UNIVERSITÄT KOBLENZ · LANDAU
Institut für Wirtschafts- und Verwaltungsinformatik

Fachbereich 4 Informatik

Einfluss von Wahlszenario auf Geheimheit, Privatheit und Öffentlichkeit der Wahl

Katharina Bräunlich
Rüdiger Grimm

Nr. 2/2016

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

Katharina Bräunlich, Rüdiger Grimm
Institut für Wirtschafts- und Verwaltungsinformatik
Fachbereich Informatik
Universität Koblenz-Landau
Universitätsstraße 1
D-56070 Koblenz
E-Mail: braeunlich@uni-koblenz.de, grimm@uni-koblenz.de

Einfluss von Wahlszenario auf Geheimheit, Privatheit und Öffentlichkeit der Wahl

Katharina Bräunlich, Rüdiger Grimm

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

Abstract: Im Rahmen dieser Arbeit wird der Einfluss des Wahlszenarios auf die Geheimheit und Öffentlichkeit der Wahl herausgearbeitet. Ein Wahlszenario wird durch seine Wahlform und die verwendete Wahltechnik bestimmt. Bei der Wahlform kann zwischen einer Präsenz- und einer Fernwahl unterschieden werden. Bei der Wahltechnik zwischen der Papier- und der elektronischen Wahl. Mit der Papier-Präsenzwahl, der Briefwahl (Papier-Fernwahl) und der Internetwahl (elektronische Fernwahl) werden drei prominente Wahlszenarien und ihr Einfluss auf Geheimheit, Privatheit und Öffentlichkeit untersucht.

1 Einleitung

In den letzten Jahren konnte ein signifikanter Anstieg der Briefwahlstimmen[1] festgestellt werden[2]. Die wachsende Nutzung der Briefwahl wird meist mit dem heutigen Zeitgeist bezüglich örtlicher Mobilität und zeitlicher Flexibilität begründet. Mit einem Rückgang der Briefwahlstimmen ist nicht zu rechnen. Der hohe Anteil der Briefwahlstimmen von 24,3% bei der letzten Bundestagswahl 2013 wirft wiederum die Frage auf, ob die Briefwahl auch bei wachsender Nachfrage den Anforderungen an politische Wahlen gerecht wird [Ric10] und ob Internetwahlen eine Alternative bzw. einen Ersatz zur Briefwahl darstellen. Das bildet den Untersuchungsgegenstand dieses Artikels. Konkret wird den folgenden Fragen nachgegangen: Hat das Wahlszenario Einfluss auf die Anforderungen nach geheimen, privaten und öffentlichen Wahlen? Wenn ja, inwiefern? Welche Konsequenzen hat dies letztendlich für das Vertrauen der Wähler bzw. der Wahlöffentlichkeit in die Legitimität der Wahl.

Ein *Wahlszenario* wird durch seine Wahlform und die verwendete Wahltechnik bestimmt. Bei der *Wahlform* kann unterschieden werden zwischen der Präsenzwahl und der

[1] Bis 2008 wurde die Briefwahl als Ausnahme (bei Verhinderung, auf Antrag) zur regulären Wahl im Wahllokal zur Steigerung der allgemeinen Wahl zugelassen. Danach wurde diese Ausnahmeregelung aufgehoben und die Briefwahl wurde ohne Begründung für jeden Wähler freigegeben.

[2] Lag der Anteil der Briefwahlstimmen 1990 noch bei 9,8% aller Stimmen, ist dieser seitdem kontinuierlich gestiegen. Vor der Freigabe der Briefwahl im Jahr 2008 lag der Briefwahlanteil 2005 bereits bei 18,7%. Bei der Bundestagswahl 2013 lag er bereits bei 24,3% aller Stimmen.
[http://www.bundeswahlleiter.de/de/glossar/texte/Briefwahl.html]

Fernwahl. Bei der Präsenzwahl erfolgt die Stimmabgabe durch den Wähler in eigens zur Wahl eingerichteten Wahllokalen. Bei der Fernwahl erfolgt die Stimmabgabe durch den Wähler dezentral im privaten Umfeld des Wählers. Die *Wahltechnik* spezifiziert, in welcher Form die Stimme des Wählers „verarbeitet" wird. Grundsätzlich kann zwischen der Papierwahl und der elektronischen Wahl unterschieden. Bei der Papierwahl erfolgt die Stimmabgabe durch Ankreuzen der Wahlentscheidung auf dem Papierstimmzettel und Einwurf des Stimmzettels in eine Urne bzw. Versenden des Stimmzettels als Brief mit anschließender Aufbewahrung in einer zentral gelagerten Briefwahlurne. Bei der elektronischen Wahl erfolgt die Stimmabgabe, -übertragung und/oder –auswertung elektronisch. Im Rahmen dieser Arbeit werden drei Wahlszenarien betrachtet: Die traditionelle Wahl im Wahllokal als Vertreter der *Papier-Präsenzwahl*, die Briefwahl als Vertreter der *Papier-Fernwahl* und die Internetwahl[3] als Vertreter der *elektronischen Fernwahl*.

