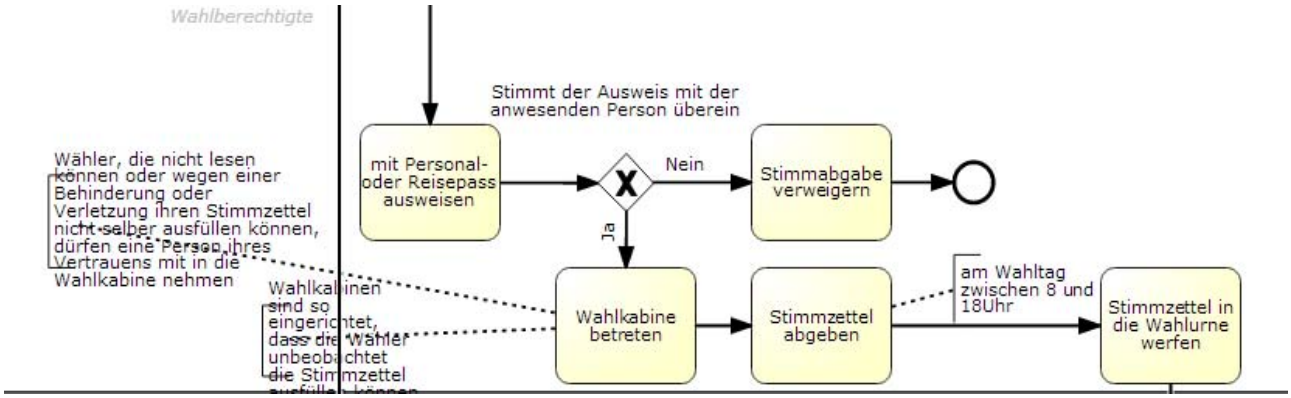

Abbildung 11: Übergang zur Stimmabgabe

Die Aktivität der Stimmabgabe wurde im Referenzprozess kurz gefasst und in fünf Aktivitäten angegeben. Sonderfälle wurden mit einer Textanmerkung angezeigt, jedoch nicht weiter ausmodelliert. In den später ausgearbeiteten Einzelprozessen der Kommunalwahl in Koblenz, wird auf die Sonderfälle näher eingegangen und die Modellierung ist wesentlich detaillierter. Auch die Stimmauszählung ist im Referenzprozess sehr kurz gehalten.

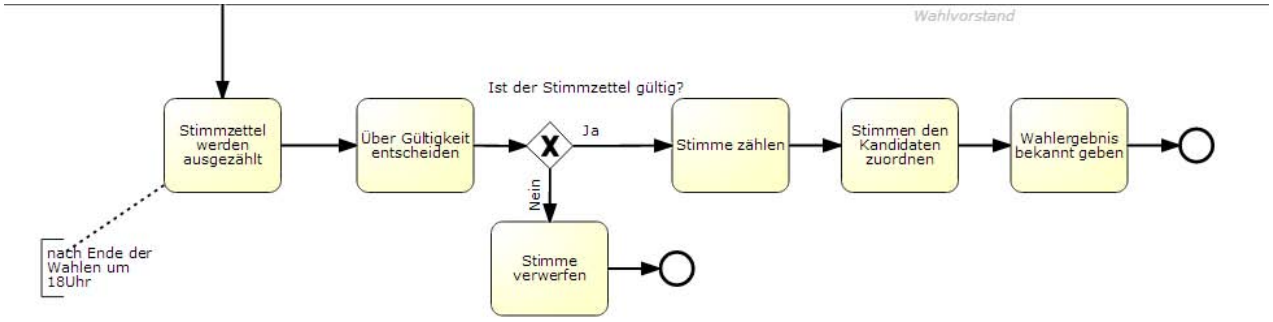

Abbildung 12: Stimmauszählung

Direkt nach der Stimmauszählung wurde der Prozess beendet und die weitere Wahlnachbereitung wurde erstmal nicht weiter betrachtet (siehe Abbildung 12).
Im Allgemeinen dient der Referenzprozesses dazu, sich mit dem gesamten Wahlvorgang vertraut zu machen und die Modellierungsmöglichkeiten von BPMN festzustellen. Erst in den späteren Modellen wurden die einzelnen Abschnitte differenzierter modelliert und auf den Wahlvorgang in Koblenz angepasst. Aus diesem Grund ist dieser Prozess auch sehr kurz ge-

halten und Sonderfälle, sowie nähere Ausführungen verschiedener Schritte werden nicht betrachtet.

6.1.2. Use-Cases und Beschreibungen

Wie in Abbildung 1 zu sehen, sollen im zweiten Schritt Use-Cases und Use-Case-Beschreibungen angefertigt werden. Dies dient dazu alle Rollen und Anwendungsfälle sichtbar zu machen und detailliert zu beschreiben.

Als Grundlage für die Modellierung diente der oben beschriebene Referenzprozess aus Zossen. Anschließend wurde eine Schablone für die Use-Case-Beschreibungen erarbeitet, um einheitliche Beschreibungen zu ermöglichen. Die Modelle und ihre textuellen Beschreibungen dienen dann in Schritt 3 des Vorgehensmodells als Grundlage für die Modellierung der Geschäftsprozesse.

Use-Case-Beschreibungsschablone

Name	**Der Name des Use-Cases**
Akteure	Die Personen, die an dem Use-Case beteiligt sind.
Ziel	Der Zustand, welcher nach erfolgreicher Ausführung des Use-Case eintreten soll.
Auslösendes Ereignis	Tritt dieses Ereignis ein, wird der Use-Case initiiert.
Kurzbeschreibung	Der Use-Case wird kurz natürlichsprachlich spezifiziert/beschrieben.
Vorbedingung	Dieser Zustand wird erwartet, bevor der Use-Case beginnen kann.
Essenzielle Schritte	Aufzählung der essenzielle Schritte, die bei dem Use-Case unternommen werden müssen. Diese sollen in einer bestimmten Reihenfolge abgearbeitet werden.
Ausnahmefälle	Mögliche Ausnahmefälle sind hier zu nennen.
Nachbedingung	Dieser Zustand wird nach der erfolgreichen Ausführung des Use-Cases erwartet

Tabelle 1: Einheitliche Schablone für Use-Case-Beschreibungen

Tabelle 1 zeigt die vereinheitlichte Use-Case-Schablone. Diese dient als Grundlage einer detaillierten textuellen Beschreibung der Anwendungsfälle mit allen wichtigen Attributen und Eigenschaften.

Einleitend werden der Name des Anwendungsfalls, alle beteiligten Akteure und das auslösende Ereignis beschrieben. Danach wird der Use-Case kurz umschrieben und umgangssprachlich erklärt. Anschließend wird der betrachtete Anwendungsfall vertiefter untersucht und beschrieben, indem die zu erfüllenden Vorbedingungen und ein Schritt-für-Schritt Ablauf angegeben werden. Abschließend werden eventuelle Ausnahmefälle und Nachbedingungen erklärt.

Im Folgenden werden die Use-Cases für den untersuchten Wahlprozess in Koblenz beschrieben und erläutert. Bei der Auswahl dieser Use-Cases wurde versucht, den Wahlprozess in

seiner gesamten Breite abzubilden, allerdings sollte die Gesamtzahl der Use-Cases überschaubar bleiben. Zu viele Use-Cases hätten sich dabei auch auf ein dazugehöriges Diagramm negativ ausgewirkt. Um dieser Komplexität gerecht zu werden, wurden sie entsprechend der unterschiedlichen Wahlphasen (bzw. gemäß dem Ablauf der Wahl) getrennt: Wählerverzeichnis erstellen (Abbildung 13, Tabellen 2-6), Einreichung der Wahlvorschläge (Abbildung 14, Tabellen 7-10), Zulassung der Wahlvorschläge (Abbildung 15, Tabellen 11-15), die technische Durchführung der Wahl (Abbildung 16, Tabellen 16-19), der Wahlvorgang (Abbildung 17, Tabellen 20-23) und die Auszählung (Abbildung 18, Tabellen 24-29). Mit dieser Aufteilung konnte der gesamte Wahlprozess mittels Use-Cases abgebildet werden, ohne die Überschaubarkeit, auch in Hinblick auf die folgenden Diagramme, zu gefährden.

Es folgen die Use-Cases und Use-Case-Beschreibungen des untersuchten Wahlprozesses. Diese werden, gemäß der oben genannten Einteilung in die unterschiedlichen Wahlphasen, mit einer Überschrift eingeleitet. Danach folgt das dazugehörige Use-Case-Diagramm. Für die auf dem Diagramm abgebildeten Use-Cases folgen danach die entsprechenden Use-Case-Beschreibungen.

Wählerverzeichnis erstellen

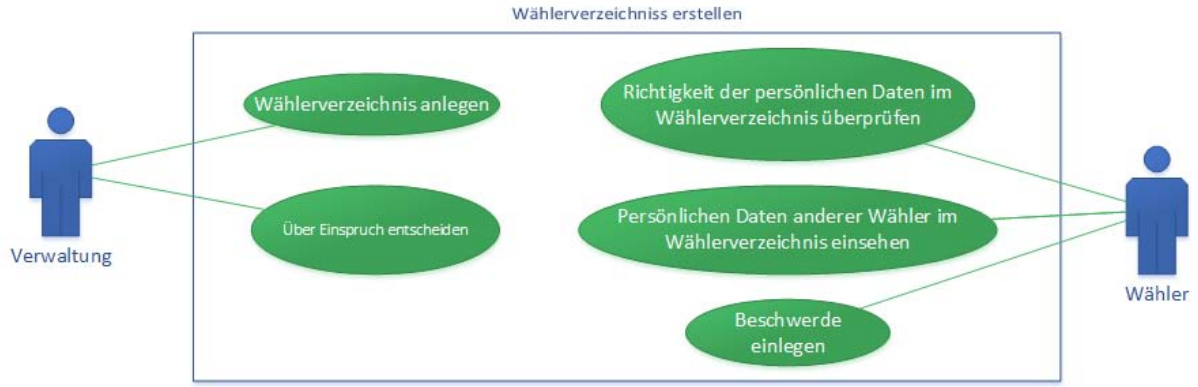

Abbildung 13: Wählerverzeichnis erstellen

Abbildung 13 veranschaulicht die Vorgänge, die beim Aufstellen des Wählerverzeichnisses eine Rolle spielen. Die folgenden fünf Use-Cases[25] wurden dabei identifiziert: „Wählerverzeichnis anlegen“, „Richtigkeit der persönlichen Daten im Wählerverzeichnis überprüfen“, „Persönliche Daten anderer Wähler im Wählerverzeichnis einsehen“, „Beschwerde einlegen“

[25] Anm. der Betreuer: Nach einem einleitenden Text, der sich auf die nachfolgenden Tabellen bezieht, folgen fünf Tabellen hintereinander. Hier wäre es besser gewesen, den erläuternden Text an Ort und Stelle – d.h. passend zu den jeweiligen Tabellen – zu platzieren. Diese Kritik gilt für die Darstellung aller folgenden Wahlphasen in gleicher Weise.

und „Über Einspruch entscheiden“. Damit Wahlberechtigte ihre Stimme abgegeben können, müssen diese im Wählerverzeichnis aufgelistet sein. Einer der ersten Schritte bei der Wahlvorbereitung ist daher das Anlegen eines Wählerverzeichnisses, in dem alle Wahlberechtigten zur Wahl aufgelistet sind (Tabelle 2). Nachdem das Wählerverzeichnis fertig erstellt wurde, hat der Wähler die Möglichkeit seine personenbezogenen Daten zu überprüfen. So stellt er sicher, dass er an der Wahl auch teilnehmen kann (Tabelle 3). Legt der Wahlberechtigte begründete Zweifel vor, so kann er auch die personenbezogenen Daten anderer Wähler einsehen (Tabelle 4). Findet der Wähler bei der Einsicht des Wählerverzeichnisses falsche Daten vor, so kann er bei der Verwaltung Einspruch gegen das bestehende Wählerverzeichnis einlegen (Tabelle 5). Die Verwaltung muss daraufhin über den Einspruch entscheiden (Tabelle 6).

Name	**Wählerverzeichnis anlegen**
Akteure	Verwaltung
Ziel	Im Wählerverzeichnis sollen alle Wahlberechtigten eingetragen sein.
Auslösendes Ereignis	Zeitliches Event: Spätestens am 35. Tag vor der Wahl.
Kurzbeschreibung	Die Gemeinde legt ein Wählerverzeichnis an, in welches alle wahlberechtigten Personen eingetragen sind.
Vorbedingung	-
Essenzielle Schritte	1. Grundlage für das Wählerverzeichnis bietet das zur vorherigen Wahl verwendete Wählerverzeichnis. 2. Überprüfung der Eintragungen im Wählerverzeichnis.
Ausnahmefälle	-
Nachbedingung	-

Tabelle 2: Use-Case „Wählerverzeichnis anlegen“

Name	**Richtigkeit der personenbezogenen Daten im Wählerverzeichnis überprüfen**
Akteure	Wähler

Prozess 1: Kommunalwahlen 2014 in Koblenz

Ziel	Der Wähler soll die personenbezogenen Daten im Wählerverzeichnis überprüfen können.
Auslösendes Ereignis	Der Wahlberechtigte möchte seine personenbezogenen Daten im Wählerverzeichnis überprüfen.
Kurzbeschreibung	Der Wahlberechtigte überprüft die Richtigkeit seiner Daten im Wählerverzeichnis.
Vorbedingung	-
Essenzielle Schritte	1. Einsicht personenbezogener Daten im Wählerverzeichnis beantragen. 2. Einsicht der personenbezogenen Daten im Wählerverzeichnis. 3. Richtigkeit der Angaben: a. Nein: Antrag auf Berichtigung des Wählerverzeichnisses stellen. b. Ja: keine Korrektur nötig.
Ausnahmefälle	-
Nachbedingung	-

Tabelle 3: Use-Case „Richtigkeit der personenbezogenen Daten im Wählerverzeichnis überprüfen“

Name	**Persönliche Daten anderer Wähler im Wählerverzeichnis einsehen**
Akteure	Wähler
Ziel	Der Wähler soll Einsicht in das Wählerverzeichnis bekommen, damit dieser die Vollständigkeit und Korrektheit der eingetragenen auf ihn bezogenen Daten sicherstellen kann.
Auslösendes Ereignis	Glaubhafte Zweifel sind vorhanden, dass das Wählerverzeichnis bezüglich a Personendaten nicht korrekt ist.
Kurzbeschreibung	Der Wahlberechtigte darf bei glaubhaft dargelegten Zweifeln das Wählerverzeichnis einsehen.

Prozess 1: Kommunalwahlen 2014 in Koblenz

Vorbedingung	-
Essenzielle Schritte	1. Der Wahlberechtigte muss glaubhafte Zweifel darlegen, dass das Wählerverzeichnis unvollständig oder unrichtig ist. 2. Der Wahlberechtigte kann das Wählerverzeichnis hinsichtlich Daten anderer Personen einsehen[26]. 3. Richtigkeit der Angaben: a. Nein: Antrag auf Berichtigung des Wählerverzeichnisses stellen. b. Ja: Keine Korrektur nötig.
Ausnahmefälle	-
Nachbedingung	-

Tabelle 4: Use-Case „Persönliche Daten anderer Wähler im Wählerverzeichnis einsehen“

Name	**Beschwerde einlegen**
Akteure	Wähler
Ziel	Das Wählerverzeichnis soll korrigiert werden.
Auslösendes Ereignis	Der Wahlberechtigte hat festgestellt, dass das Wählerverzeichnis nicht richtig oder unvollständig ist.
Kurzbeschreibung	Der Wahlberechtigte legt Beschwerde gegen die Richtigkeit des Wählerverzeichnisses ein.
Vorbedingung	-
Essenzielle Schritte	1. Der Wahlberechtigte verfasst einen Antrag auf Berichtigung des Wählerverzeichnisses. Die Unrichtigkeit oder Unvollständigkeit des Wählerverzeichnisses ist darzulegen und zu begründen. 2. Der Antrag auf Berichtigung des Wählerverzeichnisses wird vom Wahlberechtigten in einen Brief gesteckt und

[26] Anm. der Betreuer: Das ist im Allgemeinen nicht der Fall.

	zugeklebt. 3. Adressiert wird der Brief an die Gemeinde. 4. Der Wahlberechtigte gibt den Antrag bei der Post ab.
Ausnahmefälle	-
Nachbedingung	-

Tabelle 5: Use-Case „Beschwerde einlegen“

Name	**Über Einspruch entscheiden**
Akteure	Verwaltung
Ziel	Entscheidung über Einspruch soll gefällt werden.
Auslösendes Ereignis	Wahlberechtigter stellt Antrag auf Berichtigung des Wählerverzeichnisses.
Kurzbeschreibung	Die Gemeinde entscheidet über den vom Wahlberechtigten gestellten Antrag auf Berichtigung des Wählerverzeichnisses.
Vorbedingung	-
Essenzielle Schritte	1. Die Gemeinde erhält den Antrag zur Korrektur des Wählerverzeichnisses vom Wahlberechtigten. 2. Die Gemeinde prüft die Kriterien für den Einspruch. 3. Über den Einspruch des Wahlberechtigten wird entschieden: a. Ablehnung: keine Korrektur des Wählerverzeichnisses b. Annahme: Korrektur des Wählerverzeichnisses
Ausnahmefälle	-
Nachbedingung	-

Tabelle 6: Use-Case „Über Einspruch entscheiden“

Einreichung der Wahlvorschläge

Abbildung 14: Einreichung der Wahlvorschläge

Abbildung 14 zeigt den Vorgang „Einreichung der Wahlvorschläge“, welcher aus den folgenden vier Use-Cases besteht: „Wahlvorschlag einreichen“, „Wahlvorschlag prüfen“, „Vertrauensperson benachrichtigen“ und „Unterstützungsunterschriften unterschreiben“. Der Prozess beginnt damit, dass die Wahlvereinigung ihre Wahlvorschläge einreicht (Tabelle 7). Anschließend werden diese von dem Wahlleiter auf formale Mängel untersucht (Tabelle 8). Dieser entscheidet über die Zulassung oder Ablehnung der Wahlvorschläge. Wird der Wahlvorschlag abgelehnt, wird die Vertrauensperson der betroffenen Partei/Kandidaten benachrichtigt (Tabelle 9). Diese unterrichtet daraufhin die Betroffenen über die Ablehnung und deren Gründe. Des Weiteren müssen Parteien oder Kandidaten durch Unterstützungsunterschriften, die sie von den Wählern erhalten, zur Wahl aufgestellt werden (Tabelle 10). Die nachfolgenden Tabellen beleuchten ausführlich jeden einzelnen Use-Case.

Name	**Wahlvorschlag einreichen**
Akteure	Wahlvereinigung
Ziel	Die eingereichten Wahlvorschläge sollen durch den Wahlleiter vorgeprüft werden und dem Wahlausschuss zur endgültigen Zulassung vorgelegt werden.
Auslösendes Ereignis	Bekanntmachung über die Anzahl der Gemeindevertreter, die An-

	zahl der Wahlkreise sowie deren Abgrenzung, die Höchstzahl der auf einem Wahlvorschlag zu benennenden Bewerber.
Kurzbeschreibung	Bei der Einreichung der Wahlvorschläge müssen die entsprechenden Interessengruppen zunächst ihre Wahlvorschläge beim zuständigen Wahlleiter einreichen. Treten bei diesem Vorgang Mängel auf, so wird eine Vertrauensperson davon in Kenntnis gesetzt und die Bewerber besitzen die Möglichkeit diese zu beheben.
Vorbedingung	Bekanntgabe über die genauen Details der Wahl (Anzahl der Gemeindevertreter, Anzahl der Wahlkreise, etc…).
Essenzielle Schritte	1. Einreichung der Wahlvorschläge beim Wahlleiter. 2. Benachrichtigung der Vertrauensperson bei Mängeln durch den Wahlleiter sowie deren Korrektur durch die Parteien.
Ausnahmefälle	-
Nachbedingung	Nachdem die Wahlvorschläge eingereicht und vorgeprüft sind, wird über eine endgültige Zulassung dieser Vorschläge durch den Wahlausschuss entschieden.

Tabelle 7: Use-Case „Wahlvorschlag einreichen“

Name	**Wahlvorschlag prüfen**
Akteure	Wahlleiter
Ziel	Es soll eine Entscheidung über Zulassung/Ablehnung des Wahlvorschlages getroffen werden.
Auslösendes Ereignis	Alle Wahlvorschläge wurden vollständig von den Wahlvereinigungen eingereicht.
Kurzbeschreibung	Der Wahlleiter überprüft alle eingereichten Wahlvorschläge auf ihre formale Korrektheit.
Vorbedingung	Die Wahlvorschläge werden bis zum 48. Tag vor der Wahl eingereicht bzw. von wesentlichen Mängel beseitigt
Essenzielle Schritte	1. Die eingereichten Wahlvorschläge werden vom Wahlleiter

	geprüft. 2. Es wird geprüft, ob alle Bedingungen die nötig sind um die Wahlvereinigung zur Wahl aufzustellen, erfüllt wurden. 3. Sind diese Bedingungen erfüllt, wird der eigereichte Wahlvorschlag zur Wahl zugelassen. 4. Sind die Bedingungen nicht erfüllt, wird der Wahlvorschlag zurückgewiesen.
Ausnahmefälle	-
Nachbedingung	Die vorgeprüften Wahlvorschläge werden dem Wahlausschuss vorgelegt.

Tabelle 8: Use-Case „Wahlvorschlag prüfen“

Name	**Vertrauensperson benachrichtigen**
Akteure	Wahlleiter
Ziel	Die politische Vertrauensperson soll über einen zurückgewiesenen Wahlvorschlag in Kenntnis gesetzt werden.
Auslösendes Ereignis	Der Wahlvorschlag einer Wahlvereinigung wurde zurückgewiesen.
Kurzbeschreibung	Der Wahlleiter unterrichtet die politische Vertrauensperson über die Zurückweisung des eingereichten Wahlvorschlages.
Vorbedingung	Der eingereichte Wahlvorschlag wurde vom Wahlleiter aufgrund formaler Mängel zurückgewiesen.
Essenzielle Schritte	1. Der Wahlvorschlag wurde zurückgewiesen bzw. der Wahlvorschlag wurde gegen die Bedenken des Wahlleiters zugelassen. 2. Die politische Vertrauensperson der jeweiligen Wahlvereinigung wird durch den Wahlleiter über die oben genannten Umstände sofort unterrichtet.
Ausnahmefälle	-
Nachbedingung	Die politische Vertrauensperson unterrichtet die jeweilige Wahl-

	vereinigung über die Zulassung/Zurückweisung des Wahlvorschlages.

Tabelle 9: Use-Case „Vertrauensperson benachrichtigen“

Name	**Unterstützungsunterschriften unterschreiben**
Akteure	Wähler
Ziel	Die Partei/ der Kandidaten soll zur Wahl zugelassen werden.
Auslösendes Ereignis	Partei/Kandidat wurde anderweitig nicht zur Wahl aufgestellt.
Kurzbeschreibung	Dieser Use-Case verfolgt das Ziel eine Partei / einen Kandidaten zur Wahl aufzustellen, sofern er über genügend Unterstützung in der Bevölkerung verfügt. Diese Unterstützung erfolgt in Form von Unterschriften für die Partei / den Kandidaten.
Vorbedingung	Partei/Kandidat wurde nicht direkt zur Wahl zugelassen.
Essenzielle Schritte	1. Keine direkte Nominierung der Partei / des Kandidaten bei der Wahlbekanntmachung. 2. Sammeln von Unterstützungsunterschriften für Partei/Kandidat bei Wahlberechtigten. 3. Einreichung der Unterstützungsunterschriften.
Ausnahmefälle	-
Nachbedingung	Bei einer ausreichenden Anzahl von Unterstützungsunterschriften wird die Partei / der Kandidat für die Wahl aufgestellt und auf dem Wahlzettel vermerkt.

Tabelle 10: Use-Case „Unterstützungsunterschriften unterschreiben“

Zulassung der Wahlvorschläge

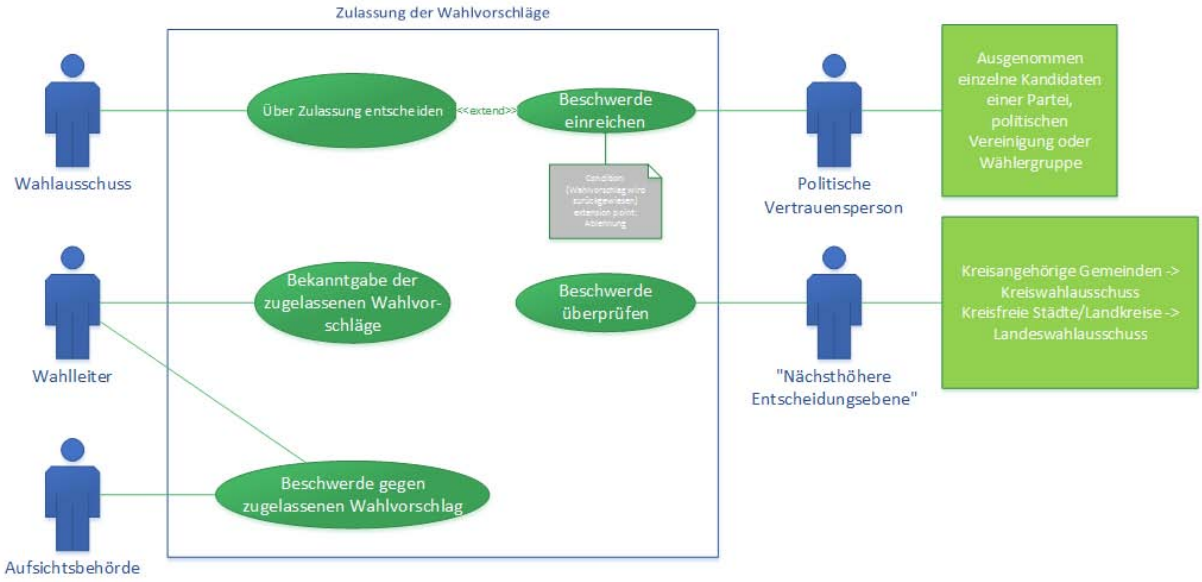

Abbildung 15: Zulassung der Wahlvorschläge

In Abbildung 15 sind die Use-Cases zur Zulassung der Wahlvorschläge abgebildet. Insgesamt werden in diesem Vorgang fünf Use-Cases beschrieben: „Über Zulassung entscheiden“, „Bekanntgabe der zugelassenen Wahlvorschläge“, „Beschwerde gegen zugelassenen Wahlvorschlag“, „Beschwerde einreichen“ und „Beschwerde überprüfen“. Auch hier werden die einzelnen Use-Cases in einer Tabelle näher erläutert. In Tabelle 11 wird der Use-Case „Über Zulassung entscheiden“ beschrieben. Hierbei fällt auf, dass keine Ausnahmefälle bestehen. Das Ziel dieses Use-Cases ist es, die Wahlvorschläge zu prüfen und zur Wahl zuzulassen. Der Use-Case „Bekanntgabe der zugelassenen Wahlvorschläge“ wird in Tabelle 12 beschrieben. Das Ziel ist es, nach öffentlicher Bekanntgabe der Wahlvorschläge, nur Wahlzettel mit zugelassenen Wahlvorschlägen zu drucken. Wird alles ordnungsgemäß durchgeführt, so entsteht die Nachbedingung, dass die technische Durchführung der Wahl vorbereitet werden kann. Der nächste Use-Case ist die „Beschwerde gegen zugelassene Wahlvorschläge“ (siehe Tabelle 13). Dort gibt es Ausnahmefälle und Nachbedingungen. Das Ziel dieses Use-Cases ist, dass der eingereichten Beschwerde stattgegeben wird und zieht gleichzeitig die Nachbedingung mit sich, dass die nächsthöhere Ebene über die Beschwerde entscheidet. In Tabelle 14 wird der Use-Case „Beschwerde einreichen“ erläutert. Hier wird das Ziel verfolgt, dass die abgelehnte Organisation durch eine Beschwerde doch noch am Wahltag wählbar ist. Bei diesem Use-Case finden jedoch keine Ausnahmefälle, sowie Nachbedingungen statt. Als letzter Use-Case zu dieser Abbildung zählt die „Beschwerde überprüfen“ (siehe Tabelle 14). Das Ziel ist die endgültige Entscheidung über die Beschwerde über einen Wahlvorschlag und nimmt so-

mit Bezug auf den Use-Case „Beschwerde gegen zugelassene Wahlvorschläge“. Als Nachbedingung wird eine finale Entscheidung über die Beschwerde getroffen.

Name	**Über Zulassung entscheiden**
Akteure	Wahlausschuss
Ziel	Die Wahlvorschläge sollen geprüft werden und vom Wahlausschuss zur Wahl zugelassen werden.
Auslösendes Ereignis	Die vorgeprüften Wahlvorschläge wurden beim Wahlausschuss eingereicht und liegen diesem vor.
Kurzbeschreibung	Der Wahllausschuss prüft die eingereichten und durch den Wahlleiter zugelassenen Wahlvorschläge. Er entscheidet nun endgültig darüber, ob die Wahlvorschläge zur Wahl zugelassen werden. Gegen die Entscheidung kann von der jeweiligen Vertrauensperson Beschwerde eingereicht werden (davon sind einzelne abgelehnte Kandidaten einer Partei, politischen Vereinigung oder Wählergruppe allerdings ausgeschlossen).
Vorbedingung	Die beim Wahlleiter eingereichten Wahlvorschläge müssen von diesem vorgeprüft und an den Wahlausschuss weitergeleitet werden.
Essenzielle Schritte	1. Entscheidung über die Wahlvorschläge durch den Wahlausschuss in öffentlicher Sitzung. 2. Innerhalb von zwei Tagen kann von einer Vertrauensperson Beschwerde gegen die Entscheidung eingereicht werden (davon sind einzelne abgelehnte Kandidaten einer Partei, politischen Vereinigung oder Wählergruppe allerdings ausgeschlossen).
Ausnahmefälle	-
Nachbedingung	Nachdem die Wahlvorschläge nun zugelassen sind muss die Beschwerdefrist von zwei Tagen eingehalten werden.

Tabelle 11: Use-Case „Über Zulassung entscheiden“

Name	**Bekanntgabe der zugelassenen Wahlvorschläge**
Akteure	Wahlleiter
Ziel	Nach der öffentlichen Bekanntgabe der Wahlvorschläge sollen die Wahlzettel mit den zugelassenen Wahlvorschlägen gedruckt werden.
Auslösendes Ereignis	Die Überprüfung der eingereichten Beschwerden sowie deren endgültige Entscheidung haben in einer öffentlichen Sitzung stattgefunden.
Kurzbeschreibung	Der Wahlleiter gibt die zur Wahl zugelassenen Wahlvorschläge der Öffentlichkeit unverzüglich bekannt.
Vorbedingung	Es wurde über die zur Wahl eingereichten Wahlvorschläge sowie über die eingereichten Beschwerden endgültig entschieden.
Essenzielle Schritte	1. Der Wahlleiter gibt die zur Wahl zugelassenen Wahlvorschläge öffentlich bekannt. 2. Die Bekanntgabe muss unverzüglich und bis spätestens zum 22. Tag vor der Wahl geschehen.
Ausnahmefälle	-
Nachbedingung	Nach der Bekanntgabe der zur Wahl zugelassenen Wahlvorschläge kann nun die technische Durchführung der Wahl vorbereitet werden.

Tabelle 12: Use-Case „Bekanntgabe der zugelassenen Wahlvorschläge“

Name	**Beschwerde gegen zugelassenen Wahlvorschlag**
Akteure	Wahlleiter, Aufsichtsbehörde
Ziel	Der eingereichten Beschwerde soll stattgegeben werden.
Auslösendes Ereignis	Der Wahlausschuss entscheidet in einer öffentlichen Sitzung über die Zulassung der Wahlvorschläge.
Kurzbeschreibung	Der Wahlleiter/ das Ordnungsamt reicht Beschwerde ein.

Prozess 1: Kommunalwahlen 2014 in Koblenz

Vorbedingung	Die öffentliche Sitzung des Wahlausschusses über die Zulassung der Wahlvorschläge hat stattgefunden.
Essenzielle Schritte	1. Der Wahlleiter/ das Ordnungsamt reicht eine Beschwerde ein. 2. Eine Beschwerde kann auch gegen die Zulassung von Wahlvorschlägen erfolgen.
Ausnahmefälle	Alle Beschwerden, die nicht innerhalb von zwei Tagen nach der öffentlichen Sitzung des Wahlausschusses eingereicht werden, finden keine Beachtung.
Nachbedingung	Die nächsthöhere Entscheidungsebene entscheidet über die Beschwerde.

Tabelle 13: Use-Case „Beschwerde gegen zugelassenen Wahlvorschlag“

Name	**Beschwerde einreichen**
Akteure	Politische Vertrauensperson
Ziel	Die zunächst abgelehnte politische Organisation soll durch eine Beschwerde doch noch am Wahltag wählbar sein.
Auslösendes Ereignis	Der Wahlausschuss hat den Wahlvorschlag einer politischen Organisation abgelehnt.
Kurzbeschreibung	Nachdem der Wahlvorschlag einer politischen Organisation abgelehnt wurde, legt die Vertrauensperson dagegen Beschwerde ein.
Vorbedingung	Der Wahlvorschlag wurde vom Wahlausschuss abgelehnt.
Essenzielle Schritte	1. Die Vertrauensperson spricht sich mit der betroffenen politischen Organisation ab. 2. Die Vertrauensperson legt eine Beschwerde gegen die Ablehnung des Wahlvorschlags ein.
Ausnahmefälle	-
Nachbedingung	-

Tabelle 14: Use-Case „Beschwerde einreichen“

Name	**Beschwerde überprüfen**
Akteure	Nächsthöhere Entscheidungsebene
Ziel	Nach der finalen Entscheidung über die eingereichte Beschwerde, sollen die Wahlvorschläge endgültig zugelassen werden.
Auslösendes Ereignis	Einreichung einer Beschwerde bei der nächsthöheren Entscheidungsebene.
Kurzbeschreibung	Die Beschwerde wird durch die nächsthöhere Entscheidungsebene geprüft und es wird in einer öffentlichen Sitzung darüber entschieden.
Vorbedingung	Die Beschwerde wurde innerhalb der vorgesehenen Frist eingereicht und liegt nun der nächsthöheren Ebene zur Überprüfung vor.
Essenzielle Schritte	1. Überprüfung der Beschwerde. 2. Entscheidung über die Beschwerde in einer öffentlichen Sitzung.
Ausnahmefälle	-
Nachbedingung	Es findet eine Entscheidung über die Beschwerde statt.

Tabelle 15: Use-Case „Beschwerde überprüfen“

Die technische Durchführung der Wahl

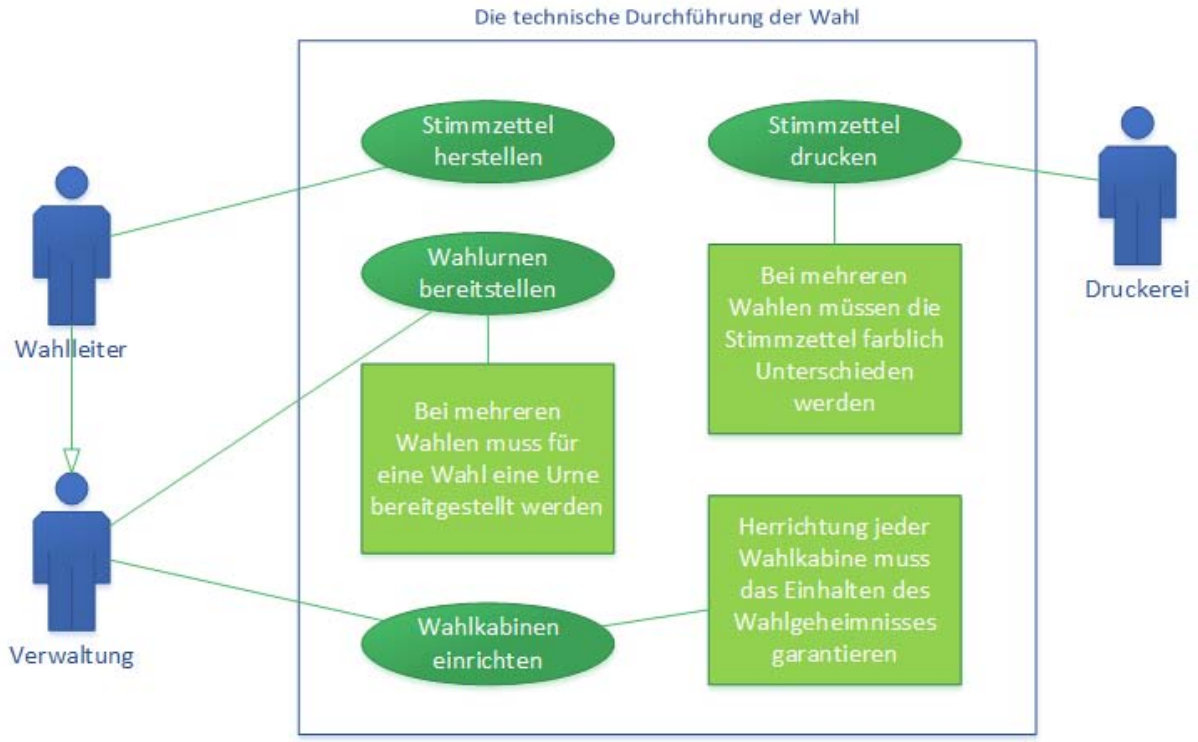

Abbildung 16: Die technische Durchführung der Wahl

Abbildung 16 veranschaulicht die Vorgänge, die für die technische Durchführung der Wahl notwendig sind. Vier Use-Cases konnten identifiziert werden: „Stimmzettel herstellen“, „Stimmzettel drucken“, „Wahlurnen bereitstellen“ und „Wahlkabinen einrichten“. Damit die Wähler im Wahllokal ihre Stimme abgeben können, benötigen sie einen Stimmzettel. Für den Druck der Stimmzettel ist der Wahlleiter verantwortlich (Tabelle 16). Damit die Stimmzettel nicht von jeder Person selbst angefertigt werden kann, müssen bestimmte Vorgaben erfüllt werden. Der Wahlleiter gibt den Auftrag an eine Druckerei, die vorgegebene Anzahl von Stimmzettel drucken soll (Tabelle 17). Des Weiteren ist die Verwaltung für die ordnungsgemäße Bereitstellung der Wahlurnen zuständig (Tabelle 18). Zu den Aufgaben der Verwaltung gehört auch das Einrichten der Wahlkabinen (Tabelle 19). Diese sollen so platziert werden, dass das Einhalten des Wahlgeheimnisses gewährleistet wird. Die nachfolgenden Tabellen beleuchten ausführlich jeden einzelnen Use-Case.

Name	**Stimmzettel herstellen**
Akteure	Wahlleiter

Prozess 1: Kommunalwahlen 2014 in Koblenz

Ziel	Stimmzettel sollen nach Vorgaben angefertigt werden.
Auslösendes Ereignis	Zugelassene Wahlvorschläge bekanntmachen.
Kurzbeschreibung	Wahlleiter gibt den Auftrag an eine Druckerei, die die Stimmzettel drucken soll.
Vorbedingung	-
Essenzielle Schritte	1. Grundlage für die Stimmzettel bilden die zugelassenen Wahlvorschläge. 2. Weitergabe des Druckauftrages an eine Druckerei.
Ausnahmefälle	-
Nachbedingung	-

Tabelle 16: Use-Case „Stimmzettel herstellen“

Name	**Stimmzettel drucken**
Akteure	Druckerei
Ziel	Für den Wahlvorgang sollen jederzeit genug Stimmzettel zur Verfügung stehen.
Auslösendes Ereignis	Die Verwaltung erteilt den Druckauftrag.
Kurzbeschreibung	Die Druckerei fertigt eine von der Verwaltung festgelegte Anzahl von Stimmzetteln an.
Vorbedingung	Das endgültige Layout des Stimmzettels steht fest.
Essenzielle Schritte	1. Die Verwaltung erteilt den Druckauftrag. 2. Die Druckerei fertigt die festgelegte Anzahl an Stimmzetteln an. 3. Die Druckerei übergibt die Stimmzettel an die Verwaltung.
Ausnahmefälle	-
Nachbedingung	Am Wahltag sind genügend korrekte Stimmzettel vorhanden

Tabelle 17: Use-Case „Stimmzettel drucken“

Name	**Wahlurnen bereitstellen**
Akteure	Verwaltung
Ziel	Am Wahltag sollen in den Wahllokalen Wahlurnen bereit stehen.
Auslösendes Ereignis	-
Kurzbeschreibung	Die Verwaltung stellt am Wahltag von ihnen kontrollierte Urnen bereit.
Vorbedingung	-
Essenzielle Schritte	1. Die Urnen werden geöffnet 2. Die Urnen und Schlösser werden auf eventuelle Beschädigungen überprüft 3. Die kontrollierten Urnen werden verschlossen.
Ausnahmefälle	- Beschädigte Urnen und Schlösser müssen ausgetauscht werden.
Nachbedingung	Die Urnen sind in einem für die Wahl ordnungsgemäßen Zustand.

Tabelle 18: Use-Case „Wahlurnen bereitstellen“

Name	**Wahlkabinen einrichten**
Akteure	Verwaltung
Ziel	Wahlräume für die Wahl sollen eingerichtet werden (einschließlich: Bereitstellung der Urnen).
Auslösendes Ereignis	Spätestens 1. Tag vor der Wahl.
Kurzbeschreibung	Die Gemeindeverwaltung ist zur Einrichtung der Wahlräume verpflichtet. Dies soll spätestens ein Tag vor der Wahl stattfinden.
Vorbedingung	-
Essenzielle Schritte	1. Alle übrigen vorbereitenden Aufgaben sollen erledigt werden.

Prozess 1: Kommunalwahlen 2014 in Koblenz

	2. Wahlräume sollen eingerichtet werden.
Ausnahmefälle	-
Nachbedingung	-

Tabelle 19: Use-Case „Wahlkabinen einrichten“

Der Wahlvorgang

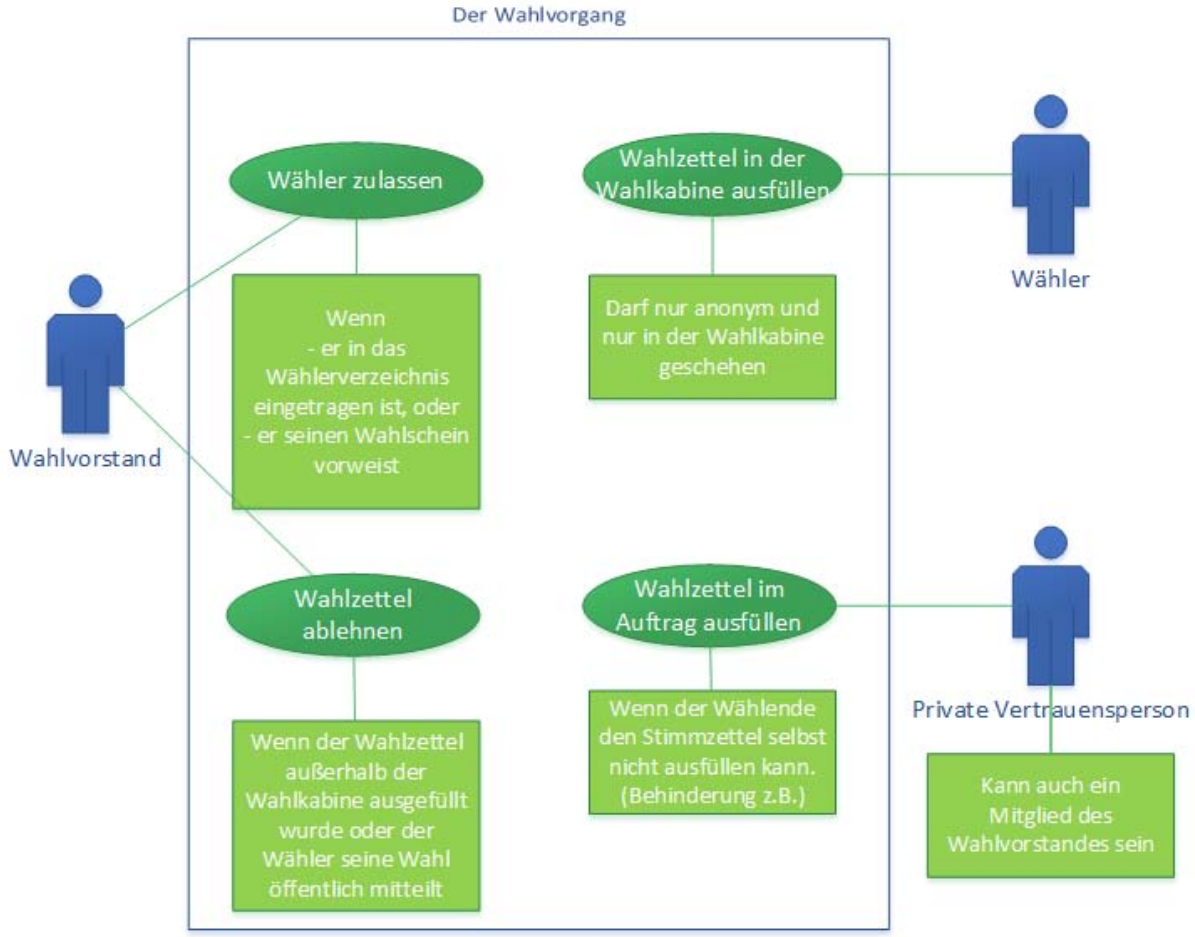

Abbildung 17: Der Wahlvorgang

Wie Abbildung 17 entnommen werden kann, besteht der Wahlvorgang aus insgesamt vier Use-Cases: „Wähler zulassen“, „Wahlzettel in der Wahlkabine ausfüllen“, „Wahlzettel ablehnen“, sowie „Wahlzettel im Auftrag ausfüllen“. Zu jeder Aktivität wurden verschiedene Rollen zugewiesen und in der Use-Case näher erläutert (siehe Tabelle 20-23).

In Tabelle 20 wird der Use-Case „Wähler zulassen“ näher erläutert. Werden alle essenziellen Schritte innerhalb des Use-Cases erfüllt, erhält der Wähler einen Wahlzettel zur Abstimmung. Tabelle 21 beschreibt den Vorgang das Ausfüllen des Wahlzettels in der Wahlkabine. Hierbei

wird bei den Ausnahmefällen inhaltlich auf Tabelle 22 verwiesen. Ist es dem Wähler nicht möglich den Wahlzettel selbstständig auszufüllen, so hat dieser die Möglichkeit den Wahlzettel im Auftrag ausfüllen zu lassen. In Tabelle 23 wird der Fall erläutert, falls der Wahlzettel des Wählers vom Wahlvorstand abgelehnt wird.

Name	**Wähler zulassen**
Akteure	Wahlvorstand
Ziel	Die Wähler sollen zur Wahl zugelassen werden und den Wahlzettel überreicht bekommen.
Auslösendes Ereignis	Der Wähler verlangt einen Wahlzettel vom Wahlvorstand.
Kurzbeschreibung	Der Wahlvorstand überprüft die Identität des Wählers, indem der Wahlschein und/oder ein Personalausweis oder ein Reisepass vom Wähler vorgezeigt wird.
Vorbedingung	Der Wähler weist sich aus.
Essenzielle Schritte	1. Der Wähler tritt an den Wahlvorstand heran. 2. Der Wahlvorstand fordert den Wähler auf sich auszuweisen. 3. Der Wahlvorstand überprüft, ob der Wähler wahlberechtigt ist. 4. Bei Berechtigung zur Wahl wird dem Wähler ein Wahlzettel übergeben.
Ausnahmefälle	-
Nachbedingung	Der Wähler erhält den Wahlzettel zur Abstimmung.

Tabelle 20: Use-Case „Wähler zulassen“

Name	**Wahlzettel in der Wahlkabine ausfüllen**
Akteure	Wähler
Ziel	Der Wähler soll innerhalb der Wahlkabine seinen Wahlzettel ausfüllen.

Prozess 1: Kommunalwahlen 2014 in Koblenz

Auslösendes Ereignis	Dem Wähler wird ein Wahlzettel ausgehändigt.
Kurzbeschreibung	Der Wähler gibt im Schutz der Wahlkabinen seine Stimme ab.
Vorbedingung	Der Wähler wurde zur Wahl zugelassen.
Essenzielle Schritte	1. Der Wähler geht mit dem Wahlzettel in die Wahlkabine. 2. Der Wähler füllt diesen in geheimer Wahl aus. 3. Der Wahlzettel wird in die Wahlurne eingeworfen.
Ausnahmefälle	Wenn der Wähler nicht in der Lage ist, den Wahlzettel selber auszufüllen, kann dieser von einer Vertrauensperson (wird vom Wähler selber gewählt, kann auch der Wahlvorstand sein) ausgefüllt werden.
Nachbedingung	Der Wahlzettel wird in die Wahlurne eingeworfen.

Tabelle 21: Use-Case „Wahlzettel in der Wahlkabine ausfüllen“

Name	**Wahlzettel im Auftrag ausfüllen**
Akteure	Private Vertrauensperson
Ziel	Die Vertrauensperson soll im Namen des Wählers den Wahlzettel ausfüllen.
Auslösendes Ereignis	Der Wähler hat einen Wahlzettel überreicht bekommen, ist jedoch nicht in der Lage den Wahlzettel auszufüllen.
Kurzbeschreibung	Der Wähler ist z.B. blind oder anderweitig verhindert, den Wahlzettel auszufüllen. Dadurch ist ihm erlaubt, eine Vertrauensperson mit in die Wahlkabine zu nehmen, die im Namen des Wählers den Wahlzettel ausfüllt.
Vorbedingung	Der Wähler ist wahlberechtigt, jedoch nicht in der Lage den Wahlzettel auszufüllen und hat demzufolge eine Vertrauensperson ernannt.
Essenzielle Schritte	1. Der Wahlvorstand überprüft die Wahlberechtigung des Wählers. 2. Der Wahlvorstand überreicht den Wahlzettel an den

	Wähler oder an die Vertrauensperson. 3. Der Wähler ernennt seine Vertrauensperson. 4. Der Wähler geht mit der Vertrauensperson in eine freie Wahlkabine. 5. Die Vertrauensperson füllt den Zettel im Auftrag des Wählers anonym aus. 6. Der Wähler oder die Vertrauensperson wirft den Wahlzettel in die Urne.
Ausnahmefälle	-
Nachbedingung	Der Wahlzettel wird in die Urne eingeworfen.

Tabelle 22: Use-Case „Wahlzettel im Auftrag ausfüllen“

Name	**Wahlzettel ablehnen**
Akteure	Wahlvorstand
Ziel	Der Wahlzettel soll nicht zur Wahl zugelassen werden.
Auslösendes Ereignis	Der Wähler hat nicht rechtmäßig den Wahlzettel ausgefüllt.
Kurzbeschreibung	Durch falsches Ausfüllen des Wahlzettels lehnt der Wahlvorstand den Wahlzettel ab und kann nicht in die Wahlurne geworfen werden.
Vorbedingung	Der Wähler hat den Wahlzettel außerhalb der Wahlkabine ausgefüllt oder teilt seine Wahl öffentlich mit.
Essenzielle Schritte	1. Der Wahlvorstand verweigert die Annahme des Wahlzettels. 2. Der Wahlzettel muss vom Wähler eigenhändig unleserlich gemacht werden.
Ausnahmefälle	-
Nachbedingung	Der Wahlzettel wird vernichtet.

Tabelle 23: Use-Case „Wahlzettel ablehnen“

Die Auszählung

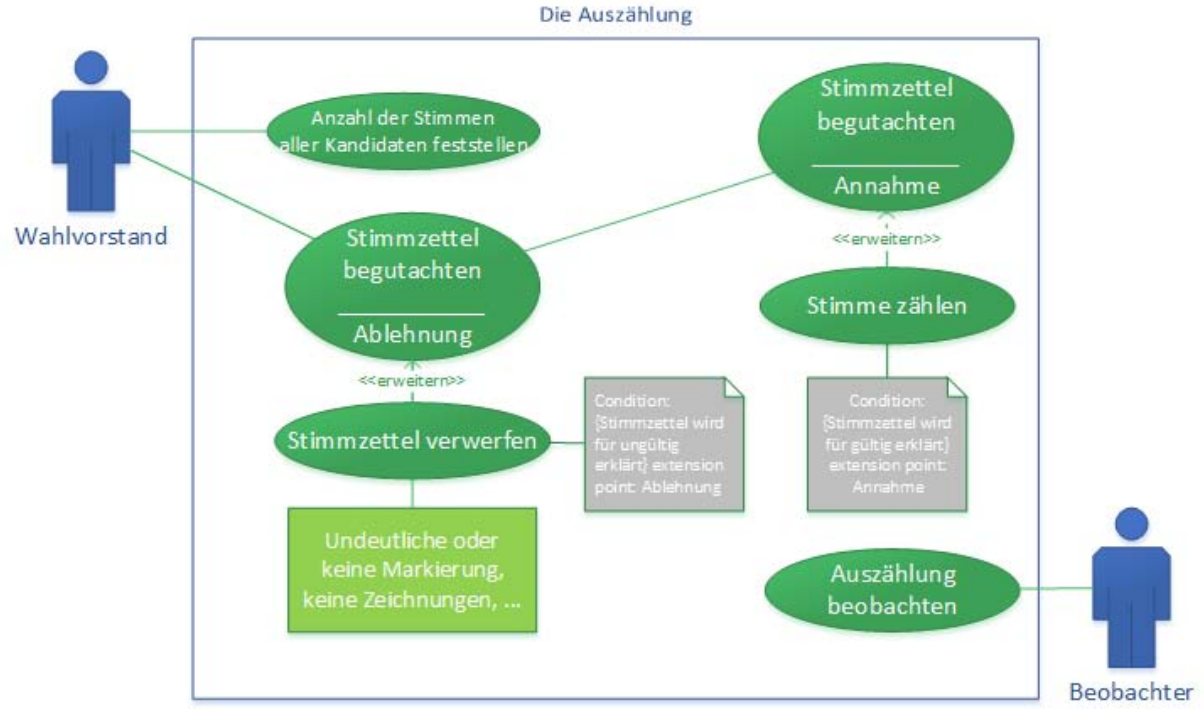

Abbildung 18: Die Auszählung

Die Abbildung 18 veranschaulicht die Vorgänge, die bei der Auszählung eine Rolle spielen. Die folgende sechs Use-Cases wurden dabei identifiziert: „Stimmzettel begutachten - Ablehnen“, „Stimmzettel verwerfen“, „Stimmzettel begutachten - Annahme“, „Stimme zählen“, „Anzahl der Stimmen aller Kandidaten feststellen“ und „Auszählung beobachten“. Nachdem die Präsenzwahl beendet wurde, werden die abgegebenen Stimmen gezählt mit dem Ergebnis die Anzahl der Stimmen für jede Partei/Kandidaten festzustellen (Tabelle 24). Dafür wird jeder Stimmzettel einzeln von mindestens einem Mitglied des Wahlvorstandes begutachtet und über dessen Gültigkeit wird entschieden. In der Abbildung wird dies über einen Extension-Point dargestellt. Wird der Stimmzettel abgelehnt (Tabelle 25), so wird er verworfen und geht nicht mit in das Wahlergebnis ein (Tabelle 26). Die Gründe dafür können vielseitig sein, zum Beispiel aufgrund von undeutlichen oder keinen Markierungen, zusätzliche Zeichnungen oder Anmerkungen. Kommt das Mitglied des Wahlvorstandes zu der Entscheidung, dass der Stimmzettel gültig ist (Tabelle27), werden die auf dem Stimmzettel enthaltenen Stimmen gezählt (Tabelle 28). Jede Person hat die Möglichkeit der Auszählung beizuwohnen und diese zu beobachten. Dadurch kann die Richtigkeit der Auszählung überprüft werden (Tabelle 29).

