Prozessmodell und -analyse für die Stadtrats- und Kommunalwahl 2014 in Koblenz

Daniela Simic-Draws, Katharina Bräunlich

Universität Koblenz-Landau
Fachbereich Informatik
Universitätsstr. 1
56070 Koblenz
{dsimic, braeunlich}@uni-koblenz.de

Abstract: Im Rahmen dieser Arbeit wurde der Ablauf der Stadtratswahl in Koblenz 2014 als Prozessmodell spezifiziert. Dieses Prozessmodell besteht aus vier Teilprozessen: Der Wahlvorbereitung, der Stimmabgabe, der Stimmauszählung und der Wahlnachbereitung. Die Wahlvorbereitung und Stimmauszählung werden bei der genannten Wahl durch elektronische Hilfsmittel unterstützt. Dies ist in Hinblick auf die Diskussion bezüglich des Einsatzes und Umfangs elektronischer Hilfsmittel und deren Rechtmäßigkeit im Kontext von Wahlen interessant. Das hier spezifizierte Prozessmodell kann ein tieferes Verständnis für die komplexen Abläufe der Wahl schaffen, die Nachvollziehbarkeit sowohl für Wahlorganisatoren als auch die Wahlöffentlichkeit verbessern als auch helfen, sicherheitskritische Aspekte aufzudecken und so die Rechtmäßigkeit der eingesetzten elektronischen Hilfsmittel zu bewerten.

1 Einleitung

Am 25. Mai 2014 findet in Koblenz neben der Europawahl auch die Kommunalwahl statt. Die Durchführung dieser Wahl ist aufgrund ihrer Eigenheiten nicht nur für den Bürger, sondern auch für Wahlorganisatoren eine komplexe Angelegenheit. Aus der Perspektive der Wahlorganisatoren sind über den Zeitraum des eigentlichen Wahlvorgangs hinweg komplexe Abläufe erforderlich. Im Rahmen einer Kooperation mit dem Ordnungsamt Koblenz wurde der Ablauf der Stadtratswahl[1] als Prozess modelliert. Dieses Prozessmodell kann nicht nur einer besseren Verständlichkeit der Abläufe für die Wahlorganisatoren dienen, sondern kann auch dem Bürger öffentlich zugänglich gemacht werden und somit zu einer besseren Nachvollziehbarkeit der Wahl gemäß dem Öffentlichkeitsgrundsatz[2] beitragen. Darüber hinaus erlaubt das Prozessmodell eine Untersuchung der Wahlabläufe in Hinblick auf sicherheitskritische Aspekte [Sim14].

Das in diesem Artikel vorgestellte Prozessmodell spezifiziert die Durchführung der Stadtratswahl für die Stadt Koblenz 2014. Es besteht aus vier Teilprozessen: Der Wahlvorbereitung, der Stimmabgabe, der Stimmauszählung und der Wahlnachbereitung.

[1] Die Stadtratswahl ist Bestandteil der Kommunalwahl.
[2] BVerfG: Art 38 Abs. 1 GG i.V.m. Art. 20 Abs. 1, 2 GG

Die Stimmabgabe kann bei der Europa- sowie Kommunalwahl 2014 in Koblenz in Papierform vor Ort (Urnenwahl) oder per Briefwahl erfolgen. Die Erstellung des Wählerverzeichnisses in der Wahlvorbereitung und die Stimmauszählung erfolgen bei der genannten Wahl unter Zuhilfenahme elektronischer Hilfsmittel. Dies erscheint im Zuge der Diskussionen um die Rechtmäßigkeit elektronischer Wahlen[3] und der Einhaltung der Wahlrechtsgrundsätze interessant. Das hier vorgestellte Prozessmodell kann dazu beitragen, sicherheitskritische Aspekte aufzudecken und die Rechtmäßigkeit der eingesetzten elektronischen Hilfsmittel zu bewerten.

Nach [SS08, S. 62] besteht ein Prozess aus einer „Reihe von Aktivitäten, die aus einem definierten Input ein definiertes Ergebnis (Output) erzeugt". Es lassen sich somit auch nicht-wertschöpfende Aktivitätsabfolgen[4] wie beispielsweise in der öffentlichen Verwaltung mit diesem Prozessbegriff fassen. Zur Erhebung und Dokumentation können die aus dem Geschäftsprozessmanagement bekannten Verfahren z. B. nach [Fi06] verwendet werden. Ein Prozess startet i.d.R. mit einer Anforderung, die als Startereignis aufgefasst wird und endet mit der Erfüllung dieser Anforderung. Das Endereignis ist somit das Erreichen des vordefinierten Resultats. Dieses Ergebnis soll innerhalb der gegebenen Anwendungsumgebung erreicht werden. Ein Prozess beschreibt demnach die Interaktion unterschiedlichster Ressourcen (Menschen, IT-Systeme, Informationen, Güter,…) miteinander unter Berücksichtigung vorgegebener Regelwerke[5] zur Erreichung des vorgegebenen Ergebnisses. Die Prozessmodellierung dient der systematischen Dokumentation von Prozessen, welche als Grundlage der Prozessanalyse und -optimierung dient. Ein Prozessmodell erlaubt somit auch die Sicherheitsanalyse sowohl der Prozesse als auch deren Einbettung in die Einsatzumgebung.

Dieser Artikel ist wie folgt gegliedert: Zunächst erfolgt in Abschnitt 2 ein Überblick über verwandte Arbeiten, welche die Spezifizierung von Sicherheitsanforderungen zum Ziel haben. Dabei werden insbesondere prozessorientierte Methoden berücksichtigt. Darüber hinaus werden solche Arbeiten vorgestellt, welche sich mit der Spezifikation von Sicherheitseigenschaften bei elektronischen Wahlen auseinandersetzen. Die Eigenschaften und Besonderheiten von Kommunalwahlen werden anschließend in Abschnitt 3 vorgestellt. In Abschnitt 4 erfolgt dann die Beschreibung und Darstellung eines der IT-gestützten Teilprozesse, die im Rahmen der diesjährigen Kommunalwahl in Koblenz durchlaufen werden: Die Auszählung der Stimmen. Dieser Teilprozess wird in Abschnitt 5 einer Sicherheitsanalyse unterworfen. Der Artikel schließt mit einer Zusammenfassung der Ergebnisse sowie einem Fazit.

[3] Gemäß [Kr02] bezeichnet „e-Voting im Allgemeinen" die elektronisch unterstützte Durchführung mindestens einer der Prozesse Wähleridentifizierung, Stimmabgabe und/oder Stimmauszählung. D.h., es können sowohl der gesamte Wahlablauf als auch nur einzelne Schritte wie Wählerauthentifizierung, Erfassung, Weiterleitung, Speicherung und/oder Auswertung der Stimmen elektronisch erfolgen.