Die Anforderungen an politische Wahlen sind in Deutschland mit Art.38 Abs.1 Satz 1 GG[4] sowie Art.38 in Verbindung mit Art.20 Abs.1 und Abs.2 GG in der Verfassung verankert. Demnach müssen die Wahlrechtsgrundsätze der freien, gleichen, unmittelbaren, allgemeinen, geheimen und öffentlichen Wahl gelten. Der nachfolgende Artikel konzentriert sich auf die scheinbar in Konflikt stehenden Anforderungen der Geheimheit und Öffentlichkeit der Wahl sowie der damit verbundenen Privatheit des Wählers. Gemäß der *Geheimheit* der Wahl dürfen Stimme und Wähleridentität nicht verknüpfbar sein. Auf diese Weise schützt die geheime Wahl die freie Wahl. Nur wenn der Wähler seine Stimme unbeobachtet abgeben kann, kann er seine Wahlentscheidung frei treffen. Es sei hier angemerkt, dass gemäß der geheimen Wahl sowohl die Stimme alleine als auch die Wähleridentität alleine nicht zwangsläufig geheim sein müssen. Sie dürfen jedoch nicht miteinander in Verbindung gebracht werden können. Weiterhin sei hier angemerkt, dass die Geheimheit der Wahl nicht gleichzusetzen ist mit der Privatheit des Wählers. *Privatheit* bezeichnet im Folgenden die Vertraulichkeit sämtlicher personenbezogener Daten. Im Kontext von Wahlen können dies zum Beispiel Name oder Adresse sein. Als privat können aber auch Informationen angesehen werden, welche sich aus der Interaktion des Wählers im Wahllokal ergeben wie zum Beispiel Zeitpunkt der Wahl oder Gespräche zwischen Personen im Wahllokal. Der Grundsatz der *Öffentlichkeit* der Wahl wurde über seine Verankerung in der Verfassung hinaus vom Bundesverfassungsgericht explizit hervorgehoben. Demnach müssen *„die wesentlichen Schritte der Wahlhandlung und Ergebnisermittlung vom Bürger zuverlässig und ohne besondere Sachkenntnis überprüft werden können"* [BVerfG09]. Der Öffentlichkeitsgrundsatz ist im Rahmen einer Wahl so zu realisieren, dass er seinem Schutzcharakter gegenüber den anderen Wahlrechtsgrundsätzen gerecht wird, jedoch nicht zur Gefährdung für die Privatheit des Wählers und erst recht nicht der Geheimheit der Stimme wird.

Es sei hier erwähnt, dass die besondere Herausforderung bei Wahlen darin besteht, sowohl Öffentlichkeit als auch Geheimheit gleichzeitig so umzusetzen, dass beide Anforderungen alleine in hinreichendem Maße erfüllt sind und die diese realisierenden Maßnahmen die jeweils andere Anforderung nicht gefährden. So ist es grundsätzlich mög-

[3] Bei der Internetwahl erfolgt die Stimmabgabe auf einem Endgerät, dem sogenannten Wahl-Client. Die Stimmen werden von dem Endgerät an den Wahlserver über das Internet übertragen.
[4] Grundgesetz

lich, Wahlen öffentlich, aber nicht geheim auszuführen. Dies wäre zum Beispiel durch eine öffentliche Abstimmung per Handzeichen möglich. Eine solche Wahl käme der Forderung nach Gleichheit, Unmittelbarkeit, Allgemeinheit und Öffentlichkeit nach. Sie wäre aber nicht geheim und somit auch nicht frei, da das Abstimmungsverhalten eines jeden Einzelnen beobachtbar wäre und der Wähler nicht vor unberechtigter Einflussnahme geschützt wäre. In der Umkehrung wäre auch eine geheime, aber nicht öffentliche Wahl möglich. In diesem Fall wären die Wahlrechtsgrundsätze der Gleichheit, Unmittelbarkeit, Allgemeinheit, Geheimheit und Freiheit, nicht aber der Öffentlichkeit erfüllt. Dieses Beispiel zeigt jedoch die Bedeutung des Öffentlichkeitsgrundsatzes für den Bürger bzw. die Wahlöffentlichkeit. Ohne eine Öffentlichkeit (hier im Sinne einer Beobachtbarkeit/Nachvollziehbarkeit) hat die Wahlöffentlichkeit keine Kontrolle über die korrekte Durchführung der Wahl und somit auch keine Kontrolle über die Durchsetzung der anderen Wahlrechtsgrundsätze wie Gleichheit, Unmittelbarkeit, Allgemeinheit, Geheimheit und Freiheit.