Name	**Anzahl der Stimmen aller Kandidaten feststellen**
Akteure	Wahlvorstand
Ziel	Die korrekte Stimmenverteilung soll festgestellt werden.
Auslösendes Ereignis	Die Wahl ist abgeschlossen und die Auszählung beginnt.
Kurzbeschreibung	Das Ergebnis dieser Zählung bestimmt das Ergebnis der Wahl und die Anzahl der Stimmen für jeden wählbaren Kandidaten.
Vorbedingung	-
Essenzielle Schritte	1. Die abgegebene Stimme wird laut vorgelesen. 2. Diese wird in notiert und in eine digitale Datenbank eingetragen Diese Schritte werden einzeln nach dem Vier-Augen-Prinzip kontrolliert.
Ausnahmefälle	-
Nachbedingung	-

Tabelle 24: Use-Case „Anzahl der Stimmen aller Kandidaten feststellen“

Name	**Stimmzettel begutachten, Extension Point: Ablehnung**
Akteure	Wahlvorstand
Ziel	Der Stimmzettel soll unter Begutachtung und Beachtung der Regeln abgelehnt werden.
Auslösendes Ereignis	Der Stimmzettel ist nicht ordnungsgemäß ausgefüllt oder in einer anderen ordnungswidrigen Art und Weise entwertet.
Kurzbeschreibung	Der Wahlvorstand begutachtet den Stimmzettel und kommt darin überein, dass der Stimmzettel nicht verwertbar ist.
Vorbedingung	Der Stimmzettel wurde in irgendeiner Form nicht ordnungsgemäß ausgefüllt.
Essenzielle Schritte	1. Jedes Mitglied des Wahlvorstandes begutachtet den Stimmzettel. Sie kommen darin überein, dass der

	Stimmzettel nicht ordnungsgemäß ausgefüllt wurde und somit nicht gezählt werden kann.
Ausnahmefälle	Einer oder mehrere Mitglieder des Wahlvorstandes legen Einspruch ein und begründen, warum der vorliegende Stimmzettel doch gewertet werden sollte.
Nachbedingung	Der Stimmzettel ist nicht zählbar und wird somit nicht gewertet.

Tabelle 25: Use-Case „Stimmzettel begutachten, Extension Point: Ablehnung“

Name	**Stimmzettel verwerfen**
Akteure	Wahlvorstand
Ziel	Ein Stimmzettel, der vorher als ungültig entschieden wurde, soll verworfen und nicht gezählt werden.
Auslösendes Ereignis	Es wurde beobachtet und festgestellt, dass der Stimmzettel nicht ordnungsgemäß ausgefüllt wurde.
Kurzbeschreibung	Der falsch ausgefüllte Stimmzettel wird aus dem Pool der zu zählenden Stimmen entnommen.
Vorbedingung	Der Stimmzettel ist den Regeln entsprechend nicht verwertbar ausgefüllt. Das kann beispielsweise durch falsches Ausfüllen oder durch Kritzeleien geschehen.
Essenzielle Schritte	1. Der Wahlzettel wird verworfen. 2. Wenn die Wahl beendet ist, wird der Stimmzettel mit in das Paket übernommen, in dem die falsch ausgefüllten Stimmzettel gesammelt werden.
Ausnahmefälle	Der Wähler kann den Stimmzettel auch selbst vor den Augen des Wahlvorstandes vernichten, sofern er glaubhaft machen kann, dass dieser von ihm falsch ausgefüllt wurde und erhält einen neuen.
Nachbedingung	Der betreffende Stimmzettel wurde nicht gezählt.

Tabelle 26: Use-Case „Stimmzettel verwerfen“

Name	**Stimmzettel begutachten, Extension Point: Annahme**
Akteure	Wahlvorstand
Ziel	Der Stimmzettel soll unter Begutachtung und Beachtung der Regeln angenommen.
Auslösendes Ereignis	Der Stimmzettel ist ordnungsgemäß ausgefüllt.
Kurzbeschreibung	Der Wahlvorstand begutachtet den Stimmzettel und kommt darin überein, dass der Stimmzettel verwertbar ist.
Vorbedingung	Der Stimmzettel wurde ordnungsgemäß ausgefüllt.
Essenzielle Schritte	1. Jedes Mitglied des Wahlvorstandes begutachtet den Stimmzettel. Sie kommen darin überein, dass der Stimmzettel ordnungsgemäß ausgefüllt wurde und gezählt werden kann.
Ausnahmefälle	Einer oder mehrere Mitglieder des Wahlvorstandes legen Einspruch ein und begründen, warum der vorliegende Stimmzettel nicht gewertet werden sollte.
Nachbedingung	Der Stimmzettel ist zählbar und das Ergebnis geht mit in das Wahlergebnis ein. Danach wird dieser in das entsprechende Paket gepackt, in dem nur die angenommenen Stimmzettel gesammelt werden, um danach bis kurz vor der nächsten Wahl gelagert zu werden.

Tabelle 27: Use-Case „Stimmzettel begutachten, Extension Point: Annahme“

Name	**Stimme zählen**
Akteure	Wahlvorstand
Ziel	Ein Stimmzettel, der vorher als gültig entschieden wurde, soll gewertet werden.
Auslösendes Ereignis	Der Stimmzettel wurde begutachtet und als verwertbar eingestuft.
Kurzbeschreibung	Der korrekt ausgefüllte Stimmzettel wird in den Pool der zu zäh-

	lenden Stimmen aufgenommen.
Vorbedingung	Der Stimmzettel ist den Regeln entsprechend verwertbar ausgefüllt.
Essenzielle Schritte	1. Er wird positiv beurteilt 2. Die abgegebene Stimme wird gezählt
Ausnahmefälle	-
Nachbedingung	Der betreffende Stimmzettel wird gezählt und der Inhalt geht in die Wahl mit ein.

Tabelle 28: Use-Case „Stimme zählen“

Name	**Auszählung beobachten**
Akteure	Beobachter
Ziel	Der Beobachter soll die Korrektheit der Auszählung verifizieren.
Auslösendes Ereignis	Die Stimmzettel sind korrekt sortiert und nur die verwertbaren Stimmzettel liegen zur Zählung vor.
Kurzbeschreibung	Die Beobachter wohnen der Auszählung bei und bestätigen damit die Korrektheit eben dieser.
Vorbedingung	-
Essenzielle Schritte	1. Der Auszählung beiwohnen.
Ausnahmefälle	Sollte der Beobachter Fehler bei der Auszählung feststellen, so sollte er dies beim Wahlvorstand ansprechen und eine Neuzählung erwirken.
Nachbedingung	-

Tabelle 29: Use-Case „Auszählung beobachten“

6.2. Wahlprozess in BPMN[27]

Nach einer allgemeinen Einarbeitung in die Thematik Wahlen sowie BPMN hat das Projektteam mit der detaillierten Modellierung des Wahlprozesses begonnen. Hierbei wurden die Kommunalwahlen Koblenz 2014 als Anwendungsfall genommen. Der Modellierung zu Grunde lagen die Kommunalwahlordnung sowie einen vom Ordnungsamt erhaltenen Terminkalender für die Vorbereitung und Durchführung der Kommunalwahlen. Diese beiden Dokumente wurden durch die Stadtverwaltung Koblenz zur Verfügung gestellt. Des Weiteren konnten bei einem Workshop im Ordnungsamt weiteres Wissen sowie genauere Kenntnisse darüber gewonnen werden, welche für die Erstellung des spezifischen Prozessmodells hilfreich waren. Aufgrund der Komplexität des Wahlprozesses wurde für jede Wahlphase ein seperates BPMN-Modell erstellt. Damit konnte die Transparenz und Verständlichkeit gewährleistet werden. Die Lanes wurden nach den identifizierten Zuständigkeiten benannt und die Aufgaben und Verantwortlichkeiten konnten auf Grundlage der vorliegenden Dokumente strukturiert dargestellt werden. Aufgrund von Überlappungen bei der Zuständigkeit wurde das Ordnungsamtes und der Oberbürgermeister zur Vereinfachung als Verwaltung zusammengefasst.

Um die Reihenfolge der verschiedenen Aktivitäten aufzuzeigen, wurden sogenannte Identifier eingesetzt. Insgesamt wird zwischen vier verschiedenen Identifiern unterschieden. Die Aktivitäten werden vor der Nummerierung mit einem „A“ gekennzeichnet, Gateways mit einem „G“, Startereignisse mit einem „S“ und Zwischenereignisse mit einem „Z“. Des Weiteren zeigen sich die verschiedenen Phasen in den Identifiern. Bei der Wahlvorbereitung steht zuerst eine „0“, bei der Stimmabgabe eine „1“, bei der Stimmauszählung eine „2“ und bei der Wahlnachbereitung eine „3“. Die Aktivitäten, Gateways und Ereignisse wurden anhand des Ablaufes aufsteigend nummeriert.

6.2.1. BPMN-Prozessmodell: Wahlvorbereitung

Die Wahlvorbereitung stellt den ersten Teilprozess der Wahl dar. Hierbei wird das Augenmerk auf die Vorbereitung der Kommunalwahl gelegt.

[27] Anm. der Betreuer: Die Darstellung bzw. die Beschreibung des Wahlprozesses ist ohne Anspruch auf Vollständigkeit oder absolute Korrektheit. Eine umfassende Prozessaufnahme mit Vollständigkeitsprüfung hätte den zeitlichen und fachlichen Rahmen eines studentischen Forschungspraktikums gesprengt.

Prozess 1: Kommunalwahlen 2014 in Koblenz

Um eine Übersicht über die Wahlvorbereitung zu schaffen, wurden die beteiligten Parteien mit Hilfe der Kommunalwahlordnung und einem Expertengespräch mit dem Ordnungsamt identifiziert. Diese wurden in Form der folgenden Rollen berücksichtigt: *Parteien und Wählergruppen*, *Vertrauensperson der Partei*, *Wähler* sowie die *Wahlorganisation*, die aus den Lanes *Verwaltung* und *Wahlausschuss* zusammengesetzt wurde. Die *Vertrauensperson der Partei* wurde als sogenannte „black box" dargestellt, da diese eine geringere Rolle in der Wahlvorbereitung spielt. In einer groben Übersicht ist der Verlauf der Wahlvorbereitung zu erkennen (siehe Abbildung 19).

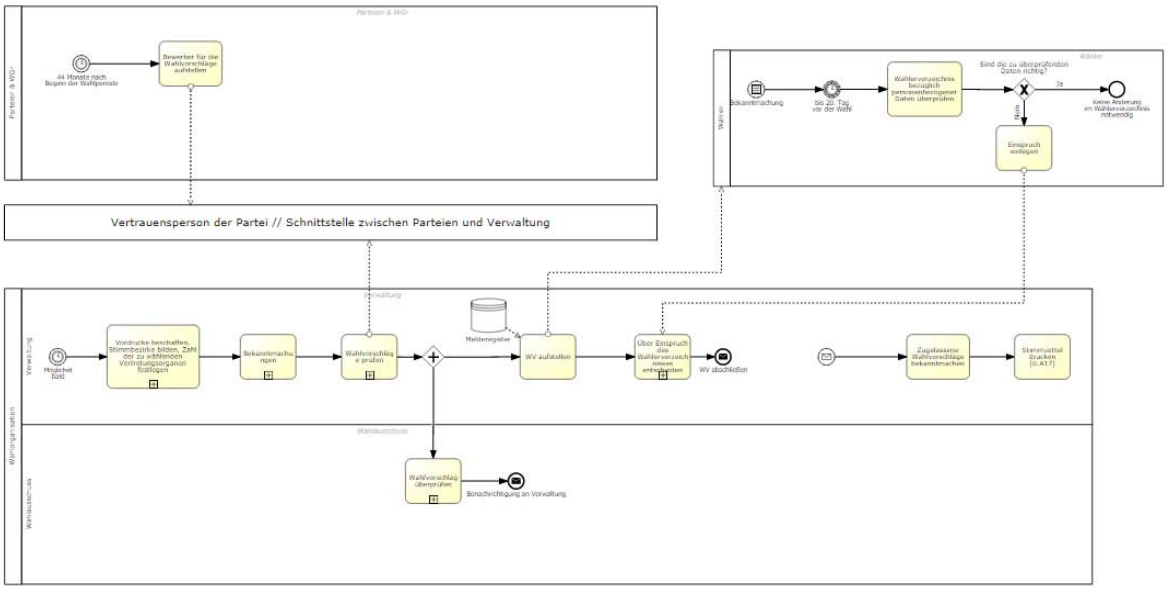

Abbildung 19: Übersicht der Wahlvorbereitung

Den einzelnen Rollen – dargestellt durch Pools und Lanes - wurden, basierend auf der Wahlverordnung, Aktivitäten zugewiesen und chronologisch dargestellt. Die Anfangsaktivität startet bei der *Verwaltung*. Hier werden zum frühest möglichen Zeitpunkt Vordrucke beschafft, Stimmbezirke gebildet und die Zahl der Vertretungsorgane festgelegt [0.A03]. Da diese Aktivitäten wenig Einfluss auf den anschließenden Wahlvorgang hat und wesentliche Informationen zur richtigen Darstellung fehlen, wurde diese Aktivität als zugeklappter Unterprozess dargestellt. Als nächstes gibt die *Verwaltung* öffentlich die Aufforderung zur Einreichung der Wahlvorschläge in der Rhein-Zeitung und die Aufforderung zur Eintragung der von der Meldepflicht befreiten wahlberechtigten EU-Bürger in das Wählverzeichnis bekannt [0.A04] und [0.A05]. Diese beiden Aktivitäten wurden in einem aufgeklappten Unterprozess dargestellt. Der zugeklappte Unterprozess wurde gewählt, da der Prozess „Bekanntmachungen" zusam-

mengefasst dargestellt werden kann. Jedoch wurde der aufgeklappte Unterprozess gewählt, damit eingesehen werden kann, welche Aktivitäten beteiligt sind (siehe Abbildung 20).

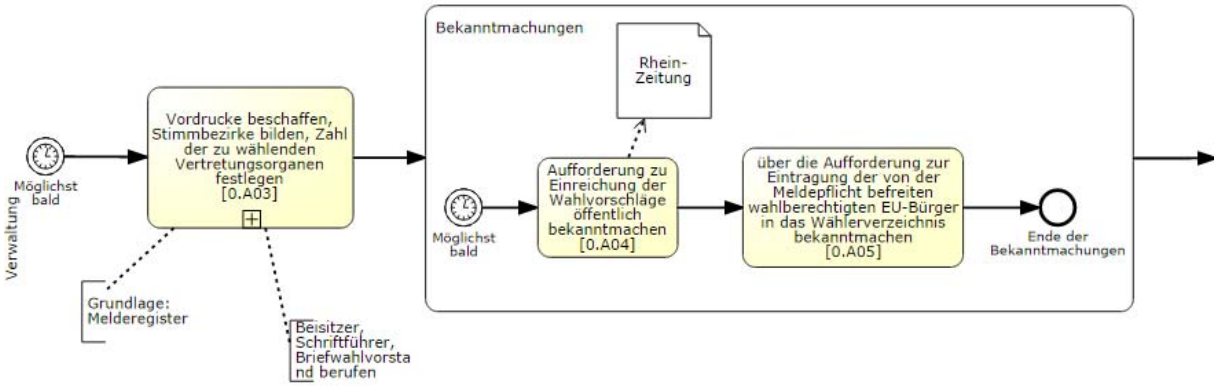

Abbildung 20: Startereignis des Prozesses Wahlvorbereitung

Parallel werden in der Lane *Parteien und Wählergruppe* 44 Monate nach Beginn der Wahlperiode die Bewerber für die Wahlvorschläge aufgestellt [0.A01]. Als Voraussetzung hierfür müssen allerdings genügend Unterstützungsunterschriften vorliegen (siehe Abbildung 21). Diese Wahlvorschläge werden anschließend an die *Vertrauensperson* weitergegeben, um diese von der *Verwaltung* überprüfen zu lassen. Im aufgeklappten Unterprozess werden spätestens am 48.Tag vor der Wahl die Wahlvorschläge überprüft [0.A06]. Danach wird in einem datenbasierten exklusivem Gateway festgestellt, ob Wahlvorschläge angenommen [0.A07] oder zurückgewiesen wurden [0.A08]. Dieser Unterprozess wird mit einem Nachrichtenendereignis an die *Vertrauensperson* abgeschlossen.

Prozess 1: Kommunalwahlen 2014 in Koblenz

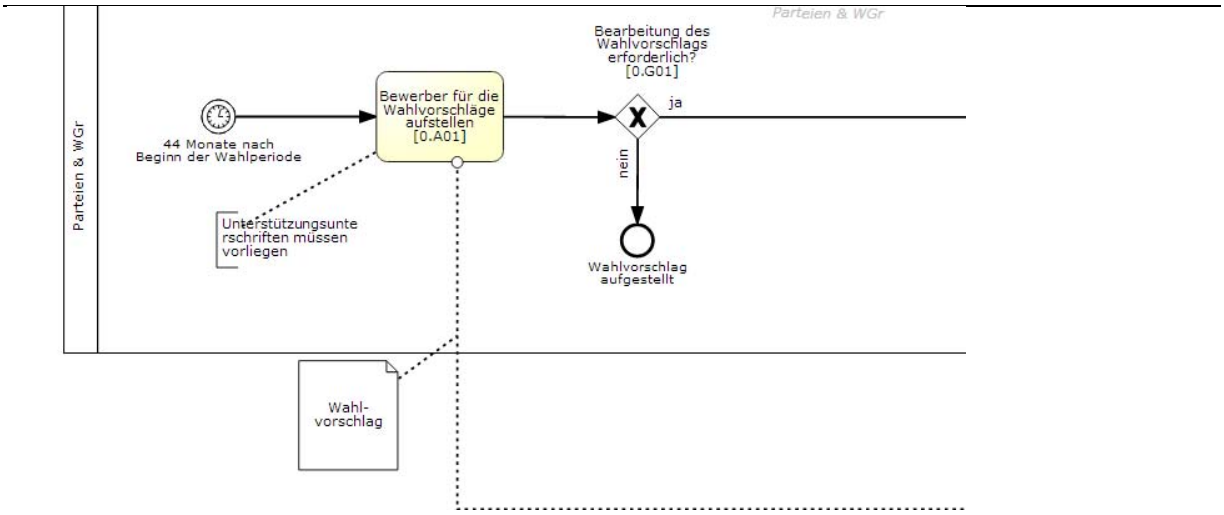

Abbildung 21: Bewerber für die Wahl aufstellen

Die *Vertrauensperson* gibt Rückmeldung an die *Parteien und Wählergruppen*, um bei einer negativen Antwort der *Verwaltung* die Wahlvorschläge erneut zu bearbeiten [0.A02]. Die überarbeiteten Wahlvorschläge werden anschließend wieder von der *Verwaltung* überprüft, solange diese im bestimmten Zeitrahmen eingereicht wurden (siehe Abbildung 22).

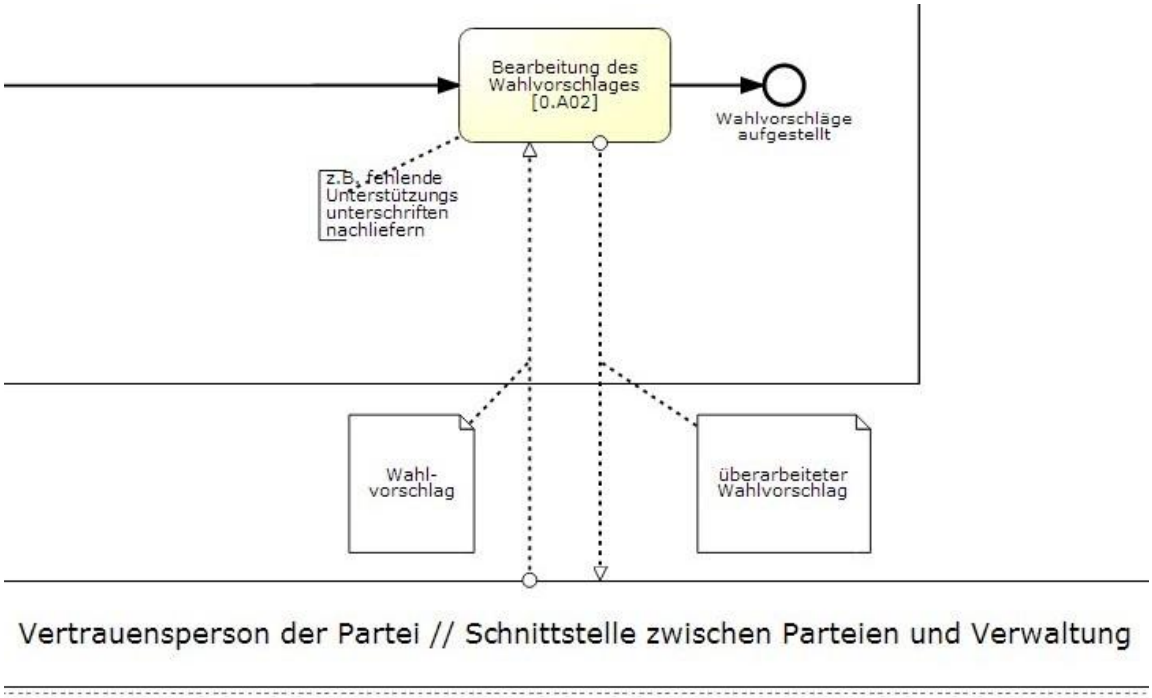

Abbildung 22: „Zusammenspiel zwischen Parteien und Wählergruppen“ und der „Vertrauensperson“

Nach der Überprüfung des Wahlvorschlages der *Verwaltung* werden diese an den *Wahlausschuss* weitergeleitet, die wiederum eine Prüfung der Wahlvorschläge vollziehen. Gleichzeitig begibt sich die *Verwaltung* an weitere Aufgaben der Wahlvorbereitung, welches durch ein paralleles Gateway [0.G03] gekennzeichnet ist.

Der Überprüfung des Wahlvorschlages des *Wahlausschusses* wird in einem aufgeklappten Unterprozess dargestellt, damit die Zugehörigkeit der einzelnen Aktivitäten verdeutlicht wird (siehe Abbildung 23).

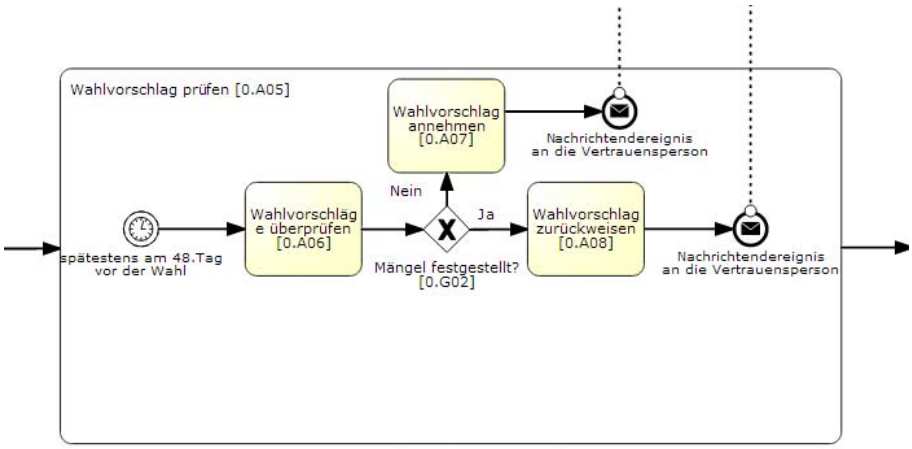

Abbildung 23: Unterprozess „Wahlvorschlag prüfen“

Um die Entscheidung über die Wahlvorschläge festzusetzen, wird eine Sitzung zur Entscheidung über die Zulassung der erhaltenen Wahlvorschläge abgehalten [0.A09] und die abschließende Annahme des Wahlvorschlages überprüft [0.A10]. Dies basiert auf den bereits überprüften und genehmigten Wahlvorschlägen der *Verwaltung*. Bei einer Feststellung von Mängeln des *Wahlausschusses* wird der Wahlvorschlag abgelehnt [0.A11] und der Prozess an dieser Stelle beendet. Bei einer positiven Antwort wird jedoch der Wahlvorschlag angenommen [0.A12] und anschließend die *Verwaltung* unterrichtet, sowie der *Landeswahlleiter* informiert. Spätestens am 47.Tag vor der Wahl werden von der *Verwaltung* die Beisitzer und deren Stellvertreter in den Wahlausschuss berufen [0.A13] und spätestens 45-40 Tage vor der Wahl das Wählerverzeichnis aufgestellt [0.A14]. Diese Daten basieren auf dem Melderegister; nach dem Abschluss des Wählerverzeichnisses wird dies in der Rhein-Zeitung bekanntgegeben. Am 20.Tag vor der Wahl werden die Wahlvorsteher, Briefwahlvorsteher und ihre Stellvertreter bestellt und verpflichtet [0.A15].

Als nächstes werden nach einem parallelen Gateway [0.G06] zum einen Wahlvorstand und Briefwahlvorsteher unterrichtet [0.A21] und die Wahlräume [0.A22] bestimmt. Spätestens einen Tag vor der Wahl werden die Wahlräume eingerichtet [0.A23]. Der Prozess wird an dieser Stelle beendet.

Gleichzeitig werden vorbereitende Maßnahmen für den Einsatz der elektronischen Software getroffen [0.A24] und die JVA in einem Rundschreiben über die bevorstehende Wahl unterrichtet [0.A25]. Auch an dieser Stelle wird der Prozess beendet (siehe Abbildung 24).

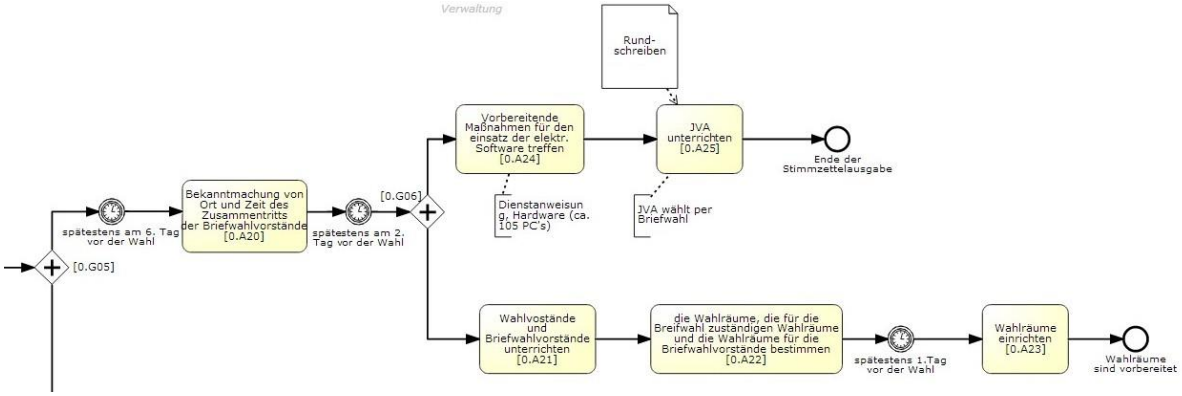

Abbildung 24: Wahlbekanntmachung und abschließende Vorbereitungen

Eine weitere Lane sind die *Wähler*. Hier können nach der Bekanntmachung über die Erstellung des Wählerverzeichnisses bis 20 Tage vor der Wahl personenbezogene Daten im Wählerverzeichnis überprüft werden [0.A26]. Anschließend wird überprüft, ob alle Angaben seine Richtigkeit haben [0.G08]. Wird ein Fehler vom *Wähler* festgestellt, so hat dieser die Möglichkeit einen Einspruch einzulegen [0.A27]. Falls keine Fehler vorhanden sind, findet keine Änderung im Wählerverzeichnis statt und der Prozess ist beendet (siehe Abbildung 25).

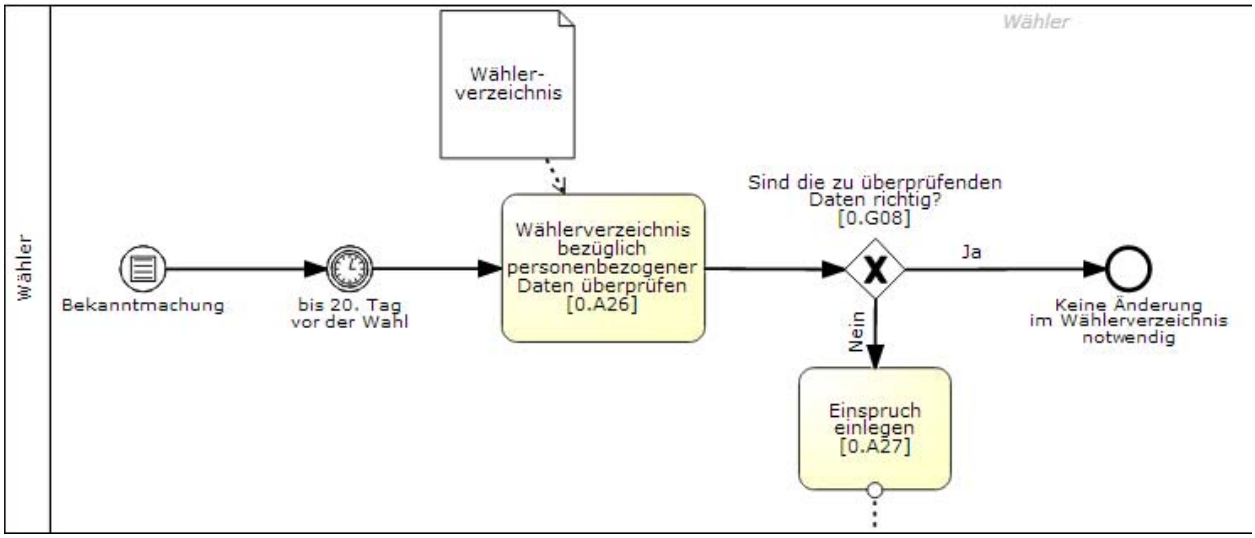

Abbildung 25: Einspruch des Wählerverzeichnisses

Der Einspruch über das Wählerverzeichnis wird von der *Verwaltung* entschieden. Dies wird in einem aufgeklappten Unterprozess dargestellt. Diese Modellierung wurde ausgewählt, um den Zusammenhang der einzelnen Aktivitäten zu verdeutlichen. Die *Verwaltung* entscheidet durch das Eintreffen eines Nachrichtensignals über den Einspruch [0.A28]. Im XOR-Gateway

wird festgestellt, ob der Einspruch berechtigt ist. Ist dies nicht der Fall, wird der *Wähler* über die Ablehnung des Einspruches benachrichtigt und der Prozess beendet. Ist der Einspruch berechtigt, dann wird das Wählerverzeichnis geändert [0.A29] und eine neue Wahlbenachrichtigung an den *Wähler* geschickt. Am 2.Tag vor der Wahl wird das Wählerverzeichnis abgeschlossen [0.A30]. Das aktualisierte Wählerverzeichnis wird freigegeben und der Prozess beendet (siehe Abbildung 26).

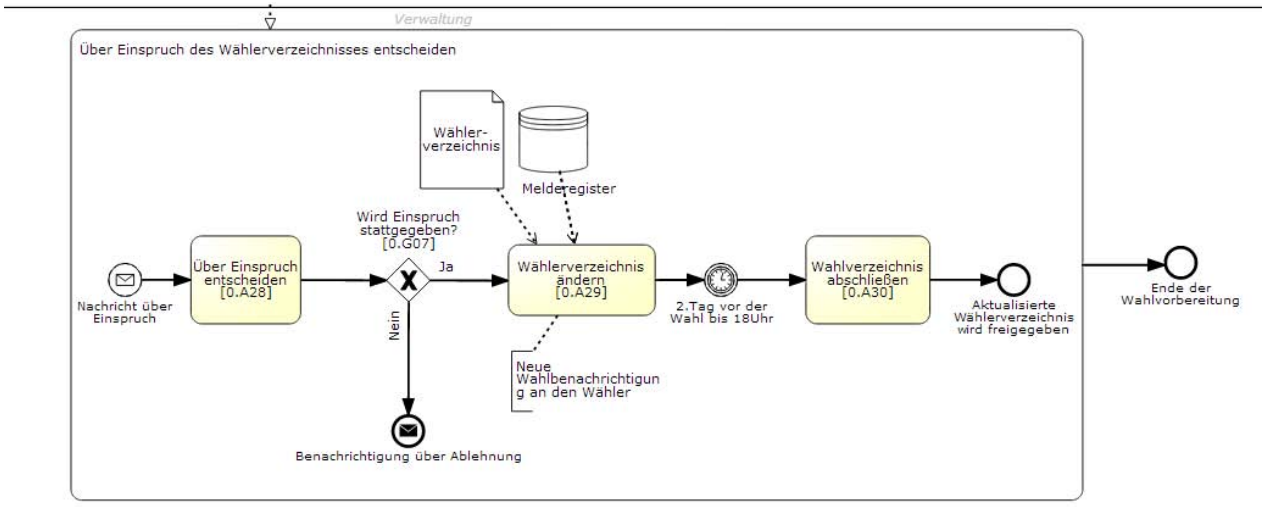

Abbildung 26: Ende des Prozesses Wahlvorbereitung

6.2.2. BPMN-Prozessmodell: Stimmabgabe

Zunächst wurden für die Modellierung der Stimmabgabe in BPMN die beteiligten Akteure bestimmt. An der Stimmabgabe vor Ort beziehungsweise an der Briefwahl sind der *Wähler*, die *Verwaltung* sowie der *Wahlvorstand* beteiligt. Abbildung 27 gibt eine vereinfachte Übersicht über die zu betrachtenden Schritte bei der Stimmabgabe. Auf jeden einzelnen Aspekt wird in der nachfolgenden Ausarbeitung genauer eingegangen.

Prozess 1: Kommunalwahlen 2014 in Koblenz

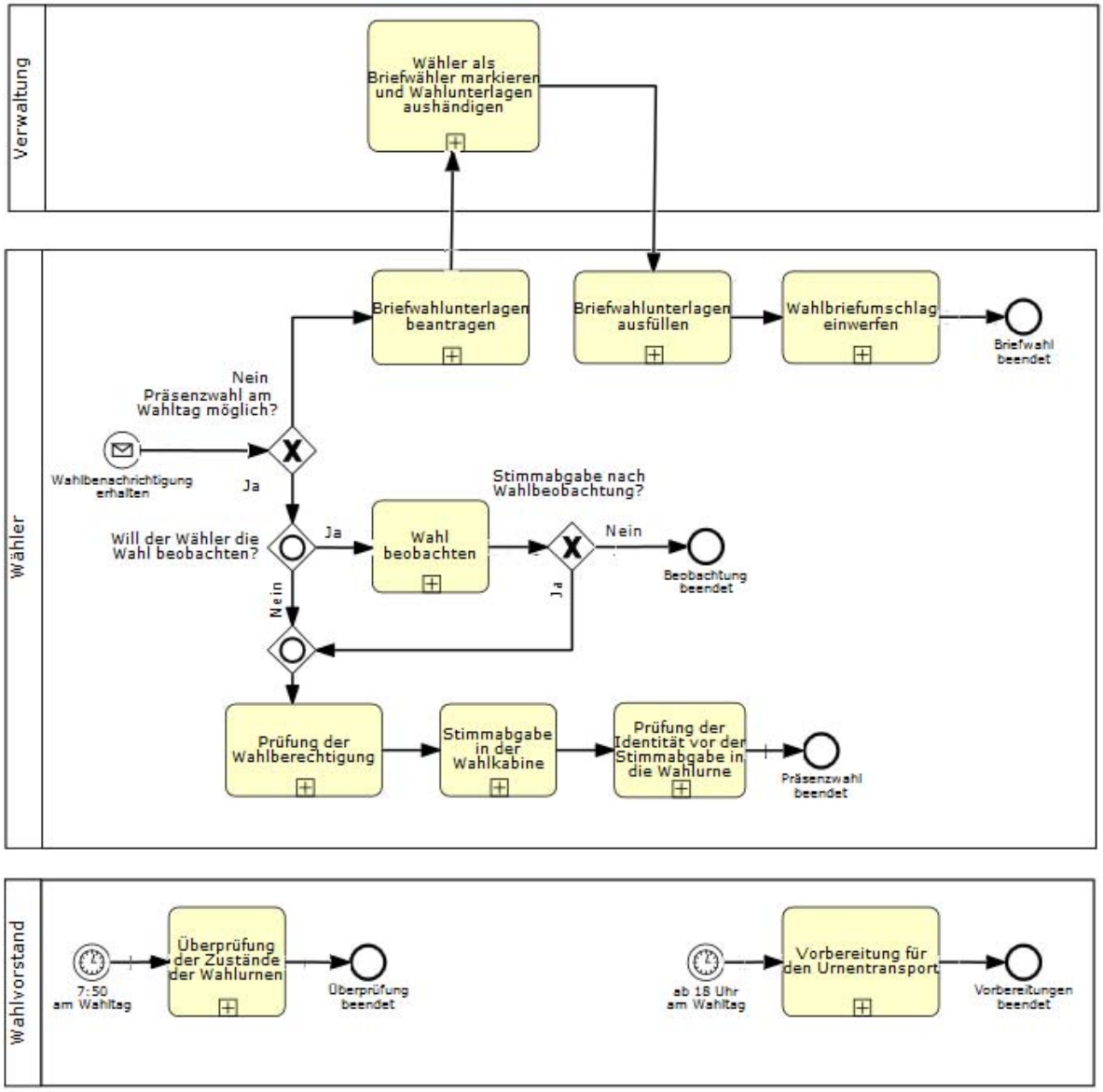

Abbildung 27: Vereinfachte Darstellung der Stimmabgabe

Bevor das Wahllokal um 8 Uhr für alle Wähler bis 18 Uhr öffnet, muss der *Wahlvorstand* gegen 7:50 Uhr den leeren Zustand der Wahlurne sicherstellen [1.A47]. Ist dies geschehen, wird die Wahlurne vom *Vorsitzenden des Wahlvorstandes* mit einem Schloss versehen und verschlossen [1.A48]. Den Schlüssel behält der Vorsitzende des Wahlvorstandes bei sich und gibt ihn keiner Person ab. Die Sicherstellung der leeren Wahlurne ist somit abgeschlossen (siehe Abbildung 28).

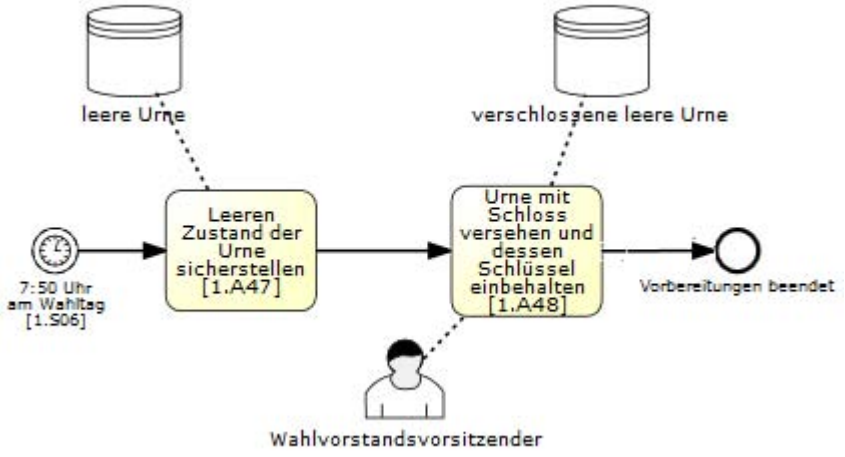

Abbildung 28: Überprüfen der Zustände der Wahlurnen

Wie Abbildung 29 zeigt, muss der *Wahlberechtigte* nach Erhalt der Wahlbenachrichtigung entscheiden, ob die Präsenzwahl am Wahltag möglich ist [1.G01]. Sollte dies nicht der Fall sein, wird angenommen, dass der *Wahlberechtigte* durch Briefwahl seine Stimme abgibt [1.S01]. Die Beantragung der Briefwahlunterlagen wurde als aufgeklappter Unterprozess modelliert, da mehrere Beantragungsalternativen möglich sind. Dies wird im Diagramm durch die Modellierung der Auswahlmöglichkeiten [1.G02] abgebildet. Der *Wahlberechtigte* hat die Möglichkeit seine Briefwahlunterlagen persönlich vor Ort abzuholen [1.A02], sie formlos per Mail oder Telefon bei der *Verwaltung* zu beantragen [1.A04] oder von einem Bevollmächtigten mitgebracht zu bekommen [1.A03]. Der Bevollmächtigte muss bei Abholung der Briefwahlunterlagen die Vollmachten sowie seinen Personalausweis vorzeigen. Insgesamt darf er nicht mehr als vier Wahlunterlagen mitnehmen, da sonst ein Wahlbetrug in größerem Ausmaß möglich wäre. Die Beantragung durch das Ausfüllen des Wahlscheins ist durch die Übersendung des Wahlantrages an die *Verwaltung* dargestellt. Briefwahlunterlagen können bis zum zweiten Tag vor der Wahl bis 18 Uhr beantragt werden; im Krankheitsfall sogar bis 15 Uhr am Wahltag.

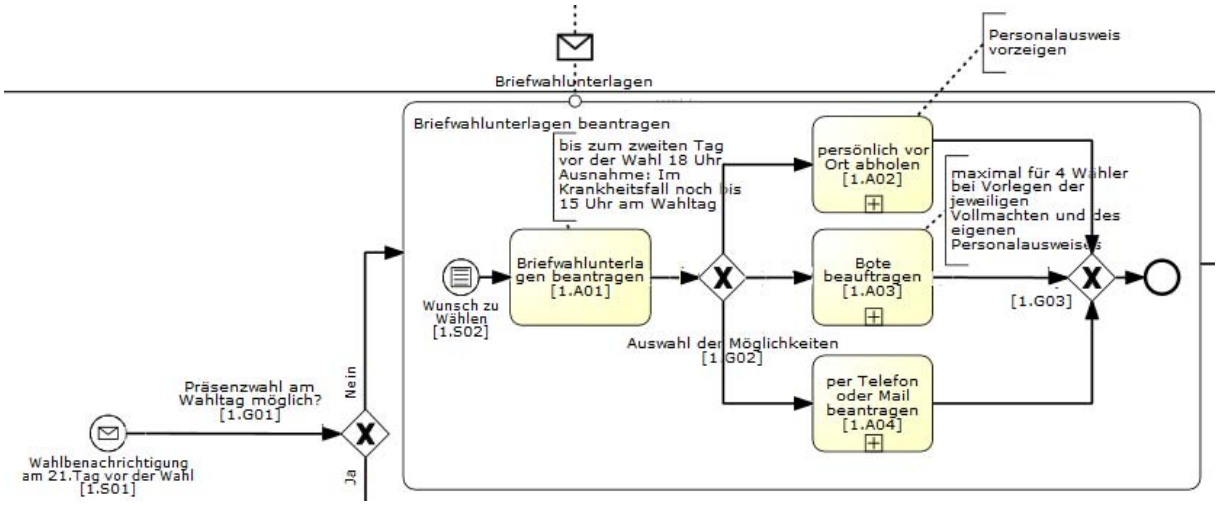

Abbildung 29: Briefwahlunterlagen beantragen

Trifft der Briefwahlantrag des *Wahlberechtigten* bei der *Verwaltung* ein, wird dieser in dem von PC-Wahl gespeicherten Wählerverzeichnis als Briefwähler markiert [1.A05]. In einem nächsten Schritt werden die Wahlunterlagen dem *Wähler* ausgehändigt [1.A06]. Die Übersendung der Unterlagen wird im BPMN-Diagramm durch den Kommunikationsfluss zwischen *Verwaltung* und dem *Wähler* dargestellt. Während der Bearbeitung des Briefwahlantrages gilt ein Vier-Augen-Prinzip bei der *Verwaltung*, d.h. alle Vorgänge werden von mindestens zwei Personen ausgeführt. Diese Maßnahme wurde eingeführt, um interne Manipulationen am Wählerverzeichnis oder an den erhaltenen Wahlanträgen beziehungsweise der Versendung der Wahlunterlagen zu verhindern (siehe Abbildung 30).

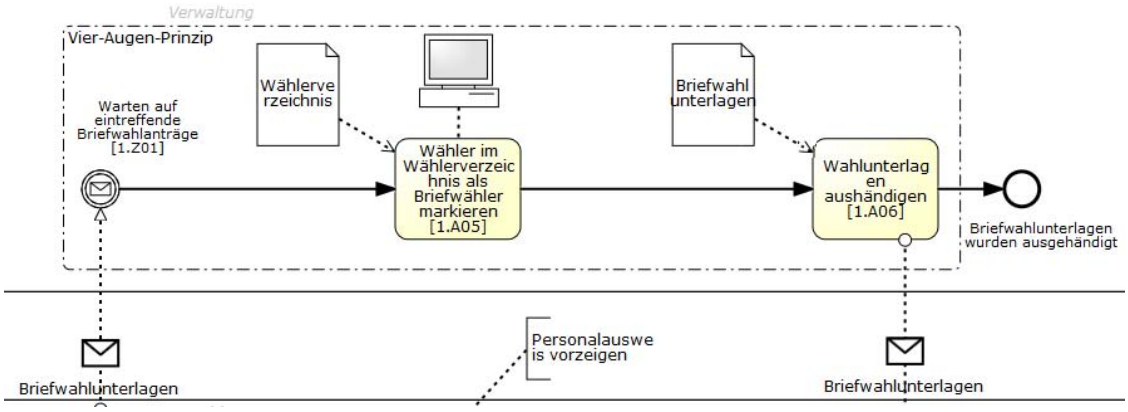

Abbildung 30: Wähler als Briefwähler markieren und Unterlagen aushändigen

Abbildung 31 beginnt mit dem Erhalt der Briefwahlunterlagen beim *Wähler* [1.S03], welcher daraufhin ausgefüllt werden. Das Ausfüllen der Briefwahlunterlagen wurde als aufgeklappter Unterprozess modelliert, da sich die Aktivitäten zusammenfassen lassen. Der *Wähler* füllt den

Wahlschein [1.A10] und den Stimmzettel aus. Den Stimmzettel hat er nach den Vorgaben der KWO §49.1 zu markieren [1.A07], um eine gültige Stimmabgabe zu tätigen. Den markierten Stimmzettel faltet der *Wähler* und legt diesen in den blauen Stimmzettelumschlag [1.A08], den er im nächsten Schritt verschließt [1.A09]. Wahlschein und blauer Stimmzettel werden danach in den orangen Wahlbriefumschlag gelegt [1.A11]. Anschließend wird dieser ebenfalls verschlossen [1.A12]. Das Ausfüllen der Briefwahlunterlagen ist damit beendet.

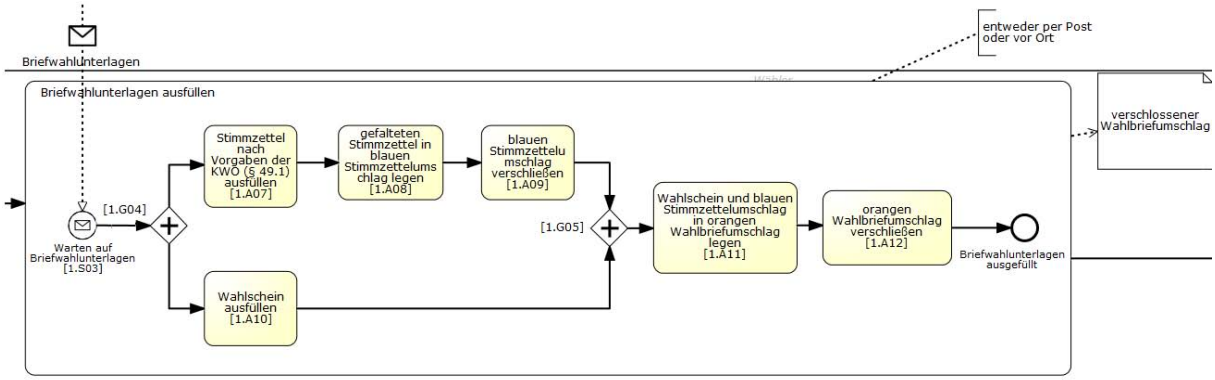

Abbildung 31: Briefwahlunterlagen ausfüllen

Der *Wähler* muss nun entscheiden, ob er den Wahlbriefumschlag vor Ort abgeben wird [1.G06]. Entscheidet er sich für die Abgabe vor Ort, so muss der *Wähler* den Wahlbriefumschlag bis spätestens um 18 Uhr am Wahltag bei der zentralen Wahlurne in der *Verwaltung* eingeworfen haben [1.A13]. Wirft er den Wahlbriefumschlag stattdessen in den Briefkasten [1.A14], so hat er dies bis um 15 Uhr am Wahltag zu erledigen. Der Wahlbriefumschlag wird nun auf dem Postweg die Verwaltung erreichen. Im BPMN-Diagramm wird die Übermittlung als Kommunikationsfluss zwischen den Pools dargestellt. Trifft der Wahlbriefumschlag in der Verwaltung ein [1.Z05], so wird er dort von mindestens zwei Mitarbeitern der *Verwaltung* entgegengenommen [1.A15]. Durch ein Vier-Augen-Prinzip als Sicherheitsmaßnahme soll sichergestellt werden, dass diese in die Wahlurne eingeworfen werden. Das Szenario der Briefwahl ist damit abgeschlossen (siehe Abbildung 32).

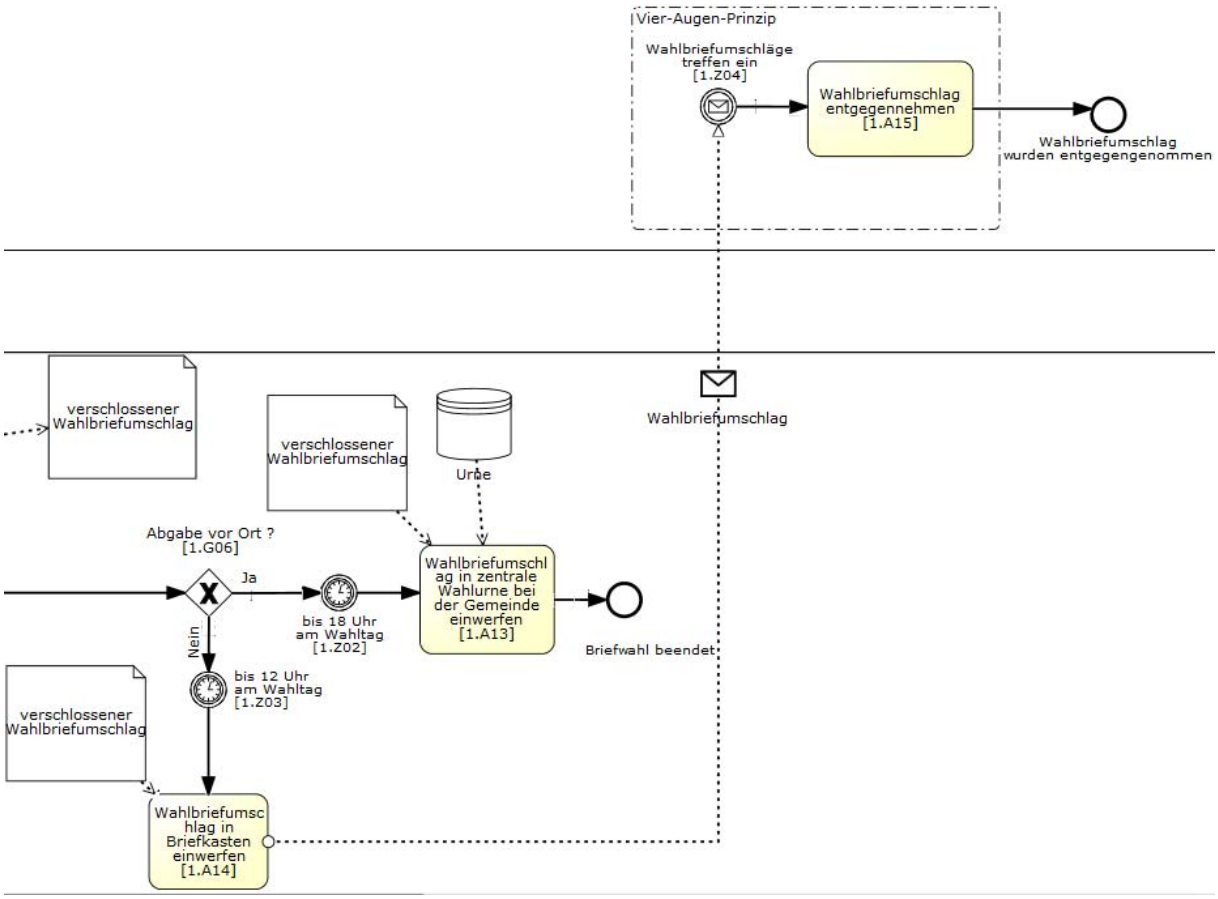

Abbildung 32: Wahlbriefumschlag einwerfen

Entscheidet sich der *Wähler*, wie in Abbildung 33 zu sehen, für die Abgabe seiner Stimme vor Ort, so kann er am Wahltag zwischen 8 und 18 Uhr das Wahllokal aufsuchen [1.A16]. Die Adresse des Wahllokals, in dem der *Wähler* seine Stimme abgeben kann, ist auf der Wahlbenachrichtigung angegeben. Der *Wähler* kann neben der Stimmabgabe auch die Wahl beobachten. Daher wird unterschieden, ob der *Wähler* die Wahl beobachtet, oder nicht [1.G07]. Entscheidet sich der *Wähler* für die Wahlbeobachtung, so kann er dies entweder vor oder nach der Stimmabgabe machen [1.G08]. Je nach Entscheidung des *Wählers* beobachtet er die Wahl vor [1.A18] oder nach der Stimmabgabe [1.A17]. Da der *Wähler* auch nach der Beobachtung erst seine Stimme abgeben kann, muss ein inklusives Gateway verwendet werden.