[4] Eine Abgrenzung zwischen Prozess und Geschäftsprozess ist wichtig, da bei letzterem die Anforderungen des und die zu erbringenden Leistungen für den Kunden – repräsentiert durch die wertschöpfenden Tätigkeiten eines Unternehmens – im Fokus stehen. Im Kontext der öffentlichen Verwaltung findet in der Regel keine Transformation in Güter / Dienstleistungen mit höherem Geldwert statt.

[5] Dies umfasst organisationsinterne Regelwerke wie z. B. Prüfungen, Rückkopplungen, Aufteilen von Verantwortlichkeiten etc.; diese können auch Governance Richtlinien entstammen.

2 Verwandte Arbeiten

Sicherheitsanforderungen können mit Hilfe einer Vielzahl unterschiedlicher Methoden spezifiziert werden: Eine international anerkannte und etablierte Methode zur Spezifikation von Sicherheitsanforderungen an IT-Produkte und die Evaluierung dieser IT-Produkte in Hinblick auf die spezifizierten Sicherheitsanforderungen sind die Common Criteria[6] [CC12]. Diese bieten einen umfassenden Katalog an standardisierten funktionalen Sicherheitsanforderungen, welche von einem spezifischen IT-Produkt oder einer generischen Produktgruppe gefordert werden. Die Common Criteria können daher sowohl im Produktentstehungs- als auch im eigentlichen Produktlebenszyklus angewendet werden. Ein Vorgehen, welches speziell für Softwareentwicklungsprojekte konzeptioniert wurde, ist SQuaRE (Security Quality Requirements Engineering) nach [MHS05]. Diese Methode zielt darauf ab, in neun Schritten kategorisierte und priorisierte Sicherheitsanforderungen zu spezifizieren. Ebenfalls eine Anwendung im frühen Stadium der Software-Entwicklung sieht CLASP (Comprehensive Lightweight Application Security Process) nach [Vie05] vor. CLASP liefert eine Systematik in Form von Prozessbausteinen, welche in den regulären Software-Entwicklungs- bzw. Verbesserungsprozess integriert werden können. Dabei werden basierend auf Rollen, Ressourcen und erwarteten Interaktionen korrespondierende Sicherheitsanforderungen abgeleitet. Eine Vorgehensweise, mit der rechtliche Anforderungen in technische Implementierungsvorschläge konkretisiert werden, liefert [HPR93] mit KORA (Konkretisierung rechtlicher Anforderungen). Technische Sicherheitsanforderungen können aufgrund der Zusammenführung juristischen und informatischen Fachwissens systematisch und für beide Seiten nachvollziehbar von den abstrakten rechtlichen Vorgaben abgeleitet werden. In [Sim+13] erfolgt eine Integration von KORA, den Common Criteria und den BSI-Grundschutzkatalogen [BSI11]. Die Sprachmodelle der Common Criteria und des IT-Grundschutz werden hierbei durch das methodische Vorgehen von KORA angereichert und umgekehrt. Die Berücksichtigung sowohl rechtlicher als auch technischer und organisatorischer Aspekte erlaubt somit eine ganzheitliche Sicht auf IT-Sicherheit.

Eine Integration der Prozess- mit der Sicherheitsperspektive wird bereits in einigen Arbeiten thematisiert: Das SLP-Konzept nach [MBH14] basiert auf etablierten Standards und beschreibt deren Zusammenspiel, um sichere Logistikprozesse entwerfen zu können. Die Erweiterung bestehender Notationen zur Geschäftsprozessmodellierung wird von einigen Arbeiten mit jeweils unterschiedlichen Schwerpunkten thematisiert: eine Menge festgelegter Sicherheitsanforderungen wird in Form grafischer Elemente repräsentiert, mit denen bestehende Prozessmodelle annotiert werden wie z. B. in [DK06], [Ci+11] und [Pa+12]. Eine syntaktische Erweiterung der BPMN, indem neue Notationselemente spezifiziert werden, nehmen z. B. [RFP07a], [RFP07b] und [Lo+05] vor. Das Versehen bestehender Notationselemente mit einer neuen Bedeutung im Sinne einer semantischen Erweiterung nehmen z. B. [AMA12] vor.

Im Anwendungsbereich der elektronischen Wahlen existieren zahlreiche Arbeiten, welche sich mit der Spezifikation von Sicherheitseigenschaften beschäftigen:

[6] Die drei Teile der Common Criteria wurden als DIN ISO/IEC 15408-1...3 veröffentlicht.

Anforderungen an elektronische Wahlen bzw. Internetwahlen im Allgemeinen werden z.B. in [CoE04], [VV08] oder [Br+13] adressiert. Bei der prozessorientierten Anforderungsanalyse für elektronische Wahlen wird oftmals der Fokus auf bestimmte Sicherheitsziele wie z.B. Quittungsfreiheit, Verifizierbarkeit oder Wahlgeheimnis gelegt. Diese Sicherheitsziele werden formal spezifiziert. Anschließend kann für ein ebenfalls formal spezifiziertes Produkt bzw. Protokoll die Erfüllung dieser Sicherheitseigenschaft nachgewiesen werden. Dies erfolgt z.B. in [DKR09], [JP06] in Bezug auf das Wahlgeheimnis für Receipt-Freeness und Privacy, z.B. in [KRS10] für Verifizierbarkeit und z.B. in [KR05], [BHM08] für Gleichheit (Fairness) und Wahlberechtigung (Eligibility).

In keiner der genannten Arbeiten wird der gesamte Prozess einer Wahl über alle Wahlphasen hinweg, von Wahlvorbereitung über Stimmabgabe bis hin zur Ergebnisermittlung, unter Einbezug der beteiligten Menschen und ihrer Interessen betrachtet. Diese Arbeiten erlauben somit keine ganzheitliche Schwachstellenanalyse wie die in dieser Arbeit angewandte Vorgehensweise nach [Sim14], auf welche im Abschnitt 5 näher eingegangen wird.

3 Kommunalwahlen

Kommunalwahlen zählen ebenso wie Bundestags- oder Landtagswahlen zu den parlamentarischen Wahlen und unterliegen somit den verfassungsrechtlichen Wahlrechtsgrundsätzen der allgemeinen, freien, gleichen, geheimen, unmittelbaren und öffentlichen Wahl gemäß Art.38 Abs. 1 Satz 1 GG[7] sowie Art. 38 in Verbindung mit 20 Abs. 1 und Abs. 2 GG. Bei Kommunalwahlen werden beispielsweise Gemeinde-, Stadt- oder Landräte oder in der Direktwahl Bürgermeister gewählt. Im föderalistischen System der Bundesrepublik Deutschland ist das Kommunalwahlrecht Landesrecht. Die genaue Ausgestaltung von Kommunalwahlen kann sich daher von Bundesland zu Bundesland unterscheiden[8]. Da diese Arbeit sich mit der Kommunal- und Stadtratswahl der Stadt Koblenz in 2014 beschäftigt, beziehen sich die nachfolgenden Erläuterungen auf das Kommunalwahlrecht in Rheinland-Pfalz wie es durch das Kommunalwahlgesetz [KWG94] des Landes Rheinland-Pfalz festgeschrieben ist. Die Kommunalwahl in Rheinland-Pfalz ist eine Verhältniswahl mit offenen Listen. Bei der Verhältniswahl erhält eine Partei entsprechend ihrem Stimmanteil Mandate.[9] Die Wahllisten werden in der Regel durch die Parteien aufgestellt. Da die Parteien bei der Zusammenstellung der Wahllisten nicht auf Parteimitglieder beschränkt sind, spricht man von offenen Listen. Die Anzahl der zu vergebenden Stimmen ist hierbei abhängig von der Zahl der zu vergebenden Sitze [KWG94, §32]. Des Weiteren erlaubt das KWG von Rheinland-Pfalz das Kumulieren und Panaschieren (vgl. §32 Sätze 3 und 4). Kumulieren bezeichnet die Möglichkeit, einem Kandidaten mehrere Stimmen geben zu können, um so dessen