Im nachfolgenden Artikel wird herausgearbeitet, welchen Einfluss die oben genannten Wahlszenarien auf die Geheimheit der Stimme, Privatheit des Wählers und Öffentlichkeit der Wahl haben.

Dieser Artikel ist wie folgt gegliedert: Im Anschluss an diesen Abschnitt werden in Abschnitt 2 Geheimheit, Privatheit und Öffentlichkeit für die drei oben genannten Wahlszenarien analysiert. Dabei wird die Papier-Präsenzwahl in Abschnitt 2.1, die Briefwahl in Abschnitt 2.2 und die Internetwahl in Abschnitt 2.3 behandelt. Der Artikel schließt in Abschnitt 3 mit Zusammenfassung, Fazit und Ausblick.

2 Geheimheit, Privatheit und Öffentlichkeit in verschiedenen Wahlszenarien

Bei der nachfolgenden Analyse wird wie folgt vorgegangen: Zunächst werden die Anforderungen aus den Wahlrechtsgrundsätzen hinsichtlich Geheimheit und Öffentlichkeit konkretisiert. Diese werden dann mit zu schützenden Werten im Sinne der IT-Sicherheit assoziiert. Parallel dazu werden die an Wahlen beteiligten Akteure identifiziert. Anschließend erfolgt eine Analyse der drei genannten Wahlszenarien daraufhin, welche der zuvor identifizierten Sicherheitsanforderungen mittels welchem Sicherheitsmechanismus realisiert wird und wer diesen Sicherheitsmechanismus kontrolliert. Dabei wird Kontrolle als aktive Umsetzung im Sinne eines *Enforcements* und passive Kontrolle im Sinne einer *Überprüfung* betrachtet. Es sei hier angemerkt, dass die Möglichkeit der Überprüfung ebenfalls einen durchsetzenden Charakter besitzt. Zum einen wird der durchsetzende Akteur in seinem Tun kontrolliert/überprüft und dadurch zu korrektem Handeln angehalten. Zum anderen kann der überprüfende Akteur im Falle eines Fehlverhaltens Beschwerdemaßnahmen wahrnehmen und somit korrigierend eingreifen. Die unterschiedlichen Arten der Kontrolle werden in der nachfolgenden Analyse mit *E* (für Enforcement) und *Ü* (für Überprüfung) gekennzeichnet. Basierend auf dieser Analyse wird der Einfluss des Wahlszenarios auf die Geheimheit der Stimme, Privatheit des Wählers und Öffentlichkeit der Wahl bewertet sowie deren Bedeutung für das Vertrauen in die Legitimität der Wahl betrachtet.

Im Kontext von Wahlen im Allgemeinen und von Internetwahlen im Speziellen können die folgenden Daten als zu schützende Werte identifiziert werden:

- *Identifikationsdaten*
- *Authentifikationsdaten*
- *Wählerverzeichnis*
- *Stimmzettel*
- *Stimme* (=ausgefüllter Stimmzettel)
- *Urne*
- *Wahlergebnis*

Der nachfolgende Artikel konzentriert sich dabei auf die Stimme, da hier der Konflikt zwischen Geheimheit und Öffentlichkeit am Stärksten ausgeprägt ist. Es ergeben sich somit folgende Anforderungen:

- *Unverknüpfbarkeit* von Stimme und Wähleridentität
- *Authentizität* des Wählers
- *Korrektheit*[5] der Wahlhandlung
- *Korrektheit*[6] und *Vollständigkeit* des Wahlergebnisses

Für die nachfolgende Analyse ist eine Unterscheidung der involvierten Akteure notwendig. Im Folgenden wird zwischen den folgenden drei Gruppen von Akteuren differenziert:

- *Wähler*
- *Wahlbeobachter*
- *Wahlvorstand*

Es sei hier angemerkt, dass die drei oben genannten Gruppen keine disjunkten Mengen darstellen. Eine Person kann zum Beispiel sowohl als Wähler als auch als Wahlbeobachter agieren. Es wird jedoch im Folgenden angenommen, dass eine Person zu einem Zeitpunkt immer nur innerhalb einer Rolle agieren kann. Im Moment der Stimmabgabe agiert eine Person beispielsweise als Wähler und wechselt nach Beendigung der Stimmabgabe dann in die Rolle des Wahlbeobachters. Weiterhin sei angemerkt, dass die Menge aller Wahlbeobachter die sogenannte *Wahlöffentlichkeit* repräsentiert. Die Begriffe Wahlbeobachter und Wahlöffentlichkeit werden daher im Folgenden synonym verwendet.