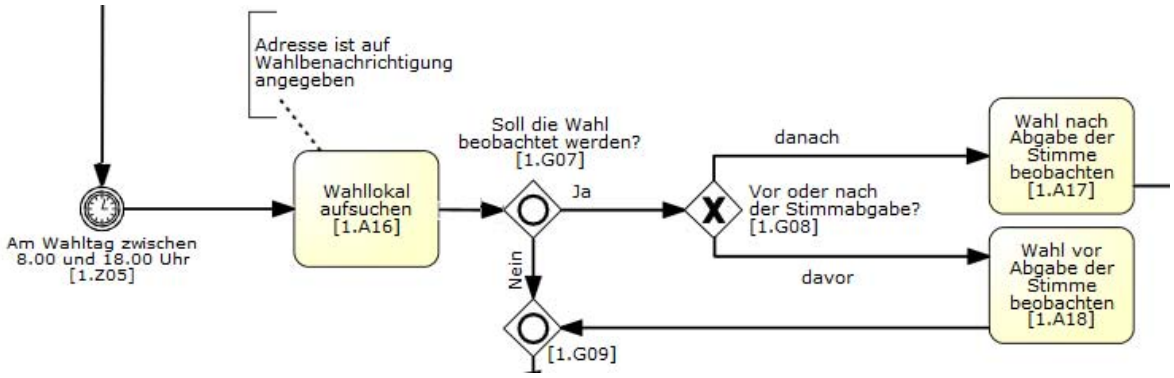

Abbildung 33: Wahl beobachten

Möchte der *Wähler* seine Stimme abgeben, so muss er dem *Wahlvorstand* seine Wahlbenachrichtigung vorlegen [1.A19]. Ein Mitglied des *Wahlvorstandes* überprüft, ob die auf dem Wahlschein genannte Person als Wahlberechtigter im Wählerverzeichnis aufgelistet ist [1.A20]. Dabei wird dieser durch ein weiteres Wahlvorstandmitglied kontrolliert. Das Vier-Augen-Prinzip wird als Sicherheitsmaßnahme verwendet, damit Manipulationen am Wählerverzeichnis, wie das Hinzufügen von Nicht-Wahlberechtigten, verhindert werden. Sollte der *Wahlberechtigte* keine Wahlbenachrichtigung bekommen haben, wird anhand des Personalausweises geprüft, ob dieser zur Wahl berechtigt ist. Ist die Person nicht im Wählerverzeichnis eingetragen, so wird diese über die Nichtzulassung der Wahl benachrichtigt [1.A21]. Die Rückmeldung über die Nichtzulassung zur Stimmabgabe wird im BPMN-Diagramm als Kommunikationsfluss dargestellt. Eine Stimmabgabe ist somit für die Person nicht möglich [1.A22]. Ist der *Wähler* zur Wahl berechtigt, so bekommt er von einem Mitglied des *Wahlvorstandes* einen Stimmzettel ausgehändigt. Die Prüfung der Wahlbenachrichtigung ist damit beendet (siehe Abbildung 34).

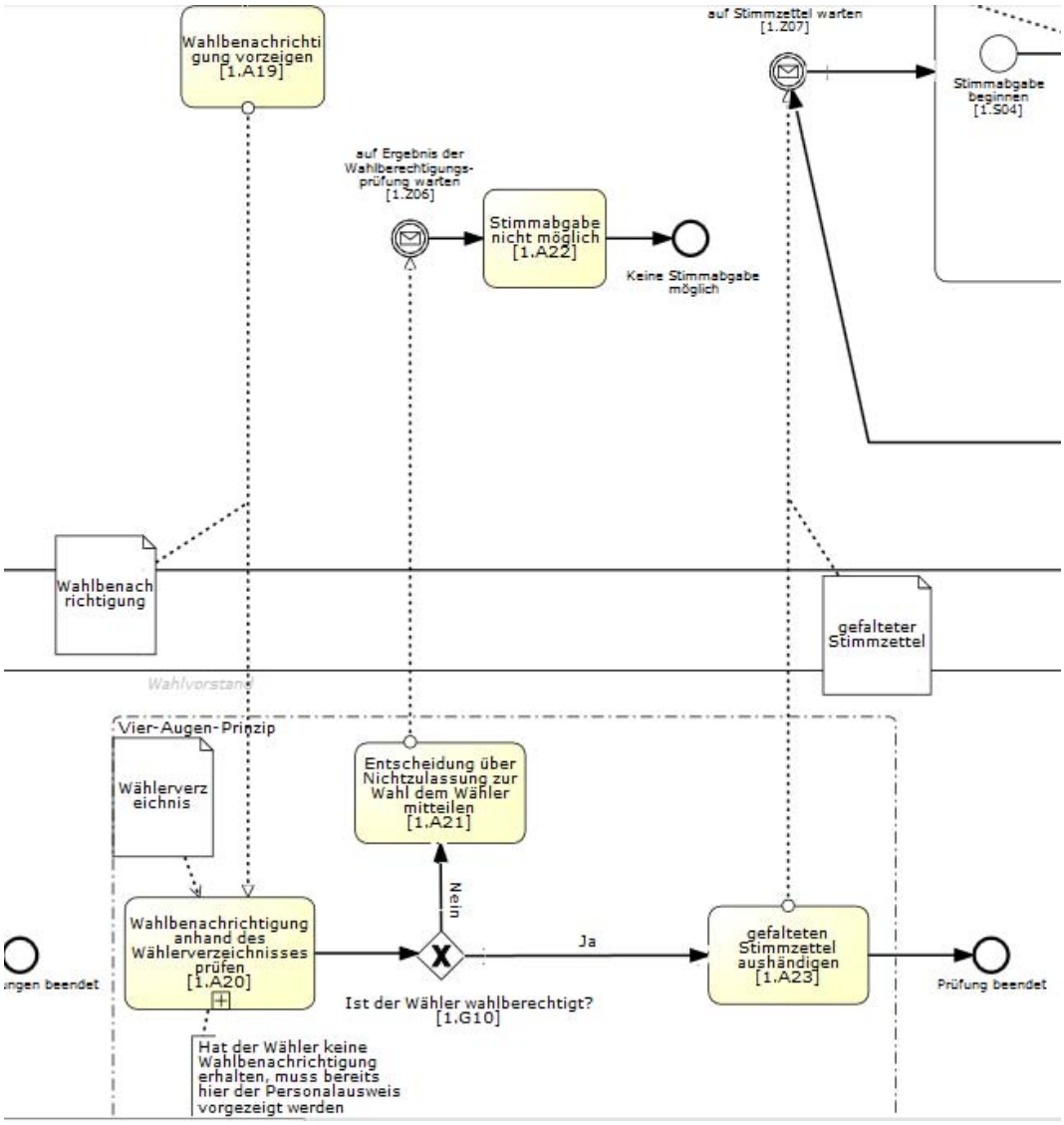

Abbildung 34: Wahlberechtigung prüfen

Abbildung 35 beginnt mit der Entgegennahme des Stimmzettels durch den *Wähler* [1.Z07]. Der *Wähler* kann daraufhin mit der Stimmabgabe beginnen, die wie schon bei der Briefwahl als aufgeklappter Unterprozess modelliert ist. Sollten *Wahlberechtigte* gemäß KWO §47 eine Hilfsperson benötigen, so können sie diese frei wählen [1.A24], darunter zählen auch Mitglieder des Wahlvorstandes. In einem nächsten Schritt sucht der *Wähler* eine leere Wahlkabine auf [1.A25], in der er den Stimmzettel nach den Vorgaben der KWO §46 ausfüllt [1.A26]. Hat der *Wähler* seine Stimme abgegeben, so sollte er in der Wahlkabine prüfen, ob der

Stimmzettel seine Wahl wiedergibt [1.A27]. Ist dies der Fall, kann der Stimmzettel gefaltet werden [1.A28]. Die Stimmabgabe ist damit beendet und der *Wähler* kann die Wahlkabine verlassen [1.A29]. Sollte der Stimmzettel seine Entscheidung nicht wiedergeben, so kann er sich beim *Wahlvorstand* melden [1.A30]. Der *Wähler* vernichtet daraufhin im Beisein eines Mitgliedes des *Wahlvorstandes* seinen markierten Stimmzettel. In diesem Fall beginnt die Stimmabgabe von Neuen, indem der *Wähler* einen neuen Stimmzettel erhält. Eine Begrenzung der Korrekturen gibt es nicht.

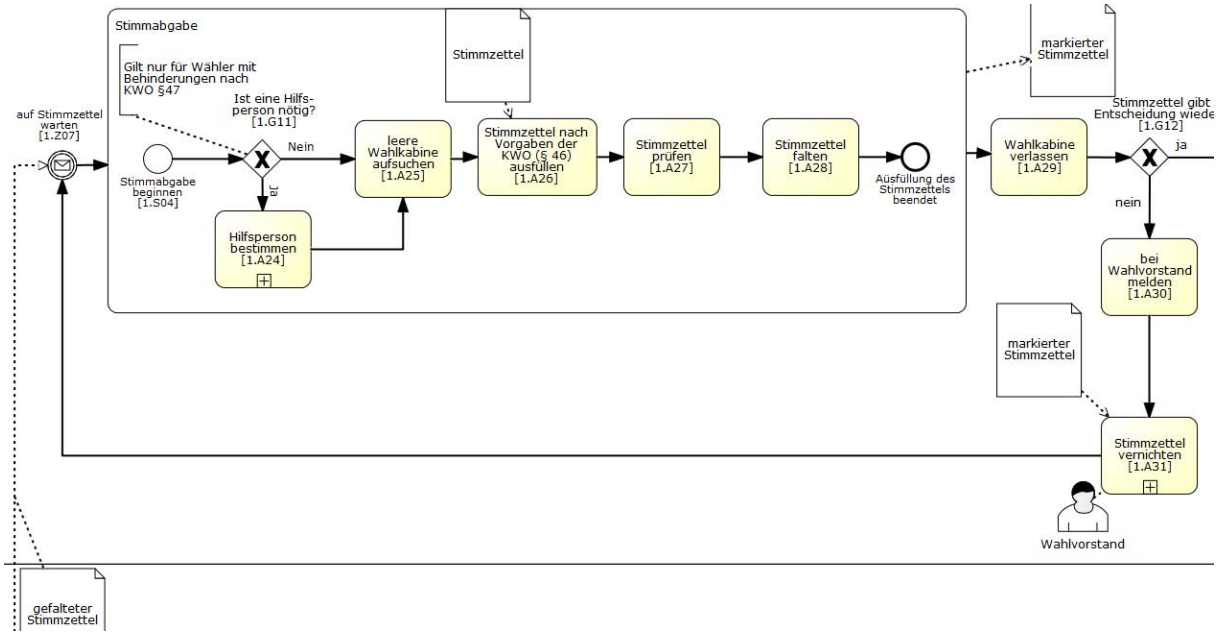

Abbildung 35: Stimmabgabe Präsenzwahl

Gibt der Stimmzettel die Entscheidung des *Wählers* wieder, so sind dem *Wahlvorstand* Personalausweis und Wahlbenachrichtigung vorzulegen. Nachfolgend gilt bei den Aktivitäten des *Wahlvorstandes* das Vier-Augen-Prinzip, um mögliche Manipulationen zu verhindern. Die Identität des *Wählers* wird vom *Wahlvorstand* überprüft [1.A33]. Stimmt die Identität des *Wählers* nicht mit der im Wahllokal anwesenden Person überein, so ist er nicht wahlberechtigt und wird über die Nichtzulassung seiner Stimmabgabe informiert [1.A34]. Der von ihm markierte Stimmzettel wird vernichtet [1.A35] und der Wahlvorgang ist für ihn beendet. Ist der *Wähler* zur Wahl berechtigt, d.h. die Authentifizierung war erfolgreich, muss er die Wahlbenachrichtigung beim *Wahlvorstand* abgeben [1.A36]. Der Stimmzettel wird von außen geprüft, sodass eine Abgabe von zwei Stimmzetteln nicht möglich ist [1.A37]. Parallel ausgeführt wird die Aktivität Öffnen des Wahlurnenschlitzes [1.A38] beziehungsweise Schließen dessen [1.A40] sowie die Eintragung des Stimmabgabevermerks bei der identifizierten Person im Wählerverzeichnis durch den *Schriftführer* [1.A41]. Dadurch ist keine er-

neute Stimmabgabe möglich. Sobald der Wahlurnenschlitz geöffnet ist, kann der *Wähler* seinen Stimmzettel in die Wahlurne werfen [1.A39]. Der Wahlvorgang ist damit beendet (siehe Abbildung 36).

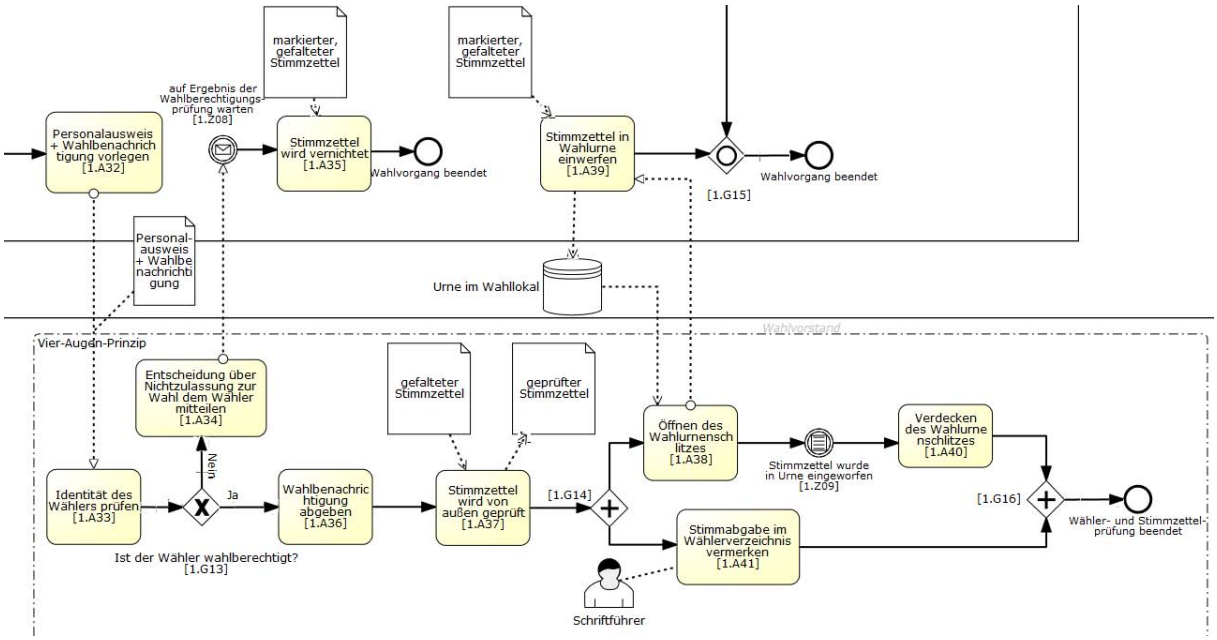

Abbildung 36: Prüfung der Identität vor der Stimmabgabe in die Wahlurne

Haben die letzten Wähler um 18 Uhr ihre Stimmen abgegeben, wird mit den Vorbereitungen für den Urnentransport zur Rhein-Mosel-Halle begonnen, wie in Abbildung 37 zu sehen ist. Aufgrund der Zusammengehörigkeit wurden die Aktivitäten als aufgeklappter Unterprozess modelliert. Für die Stimmauszählung müssen mindestens fünf Mitglieder des *Wahlvorstandes* anwesend sein. Ist dies gewährleistet, wird die Wahlurne zunächst geöffnet [1.A42]. Daraufhin werden die Stimmzettel entnommen [1.A43]. Die abgegebenen Stimmzettel werden gezählt und mit der Anzahl der Stimmabgabenvermerke verglichen [1.A44]. Ist dies geschehen, werden die Stimmzettel in Umschläge verpackt und versiegelt und in die Urne zurückgelegt [1.A45]. Die Pakete werden in die Wahlurne gelegt und vom *Wahlvorsteher* wieder verschlossen [1.A46]. Die Vorbereitungen für den Urnentransport sind abgeschlossen, sodass diese von den Sicherheitsleuten übernommen werden kann.

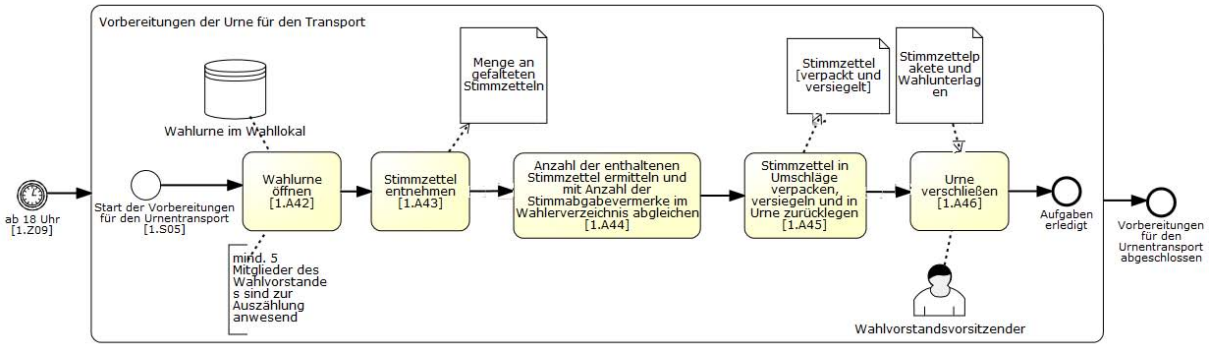

Abbildung 37: Vorbereitungen für den Urnentransport

6.2.3. BPMN-Prozessmodell: Stimmauszählung

Um die Stimmauszählung in BPMN möglichst genau modellieren zu können, wurden zunächst die notwendigen Parteien für diesen Vorgang identifiziert. Dies sind der *Briefwahlvorstand* (*Wahlvorsteher* und *Schriftführer*), die *Verwaltung*, die *Wahlorganisation* (*Wahlvorstand* und *Wahlvorsteher*) sowie der *Sicherheitsdienst*.

Im Anschluss wurden diesen Parteien Pools und Lanes zugeteilt. Zunächst wurden die *Verwaltung* und der *Sicherheitsdienst* in eigenen Pools angelegt, da es sich hier um verschiedene Benutzer handelt. Der *Briefwahlvorstand* wurde in die beiden Lanes *Wahlvorsteher* und *Schriftführer* unterteilt. Der Pool Wahlorganisation besteht aus den beiden Lanes *Wahlvorsteher* und *Wahlvorstand*. Sobald diese Zuordnung fertig gestellt war wurde die Anfangsaktivität modelliert. Diese beginnt beim Mitglied des *Wahlvorstandes der Briefwahl* indem die orangenen Umschläge geöffnet [2.A01] und anschließend in einer neuen Aktivität die Wahlscheine entnommen werden [2.A02]. Nach Abschluss dieser beiden Aktivitäten wurde ein erstes datenbasiertes, exklusives Gateway modelliert [2.G01].

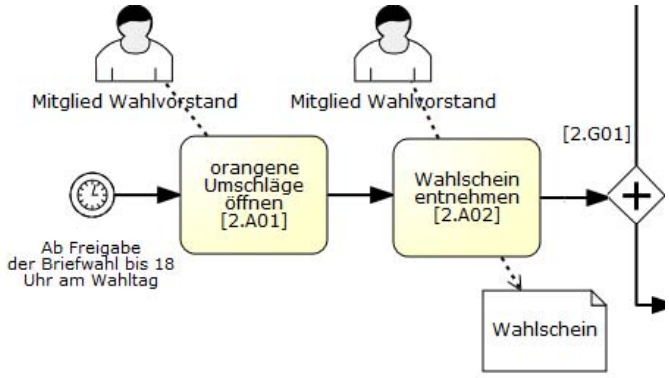

Abbildung 38: Entpacken der Wahlbriefunterlagen

Hier wird zunächst der Wahlschein an den *Schriftführer* übergeben [2.A03], welcher anschließend die Namen der *Wähler* im Wählerverzeichnis überprüft [2.A04]. Diese Aktivität führt zu dem zweiten datenbasierten, exklusiven Gateway [2.G02]. Hier besteht zum einen die Möglichkeit, dass der Name des *Wählers* im Wählerverzeichnis vermerkt ist. Alternativ ist der Name des *Wählers* hingegen nicht im Wählerverzeichnis gelistet. Ist die der Fall, so muss zum einen ein Vermerk [2.A05] über diese Tatsache gemacht werden. Außerdem müssen alle Wahlscheine gesammelt werden [2.A06], bei denen der Name des *Wählers* nicht im Wählerverzeichnis aufgeführt war.

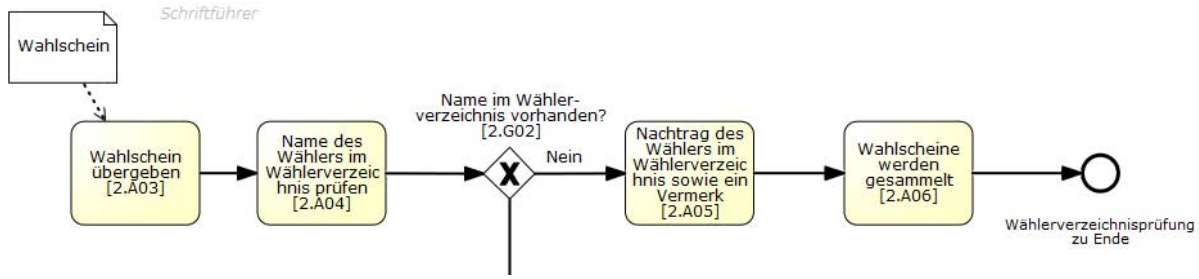

Abbildung 39: Überprüfung des Wählerverzeichnisses

Dem *Wahlvorsteher* der Briefwahl werden ab 18 Uhr die Stimmzettelumschläge übergeben [2.A07]. Wird der Name des *Wählers* im Wählerverzeichnis geführt [2.G02], so wird darauffolgend der Stimmzettel dem Umschlag entnommen [2.A08]. Anschließend findet in der Nachfolgeaktivität eine Stimmzettelüberprüfung nach KWO §39.1 statt [2.A09]. Hier wird ein weiteres datenbasiertes, exklusives Gateway benötigt [2.G03], da die Möglichkeit besteht

das der Stimmzettel ungültig ist. Ist dies der Fall, so wird dieser nach KWO §56.3 erfasst [2.A10]. Ist der Stimmzettel jedoch gültig, so wird dieser ungesehen in die Wahlurne eingeworfen.

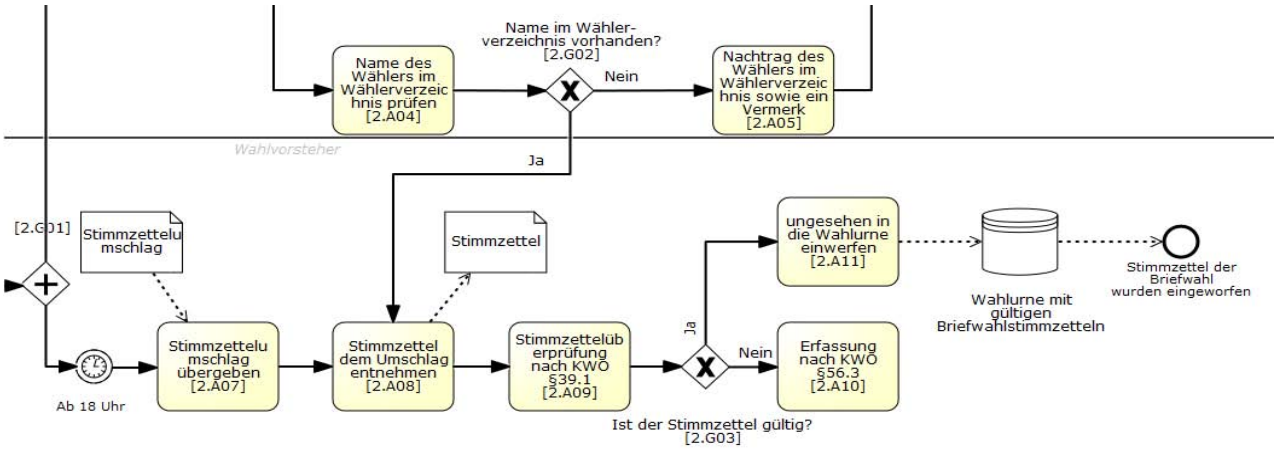

Abbildung 40: Überprüfung der Stimmzettel

Sobald die Urnen, nach der Stimmabgabe, zur Übernahme bereit sind, werden diese durch die *Verwaltung* übernommen [2.A12]. Das Übernahmeprotokoll wird von den Mitarbeitern der *Verwaltung* unterzeichnet [2.A13] und im Anschluss werden die Urnen zur Rhein-Mosel-Halle transportiert [2.A14]. Danach ordnen die *Verwaltungsmitarbeiter* die Urnen dem jeweiligen Stimmbezirk zu [2.A15]. Hierbei werden die Urnen an den korrekten Tischen, die für die jeweiligen Auszähler der Stimmbezirke aufgestellt wurden, platziert.

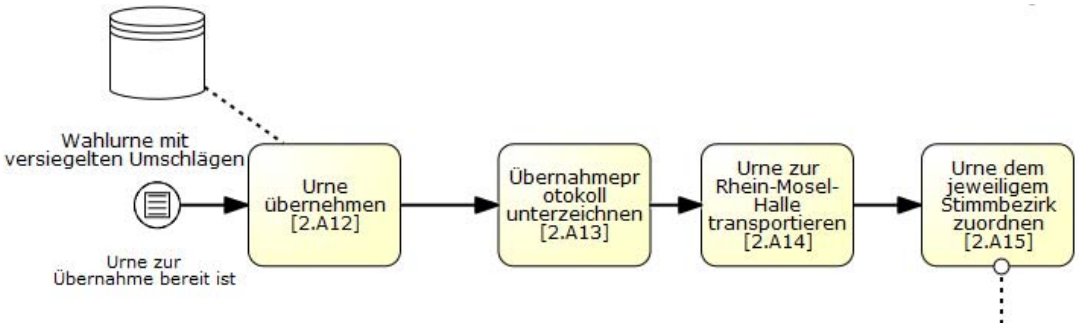

Abbildung 41: Übernahme und Transport der Wahlurnen

Die nächste Aktivität wird vom *Sicherheitsdienst* übernommen da diesem die Aufgabe zufällt, die Urnen zu überwachen [2.A16], bis diese am darauffolgenden Morgen um sieben Uhr wieder von der *Verwaltung* übernommen werden.

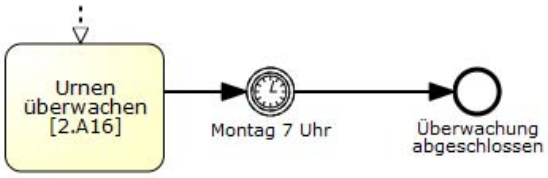

Abbildung 42: Überwachung der Wahlurnen

Die Mitarbeiter der Verwaltung übernehmen die organisatorische Vorbereitung der Wahl [2.A17], damit um neun Uhr die Urnen vom *Wahlvorstand* geöffnet und die Umschläge auf den jeweiligen Tischen ausgeschüttet werden können [2.A18]. Daraufhin hält der *Wahlvorstand* außerdem die Übergabe der USB-Sticks in einem Übergabeprotokoll fest [2.A19]. Anschließend werden die USB-Sticks in ihren Umschlägen an die *Wahlvorsteher* der Stimmbezirke weitergegeben, woraufhin der *Wahlvorstand* die benötigten Computerprogramme zur Wahlauszählung startet [2.A20]. Es folgt die Aktivität Prüfziffer eingeben [2.A21], bei welcher der *Wahlvorstand* die ersten beiden Prüfziffern für das Programm und dem Bezirk eingeben muss, um das Programm korrekt starten zu können.

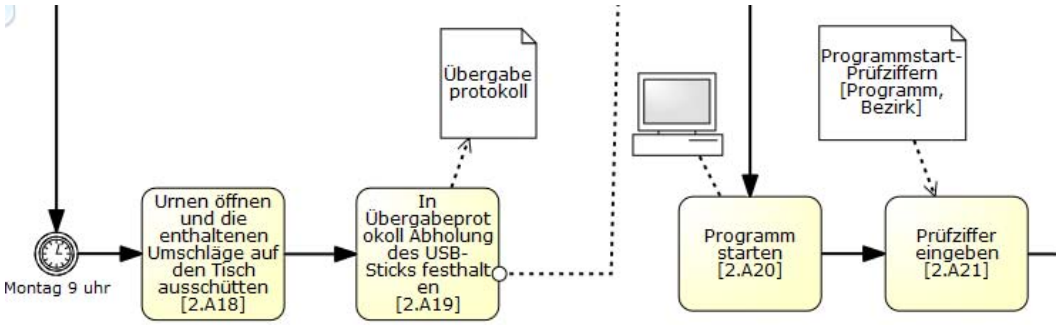

Abbildung 43: Start des Wahlprogrammes

Da hier entweder das Programm starten kann oder nicht, wurden die beiden Möglichkeiten durch ein weiteres Gateway [2.G04] modelliert, wie in der Abbildung oben zu sehen ist. Für den Fall, dass die Programmversion veraltet ist und das Programm somit nicht startet [2.A22], ist eine Fortführung der Stimmauszählung nicht mehr möglich. Handelt es sich jedoch um die aktuelle Programmversion, startet das Programm wie vorgesehen [2.A23] und die Stimmauszählung startet mit einem Test, der zeigen soll, ob das Programm die eigegebenen Daten kor-

rekt erfasst. Hierfür werden fünf beliebige Teststimmzettel gezogen und im Programm erfasst [2.A24]. Im Anschluss erfolgen ein Ausdruck der erfassten Teststimmzettel und eine Kontrolle darüber, ob die Daten vom Programm korrekt erfasst wurden [2.A25]. Nachfolgend befindet sich an dieser Stelle ebenfalls ein Gateway [2.G05], da die Teststimmzettel entweder korrekt erfasst wurden oder signifikante Fehler bei der Datenerfassung auftraten. Für den Fall, dass eine fehlerhafte Erfassung der Daten vorliegt, müssen erneut fünf Teststimmzettel erfasst werden, um zu überprüfen, ob das Programm richtig arbeitet. Aus diesem Grund ist in Abbildung sieben ein Pfeil vom Gateway zurück zur Aktivität [2.A24] zu sehen. Sofern keine schwerwiegenden Fehler bei der Testerfassung aufgetreten sind, wird die Auszählung fortgeführt, indem die Stimmzettel in den Stapel zurückgelegt werden [2.A26]. Nachfolgend findet die Auszählung der verbliebenen Stimmzettel statt, da hier die Stimmzettel ab dem sechsten weitererfasst werden [2.A27].

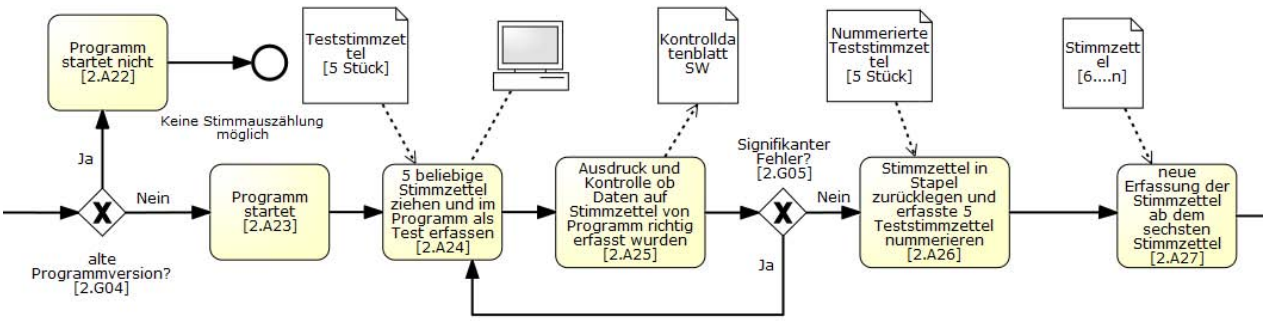

Abbildung 44: Erfassung der Teststimmzettel

Bei diesem Prozess wurden die einzelnen Schritte modelliert, indem zunächst der Stimmzettel aus dem Stapel entnommen [2.A28], der Stimmzettel entfaltet wird [2.A29] und die vergebenen Stimmen nacheinander vorgelesen sowie nummeriert werden [2.A30]. Danach werden die Stimmen erfasst [2.A31]. Anschließend wird, wie in Abbildung 8 zu erkennen ist, die Nummerierung der Stimmzettel im System vermerkt [2.A32]. Nachfolgend wurde ein weiteres datenbasiertes, exklusives Gateway modelliert [2.G06], da zum einen die Möglichkeit besteht, dass die Stimmzettel von den Wählern so ausgefüllt wurden, dass sie als ungültig anzusehen sind. Ist dies der Fall, so werden diese Stimmzettel nach § 37 aussortiert und im Protokoll vermerkt [2.A33]. Zum anderen können die Stimmzettel aber auch korrekt ausgefüllt sein, was bedeutet, dass diese als gültige Stimmen in die Auszählung miteinbezogen werden. In

diesem Fall werden die Stimmzettel auf den gültigen Stapel gelegt [2.A34]. Der ganze Prozess ist mit der Erfassung des letzten Stimmzettels im PC abgeschlossen [2.A35].

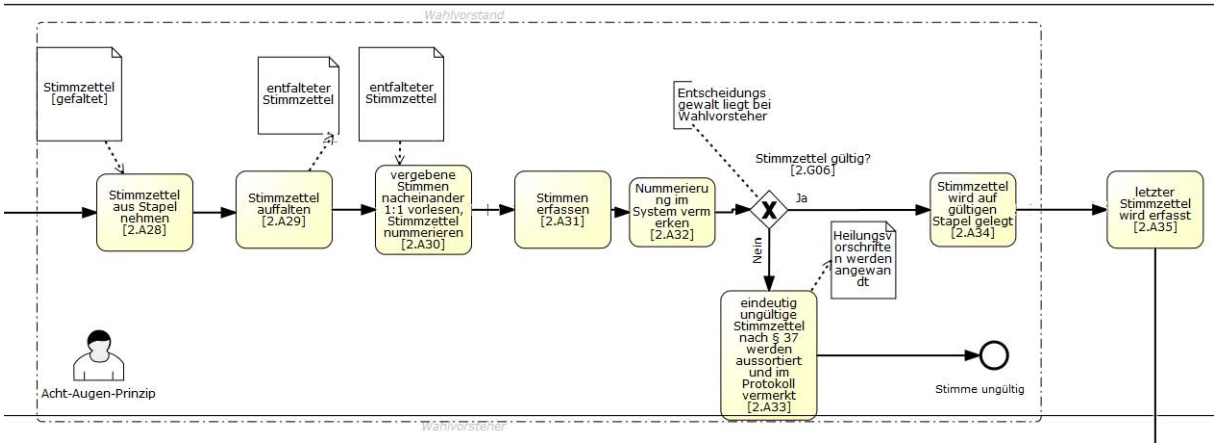

Abbildung 45: Erfassung der Stimmzettel

Nach Abschluss der Stimmzettelerfassung gibt der *Wahlvorsteher* den Schlüssel für den spezifischen Stimmbezirk bei Programmstart ein [2.A36], erfasst elektronisch alle gültigen Stimmen die auf den Papierstimmzettel abgegeben wurden, speichert diese auf dem USB-Stick und schließt den jeweiligen Stimmbezirk im Programm ab [2.A37]. Anschließend erzeugt dieser eine neue Schlüsselnummer sowie Notation auf dem Beiblatt [2.A38] und übergibt den USB-Stick mit dem Beiblatt an den *Wahlvorstand* [2.A39].

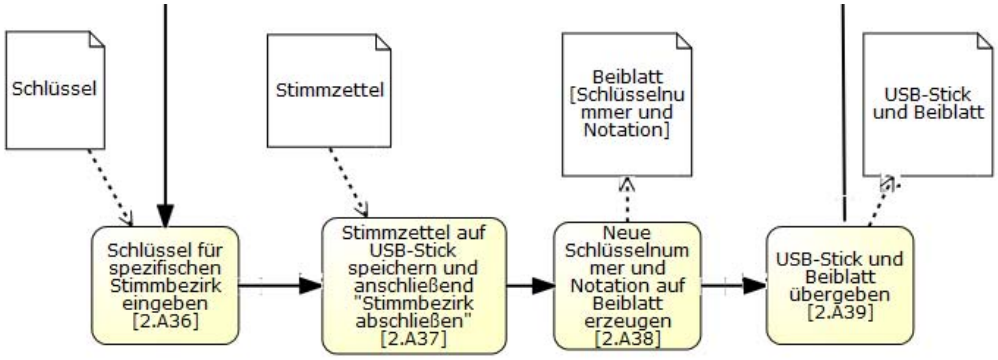

Abbildung 46: Abschluss der Stimmbezirke

Daraufhin erhält der *Wahlvorstand* den USB-Stick mit der dazugehörigen Verschlüsslungsnummer und die Ergebnisse der jeweiligen Stimmbezirke werden im zentralen Erfassungs-PC

festgehalten. Danach wird von der Software (SW) die Prüfziffer[28] ermittelt, welche vom *Wahlvorstand* in das Protokoll eingetragen wird [2.A40]. Anschließend wird das Ergebnis pro Stimmbezirk ausgedruckt [2.A41] und darauffolgend der jeweilige USB-Stick entnommen [2.A43]. Um die Korrektheit der Ergebnisse zu gewährleisten, überprüft der *Statistiker* als zusätzlicher Beteiligter die Ergebnisse in den jeweiligen Stimmbezirken auf eklatante Abweichungen in Relation zu den Ergebnissen der vorherigen Wahl [2.A44].

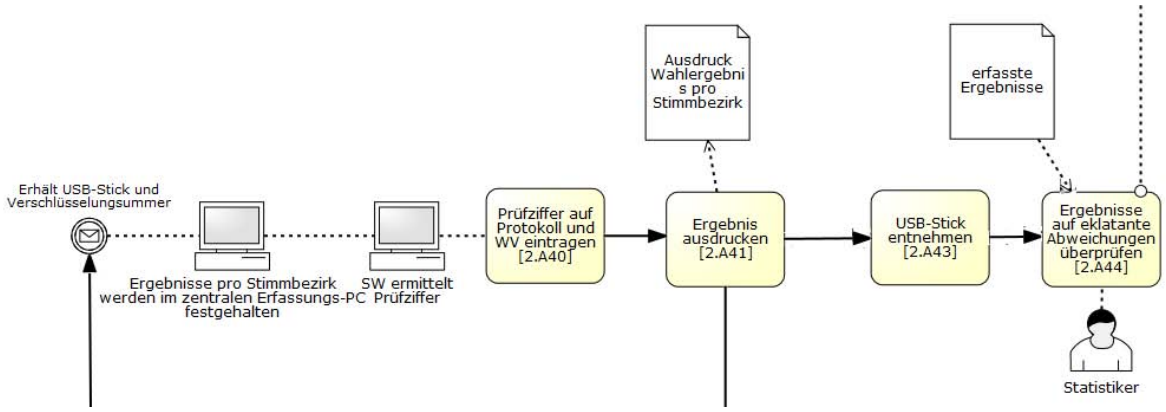

Abbildung 47: Übermittlung und Überprüfung der Wahlergebnisse

Um den Prozess der Stimmauszählung abzuschließen, erstellt die *Verwaltung* eine Bescheinigung über das Einlesen der Wahlergebnisse [2.A45], welche an den *Wahlvorsteher* weitergeleitet und von diesem ausgefüllt, unterschrieben und verpackt wird [2.A46].

[28] Anmerkung der Betreuer: Die dritte Prüfziffer stellt die Integrität der erfassten Stimmen sicher. Wird nach Abschluss des Wahlbezirks erzeugt und auf dem Beiblatt notiert, das abschließend von allen Mitgliedern des Wahlvorstands unterzeichnet wird. Die zentrale Erfassung erfolgt durch andere Mitarbeiter der Verwaltung – diese erhalten den USB-Stick sowie die begleitenden Dokumente – darunter auch die dritte Prüfziffer

Prozess 1: Kommunalwahlen 2014 in Koblenz

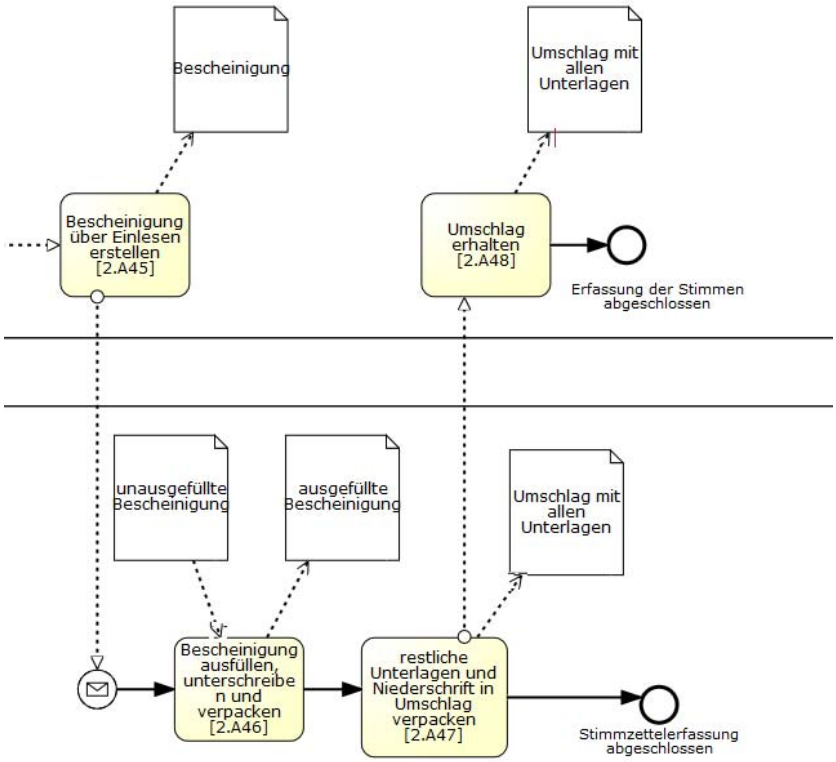

Abbildung 48: Abschluss der Stimmauszählung

Zusätzlich verpackt der *Wahlvorsteher* die restlichen Unterlagen sowie die Wahlniederschrift in einen Umschlag [2.A47] und leitet diesen an die *Verwaltung* weiter [2.A48]. Diese ist nun im Besitz des Umschlags mit allen Wahlunterlagen und mit diesem Schritt kann die Stimmauszählung final als abgeschlossen betrachtet werden.

6.2.4. BPMN-Prozessmodell: Wahlnachbereitung

Die Phase der Wahlnachbereitung beginnt unverzüglich, nachdem die Auszählungen abgeschlossen wurden.

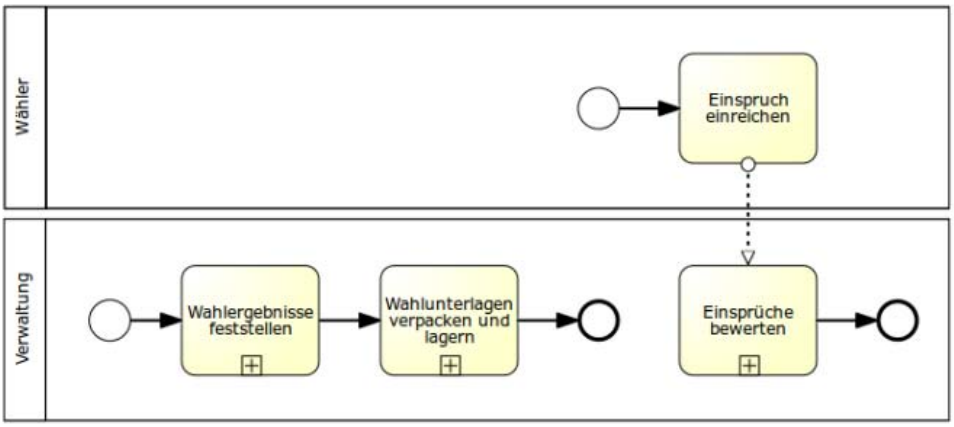

Abbildung 49: Vereinfachte Darstellung der Wahlnachbereitung

Wie Abbildung 49 zeigt, kann die Wahlnachbereitung vereinfacht in vier Schritte unterteilt werden: Wahlergebnisse feststellen, Wahlunterlagen verpacken und lagern, Einspruch einreichen und Einspruch bewerten.

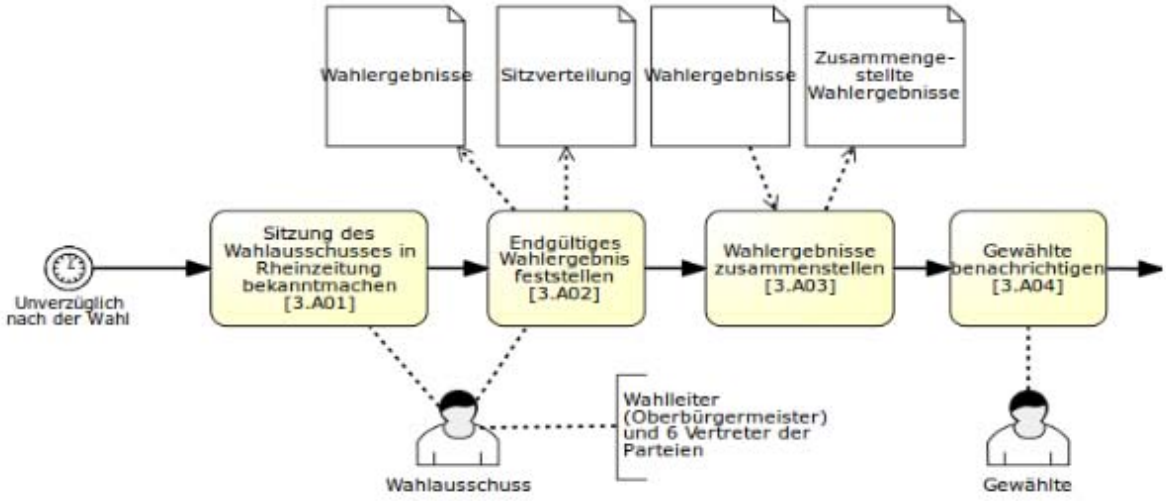

Abbildung 50: Wahlergebnisse feststellen

Wie das Startereignis in Abbildung 50 zeigt, beginnt diese Wahlphase, sobald die Auszählungen abgeschlossen sind und die Wahl damit abgeschlossen ist. Bei der ersten Aktivität *[3.A01]* geben die *Verwaltung* und der *Wahlausschuss* die Sitzung in der Rheinzeitung bekannt, wann die endgültigen Wahlergebnisse festgestellt und öffentlich verkündet werden. Das passiert in der nachfolgenden Aktivität *[3.A02]*. Aus dieser Aktivität gehen die Wahlergebnisse und die Sitzverteilung für die nächste Amtsperiode hervor.

Die Wahlergebnisse gehen in Aktivität *[3.A03]* als Input mit ein. In dieser Aktivität werden die Wahlergebnisse der einzelnen Wahlbezirke zu einem zusammengestellten Wahlergebnis zusammengefasst. Anschließend werden die *Gewählten* (hier: Stadträte) in Aktivität *[3.A04]* benachrichtigt.

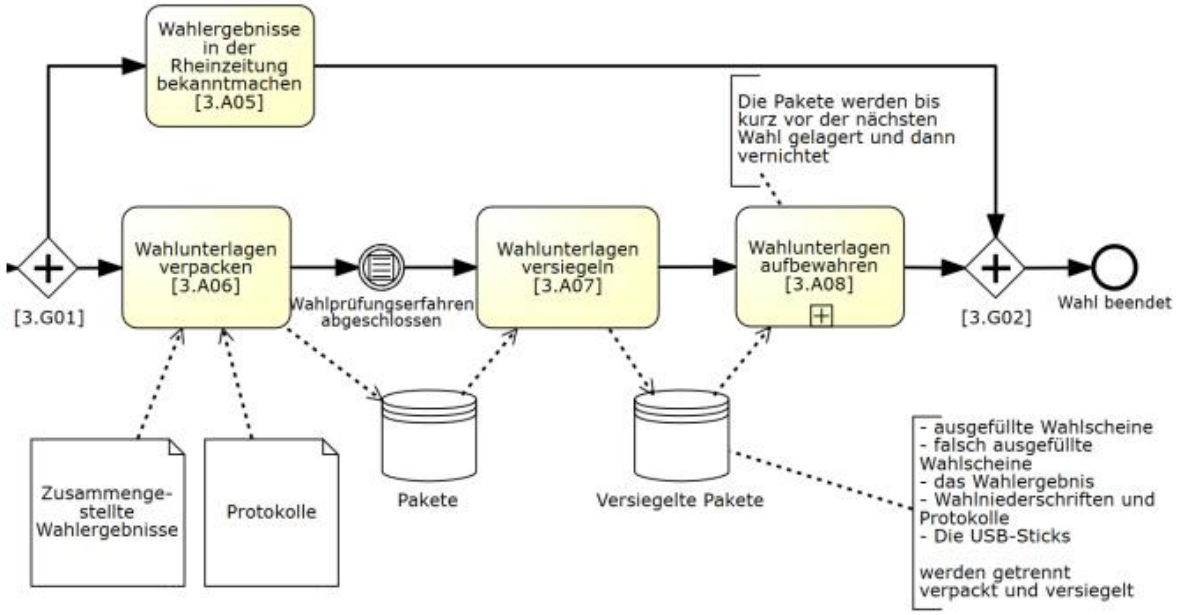

Abbildung 51: Wahlunterlagen verpacken und lagern

Der Pfeil am rechten Rand aus Abbildung 50 führt in das auf Abbildung 51links zu sehende parallele Gateway *[3.G01]*. Der obere ausgehende Pfad des Gateways zeigt die Aktivität *[3.A05]*, bei der die *Verwaltung* die Wahlergebnisse in der Rheinzeitung bekannt macht. Wenn dieser Schritt abgeschlossen ist, führt das folgende parallele Gateway *[3.G02]* in das Endereignis „Wahl beendet“ über.

Der untere Pfad des Gateways führt in die Aktivität *[3.A06*]. In diese Aktivität gehen die zusammengestellte Wahlergebnisse und Protokolle mit ein. Dabei werden die genannten Dokumente verpackt und zu Paketen zusammengeführt. Es folgt das bedingte Zwischenereignis Wahlprüfungsverfahren abgeschlossen, bei dem das Wahlergebnis geprüft und validiert wird. Die Pakete werden erst dann von der *Verwaltung* versiegelt (siehe Aktivität *[3.A07]*), wenn die Prüfverfahren abgeschlossen sind. Der zugeklappte Unterprozess *[3.A08]* beschreibt das Aufbewahren der Pakete. Diese werden bis kurz vor der nächsten Wahl gelagert und dann vernichtet (siehe Kommentar). Ist dieser Prozess abgeschlossen, führt das Gateway *[3.G02]* den Aktivitätsfluss wieder in oben genanntes Endereignis.

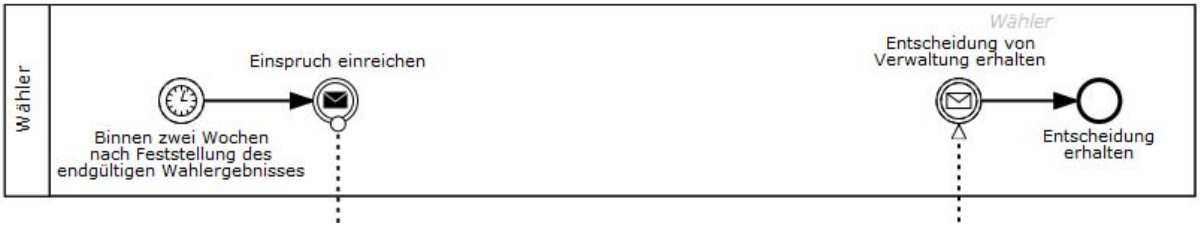

Abbildung 52: Einspruch einreichen

Nachdem die Ergebnisse festgestellt und verkündet worden sind, siehe Abbildung 52, haben die *Wähler* das Recht einen Einspruch gegen das Wahlergebnis einzulegen (siehe KWG §48). Dies wird durch das Zeit-Startereignis modelliert. Danach folgt ein Nachrichten-Zwischenereignis (throw), wodurch der Einspruch in die *Verwaltungs*-Lane übergeben wird. Der Aktivitätsfluss kehrt nach der Bewertung in die Lane des *Wählers* zurück, indem er die Entscheidung der *Verwaltung* als Nachricht erhält. Dies wird durch ein Nachrichten-Zwischenereignis (catch) modelliert, welches am Ende in das Endereignis Entscheidung erhalten führt.

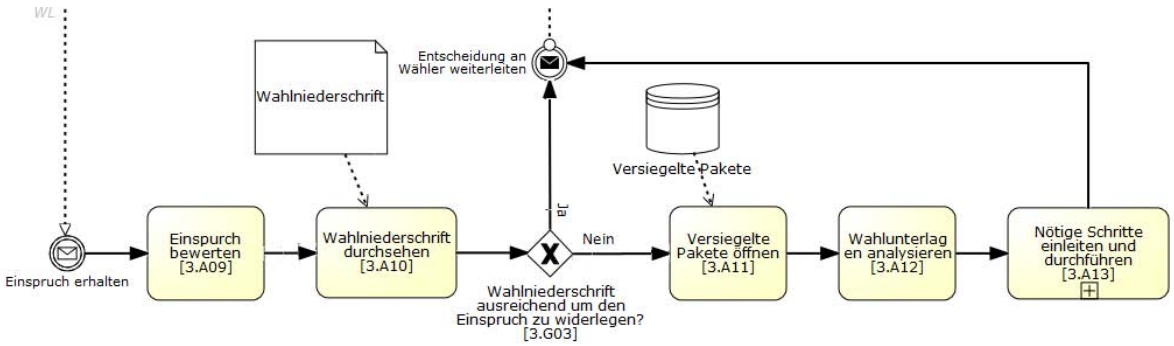

Abbildung 53: Einspruch bewerten

Hat ein *Wähler* einen Einspruch eingelegt, erhält die *Verwaltung* diesen und beginnt die Bewertung, welche auf Abbildung 53 zu sehen ist. Sie beginnt mit der Aktivität *[3.A09]*. Danach wird in *[3.A10]* die Wahlniederschrift durchgesehen, um im anschließenden Gateway *[3.G03]* zu entscheiden, ob die darin enthaltenen Informationen ausreichend sind, um den Einspruch zu widerlegen. Ist dies der Fall, sendet die *Verwaltung* die Entscheidung zum *Wähler*, was durch das Nachrichten-Zwischenereignis (throw) gekennzeichnet ist. Reichen die Niederschriften nicht aus, werden die Pakete wie in Aktivität *[3.A11]* zu sehen geöffnet und anschließend analysiert *[3.A12]*. Der zugeklappte Unterprozess *[3.A13]* fasst das weitere Vorgehen zusammen und führt ebenfalls zu dem oben genannten Nachrichten-Zwischenereignis, sodass der *Wähler* eine Rückmeldung erhält.