[7] Grundgesetz

[8] Unterschiede bestehen z. B. hinsichtlich dem aktiven / passiven Wahlalter (18/18), der Wahlperiode (5 Jahre), dem Sitzzuteilungsverfahren (Hare/Niemeyer), der Listenform (offen) und der Anzahl an Stimmen (Zahl der zu vergebenden Sitze) – vgl. dazu [KWG94].

[9] Im Gegensatz dazu wird das Wahlgebiet bei Mehrheitswahlen entsprechend der zu vergebenen Mandate in Wahlkreise eingeteilt. Das Mandat erhält dann der Kandidat mit den meisten Stimmen in seinem Wahlkreis.

Position innerhalb der Wahlliste zu stärken. Panaschieren beschreibt das Verteilen mehrerer verfügbarer Stimmen durch den Wähler auf Kandidaten von unterschiedlichen Wahllisten [Br+13].
Das in diesem Artikel vorgestellte Prozessmodell spezifiziert die Durchführung der Stadtratswahlen in Koblenz 2014. Die Stadtratswahl folgt den oben aufgeführten Reglementierungen der Kommunalwahl.

4 Prozessmodell für die Stadtratswahl 2014 in Koblenz

Im Rahmen einer Kooperation mit dem Ordnungsamt Koblenz wurde der gesamte Ablauf der Stadtratswahl 2014 für die Stadt Koblenz als Prozess modelliert. Im Folgenden wird ein Auszug aus diesem Prozessmodell vorgestellt. Dabei liegt der Fokus auf einem der beiden IT-gestützten Teilprozesse, nämlich der elektronisch unterstützten Stimmauszählung[10]. Dieser Teilprozess wird nachfolgend hinsichtlich seines Ist-Zustandes beschrieben. Eine Analyse hinsichtlich sicherheitskritischer Aspekte erfolgt in Abschnitt 5.

Das Kumulieren und Panaschieren steht häufig in der Kritik, die Stimmabgabe zu verkomplizieren und so als Fehlerquelle für ungewollt ungültige Stimmzettel bei der Stimmabgabe durch den Wähler sowie als Fehlerquelle bei der Stimmauszählung zu dienen. Bei der Kommunalwahl in Koblenz werden für die 76 Stimmbezirke und Briefwahlbezirke über 900 Mitglieder des Wahlvorstandes an der Auszählung beteiligt sein. Bei diesen handelt es sich überwiegend um juristische Laien. Hierbei besteht z.B. die Gefahr, dass falsch ausgefüllte Stimmzettel nicht gesetzeskonform erfasst oder unterschiedlich interpretiert werden. Zudem müssen die ermittelten Stimmen mit Hilfe eines Sitzzuteilungsverfahrens in die Abgeordnetensitze umgerechnet werden, was manuell recht langwierig ist. Dies könnten Gründe sein, warum in Koblenz (wie in vielen anderen Kommunen auch) die Stimmauszählung unter Zuhilfenahme elektronischer Hilfsmittel durchgeführt wird.

Im Rahmen der Kommunalwahl Koblenz wurde vom Landeswahlleiter Rheinland-Pfalz das Stimmenauszählungs-Programm „PC Wahl“ (genauer: die Module „Heiler“ und „Berechnung der Sitzverteilung“) der Berninger Software GmbH freigegeben[11]. Die Freigabe erfolgt gemäß [KWO83, §55a] und umfasst bspw. die algorithmisch korrekte Implementierung der juristisch vorgegebenen Heilungsvorschriften[12].

[10] Die elektronisch unterstützte Erstellung des Wählerverzeichnisses wird hier nicht weiter betrachtet.
[11] http://www.wahlen.rlp.de/kw/bek/20140212_Bekanntmachung_Freigabe_PCWahl_Staatsanzeiger.pdf (Abrufdatum: 01.04.2014)
[12] Beispiel: Laut KWG können für einen Kandidaten max. drei Stimmen vergeben werden. Vergibt ein Wähler nun sechs Stimmen an einen Kandidaten, so wird der Stimmzettel nicht ungültig, sondern er wird bei der Erfassung „geheilt“. Das heißt, der Stimmzettel wird 1:1 mit den betreffenden sechs Stimmen erfasst, es fließen aber nur drei dieser Stimmen in die Berechnung mit ein (vgl. §37 (3) KWG).

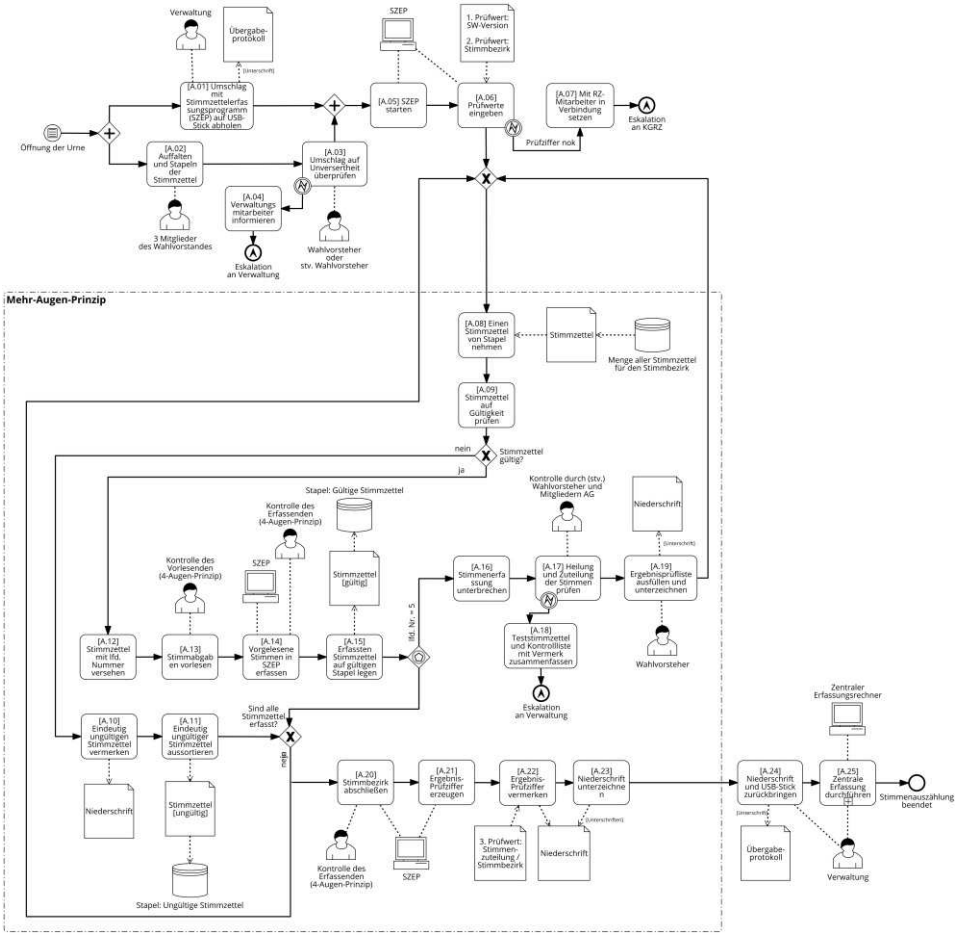

Abbildung 1: Die elektronisch unterstützte Ergebnisermittlung als Prozessverlauf

Die Auszählung[13] beginnt bei dem vorliegenden Teilprozess mit der Öffnung der Urne an dem Tag nach der Wahl durch den Wahlvorsteher[14]. Die Stimmzettel werden von drei Mitgliedern des Wahlvorstandes zunächst aufgefaltet und gestapelt. Ein weiteres Mitglied des Wahlvorstands lässt sich den USB-Stick mit dem Stimmzettelerfassungsprogramm (SZEP) von Mitarbeitern der Verwaltung aushändigen. Dieser Vorgang wird in einem Übergabeprotokoll festgehalten (Name, Funktion der Person). Bevor der Umschlag geöffnet und der Datenträger durch den Wahlvorsteher

[13] Die Ausstattung und Lage der Arbeitsplätze zur Auszählung je Stimmbezirk sind in der „Dienstanweisung für den Einsatz von Personal-Computern“ geregelt.

[14] Die Urnen inklusive der begleitenden Dokumente wurden zuvor durch zwei Mitarbeiter der Verwaltung von den einzelnen Wahllokalen in die Rhein-Mosel-Halle transportiert. Dort wurden die Urnen über Nacht unter Bewachung durch ein privates Sicherheitsunternehmen verwahrt. Die Schlüssel für die Urnen befinden sich währenddessen in Besitz des jeweiligen Wahlvorstehers.

oder dessen Stellvertreter entnommen wird, ist der Umschlag auf seine Unversehrtheit zu überprüfen[15]. Sind Beschädigungen zu erkennen, dann muss die Verwaltung informiert und der Datenträger ausgetauscht werden.

Das Einlesen der Stimmzettel erfolgt gesondert für jeden Wahlbezirk auf Stand-Alone-Rechnern. Das Software-Modul „Heiler“ ist wahlbezirksspezifisch und wird direkt vom USB-Stick gestartet. Bevor Stimmen erfasst werden können, müssen zwei Prüfziffern (PZ) eingegeben werden. Die erste PZ garantiert die Verwendung der freigegebenen Programmversion. Die zweite PZ stellt den korrekten Wahlbezirk sicher. Die Bedienung erfolgt durch die sogenannte Arbeitsgruppe, welche sich als Teilmenge aus dem sechsköpfigen Wahlvorstand bildet und gemäß [KWO83, §55b] aus mindestens drei Personen besteht.

Initial wird die korrekte Erfassung der Stimmzettel getestet: Dazu werden die ersten fünf Stimmzettel im Programm erfasst. Anschließend prüft die Arbeitsgruppe im Beisein des Wahlvorstehers, ob das SZEP die Heilung und Zuteilung der Stimmen korrekt durchführt[16]. Das Ergebnis des Testlaufs wird in der Niederschrift dokumentiert und vom Wahlvorsteher unterschrieben. Anschließend erfolgt die Erfassung der restlichen Stimmzettel. Eindeutig ungültige Stimmzettel nach §37 KWG werden von der Arbeitsgruppe aussortiert und im Protokoll vermerkt. Diese werden nicht elektronisch erfasst. Alle anderen Stimmzettel werden von einem Mitglied der Arbeitsgruppe laut vorgelesen und von einem zweiten Mitglied in identischer Form in das SZEP übernommen. Sowohl der „Vorlesende“ als auch der „Erfasser“ werden durch je eine Person kontrolliert. Sowohl der Papierstimmzettel als auch sein digitales Äquivalent werden mit einer laufenden Nummer versehen. Damit kann jeder im SZEP erfasste Stimmzettel im Nachhinein mit dem Original verglichen werden (Nachvollziehbarkeit). Nach der Erfassung des letzten Stimmzettels erfolgt die abschließende Speicherung der Stimmauszählung. Dieser Vorgang erzeugt die dritte Prüfziffer – die sog. Ergebnisprüfziffer, welche auf der Niederschrift vermerkt wird. Diese Prüfziffer garantiert die Integrität der erfassten Ergebnisse. Die Ergebnisse der jeweiligen Wahlbezirke werden mittels USB-Sticks von dem Wahlvorsteher zur zentralen Erfassung an Mitarbeiter der Verwaltung übergeben. Die zentrale Erfassung erfolgt an einem separaten Rechner, welcher mit dem Internet verbunden ist. Die Mitarbeiter der Verwaltung nehmen die Wahlniederschrift inklusive aller begleitenden Dokumente und den USB-Stick entgegen und protokollieren den Erhalt dieser Dokumente.

[15] Gemäß Bescheid über die Freigabe des Stimmenauswertungsprogramms des Landeswahlleiters, vgl. http://www.wahlen.rlp.de/kw/bek/20140212_Bekanntmachung_Freigabe_PCWahl_Staatsanzeiger.pdf (Abrufdatum: 16.04.2014)

[16] Endet der Testlauf nicht wie erwartet, erfolgt eine Meldung an die Verwaltung. Es werden dann sowohl die Teststimmzettel als auch das Kontrolldatenblatt mit einem entsprechenden Vermerk der Wahlniederschrift beigefügt. Die Verwaltung nimmt anschließend eine Überprüfung in eigener Zuständigkeit vor. Dieser Vorgang wird an den Wahlausschuss berichtet.

5 Identifikation sicherheitskritischer Aspekte

Im Folgenden wird der im vorherigen Abschnitt beschriebene Teilprozess bezüglich der Stimmauszählung hinsichtlich sicherheitskritischer Aspekte nach der in [Sim14] beschriebenen Vorgehensweise analysiert. Die Strukturierung der nachfolgenden Unterabschnitte orientiert sich an den Arbeitsschritten der verwendeten Methodik.