6.3. Interessenkonflikte und resultierende Sicherheitsanforderungen

Das Vorgehen zur Erfassung der Interessenkonflikte wurde anfangs anhand der beteiligten Rollen dargestellt. Hierbei wurde untersucht, wie die beteiligte Rolle allein oder in Kooperation mit anderen Rollen einen Prozess kompromittieren kann[29]. Dieses Verfahren war allerdings nicht strukturiert und orientierte sich nicht an den zuvor erstellten BPMN-Diagrammen. Es war mehr ein erster Ansatz, bei dem anhand des gewonnenen Wissens mögliche Interessenkonflikte identifiziert wurden. Damit die Interessenkonflikte strukturiert und möglichst vollständig erfasst werden können, wurde jede einzelne Aktivität der BPMN-Diagramme nach möglichen Interessenkonflikten untersucht.
Um die Interessenkonflikte einheitlich zu erfassen, wurde auch an dieser Stelle eine Schablone entwickelt. Diese sieht vor, dass zunächst die zu untersuchende Aktivität beschrieben wird, bevor aufgezeigt wird, welche Rollen beziehungsweise IT-Systeme daran beteiligt sind. Input und Output dieser Aktivität werden genannt. Dabei handelt es sich um Informationen, Daten oder sonstige Artefakte. Nachfolgend werden der Normalfall sowie die böswillige Absicht der Beteiligten aufgezeigt. Dabei wird erläutert, welche Sicherheitsanforderung durch die böswillige Absicht verletzt wird und welche Sicherheitsmaßnahmen bereits existieren (IST-Zustand) und durch welche möglichen Sicherheitsmaßnahmen (SOLL-Zustand) erst gar kein Angriff möglich wäre. Abschließend folgt eine Bewertung der Auftrittswahrscheinlichkeit. Dabei wird zwischen den drei Levels - geringe, mittlere und hohe Wahrscheinlichkeit - unterschieden. In den BPMN-Diagrammen wird diese Bewertung durch eine Ampel-Markierung deutlich. Dabei steht eine grüne Markierung der Aktivität für eine geringe, Gelb für eine mittlere und Rot für eine hohe Wahrscheinlichkeit.

Nachfolgend werden alle identifizierten Interessenkonflikte in den einzelnen Wahlphasen anhand dieser Schablone erläutert. Die Identifizierung der Interessenkonflikte basiert dabei auf Einschätzungen. Hierfür wurde auf Hintergrundwissen zurückgegriffen.

[29] Anm. der Betreuer: Interessenkonflikte beziehen sich auf das Ziel eines Prozesses bzw. einer dem Ziel untergeordneten Aktivität. Beispielsweise hat eine Aktivität die Auszählung der Stimmen zum Ziel. Interessenkonflikte können nun darin bestehen, dass eine beteiligte Person die Auszählung manipulieren möchte. Sollte ihr dies gelingen, ist auch der gesamte Prozess – die Durchführung der Wahl – hinsichtlich seiner Zielerreichung gefährdet.

Da für die Konsistenzprüfung im nächsten Kapitel die geltenden Sicherheitsanforderungen der untersuchten Aktivität eine wichtige Rolle spielen, werden diese am Ende noch einmal zusammengefasst.

6.3.1. Wahlvorbereitung

Wählerverzeichnis aufstellen [0.A14]

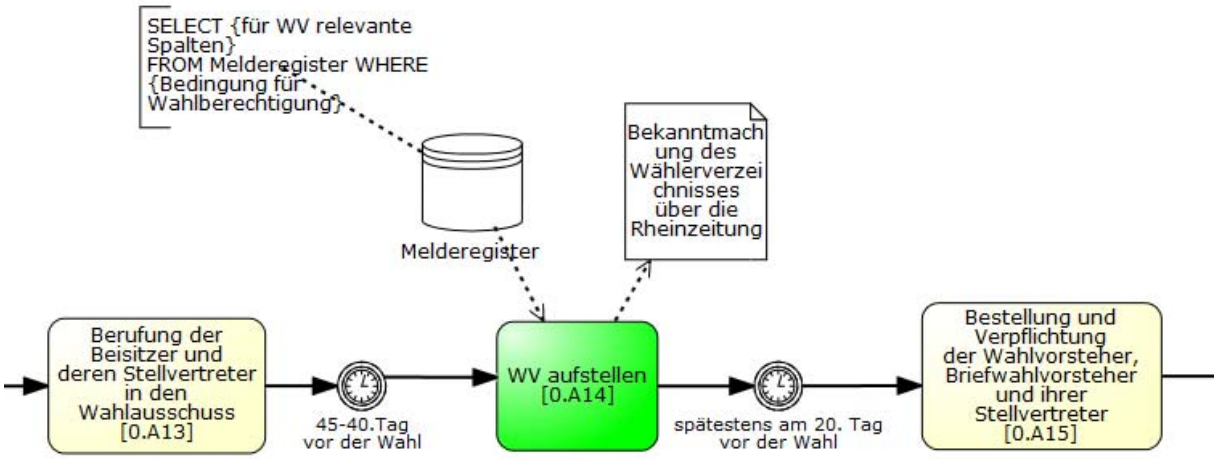

Abbildung 54: Wählerverzeichnis aufstellen

Die Daten jedes *Wählers* müssen im Wählerverzeichnis richtig eingegeben werden. Neben der Feststellung der Wähler ist hier außerdem festzustellen, in welchen Bezirk die Wahlberechtigung vorliegen wird. Doppelte, bzw. fehlende Eintragungen sind zu vermeiden. Um die Richtigkeit des Wählerverzeichnisses zu gewährleisten, prüft die *Verwaltung*, ob alle Daten korrekt sind. Dies geschieht bevor öffentlich bekannt gemacht wird, dass den Bürgern in einem begründeten Fall Einsicht in das Verzeichnis gewährleistet wird. Die beteiligten Personen sind die *Wähler* und die *Verwaltung*. Im Melderegister werden die Daten der *Wähler*, wie z.B. Name, Wohnort und Alter, gespeichert und die *Verwaltung* verwertet die Daten und erstellt daraus als Output ein Wählerverzeichnis. Im Normalfall wird das Wählerverzeichnis korrekt angegeben. Falls Fehler vorhanden sind, hat der *Wähler* die Möglichkeit diese bei einer terminlich vereinbarten Einsicht in das Wählerverzeichnis korrigieren zu lassen. Jedoch werden Fehler ohne Einsichtnahme nicht ersichtlich. Bei der böswilligen Absicht möchte ein *Verantwortlicher des Wählverzeichnisses* nicht, dass eine bestimmte Person die Möglichkeit hat, an der Wahl teilzunehmen und lässt diesen absichtlich nicht in das Verzeichnis eintragen. Dadurch wird die Integrität[30] des Wählerverzeichnisses verletzt, da die Daten nicht mehr unversehrt sind und manipuliert wurden. Als Sicherheitsmaßnahme hat der *Bürger* nun die Mög-

[30] Anm. der Betreuer: Die Integrität des Wählerverzeichnisses ist erst dann verletzt, wenn enthaltene Datensätze nach dessen Erstellung hinzugefügt, modifiziert oder gelöscht würden. Das hier Beschriebene lässt sich sinnvoller als „Korrektheit des Prozesses“ ausdrücken. Diese Anforderung gilt für den kompletten Prozess, weswegen sie nicht mehr weiter betrachtet wird.

lichkeit, seine eigenen Angaben im Wählerverzeichnis zu kontrollieren, und wenn notwendig Einspruch einzulegen. Jedoch kann die *Verwaltung* diesen Einspruch weiterhin ignorieren[31], da nur in einem begründeten Fall der *Wähler* Einsicht in das Verzeichnis hat. Allerdings entscheidet weiterhin die *Verwaltung*, ob die Begründung des *Wählers* ausreichend für die Kontrolle des Wählerverzeichnisses ist. Generell wird als IST-Zustand ein Vier-Augen-Prinzip bei der Erstellung des Wählerverzeichnisses durchgesetzt. Zusätzlich kann der *Wähler* das Wählerverzeichnis einsehen, um seine eigenen Daten zu überprüfen. Sollten allerdings beide Mitarbeiter der *Verwaltung* korrupt sein, so ist weiterhin eine Manipulation am Wählerverzeichnis[32] möglich. Zudem überprüft kaum ein *Wähler*, ob dieser korrekt im Wählerverzeichnis erfasst wird. Zusätzliche Sicherheitsmaßnahmen im SOLL-Zustand könnten deshalb sein, dass das Wählerverzeichnis abschließend durch zwei unabhängige Mitarbeiter überprüft wird. Insgesamt ist es zwar möglich, dass das Wählerverzeichnis auf mehreren Ebenen kontrolliert wird, jedoch ist die Möglichkeit der Manipulation nur sehr gering und der Aufwand eines Mehr-Augen-Prinzips entspricht nicht dem Aufwand der Manipulationsmöglichkeit. Aus diesem Grund wurde die Gefahr und die daraus resultierenden Folgen der Manipulation für die Wahl als sehr gering eingestuft.

Für die Aktivität [0.A14] konnte eine Sicherheitsanforderungen[33] identifiziert werden: Vertraulichkeit der personenbezogenen Daten im Wählerverzeichnis.

[31] Anm. der Betreuer: Die Anforderung, einen Einspruch nicht zu ignorieren, gehört zur Sicherheitsanforderung „Verfügbarkeit des Dienstes“.
[32] Anm. der Betreuer: Dieses betrifft die Sicherheitsanforderung „Integrität des Wählerverzeichnisses“.
[33] Anm. der Betreuer: Aus unseren anderen Anmerkungen geht hervor, dass aus der oben dargestellten Analyse sich zwei weitere Sicherheitsanforderungen zusätzlich zu der genannten ableiten lassen: Verfügbarkeit des Dienstes, Integrität des Wählerverzeichnisses

Abschließende Annahme des Wahlvorschlages überprüfen [0.A10]

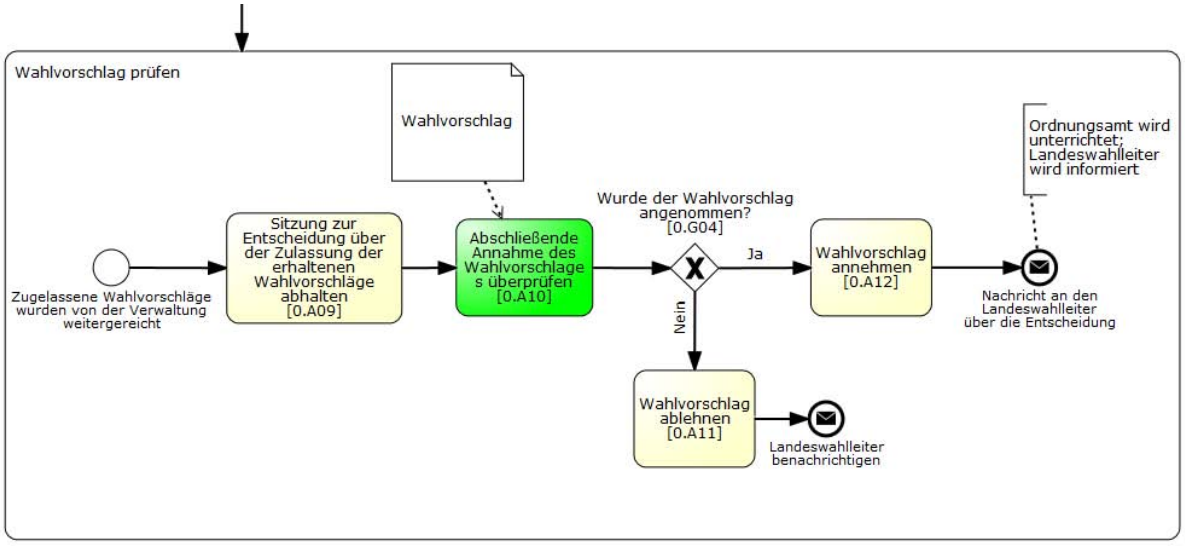

Abbildung 55: Überprüfung des Wahlvorschlages

Die *Parteien* reichen Wahlvorschläge bei der *Verwaltung* ein. Diese kontrolliert, ob genügend Unterstützungsunterschriften vorhanden sind und ob die Wahlvorschläge rechtskonform sind. Zusätzlich wird geprüft, ob die *Parteien* keine rechtswidrigen Aktivitäten vertreten. Die eigentliche Annahme des Wahlvorschlages erfolgt jedoch beim *Wahlausschuss*. Die angenommenen Wahlvorschläge der *Verwaltung* werden dem *Wahlausschuss* zur abschließenden Überprüfung übergeben. Nach erfolgreicher Kontrolle des Wahlvorschlages über die Annahme bzw. Ablehnung, wird der Wahlvorschlag abschließend auf den Stimmzettel gesetzt. Die beteiligten Personen an dieser Aktivität sind die *Parteien*, die als Input den Wahlvorschlag einreichen und der *Wahlausschuss*, der als Output den kontrollierten Wahlvorschlag freigibt oder ablehnt. Als Sicherheitsmaßnahme gilt im IST-Zustand ein Mehr-Augen-Prinzip. Speziell zur Annahme oder Ablehnung des Wahlvorschlages wird eine Sitzung des gesamten *Wahlausschusses* abgehalten, was einem Mehr-Augen-Prinzip entspricht. Im Normalfall werden verfassungswidrige *Parteien* nicht zugelassen. Ist der *Wahlausschuss* jedoch böswillig, so kann er *Parteien nicht zulassen*, die jedoch alle Voraussetzungen zur Wahlteilnahme erfüllen. Dies geschieht z. B. durch gemeinsame Absprache oder durch Bestechung des Wahlausschusses. Dadurch wird die Sicherheitsanforderung Authentizität[34] verletzt, da sowohl Wahlvor-

[34] Anm. der Betreuer: Die Sicherheitsanforderung „Authentizität“ ist hier unpassend, da die angegebenen Daten (hier: Wahlvorschläge) von der angegebenen – d.h. korrekten – Quelle erstellt wurden. Der hier beschriebene Angriff wirkt sich jedoch im weiteren Verlaufe des Prozesses auf die Verfügbarkeit der Wahl für die Wahlvor-

schläge nicht vollständig vorhanden sind und nicht korrekt gedruckt werden. Im IST-Zustand gibt es keine weitere Instanz, die die Aktivitäten des *Wahlausschusses* überprüft und so eine gemeinsame Absprache verhindern könnten. Um dies zu verhindern, sollten die betroffenen *Parteien* mit einer guten Begründung Einspruch einlegen können und der *Landeswahlleiter* überprüft, ob der Entscheid des *Wahlausschusses* rechtens ist. Mit Hilfe eines Vetorechtes kann der *Landeswahlleiter* die Entscheidung des *Wahlausschusses* so widerlegen. Der SOLL-Zustand ist letztendlich ein verbessertes Mehr-Augen-Prinzip mit mehr kontrollierenden Parteien. Insgesamt ist dieser Aufwand denkbar, um Möglichkeiten der Absprachen gegen eine bestimmte *Partei* zu unterbinden. Die Gefahr der Manipulation jedoch wird hierbei als sehr gering eingestuft, da es für die Wahl zwar große Folgen haben könnte, aber der Aufwand nicht die Maßnahme gerechtfertigt. Die bereits eingeführten Maßnahmen sind dementsprechend ausreichend.

Für die Aktivität [0.A10] konnte eine Sicherheitsanforderung identifiziert werden: Integrität der Wahlvorschläge.

Stimmzettel drucken [0.A17]

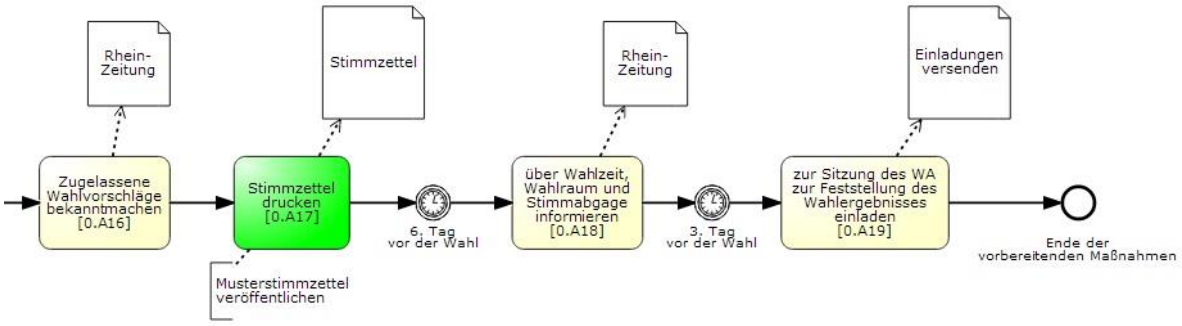

Abbildung 56: Drucken des Stimmzettels

Der Stimmzettel wird unter spezifischen Vorgaben, wie die Qualität und Farbe des Papiers, sowie Format, Schriftgröße und Schriftart von der *Auftragsdruckerei* gedruckt. Vorerst wird

schlagsträger aus. Besser wäre die Sicherheitsanforderung als Integrität (= Vollständigkeit und Unversehrtheit) der vorhandenen Daten zu bezeichnen.

ein Muster vorgedruckt, welches von der *Verwaltung* und dem *Wahlleiter* kontrolliert wird und anschließend für den gesamten Druckablauf freigegeben wird. Die beteiligten Personen in diesem Prozess sind zum einen der *Wahlleiter*, der als Input Daten über den Stimmzettel, wie Farbe, Papier, Schrift, sowie Inhalt an die *Druckerei* weitergibt, zum anderen die *Druckerei* selbst, die die Vorgaben des *Wahlleiters* umsetzt und als Output die Stimmzettel ausgibt. Im Normalfall wird der Stimmzettel nach Mustervorgaben gedruckt und alle *Parteien* und ihre Mitglieder finden sich in richtiger Schreibweise auf den Stimmzetteln. Bei böswilliger Absicht gibt der *Wahlleiter* absichtlich einen Stimmzettel mit falschen *Parteienmitgliedern* als Druckvorlage ab, ein bewusstes Falschschreiben der Namen auf dem Stimmzettel, bzw. lässt ganze Parteien nicht auf dem Stimmzettel erscheinen. Auch hier wird die Sicherheitsanforderung der Integrität verletzt. Der Stimmzettel entspricht nicht den beschlossenen Angaben, da die Daten verändert wurden. Der Stimmzettel wird im Voraus vom *Wahlausschuss* festgelegt. Dadurch besteht die Möglichkeit, dass dem *Wahlausschuss* der fehlerhafte Druck auffällt. Jedoch besteht keine zusätzliche Aktivität zur Kontrolle des Stimmzettels. Durch Vorlage des fertiggedruckten Stimmzettels an den *Wahlausschuss* kann noch einmal die Richtigkeit des Stimmzettels kontrolliert werden. Zwar besteht der IST-Zustand schon aus einem Vier-Augen-Prinzip, aber durch die Verbesserungsmöglichkeiten der Kontrollinstanz, sollte im SOLL-Zustand ein Mehr-Augen-Prinzip verwendet werden. Insgesamt ist dieser Aufwand denkbar, um die Möglichkeiten der Absprachen gegen eine bestimmte *Partei* oder einer bestimmte *Person* zu unterbinden. Jedoch ist auch hier die Wahrscheinlichkeit der Manipulation sehr gering, da eine größere Manipulation von der *Druckerei* selbst und anderen mitwirkenden *Parteien* durch die Veröffentlichung des Musterstimmzettels auffallen würde.

Für die Aktivität [0.A17] konnten zwei Sicherheitsanforderungen identifiziert werden: Integrität und Verfügbarkeit des Stimmzettels[35].

[35] Anm. der Betreuer: Im vorangehenden Text wurde diese Sicherheitsanforderung nicht begründet. Ein Unterschlagen des Muster-Stimmzettels würde dazu führen, dass der Druckvorgang nicht starten könnte. Dieser Angriff würde daher zu einer zeitlichen Verzögerung des Prozesses führen.

6.3.2. Stimmabgabe

Briefwahlunterlagen beantragen

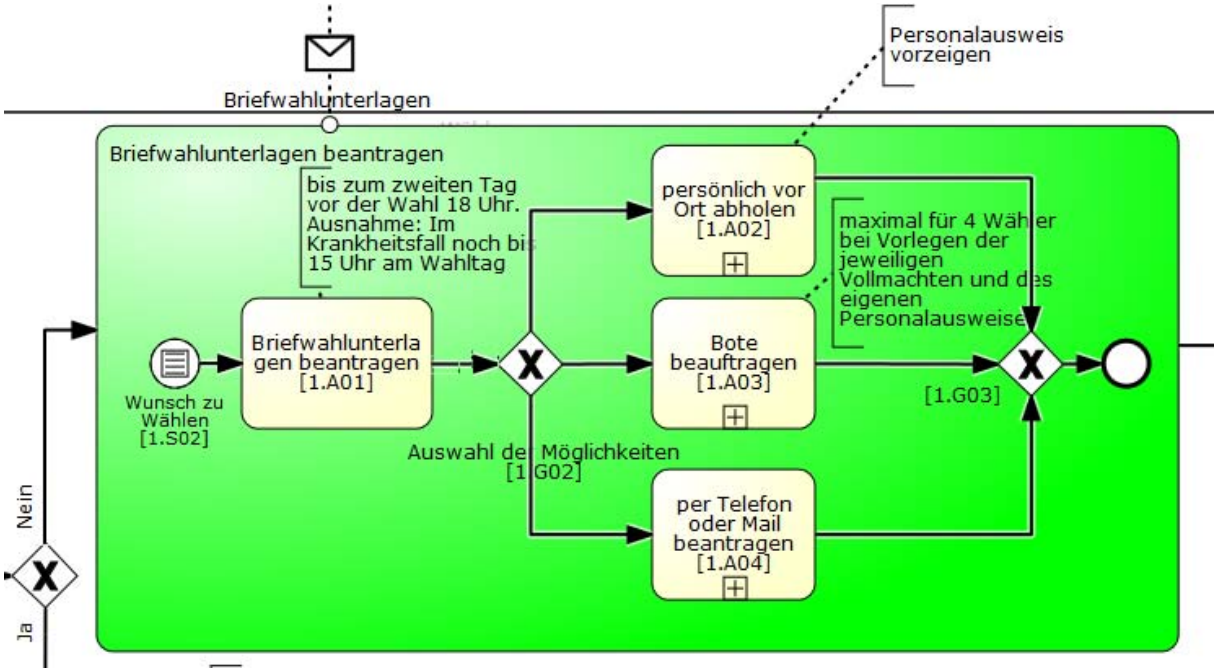

Abbildung 57: Briefwahlunterlagen beantragen

Der *Wähler* sieht entweder die Wahlbekanntmachung in der Rhein-Zeitung oder bekommt seine Wahlbenachrichtigung zugesendet. Da er am Wahltag verhindert ist beziehungsweise schon vorab wählen möchte, beantragt der *Wähler* per Post bei der Verwaltung Briefwahlunterlagen für sich selbst. Dafür füllt er entweder das dem Wahlschein hinzugefügt Formular aus oder meldet sich schriftlich bzw. telefonisch bei der *Verwaltung*. Eine andere Möglichkeit ist die Briefwahlunterlagen vor Ort bei der *Verwaltung* abzuholen. Dafür muss der *Wähler* sich mit Personalausweis und Wahlschein ausweisen. Zudem kann der *Wähler* bei Vorweisen einer Vollmacht für vier weitere Personen Briefwahlunterlagen mitnehmen. An der Aktivität sind der *Wähler* und die *Verwaltung* beteiligt, IT-Systeme werden keine verwendet. Der Input für die betrachtete Aktivität ist entweder die Wahlbekanntmachung in der Rhein-Zeitung oder die erhaltene Wahlbenachrichtigung. Der Output besteht in der Beantragung der Briefwahlunterlagen. Im Normalfall füllt der Wähler den Wahlscheinantrag gemäß §18 der Kommunalwahlordnung aus. Verfolgt der *Wähler* ein böswilliges Interesse, so beantragt er durch Fälschung der Vollmacht die Briefwahlunterlagen für andere Mitmenschen. Der IST-Zustand der Sicherheitsmaßnahmen sieht eine Beschränkung der Vollmachten auf eine Anzahl von maximal vier vor. Da die Vollmachten keiner besonderen Kontrolle unterzogen werden, fällt das

Fälschen von Vollmachten im kleinen Kreis nicht auf. Da der Anteil der Vollmachtstellenden und somit der mögliche Einfluss auf das Wahlergebnis sehr gering sind, wird diese Sicherheitslücke seitens der *Verwaltung* geduldet. Schließlich kann der Betrüger lediglich vier Stimmabgaben fälschen. Würden sich mehrere Betrüger zusammenschließen, würde die Manipulation recht schnell seitens der Verwaltung aufgrund von Beschwerden der Wähler entdeckt. Aufgrund der Eingrenzung auf vier Vollmachten und somit zu vernachlässigenden Nutzen wird die Wahrscheinlichkeit als gering eingestuft.

Für die Aktivität [1.A02] konnten eine Sicherheitsanforderung identifiziert werden: Verfügbarkeit der Briefwahlunterlagen.

Warten auf eintreffende Briefwahlanträge [1.Z01][36]

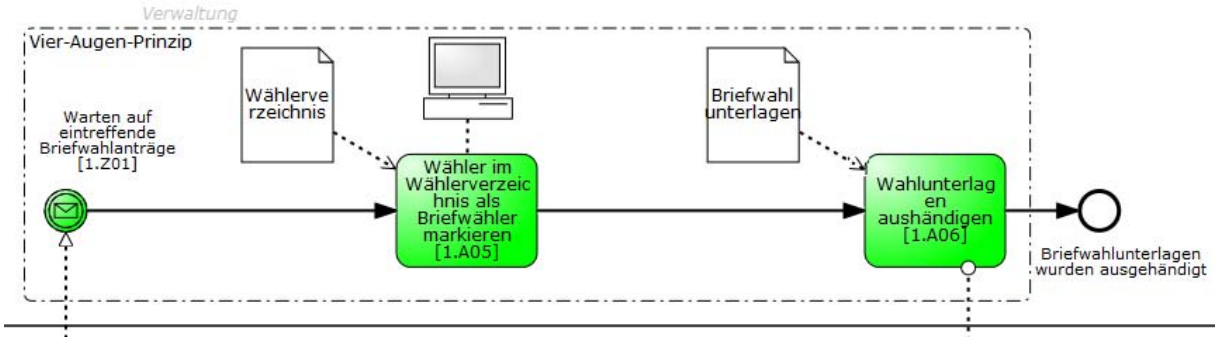

Abbildung 58: Interessenkonflikte bei der Bearbeitung der Briefwahlanträge

Die Mitarbeiter der *Verwaltung* warten auf eintreffende Briefwahlanträge der *Wähler*, um diesen ihre beantragten Briefwahlunterlagen auszuhändigen. An der Aktivität sind mindestens zwei Mitarbeiter der *Verwaltung* beteiligt, IT-Systeme werden keine verwendet. Input und Output sind die eingehenden Briefwahlanträge. Im Normalfall werden die eingehenden Briefwahlanträge von den zuständigen Mitarbeitern der *Verwaltung* bearbeitet. Verfolgen die Mitarbeiter ein böswilliges Interesse, so können die eingegangenen Briefwahlanträge bis zur Frist zum Eingang der Briefwahlanträge missachtet oder nach Erhalt weggeworfen werden. Wenn die Bearbeitung der Briefwahlanträge nur durch eine Person erfolgt, ist hier eine Manipulation leicht möglich. Allerdings stellt sich die Frage, was der Mitarbeiter damit erreichen kann. Der *Wähler* könnte nämlich bei Nicht-Eintreffen der Briefwahlunterlagen stutzig wer-

[36] Anm. der Betreuer: Das Vorgehensmodell sieht die Untersuchung von Aktivitäten und nicht – wie hier geschehen – Ereignissen vor. Ein Ereignis selbst kann keiner Sicherheitsanalyse unterzogen werden, sondern vielmehr die auslösende Aktivität. Von dem Ereignis beeinflusst wird zudem die nachfolgende Aktivität. Diese (z. B. „Bearbeiten der Briefwahlunterlagen“) fehlt in der Darstellung und hätte anstelle des Ereignisses untersucht werden können.

den und sich erneut an die *Verwaltung* wenden. In diesem Fall hätte der korrupte Mitarbeiter der *Verwaltung* keinen Mehrwert erreicht. Sollte dieser die politischen Interessen der Briefwähler kennen, so könnte er dadurch gezielt Briefwahlanträge nicht bearbeiten. Allerdings ist dieser Manipulationsaufwand im Vergleich zum erreichten Resultat sehr gering, denn der Anteil der Briefwähler ist niedrig. Das liegt daran, dass den *Wählern* bewusst ist, dass diese Form der Wahl als unsicher gilt[37]. Durch diese Art der Manipulation wird die Sicherheitsanforderung der Verfügbarkeit der Briefwahlunterlagen verletzt. Der IST-Zustand der Sicherheitsmaßnahmen sieht ein Vier-Augen-Prinzip vor. Sollten beide Mitarbeiter korrupt sein, so ist eine Manipulation weiterhin möglich. Um dies zu verhindern, werden für das Vier-Augen-Prinzip Mitarbeiter ausgewählt, die unterschiedliche politische Interessen vertreten. Die genannten Sicherheitsmaßnahmen des IST-Zustandes sind ausreichend, sodass keine weiteren Maßnahmen für den SOLL-Zustand umgesetzt werden müssen. Da diese Betrugsart wenig Nutzen bringt, wird sie als unwahrscheinlich bzw. unrealistisch eingeschätzt. Dementsprechend wird die Wahrscheinlichkeit als gering eingestuft.

Für das Zwischenereignis [1.Z01] konnte eine Sicherheitsanforderung identifiziert werden: Authentizität der eintreffenden Briefwahlanträge[38].

Wähler im Wählerverzeichnis als Briefwähler markieren [1.A05]

Beantragt der *Wähler* Briefwahlunterlagen, so wird er im Wählerverzeichnis als Briefwähler markiert. An der Aktivität sind zwei Mitarbeiter der *Verwaltung* beteiligt und PC-Wahl wird als IT-System verwendet. Der Input ist das aktuelle Wählerverzeichnis und der Output ein Vermerk im Wählerverzeichnis, dass die antragstellende Person per Briefwahl seine Stimme abgeben möchte. Im Normalfall wird der *Wähler* im Wählerverzeichnis als Briefwähler markiert. Der Briefwähler erhält damit einen sogenannten Sperrvermerk. Damit wird sichergestellt, dass der Wahlberechtigte auch nur einmal seine Stimme abgeben darf und nicht zusätzlich zur Briefwahl auch seine Stimme im Wahllokal abgibt. Sind die beiden Mitarbeiter der

[37] Anm. der Betreuer: Diese Aussage wurde nicht belegt

[38] Anm. der Betreuer: Eine weitere, hier nicht hergeleitete Sicherheitsanforderung ist die „Verfügbarkeit der Briefwahlunterlagen“. Es ist theoretisch möglich, dass eine Person versucht, unrechtmäßig an Briefwahlunterlagen zu gelangen. Die Rechtmäßigkeit der Quelle (hier: Verwaltung als ausstellende Stelle) ist hier also nicht mehr gegeben. Es kann jedoch angenommen werden, dass der Aufwand im Vergleich zum erwarteten Nutzen für diesen Angriff zu hoch ist.

Verwaltung korrupt, markieren sie den Antragstellenden nicht als Briefwähler[39]. Der Antragsteller hätte nun die Möglichkeit sowohl per Briefwahl, als auch vor Ort seine Stimme abzugeben. Aber auch ein korrupter *Wahlvorstand* kann den *Wahlberechtigten* zu Manipulationen verwenden. Durch diesen Betrug wird die Integrität der Wählerverzeichnisse verletzt, da der *Wähler* keinen Sperrvermerk erhält. Der IST-Zustand der Sicherheitsmaßnahmen versucht diesen Betrug durch das Mehr-Augen-Prinzip zu verhindern. Eine mögliche Verbesserung für den SOLL-Zustand wäre, dass die beiden Mitarbeiter der *Verwaltung* unterschiedliche politische Interessen vertreten. So könnte diese Art von Betrug verhindert werden. Diese Form der Manipulation ist nur in kleinem Maße ohne Entdeckung möglich, da die Anzahl der Stimmabgaben mit den Vermerken im Wählerverzeichnis bis auf kleine Abweichungen übereinstimmen muss. Der Nutzen des Betruges ist für den hohen Aufwand sehr gering. Dementsprechend wird das Risiko als gering eingestuft.

Für die Aktivität [1.A05] konnten drei Sicherheitsanforderungen[40] identifiziert werden: Integrität und Verfügbarkeit des Briefwahlverzeichnisses sowie Vertraulichkeit der personenbezogenen Daten[41].

Wahlunterlagen aushändigen [1.A06]

Der *Wähler* hat bei der *Verwaltung* Briefwahlunterlagen beantragt und erwartet, dass die *Verwaltung* diese ihm auch zusendet. An der Aktivität sind der *Wähler* und mindestens zwei Mitarbeiter der *Verwaltung* beteiligt, IT-Systeme werden keine verwendet. Der Input ist der Antrag von Briefwahlunterlagen und Output die an den Wähler gesendeten Briefwahlunterlagen. Im Normalfall versendet die *Verwaltung* die Briefwahlunterlagen sofort nach Eingang des Antrags an den *Wähler* (§19 KWO). Verfolgen die Mitarbeiter der *Verwaltung* böswillige Interessen oder wird das Mehr-Augen-Prinzip nicht konsequent umgesetzt, so werden die Briefwahlunterlagen nicht an den *Wähler* versendet. Somit erhält der *Wähler* keine Briefwahlunterlagen und muss diese erneut anfordern, indem er diese nun vor Ort abholen muss. Dadurch wird sichergestellt, dass der Wahlberechtigte die Briefwahlunterlagen erhält. Hier

[39] Anm. der Betreuer: Ebenso ist der umgekehrte Fall denkbar: Es wird eine Stimmabgabe im Briefwahlverzeichnis vermerkt obwohl der betreffende Wahlberechtigte keine Briefwahl beantragt hat. Somit ist die Verfügbarkeit der Wahl für diese Person nicht mehr gegeben.

[40] Anm. der Betreuer: Zusätzliche Sicherheitsanforderung: Verfügbarkeit der Wahl

[41] Anm. der Betreuer: Die Sicherheitsanforderung „Vertraulichkeit der personenbezogenen Daten“ ist nicht relevant, da die Wahlverzeichnisse im Vergleich zum Melderegister einen reduzierten Datensatz beinhalten.

stellt sich allerdings wie schon bei der Manipulation des Briefwahlantrages die Frage, welchen Nutzen die *Verwaltung* verfolgt. Denn die meisten Antragsteller werden sich nun die Briefwahlunterlagen vor Ort abholen oder sich überlegen die Stimme doch bei der Präsenzwahl abzugeben. Nur die allerwenigsten werden durch diesen Mehraufwand, die Briefwahlunterlagen vor Ort abzuholen, ihre Stimme nicht abgeben. Diese Manipulation ist nur in kleinem Ausmaß möglich, da bei einer Häufung von Wählerbeschwerden über Nicht-Erhalt der Briefwahlunterlagen der Betrug auffallen würde. Liegen bei anderen *Wählern* böswillige Interessen vor, so können durch Abfangen der Briefwahlunterlagen Personen möglicherweise an der Stimmabgabe gehindert werden. Bei diesen Möglichkeiten des Betruges wird die Verfügbarkeit der Briefwahlunterlagen verletzt. Der IST-Zustand sieht vor, dass ein Mehr-Augen-Prinzip umgesetzt wird. Wenn wir davon ausgehen, dass es konsequent umgesetzt wird, so sind keine weiteren Maßnahmen für den SOLL-Zustand zu ergreifen. Diese Art des Betruges nimmt sehr wenig Einfluss auf das Wahlergebnis, ist sehr aufwendig und durch Beschwerden leicht zu entdecken. Deshalb wird die Wahrscheinlichkeit dieser Manipulationsart als gering eingestuft.

Für die Aktivität [1.A06] konnten zwei Sicherheitsanforderungen identifiziert werden: Integrität[42] und Verfügbarkeit der Briefwahlunterlagen.

[42] Anm. der Betreuer: Die Sicherheitsanforderung der Integrität der Briefwahlunterlagen wurde im vorangehenden Text nicht hergeleitet und ist auch nicht von Bedeutung.

Prozess 1: Kommunalwahlen 2014 in Koblenz

Wahlbriefumschlag entgegennehmen [1.A15]

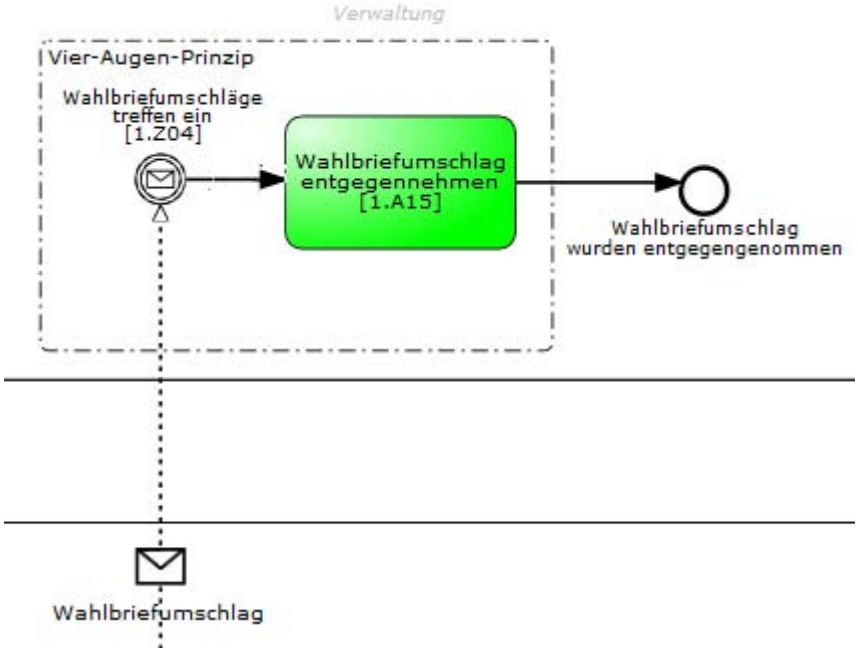

Abbildung 59: Wahlbriefumschlag entgegennehmen

Die in den Briefkasten geworfenen Wahlbriefumschläge werden von der Post übermittelt und von Mitarbeitern der *Verwaltung* entgegengenommen. An der Aktivität sind mindestens zwei Mitarbeiter der *Verwaltung* beteiligt, IT-Systeme werden keine verwendet. Input und Output ist der eingegangene Wahlbriefumschlag. Im Normalfall werden die bei der *Verwaltung* eingetroffenen Wahlbriefumschläge entgegengenommen; nach Öffnung und Entnahme des Wahlscheins wird der blaue Stimmzettelumschlag in die Wahlurne geworfen. Liegt bei den Mitarbeitern der *Verwaltung* ein böswilliges Interesse vor, so können die eingegangenen Wahlbriefumschläge entweder vernichtet (Verfügbarkeit) oder durch andere ersetzt (Authentizität) werden. Verletzt wird hierbei die Authentizität des Wahlbriefumschlages. Der IST-Zustand der Sicherheitsmaßnahmen versucht diesem Betrug durch ein Mehr-Augen-Prinzip entgegenzuwirken. Wird dieses konsequent umgesetzt, reicht die Sicherheitsmaßnahme aus, um die verschiedenen Betrugsmöglichkeiten zu verhindern, da die zuständigen Mitarbeiter unterschiedliche politische Interessen vertreten. Somit werden keine weiteren Sicherheitsmaßnahmen für den SOLL-Zustand gemacht. Der Anteil der Briefwähler, die ihre Wahlbriefumschläge per Post versenden, ist im Gegensatz zu der Gesamtanzahl der Wähler sehr gering. Vielen Wählern ist bewusst, dass der Postweg eine Schwachstelle bei der Briefwahl darstellt. Aufgrund dieser Einschätzung wird die Wahrscheinlichkeit als gering eingestuft.

Für die Aktivität [1.A15] konnten zwei Sicherheitsanforderungen identifiziert werden: Authentizität und Verfügbarkeit der Wahlbriefumschläge.

Stimmzettel aushändigen [1.A23]

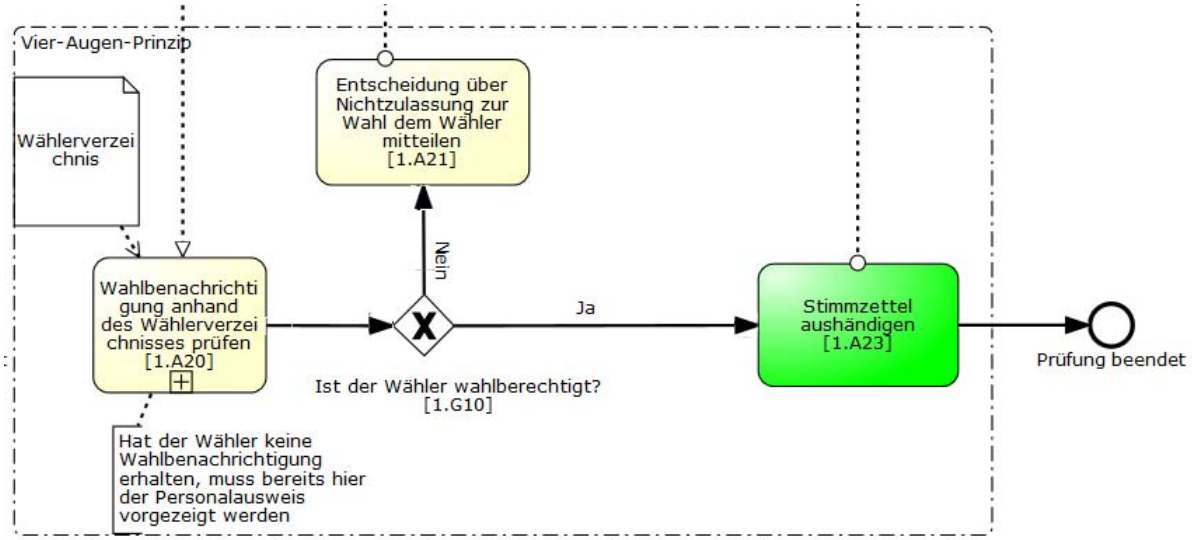

Abbildung 60: Stimmzettel aushändigen

Der *Wähler* bekommt nach der Überprüfung des Wahlscheines und der Feststellung, dass er zur Wahl berechtigt ist, d.h. er ist wahlberechtigt und befindet sich darüber hinaus im richtigen Wahlbezirk, seinen Stimmzettel von einem Mitglied des *Wahlvorstandes* ausgehändigt. An der Aktivität sind der *Wähler* und mindestens ein Mitglied des *Wahlvorstandes* beteiligt, IT-Systeme werden keine verwendet. Die Aktivität wird gestartet, nachdem die Überprüfung des Wahlscheins positiv verlaufen ist; der Output besteht in dem Stimmzettel, der dem *Wähler* ausgehändigt wird. Im Normalfall erhält der *Wähler* von einem Mitglied des *Wahlvorstandes* genau einen Stimmzettel (§46.1 KWO). Verfolgen beide Parteien ein böswilliges Interesse, so kann ein korruptes *Wahlvorstandsmitglied* in Absprache mit eingeweihten *Wählern* diesen anstatt einem Stimmzettel zwei aushändigen und damit das Wahlergebnis manipulieren. Der *Wahlvorstand* muss allerdings einen weiteren Stimmabgabenvermerk im Wählerverzeichnis tätigen; diesaAm besten bei solchen *Wahlberechtigten*, die wegen Abwesenheit nicht wählen gehen können, damit die Manipulation nicht entdeckt wird. Können keine weiteren Stimmabgabevermerke gemacht werden, so ist die Manipulation nur in einem geringen Maße möglich, da ansonsten die Zahl der Stimmabgabevermerke im Wählerverzeichnis mit der Stimmzettelanzahl in der Wahlurne zu starke Unterschiede aufweisen würde und somit ggfls. das Resultat des Stimmbezirks nicht anerkannt wird. Sollte nur das Mitglied vom *Wahlvorstand* korrupt sein, so kann er durch das Hinzufügen weiterer Stimmzettel versuchen, die Wahl ungültig zu machen. Allerdings stellt sich hier die Frage, warum dieser Betrug ausge-

führt werden soll. Er bezweckt damit lediglich eine Neuwahl, die hinsichtlich der zu erwartenden Ergebnisse keine großen Unterschiede zur originären Wahl aufweisen würde. Die Manipulation würde somit schnell entdeckt. In diesem Fall wird die Authentizität der Stimmzettel und ggf. die Verfügbarkeit der Stimmabgabe verletzt. Der IST-Zustand sieht momentan eine gegenseitige Kontrolle der jeweiligen *Wahlvorstandsmitglieder* vor. Aufgrund der Anzahl der Wahlvorstandsmitglieder ist das personell gesehen ein großer Aufwand. Eine zusätzliche Maßnahme[43] für den SOLL-Zustand könnte sein, dass der Stimmzettelstapel jeweils so aufgebaut ist, dass ein Stimmzettel längs liegt und der darauffolgenden quer. Dadurch würde eine Manipulation dieser Art zusätzlich erschwert. Da diese Betrugsart nur in kleinem Maße ohne Entdeckung möglich ist und der Nutzen niedrig ist, wird das Risiko[44] als gering eingeschätzt.

Für die Aktivität [1.A23] konnten zwei Sicherheitsanforderungen[45] identifiziert werden: Integrität des Stimmzettels[46] und Verfügbarkeit des Stimmzettels.

[43] Anm. der Betreuer: Die Sinnhaftigkeit dieser Sicherheitsmaßnahme ist fraglich, wenn davon ausgegangen wird, dass der Wahlvorstand korrupt ist

[44] Anm. der Betreuer: Der Aufbau der Analyse ist etwas unglücklich: Erst wird die Bedrohung beschrieben, dann der Ist-Zustand. Anschließend folgt der Vorschlag (= Soll-Zustand), und zuletzt wird auf das Risiko der Gefährdung eingegangen. Letzteres wäre besser direkt bei den korrespondierenden Bedrohungen / Gefährdungen aufgehoben.

[45] Anm. Der Betreuer: Zusätzliche Sicherheitsanforderung „Authentizität des Stimmzettels“ bezieht sich darauf, dass jedes Mitglied des Wahlvorstands nicht selbst mehr als einen Stimmzettel abgibt (oder einem Wahlberechtigten mehr als einen Stimmzettel gibt).

[46] Anm. der Betreuer: Die Sicherheitsanforderung „Integrität der Stimmzettel“ wurde im vorangehenden Text nicht hergeleitet. Sie könnte bei der Übergabe insofern beeinträchtigt werden, als dass der Herausgebende einfache „Markierungen“ z. B. mit Hilfe des Fingernagels vornehmen könnte. Damit könnte dieser prinzipiell die Trennung zwischen einem bestimmten Wähler und dessen Stimme aufheben.

Hilfsperson bestimmen [1.A24]

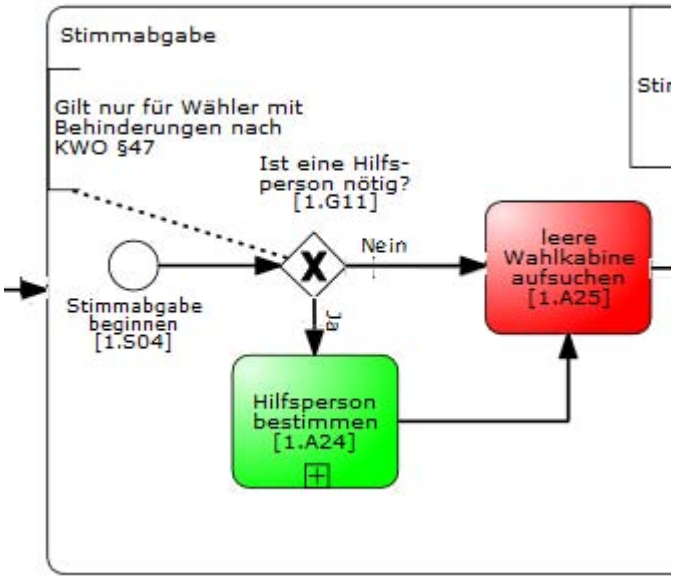

Abbildung 61: Hilfsperson bestimmen

„Ein Wähler, der des Lesens unkundig oder wegen körperlicher Beeinträchtigung nicht in der Lage ist, den Stimmzettel zu kennzeichnen, zu falten und diesen selbst in die Wahlurne zu legen“ (§47 KWO), darf eine *Hilfsperson* bestimmen, die ihm bei der Stimmabgabe behilflich ist. Die *Hilfsperson* kann der *Wähler* entweder aus dem Familien- oder Freundeskreis bestimmen und zur Wahl mitbringen oder vor Ort aus dem *Wahlvorstand* wählen. Dabei ist sicherzustellen, dass der *Wähler* die Hilfsperson selber bestimmt und sich nicht Personen als solche aufdrängen. An der Aktivität sind der *Wähler* und eine *Hilfsperson* beteiligt, IT-Systeme werden keine verwendet. Es gibt keinen In- und Output für diese Aktivität. Im Normalfall stimmt die *Hilfsperson* im Interesse des *Wählers* ab (§47 KWO). Verfolgt die *Hilfsperson* ein böswilliges Interesse, so stimmt sie nicht im Interesse des *Wählers*, sondern in eigenem Interesse ab. Den Betrug muss die *Hilfsperson* so anstellen, dass der eigentliche *Wähler* die falsche Stimmabgabe nicht mitbekommt und dadurch keinen Widerstand leistet. Die Authentizität der Wählerstimme wird durch diese Möglichkeit des Betruges verletzt. Der IST-Zustand sieht keine Sicherheitsmaßnahmen für diesen Fall vor. Dies ist auch nicht notwendig, da der *Wähler* als *Hilfsperson* auch ein Mitglied des *Wahlvorstandes* wählen kann. Eine Sicherheitsmaßnahme für den SOLL-Zustand ist demnach auch nicht nötig. Es wird angenommen, dass in den meisten Fällen der *Wähler* nicht erst im Wahllokal die *Hilfsperson* bestimmt, sondern einen engen vertrauenswürdigen Verwandten oder Freund als *Hilfsperson* mitnimmt. Da der Anteil von hilfsbedürftigen Wählern, die an der Präsenzwahl teilnehmen,

wahrscheinlich sehr gering ist und der zu erwartende Nutzen sich in Grenzen hält, wird die Wahrscheinlichkeit des Auftretens dieser Manipulation als gering eingestuft.

Für die Aktivität [1.A24] konnte drei Sicherheitsanforderungen identifiziert werden: Verfügbarkeit und Integrität der Hilfsperson und vertrauliches Agieren der Hilfsperson.

Leere Wahlkabine aufsuchen [1.A25]

Der *Wahlvorstand* lässt einen *Wähler* seine Stimme abgeben, sobald eine Wahlkabine frei ist. Die Wahlkabine dient dem Schutz der Stimme, sodass diese nur dem *Wähler* bekannt ist und für alle anderen geheim. An der Aktivität sind der *Wähler* und mindestens ein Mitglied des *Wahlvorstandes* beteiligt, IT-Systeme werden keine verwendet. Input ist der leere, d.h. nicht markierte Stimmzettel und Output ist der vom *Wähler* markierte Stimmzettel. Im Normalfall gibt der *Wähler* seine Stimme unbeobachtet und somit geheim ab (§38 KWO). Nur ihm ist seine Stimmabgabe somit bekannt. Verfolgt der *Wahlvorstand* oder ein Außenstehender, der Zugriff zum Wahlraum hat, böswillige Interessen, so könnten diese eine Kamera im Raum anbringen. Diese wird so angebracht, dass sie den Tisch in der Wahlkabine einfängt, auf dem der *Wähler* seine Stimme abgibt. Somit sind die Beteiligten in der Lage, den Stimmenstand des Wahlbezirkes zu verfolgen und gegebenenfalls durch andere Maßnahmen wie Stimmenkauf oder durch Manipulationen bei der Stimmenauszählung weiter zu beeinflussen. Die Kamera muss möglichst klein und so angebracht sein, dass sie dem *Wähler* nicht auffällt; wie zum Beispiel als Rauchmelder getarnt. Verletzt wird durch diesen Betrug die Vertraulichkeit der Stimmabgabe des Wählers. Der IST-Zustand der Sicherheitsmaßnahmen besteht in dem Vertrauen gegenüber dem Schlüsselbesitzer, dass dieser den Schlüssel zum Wahllokal an keine Person weitergibt und selbst nicht korrupt handelt. Zudem wird um die Wahlkabine ein Sichtschutz aufgestellt, der die Stimmabgabe des Wählers nicht einsehbar macht. Die Kabinen und der dazugehörige Sichtschutz werden so platziert, dass die offene Seite weder vom *Wahlvorstand* bzw. anderen *Wählern* einsehbar ist. Zudem darf diese Seite nicht zum Fenster oder einer Türe stehen, da sonst die Geheimhaltung der Stimmabgabe gefährdet ist. Eine weitere Sicherheitsmaßnahme für den SOLL-Zustand könnte sein, dass die Räume vor Wahlbeginn von geschultem Personal auf Kameras untersucht werden. Dadurch würde diese Art des Betruges zumindest erschwert, wenn nicht sogar unmöglich gemacht.

Für die Aktivität [1.A25] konnten zwei Sicherheitsanforderungen identifiziert werden: Vertraulichkeit der Stimmabgabe [47]und Verfügbarkeit der Wahlkabine.

Stimmabgabe im Wählerverzeichnis vermerken [1.A41]

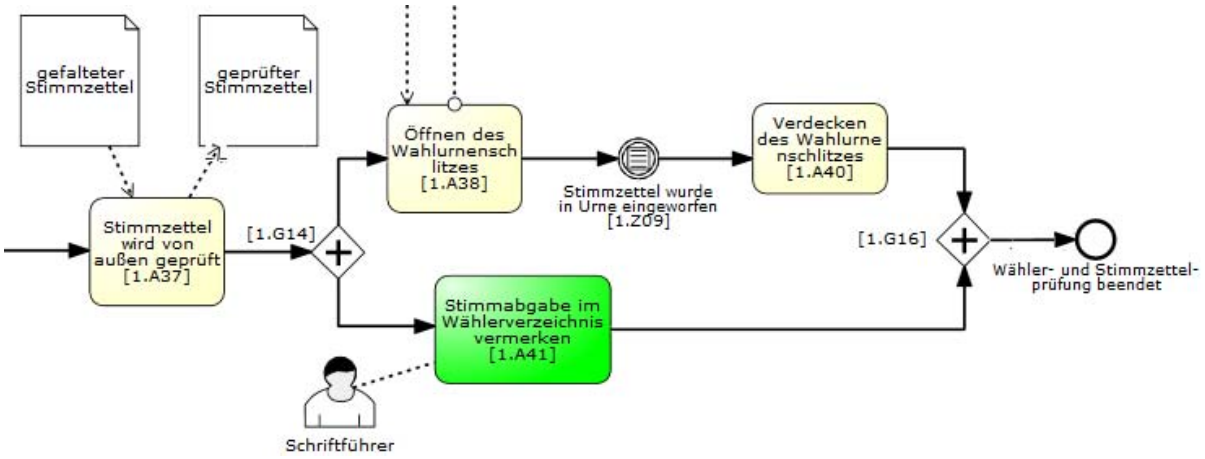

Abbildung 62: Stimmabgabe im Wählerverzeichnis vermerken

Nach der Identitätsprüfung wird im Wählerverzeichnis markiert, dass der *Wähler* seine Stimme abgegeben hat. Damit wird verhindert, dass dieser nochmals seine Stimme abgeben kann. An der Aktivität sind der *Wähler* und mindestens zwei Mitglieder des *Wahlvorstandes* beteiligt, IT-Systeme werden keine verwendet. Der Input ist der vom *Wähler* ausgefüllte Stimmzettel und der Output der Stimmabgabenvermerk beim *Wähler* im Wählerverzeichnis. Im Normalfall wird für den *Wähler* ein Stimmabgabenvermerk im Wählerverzeichnis gemacht, damit ersichtlich ist, dass er seine Stimme abgegeben hat (§46.2 KWO). Sind Mitglieder des *Wahlvorstandes* korrupt, können sie den Stimmabgabenvermerk für den *Wähler* nicht tätigen oder absichtlich bei einer anderen Person, die sie damit an der Stimmabgabe hindern. Mit ersterem würden sie eine Differenz zwischen abgegebenen Stimmen und Stimmabgabevermerken verursachen. Ist diese zu groß und somit nicht mehr tolerabel, kommt es zu Neuwahlen für den Stimmbezirk, welches ggfls. das Ziel des korrupten *Wahlvorstandmitgliedes* sein kann. Zusätzlich könnte der *Wahlvorstand* auch für mehr als eine Person einen Stimmabgabenvermerk machen und somit selbst die Möglichkeit haben, noch Stimmzettel nach Wahlschluss der Wahlurne hinzuzufügen. Während der Wahl verletzt dieser Betrug die Verfügbarkeit, ansonsten die Authentizität der Stimmen[48] und die Integrität des Wählerverzeichnisses.

[47] Anm. der Betreuer: Diese Sicherheitsanforderung spielt beim Aufsuchen der leeren Wahlkabine noch keine Rolle. Erst im Anschluss, wenn die Stimmabgabe erfolgt, ist diese Sicherheitsanforderung von Bedeutung. Ggfls. könnte hier die Vertraulichkeit schon als Vorbedingung aufgefasst werden.

[48] Anm. der Betreuer: Das Eintragen von Stimmabgabevermerken kann als vorbereitender Angriff angesehen werden, wenn der Urne nachträglich Stimmzettel hinzugefügt werden sollen. Ein Betrug könnte so nicht aufge-

Der IST-Zustand der Sicherheitsmaßnahmen versucht diesen Betrug durch das Vorhandensein von unterschiedlichen politischen Interessen im *Wahlvorstand* sowie einem Mehr-Augen-Prinzip zu verhindern. Da es aufgrund der Personenzahl sehr unwahrscheinlich ist, dass der gesamte *Wahlvorstand* korrupt ist, reichen diese Sicherheitsmaßnahmen aus. Verstärkt werden könnte diese im IST-Zustand durch das Markieren der *Wähler* im zwei unabhängigen Wählerverzeichnis von zwei verschiedenen Mitgliedern des *Wahlvorstandes*. Bei Nichtübereinstimmen der beiden Wählerverzeichnisse würde ein Betrug sehr schnell aufgedeckt werden. Da diese Betrugsart nur in kleinem Maße ohne Entdeckung möglich ist, wird das Risiko als gering eingeschätzt.

Für die Aktivität [1.A41] konnten drei Sicherheitsanforderungen identifiziert werden: Integrität und Verfügbarkeit des Wählerverzeichnisses und Nichtabstreitbarkeit der Stimmabgabe[49] durch den Wähler.

Vorbereitungen für den Urnentransport

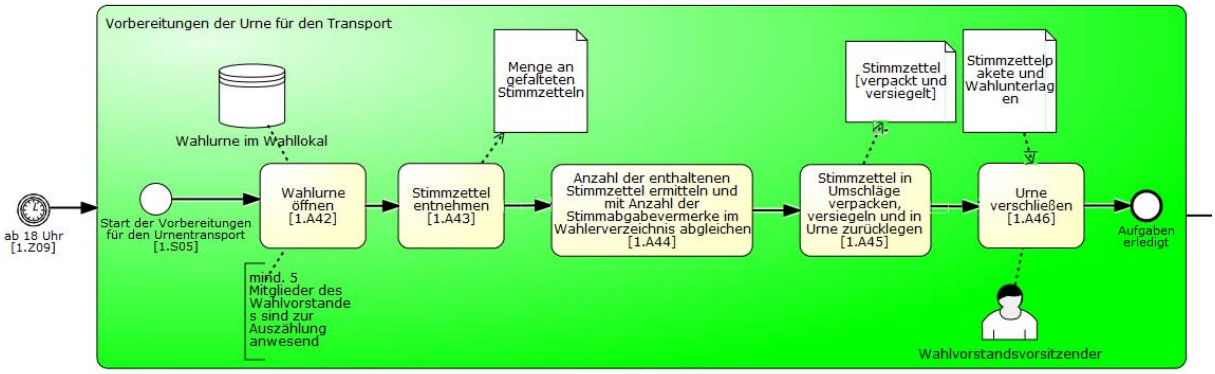

Abbildung 63: Vorbereitung für den Urnentransport

Zwischen der letzten Stimmabgabe und dem Eintreffen der *Sicherheitsleute*, die für den Transport der Urne verantwortlich sind, vergeht Zeit, die der *Wahlvorstand* ggf. alleine im Wahllokal verbringt. Sollten *Beobachter* anwesend sein, ist die Manipulation nicht durchführbar. An der Aktivität ist der gesamte *Wahlvorstand* des Wahllokales beteiligt, IT-Systeme

deckt werden, da die Anzahl der Stimmen in der Urne mit der Anzahl der Stimmabgabevermerke übereinstimmt. Über die Authentizität der Stimme sollte an dieser Stelle aber nicht gesprochen werden, da der Urheber einer Stimme laut Wahlrechtsgrundsatz (Geheimheit) nicht bekannt sein darf.

[49] Anm. der Betreuer: Diese Sicherheitsanforderung wurde im vorangehenden Text nicht hergeleitet, wenngleich sie korrekt ist: Mit Hilfe des Stimmabgabevermerks wird sichergestellt, dass ein Wähler der Urne genau einen Stimmzettel zuführen darf. Ihm ist es also nicht möglich, eine Stimmabgabe zu bestreiten. Dadurch ist jedoch auch die Gefahr gegeben, dass Wahlberechtigte, die noch nicht gewählt haben, von der Wahl ausgeschlossen werden. Der Nutzen dieses Angriffs ist jedoch fraglich, weswegen dieser eher als „theoretisch möglich“ angesehen werden soll.

werden keine verwendet. Input ist das Wählerverzeichnis sowie die Wahlurne samt den enthaltenen Stimmzetteln. Output ist die zum Abtransport bereitstehende Urne. Im Normalfall beginnt der *Wahlvorstand* nach der letzten Stimmabgabe damit, die Wahlurne für den Transport fertig zu machen. Die Wahlurnen werden geöffnet und die Stimmzettel werden entnommen. Danach wird die Zahl der Stimmabgabenvermerke im Wählerverzeichnis mit der Anzahl der enthaltenen Stimmen abgeglichen. Stimmt die Zahl überein oder ist die Abweichung tolerabel, so werden die Stimmzettel in Pakete verpackt. Zusammen mit den Wahlunterlagen werden diese in die Urne gelegt und diese wird verschlossen. Verfolgt der gesamte *Wahlvorstand* böswillige Interessen, so könnte dieser, wenn sich im Wahllokal nach der letzten Stimmabgabe keine Beobachter befinden, im Namen von *Nicht-Wählern* abstimmen. Dementsprechend müsste natürlich auch das Wählerverzeichnis manipuliert werden. Je nach Wahlbeteiligung ist die Anzahl der Nicht-Wähler unterschiedlich groß. Aus den vorherigen Wahlen existieren Vergleichszahlen zur Wahlbeteiligung. Große Schwankungen würden den Verdacht einer Manipulation nahe legen. Verletzt werden durch diesen Betrug die Integrität des Wählerverzeichnisses sowie der Wahlurne und die Authentizität von Stimmen. Der IST-Zustand der Sicherheitsmaßnahmen sieht vor, dass der Wahlvorstand aus verschiedenen Parteienangehörigen besteht. Dadurch wird die Wahrscheinlichkeit eines gesamten korrupten *Wahlvorstandes* eigentlich ausgeschlossen. Denn welches Ziel würde die Manipulation durch den gesamten *Wahlvorstand* haben, wenn jeder Einzelne unterschiedliche Interessen vertritt. Eine weitere Sicherheitsmaßnahme für den SOLL-Zustand ist demnach nicht notwendig. Aufgrund der getroffenen Sicherheitsmaßnahme und dem geringen Nutzen wird dieser Manipulationsversuch als sehr unwahrscheinlich eingeschätzt.

Für den Unterprozess konnten zwei Sicherheitsanforderungen identifiziert werden: Verfügbarkeit und Integrität der Wahlurne.

Externe Angriffe[50]

Neben den Interessenkonflikten zwischen den Beteiligten kann die Stimmabgabe noch durch externe Angriffe beeinflusst werden. Ein möglicher externer Angriff ist das Abfangen der Wahlunterlagen durch den *Postboten*. In kleinem Maße ist diese Manipulation möglich, hat aber auch fast gar keinen Einfluss auf das Wahlergebnis. Ein groß angelegter Angriff auf den

[50] Anm. der Betreuer: Die möglichen externen Angriffe werden immer zu Ende jedes Teilprozesses betrachtet.

kompletten Bezirk des *Postboten* wäre einflussreicher auf das Wahlergebnis. Allerdings würde dieser von der *Verwaltung* sehr schnell aufgedeckt und alle eingehenden Briefwahlunterlagen aus dem zugehörigen Bezirk würden aussortiert werden. Wie sich herausstellt, ist die Wahrscheinlichkeit für diesen Angriff relativ gering, da er sehr schnell ersichtlich ist und auch nicht in großer Anzahl durchführbar ist.

Ein weiterer externer Angriff, der allerdings weitaus vielversprechender ist, ist der des Stimmenkaufs. Dabei versucht ein *Außenstehender* im Vorfeld der Wahl *Wahlberechtigte* durch Erpressung oder durch Anreize in Form von Geld oder anderen Annehmlichkeiten zu beeinflussen, die von ihm favorisierte Partei zu wählen. In Verbindung mit einer Kameraüberwachung im Wahllokal könnte die Stimmabgabe der *Wähler* auch überprüft werden und mit Sanktionen gedroht werden, wenn der Wähler nicht im Sinne des Stimmenkäufers abstimmt. Dafür müsste der Erpresser allerdings vor Wahlbeginn Zugang zum Wahllokal haben, um eine Kamera in diesem anzubringen. Mit genügend Geld oder Einfluss lässt sich die Wahl also in größerem Maße manipulieren. Der *Statistiker* würde die etwas größeren Abweichungen bemerken, allerdings könnte nicht nachgewiesen werden, dass es wirklich eine Manipulation gab, wenn alle Erpressten beziehungsweise Gekauften den Stimmenkauf nicht publik machen. Gerade davon ist der Stimmenkauf nämlich abhängig. Aber auch hier gilt: je mehr Personen involviert sind, umso größer die Gefahr des Aufdeckens.

6.3.3. Stimmauszählung

Urnen übernehmen [2.A12]

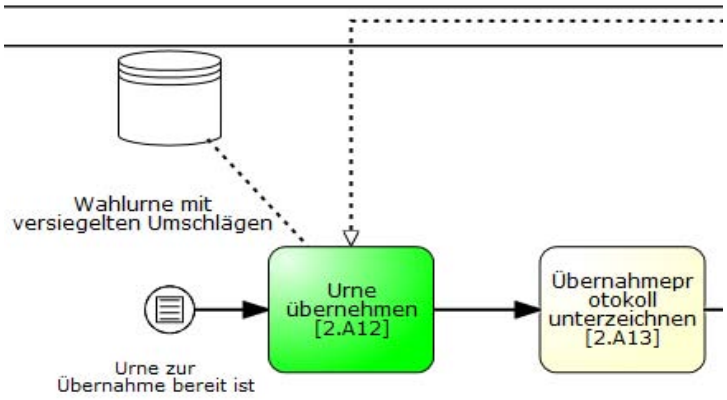

Abbildung 64: Urne übernehmen

Die verschlossenen Wahlurnen, in denen sich die abgegebenen Stimmen der *Wähler* in versiegelten und beschrifteten Paketen befinden, werden von mindestens zwei Personen des *Si-*

cherheitsdienstes übernommen. Diese Aktivität wird von der *Verwaltung* ohne die Beteiligung weiterer IT-Systeme ausgeführt. Der Input besteht aus den Wahlurnen mit den darin enthaltenen versiegelten und beschrifteten Stimmzetteln der Briefwahl sowie der Direktwahl. Der Output setzt sich ebenfalls aus den Wahlurnen mit den darin enthaltenen versiegelten und beschrifteten Stimmzetteln der Briefwahl sowie der Direktwahl zusammen. Im Normalfall übernimmt die *Verwaltung* die versiegelten, befüllten Wahlurnen nach der Wahl, ohne die darin enthaltenen Daten einzusehen oder zu verändern. Um den Verbleib der Wahlurnen nachweisen zu können, muss die *Verwaltung* ein Übernahmeprotokoll unterschreiben. Die Aktivität sieht neben der Urnenübernahme keinerlei weitere Interaktionen mit den Urnen vor. Verfolgen die bei der Urnenübernahme anwesenden Vertreter der *Verwaltung* zusammen mit dem *Wahlleiter* böswillige Absichten, so können sie die in den Urnen enthaltenen Wahlzettel, durch bereits vorher präparierte Stimmzettel, austauschen. Als Vorbedingung für diese Wahlmanipulation muss ein *Verwaltungsmitglied* oder der *Wahlleiter* bei den Wahlvorbereitungen oder während der Stimmabgabe, die benötigten Originalstimmzettel entwenden. Bei diesem Vorgehen könnte die Integrität, d. h. die Unveränderbarkeit der in den Urnen enthaltenen Daten verletzt werden und somit auch die Authentizität des späteren Wahlergebnisses. Der IST-Zustand der Sicherheitsmaßnahmen ist so konzipiert, dass lediglich Mitglieder der *Verwaltung* sowie der *Wahlleiter* Zugriff auf die Urnen haben. Des Weiteren werden die Urnen in einem abgeschlossenen Raum aufbewahrt. Dieser darf jeweils nur von mindestens zwei Personen betreten werden, um das Vier-Augen-Prinzip sicherzustellen. Diese Maßnahme wird getroffen um zu verhindern, dass zugriffsberechtigte Parteien die versiegelten Stimmzettel nicht einsehen, manipulieren oder die Wahlurnen verschwinden lassen.

Um die Sicherheitsvorkehrungen noch weiter zu stärken, könnte ein SOLL-Zustand angestrebt werden, indem noch weitere Parteien wie beispielsweise die *Sicherheitsfirma* zur Übernahme der Urnen hinzugezogen werden. Allerdings sollte nur dann eine Firma oder eine dritte Partei von außen hinzugezogen werden, wenn dieser vollständiges Vertrauen entgegengebracht wird. Diese zusätzliche Partei könnte nämlich ebenso ein weiteres Sicherheitsrisiko darstellen. Ebenso denkbar wäre es, als Sicherheitsmaßnahme unabhängige *Wahlbeobachter* bei dem Transport der Urnen sowie bei dem Einschließen der Urnen zuzulassen. Durch die Anwendung der zuvor genannten Möglichkeiten der Wahlmanipulation wäre eine Verfälschung des Wahlergebnisses möglich. Um eine starke Beeinflussung vorzunehmen, müsste jedoch im Vorhinein eine immense Anzahl an authentischen, nicht markierten Stimmzetteln beschafft werden. Dies wiederum setzt einen sehr hohen, organisatorischen Aufwand voraus,

der mit der Gefahr der Entdeckung der Wahlmanipulation einhergeht. Gelingt es, die gewünschte Anzahl an authentischen, nicht markierten Stimmzetteln zu beschaffen und die Wahlzettel in den Urnen unbemerkt auszutauschen, ist es dennoch wahrscheinlich, dass die Wahlmanipulation bei der Überprüfung der Ergebnisse durch den *Statistiker* entdeckt wird. Aus diesem Grund ist es nicht zwingend erforderlich weitere Maßnahmen zu treffen, um den IST-Zustand zu verbessern. Um das Prinzip der Öffentlichkeit jedoch weiter voranzutreiben, sollte darüber nachgedacht werden unbeteiligte *Wahlbeobachter* bei dem Transport der Urnen sowie bei deren Wegschließen zuzulassen.

Für die Aktivität [2.A12] konnte eine Sicherheitsanforderung identifiziert werden: Integrität der in den Urnen enthaltenen Daten.

Urnen überwachen [2.A16]

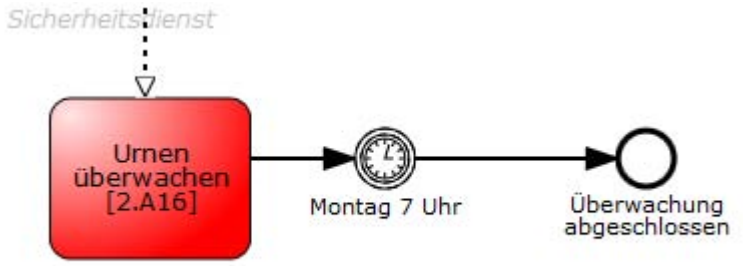

Abbildung 65: Urne überwachen

Die sich in der Rhein-Mosel-Halle befindenden Wahlurnen werden über Nacht von einem *Sicherheitsdienst* überwacht. An der Aktivität ist der *Sicherheitsdienst* als alleinige Partei beteiligt. Als Input sind hier die Wahlurnen mit den darin enthaltenen versiegelten Umschlägen zu betrachten. Ein Output kommt bei dieser Aktivität nicht vor, da die Urnen in ihrem Zustand unverändert bleiben sollen. Im Normalfall übernimmt der von der *Verwaltung* ausgewählte *Sicherheitsdienst* sonntagabends die Überwachung der versiegelten Urnen in der Rhein-Mosel-Halle bis zum nächsten Morgen um 7 Uhr. Dabei ist es seine Aufgabe sicherzustellen, dass die Wahlurnen nicht gestohlen und die Stimmzettel weder eingesehen noch manipuliert werden können. Hierfür werden mindestens zwei Mitarbeiter des *Sicherheitsdienstes* herangezogen. Ist es die alleinige Absicht des *Sicherheitsdienstes* eine Wahlmanipulation vorzunehmen, könnte dieser die Urnen zerstören oder verschwinden lassen. Verfolgt der *Sicherheitsdienst* zusammen mit dem *Wahlleiter* böswillige Absichten, so kann ein Austausch

der in den Urnen enthaltenen Stimmzettelpakete vorgenommen werden. Ein weiteres mögliches Angriffsszenario wäre die Bestechung des *Sicherheitsdienstes* durch eine *Dritte Partei*. Dies könnte die Zerstörung oder Manipulation der Stimmzettel oder das Verschwinden der Wahlurnen zur Folge haben. Wird das erste Szenario betrachtet, so wird die Verfügbarkeit der abgegebenen Stimmen verletzt und es müssten als Konsequenz Neuwahlen durchgeführt werden. Bei Eintritt des zweiten Szenarios wird die Integrität der Stimmen verletzt. Das dritte Szenario würde ebenfalls die Verfügbarkeit der abgegebenen Stimmen einschränken und hätte eine Neuwahl und somit eine Verzögerung der Wahl zur Folge. Der IST-Zustand der Sicherheitsmaßnahmen ist so konzipiert, die Urnen über Nacht durch einen *Sicherheitsdienst* überwachen zu lassen, um potentiellen Manipulationsversuchen der Wahlen entgegenzuwirken. Hierbei muss sichergestellt werden, dass niemand (inklusive des *Sicherheitsdienstes)* die Gelegenheit hat, die Urnen zu manipulieren oder verschwinden zu lassen. Um die Überwachung der Urnen sicher zu gestalten, wird auch hier auf ein Mehr-Augen Prinzip zurückgegriffen, da immer mindestens zwei Sicherheitsbeauftragte zur Bewachung der Urnen herangezogen werden. Der SOLL-Zustand könnte so ausgestaltet werden, dass neben dem *Sicherheitsdienst* auch Mitglieder der *Verwaltung* zur Bewachung der Urnen hinzugezogen werden. Bei diesen ist anzunehmen, dass ein starkes Motiv vorliegt, die Unveränderbarkeit der Wahlergebnisse zu schützen. Somit würden die Sicherheitsmaßnahmen bei dieser Aktivität noch weiter ausgebaut werden.

Im ersten Szenario ist der *Sicherheitsdienst* der einzige Wahlmanipulator. Alleine wäre es ihm möglich, die Verfügbarkeit der abgegebenen Stimmen zu beeinträchtigen. Hierbei müsste er die Stimmzettel in den Urnen lediglich verschwinden lassen oder die Urnen an einen anderen Ort transportieren. Dies setzt keinen bis einen geringen Organisationsaufwand voraus und birgt geringe Gefahren wie beispielsweise das Hinzukommen eines Unbeteiligten während der Urnenüberwachung. Folglich wäre es möglich, die Verfügbarkeit der Stimmen durch eine Manipulation des *Sicherheitsdienstes*, nicht gewährleisten zu können. Tritt das zweite Szenario, die Zusammenarbeit des *Sicherheitsdienstes* mit dem *Wahlvorsteher* ein, wäre eine signifikante Modifikation des Wahlergebnisses realisierbar. Um das Wahlergebnis beträchtlich zu verfälschen, muss im Vorfeld unentdeckt eine erhebliche Anzahl an authentischen, nicht markierten Stimmzetteln akquiriert werden. Dies setzt einen hohen Organisationsaufwand voraus und birgt zudem die Gefahr, dass die zusätzliche Beschaffung der Stimmzettel durch ein Mitglied der *Verwaltung* entdeckt beziehungsweise an im Wahlprozess beteiligte Parteien weitergetragen wird. Um diesen Fall zu vermeiden, wäre es zwar denkbar die beteiligten Parteien zu

korrumpieren, allerdings ist es schwer vorstellbar dass diese darauf eingehen. Denn bei diesen besteht ein ausgeprägtes Interesse daran, die Einhaltung der Wahlrechtsgrundsätze wie beispielsweise die Korrektheit des Ablaufes zu wahren. Gelingt es, die Stimmzettel unbemerkt zu besorgen, müssen diese so ausgefüllt werden, dass die vorgenommene Modifikation der abgegebenen Stimmen nicht offensichtlich erkennbar ist. Bei einem geschickten Vorgehen wäre es also möglich, die Stimmzettel unbemerkt auszutauschen und somit die Authentizität der abgegebenen Stimmen in einem hohen Maße zu verletzten. Grundvoraussetzung für das dritte Szenario ist, dass eine Zusammenarbeit mit dem *Sicherheitsdienst* stattfindet. Nur so können externe *Angreifer* einen Angriff auf die Wahlurnen durchführen. Gelingt es, den *Sicherheitsdienst* für eine Wahlmanipulation zu akquirieren, wäre es externen *Angreifern* möglich die Wahlurnen mitzunehmen oder diese zu zerstören. Für dieses Angriffsszenario können die Sicherheitsleute bestochen oder erpresst werden, und somit sollte über eine Verbesserung der Sicherheitsmaßnahmen nachgedacht werden. Die Wahlergebnisse werden durch diese Angriffsform eventuell beeinflusst, da Neuwahlen durchgeführt werden müssten die zu einem anderen Ergebnis führen könnten. Zudem wäre eine Durchführung von Neuwahlen mit hohen Kosten verbunden.

Für die Aktivität [2.A16] konnten zwei Sicherheitsanforderungen identifiziert werden: Integrität der abgegebenen Stimmen und Verfügbarkeit der abgegebenen Stimmen.

Ausdruck und Kontrolle ob Daten auf Stimmzettel von Programm richtig erfasst wurden [2.A25]

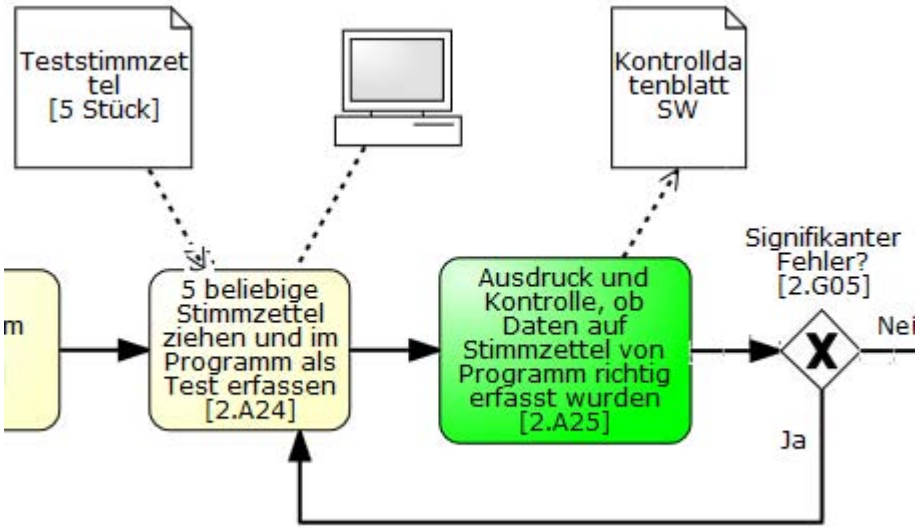

Abbildung 66: Ausdruck und Kontrolle der richtigen Erfassung des Stimmzettels durch das Programm

Die Stimmzettel, welche zu Beginn des Prozesses zum Test im Programm erfasst worden sind, werden ausgedruckt. Dieser Schritt ist notwendig, um zu kontrollieren, ob das Programm die eingegebenen Daten auf dem Stimmzettel richtig erfasst hat. An dieser Aktivität ist der *Wahlvorstand* beteiligt sowie mehrere IT-Systeme. Darunter die Auszahlungs-Software, der Stand-Alone-PC sowie der USB-Stick, auf dem sich das Wahlauszählungsprogramm befindet und auf dem die Daten der Stimmzettel gespeichert werden. Als Input gelten die entfalteten fünf Teststimmzettel, welche zu Beginn der Auszählung als Test im Programm erfasst worden sind. Durch den Test soll sichergestellt werden, dass das Programm einwandfrei funktioniert und die Stimmzettel richtig erfasst werden. Als Output gilt das Kontrolldatenblatt, welches wichtige Daten für die spätere Kontrolle der möglichen Abweichungen enthält. Im Normalfall müssen gemäß der Kommunalwahlordnung §§ 51 und 52 die erfassten Daten auf Richtigkeit überprüft werden, d.h. ob diese Daten auch mit den tatsächlichen übereinstimmen und somit richtig von dem Programm erfasst wurden. In dem Fall, dass sie von den Daten auf dem Stimmzettel abweichen, sollen sie erneut erfasst werden. Wenn der *Wahlvorstand* hierbei eine böswillige Absicht verfolgt, könnte er behaupten, dass das Programm nicht richtig arbeitet. Damit würde der Prozess etwas verzögert, da Ersatz-Rechner an dieser Stelle eingesetzt werden müssten. Zudem könnte es zu der Situation kommen, dass das Programm die Stimmen z.B. nicht richtig berechnet und der *Wahlvorstand* würde es nicht melden. Somit könnte die Wahl

manipuliert werden und dadurch würde die Integrität der Stimmzettel verletzt. Falls die Abweichungen nicht statistisch signifikant wären, wäre diese Situation nur schwer zu entdecken. Es ist also wichtig festzustellen, dass das Programm einwandfrei arbeitet, was z.B. durch eine Verwendung der richtigen, d.h. vom Landeswahlleiter freigegebenen Software-Version sichergestellt wird. Dafür wird im Ist-Zustand die Aktivität 2.A21 (Prüfziffer eingeben) durchgeführt. Die beschriebenen Manipulationen sind in der Praxis unwahrscheinlich, da bereits genügend Kontrolle durch die angewendeten Sicherheitsmaßnahmen gewährleistet wird und dadurch die vorhandenen Sicherheitsanforderungen umgesetzt werden.

Für die Aktivität [2.A25] konnten drei Sicherheitsanforderungen[51] identifiziert werden: Integrität der Stimmzetteldaten, Nichtabstreitbarkeit der richtigen Erfassung sowie Verfügbarkeit der Stimmzettel, der Arbeitsgruppe und der Systeme.

Vergebene Stimmen nacheinander 1:1 vorlesen, Stimmzettel nummerieren [2.A30]

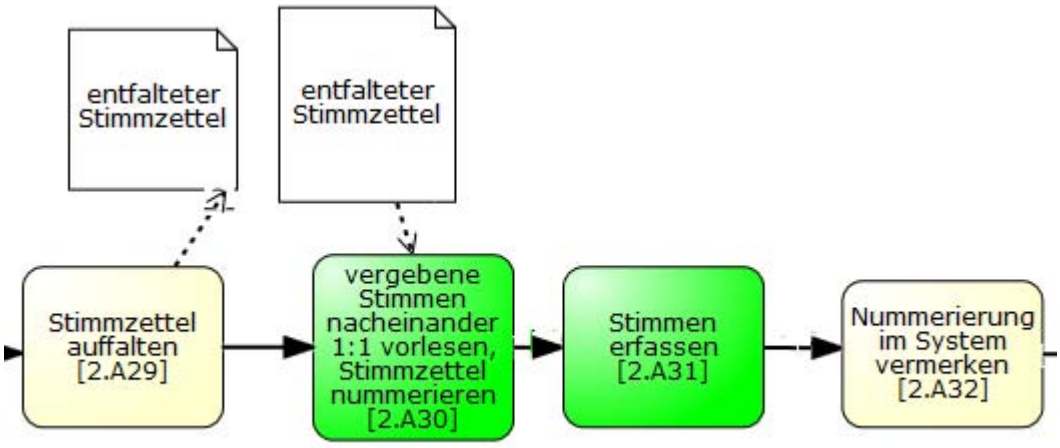

Abbildung 67: Stimmen vorlesen und Stimmzettel nummerieren

Ein Mitglied der *Arbeitsgruppe* liest für jeden Stimmzettel laut vor, welche *Partei* beziehungsweise welcher *Kandidat* wie viele Stimmen erhalten hat. Durch ein weiteres Mitglied wird die Aussage überprüft. Nach dem das geschehen ist, werden die Stimmzettel nummeriert. An der Aktivität sind zwei Mitglieder der *Arbeitsgruppe* des Stimmbezirks beteiligt und keine IT-Systeme werden benutzt. Als Input für die Aktivität gilt der entfaltete Stimmzettel

[51] Anm. der Betreuer: Die hier genannten Sicherheitsanforderungen beziehen sich auf vorangehende Aktivitäten. Die hier untersuchte Aktivität selbst stellt eine Sicherheitsmaßnahme dar. Hierbei werden bspw. die Integrität der Stimmzetteldaten oder die Authentizität der verwendeten Software belegt

und als Output die genannten Stimmen sowie die vergebenen Nummern. Durch die Nummerierung lässt sich zu jedem digitalen Stimmzettel sein analoges Pendant finden. Im Normalfall müssen gemäß der Kommunalwahlordnung §55b die vergebenen Stimmen laut vorgelesen werden. Verfolgen beide Mitglieder der *Arbeitsgruppe* böswillige Absichten, so könnte die Stimme falsch vorgelesen werden, z.B. ein Wähler hat Hr. Meier gewählt und Hr. Müller wird laut vorgelesen. Somit würde die Wahl manipuliert. Sollte dieses Vorgehen im großen Maße geschehen, müssten die beiden Mitglieder der *Arbeitsgruppe* mit dem *Statistiker* kooperieren, damit dieser die Auffälligkeiten nicht melden würde. Eine andere Möglichkeit der Wahlmanipulation besteht darin, dass die Stimmabgabe eines *Wählers* als ungültig erklärt wird, obwohl sie in Wirklichkeit gültig ist (z.B. Angabe, dass der Stimmzettel einen Vermerk enthalten hat). Bei solchen Vorgehen wird die Integrität des Stimmzettels verletzt. Der IST-Zustand sieht hier ein Mehr-Augen-Prinzip vor. Der *Vorlesende* wird durch ein weiteres Mitglied der *Arbeitsgruppe* beobachtet, der die Aussage des Vorlesenden überprüft. Wenn beide Mitglieder unterschiedliche politische Interessen besitzen, ist diese Art der Manipulation praktisch unmöglich. Bei den einzelnen Teams kann dies jedoch nicht sichergestellt werden. Um den entgegenzuwirken könnten bei dem Wahlvorgang z.B. rote Stifte[52] eingesetzt werden (SOLL-Zustand), d.h. die *Wähler* markieren die gewählte Partei mit einem roten Stift. Damit wird vermieden, dass Stimmzettel ungültig markiert oder modifiziert (d.h. Hinzufügen von neuen Stimmen bzw. Streichungen) werden.

Für die Aktivität [2.A30] konnten zwei Sicherheitsanforderungen identifiziert werden: Integrität und Verfügbarkeit der Stimmzettel sowie deren Stimmen.

Stimmen erfassen [2.A31]

Bei dieser Aktivität werden die vorgelesenen Stimmen ins System übertragen. An dieser Aktivität sind zwei Mitglieder der *Arbeitsgruppe* beteiligt und die Auszählungssoftware „Berninger PC-Wahl“ wird verwendet. Als Input gelten die vorgelesenen Stimmen und als Output gelten die im System erfassten Stimmen. Im Normalfall sollen gemäß der Kommunalwahlordnung §§ 51 und 52 die Stimmzettel erfasst werden. Bei böswilliger Absicht könnte die Wahl durch die Erfassung von gefälschten Stimmen manipuliert werden, d.h. wenn Wähler A den Kandidaten X gewählt hat, könnte bei dem Vorlesen der Kandidat Z angeben und im Programm erfasst werden. Hierbei wird die Integrität der Stimmzettel verletzt. An dieser Stelle

[52] Interessanterweise ist dies der Ist-Zustand: Die Wähler markieren den Stimmzettel mit einem blauen / schwarzen Stift; bei der Auszählung bzw. Vergabe der Nummer werden rote Stifte benutzt.

greift jedoch das Vier-Augen-Prinzip (IST-Zustand) ein, indem wechselnde Teams die einzelnen Stimmen erfassen. Damit wird der Vorgang sichergestellt und somit ist die Eintrittswahrscheinlichkeit gering.

Für die Aktivität [2.A31] konnten drei Sicherheitsanforderungen identifiziert werden: Integrität und Verfügbarkeit der Stimmzettel[53] sowie Nachvollziehbarkeit der Übertragung[54].

USB-Stick und Beiblatt übergeben [2.A39][55]

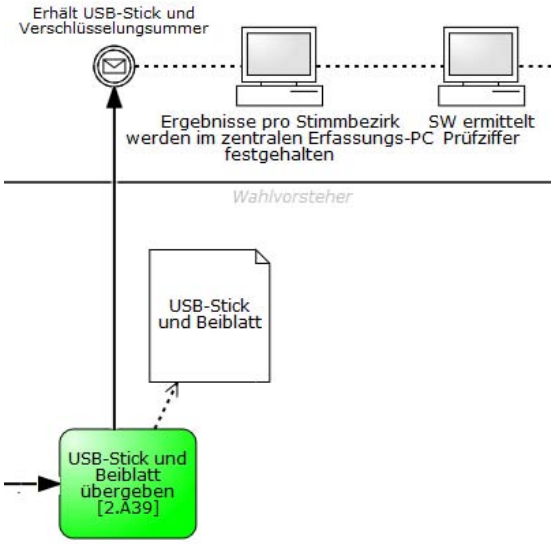

Abbildung 68: USB-Stick und Beiblatt übergeben

An der Aktivität „USB-Stick und Beiblatt übergeben [2.A39]“ ist der *Wahlvorsteher* beteiligt. Im Normalfall erhalten die *Wahlvorsteher* vom *Kommunalen Gebietsrechenzentrum (KGRZ)* überprüfte und mit einer ID versehene USB-Sticks, welche vom *Wahlvorstand* ausgeteilt werden. Die *Wahlvorsteher* benutzen diese, um die eingegebenen Ergebnisse der Stimmzettelauszählung für ihren Wahlbezirk zu speichern und eine neue Schlüsselnummer auf einem Beiblatt zu erzeugen. Nach der Datenübertragung von dem USB-Stick an den zentralen Erfassungs-PC wird der USB-Stick anschließend wieder entfernt.

[53] Anm. der Betreuer: Diese Sicherheitsanforderung wurde im vorangehenden Text nur implizit erwähnt. Beispielsweise ist es möglich, dass die Eingabe eines gesamten Stimmzettels nicht vorgenommen wird. Eine bereits eingesetzte Sicherheitsmaßnahme hier ist die Kontrolle der Eingabe durch eine zweite Person.
[54] Die Nachvollziehbarkeit wird über eine fortlaufend folgende Nummerierung hergestellt, die sowohl auf dem virtuellen als auch auf dem physischen Stimmzettel vorhanden is.t
[55] Anm. der Betreuer: Die hier beschriebene Aktivität wurde falsch verstanden

Verfolgt ein *Wahlvorsteher* böswillige Absichten, so könnte ein externer, mit einem Virus versehener USB-Stick an den organisatorischen Sicherheitskontrollen vorbei eingeschleust werden. Sobald der USB-Stick und das Beiblatt an den *Wahlvorstand* übergeben werden sollen, könnte sich der *Wahlvorsteher* zunächst in die „stille Ecke" begeben und den von der *KGRZ* ausgegebenen USB-Stick mit dem extern eingeschleusten USB-Stick vertauschen. Anschließend übergibt er den mit dem Virus versehenen USB-Stick zur zentralen Erfassung und lässt die Ergebnisse an den zentralen Erfassungs-PC übertragen. Bei diesem Vorgang wird der zentrale Erfassungs-PC gleichzeitig mit dem Virus infiziert. Anschließend begibt er sich erneut in die „stille Ecke" und tauscht den externen USB-Stick erneut mit dem von der *KGRZ* ausgegebenen USB-Stick aus, damit dieser einer eventuellen Überprüfung standhält. Wird dieses Angriffsszenario durchgeführt so könnte die Integrität, d. h. die Unveränderbarkeit der gespeicherten Daten verletzt werden.

Der IST-Zustand der Sicherheitsmaßnahmen ist so konzipiert, dass lediglich die vom *KGRZ* mit einer ID versehene und geprüfte USB-Sticks benutzt werden dürfen. Dies wird durch die Ausgabe dieser speziellen USB-Sticks sowie durch das Überprüfen der *Wahlhelfer* sichergestellt. Der SOLL-Zustand könnte so gestaltet werden, dass neben den technischen Sicherheitsmaßnahmen zu Beginn eine Durchsuchung der an der Wahl beteiligten Personen stattfindet. Alle an der Stimmauszählung beteiligten Personen müssten bei dieser Durchsuchung explizit auf mitgebrachte, unerlaubte Gegenstände untersucht werden. Des Weiteren sollte sichergestellt werden, dass sich in der Rhein-Mosel-Halle keine unbeobachtete „stille Ecke befindet, in welcher es möglich ist beispielsweise das Vertauschen eines USB-Sticks durchzuführen.

Dieses Angriffsszenario könnte zum einen die Integrität der Daten, die im Computersystem gespeichert sind, durch den Virus verletzen. Zum anderen wäre es möglich durch den Virus alle im zentralen Erfassungs-PC enthaltenen Daten zu löschen und somit die Datenverfügbarkeit nicht zu gewährleisten. Allerdings werden die vom *Wähler* abgegebenen Papierstimmzettel bei diesem Szenario nicht verändert. Aus diesem Grund würde diese Art der Wahlmanipulation lediglich zu einer erneuten, elektronischen Erfassung der Papierstimmzettel führen und somit die Bekanntgabe des offiziellen Wahlergebnisses verhindern.

Für den *Angreifer* wäre ein hoher organisatorischer Aufwand unabdingbar, da er einen USB-Stick, welcher den Originalen von der *KGRZ* nachempfunden ist, beschaffen und diesen mit einem entsprechenden Virus versehen müsste. Dieser organisatorische Aufwand ist nötig, um

bei einer nachträglichen Überprüfung der USB-Sticks nicht aufzufallen. Aus diesem Grund, sollten keine zusätzlichen und aufwendigen Sicherheitsmaßnahmen umgesetzt werden.

Für die Aktivität [2.A38] konnte eine Sicherheitsanforderung[56] identifiziert werden: Integrität der auf dem USB-Stick gespeicherten Daten.

Ergebnisse auf eklatante Abweichungen überprüfen [2.A44]

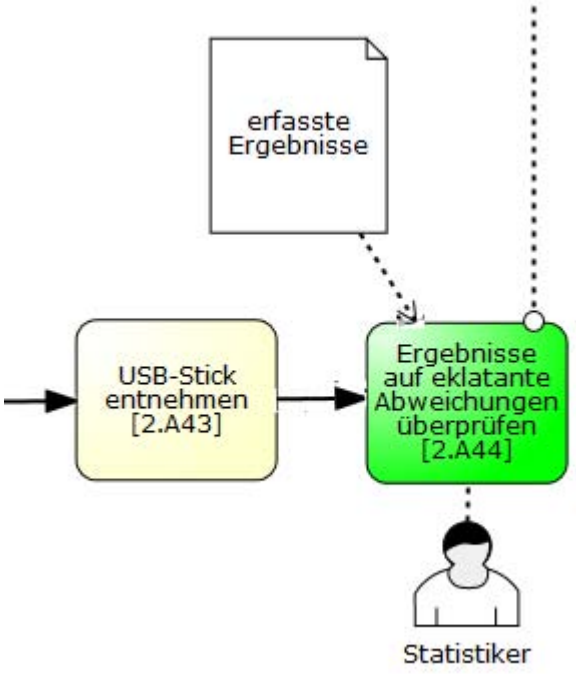

Abbildung 69: Ergebnisse auf eklatante Abweichungen überprüfen

Bei dieser Aktivität werden die Wahlergebnisse auf eklatante Abweichungen überprüft. Es wird überprüft, ob große Unterschiede im Wahlverhalten im Vergleich zu den Vorjahren bestehen. Falls ein Stimmbezirk mehrheitlich die Partei A gewählt hat, aber im aktuellen Wahlvorgang hingegen die Partei B die Stimmenmehrheit besitzt, ist dieser Umstand verdächtig und es liegt möglicherweise ein Versuch der Manipulation vor. Diese Ausnahmesituation könnte jedoch durch ein besonderes Ereignis begründet werden, z.B. wenn ein politischer Skandal offen gelegt würde. An dieser Aktivität ist der *Wahlvorstand* beteiligt und der *Statistiker*, der die Updates bekommt, wenn wieder Daten eines Stimmbezirks zentral erfasst werden. Als Input gelten die bei dem *Statistiker* eingegangenen Ergebnisse und als Output die

[56] Anm. der Betreuer: Ebenso sollte die Authentizität des übergebenen USB-Sticks gewährleistet werden. Die Umsetzung dieser Sicherheitsanforderung erfolgt über optische Gleichartigkeit und deutlich sichtbaren Identifikationsmerkmalen (die ausgegebenen USB-Sticks sind registriert).

erstellten Statistiken. Im Normalfall sollen gemäß der Kommunalwahlordnung §§ 51 und 52 die bei dem *Statistiker* eingegangenen Ergebnisse auf eklatante Abweichungen überprüft werden. Die böswillige Absicht wäre eine Manipulation der Ergebnisse. Des Weiteren könnte vermieden werden, dass der *Statistiker* die Abweichungen meldet. Ein möglicher Angriff, um das zu bewerkstelligen, wäre der man-in-the-middle (MITM), d.h. der *Statistiker* erhält Daten, die nicht auffallen. Diese müssten dem MITM bekannt sein (z. B. von den Ergebnissen der letzten Wahl aus der Wahl n-1 übernommene Daten). In der Realität besteht der Fall, dass der *Statistiker* die vorläufigen Ergebnisse im Internet für die Öffentlichkeit freigibt. Somit würde es auffallen, wenn am Vorabend Partei X mit „hoher Wahrscheinlichkeit" gewinnt und offiziell aber Partei Y genannt würde. Schließlich könnte die Wahl angefochten und wiederholt werden. Die Sicherheitsanforderung, die dadurch bedroht wäre, ist die Integrität der ermittelten Ergebnisse. Bei dem aktuellen Zustand (IST-Zustand) konnte identifiziert werden, dass eine Sicherheitsmaßnahme durch die Öffentlichkeit gewährleistet wird, indem diese die Abweichungen erkennen könnte. Um die Manipulationen zu vermeiden, sollen Sicherheitsmaßnahmen wie Signatur oder Message Authentication Code getroffen werden (SOLL-Zustand). Bei der letzten Maßnahme handelt es sich um ein Vorgehen, mit dessen Hilfe festgestellt werden kann, woher die Daten ursprünglich kommen (Authentizität der Daten) und ob die Sicherheitsanforderung Integrität nicht verletzt wurde. Die Sicherheitsmaßnahmen der nochmaligen Kontrolle der erfassten Ergebnisse sowie Zugriffskontrollen könnten zur Optimierung beitragen (SOLL-Zustand). Durch die Zugriffskontrollen könnte überwacht werden, wer Zugriff auf die Ergebnisse in dem früheren Verlauf des Prozesses hatte. Dadurch könnte die Integrität der Ergebnisse sichergestellt werden. Der MITM-Angriff ist sehr gefährlich, aber der Grundsatz der Öffentlichkeit (IST-Zustand) kann diese Situation bzw. ihre Folgen teilweise mildern, indem die Angriffe auf die Integrität der Ergebnisse auffallen und gemeldet würden, so dass die Wahl wahrscheinlich erneut durchgeführt werden müsste. Durch die vorhandene Sicherheitsmaßnahme ist die Eintrittswahrscheinlichkeit gering.

Für die Aktivität [2.A44] konnten zwei Sicherheitsanforderungen[57] identifiziert werden: Integrität und Verfügbarkeit der Ergebnisse.

[57] Anm. der Betreuer: Im vorangehenden Text wird eine Sicherheitsmaßnahme beschrieben, welche die hier angegebenen Sicherheitsanforderungen umsetzt. Die hier aufgeführten Sicherheitsanforderungen müssten demnach bei einer vorangehenden Aktivität identifiziert worden sein.

6.3.4. Wahlnachbereitung

Wahlunterlagen aufbewahren [3.A08]

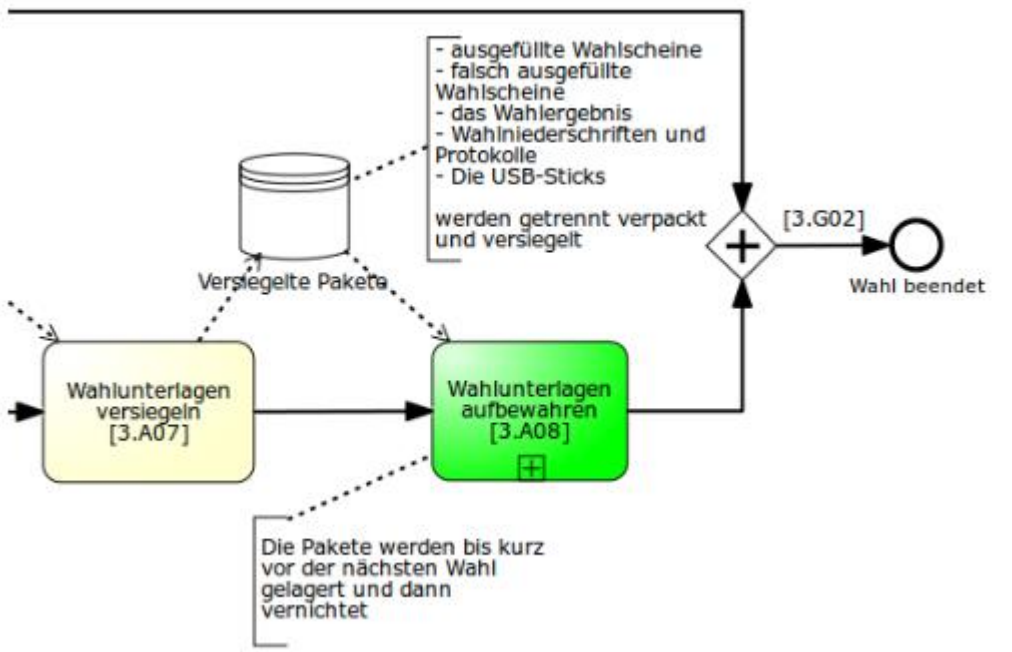

Abbildung 70: Wahlunterlagen aufbewahren

Die *Verwaltung* bewahrt die versiegelten Pakete bis circa vier Wochen vor der nächsten Wahl auf. Danach werden diese vernichtet. Die Pakete enthalten die sortierten Wahlunterlagen (korrekt ausgefüllte Wahlscheine, nicht korrekt ausgefüllte Wahlscheine, USB-Sticks, ...). Der Normalfall sieht vor, dass nach dem ordnungsgemäßen Verpacken und Versiegeln die Pakete wie in den Vorgaben beschrieben aufbewahrt werden. Weiter werden keine manipulierenden Handlungen vorgenommen und jede Interaktion mit den Paketen wird dokumentiert. Dazu zählen zum Beispiel das Öffnen der Pakete oder das Entnehmen der Wahlunterlagen. Ein möglicher Angriff kann z. B. durch die Zusammenarbeit von mindestens einem autorisierten Mitarbeiter der *Verwaltung* und einem *Bürger* durchgeführt werden. Der Mitarbeiter verschafft sich Zugang zu den Paketen, bricht die Versiegelungen auf, manipuliert die Wahlunterlagen und verpackt und versiegelt diese wieder, ohne diese Veränderungen zu dokumentieren. Wenn dieser Teil abgeschlossen ist, kann ein *Bürger* bei der Verwaltung einen Einspruch gegen das Wahlergebnis einlegen und bei einer erneuten Auszählung würde das veränderte Wahlergebnis festgestellt werden. Die Anzahl der Personen, die die einzelnen Teilaufgaben übernehmen, ist nach oben frei. Vor allem bei der ersten Teilaufgabe ist die Zusammenarbeit

mehrerer Personen von Vorteil. Dieser Angriff würde der Integrität des Wahlergebnisses schaden. Der IST-Zustand der Sicherheitsmaßnahmen ist so konzipiert, dass nur wenige autorisierte Personen Zugang zu den Räumlichkeiten, in welchen die Wahlunterlagen aufbewahrt werden, haben. Diese sind abgeschlossen. Weiter müssen sich immer mindestens zwei Personen gleichzeitig im Raum aufhalten, wodurch das Mehr-Augen-Prinzip gilt. Alle interagierenden Handlungen mit den Paketen und Unterlagen sind zu protokollieren. Es kann ebenfalls davon ausgegangen werden, dass die Siegel der Pakete regelmäßig kontrolliert werden. Der SOLL-Zustand kann so aussehen, dass vor allem in der Zeit nach den Wahlen auch nicht autorisierte Personen mit in die Räume dürfen, damit sie die Siegel überprüfen. Weiter ist es denkbar, dass *Landesbeamte* unangekündigt Prüfungen aus dem gleichen Grund durchführen. Eine nachträgliche Verfälschung des Wahlergebnisses wäre auf diesem Wege denkbar, doch ist der Aufwand immens. Das ursprüngliche Wahlergebnis darf nur knapp entschieden worden sein, da eine konsistente und glaubwürdige Manipulation mit zunehmender Anzahl der zu manipulierenden Stimmen schwieriger wird. Deshalb müssen hier viele Personen auf der Seite der *Verwaltung* zusammen arbeiten, die alle die gleichen politischen Ansichten teilen müssen. Weiter müssen sie die Möglichkeit haben die gebrochenen Siegel zu kopieren und erneut anzubringen, da ansonsten für Außenstehende klar erkennbar wäre, dass die Pakete geöffnet wurden.

Für die Aktivität [3.A08] konnten drei Sicherheitsanforderungen identifiziert werden: Integrität der Wahlunterlagen (sichergestellt durch das Siegel), Verfügbarkeit und Integrität der Wahlunterlagen.

Einspruch bewerten [3.A09]

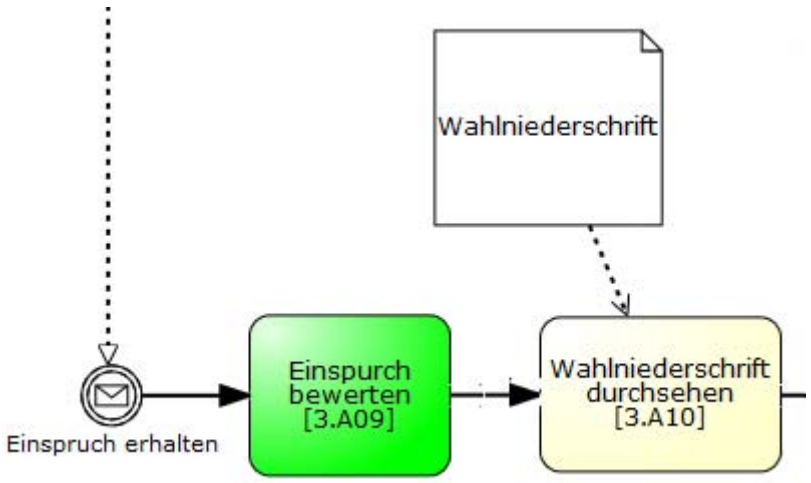

Abbildung 71: Einspruch bewerten

Bürger haben in den ersten zwei Wochen, nachdem das Wahlergebnis bekannt gegeben wurde, die Möglichkeit einen Einspruch einzureichen. Dieser Einspruch kann beim *Wahlleiter* oder bei der *Verwaltung* eingereicht werden, wobei letztere immer für die Bearbeitung verantwortlich ist (Siehe KWG §48). Im Normalfall wird der eingereichte Einspruch von der *Verwaltung* durchgesehen, kontrolliert und bewertet. Abschließend wird die Person, die diesen Einspruch eingereicht hatte, über das Ergebnis der Bearbeitung benachrichtigt. Dabei werden, je nach Art des Einspruches, alle notwendigen Schritte für eine korrekte Bewertung eingeleitet. In den meisten Fällen wird das Wahlverfahren kritisiert, wodurch die Wahlniederschrift kontrolliert wird. Bei gravierenderen Einsprüchen kann es auch soweit kommen, dass Personen befragt und die versiegelten Pakete geöffnet und die darin enthaltenen Unterlagen durchgearbeitet und nachvollzogen werden. Der hier beschriebene Angriff setzt eine Manipulation des Wahlergebnisses oder einen oder mehrere Fehler bei der Wahldurchführung voraus. Genauer handelt es sich hier um eine Vertuschung. Eine einzelne Person könnte einzelne Einsprüche abfangen. Allerdings spielt die Qualität des Einspruchs und die Anzahl der Vertreter eine wesentliche Rolle, sodass eine große Bandbreite an Szenarien entsteht. Einerseits kann ein einzelner *Wähler* einen nur durch Verdacht begründeten Einspruch einreichen, obwohl bei genauerer Untersuchung festgestellt werden würde, dass wirklich ein Fehler vorliegen würde. Andererseits könnte sich auch eine Gruppierung mit fundiertem Beweismaterial (bspw. Fotos und Kameraaufnahmen) melden. Beim ersten Szenario könnte der Einspruch vernichtet oder entsorgt werden und sofern sich die einzelne Person nicht mehr meldet, wären die Fehler erfolgreich vertuscht worden. Bei einer politisch engagierten Gruppe würde dieses Vorgehen wahrscheinlich nicht funktionieren, da diese auf Landesebene eine Beschwerde einlegen wür-

den und der Vertuschungsversuch bei weiterer Recherche eventuell auffliegen würde. Selbst wenn mehrere Personen auf der Seite der *Verwaltung* zusammen arbeiten würden, ließen sich auch hier Fehler gemäß dem zweiten Szenario nicht vertuschen. Allerdings könnten einzelne Einsprüche durch den Zusammenhalt mehrerer Mitarbeiter noch effektiver blockiert und daraus folgende Maßnahmen wie Neuwahlen oder Strafen umgangen werden, indem sie Fehler und Anschuldigungen einfach abstreiten. Diese Angriffe würden die Verfolgbarkeit dieser Aktivität angreifen. Diese Fälle werden teilweise durch die Sicherheitsmaßnahmen des IST-Zustands abgedeckt. Wie oben gezeigt, können fundierte Einsprüche nur sehr schwer oder gar nicht blockiert werden. Einzelne Einspruchsteller können sich zusätzlich durch das Mehr-Augen-Prinzip absichern, indem sie andere Personen als Zeugen hinzuziehen (bspw. als Augenzeuge bei einem Treffen im Ordnungsamt). Problematisch sind und bleiben die oben genannten Fälle, wenn gravierende Fehler zwar beobachtet wurden, diese aber nicht als solche erkannt wurden (siehe vorherigen Aktivitätsanalysen für Beispiele). Bleibt der Einspruchsteller hier nicht hartnäckig, so könnte im schlimmsten Fall eine Wahlmanipulation nicht aufgedeckt werden. Eine Überführung in einen verbesserten SOLL-Zustand ist hier fast unmöglich. Es ist lediglich denkbar, dass sich eine breite Wählerschaft im Vorfeld über den Wahlvorgang und die Wahlgesetze informiert und aufklärt und sich bei einem Verdacht auf Betrug oder Vertuschung zusammenschließt. Wie gezeigt wurde, könnte dir *Verwaltung* Fehler vertuschen und abstreiten. Auch hier gilt, dass mehrere Mitarbeiter die zusammenhalten diesen Plan besser umsetzen können als einzelne Mitarbeiter, die höchstens kleinere Einsprüche abfangen könnten. Der Aufwand der Vertuschung verhält sich linear mit dem Nutzen der Fehler und Manipulationsversuche. Allerdings sind die Möglichkeiten nach oben limitiert.