5.1 Zieldefinition

Zunächst erfolgt eine informelle Festlegung der zu betrachtenden Problemstellung. Diese sollte einen Prozess (d.h. eine zu erfüllende Anforderung) adressieren und kann z. B. für Interessenkonflikte oder einzelne Sicherheitsaspekte konkretisiert werden. Für den zu untersuchenden Teilprozess könnte sie lauten: „An welchen Stellen kann der elektronisch unterstützte Auszählungsvorgang durch die am Prozess beteiligten Personen gefährdet sein?“.

5.2 Modellierung des Prozesses

Sobald der Untersuchungsgegenstand festgelegt worden ist, wird der zu betrachtende Prozess z. B. im Rahmen von Prozessworkshops erarbeitet und modelliert. Der dem Teilprozess zugrunde liegende Hauptprozess („Durchführung der Stadtratswahl Koblenz 2014“) wurde in Zusammenarbeit mit dem Ordnungsamt Koblenz auf Basis eines Referenzprozessmodells konkretisiert. Die detaillierte Erfassung des Teilprozesses erfolgte anschließend mit Hilfe von Experteninterviews.

5.3 Identifikation der globalen Interessenlagen

Anschließend werden für den zu untersuchenden Prozess die globalen Interessenlagen[17] der beteiligten Anwender sowie eines potenziellen externen Angreifers erfasst. Stark abstrahiert sind vier Fälle möglich:

- Es existiert kein externer Angreifer und die Prozessbeteiligten agieren regelkonform.
- Die Prozessbeteiligten agieren regelkonform; ein externer Angreifer versucht das Prozessziel zu manipulieren[18].
- Es findet ein Kompromittieren des Prozesses durch einen oder Kooperation mehrerer interner Angreifer statt.
- Es findet eine Kooperation zwischen Innen- und Außentäter statt.

An dem zu betrachtenden Teilprozess (Auszählung der Stimmen) sind die sechs Mitglieder des Wahlvorstands sowie optionale Hilfspersonen beteiligt. Der betrachtete Prozess ist solange nicht gestört, wie die Interessen der Beteiligten in der regelkonformen Auszählung der Stimmen bestehen. Umgekehrt kann der Prozessverlauf

[17] Die „globale Interessenlage“ bezieht sich auf den Hauptprozess; eine „lokale Interessenlage“ ist spezifisch für einen Teilprozess bzw. eine Aktivität. Globale und lokale Interessenlagen unterscheiden sich hinsichtlich ihres Abstraktionsgrades (global = „Manipulation der Wahl“ vs. lokal = „Manipulation bei der Auszählung“).
[18] Für diese Untersuchung ist die Motivation der unterschiedlichen Interessenlagen nicht von Bedeutung.

gestört werden, sobald einer oder mehrere der am Prozess Beteiligten versuchen, ihre eigenen Interessen durchzusetzen. Beispielsweise könnte ein Mitglied des Wahlvorstands bestochen worden sein, Stimmen für einen bestimmten Kandidaten zu unterschlagen. Die auf den Interessenkonflikten von Innentätern basierenden Bedrohungen, welche den Prozessverlauf stören, wurden mittels einer Analyse der Aktivitäten identifiziert.

5.4 Zerlegung des Prozessmodells

Da das Abstraktionsniveau des erfassten Hauptprozesses zu groß ist und daher detaillierte Abläufe noch nicht sichtbar sind, erfolgt zunächst dessen Zerlegung in Teilprozesse. Der im Rahmen dieser Arbeit zu untersuchende Teilprozess wird weiter zerlegt, bis dass die einzelnen durchzuführenden Aufgaben ersichtlich werden. Diese werden als Aktivitäten bezeichnet und stehen für die kleinstmöglichen Elemente von Prozessen. Sie haben den Charakter von Handlungsanweisungen. Beispielsweise ergibt sich aus dem Hauptprozess „Durchführung der Stadtratswahlen Koblenz 2014“ u.a. der Teilprozess „Wahlergebnis ermitteln“. Dort wird die elektronische Erfassung der Stimmzettel als Aktivität modelliert. Bei genauerer Betrachtung kann diese als weiterer Unterprozess mit den entsprechenden Aktivitäten modelliert werden. Was als Aktivität oder Sub-Prozess aufgefasst wird, ist also abhängig von der Zieldefinition. Der im Folgenden zu untersuchende Teilprozess wurde in Abschnitt 4 modelliert und detailliert erläutert.

5.5 Aktivitätsanalyse

Zunächst wird jede Aktivität unter Berücksichtigung der angebundenen Prozessbausteine wie beteiligte Rollen (hier: Wahlvorstand, Verwaltung), verwendete IT-Systeme (hier: SZEP auf USB-Stick, Desktop-PC, netzwerkfähiger zentraler Erfassungsrechner), Datenobjekte (hier: Stimmzettel, Protokolle) etc. beschrieben. Für jede Aktivität wurden mögliche Bedrohungen[19] in abstrahierter Form identifiziert (vgl. Tab. 1). Diese richten sich gegen das Prozessziel (global) bzw. davon abgeleitet auf das Aktivitätsziel (lokal) und basieren auf den in 5.3 identifizierten Interessenkonflikten.

Bedrohung [B.n]	**Aktivität [A.n]**
[B.01]: Umschlag mit USB-Stick (SZEP) wird durch Mitglied des Wahlvorstands oder Verwaltungsmitarbeiter unterschlagen	[A.01], [A.24]
[B.02]: Umschlag mit USB-Stick (SZEP) wird durch Mitglied des Wahlvorstands oder Verwaltungsmitarbeiter manipuliert	[A.01], [A.24]

[19] Eine Abgrenzung der Begriffe Bedrohung, Angriffstechnik und Angriff wird in [Gr+14] vorgenommen.

[B.03]: Unterschlagen von Stimmzetteln („löschen“)	[A.02], [A.08], [A.09], [A.10], [A.11], [A.12], [A.13], [A.14], [A.15], [A.24]
[B.04]: Hinzufügen von Stimmzetteln	[A.02], [A.08], [A.09], [A.10], [A.13], [A.14], [A.15], [A.24]
[B.05]: Manipulation bestehender Stimmzettel (Kreuz hinzufügen, Streichung vornehmen, ungültig markieren, falsche lfd. Nr., etc.)	[A.02], [A.08], [A.12], [A.13], [A.14], [A.15], [A.24]
[B.06]: Bewusste Falschmeldung vornehmen (Anwender)[20]	[A.03], [A.17], [A.19], [A.20], [A.22], [A.23]
[B.07]: Unterschlagen einer erforderlichen Meldung (Anwender)[21]	[A,03], [A.17], [A.19], [A.20], [A.22], [A.23]
[B.08]: Nicht freigegebene Software wird verwendet	[A.05], [A.25]
[B.09]: Das System gibt fälschlicherweise eine Fehlermeldung aus	[A.06], [A.14], [A.20], [A.21], [A.25]
[B.10]: Das System gibt fälschlicherweise keine Fehlermeldung aus	[A.06], [A.14], [A.20], [A.21], [A.25]
[B.11]: SZEP erzeugt falsche Prüfziffer	[A.21]