Für die Aktivität [3.A09] konnten zwei Sicherheitsanforderungen identifiziert werden: Verfügbarkeit[58] und Nachvollziehbarkeit des Einspruches.

6.4. Konsistenzprüfung

Im vorherigen Kapitel wurden anhand einer Aktivitäten-Analyse der BPMN-Diagramme Interessenkonflikte identifiziert. Dabei wurden unter anderem die verletzten Sicherheitsanforderungen sowie die bisher umgesetzten Sicherheitsmaßnahmen (IST-Zustand) und die noch umzusetzenden Sicherheitsmaßnahmen (SOLL-Zustand) für die Aktivität thematisiert. Bei der nachfolgend durchgeführten Konsistenzprüfung stehen die ermittelten Sicherheitsanforderun-

[58] „Verfügbarkeit“ bedeutet hier die Möglichkeit, Einspruch zu erheben

gen[59] der untersuchten Aktivität im Zentrum der Betrachtung, weshalb sie jeweils am Ende der Untersuchung nochmal zusammengefasst wurden. Die bei der Aktivität identifizierten Sicherheitsanforderungen können durch geeignete Sicherheitsmaßnahmen umgesetzt werden. Nun gilt es zu prüfen, ob die geforderten Sicherheitsanforderungen und -maßnahmen der Aktivitäten sich bei der Synthese auch nicht ausschließen. Eine Prüfung auf Widerspruchsfreiheit wird notwendig, da die Aktivitäten abhängig voneinander sind. Bei der Konsistenzprüfung werden die Sicherheitsanforderungen und -maßnahmen der Aktivität, bei der ein Interessenkonflikt zwischen den Akteuren besteht, mit denen der vorherigen und nachfolgenden Aktivität verglichen. Dabei wird untersucht, ob es zu Inkonsistenzen kommt, d.h. ob sich die identifizierten Sicherheitsanforderungen bzw. -maßnahmen gegenseitig ausschließen. Nachfolgend wird die gerade erläuterte Vorgehensweise der Konsistenzprüfung bei den zuvor identifizierten Interessenkonflikten angewandt.

6.4.1. Wahlvorbereitung

Wählerverzeichnis aufstellen [0.A14]

Bei der zu untersuchenden Aktivität handelt es sich um das **„Aufstellen des Wählerverzeichnisses [0.A14]“** mit der Sicherheitsanforderung[60] der Vertraulichkeit, da die Daten der Wähler nur von bestimmten Personen einsehbar und nicht öffentlich zugänglich sind. Die zu verbessernde Sicherheitsanforderung ist jedoch die Korrektheit. Als Lösungsansatz gilt hier ein „Mehr-Augen-Prinzip“. Hierbei haben mehrere Parteien der Gemeindevertretung und der Wahlleiter die Möglichkeit, das Wählerverzeichnis zu überprüfen.

Vor dieser Aktivität ist ein paralleles Gateway[61] [0.G03], sowie die Aktivität „Berufung der Beisitzer und deren Stellvertreter in den Wahlausschuss [0.A13]“. Im Gateway werden die Aufgaben in verschiedene Bereiche aufgeteilt, welche keinen direkten Einfluss auf die Aktivi-

[59] Anm. der Betreuer: Die in den vorangehenden Unterkapiteln hergeleiteten Sicherheitsanforderungen wurden von den Betreuern teilweise angepasst. Diese Anpassungen sind in den Fußnoten angemerkt und wurden für die nachfolgende Untersuchung übernommen.
[60] Relevante Sicherheitsanforderungen: Vertraulichkeit der personenbezogenen Daten, Verfügbarkeit des Dienstes, Integrität des Wählerverzeichnisses
[61] Anm. der Betreuer: Gateways sind Entscheidungspunkte, für die keine Sicherheitsanforderungen definiert werden.

tät [0.A14] haben. Auch die vorherige Aktivität „Berufung der Beisitzer und deren Stellvertreter in den Wahlausschuss“ beeinflusst nicht das Wählerverzeichnis.

Das Aufstellen des Wählerverzeichnisses hat des Weiteren die Aufgaben öffentlich bekanntzugeben, dass das Wählerverzeichnis aufgestellt wurde. Die Bekanntmachung erfolgt durch die Rhein-Zeitung- Dies zieht auch als Sicherheitsanforderung die Korrektheit des Wählerverzeichnisses nach sich. Des Weiteren ist die Verfügbarkeit zur Kontrolle des Verzeichnisses ein wichtiger Faktor dieser Aktivität, um jederzeit das Verzeichnis zu prüfen und dem Wähler die Möglichkeit zur Einsicht zu gewähren.

Die Sicherheitsanforderungen schließen sich diesbezüglich nicht gegenseitig aus und eine Umsetzung der Maßnahme ist möglich.

Abschließende Annahme des Wahlvorschlages überprüfen [0.A10]

Bei der zu untersuchenden Aktivität handelt sich um **„die abschließende Annahme des Wahlvorschlages durch den Wahlausschuss [0.A10]“**. Hierbei muss die Integrität als relevante Sicherheitsanforderungen gelten. Dies bedeutet, dass der Wahlvorschlag unversehrt ist und die Daten nur für bestimmte Personen einsehbar sind. Die rechtsgültigen Wahlvorschläge müssen angenommen werden, bzw. rechtsungültige Wahlvorschläge abgelehnt werden. Als Lösungsansatz gelten hier ein „Mehr-Augen-Prinzip“, sowie das Vorweisen von genügend Unterstützungsunterschriften. Durch Protokollierung des Verfahrens sollte jedem die Möglichkeit geboten werden, eine Kontrolle durchzuführen. Des Weiteren sollte der Landeswahlleiter bei Verdacht auf ein rechtswidriges Verfahren einschreiten können.

Die vorherige Aktivität ist die „Sitzung zur Entscheidung über Zulassung der erhaltenden Wahlvorschläge [0.A09]“, die jedoch keine Sicherheitsanforderung und Maßnahmen fordert.

Im Anschluss folgt ein Gateway [0.G04], welches überprüft, ob der Wahlvorschlag angenommen oder abgelehnt wird. Dies geht in die Aktivität [0.A11] über, dem Ablehnen des Wahlvorschlages. Die Sicherheitsanforderungen hier sind die Korrektheit der Daten, sowie der Integrität und Vertraulichkeit. Der Prozess endet nach dieser Aktivität. Die andere Aktivität, die aus dem Gateway [0.G04] herausgeht ist die „Annahme des Wahlvorschlages [0.A12]“. Die Sicherheitsanforderungen sind auch hier die Korrektheit der Daten, Integrität und Vertraulichkeit.

Die Maßnahme, um die Korrektheit der Daten festzustellen, ist durch verschiedene Parteien die Überprüfung zu beobachten und, falls notwendig, Einspruch einzulegen.

Zusammenfassend ist ein Zusammenspiel zwischen den Sicherheitsanforderungen und den Maßnahmen möglich.

Stimmzettel drucken [0.A17]

Die zu untersuchende Aktivität ist der **„Druck der Stimmzettel [0.A17]“**. Die Sicherheitsanforderungen sind hier die Integrität der Daten, sowie Verfügbarkeit der Daten. Dies bedeutet, dass die Daten auf dem Stimmzettel unversehrt sind und nicht ohne weiteres korrumpiert werden können, aber auch gleichzeitig verfügbar für die Druckerei und die Verwaltung. Um dies zu gewährleisten, sollte ein „Mehr-Augen-Prinzip“ verfolgt werden.

Die vorherige Aktivität ist die „zugelassenen Wahlvorschläge bekanntmachen [0.A16]“. Hier gilt die Sicherheitsanforderung der Integrität der Wahlvorschläge, die auch mit der Maßnahme des „Mehr-Augen-Prinzip“ durchgeführt wird.

Nach einem Gateway folgen zwei Aktivitäten. Die Aktivitäten sind den Wähler [0.A18] „über Wahlzeit, Wahlraum und Stimmabgabe informieren“, sowie [0.A19], „zur Sitzung zur Feststellung des Wahlergebnisses einladen“ haben keinen direkten Einfluss auf den Druck des Stimmzettels. Hier wird auch die Korrektheit der Daten, sowie die Verfügbarkeit der Daten als Sicherheitsanforderung vorausgesetzt.

Zwischen den Aktivitäten [0.A17] besteht keine Gefahr von Inkonsistenzen und ein Zusammenspiel der Sicherheitsanforderungen und Maßnahmen ist möglich.

6.4.2. Stimmabgabe

Briefwahlunterlagen beantragen

Bei der zu untersuchenden Aktivität handelt es sich um den aufgeklappten Unterprozess **„Briefwahlunterlagen beantragen“**. Die Verfügbarkeit der Briefwahlunterlagen wird als Sicherheitsanforderung umgesetzt. Gewährleistet wird diese durch die Beantragung der Briefwahlunterlagen auf mehreren Wegen. Der Wähler kann die Briefwahlunterlagen per Postantrag auf dem Wahlschein beantragen oder persönlich vor Ort bei der Verwaltung die Wahlunterlagen entgegennehmen. Außerdem kann der Wahlberechtigte die Briefwahlunterlagen formlos per Mail oder per Telefon beantragen sowie eine Vollmacht für eine Person ausstellen, der sich um die Abholung kümmert.

Vorab steht keine Aktivität, sodass keine Sicherheitsanforderungen bzw. Sicherheitsmaßnahmen bestehen.

Im Anschluss folgt das Zwischenereignis „Warten auf eintreffende Briefwahlanträge [1.Z01]“. Umgesetzt wird hierbei die Sicherheitsanforderung der Authentizität der eintreffenden Briefwahlanträge. Damit die Briefwahlanträge authentisch sind, wird ein Mehr-Augen-Prinzip bei der Annahme der Briefwahlanträge umgesetzt. Diese Sicherheitsmaßnahme gewährleistet, dass die Briefwahlanträge bei der Annahme nicht verändert werden.

Da die beschriebenen Sicherheitsanforderungen und die dazugehörigen Sicherheitsmaßnahmen sich nicht ausschließen, ist deren Zusammenspiel möglich.

Warten auf eintreffende Briefwahlanträge [1.Z01]

Bei dem zu untersuchenden Zwischenereignis handelt es sich um „**Warten auf eintreffende Briefwahlanträge [1.Z01]“**. Umgesetzt wird hierbei die Sicherheitsanforderung der Authentizität der eintreffenden Briefwahlanträge. Damit die Briefwahlanträge authentisch sind, wird ein Mehr-Augen-Prinzip bei der Annahme der Briefwahlanträge umgesetzt. Diese Sicherheitsmaßnahme gewährleistet, dass die Briefwahlanträge bei der Annahme nicht verändert werden.

Vorab steht die zu Anfang beschriebene Aktivität „Briefwahlunterlagen beantragen [1.A01]“. Die Verfügbarkeit der Antragstellung als Sicherheitsanforderung wird dabei durch die verschiedenen Wege der Beantragung sichergestellt.

Im Anschluss folgt die Aktivität „Wähler im Wählerverzeichnis als Briefwähler markieren [1.A05]“. Die Integrität des Briefwahlverzeichnisses sowie die Verfügbarkeit des Briefwahlverzeichnisses gelten als Sicherheitsanforderungen. Zusätzlich wird die Vertraulichkeit der personenbezogenen Daten gefordert. Die Integrität wird durch ein Mehr-Augen-Prinzip sichergestellt und das Wählerverzeichnis ist im Notfall auch offline verfügbar. Durch die Beschränkung der Gemeindemitarbeiter, die zuständig für das Eintragen der Wähler in das Briefwählerverzeichnis sind, sowie eine begrenzte Ansicht bei dessen Einsicht, gewährleisten die Vertraulichkeit der personenbezogenen Daten.

Da die beschriebenen Sicherheitsanforderungen und die dazugehörigen Sicherheitsmaßnahmen sich nicht ausschließen, ist deren Zusammenspiel möglich.

Wähler im Wählerverzeichnis als Briefwähler markieren [1.A05]

Bei der zu untersuchenden Aktivität handelt es sich um **„Wähler im Wählerverzeichnis als Briefwähler markieren [1.A05]“**. Hierbei gelten Integrität und Verfügbarkeit des Briefwahlverzeichnisses sowie Vertraulichkeit der personenbezogenen Daten als Sicherheitsanforderung[62]. Ein Mehr-Augen-Prinzip stellt die Integrität des Briefwahlverzeichnisses sicher. Durch die Begrenzung der zuständigen Mitarbeiter, sowie das Anzeigen eines Teilausschnittes bei der Einsicht des Wählerverzeichnisses, wird die Vertraulichkeit der personenbezogenen Daten gewährleistet. Damit das Wählerverzeichnis zu jeder Zeit aufrufbar ist, ist es auch offline verfügbar.

Vorab steht der aufgeklappte Unterprozess „Briefwahlunterlagen beantragen“. Die Verfügbarkeit der Antragstellung als Sicherheitsanforderung wird dabei durch die verschiedenen Möglichkeiten der Beantragung sichergestellt.

Im Anschluss folgt die Aktivität „Wahlunterlagen aushändigen [1.A06]“. Umgesetzt werden hierbei die Integrität der Briefwahlunterlagen sowie die Verfügbarkeit dieser. Durch ein Mehr-Augen-Prinzip als Sicherheitsmaßnahme wird die Integrität der Briefwahlunterlagen sichergestellt. Damit die Verfügbarkeit der Wahlunterlagen gewährleistet werden kann, werden Reservedrucke angefertigt und in der Verwaltung gelagert. Zusätzlich sollte die Sicherheitsanforderung der Anonymität der Wahlunterlagen umgesetzt werden, damit diese nicht auf einfachste Weise abgefangen werden können. Es muss also gewährleistet werden, dass die die Briefwahlunterlagen nicht gleich als solche erkannt werden können.

Da die beschriebenen Sicherheitsanforderungen und die dazugehörigen Sicherheitsmaßnahmen sich nicht ausschließen, ist deren Zusammenspiel möglich.

Wahlunterlagen aushändigen [1.A06]

Bei der zu untersuchenden Aktivität handelt es sich um „**Wahlunterlagen aushändigen [1.A06]“.** Umgesetzt werden hierbei die Sicherheitsanforderung der Integrität der Briefwahlunterlagen sowie – besonders relevant – die Verfügbarkeit dieser. Zusätzlich sollte die Sicherheitsanforderung der Anonymität der Wahlunterlagen umgesetzt werden, damit diese nicht auf einfachste Weise abgefangen werden können. Um die geltenden Sicherheitsanforde-

[62] Anm. der Betreuer: Relevante Sicherheitsanforderungen: Integrität des Briefwahlverzeichnisses, Verfügbarkeit der Wahl, Verfügbarkeit des Briefwahlverzeichnisses

rungen zu gewährleisten, wird bereits ein Mehr-Augen-Prinzip als Sicherheitsmaßnahme umgesetzt, welches die Integrität der Briefwahlunterlagen sowie eine korrekte Adressierung an den Briefwähler sicherstellen soll. Durch Reservedrucke der Briefwahlunterlagen wird die Verfügbarkeit dieser sichergestellt. Die Sicherheitsmaßnahmen können insofern erweitert werden, dass ein Erkennen der Briefwahlunterlagen nicht gleich ersichtlich ist und damit auch die Anonymität umgesetzt wird.

Im Voraus folgt die Aktivität „Wähler als Briefwähler im Wählerverzeichnis markieren[63] [1.A05]“. Hier wird die Integrität des Briefwahlverzeichnisses als Sicherheitsanforderung umgesetzt sowie die Verfügbarkeit des Briefwahlverzeichnisses. Zusätzlich wird die Vertraulichkeit der Daten gewährleistet. Ein Mehr-Augen-Prinzip stellt die Integrität des Briefwahlverzeichnisses sicher. Die Begrenzung der zuständigen Mitarbeiter sowie das Anzeigen eines Teilausschnittes bei der Einsicht des Wählerverzeichnisses gewährleisten die Vertraulichkeit der personenbezogenen Daten. Damit das Wählerverzeichnis zu jeder Zeit aufrufbar ist, ist es auch offline verfügbar.

Im Anschluss folgt der aufgeklappte Unterprozess „Briefwahlunterlagen ausfüllen“. Dabei muss die Anonymität der Stimmabgabe gewährleistet werden. Für die Sicherstellung dieser ist der Briefwähler selber verantwortlich. Bei der Stimmabgabe vor Ort in der Verwaltung wird die Anonymität der Stimmabgabe durch eine Wahlkabine gewährleistet. Diese ist in dem Raum so platziert, dass weder die Zuständigen der Verwaltung noch andere Briefwähler die Stimmabgabe des Wählers beobachten können.

Da die beschriebenen Sicherheitsanforderungen und die dazugehörigen Sicherheitsmaßnahmen sich nicht ausschließen, ist deren Zusammenspiel möglich.

Wahlbriefumschlag entgegennehmen [1.A15]

Bei der zu untersuchenden Aktivität handelt es sich um **„Wahlbriefumschlag entgegennehmen [1.A15]“**. Geltende Sicherheitsanforderungen sind zum einen Authentizität der Wahlbriefumschläge sowie die Verfügbarkeit der Wahlbriefumschläge für die Verwaltungsmitarbeiter. Ein Mehr-Augen-Prinzip stellt sicher, dass die eintreffenden Wahlbriefumschläge authentisch sind bis zum Einwurf in die Wahlurne. Da die Zustellung der Wahlbriefumschläge durch den Postboten nur während der regulären Arbeitszeiten der Mitarbeiter erfolgt, ist die

[63] Anm. der Betreuer: Der Vorgang des Markierens bezieht sich auf die Nichtabstreitbarkeit. Wird eine Briefwahl vorgenommen, dann kann die betreffende Person nicht mehr an der Präsenzwahl teilnehmen.

Verfügbarkeit der Verwaltungsmitarbeiter auf die Wahlbriefumschläge zuzugreifen auch gewährleistet.

Vorab steht die Aktivität „Wahlbriefumschlag in Briefkasten einwerfen [1.A14]. Geltende Sicherheitsanforderung ist die Authentizität des Briefkastens. Die Integrität des Briefkastens wird sichergestellt, indem lediglich Postboten den Inhalt des Briefkastens ausleeren können. Die Verfügbarkeit dessen wird durch die bloße Anwesenheit und der Angabe der Leerungszeiten sichergestellt.

Im Anschluss folgt keine Aktivität, sondern ein Endereignis, welches die erfolgreiche Entgegennahme der Wahlbriefumschlage darstellt. Somit gibt es keine Sicherheitsanforderungen bzw. Sicherheitsmaßnahmen, die umzusetzen sind.

Da die beschriebenen Sicherheitsanforderungen und die dazugehörigen Sicherheitsmaßnahmen sich nicht ausschließen, ist deren Zusammenspiel möglich.

Gefalteten Stimmzettel aushändigen [1.A23]

Bei der zu untersuchenden Aktivität handelt es sich um **„gefalteten Stimmzettel aushändigen [1.A23]“.** Umgesetzt werden hierbei die Sicherheitsanforderung der Authentizität (Integrität und Originalität) des Stimmzettels sowie die Verfügbarkeit des Stimmzettels. Um die geltenden Sicherheitsanforderungen zu gewährleisten, wird bereits ein Mehr-Augen-Prinzip als Sicherheitsmaßnahme verwendet sowie der Druck von Reservestimmzetteln. Die Sicherheitsmaßnahmen können insofern erweitert werden, indem die Korrektheit der Aushändigung eines Stimmzettels vereinfacht wird. Dies kann durch ein abwechselndes Stapeln der Stimmzettel (erst längs und dann quer) geschehen.

Bei der vorherigen Aktivität handelt es sich um das „Prüfen der Wahlberechtigung [1.A20]“. Umgesetzt wird hierbei die Korrektheit der Prüfung[64]. Die Verfügbarkeit der Prüfung wird durch die Anwesenheit des Wahlvorstandes während der gesamten Wahlzeit sichergestellt. Die Integrität der Prüfung wird durch ein Vier-Augen-Prinzip gewährleistet.

Im Anschluss folgt der aufgeklappte Unterprozess „Stimmabgabe“. Bei dieser Aktivität wird die Anonymität der Stimmabgabe als Sicherheitsanforderung sichergestellt. Die dazugehörige

[64] Anm. der Betreuer: Das ist so nicht richtig. Vielmehr handelt es sich bei dieser Aktivität um eine Sicherheitsmaßnahme, da ein Prüfvorgang stattfindet. Die hierfür relevanten Sicherheitsanforderungen sind in den vorangehenden Aktivitäten zu suchen.

Sicherheitsmaßnahme besteht in dem Aufstellen von Wahlkabinen im Wahllokal, in denen die Wähler ihre Stimmabgabe anonym abgeben. Die Wahlkabinen sind dabei so platziert, dass weder der Wahlvorstand noch anderer Wähler bzw. Beobachter die Stimmabgabe beobachten können.

Da die beschriebenen Sicherheitsanforderungen und die dazugehörigen Sicherheitsmaßnahmen sich nicht ausschließen[65], ist deren Zusammenspiel möglich.

Hilfsperson bestimmen [1.A24]

Bei der zu untersuchenden Aktivität handelt es sich um **„Hilfsperson bestimmen [1.A24]“.** Vertrauliches Agieren der Hilfsperson sowie die Verfügbarkeit der Hilfsperson sind Sicherheitsanforderungen die für diese Aktivität gelten. Durch die freie Wahl der Hilfsperson durch den Wähler, kann dieser eine Hilfsperson wählen, der er vertraut. Die Hilfsperson darf sich dem Wähler auch nicht aufdrängen. Die Verfügbarkeit einer Hilfsperson wird während des Wahltages gewährleistet, indem auch jederzeit ein Mitglied des Wahlvorstandes als Hilfsperson fungieren kann.

Vorab steht die Aktivität „gefalteten Stimmzettel aushändigen [1.A23]“. Umgesetzt werden hierbei die Sicherheitsanforderung der Integrität des Stimmzettels sowie die Verfügbarkeit des Stimmzettels. Um die geltenden Sicherheitsanforderungen zu gewährleisten, wird bereits ein Mehr-Augen-Prinzip als Sicherheitsmaßnahme verwendet sowie der Druck von Reservestimmzetteln. Die Sicherheitsmaßnahmen können insofern erweitert werden, indem die Korrektheit der Aushändigung eines Stimmzettels vereinfacht wird durch das Stapeln der Stimmzettel durch abwechselnd längs und quer legen.

Im Anschluss folgt die Aktivität „leere Wahlkabine aufsuchen [1.A25]“. Hier gelten Vertraulichkeit der Stimmabgabe in der Wahlkabine sowie die Verfügbarkeit dieser als Sicherheitsanforderungen. Umgesetzt wird die Vertraulichkeit der Stimmabgabe durch ein richtiges Platzieren der Wahlkabine, sodass weder der Wahlvorstand noch Außenstehende, beispielsweise durch ein Fenster, die Stimmabgabe beobachten könnte. Durch das Aufstellen mehrerer Wahlkabinen wird deren Verfügbarkeit sichergestellt.

[65] Auf den ersten Blick schließen sich hier die Anonymität und die Authentizität aus. Da sich die Sicherheitsanforderungen aber auf unterschiedliche Objekte (hier: Anonymität der Stimme und Authentizität des Wahlberechtigten) beziehen, ist der scheinbare Widerspruch aufgelöst.

Da die beschriebenen Sicherheitsanforderungen und die dazugehörigen Sicherheitsmaßnahmen sich nicht ausschließen, ist deren Zusammenspiel möglich.

Leere Wahlkabine aufsuchen [1.A25]

Bei der zu untersuchenden Aktivität handelt es sich um **„leere Wahlkabine aufsuchen [1.A25]“.** Die Wahlkabine soll dem Wähler eine vertrauliche Stimmabgabe gewährleisten. Zudem muss eine leere Wahlkabine für die Stimmabgabe verfügbar sein. Durch das richtige Platzieren der Wahlkabinen als Sicherheitsmaßnahme können weder der Wahlvorstand noch Außenstehende z.B. durch ein Fenster die Stimmabgabe des Wählers beobachten. Die Verfügbarkeit wird durch das Aufstellen mehrerer Wahlkabinen im Wahllokal zur Stimmabgabe sichergestellt.

Vorab steht die Aktivität „Hilfsperson bestimmen [1.A24]“. Vertraulichkeit gegenüber der Hilfsperson sowie deren Verfügbarkeit gelten als Sicherheitsanforderung. Die freie Wahl bei der Bestimmung der Hilfsperson stellt die Vertraulichkeit dieser sicher. Durch die Wahl von Wahlvorstandsmitgliedern als Hilfsperson ist die Verfügbarkeit während des Wahltages gewährleistet.

Im Anschluss folgt die Aktivität „Stimmzettel nach Vorgaben der KWO (§ 46) ausfüllen [1.A26]“. Die Vertraulichkeit der Stimmabgabe muss dabei sichergestellt werden. Die Wahlkabine als Sichtschutz sowie dessen richtige Platzierung sind Sicherheitsmaßnahmen, um die Vertraulichkeit der Stimmabgabe zu gewährleisten.

Da die beschriebenen Sicherheitsanforderungen und die dazugehörigen Sicherheitsmaßnahmen sich nicht ausschließen, ist deren Zusammenspiel möglich.

Stimmabgabe im Wählerverzeichnis vermerken [1.A41]

Bei der zu untersuchenden Aktivität handelt es sich um **„Stimmabgabe im Wählerverzeichnis vermerken [1.A41]“**. Als Sicherheitsanforderung für diese Aktivität gelten die Integrität des Wählerverzeichnisses sowie die Nichtabstreitbarkeit der Stimmabgabe durch den Wähler. Durch ein Mehr-Augen-Prinzip wird sichergestellt, dass der Stimmabgabenvermerk bei dem Wähler getätigt wird, der zuvor seine Stimme in die Wahlurne geworfen hat. Somit wird die Integrität des Wählerverzeichnis und die Verfügbarkeit jedes Wahlberechtigten an der Wahl

teilzunehmen, sichergestellt. Durch den Vermerk im Wählerverzeichnis kann der Wähler nicht abstreiten, dass er seine Stimme nicht abgegeben hat.

Bei der vorherigen Aktivität handelt es sich um „Stimmzettel wird von außen geprüft [1.A37]“. Die Anonymität des Stimmzettels muss dabei sichergestellt werden. Gewährleistet wird die Anonymität des Stimmzettels, indem die zwei Mitglieder des Wahlvorstandes den Stimmzettel nur von außen prüfen. Diese stellen sicher, dass der Stimmzettel keinerlei Markierungen aufweist, wie z.B. ein Eselsohr oder ein Kreuz in anderer Form, sodass keine Verbindung zwischen Wähler und Stimmzettel besteht.

Eine nachfolgende Aktivität gibt es nicht, da die Identitätsprüfung des Wählers sowie die Prüfung des Stimmzettels von außen beendet sind.

Da die beschriebenen Sicherheitsanforderungen und die dazugehörigen Sicherheitsmaßnahmen sich nicht ausschließen, ist ein Zusammenspiel dieser möglich.

Vorbereitungen der Urne für den Transport

Bei der zu untersuchenden Aktivität handelt es sich um den aufgeklappten Unterprozess **„Vorbereitungen der Urne für den Transport“**. Relevante Sicherheitsanforderungen sind die Integrität und Verfügbarkeit der Wahlurne, eine weitere Sicherheitsanforderung ist die Authentizität der enthaltenen Stimmen. Ein Mehr-Augen-Prinzip durch den Wahlvorstand sowie die unterschiedliche Parteizugehörigkeit dieser stellen die beiden Sicherheitsanforderungen sicher.

Vorab steht keine Aktivität, sondern ein Startzeitereignis, dass ab 18 Uhr mit den Vorbereitungen für den Urnentransport begonnen werden kann, wenn sich keine Wähler mehr im Wahllokal befinden. Somit gelten keine Sicherheitsanforderungen und somit auch keine Sicherheitsmaßnahmen.

Im Anschluss folgt keine Aktivität, sondern das Endereignis, welches die Beendigung der Vorbereitungen für den Urnentransport darstellt. Bis die Urnen abgeholt wird, muss die Integrität derer sichergestellt werden. Dies erfolgt durch ein Mehr-Augen-Prinzip der Wahlvorstandsmitglieder.

Da die beschriebenen Sicherheitsanforderungen und die dazugehörigen Sicherheitsmaßnahmen sich nicht ausschließen, ist ein Zusammenspiel dieser möglich.

Durch das angewandte Verfahren wurden externe Angriffe, die im BPMN-Diagramm nicht abgebildet wurden, nicht erfasst. Es wurde sich gegen eine Abbildung von externen Beteiligte entschieden, da diese die schon vorhandene Komplexität des Prozesses nur weiter erhöht hätte. Zudem konnte das Verfahren, lediglich benachbarte Aktivitäten zu betrachten, bestehende Inkonsistenzen bei der Stimmabgabe nicht aufdecken. Anhand eines Ausschnittes aus dem Überblick lässt sich verdeutlichen, dass sich ausschließende Sicherheitsanforderungen vorliegen.

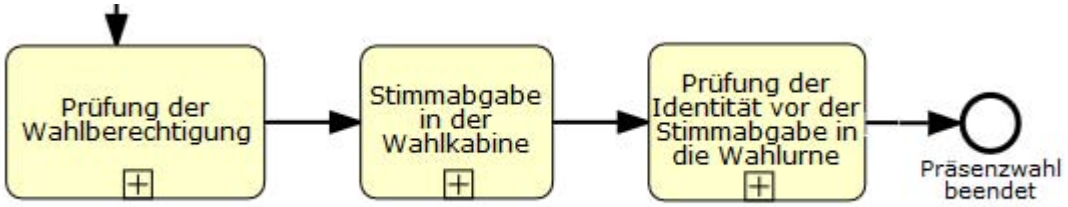

Abbildung 72: Sich ausschließende Sicherheitsanforderungen bei der Stimmabgabe

Zunächst muss sich der Wähler gegenüber dem Wahlvorstand authentifizieren. Dies geschieht mittels Wahlbenachrichtigung oder Personalausweis. Somit ist der Name des Wählers bekannt. Danach markiert der Wähler in der Wahlkabine den ausgehändigten Stimmzettel geheim. Die Stimmabgabe sollte nur dem Wähler bekannt sein und ist somit vertraulich. Bis zur Abgabe des Stimmzettels in die Wahlurne besteht allerdings eine Verbindung zwischen dem Wähler und seiner Stimmabgabe. Dies ist möglich, da Authentizität und Vertraulichkeit sich ausschließende Sicherheitsanforderungen sind. Diese Inkonsistenz ist bekannt und lässt sich auflösen, da sich die ausschließenden Sicherheitsanforderungen auf unterschiedliche Datenobjekte beziehen. Die Wähleridentität ist authentisch und der Stimmzettel anonym.

6.4.3. Stimmauszählung

Urne übernehmen [2.A12]

Bei der Aktivität, welche bei dem Vorgang Stimmauszählung als erstes auf ihre Konsistenz überprüft werden soll, handelt es sich um die Aktivität **„Urne übernehmen [2.A12]“.** Die Sicherheitsanforderung, welche hier gewährleistet werden soll, ist die Integrität der in der Urne enthaltenen Daten. Dadurch wird sichergestellt, dass die Daten bei der Übernahme der Urne von der *Verwaltung* nicht verändert werden. Deswegen wird ein Mehr-Augen-Prinzip umgesetzt. So sollten mehrere Vertreter der *Gemeindevertretung,* mit unterschiedlichen Par-

teizugehörigkeiten, die Urnen gemeinsam übernehmen und sicherstellen, dass ihnen die Urnen verschlossen übergeben werden.

Die vorherige Aktivität „Briefwahlumschläge ungesehen in die Wahlurne einwerfen [2.A11]“, bringt die Sicherheitsanforderung der Integrität mit sich, da die in den Briefwahlumschlägen befindlichen Daten unverändert weitergegeben werden müssen. Zudem muss die Verfügbarkeit der Daten sichergestellt werden. Weiterhin ist hier die Vertraulichkeit zu gewährleisten, da die in den Briefwahlumschlägen enthaltenen Dokumente eine Zuordnung zwischen Wähler und Stimme erlauben. Eine Maßnahme, die zu diesem Schutz eingesetzt wird, ist z. B. die physische – d.h. mittels verschiedener Umschläge – Trennung dieser Unterlagen.

Bei der nachfolgenden Aktivität handelt es sich um „Übernahmeprotokoll unterzeichnen [2.A13]“. Die dazugehörige Sicherheitsanforderung legt eine Nichtabstreitbarkeit der Urnenübernahme zu Transportzwecken fest. Damit kann bei einem Verlust der Wahlurnen zurückverfolgt werden, von wem diese übernommen wurden, um den Transport durchzuführen. Dadurch, dass die Sicherheitsmaßnahme des Mehr-Augen-Prinzip besteht, da das Protokoll von mindestens zwei Parteien unterzeichnet werden muss, könnte hier als zusätzliche Sicherheitsmaßnahme eine Überprüfung des Personalausweises stattfinden. Dies geschieht, um die Gewissheit zu erlangen, dass der Name auf dem Protokoll mit dem auf dem Personalausweis übereinstimmt. Allerdings ist anzunehmen, dass sich die Mitwirkenden am Wahlprozess bereits kennen und sich gegenseitig identifizieren können.

Da sich die Sicherheitsanforderungen der Nichtabstreitbarkeit und der Authentizität nicht gegenseitig ausschließen, ist eine Umsetzung beider Maßnahmen durchführbar.

Urne überwachen [2.A16]

Die zu untersuchende Aktivität **„Urne überwachen [2.A16]“** beinhaltet, die in der Rhein-Mosel-Halle gelagerten Urnen über Nacht zu bewachen und sicherzustellen damit diese zur Auszählung in ihrem abgelieferten Zustand vorgefunden werden. Die bereits bestehende Sicherheitsanforderung legt die Integrität der in den Urnen enthaltenen Daten fest. Sicherheitsanforderungen, welche diese Aktivität noch weiter verbessern sollen, sind die Korrektheit sowie die Verfügbarkeit der Daten. Um die bereits bestehende Sicherheitsanforderung zu gewährleisten, wird bereits ein *Sicherheitsdienst*, welcher die Urnen über Nacht bewacht eingesetzt. Um die Korrektheit der Überwachung sicherzustellen, sollten mehrere Sicherheitsbeamte von unterschiedlichen *Sicherheitsdiensten* eingesetzt werden, die sich gegenseitig kontrol-

lieren. Zudem wäre es denkbar, bei diesem Vorgang ebenfalls Mitglieder der *Verwaltung* zur Überwachung hinzuzuziehen.

Die vorherige Aktivität „Urne dem jeweiligem Stimmbezirk zuordnen [2.A15]“, bringt die Sicherheitsanforderung der Korrektheit sowie die Verfügbarkeit der in den Urnen enthaltenen Daten mit sich. Eine weitere Sicherheitsanforderung ist die Nichtabstreitbarkeit, da auf den Protokollen vermerkt wird, welche Urne welchem Stimmbezirk zugeordnet wurde. Hierbei wird von mehreren Mitgliedern der *Gemeindevertretung* unabhängig voneinander überprüft, ob die Urnen den jeweiligen Stimmbezirken korrekt zugeordnet wurden.

Im Anschluss an die Aktivität [2.A16] folgt ein Zwischenereignis, welches darauf hinweist, dass die Urnen bis zum Montag um 7Uhr überwacht werden. Da es sich um keine Aktivität handelt, gelten hier keine Sicherheitsanforderungen und keine Maßnahmen.

Da sich die Sicherheitsanforderungen nicht gegenseitig ausschließen, ist eine Umsetzung beider Maßnahmen durchführbar.

Ausdruck und Kontrolle, ob Daten auf Stimmzettel von Programm richtig erfasst wurden [2.A25]

Bei der zu untersuchenden Aktivität handelt es sich um: **„Ausdruck und Kontrolle ob Daten auf Stimmzettel von Programm richtig erfasst wurden [2.A25]“** bei der bereits folgende Sicherheitsanforderung gelten: Integrität der Stimmzettel.[66] Die Sicherheitsmaßnahme Acht-Augen-Prinzip wird bereits angewendet, in dem vier Personen überprüfen, ob die Daten auf den Stimmzetteln vom Programm tatsächlich richtig erfasst wurden. Somit wird die Integrität der Stimmzettel, sowie die Nichtabstreitbarkeit der richtigen Erfassung gewährleistet. Um die Ausfallsicherheit zu erhöhen, besteht die Möglichkeit redundante Systeme einzusetzen. In dem Fall, dass z.B. ein System ausfällt, werden die Aufgaben sofort von einem zweiten baugleichen System übernommen. Sie können ohne Unterbrechung weiterarbeiten und haben keine etwaigen Produktivitätsverluste. Tatsächlich besteht die Möglichkeit auf das *KGRZ*-Ersatz-Rechner zuzugreifen. Der aktuelle Zustand ist gut gegen den eventuellen Angriffen abgesichert, da bereits Kontrolle durch die angewendeten Sicherheitsmaßnahmen (Acht-Augen-Prinzip und Eingabe der Prüfziffer) und dadurch die zwei der drei vorhandenen Sicherheitsanforderungen gewährleistet wird. Wie schon erwähnt wurde, könnten redundante

[66] Anm. der Betreuer: Hier gibt es keine relevante Sicherheitsanforderung. Bei der hier beschriebenen Aktivität handelt es sich um eine Sicherheitsmaßnahme.

Systeme eingesetzt werden, um z.B. die Verfügbarkeit des Systems zu gewährleisten. Diese Maßnahme wird jedoch bereits durch den Einsatz der *KGRZ*-Ersatz-Rechner umgesetzt.

Bei der vorherigen Aktivität: „Fünf beliebige Stimmzettel ziehen und im Programm als Test erfassen [2.A24]“ gelten die Sicherheitsanforderungen Integrität und Verfügbarkeit der Stimmzettel. Die fünf beliebigen Stimmzettel werden aus einem Stapel ausgesucht und nachfolgend im Programm in einer Testversion erfasst. Dadurch soll sichergestellt werden, dass das Programm richtig funktioniert. Durch Integrität soll sichergestellt werden, dass die Daten auch richtig übertragen werden und nicht unbemerkt verändert werden. In diesem Fall wird auch das Acht-Augen-Prinzip als Sicherheitsmaßnahme angewendet, um somit sicherzustellen, dass niemand die anzugebenden Daten auf irgendwelche Art und Weise verändert. Die bestehende Sicherheitsmaßnahme ist ausreichend, um die Sicherheit zu gewährleisten.

Im Anschluss an die Aktivität [2.A25] folgt das Gateway [2.G05], bei dem überprüft wird, ob die erfassten Daten fehlerhaft übernommen wurden. Wenn es der Fall ist, soll die Aktivität [2.A24] wiederholt werden. In dem Fall, dass die erfassten Daten richtig übernommen wurden, sollen die Stimmzettel in den Stapel zurückgelegt werden und die erfassten Stimmzettel sollen nummeriert werden (Aktivität [2.A26]). Bei dieser Aktivität gilt die Integrität und Verfügbarkeit der Stimmzettel. Die bestehenden Sicherheitsmaßnahmen begrenzen sich auf Acht-Augen-Prinzip. Dieser Schritt kann um Protokollierung erweitert werden. Dadurch ist es möglich festzustellen, wie es zu Fehlern gekommen ist.

Da sich die Sicherheitsanforderungen nicht gegenseitig ausschließen, ist eine Umsetzung aller Maßnahmen durchführbar.

Vergebene Stimmen nacheinander 1:1 vorlesen, Stimmzettel nummerieren [2.A30]

Bei der zu untersuchenden Aktivität handelt es sich um **„vergebene Stimmen nacheinander 1:1 vorlesen, Stimmzettel nummerieren [2.A30]“**. Die Sicherheitsanforderung, die bei dieser Aktivität gilt, ist Integrität und Verfügbarkeit der Stimmzettel. Um die geltenden Sicherheitsanforderungen zu gewährleisten, wird, wie schon bei früheren Aktivitäten, die Sicherheitsmaßnahme Acht-Augen-Prinzip verwendet, d.h. vier Personen passen auf, dass die Aktivität richtig durchgeführt wird. Zusätzlich werden als Sicherheitsmaßnahme rote Stifte angewendet. Hierbei werden alle Vorgänge beim Auszählen mit einem roten Stift markiert. Damit wird vermieden, dass Stimmzettel manipuliert werden können. Dies würde auffallen, da die Farbe abweichen würde.

Bei der vorherigen Aktivität „Stimmzettel auffalten [2.A29]“ gelten bereits die Integrität und Verfügbarkeit der Stimmzettel. Bei den bestehenden Sicherheitsmaßnahmen handelt es sich wieder um das Acht-Augen-Prinzip. Zusätzlich könnte Protokollierung angewendet werden, wodurch der gesamten Prozess des Stimmzettel auffalten nachvollzogen werden könnte. Die zweite vorherige Aktivität ist „Stimmzettel aus Stapel nehmen [2.A28]“, bei der die Integrität und Verfügbarkeit der Stimmzettel als bereits geltende Sicherheitsmaßnahme identifiziert werden konnte. Das Acht-Augen-Prinzip wird bereits umgesetzt, um die Sicherheitsanforderungen zu gewährleisten. Es könnte auch an dieser Stelle um Protokollierung der aufgefalteten Stimmzettel erweitert werden. Dabei könnte festgehalten werden, zu welchem Zeitpunkt welcher Stimmzettel (jeder Stimmzettel ist mit Nummerierung versehen) durch wen aufgefaltet würde. So könnte festgehalten werden, wer möglicherweise die jeweiligen Stimmzettel verändert hat.

Im Anschluss an die Aktivität [2.A30] folgt die Aktivität „Stimmen erfassen [2.A31]“. Bei den bereits geltenden Sicherheitsanforderungen handelt es sich um Integrität der Stimmen. Um die geltenden Sicherheitsanforderungen zu gewährleisten wird bereits die Sicherheitsmaßnahme Acht-Augen-Prinzip und Nummerierung der Stimmzettel [2.A30] verwendet. Der SOLL-Zustand kann durch Message Authentication Codes oder Signaturen optimiert werden (Eckert 2013, S. 387 ff.).

Da sich die Sicherheitsanforderungen nicht gegenseitig ausschließen, ist eine Umsetzung aller Maßnahmen durchführbar.

Stimmen erfassen [2.A31]

Bei der zu untersuchenden Aktivität handelt es sich um: **„Stimmen erfassen [2.A31]“**. Bei den bereits geltenden Sicherheitsanforderungen handelt es sich um Integrität und Verfügbarkeit der Stimmen, sowie um die Nachvollziehbarkeit des Vorgangs. Um die geltenden Sicherheitsanforderungen zu gewährleisten wird bereits die Sicherheitsmaßnahme Acht-Augen-Prinzip und Nummerierung der Stimmzettel [2.A30] verwendet. Der SOLL-Zustand kann durch Message Authentication Codes oder Signaturen optimiert werden. Innerhalb der Aktivität [2.A30] besteht keine Gefahr von Inkonsistenzen. Folglich ist das Zusammenspiel von Sicherheitsanforderungen und Sicherheitsmaßnahmen möglich.

Bei der vorherigen Aktivität handelt es sich um „vergebene Stimmen nacheinander 1:1 vorlesen, Stimmzettel nummerieren [2.A30]“. Die Sicherheitsanforderung, die bei dieser Aktivität

gilt, ist Integrität und Verfügbarkeit der Stimmzettel sowie der vergebenen Stimmen. Um die geltenden Sicherheitsanforderungen zu gewährleisten, wird, wie schon bei früheren Aktivitäten, die Sicherheitsmaßnahme Acht-Augen-Prinzip verwendet. Zusätzlich werden als Sicherheitsmaßnahme rote Stifte angewendet. Hierbei werden alle Vorgänge beim Auszählen mit einem roten Stift markiert. Damit wird vermieden, dass Stimmzettel manipuliert werden können.

Im Anschluss an die Aktivität [2.A31] folgt die Aktivität „Nummerierung im System vermerken [2.A32]“ bei der die bereits geltende Sicherheitsanforderung Integrität der Nummerierung und Stimmzettel sowie Verfügbarkeit der Stimmzettel und des Systems ist. An der Stelle konnte wieder das Acht-Augen-Prinzip als bestehende Sicherheitsmaßnahme identifiziert werden. Dies kann um Protokollierung erweitert werden.

Da sich die Sicherheitsanforderungen nicht gegenseitig ausschließen, ist eine Umsetzung aller Maßnahmen durchführbar.

USB-Stick und Beiblatt übergeben [2.A39]

Die zu untersuchende Aktivität **„USB-Stick und Beiblatt übergeben [2.A39]“** beinhaltet, die Übergabe des USB-Sticks und des dazugehörigen Beiblatts, damit die Ergebnisse aller Stimmbezirke im zentralen Erfassungs-PC erfasst werden können. Bei der bereits bestehenden Sicherheitsanforderung handelt es sich um die Integrität der auf dem USB-Stick enthaltenen Daten. Dadurch soll sichergestellt werden, dass diese Daten nicht unbemerkt verändert wurden. Außerdem ist die verlässliche Herkunft des USB-Sticks (Originalität) zu fordern. Eine weitere geltende Sicherheitsanforderung ist die Verfügbarkeit des zentralen Erfassungs-PCs. Um die bereits bestehende Sicherheitsanforderung zu gewährleisten, wird ein Mehr-Augen-Prinzip während des ganzen Stimmauszählungsprozesses ausgeübt. Um dies noch weiter auszubauen sollten als erste zusätzliche Sicherheitsmaßnahme alle „stille Ecken“, die vor der Übergabe des USB-Sticks, aufgesucht werden könnten durch einen weiteren Überwachungsposten (z. B. in Form des Sicherheitsdienstes) eliminiert werden. Um die die Verfügbarkeit des zentralen Erfassungs-PCs sicherzustellen, sollte an einem Dummy-PC mit entsprechender Software überprüft werden, ob der abgegebene USB-Stick schädliche Malware enthält.

Die vorherige Aktivität „neue Schlüsselnummer sowie Notation auf Beiblatt erzeugen [2.A38]“, bringt die Sicherheitsanforderung der Datenkorrektheit und –verfügbarkeit mit sich.

Die nachfolgende Aktivität „Prüfziffer auf Protokoll eintragen [2.A40]“ richtet sich an den Wahlvorstand und bringt die Sicherheitsanforderung der Integrität sowie der Korrektheit mit sich. Dies ist damit zu begründen, dass der Vorstand zunächst die korrekte Prüfziffer auf dem Protokoll signieren muss. Des Weiteren muss diese Prüfziffer für eine eventuelle Überprüfung verfügbar sein. Hierbei sollte, durch eine Zugriffskontrolle sichergestellt werden, dass nur autorisierte Personen ein Zugriffsrecht auf die Protokolle besitzen.

Da sich die Sicherheitsanforderungen nicht gegenseitig ausschließen, ist eine Umsetzung aller Maßnahmen durchführbar.

Ergebnisse auf eklatante Abweichungen überprüfen [2.A44]

Bei der zu untersuchenden Aktivität handelt es sich um **„Ergebnisse auf eklatante Abweichungen überprüfen [2.A44]“**. Bei den bereits geltenden Sicherheitsanforderungen handelt es sich um Integrität der Ergebnisse.[67] Um die geltende Sicherheitsanforderung zu gewährleisten könnten die Sicherheitsmaßnahmen nochmalige Kontrolle und das Mehr-Augen-Prinzip eingesetzt werden. In der Realität gilt die Öffentlichkeit als eine Sicherheitsmaßnahme, d.h. falls Abweichungen auftreten sollten, würde das höchstwahrscheinlich von der Öffentlichkeit gemerkt und gemeldet. Der Öffentlichkeit stehen die Wahlstatistiken online zur Verfügung, wodurch hier die Abweichungen auffallen würden.

Die vorherige Aktivität ist „USB-Stick entnehmen [2.A43]“ bei der die bereits geltende Sicherheitsanforderung Integrität des USB-Sticks und somit der auf ihm gespeicherten Daten ist. Bei dieser Aktivität reicht diese Anforderung aus bzw. diese muss nicht weiterhin ergänzt werden. Es existiert bis jetzt keine Sicherheitsmaßnahme, die an dieser Stelle eingesetzt wird. Die Aktivität könnte um eine Sicherheitsmaßnahme „Mehr-Augen-Prinzip“ erweitert werden. Dadurch könnte sichergestellt werden, dass die Daten auf dem USB-Stick nicht nachträglich verändert werden.

Im Anschluss erfolgt die Aktivität „Bescheinigung über Einlesen erstellen [2.A45]“. An dieser Stelle gilt die Sicherheitsanforderung Integrität der Bescheinigung. Bis jetzt wird keine Sicherheitsmaßnahme angewendet. Dieser Zustand könnte z.B. durch „Mehr-Augen-Prinzip“ verändert werden.

[67] Anm. der Betreuer: Das ist keine relevante Sicherheitsanforderungen, da es sich bei dieser Aktivität um einen Prüfvorgang (= Sicherheitsmaßnahme) handelt.

Da sich die Sicherheitsanforderungen nicht gegenseitig ausschließen, ist eine Umsetzung aller Maßnahmen durchführbar.

6.4.4. Wahlnachbereitung

Wahlunterlagen aufbewahren [3.A08]

Bei der zu untersuchenden Aktivität handelt es sich um **„Wahlunterlagen aufbewahren [3.A08]“**, mit den Sicherheitsanforderungen Integrität, Vertraulichkeit, Verfügbarkeit und Nachvollziehbarkeit. Dabei haben nur wenige Personen Zutritt zu den Wahlunterlagen, die jede Interaktion dokumentieren müssen. Weiter müssen jederzeit mindestens zwei Personen in der Nähe der versiegelten Pakete sein, wodurch das Mehr-Augen-Prinzip gilt.

Bei der vorherigen Aktivität „Wahlunterlagen versiegeln [3.A07]“ gelten die Sicherheitsanforderungen Integrität, Vertraulichkeit und Verfolgbarkeit. Wurde diese Aktivität erfolgreich abgeschlossen, wurden alle Wahlprüfungsverfahren ebenfalls erfolgreich abgeschlossen. Eine Person der Verwaltung versiegelt unter Beobachtung anderer Personen die Pakete und dokumentiert diesen Vorgang.

Bei dem nachfolgenden Element handelt es sich um den Endzustand „Wahl beendet“, wodurch eine Konsistenzanalyse entfällt.

Die Sicherheitsanforderungen der untersuchten Aktivität stehen in keinem Widerspruch mit denen der vorangehenden und nachfolgenden Aktivitäten. Die Sicherheitsmaßnahmen sind dadurch umsetzbar.

Einspruch bewerten [3.A09]

Bei der zu untersuchenden Aktivität handelt es sich um **„Einspruch bewerten [3.A09]“**, mit den Sicherheitsanforderungen Verfügbarkeit und Verfolgbarkeit. Dabei sehen mehrere Mitarbeiter der Verwaltung den Einspruch durch und bewerten diesen. Die verschiedenen Arbeitsschritte für jeden Einspruch werden dokumentiert und der Einspruchsteller bekommt eine Rückmeldung über das Ergebnis. Durch die Bearbeitung mehrerer Personen gilt das Mehr-Augen-Prinzip.

Bei dem vorherigen Element handelt es sich um das eingehende Nachrichtenereignis „Einspruch erhalten“, wodurch eine Konsistenzanalyse entfällt.

Bei der nachfolgenden Aktivität „Wahlniederschrift durchsehen [3.A10]“ gelten die Sicherheitsanforderungen Integrität, Vertraulichkeit, Verfügbarkeit und Verfolgbarkeit. Dabei sehen mehrere Mitarbeiter der Verwaltung die Wahlniederschrift durch. Diese ist nur für entsprechend autorisierte Personen offen zugänglich. Auch diese Zugriffe werden dokumentiert. Alle Arbeitsschritte sind zusätzlich durch das Mehr-Augen-Prinzip gesichert.

Die Sicherheitsanforderungen der untersuchten Aktivität stehen in keinem Widerspruch mit denen der vorhergehenden und nachfolgenden Aktivitäten. Die Sicherheitsmaßnahmen sind dadurch umsetzbar.

7. Zwischenfazit

Dieser Abschnitt verfolgt das Ziel, ein Zwischenfazit nach der Bearbeitung des ersten Geschäftsprozesses abzuleiten. Hierbei sollen die Herangehensweise an die Aufgabenstellung kritisch betrachtet sowie Vor- und Nachteile aufgezeigt werden. Ziel ist es, die erarbeiteten Ergebnisse in die Untersuchung des zweiten Geschäftsprozesses einfließen zu lassen sowie die Vorgehensweise entsprechend zu verbessern und anzupassen.

Zu Beginn hat sich die anfängliche Anfertigung der Use-Cases als aufwendig und zeitintensiv erwiesen. Dies ist darauf zurückzuführen, dass zunächst einmal der Gesamtprozess in einzelne Unterprozesse unterteilt werden musste. Dies gestaltete sich als besonders schwierig, da der Gesamtprozess in der Anfangsphase noch nicht bis in alle Details bekannt war. Diese Tatsache birgt die zusätzliche Gefahr, dass fehlerhafte Annahmen in die Modellierung der Use-Cases miteinfließen. Des Weiteren war es aufwendig, die Use-Cases detailliert darzustellen und sich mit der gängigen Darstellungsweise vertraut zu machen. Kritisch anzumerken bleibt, dass die Use-Cases im weiteren Untersuchungsverlauf nicht mehr zum Einsatz kamen und somit das Aufwand-Nutzen-Verhältnis als negativ zu betrachten ist.

Nach der Erstellung der Use-Cases wurde als weiterführender Schritt der Referenzprozess für die Kommunalwahlen, der sich an den Wahlen in Zossen orientiert, modelliert. Diese Vorgehensweise hat sich als besonders geeignet herausgestellt, da erste Einblicke in die Prozessabläufe und der Beschluss eine Untergliederung in die vier Teilprozesse der Wahlvorbereitung, der Stimmabgabe, der Stimmauszählung und der Wahlnachbereitung vorgenommen werden konnten. Die Schablone der Use-Case-Beschreibungen war anschließend bei der Zerlegung der einzelnen Unterprozesse hilfreich, da es durch die Vorlage des Referenzprozesses leichter gelang, eine Vorstellung über die ablaufenden Aktivitäten in den Unterprozessen zu gewin-

nen. Somit basieren weitere Vorgehensschritte auf der Erstellung des Referenzprozesses, welcher damit ein positives Aufwand-Nutzen-Verhältnis aufweist. Zudem hat dieser erste Informationen zum Wahlprozess geliefert, welche sich ebenfalls als relevant für den bearbeiteten ersten Geschäftsprozess erwiesen wie beispielsweise die Abläufe der Briefwahl.

Die Erarbeitung der Interessenkonflikte wies zunächst positive sowie negative Aspekte auf. Durch die zuvor festgelegte Vorgehensweise war ein einfaches und strukturiertes Handeln bei der Erstellung der Interessenkonflikte möglich. Diese Tatsache hat ein einheitliches Vorgehen in der Gruppe sowie eine schnelle Ausarbeitung der Interessenkonflikte befördert. Als negativ hat sich bei der Bearbeitung der Interessenkonflikte herausgestellt, dass diese lediglich auf Einschätzungen der Forschungsgruppe beruhen. Dies ist darauf zurückzuführen, dass jede Aktivität von der Gruppe durchgegangen und auf Interessenkonflikte untersucht wurde. Hierbei wurden die Aktivitäten gewählt, welche für alle Gruppenmitglieder einen Interessenkonflikt aufwiesen. Allerdings war keine direkt am Wahlprozess beteiligte Person dabei. Hätte sich dieser Umstand als zutreffend erwiesen, wären bedingt durch die Mitwirkung am Prozess, andere Bewertungen von böswilligen Absichten sowie bestehenden Sicherheitsmaßnahmen erfolgt und somit andere Interessenkonflikte aufgezeigt worden.

Bei dem nachfolgenden Schritt der Konsistenzprüfung muss zudem kritisch angemerkt werden, dass mit der angewandten Vorgehensweise es sehr schwierig ist, alle bestehenden Inkonsistenzen aufzudecken. Dies ist auf den Umstand zurückzuführen, dass lediglich die vorgelagerte und die nachfolgende Aktivität auf Inkonsistenzen untersucht wurden und demzufolge auch Inkonsistenzen unentdeckt bleiben. Bei dem Wahlprozess führte das zu dem Ergebnis, dass es bei der Betrachtung der umliegenden Aktivitäten zu keinen auftretenden Inkonsistenzen kam. Wurden allerdings mehr Aktivitäten als die vorhergehenden und die nachfolgende Aktivität betrachtet, führte dies zu nicht aufgedeckten Inkonsistenzen wie beispielsweise bei der Stimmabgabe. Hier wurde festgestellt, dass eine Inkonsistenz zwischen der Vertraulichkeit und der Authentizität besteht solange der Wähler seine Stimme noch nicht in die Wahlurne eingeworfen hat. Bis zum Einwurf des Stimmzettels in die Wahlurne kann dem Wähler seine abgegebene Stimme zugeordnet werden. Aus diesem Grund wurde beschlossen, beim zweiten Geschäftsprozess ein anderes Verfahren anzuwenden, mit dem Ziel alle bestehenden Inkonsistenzen aufzudecken.

8. Prozess 2: Geld abheben am Automaten

8.1. Überblick über den Prozess verschaffen

Der zweite Prozess behandelt das Geldabheben an einem Sparkassen-Geldautomaten. Als Standort wurde exemplarisch der Geldautomat an der Universität Koblenz ausgewählt, an dem der Prozess praktisch nachvollzogen wurde. Hierbei wurden Informationen von der Sparkasse Koblenz eingeholt, indem ein Fragenkatalog erstellt wurde, der von Verantwortlichen der Sparkasse beantwortet wurde. Des Weiteren wurde am Sparkassen Automat einmal Geld von der Forschungsgruppe abgehoben, sodass die einzelnen Prozessschritte nachvollzogen werden konnten. Auf dieser Grundlage wurde im Folgenden ein Prozess mit BPMN erstellt und dieser nach dem PrOSA-Vorgehensmodell untersucht. Das Vorgehen baut auf den Erfahrungswerten des ersten Prozesses Kommunalwahlen in Koblenz auf. Als erster Schritt wurden Use-Cases und ein BPMN-Referenzmodell erstellt, bevor der Prozess detailliert ausmodelliert wurde. Auf dessen Grundlage wurden Interessenkonflikte innerhalb des Modells untersucht und eine Konsistenzanalyse durchgeführt. Jedoch wurde anhand der Ergebnisse aus Prozess eins eine andere Vorgehensweise für die Ermittlung der Interessenkonflikte sowie die Konsistenzprüfung gewählt und neue Evaluierungsmöglichkeiten entwickelt. Bei diesem Prozess werden Interessenkonflikte in einer Matrix dargestellt, um eine bessere Übersichtlichkeit zu erzielen sowie alle bestehenden Interessenkonflikte zu identifizieren[68].

8.1.1. Referenzprozess in BPMN

Auch für den zweiten Prozess „Geld abheben am Automaten“ wurde ein Referenzprozess erstellt. Hier wurde ein Fokus auf die Aktivitäten innerhalb des Prozesses gelegt, ohne die dementsprechende Rollenverteilung zu den Aktivitäten zuzuordnen. Aus diesem Grund wurden die Rollen *Kunde und Bank* innerhalb einer Lane modelliert. Der Referenzprozess ist noch nicht auf einen spezifischen Geldautomaten angepasst, sondern wurde allgemein gehalten in der Annahme, dass er so auf jeden beliebigen Geldautomaten angewendet werden kann. Ein Prozess startet mit einem Ereignis – hier das Bedürfnis nach Bargeld. Das Startereignis ist die Motivation des Kunden, Bargeld vom Geldautomaten abzuheben. Hierbei bestehen die

[68] Anm. der Betreuer: Mit diesem Vorgehen wurde versucht, die Interessenkonflikte möglichst vollständig zu erfassen. Es wurde festgestellt, dass das Vorgehen im ersten Prozess noch nicht systematisch genug gewesen ist und mehr einem Brainstorming entsprochen hat.

ersten Schritte darin, dass ein Geldautomat aufgesucht wird. In Abbildung 73 wird das Startereignis des Prozesses Geldabheben aufgezeigt.

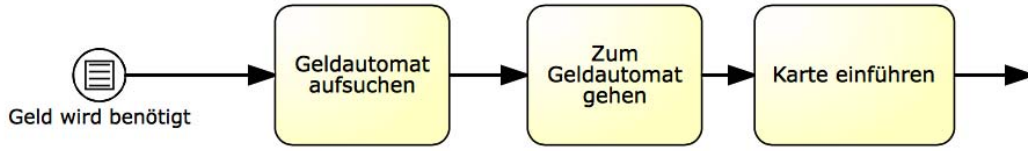

Abbildung 73: Startereignis

Diese Schritte sind von physischer Natur und haben noch keinen Einfluss auf die Aktionen am Geldautomaten selbst. Erst mit der Aktivität Karte in den Geldautomaten einfügen, wird der Automat genutzt, d.h. erst mit dem Einführen der EC-Karte findet eine Interaktion mit dem Automaten statt. Darauf folgend wird vom Kunden die Karte eingeführt, die Aktivität Auszahlen gewählt und die PIN eingegeben (siehe Abbildung 74). Jedoch werden im Referenzprozess diese Aktivitäten nicht klar zugeordnet, da keine Rollenverteilung stattfindet.

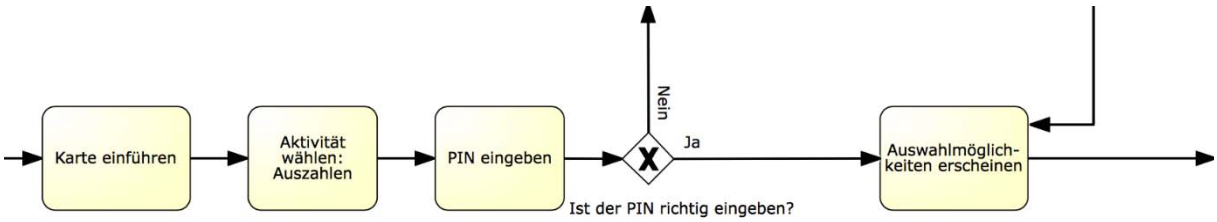

Abbildung 74: Physische Aktivitäten

Wurde die PIN dreimal hintereinander falsch eingegeben, wird die Karte einbehalten, gesperrt und der Prozess an dieser Stelle beendet (siehe Abbildung 75).

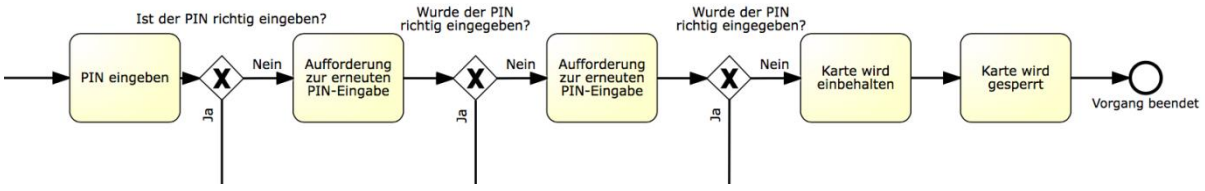

Abbildung 75: PIN-Eingabe

Wurden alle Schritte richtig befolgt und es gab keinen Abbruch innerhalb des Prozesses, kann nun der gewünschte Geldbetrag ausgewählt werden. Hier hat der Kunde generell zwei Möglichkeiten. Er kann entweder einen vorgegeben Betrag auswählen oder einen Betrag manuell eingegeben (siehe Abbildung 76).

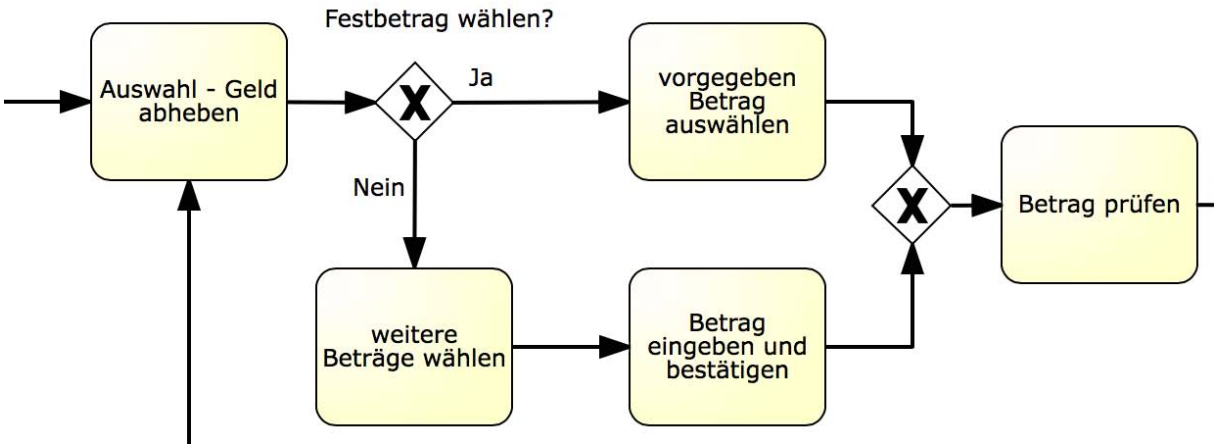

Abbildung 76: Geldbetrag auswählen

Ein weiterer wichtiger Schritt im Referenzprozess ist die Nachricht über den Verfügungsrahmen. Wurde ein Betrag gewählt, der unter dem verfügbaren Betrag des Kunden liegt, so kann das Geld nicht ausgezahlt werden und der Kunde hat die Möglichkeit den Vorgang abzubrechen oder wieder an den Anfang des Prozesses zu gehen und so einen neuen Geldbetrag auszuwählen (siehe Abbildung 77). Generell ist festzustellen, dass innerhalb des Referenzprozesses viele Abbruchmöglichkeiten bestehen.

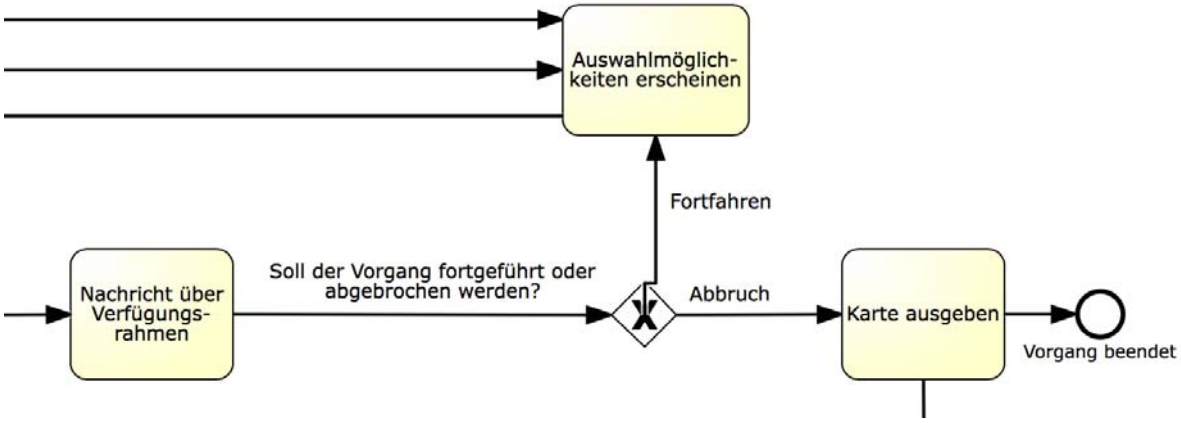

Abbildung 77: Abbruch beim Überschreiten des Verfügungsrahmens

Abbrüche des Prozesses können durch den Geldautomaten entstehen oder aber auch durch den Kunden initiiert werden. Der Abbruch des Prozesses wird im Referenzprozess als „Vor-

gang beendet“ bezeichnet und hat keine nähere Beschreibung. Wurde der Vorgang nicht vorher unterbrochen, erfolgt im letzten Schritt die Ausgabe der Karte.

Auch hier ist ein Abbruch des Prozesses möglich, wenn nach einem Timeout die Karte vom Kunden nicht entgegengenommen wurde. Die Folge ist, dass die Karte wieder vom Geldautomaten eingezogen sowie der Vorgang unterbrochen wird. Dadurch erfolgt keine Geldausgabe. Erst nach der Entgegennahme der Karte wird der gewünschte Betrag ausgegeben. Auch hier erfolgt wieder ein Timeout. Wird das Geld nicht innerhalb einer gewissen Zeitspanne entnommen, wird der Betrag wieder eingezogen und der Vorgang wird dementsprechend beendet. Im Referenzprozess wird der Betrag erst nach der Entnahme des Geldes aus dem Automaten vom Konto abgebucht und der Vorgang beendet (siehe Abbildung 78).

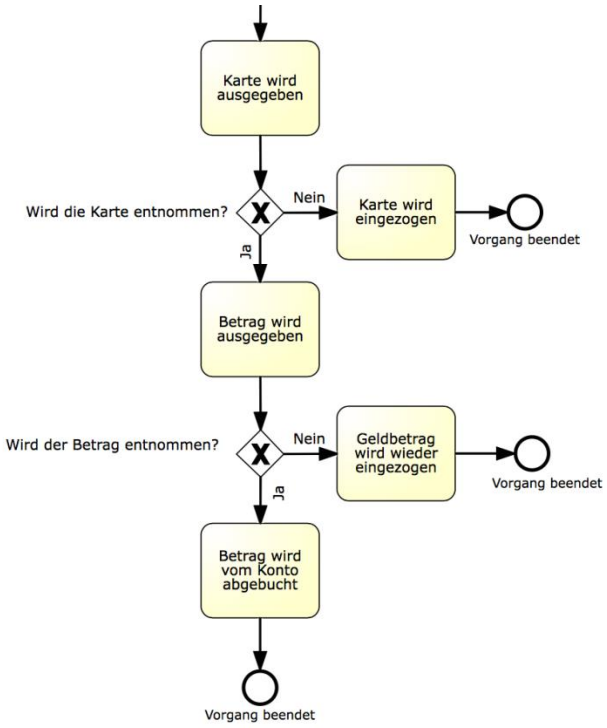

Abbildung 78: Ende des Prozesses

Im Allgemeinen fehlen im Referenzprozess Rollenverteilungen, sowie weitere Informationen zu den verschiedenen Abbrüchen der Vorgänge. Ferner können noch Ungenauigkeiten beim Modellieren des Referenzprozesses gefunden werden. Jedoch dient hier der Prozess als Vorlage für den eigentlichen Prozess und die wichtigsten Aktivitäten können nun ausgebaut und auf das spezifische Szenario (EC-Kartenautomat des Campus-Sparkassenhäuschens) angewendet werden. Auch die Rollenverteilung spielt erst im späteren Modell eine wichtige Rolle. Dadurch können Schwachstellen innerhalb des Prozesses identifiziert werden.

Prozess 2: Geld abheben am Automaten

8.1.2. Use-Cases und Beschreibungen

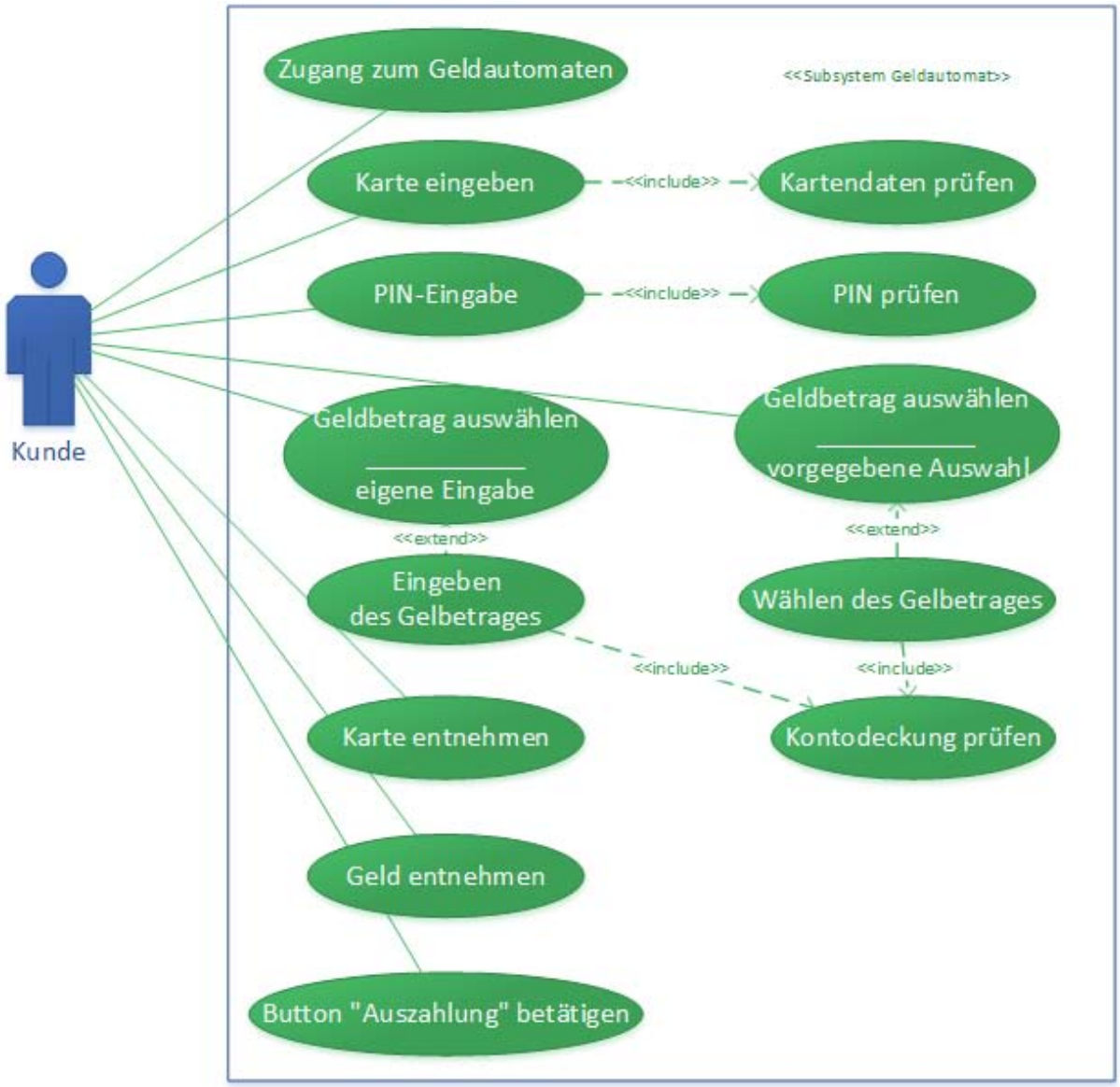

Abbildung 79: Use-Case zum Prozess Geld abheben

Wie oben erwähnt wurde und hier auf Abbildung 79 zu sehen ist, wurden alle Use-Cases in einem Diagramm abgebildet. Weiter wurde zum Wohle der Überschaubarkeit vom Best-Case Szenario ausgegangen (die Karte ist weder fehlerhaft noch abgelaufen, die PIN wurde richtig eingegeben, das Konto ist gedeckt etc.). Diese Fälle werden in Kapitel 8.2 in BPMN abgebildet und beschrieben.

Der Prozess beginnt damit, dass sich der Kunde Zutritt zum Geldautomaten verschafft (Tabelle 30) und die Karte in den Geldautomaten eingibt (Tabelle 31), worauf dieser die Karte überprüft (Tabelle 32). Wenn die Karte vom Automaten als korrekt angenommen wird, wird der Kunde gefragt, wie er den Automat nutzen möchte. Unter den aufgelisteten Optionen wählt

er, dass er eine Auszahlung vornehmen möchte (Tabelle 33). Danach wird er aufgefordert seine PIN einzugeben (Tabelle 34) und der Automat überprüft diese (Tabelle 35). War auch diese Eingabe korrekt, hat der Kunde die Möglichkeit auszuwählen, ob er den Betrag selbst eingeben möchte (Tabelle 36) oder einen vorgegebenen Betrag wählt (Tabelle 37). Entsprechend der Auswahl muss er dann den Betrag eingeben (Tabelle 41) oder nur wählen (Tabelle 42). In beiden Fällen überprüft der Automat, ob das Konto entsprechend der Auswahl gedeckt ist (Tabelle 38). Danach nimmt der Kunde zuerst seine Karte (Tabelle 39) und danach das Geld (Tabelle 40) entgegen.

Name	**Zugang zum Geldautomaten**
Akteure	Kunde, Geldautomat
Ziel	Der Kunde soll den Geldautomaten nutzen können.
Auslösendes Ereignis	Der Kunde benötigt Geld.
Kurzbeschreibung	Der Kunde kann den Geldautomaten nutzen, sofern er nicht von jemand anderem in Nutzung ist.
Vorbedingung	Der Kunde befindet sich in der Nähe eines Geldautomaten.
Essenzielle Schritte	1. Überprüfen, ob ein anderer Kunde den Geldautomaten schon benutzt. 2. Wenn ja: Im Abstand hinter dem Kunden warten bis dieser den Automaten verlässt. 1. Wenn nein: Der Geldautomat kann genutzt werden.
Ausnahmefälle	z.B. keine Zugänglichkeit (verschlossener Raum)
Nachbedingung	-

Tabelle 30: Use-Case „Zugang zum Geldautomaten“

Name	**Karte eingeben**
Akteure	Kunde, Geldautomat
Ziel	Die Karte soll in den Geldautomaten eingegeben werden.

Prozess 2: Geld abheben am Automaten

Auslösendes Ereignis	Der Automat benötigt die Karte des Kunden, um ihm vom seinen Konto Geld auszuzahlen.
Kurzbeschreibung	Der Kunde fügt seine Karte in den Kartenschlitz des Geldautomaten ein.
Vorbedingung	Der Automat war frei, sodass der Kunde diesen benutzen kann.
Essenzielle Schritte	1. Die Karte wird für den Automaten lesbar in den Kartenschlitz eigeführt.
Ausnahmefälle	-
Nachbedingung	-

Tabelle 31: Use-Case „Karte eingeben“

Name	**Kartendaten prüfen**
Akteure	Geldautomat
Ziel	Die Kartendaten sollen geprüft werden.
Auslösendes Ereignis	Die Karte befindet sich im Geldautomaten.
Kurzbeschreibung	Der Geldautomat prüft anhand des Chips auf der Karte die Daten des Kunden.
Vorbedingung	Die Karte wurde vom Kunden richtig in den Geldautomaten eingeführt.
Essenzielle Schritte	1. Der Chip wird überprüft 2. Magnetstreifen prüfen
Ausnahmefälle	Fälle, die sich auf nicht erfolglose Prüfung beziehen (z. B. Chip defekt, falsche Karte, etc.).
Nachbedingung	-

Tabelle 32: Use-Case „Kartendaten prüfen“

Name	**Button „Auszahlung“ betätigen**

Prozess 2: Geld abheben am Automaten

Akteure	Kunde, Geldautomat
Ziel	Der Kunde soll Geld abheben können.
Auslösendes Ereignis	Der Geldautomat zeigt die unterschiedlichen Aktionsmöglichkeiten an.
Kurzbeschreibung	Der Kunde wählt den Button „Auszahlung“, um Geld abzuheben.
Vorbedingung	Die Überprüfung der Kartendaten war erfolgreich.
Essenzielle Schritte	1. Der Button „Auszahlung“ wird betätigt.
Ausnahmefälle	-
Nachbedingung	-

Tabelle 33: Use-Case „Button „Auszahlung“ bestätigen“

Name	**PIN-Eingabe**
Akteure	Kunde, Geldautomat
Ziel	Der Kunde soll seinen PIN eingeben, um Geld abheben zu können.
Auslösendes Ereignis	Der Automat fragt den Kunden nach der zu seiner Karte gehörigen PIN.
Kurzbeschreibung	Der Kunde gibt seinen für die Karte zugehörigen PIN ein.
Vorbedingung	Der Menüpunkt „Auszahlung“ wurde vom Kunden gewählt.
Essenzielle Schritte	1. PIN-Eingabe zur zugehörigen Karte 2. PIN –Bestätigung
Ausnahmefälle	-
Nachbedingung	-

Tabelle 34: Use-Case „PIN-Eingabe“

Name	**PIN prüfen**
Akteure	Geldautomat

Prozess 2: Geld abheben am Automaten

Ziel	Der PIN soll validiert werden.
Auslösendes Ereignis	PIN-Eingabe des Kunden
Kurzbeschreibung	Der Geldautomat validiert die PIN-Eingabe des Kunden.
Vorbedingung	Die PIN wurde vom Kunden eingegeben.
Essenzielle Schritte	1. Der eingegebene PIN wird mit der auf dem Chip der Karte gespeicherten PIN überprüft. 2. Bei positiver Überprüfung kann der Kunde mit dem Geld-abhebe-Prozess fortfahren
Ausnahmefälle	Stimmt der PIN nicht überein, wird der Kunde erneut aufgefordert seinen PIN einzugeben. Wurde der PIN dreimal falsch eingegeben, so zieht der Geldautomat die Karte ein und der Kunde muss durch diese durch persönliches Erscheinen in der Bank abholen.
Nachbedingung	-

Tabelle 35: Use-Case „PIN prüfen“

Name	**Geldbetrag auswählen – eigene Eingabe**
Akteure	Kunde, Geldautomat
Ziel	Eingabe eines beliebigen Geldbetrages
Auslösendes Ereignis	Anzeige des Eingabefeldes durch den Automaten
Kurzbeschreibung	Der Kunde gibt einen von ihm frei gewählten Betrag, den er ausgezahlt haben möchte, in das Eingabefeld ein.
Vorbedingung	Die PIN-Eingabe des Kunden wurde als gültig validiert.
Essenzielle Schritte	1. Der Kunde gibt seinen Wunschbetrag in das Eingabefeld ein. 2. Der Automat überprüft, ob der Betrag durch 5 teilbar ist, denn nur dann kann er auch vom Automaten ausgezahlten werden.
Ausnahmefälle	-
Nachbedingung	-

Tabelle 36: Use-Case „Geldbetrag auswählen – eigene Eingabe“

Prozess 2: Geld abheben am Automaten

Name	**Geldbetrag auswählen – vorgegebene Auswahl**
Akteure	Kunde, Geldautomat
Ziel	Ein Festbetrag soll ausgewählt werden.
Auslösendes Ereignis	Anzeige der Festbeträge durch den Automaten
Kurzbeschreibung	Der Kunde wählt einen der vom Automaten vorgegebenen Festbeträge aus, die er erhalten möchte.
Vorbedingung	Die PIN-Eingabe des Kunden wurde als gültig validiert.
Essenzielle Schritte	1. Der Kunde gibt wählt einen der vorgegebenen Festbeträge aus.
Ausnahmefälle	-
Nachbedingung	-

Tabelle 37: Use-Case „Geldbetrag auswählen – vorgegebene Auswahl“

Name	**Kontodeckung prüfen**
Akteure	Geldautomat
Ziel	Die Kontodeckung soll überprüft werden.
Auslösendes Ereignis	Ein vom Kunde gewählter Geldbetrag
Kurzbeschreibung	Der Automat überprüft, ob auf dem Konto des Kunden der von ihm eingegebene Geldbetrag vorhanden ist und auch keine Beschränkung für diesen Betrag vorliegt.
Vorbedingung	Der Kunde hat den auszuzahlenden Geldbetrag eingegeben und geprüft.
Essenzielle Schritte	1. Der Automat überprüft, ob das Konto ausreichend gedeckt ist, um den Geldbetrag auszuzahlen. 2. Überprüfung, ob der Betrag durch eine Kontobeschränkung nicht ausgezahlt werden darf.
Ausnahmefälle	-

Prozess 2: Geld abheben am Automaten

Nachbedingung	-

Tabelle 38: Use-Case „Kontodeckung prüfen“

Name	**Karte entnehmen**
Akteure	Kunde, Geldautomat
Ziel	Die Karte soll dem Geldautomat entnommen werden.
Auslösendes Ereignis	Die Karte wurde von dem Geldautomaten ausgeworfen.
Kurzbeschreibung	Der Kunde entnimmt aus dem Geldautomaten seine Karte.
Vorbedingung	Der auszuzahlende Geldbetrag wurde eingegeben und bestätigt.
Essenzielle Schritte	1. Karte aus dem Geldautomat entnehmen
Ausnahmefälle	-
Nachbedingung	-

Tabelle 39: Use-Case „Karte entnehmen“

Name	**Geld entnehmen**
Akteure	Kunde, Geldautomat
Ziel	Das Geld soll dem Geldautomat entnommen werden.
Auslösendes Ereignis	Das Geld wurde von dem Geldautomaten ausgegeben.
Kurzbeschreibung	Der Kunde entnimmt aus dem Geldautomaten sein Geld.
Vorbedingung	Die Überprüfung der Kontodeckung war erfolgreich.
Essenzielle Schritte	1. Geld aus dem Geldautomat entnehmen
Ausnahmefälle	-
Nachbedingung	-

Tabelle 40: Use-Case „Geld entnehmen“

Prozess 2: Geld abheben am Automaten

Name	**Eingeben des Geldbetrags**
Akteure	Kunde
Ziel	Der gewünschte Betrag soll vom Kunden selbst eingegeben werden.
Auslösendes Ereignis	-
Kurzbeschreibung	Der Kunde findet keinen passenden Betrag in der Vorauswahl und will den Betrag selbst wählen.
Vorbedingung	Der Kunde lehnt die Vorauswahl auszahlbarer Beträge ab.
Essenzielle Schritte	1. Der Kunde lehnt die Vorauswahl ab. 2. Er gibt den gewünschten Betrag ein. 3. Er bestätigt die Eingabe.
Ausnahmefälle	Der auszuzahlende Betrag übersteigt die Kontodeckung.
Nachbedingung	-

Tabelle 41: Use-Case „Eingeben des Geldbetrags“

Name	**Wählen des Geldbetrags**
Akteure	Kunde
Ziel	Der gewünschte Betrag soll ausgewählt werden.
Auslösendes Ereignis	-
Kurzbeschreibung	Der Kunde findet einen passenden Betrag in der Vorauswahl und wählt diesen aus.
Vorbedingung	Der Kunde wählt den auszuzahlenden Betrag aus der Liste der vorgeschlagenen Beträge.
Essenzielle Schritte	1. Der Kunde nimmt einen Vorschlag aus der Vorauswahl an. 2. Er bestätigt die Eingabe.
Ausnahmefälle	Der auszuzahlende Betrag übersteigt die Kontodeckung.
Nachbedingung	-

Tabelle 42: Use-Case „Wählen des Geldbetrags “

8.2. BPMN-Prozessmodell: Geld abheben am Automaten

Der Prozess wird durch das Bedürfnis nach Bargeld des Kunden ausgelöst (siehe Abbildung 80). Um Geld abzuheben, muss der Kunde zu einem Geldautomaten gehen. Der Kunde kann den Geldautomaten nutzen, sofern kein anderer Kunde ihn nutzt.

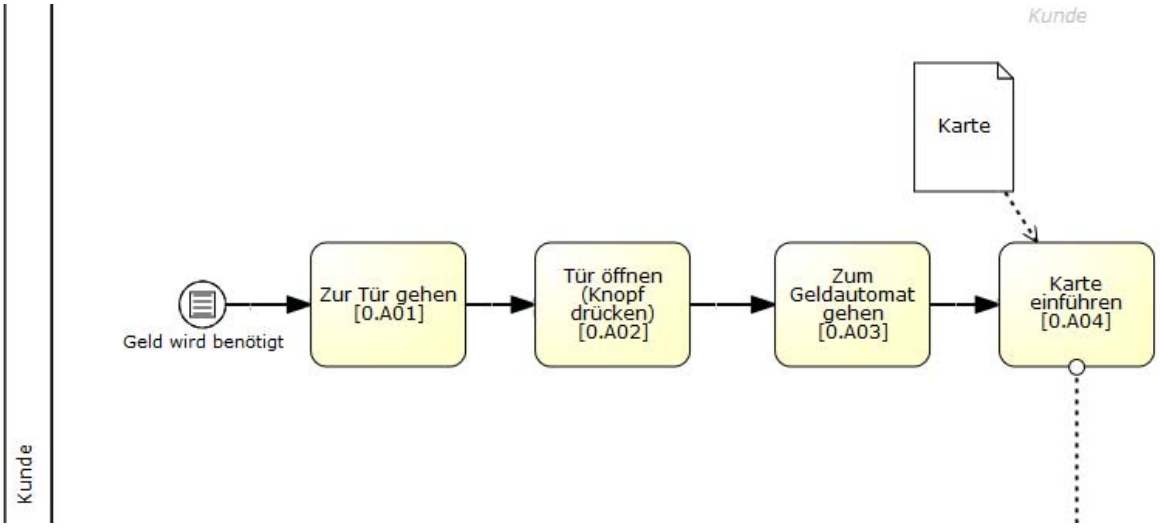

Abbildung 80: Die ersten vier Aktivitäten

Da sich der Geldautomat, welcher hier betrachtet wird, in einem Häuschen befindet, muss der Kunde zuerst zur Tür gehen [0.A01] und dann den Knopf drücken [0.A02], der die Tür automatisch entsperrt, das bedeutet, dass im konkreten Szenario keine Zutrittskontrolle besteht. Nachdem der Kunde sich unmittelbar an dem Geldautomaten befindet [0.A03], muss er die Karte einführen [0.A04]. Die Bank bzw. das System überprüft die Kartendaten [0.A05] (siehe Abbildung 81), um festzustellen ob die Karte lesbar ist (Gateway 0.G01). Falls es nicht der Fall ist, wird eine entsprechende Nachricht auf dem Bildschirm des Geldautomaten angezeigt [0.A06] und die Karte wird ausgeworfen [0.A07]. An dieser Stelle endet der Prozess. Falls die Karte lesbar ist, wird überprüft (Gateway 0.G02), ob sie gesperrt ist (falls ja, wird sie einbehalten [0.A08] und der Vorgang endet). Falls sie nicht gesperrt ist, wird überprüft (Gateway 0.G03), ob sie abgelaufen ist. Wenn das der Fall ist, wird auch überprüft (Gateway 0.G04), ob es eine Karte vom eigenen Geldinstitut ist oder ob sie von einem anderen Geldinstitut stammt. Wenn es eine interne Karte (Sparkassenkarte) ist, wird sie einbehalten und der Prozess wird

beendet. Wenn es eine externe Karte (von einem anderen Geldinstitut) ist, wird sie ausgeworfen und der Vorgang wird ebenfalls beendet.[69]

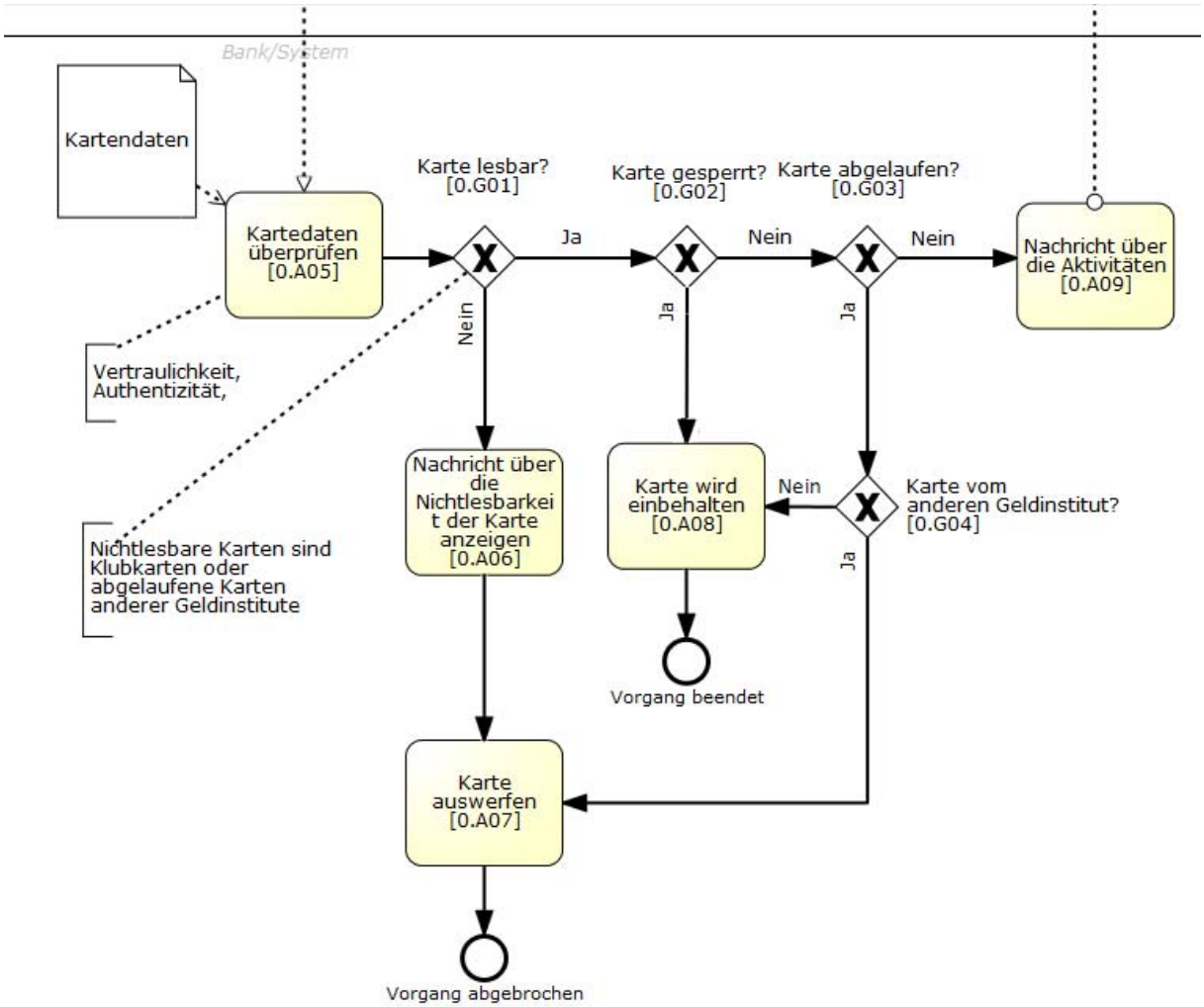

Abbildung 81: Der weitere Verlauf des Prozesses

Wenn die Karte aktiv ist, d.h. nicht gesperrt oder nicht abgelaufen ist, wird eine Nachricht über mögliche Aktivitäten angezeigt [0. A09]. Da der Kunde Geld abheben möchte[70], soll er die Funktion „Geld abheben“ auswählen [0.A10] (siehe Abbildung 82). Um den Zugriff zu gestatten, fragt der Geldautomat im nächsten Schritt nach dem PIN bzw. zeigt eine Nachricht über die PIN-Eingabe an [0.A11] (siehe Abbildung 83).

[69] Anm. der Betreuer: Diese Aussage ist zweifelhaft, da Kreditinstitute in gewissem Maße miteinander kooperieren und deren EC-Kartenautomaten z. B. gegen Gebühr auch zur Auszahlung mittels fremder Karten verwendet werden können.

[70] Anm. der Betreuer: Es wurde auch nur dieser Fall modelliert, d.h. zusätzliche Interaktionsmöglichkeiten zwischen Kunde und EC-Kartenautomat wurden hier bewusst nicht erfasst.

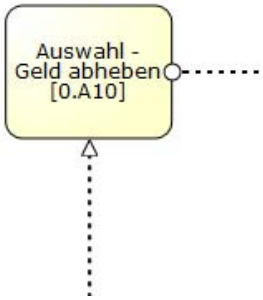

Abbildung 82: Auswahl -Geld abheben

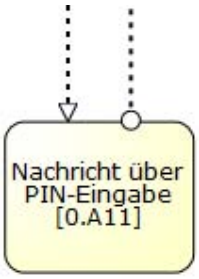

Abbildung 83: Nachricht über PIN-Eingabe

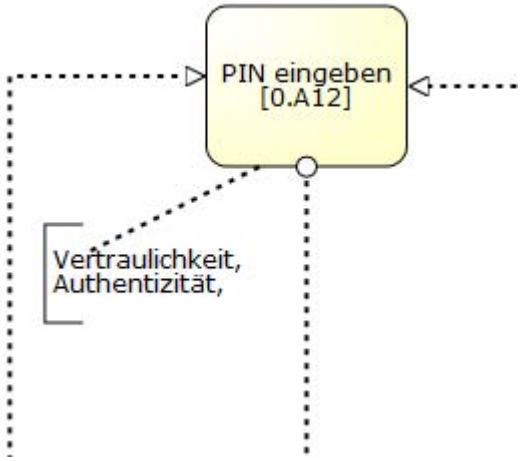

Abbildung 84: PIN eingeben

Der Kunde tippt seine PIN ein [0.A12] (siehe Abbildung 84) und der Geldautomat überprüft [0.A13], ob die PIN richtig eingegeben wurde (Gateway 0.G05) (siehe Abbildung 85). Falls das nicht der Fall ist, fordert er den Kunden zur erneuten PIN-Eingabe auf [0.A16] (siehe Abbildung 87). Bei dreimaliger Falscheingabe wird die Karte einbehalten [0.A14] und einschließlich gesperrt [0.A15]. An dieser Stelle endet der Vorgang.

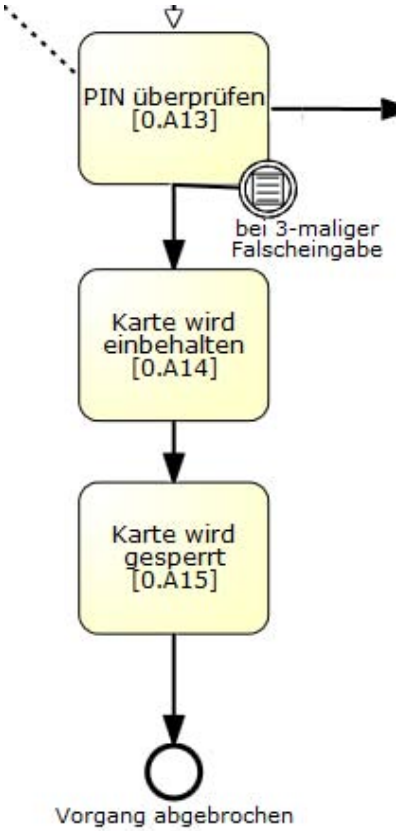

Abbildung 85: Situation bei dreimaliger Falscheingabe des PINs

Wenn der PIN richtig eingegeben ist, erscheinen Auswahlmöglichkeiten auf dem Bildschirm des Geldautomaten[0.A17] (siehe Abbildung 86).

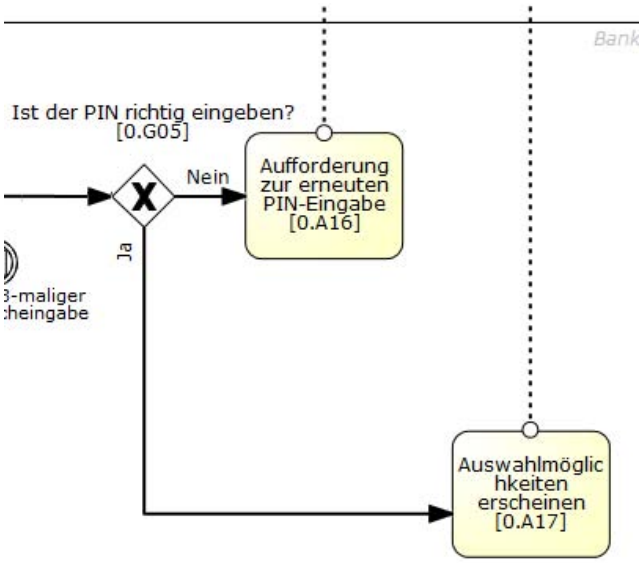

Abbildung 86: Situation bei richtiger PIN-Eingabe

Der Kunde wählt die Geldbeträge aus[0.A18] (siehe Abbildung 87).

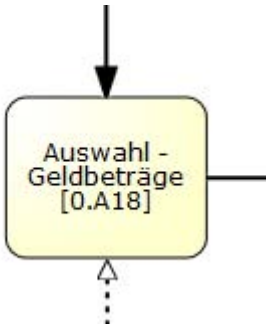

Abbildung 87: Auswahl - Geldbeträge

Er kann entweder (Gateway 0.G06) einen Festbetrag (siehe Abbildung 88) wählen [0.A22] oder die Option „weitere Beträge“ wählen [0.A19] (siehe Abbildung 89), wobei das Eingabefeld angezeigt wird [0.A20]. Der Betrag wird vom Kunden manuell eingegeben und muss daraufhin bestätigt werden [0.A21].

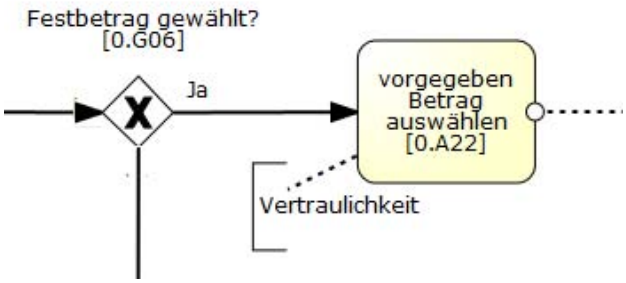

Abbildung 88: Situation, in der Festbetrag gewählt wurde

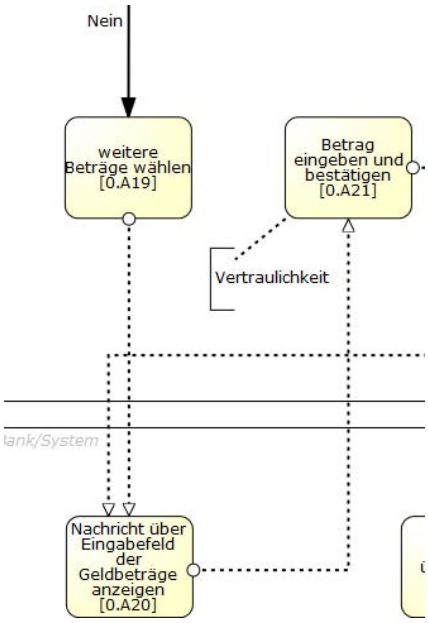

Abbildung 89: Situation, in der die Option "weitere Beträge wählen" gewählt wurde

Prozess 2: Geld abheben am Automaten

Nach diesem Schritt wird die Karte von dem System überprüft [0.A23] (siehe Abbildung 90), um festzustellen, ob die Karte von einem anderen Geldinstitut ist (Gateway 0.G07). Wenn die Karte von einem anderen Kreditinstitut ist, wird eine Nachricht über anfallende Gebühren angezeigt [0.A24]. Wenn es eine Karte der Sparkasse ist, wird die nächste Aktivität ausgeführt. Es wird überprüft [0.A25], ob der Geldbetrag durch fünf teilbar ist und im Automaten vorhanden ist. Falls das System feststellt (Gateway 0.G08), dass der gewählte Betrag nicht auszahlbar ist, wird lediglich eine Nachricht über eine mögliche Korrektur angezeigt [0.A26]. Der Kunde muss dementsprechend seine Eingaben korrigieren [0.A27] (Der Kunde wird zurück zur Aktivität 0.A20 geführt und muss ab hier den Vorgang erneut ausführen). Falls der Automat feststellt, dass der Betrag auszahlbar ist, wird eine Bestätigung der Auszahlung angezeigt [0.A28].

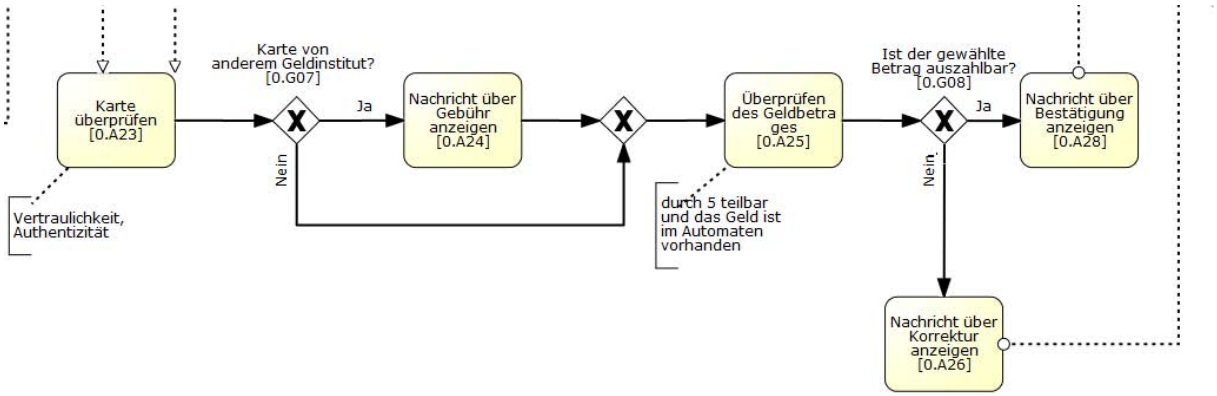

Abbildung 90: Der weitere Prozessverlauf

Um fortzufahren, muss der Kunde den Betrag bestätigen [0.A29]. Als nächstes überprüft das System den Kontostand [0.A30] (siehe Abbildung 91).

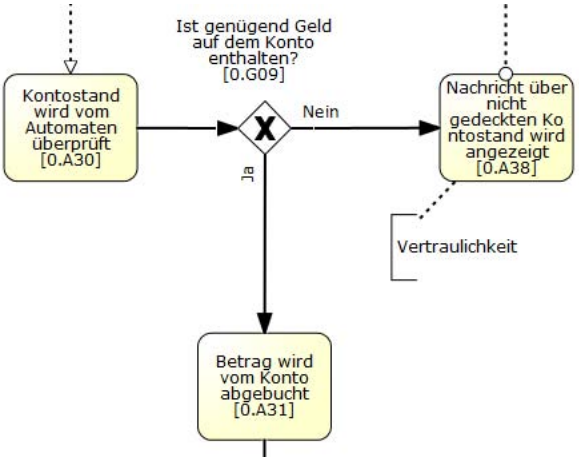

Abbildung 91: Darstellung des Gateways [0.G09]

Wenn dies der Fall ist, wird der Betrag vom Konto abgebucht [0.A31] und die Karte wird ausgegeben [0.A32]. Der Kunde hat 30 Sekunden, um die Karte zu entnehmen. Falls er das innerhalb dieser Zeitspanne nicht machen sollte, wird die Karte eingezogen [0.A33] und später an seine Bank geschickt. Somit wird der Vorgang beendet. Falls der Kunde die Karte entgegennimmt [0.A34], wird als nächstes das Geld ausgegeben [0.A35]. In diesem Fall hat der Kunde ebenfalls eine gleiche Zeitspanne, um das Geld entgegenzunehmen. Falls er das nicht schaffen sollte, wird der Geldbetrag eingezogen [0.A36] und seinem Konto wieder gutgeschrieben. Der Vorgang wird beendet. Wenn die Geldscheine vom Kunden entnommen werden [0.A37], wird der Prozess beendet.

Um den Prozess zu vervollständigen wird die Aktivität [0.A30] beschrieben, die bis jetzt nicht betrachtet wurde. Bei dieser Aktivität überprüft das System, ob der Kunde genug Geld auf dem Konto hat, um den gewünschten Auszahlungsbetrag zu erhalten. Falls der Kunde nicht über genügend Geld verfügt, wird ihm eine Nachricht über den nicht gedeckten Kontostand angezeigt [0.A38]. Nachdem der Kunde die Nachricht gelesen hat [0.A39], kann er entscheiden, ob er den Prozess fortfahren oder abbrechen möchte (Gateway 0.G10). Angenommen der Kunde möchte den Prozess fortfahren, wird er automatisch zu Aktivität [0.A18] geleitet. Wenn er sich für den Abbruch entscheidet, muss er diesen bestätigen [0.A40]. Die Karte wird ihm vom Automaten ausgegeben [0.A41]. Hierbei muss er wieder die Zeit beachten, denn wenn die 30 Sekunden abgelaufen sind, wird die Karte eingezogen [0.A42] und der Vorgang wird beendet. Wenn der Kunde die Karte rechtzeitig entnimmt [0.A43], wird der Vorgang an dieser Stelle beendet.