Tabelle 1: Bedrohungen (abstrahiert), welche die Auszählung beeinflussen können; ohne Berücksichtigung eingesetzter Sicherheitsmaßnahmen

Die von den Prozessbeteiligten durch ihre Interessenkonflikte verursachten Bedrohungen und zu deren Vermeidung getroffene Maßnahmen sollen nachfolgend betrachtet werden:

[B.01] Umschlag mit USB-Stick (SZEP) wird durch Mitglied des Wahlvorstands oder Verwaltungsmitarbeiter unterschlagen: Die Abholung des Umschlags mit dem SZEP erfolgt durch ein Mitglied des Wahlvorstands. Dieses Mitglied hat die Möglichkeit, den Umschlag verschwinden zu lassen bzw. am Auszählungsplatz dessen Erhalt zu bestreiten. Ein Erfolg dieses Angriffs ist nicht gegeben, da bei Bedarf jederzeit ein neuer stimmbezirksspezifischer USB-Stick erstellt werden kann. Ferner wird die Abholung durch die Mitarbeiter der Verwaltung protokolliert, so dass ein Verlust durch den Abholenden ihm zugerechnet werden kann. Bei einem Unterschlagen durch die ausgebende Stelle ist das Ziel fraglich. In diesem Fall würde der abholende Wahlhelfer auf Ausgabe des Umschlages beharren und gegebenenfalls existierende Möglichkeiten

[20] Resultiert in der Verzögerung des Prozessablaufs z. B. indem fälschlicherweise behauptet wird, dass der ausgegebene Umschlag beschädigt gewesen sei oder indem eine falsche Unterschrift vorgenommen wird.
[21] Entspricht dem Gegenteil von [B.07], da hier der Prozessverlauf bewusst kompromittiert wird, z. B. aufgrund von Mitwisserschaft oder auch, um den Prozess zu verzögern (fehlende Unterschrift).

der Eskalation wahrnehmen. Auch eine Kooperation beider wäre nicht zielführend, da in diesem Falle die anderen Mitglieder der Arbeitsgruppe intervenieren könnten.

[B.02] Umschlag mit USB-Stick (SZEP) wird durch Mitglied des Wahlvorstands oder Verwaltungsmitarbeiter manipuliert: Der Austausch des Umschlags ist durch den Verwaltungsmitarbeiter oder durch den Abholenden auf dem Weg von der Ausgabestelle bis zum Auszählungsplatz möglich. Ein Austausch impliziert einen vorbereiteten Angriff; d.h. es wurde ein nicht authentisches oder manipuliertes SZEP bereits im Vorfeld auf einem USB-Stick installiert. Dieser sollte von seiner äußeren Beschaffenheit so sein, dass er einer visuellen Prüfung standhält. Gleiches gilt für den Umschlag, damit die Integritätsprüfung durch den Wahlvorstand erfolgreich ist. Dieser Angriff schlägt fehl, sobald der Abgleich mit der öffentlich bekanntgegebenen Prüfziffer am Arbeitsplatz erfolgt. Auch eine Kooperation beider Akteure ist nicht zielführend, so lange der Abgleich der Prüfziffer innerhalb der Arbeitsgruppe korrekt erfolgt.

[B.03] Unterschlagen von Stimmzetteln („löschen"): Das Löschen von Stimmzetteln betrifft sowohl Papier- als auch elektronische Stimmzettel. Papierstimmzettel könnten z. B. für ungültig erklärt werden, obwohl sie gültig sind. Es ist auch denkbar, dass die Erfassung bewusst unterbleibt. Ebenso ist es nach der Auszählung und dem Abschließen des Stimmbezirks möglich, Stimmzettel zu löschen. Die genannten Angriffe werden mit Ausnahme der systemseitigen Löschung durch das Mehr-Augen-Prinzip unterbunden. Die Manipulation der elektronischen Auszählungsergebnisse wird bei der zentralen Konsolidierung aufgedeckt: Nach Abschluss des Stimmbezirks wird eine Prüfziffer generiert, die auf der Wahlniederschrift erfasst wird. Eine nachträgliche Änderung der Ergebnisse ist möglich; diese resultiert aber in einer neuen Prüfziffer. Da bei der zentralen Erfassung die Prüfziffern abgeglichen werden, wird an dieser Stelle eine Manipulation auffallen.

[B.04] Hinzufügen von Stimmzetteln: Das Hinzufügen von Papierstimmzetteln ist dann möglich, wenn am Ort der Auszählung nicht verwendete Stimmzettel verfügbar sind. Der Angriff kann als besonders erfolgreich gewertet werden, wenn der Angreifer zusätzlich Zugang zu dem Auszug des Wählerverzeichnisses hat und er zu nachträglich ausgefüllten Stimmzetteln einen entsprechenden Vermerk machen kann. Das Hinzufügen elektronischer Stimmzettel ist ebenfalls möglich; bei nachträglicher Kontrolle wird aber das Fehlen der korrespondierenden Papierstimmzettel auffallen. Beide Angriffe sind aufgrund des Mehr-Augen-Prinzips zu vernachlässigen. Eine Nacherfassung ist aufgrund der unter [B.03] genannten Aspekte nicht durchsetzbar.

[B.05] Manipulation bestehender Stimmzettel: Im Gegensatz zu [B.04] gestaltet es sich wesentlich einfacher, bestehende Stimmzettel ungültig zu markieren bzw. nicht vergebene Stimmen nachträglich zu verteilen. Dies gilt sowohl für Papier- als auch für elektronische Stimmzettel. Auch hier unterbinden das Mehr-Augen-Prinzip sowie die Kontrolle der Prüfziffern bei der Erfassung den Erfolg dieses Angriffs.

[B.06] Bewusste Falschmeldung vornehmen (Anwender): Diese Bedrohung ist nicht sicherheitsrelevant, da sie lediglich in einer Verzögerung des Prozesses resultiert. Würde z. B. fälschlicherweise ein beschädigter Umschlag gemeldet werden, so würde der

Prozess solange stoppen, bis dass ein Ersatz-USB-Stick generiert und ausgegeben wird. Gleiches gilt für falsche Unterschriften – sofern eine solche auffällt bzw. gemeldet wird, liegt es im Ermessen der Verwaltung, wie mit einem solchen Fall umgegangen wird. Eine Neuzählung ist in solchen Fällen nicht zu erwarten.

[B.07] Unterschlagen einer erforderlichen Meldung (Anwender): Im Gegensatz zu [B.06] ist diese Bedrohung sicherheitsrelevant. Z. B. wird im Rahmen der Integritätsprüfung festgestellt, dass der ausgegebene Umschlag beschädigt ist und dieser Umstand würde nicht eskaliert. Dann würde die Verwendung des manipulierten SZEP bei dem Abgleich der Prüfziffern auffallen. Auch ist es denkbar, dass die Aufzeichnung der Prüfziffer auf der Niederschrift nach Abschluss des Stimmbezirks bewusst unterbleibt, um eine Nacherfassung von Stimmen zu forcieren. Zur Vermeidung solcher bewussten und unbewussten Unterlassungen dient das Mehr-Augen-Prinzip.

[B.08] Nicht freigegebene Software wird verwendet: Bei dieser Bedrohung für [A.05] und [A.25] relevanten Bedrohung müssen zwei Fälle unterschieden werden. Im ersten Fall handelt es sich um eine versehentliche Herausgabe einer nicht freigegebenen Software-Version bzw. den Versuch, das freigegebene SZEP („Heiler"-Modul) durch ein anderes Programm oder eine nicht-freigegebene Version zu ersetzen, um so die Stimmerfassung zu manipulieren (vgl. [B.02]). Durch den Abgleich der Prüfziffer werden beide Ereignisse bei der Arbeitsgruppe auffallen. Weiterhin kann es sich bei dieser Bedrohung um den Versuch handeln, das Software-Modul „Berechnung der Sitzverteilung" zu manipulieren bzw. durch ein anderes Programm zu verwenden. Dieser Fall ist als kritisch anzusehen. Dieses Software-Modul läuft auf einem zentralen Netzwerkrechner, und dient der Zusammenführung der Ergebnisse aus den einzelnen Wahlbezirken. Diese Teilergebnisse werden mittels USB-Stick vom Wahlvorstand des jeweiligen Wahlbezirks an Mitarbeiter der Verwaltung übergeben und vom USB-Stick auf dem zentralen Rechner eingelesen und zur Ermittlung der finalen Sitzverteilung mittels Software ausgewertet. Ein manipuliertes Programm würde es somit ermöglichen, das Wahlergebnis zu verändern. Sollte dies durch keine weiteren Sicherheitsmaßnahmen abgesichert sein (z.B. Prüfziffer für freigegebene Programmversion, Testlauf zur Überprüfung der korrekten Funktionsweise der Berechnung), bliebe diese Manipulation unbemerkt.

Die Funktionalität der verwendeten Software wird von den Bedrohungen **[B.09] – [B.11]** adressiert. Diese Bedrohungen müssen im Vorfeld durch eingehende und fachmännische Analyse der zu verwendenden Software ausgeschlossen werden, so dass diese Bedrohungen für die freigegebene Softwareversion ausgeschlossen werden können.

6 Fazit

Im Rahmen einer Kooperation mit der Stadt Koblenz wurde die Stadtratswahl 2104 modelliert und analysiert. Dieses Prozessmodell spezifiziert vier Teilprozesse: Wahlvorbereitung, Stimmabgabe, Stimmauszählung und Wahlnachbereitung. Von diesen vier Teilprozessen werden die Prozesse der Wahlvorbereitung und der Stimmauszählung mittels elektronischer Hilfsmittel unterstützt. Hier wurde exemplarisch

der Teilprozess der Stimmauszählung detailliert spezifiziert und hinsichtlich sicherheitskritischer Aspekte analysiert. Dabei wurde methodisch in Anlehnung an [Sim14] vorgegangen.

Die in Abschnitt 5 beschriebene Prozessanalyse identifiziert eine Menge von möglichen Bedrohungen. Es zeigt sich jedoch, dass diese Bedrohungen durch organisatorische Sicherheitsmaßnahmen wie dem Mehr-Augen-Prinzip weitestgehend ausgeschlossen bzw. deren Risiko hinreichend minimiert werden können. Voraussetzung ist hier jedoch, dass innerhalb der Mehr-Augen-Gruppe mindestens ein Mitglied integer ist. Die Eingabe der Stimmzettel erfolgt beispielsweise so, dass eine Person den Stimmzettel vorliest und dabei durch eine weitere Person kontrolliert wird. Um die Integrität des Ergebnisses garantieren zu können, muss demnach entweder der Vorlesende oder der diesen Kontrollierende integer sein, besser noch beide. Dieser Zusammenhang lässt sich formal mittels des sogenannten k-Resilience Term ausdrücken [VG09]. Die Formulierung des k-Resilience Terms anhand des Prozessmodells ist ein Anknüpfungspunkt für zukünftige Arbeiten.

Als sicherheitskritisch konnte die Berechnung der Sitzverteilung auf dem zentralen Netzwerkrechner identifiziert werden (Aktivität [A.25] in Abb.1). Hier ist unklar, ob von Seiten der Wahlorganisatoren weitere Sicherheitsmaßnahmen ergriffen werden, um die ausschließliche Verwendung der freigegebenen Software-Version sicherzustellen, und ob Test- und/oder Kontrollroutinen existieren, um deren korrekte Funktionsweise zu gewährleisten. Hier besteht nach Meinung der Autoren sowohl wegen der Anbindung des Rechners an das Internet und der damit verbundenen Bedrohung durch einen externen Netzwerkangreifer sowie des Black-Box-Charakters der Berechnung das größte Manipulationspotenzial.

Weiterhin erfolgte die Prozessanalyse im Rahmen dieses Artikels nur auszugsweise für den Teilprozess der Stimmauszählung. Im Rahmen der Kooperation mit der Stadt Koblenz wurde jedoch der gesamte Ablauf der Stadtratswahl modelliert und analysiert. Hier zeigt sich, dass über den gesamten Prozess gesehen die öffentliche Nachvollziehbarkeit nicht durchgängig gewährleistet werden kann. Die Stimmabgabe sowie die Stimmauszählung sind in vollem Maße öffentlich nachvollziehbar. Die verschlossenen Urnen und die in der Urne enthaltene Wahlniederschrift werden von zwei Verwaltungsmitarbeitern gegen 18:00 Uhr am Wahltag vom Wahllokal in die Rhein-Mosel-Halle transportiert. Dort werden die Urnen zentral unter Bewachung durch eine private Sicherheitsfirma bis zur Auszählung am darauffolgenden Tag verwahrt. In diesem Zeitfenster ist keine öffentliche Kontrolle möglich. Das Öffnen der Urnen und der Austausch des Inhalts (abgegebene Stimmen und/oder Wahlniederschrift) wären demnach nicht erkennbar, insofern die Urne vor Abtransport aus dem Wahllokal nicht erneut versiegelt würde. Weiterhin könnte ein derartiger Angriff den Ausgang der gesamten Wahl beeinflussen. Dies wäre ein Angriff der unabhängig von dem Einsatz elektronischer Hilfsmittel rein auf Grund der Ablauforganisation erfolgen könnte, allerdings wie bei vollständig elektronisch durchgeführten Wahlen auf das gesamte Wahlergebnis skalieren. Hier wären weitere organisatorische Sicherheitsmaßnahmen oder eine Umstrukturierung innerhalb des Prozessablaufes zu diskutieren.