8.3. Interessenkonflikte

Um alle möglichen Interessenkonflikte zu erfassen, wurden die verschiedenen Rollen und alle kombinatorischen Möglichkeiten in die Zeilen und Spalten einer Matrix aufgetragen. Der Vorteil gegenüber einer szenarienorientierten Betrachtungsweise liegt in der vollständigen Erfassung aller Rollen und Konstellationen. Allerdings nimmt die Komplexität der Matrix exponentiell mit der Anzahl der Rollen zu.

	/	K	B	A	K + B	K + A	B + A	K + B + A
/	n.b.	X	X	X	X	X	X	X
K	X	n.b.		X	X	X	X	X
B	X	X	n.b.	X	X	X	X	X
A	X			n.b.		X	X	X
K + B	X	X	X	X	n.b.	X	X	X
K + A	X	X	X	X	X	n.b.	X	X
B + A	X	X	X	X	X	X	n.b.	X
K + B + A	X	X	X	X	X	X	X	n.b.

Tabelle 43: Interessenmatrix

Bei den in diesem Prozess erfassten Rollen, wie in Tabelle 43 zu sehen, handelt es sich um einen Kunden (K), der Bank bzw. dem Bankautomaten (B) und einem externer Angreifer (A) und eine leere Rolle, die hier mit „/“ gekennzeichnet ist. Die Elemente der Matrix sind so zu lesen, dass die Rollen der Zeilen gegen die Rollen der Spalten agieren. Später werden zu diesen Paarungen konkrete Szenarien beschrieben.

Bei denen mit X gekennzeichneten Elementen liegen keine Interessenkonflikte vor. Die gelben Matrixzellen weisen auf einen oder mehrere eventuelle Konflikte hin. Die mit n.b. gekennzeichneten Elemente werden nicht betrachtet, da hier die Rollen gegen sich selbst agieren müssten.

Bei einer Anzahl n Rollen, lassen sich 2^n viele Rollenkombinationen zusammenstellen, wodurch $(2^n)^2$ viele Matrixelemente entstehen, die potenziell auf Konflikte untersucht werden müssten. Um den Aufwand einzugrenzen, können viele Konstellationen nicht betrachtet werden:

- Die ersten und letzten Zeilen und Spalten beinhalten die leere Rolle und eine Kombination aus allen Rollen. Diese sind nur aus Gründen der Vollständigkeit aufgeführt und bieten keinen Mehrwert bei einer Analyse.
- Werden die Rollen symmetrisch in der ersten Zeile und Spalte aufgetragen, stehen sich in der Diagonale identische Paarungen gegenüber, womit diese Fälle nicht weiter betrachtet werden müssen.
- Das gleiche gilt für Kombinationen, die andere Kombinationen oder Rollen enthalten, beispielsweise wenn ein Interessenkonflikt zwischen dem Kunden und dem Kunden mit der Bank gesucht werden soll.
- Weiter gehen wir davon aus, dass die Bank ausschließlich gute Absichten verfolgt[71], auch wenn dies in der Realität nicht so sein muss. Diese Entscheidung wurde aus Zeitgründen getroffen, da die Verfolgung dieses neuen Vorgehens im Vordergrund stand und nicht die vollständige Erfassung aller Möglichkeiten.

Die Interessenmatrix erfasst lediglich die Szenarien, die vom Best-Case-Szenario abweichen. Dabei bedient der Kunde den Bankautomaten und erhält sein Geld, ohne dass er im Nachhinein versucht die Bank zu betrügen oder dass ein externer Angreifer Teil dieses Prozesses war. Dadurch bleiben in diesem Prozess vier Paarungen übrig, die im Weiteren genauer untersucht werden:

- Der Kunde agiert gegen die Bank
- Der Angreifer agiert gegen die Bank
- Der Angreifer agiert gegen den Kunden
- Der Angreifer agiert gegen den Kunden und die Bank

Diesen Paarungen können verschiedene Szenarien zugeordnet werden, die in eine Matrix eingetragen werden. Diese Matrix ist in Tabelle 44 abgebildet.

	Kunde	Bank	Kunde + Bank
Kunde	X	- Geldbetrug	X
Angreifer	- Trickbetrug	- Safe heraussprengen	- Karte auslesen

[71] Anm. der Betreuer: Die Analyse wurde offensichtlich aus Sicht der Bank vorgenommen. Abhängig von der eingenommenen Sicht können sich nämlich unterschiedliche und ggfls. sich widersprechende Anforderungen ermittelt werden.

Prozess 2: Geld abheben am Automaten

	- Raub/ Überfall - Erpressung	- Safe mit Fahrzeug rammen	- PIN erspähen - Cash-Trapping

Tabelle 44: Szenarienmatrix

Grundlegend zielen diese Angriffe alle auf das Geld des Opfers ab, nur werden unterschiedliche Vorgehensweisen und Mittel gewählt. Opfer können – je nach Szenario – sowohl der Kunde, als auch die Bank sein.

8.4. Szenarien

Zu den oben aufgelisteten Paarungen werden hier die Szenarien beschrieben.

Der Kunde agiert gegen die Bank

Der Kunde gibt an, dass es bei der Benutzung des Automaten Probleme gab und er den eigentlich ausgezahlten Betrag nicht oder nur zum Teil erhalten hat. Dazu könnte er beispielsweise auf einen fiktiven Angriff verweisen (siehe *physische Angriffe*) und sich unrechtmäßig als Opfer präsentieren. Weiter ist es denkbar, dass diese Person einen Zeugen angibt, der diese Aussage bekräftigt.

Durch diese Angriffe würde die Nichtabstreitbarkeit des Prozesses[72] verletzt.

Um den Prozess abzusichern, hat die Bank eine Kamera im Kassenhäuschen installiert. Mit den Aufnahmen der Kamera ist es möglich, den vermeintlichen Betrug zu widerlegen und die Schuld des Kunden aufzudecken und zu beweisen. Zusätzlich, wenn die Sicht der Kamera verdeckt ist oder ein technisches Problem vorliegt, ist der Prozess durch das Einziehen des Betrags gesichert. Entnimmt der Kunde den ausgezahlten Betrag nur teilweise oder gar nicht, wird das restliche Geld nach 30 Sekunden eingezogen und dem Konto des Kunden gutgeschrieben.

Der Angreifer agiert gegen die Bank bzw. den Bankautomaten

[72] Anm. der Betreuer: Die Nichtabstreitbarkeit bezieht sich eher auf einzelne Prozessschritte (z. B. Protokollieren von Abhebevorgängen). Um die Integrität des Verlaufs sicherzustellen, kann z. B. die Überwachung per Kamera eingesetzt werden.

Diese Angriffe werden unter dem Begriff der *physischen Angriffe* zusammengefasst. Sie stellen Angriffe auf die Verfügbarkeit der Geräte dar, so genannte „Denial of Service"-Attacken. Von einer Modellierung in BPMN wurde abgesehen, da diese Angriffe unabhängig vom eigentlichen Geldabhebeprozess sind. Sie können ihn allerdings verhindern.

Automaten sprengen, um an den Safe zu gelangen: Um an das Geld im Automaten zu gelangen, verwenden die Angreifer Sprengstoff. Die Sprengladungen werden gezielt platziert, damit der Safe mit der Explosion geöffnet oder aus eventuellen Verankerungen herausgesprengt wird, damit er im Ganzen gestohlen werden kann[73] [74] [75].

Automaten mit Fahrzeug rammen, um an den Safe zu gelangen: Bei dieser Angriffsart benutzen die Täter ein Fahrzeug um den Bankautomaten zu rammen und damit so zu beschädigen[76]. Der Automat kann so schnell entleert bzw. aufgeladen werden, um mit der Beute schnell flüchten zu können[77].

Da diese Angriffe unabhängig vom Geldabhebeprozess ablaufen können, verletzen sie die bestehenden Sicherheitsanforderungen der einzelnen Aktivitäten nicht. Allerdings wird die Verfügbarkeit des ganzen Prozesses verletzt.

Es ist wahrscheinlich, dass die Bank sehr viel Geld und Aufwand investiert um diese destruktiven Angriffe zu verhindern, zum Beispiel durch immer sicherer werdende Safes, dies bezieht sich sowohl auf den Einbau als auch auf die Sicherung der enthaltenen Geldbestände. Konkrete Angaben zu neu umgesetzten Sicherheitsmaßnahmen sind nur sehr schwer recherchierbar.

Der Angreifer agiert gegen die Bank und den Kunden

Diese Angriffe werden unter dem Begriff der *technischen Angriffe* zusammengefasst und wurden in BPMN abgebildet.

[73] http://www.welt.de/regionales/duesseldorf/article109425256/Bankraeuber-sprengen-versehentlich-Sparkasse.html
[74] http://www.tagesspiegel.de/berlin/berlin-mitte-wieder-geldautomat-gesprengt/8793568.html
[75] http://www.tagesspiegel.de/berlin/bankautomaten-in-berlin-und-brandenburg-gesprengt-polizei-knackt-bande-der-panzerknacker/8614928.html
[76] http://www.tagesspiegel.de/berlin/polizei-justiz/geldautomat-gerammt-diebe-fuhren-mit-auto-in-s-bahnhof/7680112.html
[77] http://www.hr-online.de/website/rubriken/nachrichten/indexhessen34938.jsp?rubrik=36094&key=standard_document_50556719

Prozess 2: Geld abheben am Automaten

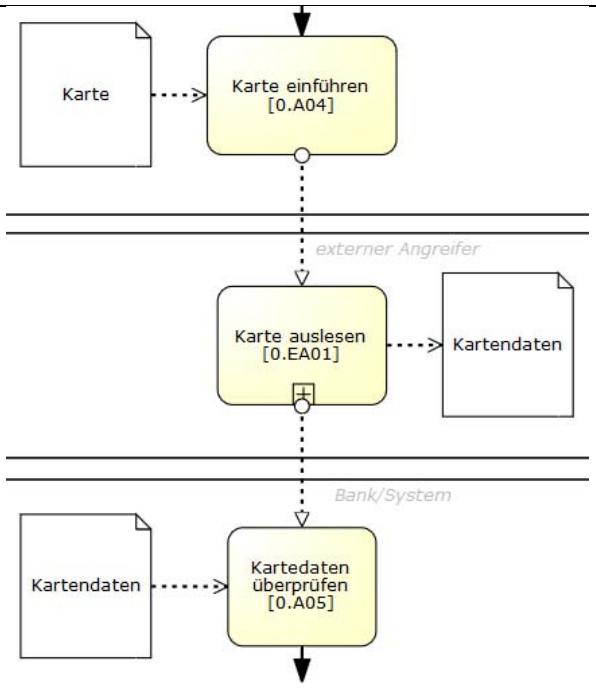

Abbildung 92: Angriff auf die Kartendaten des Kunden

Karte auslesen (Skimming) [0.EA01]: Der externe Angreifer hat den Automaten manipuliert, sodass er die Kartendaten auslesen kann, die auf dem Magnetstreifen der Bankkarte gespeichert sind. Dafür wird die Kartenöffnung mit einer Blende versehen, in der sich ein kleiner Lesekopf befindet, der die Daten, wie auf Abbildung 92 modelliert ist, auf dem Streifen ausliest und speichert[78,79]. Diese Angriffe werden oft mit dem Ausspähen der PIN kombiniert, um später gefälschte, aber für den Automaten authentische Karten anzufertigen, die einen Zugriff auf das Geldkonto des Opfers erlauben (vgl. Bachfeld, 2007)[80].

[78] http://www.abendblatt.de/wirtschaft/finanzen/article1884480/Tausende-Kunden- werden-an-Geldautomaten-abgezockt.html
[79] http://www.ka-news.de/region/karlsruhe/Manipulierte-Geldautomaten-Karlsruher-Polizei-gibt-Tipps;art6066,642868
[80] http://www.heise.de/security/artikel/Angriff-der- Karten-Kloner-270934.html

Prozess 2: Geld abheben am Automaten

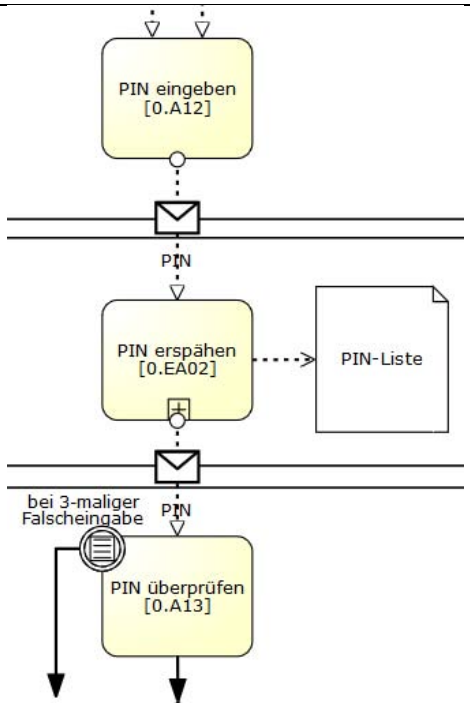

Abbildung 93: PIN erspähen

PIN erspähen (Skimming) [0.EA02]: Um an die PIN des Opfers zu kommen, bedienen sich Angreifer verschiedenster technischer Hilfsmittel. Zum Beispiel werden kleine Kameras am Automaten montiert, die das Tastenfeld aufnehmen. Bei einer anderen Methode bringen die Angreifer selbst angefertigte Tastaturen oder Blenden am Automaten an, wodurch bei der Eingabe der PIN (siehe Abbildung 93) diese aufgezeichnet wird.

Prozess 2: Geld abheben am Automaten

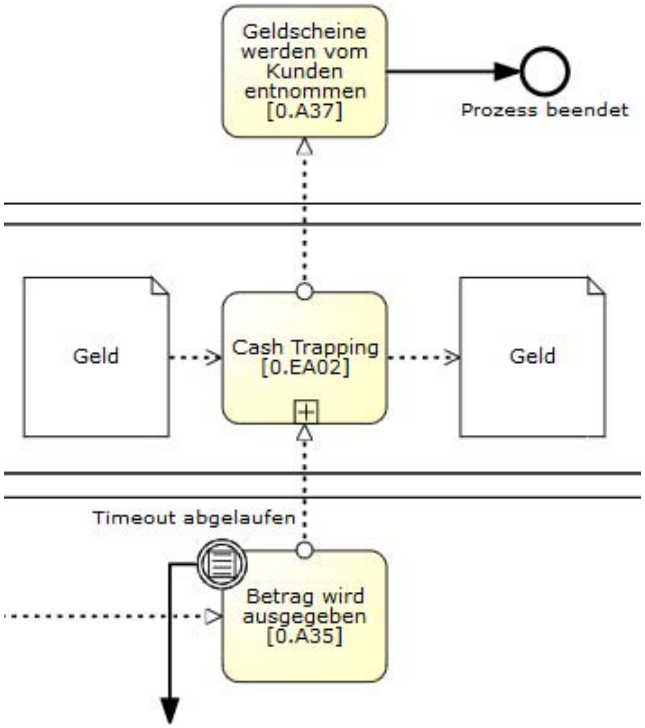

Abbildung 94: Cash Trapping

Cash-Trapping [0.EA03]: Hierbei bringen die Angreifer eine Vorrichtung am Automaten an, bei der das Geld des Kunden zurückgehalten wird[81]. Danach schaltet der Automat ab. Der Kunde glaubt an einen technischen Defekt des Gerätes und distanziert sich ohne Geld, aber mit belastetem Konto (siehe Abbildung 94), vom Automaten. Ist er außer Sichtweite, entnehmen die Angreifer das Geld und flüchten (vgl. Stoll, 2010)[82].

Durch diese Angriffe würden die Integrität, Vertraulichkeit und Authentizität des Prozesses verletzt. Die Authentizität lässt sich auf einzelne Aktivitäten des Prozesses herunterbrechen, die durch die o.a. Angriffe beeinträchtigt werden.

Auch wenn die Kameraaufnahmen die Manipulationen am Automaten dokumentieren, können sie diese Eingriffe nicht verhindern. Allerdings können sie später dafür benutzt werden, die unrechtmäßigen Abhebungen zu beweisen und den Kunden zu entschädigen. Weiter hat dieser die Möglichkeit seine Karte direkt vor Ort durch eine Notrufnummer sperren zu lassen, die am Automaten abgedruckt ist. Außerdem kann der Kunde ein tägliches Abhebemaximum

[81] http://www.nordbayern.de/nuernberger-nachrichten/nuernberg/wieder-eine-neue- masche-diebe-fangen-scheine-ab-1.385934

[82] http://www.stuttgarter-zeitung.de/inhalt.cash-trapping-in-stuttgart-das-bargeld-wird- abgefangen.672930f5-7918-4f72-8907-31e9c9cd155f.html

für sein Konto über Bankautomaten einrichten, wodurch der potentielle Schaden gering gehalten werden kann.

Zusätzliche Sicherheitsmaßnahmen können aus Sicht der Bank und aus Sicht des Kunden formuliert werden. Die Bank kann den Angriffen nur schwer präventiv begegnen, allerdings kann sie ihre Automaten derart modifizieren, dass bekannte Angriffsmethoden technisch erschwert oder nicht mehr möglich sind. Weiter können sie durch Flyer oder Briefe ihre Kunden aufklären. Durch diese Maßnahme der so genannten „Security Awareness“ wird der Kunde zum Sicherheitsträger. Der Kunde sollte den Automaten vor der Nutzung untersuchen, indem er beispielsweise den Karteneinzug und die Tastatur abtastet und überprüft. Sollte ihm dabei etwas auffallen oder an der Sicherheit zweifeln, sollte er ihn nicht nutzen und eventuelle Auffälligkeiten melden.

Der Angreifer agiert gegen den Kunden

Diese Angriffe werden, zusätzlich zu den oben genannten *physischen Angriffen* zugeordnet. Von einer Modellierung in BPMN wurde auch hier abgesehen, da diese Angriffe theoretisch an jedem Punkt des Prozesses auftreten können.

Trickbetrug: Während der Kunde am Automaten eine Auszahlung vornehmen will, betritt eine kleine Personengruppe das Kassenhäuschen. Während ein oder mehrere Mitglieder dieser Gruppe versuchen den Kunden abzulenken, belastet jemand anderes unbemerkt das Konto des Opfers. War der Angriff erfolgreich, ziehen sich die Täter zurück, ohne dass das Opfer etwas bemerkt hat.

Raub/ Überfall: Wenn der Kunde das Geld vom Automaten entgegengenommen hat, wird ihm das Geld, eventuell mit Gewalt, entwendet. Diese Angriffsart kann von dem Zeitpunkt der Geldausgabe stattfinden.

Erpressung: Ähnlich dem Trickbetrug betreten ein oder mehrere Personen das Kassenhäuschen und zwingen den Kunden eine Auszahlung vorzunehmen. Zusätzlich ist denkbar, dass er gezwungen wird seine Karte abzugeben und den Tätern seine PIN mitzuteilen, damit diese zeitnah weitere Auszahlungen vornehmen können.

Auch diese Angriffe können unabhängig vom Geldabhebeprozess ablaufen und verletzen die bestehenden Sicherheitsanforderungen nicht direkt.

Um diese Angriffe zu vermeiden, sollen die im Kassenhäuschen installierten Kameras als Prävention dienen. So können alle Angriffe, die sich innerhalb des Häuschens ereignen, dokumentiert und für spätere polizeiliche Ermittlungen genutzt werden. Ebenfalls, wie bei den technischen Angriffen, kann der Kunde seine Karte sperren lassen und durch ein Abhebemaximum den eventuellen Schaden gering halten.

Als weiterführende Sicherheitsmaßnahme kann an den *gesunden Menschenverstand* des jeweiligen Kunden appelliert werden. Er sollte sich bei Abhebeprozess nicht ablenken lassen um die Gefahr eines Trickbetrugs zu vermindern. Um einer Erpressung oder einem Raub vorzubeugen, ist es ratsam vor allem nachts nicht alleine unterwegs sein. Sollten diese Maßnahmen einen konkreten Angriff nicht verhindern, sollte schnellstmöglich die Polizei verständigt werden.

8.5.Konsistenzanalyse

Nachdem die verletzten Sicherheitsanforderungen der Szenarien beschrieben wurden, wird auf Aktivitätsebene untersucht, ob sich ausschließende Sicherheitsanforderungen aufzeigen lassen. Als sich ausschließende Sicherheitsanforderungen wurden Authentizität und Vertraulichkeit sowie Nichtabstreitbarkeit und Vertraulichkeit definiert[83].

Für den gesamten Prozess gilt die Nichtabstreitbarkeit[84], da der Kunde, um Geld abzuheben, den Aktivitätsfluss des Diagrammes durchlaufen muss. Weiter muss ab Aktivität *[0.A04] Karte einführen* die Verfügbarkeit des Automaten gelten, da der Prozess ansonsten nicht ausgeführt werden kann (siehe Abbildung 95).

Bei den Angriffen, bei denen der Kunde gegen die Bank agiert, würde wie oben beschrieben die Nichtabstreitbarkeit des Prozesses verletzt[85]. Doch es liegt kein Konsistenzproblem vor, da keine sich gegenseitig ausschließenden Sicherheitsanforderungen vorliegen. Gleiches gilt für die beschrieben Szenarien, bei denen der Angreifer gegen die Bank bzw. den Bankautomaten agiert. Hier wird die Verfügbarkeit des Geldautomaten verletzt, aber sich ausschließen-

[83] Anm. der Betreuer: Zur Analyse wurde eine Menge von Sicherheitsanforderungen angewendet. Aus dieser Menge lassen sich widersprüchliche Sicherheitsanforderungen bereits vorab identifizieren, so dass im Prozess gezielt nach diesen gesucht werden kann.
[84] Der rechtmäßige Inhaber der EC-Karte wird über zwei Faktoren authentifiziert: PIN (Wissen) und EC-Karte (Besitz). Entsprechend dieser Sichtweise lassen sich alle der Authentifizierung nachgelagerten Aktionen bis hin zur Ausgabe der EC-Karte eindeutig dem EC-Karten-Inhaber zurechnen.
[85] Anm. der Betreuer: Im Falle von Betrug versucht der betrügende Nutzer, Lücken in den Maßnahmen zur „Nicht-abstreitbarkeit der Aktion“ zu finden, um nicht erkannt und verfolgt zu werden.

de Anforderungen liegen auch hier nicht vor. Bei den physischen Angriffen wird keine der definierten Anforderungen verletzt, sodass auch hier kein Konsistenzproblem vorliegt.

Die bei den technischen Angriffen beteiligten Sicherheitsanforderungen sind die Nichtabstreitbarkeit, Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit. Je nach Angriffsszenario sind davon alle oder nur eine bestimmte Teilmenge beteiligt.

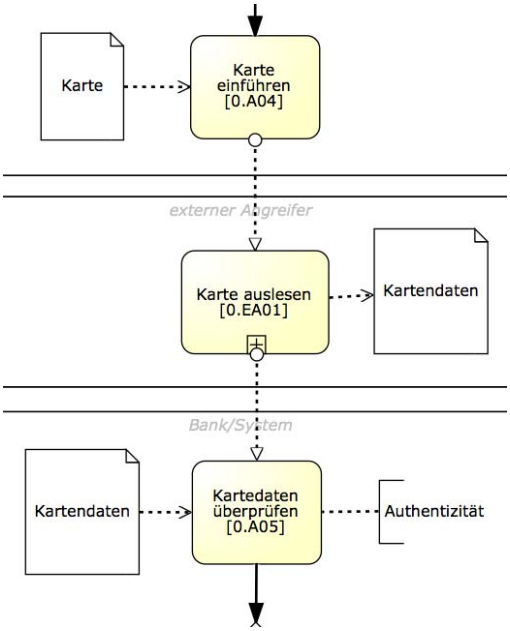

Abbildung 95: Konsistenzanalyse - Karte auslesen

Zu den beiden global bestehenden Anforderungen wird beim Auslesen der Kartendaten bei der Aktivität [0.A05] die Authentizität eines Kommunikationspartners verletzt, der nicht der ist, der er vorgibt zu sein. Genannte Anforderungen schließen sich nicht aus, sodass kein Konsistenzproblem vorliegt.

Prozess 2: Geld abheben am Automaten

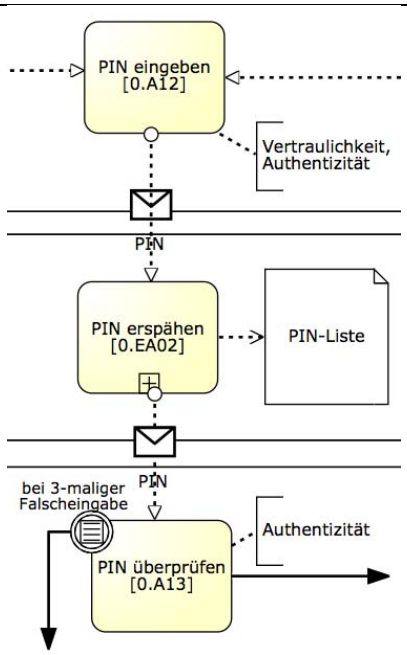

Abbildung 96: Konsistenzanalyse - PIN erspähen

Die PIN-Eingabe fungiert als Sicherheitsmaßnahme, wodurch nur autorisierte Personen Zugang zum betroffenen Konto haben sollen. Die Autorisierung erfolgt in der Regel nach der Authentifizierung. Beim Ausspähen der PIN, wie auf Abbildung 96 zu sehen ist, bestehen alle oben genannten Anforderungen. Auch wenn sich die Sicherheitsanforderungen Vertraulichkeit und Authentizität, wie oben beschrieben, gegenseitig ausschließen, liegt hier kein Konsistenzproblem vor (vgl. Aktivität [0.A12]). Das liegt daran, dass sich die Vertraulichkeit auf die PIN und die Authentizität auf den Kunden bezieht, dessen Identität durch die EC-Karte repräsentiert wird.

Ein alternatives Vorgehen zur Zugangsverifizierung gestaltet sich als sehr schwer. Würde dieser Kontrollschritt ausgelassen werden, würde der Prozess unsicherer. Denkbar wäre die Kontrolle von biometrischen Daten, wie zum Beispiel dem Scannen der Retina oder dem Überprüfen des Fingerabdrucks. Aber dies würde wahrscheinlich neuartige Szenarien generieren, bei denen Angreifer auch diese Informationen speichern würden, wodurch der Schaden insgesamt größer wäre.

Der Informationsraub, ohne Berücksichtigung des finanziellen Schadens, kann in Kauf genommen werden, da jederzeit eine neue Karte und eine neue PIN generiert werden können.

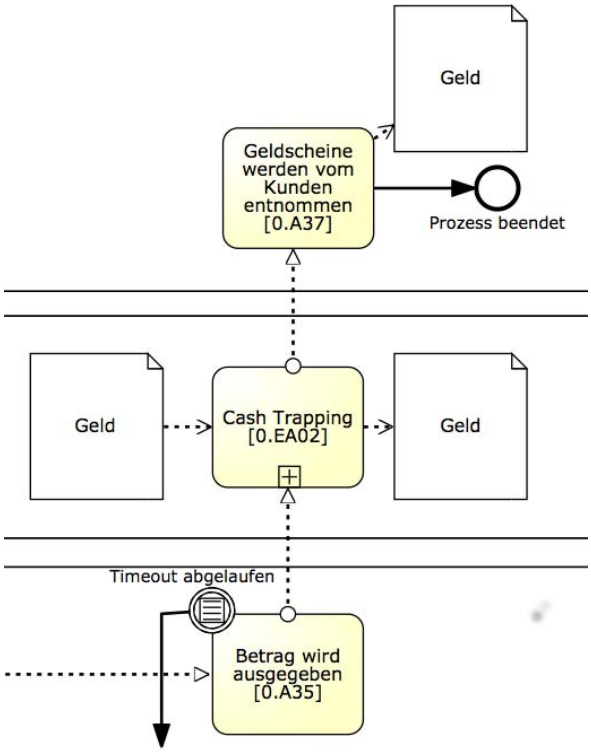

Abbildung 97: Konsistenzanalyse - Cash Trapping

Auch hier ergibt sich, wie beim ersten technischen Angriff, kein Konsistenzproblem, da sich keine Sicherheitsanforderungen ausschließen. Vergleiche dazu Abbildung 97.

9. Fazit

9.1. Lesson Learned

Wie oben beschrieben, wurden für die einzelnen Aktivitäten in BPMN die entsprechenden Sicherheitsanforderungen und Sicherheitsmaßnahmen formuliert. Im ersten Prozess wurden die Interessenkonflikte mit Hilfe von aneinander angrenzenden Aktivitäten analysiert. Dadurch besteht eine hohe Wahrscheinlichkeit, Konflikte zu missachten oder falsch zu interpretieren. Um beim zweiten Prozess diesen Interpretationsfehler nicht zu wiederholen, wurden die Interessenkonflikte getrennt von den Sicherheitsanforderungen und Sicherheitsmaßnahmen mit einer Matrix bearbeitet.

Im Zwischenfazit wurde festgehalten, dass die zu Anfang erstellten Use-Cases und deren Beschreibungen zu dem Wahlprozess sehr aufwendig und zeitintensiv waren. Um herauszufinden, welche Einstiegsmöglichkeit in den Prozess hilfreicher und sparsamer an Zeit ist, wurden

beide Vorgehensweisen Referenzprozess und Use-Cases gegeneinander evaluiert. Dafür wurden die Forschungsteilnehmer in zwei Gruppen eingeteilt, um unabhängige Ergebnisse zu erhalten. Das Resultat des Vergleiches war, dass der Referenzprozess wesentlich schneller als die Erstellung der Use-Cases und derer Beschreibungen war. Das lag vor allem an der Erstellung der Use-Case-Beschreibungen, die sehr zeitintensiv waren. Der Referenzprozess demgegenüber bietet zudem einen ersten Einstieg in BPMN und liefert als Ergebnis den vereinfachten Prozessablauf, an dem sich immer wieder orientiert werden kann. Weiter konnten bei Prozess 1 keine globalen Konsistenzprobleme aufgezeigt werden, da nur die vorangehenden und nachfolgenden Aktivitäten analysiert wurden. Dieses Problem wurde bei der Bearbeitung von Prozess 2 behoben, da hier für die Konsistenzanalyse die sich ausschließenden Sicherheitsanforderungen herangezogen werden.

9.2. Weiterführende Arbeiten

Um die Arbeit zu vollenden sind noch weiterführende Arbeiten notwendig. Ein Problem, welches bei der Evaluierung der Prozesse auftrat, war die Darstellung der Interessenkonflikte. Im ersten Prozess wurden die Interessenkonflikte veranschaulicht, indem einzelne Aktivitäten betrachtet und diese jeweils evaluiert wurden. Jedoch wurden dadurch verschieden Interessenkonflikte außer Acht gelassen oder nicht erkannt. Im zweiten Prozess wurde daher ein anderes Verfahren angewendet. Hierbei wurde eine Matrix erstellt und versucht alle Konflikte zu erfassen. Doch auch hier basieren die Konflikte auf dem Wissen des Verfassers. Verdeckte Konflikte werden auch hier möglicherweise nicht erkannt. Insbesondere bei aufwändigeren Prozessen ist dieses Verfahren nicht empfehlenswert, da dieses Verfahren sehr umfangreich würde und auch hier nicht alle Interessen erfasst werden könnten. Aus diesem Grund muss noch ein Verfahren entwickelt werden, um die Wirkung der Interessenkonflikte besser darzustellen und zu identifizieren.

Ein weiterer Punkt der noch untersucht werden sollte, ist der Nutzen der Use-Cases. Im Laufe des Prozesses wurde festgestellt, dass für die Erstellung des BPMN-Modells die Use-Cases nicht notwendig sind und diesbezüglich der Referenzprozess besser geeignet ist. Jedoch stellt sich hierbei die Frage, ob in den Use-Case-Beschreibungen enthaltenen Sonderfälle Interessenkonflikte abgeleitet werden können und die Erfassung der Konflikte erleichtert wird.

Im Verlauf des Forschungspraktikums wurden zwei Prozesse analysiert: Kommunalwahlen Koblenz und das Abheben von Bargeld an einem Geldautomaten. Der erste Prozess ist sehr komplex gewesen, da dort sehr viele Akteure beteiligt sind und viele umfangreiche Aktivitä-

ten abzuarbeiten sind. Aus diesem Grund wurde der Gesamtprozess in vier kleinere Prozesse unterteilt. So lassen sich die BPMN-Modelle besser darstellen und der Prozess kann besser verstanden und nachvollzogen werden. Der zweite Prozess ließ sich mit deutlich weniger Aufwand bearbeiten und ist weniger kompliziert gewesen. Beide Prozesse wurden mithilfe des PrOSA-Vorgehensmodells analysiert. Nach der Evaluierung des Modells konnten bereits im einige Lessons Learned (siehe Kapitel 9.1) identifiziert werden. Um weitere Aussagen zu dem Vorgehensmodell zu treffen, muss dieses an weiteren Prozessen angewendet und evaluiert werden. Dadurch wird sichergestellt, dass die zuvor dargestellten Erkenntnisse plausibel sind und weitere aussagekräftige Ergebnisse erzielt werden können.

Das PrOSA-Vorgehensmodell besteht aus mehreren Schritten, die nacheinander durchgeführt werden (Siehe Kapitel 3). Bei den beiden betrachteten Prozessen wurden die Schritte „Durchführung der Formalen Analyse“ und die „Quellcodeanalyse“ nicht umgesetzt, da kein Zugriff auf die Quellcodes sowie die IT-Systeme bestand. Bei der formalen Analyse findet eine formale Beschreibung der Aktionen des IT-Systems im Rahmen der Aktivität statt. Zudem wird untersucht, ob bestimmte Ereignisse das betrachtete Fragment in einen sicheren Systemzustand überführen. Die tiefste Ebene der Untersuchung im Rahmen des PrOSA-Vorgehensmodells wird mit der Quellcodeanalyse erreicht. Hierbei können z.B. die implementierten Verschlüsselungsverfahren für das beteiligte IT-System festgestellt werden. Für beide Schritte ist Expertenwissen notwendig (z.B. vertiefte Programmierkenntnisse, Kenntnisse der verwendeten IT-Systeme). Es lässt sich nicht eindeutig feststellen, ob die vorliegende Gesamtuntersuchung unter der fehlenden Berücksichtigung der beiden Schritte gelitten hat. Deswegen wäre es empfehlenswert, bei zukünftigen Untersuchungen diese zwei Schritte ebenfalls zu betrachten. Dafür muss sichergestellt werden, dass auf die spezifischen Quellcodes und IT-Systeme zugegriffen werden kann.

Literaturverzeichnis und Quellenverzeichnis

Accorsi, R. (2013). Sicherheit im Prozessmanagement. *digma 2013.2*, 72-74.

Allweyer, T. (2009). *BPMN 2.0 - Business Process Model and Notation: Einführung in den Standard für die Geschäftsprozessmodellierung* (2. Ausg.). Norderstedt: Books on Demand.

Amann, E., & Atzmüller, H. (1992). IT-Sicherheit, was ist das? *DuD 6/92*, 286-292.

Arbeitskreis Technik. (2003). Orientierungshilfe zum Einsatz kryptografischer Verfahren. *Konferenz der Datenschutzbeauftragten des Bundes und der Länder.* Mainz.

Bartsch, C. (2010). *Modellierung und Simulation von IT-Dienstleistungsprozessen.* Karlsruhe: KIT Scientific Publishing.

Grimm, R.; Simić-Draws, D.; Bräunlich, K.; Kasten, A.; Meletiadou, A. (2014): Referenzmodell für ein Vorgehen bei der IT-Sicherheitsanalyse. Informatikspektrum, Springer Verlag Heidelberg usw, 2014, Springer Online, DOI 10.1007/s00287-014-0807-3.

Bundesamt für Sicherheit in der Informatik. (2003). *Durchführungskonzept für Penetrationtests.* Bonn.

Bundesamt für Sicherheit in der Informationstechnik. (2012). *Leitfaden Informationssicherheit: IT-Grundschutz kompakt.* Rheinbach: Druckpartner Moser Druck + Verlag GmbH.

Eckert, C. (2013). *IT-Sicherheit: Konzepte - Verfahren - Protokolle* (8. Ausg.). München: Oldenbourg-Verlag.

Freund, J., & Rücker, B. (2012). *Praxishandbuch BPMN 3.0* (3. Ausg.). Carl Hanser Verlag GmbH & Company AG.

Frugier, F. (2009). *Die Einrichtung moderner interner Kontrollsysteme in Unternehmen mit US-amerikanischem Listing: Politische und betriebliche Rahmenbedingungen und Besonderheiten der Umsetzung des Sarbanes Oxley Act in Deutschland.* Diplomica-Verlag.

Göpfert, J., & Lindenbach, H. (2012). *Geschäftsprozessmodellierung mit BPMN 2.0 - Business Process Model and Notation.* München: Oldenbourg Verlag.

Hammer, V., Pordesch, U., & Roßnagel, A. (1993). KORA - eine Methode zur Konkretisierung rechtlicher Anforderungen zu technische Gestaltungsvorschläge für Informations- und Kommunikationssysteme. *Infotech/ I + G* (5.1), S. 21-24.

Hermann, D. (2003). *Using the Common Criteria for IT security evaluation.* Florida: Auerbach-Publications.

Hoffmann, A., Jandt, S., Hoffmann, H., & Leimeister, J. (2011). Integration rechtlicher Anforderungen an soziotechnische Systeme in frühen Phasen der Systementwicklung. *6. Konferenz Mobile ubiquitäre Informationssysteme (MMS).* Kaiserslautern.

Hofmann, J., & Schmidt, W. (2010). *Masterkurs IT-Management: Grundlagen, Umsetzung und erfolgreiche Praxisfür Studenten und Praktiker* (2. Ausg.). Vieweg+Teubner-Verlag.

Hopf, S. (2009). Fragebogen zur Identifikation von Wissensbarrieren in Organisationen. *Dissertation*. Berlin.

Forschungszentrum für Informationstechnik-Gestaltung (2011). Vorschläge zur rechtskonformen Gestaltung selbst-adaptiverAnwendungen.

Kölsch, S. (2004). Geschäftsprozessmodellierung und -optimierung mit Methoden der EPK, Petrinetze und UML. *Manuskript*.

Martin, T., & Bär, T. (2002). *Grundzüge des Risikomanagements nach KonTraG: Das Risikomanagementsystem zur Krisenfrüherkennung nach § 91 Abs. 2 AktG* . München: Oldenbourg-Verlag.

Meyer, M., Zarnekow, R., & Kolbe, L. (2003). IT-Governance. *Wirtschafsinformatik* (45.4), S. 445-448.

Möhring , M., & Vogel, C. (2013). *Geschäftsprozessmodellierung - Eine Einführung für Studierende und Praktiker.* Norderstedt: Books on Demand.

Müller, G., & Accorsi, R. (2013). Why are Busniess Processes Not Secure? *Number Theory and Crypthography* (8260), S. 240-245.

Pfitzmann, A. (2008). Vorlesung: Mehrseitige Sicherheit. Dresden, Wintersemester 2007/08. https://swt.cs.tu-berlin.de/lehre/saswt/ws0708/referate/Mehrseitig.pdf [geprüft von R.G.: 22.Nov. 2014]

Rohloff, M., & Siemens, A. (2003). IT-Governance: Modell und ausgewählte Beispiele für die Umsetzung. *GI-Jahrestagung (1).*

Rupp, C., Hahn, J., Queins, S., Jeckle, M., & Zengler, B. (2005). *UML 2 glasklar - Praxiswissen für die UML-Modellierung und -Zertifizierung* (2. Ausg.). München: Hanser-Verlag.

Schmelzer, H., & Sesselmann, W. (2003). *Geschäftsprozessmanagement in der Praxis* (3. Ausg.). München: Hanser-Verlag.

Schmidt, K. (2009). IT-Security-Management. In E. Tiemeyer, *IT-Manangement - Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis* (S. 489-535). München: Hanser-Verlag.

Schreiber, S. (April 2006). Kosten und Nutzen von Penetrationtests. *HMD - Praxis der Wirtschaftsinformatik*.

Simić-Draws, D. (2013). *Ein Vorgehensmodell zur Durchführung einer prozessorientierten Sicherheitsanalyse.* Koblenz.

von der Maßen, T., & Lichter, H. (2003). Modellierung von Variabilität mit UML Use Cases. *Softwaretechnik Trends* (23).

White, S. A., & Miers, D. (2008). *BPMN modeling and reference guide: understanding and using BPMN*. Future Strategies Inc.

Elektronische Quellen

27001 Academy, 2. (2014). *27001 Academy*. Abgerufen am 13. Oktober 2014 von Was ist ISO 27001?: http://www.iso27001standard.com/de/was-ist-iso-27001/

Bachfeld, D. (14. Dezember 2007). *heise Security*. Abgerufen am 25. September 2014 von Angriff der Karten-Kloner: http://www.heise.de/security/artikel/Angriff-der-Karten-Kloner-270934.html

beck-online: Die Datenbank. (kein Datum). Abgerufen am 10. Oktober 2014 von KonTraG: https://beck-online.beck.de/default.aspx?bcid=Y-100-G-KonTraG

BPM Offensive Berlin. (2011). *BPMN 2.0 - Business Process Model and Notation*. Abgerufen am 19. Oktober 2014 von http://www.bpmb.de/images/BPMN2_0_Poster_DE.pdf

Bundesamt für Sicherheit in der Informationstechnik (2009). *Glossar und Begriffsdefinitionen*. Abgerufen am 6. August 2014 von Glossar und Begriffsdefinitionen: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html

Bundesamt für Sicherheit in der Informationstechnik. (kein Datum). *Zertifizierung und Anerkennung*. Abgerufen am 13. Oktober 2014 von Zertifizierung und Konformitätsbewertung: https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Uebersicht/uebersicht_node.html

Der Tagesspiegel - Polizei & Justiz. (24. Januar 2013). Abgerufen am 25. September 2014 von Diebe fuhren mit Auto in S-Bahnhof: http://www.tagesspiegel.de/berlin/polizei-justiz/geldautomat-gerammt-diebe-fuhren-mit-auto-in-s-bahnhof/7680112.html

Die Welt. (24. September 2012). Abgerufen am 25. September 2014 von Bankräuber sprengen versehentlich Sparkasse: http://www.welt.de/regionales/duesseldorf/article109425256/Bankraeuber-sprengen-versehentlich-Sparkasse.html

Hamburger Abendblatt. (10. Mai 2011). Abgerufen am 25. September 2014 von Tausende Kunden werden an Geldautomat abgezockt: http://www.abendblatt.de/wirtschaft/finanzen/article1884480/Tausende-Kunden-werden-an-Geldautomaten-abgezockt.html

Hornung, G., Skistims, H., & Zirfas, J. (18. März 2013). *P23R - Non-Stop-Goverment*. Abgerufen am 10. Oktober 2014 von Modul 16 – KORA (Konkretisierung rechtlicher Anforderungen): http://mlf.p23r.de/module/modul16-kora/

hr.online.de. (13. Januar 2014). Abgerufen am 25. September 2014 von Mit Auto Geldautomat geknackt: http://www.hr-online.de/website/rubriken/nachrichten/indexhessen34938.jsp?rubrik=36094&key=standard_document_50556719

HvS Consulting. (2014). *HvS Consulting*. Abgerufen am 10. Oktober 2014 von IT-Sicherheit Penetrationtests: http://www.hvs-consulting.de/penetrationstests.aspx

ISACA. (kein Datum). Abgerufen am 10. Oktober 2014 von https://www.isaca.org/Pages/default.aspx

ISO. (kein Datum). Abgerufen am 10. Oktober 2014 von ISO/IEC 20000-2:2005: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41333

IT Governance Instiute. (kein Datum). *IT Governance Instiute*. Abgerufen am 10. Oktober 2014 von About the IT Governance Insistute: http://www.itgi.org/

ITIL. (kein Datum). Abgerufen am 10. Oktober 2014 von Welcome to the official ITIL website: http://www.itil-officialsite.com/

Janssen, S. (22. Dezember 2010). *Stuttgarter-Zeitung.de*. Abgerufen am 25. September 2014 von Cash-Trapping in Stuttgart - Das Bargeld wird abgefangen: http://www.stuttgarter-zeitung.de/inhalt.cash-trapping-in-stuttgart-das-bargeld-wird-abgefangen.672930f5-7918-4f72-8907-31e9c9cd155f.html

ka-news.de. (13. Juni 2011). Abgerufen am 25. September 2014 von Manipulierte Geldautomaten: Karlsruher Polizei gibt Tipps: http://www.ka-news.de/region/karlsruhe/Manipulierte-Geldautomaten-Karlsruher-Polizei-gibt-Tipps;art6066,642868

Karadeniz, B. (2014). *Netplanet*. Abgerufen am 13. Oktober 2014 von Einführung in die Kryptografie: http://www.netplanet.org/kryptografie/einfuehrung.shtml

Keilani, F. (15. September 2013). *Der Tagesspiegel - Berlin*. Abgerufen am 25. September 2014 von Berlin Mitte - Wieder Geldautomat gesprengt:

http://www.tagesspiegel.de/berlin/berlin-mitte-wieder-geldautomat-gesprengt/8793568.html

Kryptowissen.de - Kryptologie, Kryptographie und Kryptoanalyse. (kein Datum). Abgerufen am 13. Oktober 2014 von Kryptografie: http://www.kryptowissen.de/kryptographie.html

Lemme, A., & Wiechers, K. (8. August 2013). *Der Tagesspiegel - Berlin*. Abgerufen am 25. September 2014 von Bankautomaten in Berlin und Brandenburg gesprengt - Polizei knackt Bande der Panzerknacker: http://www.tagesspiegel.de/berlin/bankautomaten-in-berlin-und-brandenburg-gesprengt-polizei-knackt-bande-der-panzerknacker/8614928.html

Martin. (31. März 2008). *Zossen-Blog.de*. Abgerufen am 28. Oktober 2013 von Der Ablauf der Kommunalwahlen: http://www.zossen-blog.de/2008/03/ablauf-kommunalwahl/

Schöpp, C. (2014). *Business Software.* Abgerufen am 26. August 2014 von https://stquickr.fgbas.iwvi.uni-koblenz.de/LotusQuickr/business-software-2014/Main.nsf/0/E2B4751C58BC00D3C1257CD7007FB40B/$file/Class%2003%2013.05.%20BPM%20Process%20modeling%20essentials.pdf?OpenElement&nonce=66D19BA386576EA6C1257D48004F88AE abgerufen

Stoll, S. (18. Oktober 2010). *Nürnberger Nachrichten*. Abgerufen am 25. September 2014 von Wieder eine neue Masche: Diebe fangen Scheine ab: http://www.nordbayern.de/nuernberger-nachrichten/nuernberg/wieder-eine-neue-masche-diebe-fangen-scheine-ab-1.385934

TÜV Süd. (kein Datum). *Managementsysteme*. Abgerufen am 13. Oktober 2014 von ISO 27001: http://www.tuev-sued.de/management-systeme/it-dienstleistungen/iso-27001

TüVIT. (kein Datum). Abgerufen am 18. Oktober 2014 von Common Criteria - Weltweit anerkannte Sicherheitsprüfungen für IT-Produkte: https://www.tuvit.de/de/produkte/common-criteria-447.htm

Wagner, F. (kein Datum). *Gabler Wirtschafslexikon*. Abgerufen am 10. Oktober 2014 von Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG): http://wirtschaftslexikon.gabler.de/Definition/gesetz-zur-kontrolle-und-transparenz-im-unternehmensbereich-kontrag.html

Wege, O., Munde, A., & Albert, M. (3. Juli 2012). *SecuPedia - Die Plattform für Sicherheits-Informationen*. Abgerufen am 18. Oktober 2014 von Common Criteria / ISO15408: http://www.secupedia.info/wiki/Common_Criteria_/_ISO15408

Anhang

Fragenkatalog (Sparkasse Koblenz)

1. Was passiert, wenn die Karte falsch eingeführt wird?
2. Was passiert, wenn eine abgelaufene oder falsche Karte eingeführt wird?
3. Was passiert, wenn die Karte beim Einzug festgehalten wird?
4. Was passiert, wenn das Geld festgehalten wird und nur einzelne Scheine eingezogen werden?
5. Ist die Nachrichtenanzeige über den abzuhebenden Betrag gesetzlich vorgeschrieben (Übereilungsschutz)?
6. Wie lange dauert der Timeout bis die Karte bzw. das Geld eingezogen werden?
7. Wie macht sich der Timeout bemerkbar?
8. Wird das Geld vor der physischen Ausgabe schon dem Geldkonto abgezogen? (Fall: Geld wird durch Timeout wieder eingezogen)
9. Wie ist der genaue Ablauf, wenn der Kunde mehr Geld abheben möchte als er zur Verfügung hat? Ist eine Korrektur möglich oder wird die Karte direkt ausgeworfen?
10. Was passiert mit abgelaufenen Karten anderer Geldinstitute? (Können diese vom Automaten noch gelesen werden? Wird die Karte auch einbehalten?)
11. Wie genau sieht die Gebührenanzeige für Kunden anderer Geldinstitute aus? (Eine Nachricht über die Gebührenerhebung nur am Anfang oder auch später noch bei der Bestätigung?)
12. Thema Vollmachten
    a. Muss der eigentliche Inhaber des Kontos für eine Vollmachterteilung vor Ort in der Filiale sein?
    b. Was erreicht ein Angreifer mit einer gefälschten Vollmacht vor Ort in der Filiale?
    c. Bekommt der eigentliche Inhaber des Kontos Benachrichtigung über die Beantragung einer neuen Karte/PIN durch den Bevollmächtigten?
13. Was wird bei der PIN-Eingabe alles geloggt? (Nachvollziehbarkeit ↔ Vertraulichkeit)

Bisher erschienen (seit 2012)

Davor erschienene Arbeitsberichte, siehe

http://www.uni-koblenz-landau.de/koblenz/fb4/forschung/publications/Reports

Arbeitsberichte aus dem Fachbereich Informatik

Rebecca Bindarra, Lara Fiedler, Nico Merten, Sara West, Paulina Wojciechowska, IT-Sicherheitsanalyse von Geschäftsprozessen am Beispiel der Anwendungen „Kommunalwahlen“ und „Geldauszahlung am Geldautomaten“, Arbeitsberichte aus dem Fachbereich Informatik 4/2016

Heinrich Hartmann, Tim Wambach, Maximilian Meffert, Rüdiger Grimm, A Privacy Aware Mobile Sensor Application, Arbeitsberichte aus dem Fachbereich Informatik 3/2016

Katharina Bräunlich, Rüdiger Grimm, Einfluss von Wahlszenario auf Geheimheit, Privatheit und Öffentlichkeit der Wahl, Arbeitsberichte aus dem Fachbereich Informatik 2/2016

Sebastian Eberz, Mario Schaarschmidt, Stefan Ivens, Harald von Korflesch, Arbeitgeberreputation und Mitarbeiterverhalten in sozialen Netzwerken: Was treibt Social Media Nutzerverhalten im Unternehmenskontext? Arbeitsberichte aus dem Fachbereich Informatik 1/2016

Mario Schaarschmidt, Stefan Ivens, Dirk Homscheid, Pascal Bilo, Crowdsourcing for Survey Research: Where Amazon Mechanical Turks deviates from conventional survey methods, Arbeitsberichte aus dem Fachbereich Informatik 1/2015

Verena Hausmann, Susan P. Williams, Categorising Social Media Business, Arbeitsberichte aus dem Fachbereich Informatik 4/2014

Christian Meininger, Dorothée Zerwas, Harald von Korflesch, Matthias Bertram, Entwicklung eines ganzheitlichen Modells der Absorptive Capacity, Arbeitsberichte aus dem Fachbereich Informatik 3/2014

Felix Schwagereit, Thomas Gottron, Steffen Staab, Micro Modelling of User Perception and Generation Processes for Macro Level Predictions in Online Communities, Arbeitsberichte aus dem Fachbereich Informatik 2/2014

Johann Schaible, Thomas Gottron, Ansgar Scherp, Extended Description oft he Survey on Common Strategies of Vocabulary Reuse in Linked Open Data Modelling, Arbeitsberichte aus dem Fachbereich Informatik 1/2014

Ulrich Furbach, Claudia Schon, Sementically Guided Evolution of SHI ABoxes, Arbeitsberichte aus dem Fachbereich Informatik 4/2013

Andreas Kasten, Ansgar Scherp, Iterative Signing of RDF(S) Graphs, Named Graphs, and OWL Graphs: Formalization and Application, Arbeitsberichte aus dem Fachbereich Informatik 3/2013

Thomas Gottron, Johann Schaible, Stefan Scheglmann, Ansgar Scherp, LOVER: Support for Modeling Data Using Linked Open Vocabularies, Arbeitsberichte aus dem Fachbereich Informatik 2/2013

Markus Bender, E-Hyper Tableaux with Distinct Objects Identifiers, Arbeitsberichte aus dem Fachbereich Informatik 1/2013

Kurt Lautenbach, Kerstin Susewind, Probability Propagation Nets and Duality, Arbeitsberichte aus dem Fachbereich Informatik 11/2012

Kurt Lautenbach, Kerstin Susewind, Applying Probability Propagation Nets, Arbeitsberichte aus dem Fachbereich Informatik 10/2012

Kurt Lautenbach, The Quaternality of Simulation: An Event/Non-Event Approach, Arbeitsberichte aus dem Fachbereich Informatik 9/2012

Horst Kutsch, Matthias Bertram, Harald F.O. von Kortzfleisch, Entwicklung eines Dienstleistungsproduktivitätsmodells (DLPMM) am Beispiel von B2b Software-Customizing, Fachbereich Informatik 8/2012

Rüdiger Grimm, Jean-Noël Colin, Virtual Goods + ODRL 2012, Arbeitsberichte aus dem Fachbereich Informatik 7/2012

Ansgar Scherp, Thomas Gottron, Malte Knauf, Stefan Scheglmann, Explicit and Implicit Schema Information on the Linked Open Data Cloud: Joined Forces or Antagonists? Arbeitsberichte aus dem Fachbereich Informatik 6/2012

Harald von Kortzfleisch, Ilias Mokanis, Dorothée Zerwas, Introducing Entrepreneurial Design Thinking, Arbeitsberichte aus dem Fachbereich Informatik 5/2012

Ansgar Scherp, Daniel Eißing, Carsten Saathoff, Integrating Multimedia Metadata Standarts and Metadata Formats with the Multimedia Metadata Ontology: Method and Examples, Arbeitsberichte aus dem Fachbereich Informatik 4/2012

Martin Surrey,Björn Lilge, Ludwig Paulsen, Marco Wolf, Markus Aldenhövel, Mike Reuthel, Roland Diehl, Integration von CRM-Systemen mit Kollaborations-Systemen am Beispiel von DocHouse und Lotus Quickr, Arbeitsberichte aus dem Fachbereich Informatik 3/2012

Martin Surrey, Roland Diehl, DOCHOUSE: Opportunity Management im Partnerkanal (IBM Lotus Quickr), Arbeitsberichte aus dem Fachbereich Informatik 2/2012

Mark Schneider, Ansgar Scherp, Comparing a Grid-based vs. List-based Approach for Faceted Search of Social Media Data on Mobile Devices, Arbeitsberichte aus dem Fachbereich Informatik 1/2012