Abschließend lässt sich feststellen, dass das hier auszugsweise vorgestellte Prozessmodell das Verständnis für die komplexen Abläufe der Wahl vertieft und dazu beiträgt, sicherheitskritische Punkte zu identifizieren.

Literaturverzeichnis

[AMA12] Altuhova, O.; Matulevičius, R.; Ahmed, N.: Towards Definition of Secure Business Processes. LNBIR: Workshop on Information Systems Security Engineering, 1-15, 2012.

[BHM08] Backes, M.; Hritcu, C.; Maffei, M.: Automated verification of remote electronic voting protocols in the applied pi-calculus. CSF, pages 195-209, 2008.

[Br+13] Bräunlich, K.; Grimm, R.; Richter, P., Roßnagel, A.: Sichere Internetwahlen - Ein rechtswissenschaftlich- informationstechnisches Modell, Nomos-Verlag, 2013.

[BSI11] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzkataloge. Bundesanzeiger-Verlag, Köln, 12. Ergänzungslieferung, 2011.

[CC12] Common Criteria and Common Evaluation Methodology, Version 3.1, 2012.

[Ci+11] Ciuciu, I.; Zhao, G.; Mülle, J.; von Stackelberg, S.; Vasquez, C.; Haberecht, T.; Meersman, R.; Böhm, K.: Semantic Support for Security-Annotated Business Process models. LNBIP, Vol. 81, 284-298, 2011.

[CoE04] Council of Europe: Legal, Operational and Technical Standards for e-voting, recommendation rec(2004)11 adopted by the Committee of Ministers of the Council of Europe and Explanatory Memorandum. Strasbourg, 2004.

[DK06] Dzhendova, G.; Kalmring, D.: Modellierung von IT-Sicherheit. Analyse und Synthese. Proc. DACH Security, 2006.

[DKR09] Delaune, S., Kremer, S., & Ryan, M.: Verifying privacy-type properties of electronic voting protocols. Journal of Computer Security, 17(4):435-487, 2009.

[Fi06] Fischermanns, G.: Praxishandbuch Prozessmanagement. 6. Auflage, Verlag Dr. Götz Schmidt, Gießen, 2006.

[Gr+14] Grimm, R.; Simić-Draws, D.; Bräunlich, K.; Kasten, A.; Meletiadou, A.: Referenzmodell für ein Vorgehen bei der IT-Sicherheitsanalyse. Zur Veröffentlichung angenommen in: Informatik Spektrum 2014.

[HPR93] Hammer, V.; Pordesch, U.; Roßnagel, A.: KORA. Eine Methode zur Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlägen für Informations- und Kommunikationssysteme. Infotech 1/1993, S. 21ff, 1993.

[JP06] Jonker, H. L.; Pieters, W.: Receipt-freeness as a special case of anonymity in epistemic logic. Proc. IAVoSS Workshop On Trustworthy Elections, 2006

[Kr02] Krimmer, R.: e-Voting.at: Elektronische Demokratie am Beispiel der österreichischen Hochschülerschaftswahlen. Working Paper 05/2002 des Instituts für Informationsverarbeitung und -wirtschaft, Wirtschaftsuniversität Wien, 2002.

[KR05] Kremer, S.; Ryan, M.: Analysis of an electronic voting protocol in the applied pi calculus. ESOP, pages 186-200, 2005.

[KRS10] Kremer, S., Ryan, M.; Smyth, B.: Election verifiability in electronic voting protocols. ESORICS, pages 389-404, 2010.

[KWG94] Kommunalwahlgesetz online verfügbar unter http://landesrecht.rlp.de/jportal/?quelle=jlink&query=KomWG+RP&psml=bsrlpprod.psml [zuletzt eingesehen am 01.04.2014].

[KWO83] Kommunalwahlordnung, online verfügbar unter http://landesrecht.rlp.de/jportal/?quelle=jlink&query=KomWO+RP&psml=bsrlpprod.psml [zuletzt eingesehen am 21.03.2014].

[Lo+05] Lopez, J.; Montenegro, J. A.; Vivas, J. L.; Okamoto, E.; Dawson, E.: Specification and Design of Advanced Authentication and Authorization Services. Computer Standards & Interfaces 27(5), 467-478, 2005.

[MBH14] Middelhoff, M.; Böhle, C.; Hellingrath, B.: Modeling and Analyzing Information Security in Secure Logistics Business Processes. Proc. MKWI 2014, 1925-1926, 2014.

[MHS05] Mead, N. R.; Hough, E. D.; Stehney II, T. R.: Security Quality Requirement Engineering (SQUARE) Methodology. Technical Report CMU/SEI-2005-TR-009. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 2005.

[Pa+12] Paja, E.; Giorgini, P.; Paul, S.; Meland, P. H.: Security Requirements Engineering Support for Security-Annotated Business Processes. LNBIP, 77-89, 2012.

[RFP07a] Rodríguez, A.; Fernández-Medina, E.; Piattini, M.: A BPMN Extension for the Modeling of Security Requirements in Business Processes. Proc. IEICE Trans. Inf. & Syst., Vol. E90-D, No. 4, 2007.

[RFP07b] Rodríguez, A.; Fernández-Medina, E.; Piattini, M.: M-BPSec: A Method for Security Requirement Elicitation from a UML 2.0 Business Process Specification. LNI Vol. 4802, 106-115, 2007.

[Ru09] Rupp, C.: Requirements Engineering und Management. Hanser, München, 2009.

[Sim+13] Simić-Draws, D., Neumann, S.; Kahlert, A.; Richter, P.; Grimm, R.; Volkamer, M.; Roßnagel, A.: Holistic and Law Compatible IT Security Evaluation: Integration of Common Criteria, ISO 27001/IT-Grundschutz and KORA. In: IJISP, 7(3), 16-35, 2013.

[Sim14] Simić-Draws, D.: Ein Vorgehensmodell zur Durchführung einer prozessorientierten Sicherheitsanalyse. Proc. MKWI 2014, 1889–1896, 2014.

[SS08] Schmelzer, H. J.; Sesselmann, W.: Geschäftsprozessmanagement in der Praxis. Hanser, München, 2008.

[VG09] Volkamer, M.; Grimm, R.: Determine the Resilience of Evaluated Internet Voting Systems, In: IEEE CS Digital Library, doi: 10.1109/RE-VOTE.2009.2, First International Workshop on Requirements Engineering for E-Voting Systems, p. 47-54, 2009

[Vie05] Viega, J.: Building security requirements with CLASP. Proc. Workshop on software engineering for secure systems (SESS), 1-7, 2005.

[VV08] Volkamer, M., Vogt, R.: Common criteria protection profile for basic set of security requirements for online voting products. BSI-CC-PP-0037, Version 1.0, retrieved April 18, 2008, from http://www.bsi.bund.de/