Entsprechend der oben genannten Anforderungen und Akteure erfolgt nun für die drei Wahlszenarien eine Analyse hinsichtlich der Umsetzung der identifizierten Anforderungen gemäß obiger Beschreibung.

[5] im Sinne einer Umsetzung aller Wahlrechtsgrundsätze
[6] im dem Sinne, dass jede Stimme nur genau einmal gezählt wird

2.1 Geheimheit, Privatheit und Öffentlichkeit bei der Papier-Präsenzwahl

Bei der Papier-Präsenzwahl wird die Unverknüpfbarkeit von Stimme und Wähleridentität (=Geheimheit) durch zwei Sicherheitsmaßnahmen umgesetzt: Zum einen erfolgt die Stimmabgabe in nicht-einsehbaren Wahlkabinen, die immer nur von einer Person gleichzeitig betreten werden dürfen, sowie einer Verdeckung der Wahlentscheidung auf dem Weg von Wahlkabine bis Einwurf in die Urne durch Falten des Stimmzettels. Weiterhin dürfen die eingeworfenen Stimmen keine Rückschlüsse auf den Wähler zulassen (unmarkierte Stimmzettel). Die Durchsetzung dessen obliegt der Verantwortung des Wahlvorstands, wobei der Wahlöffentlichkeit die Überprüfung dessen möglich ist.

Dabei ist als Wesentlich für die Papier-Präsenzwahl herauszustellen, dass die Beobachtbarkeit der Wahlhandlung von Wählerauthentifizierung über Stimmabgabe, Stimmaufbewahrung bis hin zur Ergebnisermittlung (=Öffentlichkeit) ein wesentlicher Bestandteil für die Durchsetzung der Sicherheitsanforderungen (Integrität der Stimme, der Korrektheit der Wahlhandlung sowie der Korrektheit und Vollständigkeit des Wahlergebnisses) ist. Aktiv werden die entsprechenden Sicherheitsmechanismen zwar von dem Wahlvorstand umgesetzt. Jedoch hat die Wahlöffentlichkeit auf Grund der durchgängigen Beobachtbarkeit ein starkes Instrument zur Überprüfung und Umsetzung der Anforderungen in der Hand.

Zusammenfassend lässt sich demnach feststellen, dass eine unbeobachtete Stimmabgabe zur Umsetzung der geheimen Wahl sowie eine durchgängige Beobachtbarkeit der Wahlhandlung von Stimmabgabe, Stimmaufbewahrung bis hin zur Ergebnisermittlung zur Umsetzung der öffentlichen Wahl von entscheidender Bedeutung für die Papier-Präsenzwahl sind. Die Durchsetzung dieser Sicherheitsmaßnahmen obliegt dabei dem Wahlvorstand, wobei die Wahlöffentlichkeit eine überprüfende Funktion innehat.

Alle Ergebnisse der Untersuchung sind in Tabelle 1 zusammengefasst.

Wert	**Anforderung**	**Sicherheitsmaßnahmen**	**Akteur**
Stimme	Unverknüpfbarkeit mit Wähleridentität	• Unmarkierte Stimmzettel	• Wahlvorstand (E) • Wahlbeobachter (Ü)
		• Geheime Stimmabgabe	• Wahlvorstand (E) • Wahlbeobachter (Ü)
	Integrität	• Beobachtbarkeit der Wahlhandlung	• Wahlvorstand (E) • Wahlbeobachter (Ü)
Wähler	Authentizität	• Kontrolle von Wahlbenachrichtigung und Ausweis	• Wahlvorstand (E) • Wahlbeobachter (Ü)
Wahl-	Korrektheit	• Beobachtbarkeit	• Wahlvorstand (E)

handlung		von Stimmabgabe	• Wahlbeobachter (Ü)
		• Beobachtbarkeit von Stimmeinwurf	• Wahlvorstand (E) • Wahlbeobachter (Ü)
		• Beobachtbarkeit von Stimmaufbewahrung	• Wahlvorstand (E) • Wahlbeobachter (Ü)
Wahlergebnis	Korrektheit	• Mehraugenprinzip bei Auszählung	• Wahlvorstand (E) • Wahlbeobachter (Ü)
		• Öffentlichkeit bei Auszählung	• Wahlvorstand (E) • Wahlbeobachter (Ü)
	Vollständigkeit	• Verschlossene und versiegelte Urne	• Wahlvorstand (E) • Wahlbeobachter (Ü)
		• Durchgängige Beobachtbarkeit der Urne	• Wahlvorstand (E) • Wahlbeobachter (Ü)

Tabelle 1: Sicherheitsanforderungen und –maßnahmen für die Papier-Präsenzwahl im Überblick

Es sei hier angemerkt, dass die Öffentlichkeit der Wahl mittels durchgängiger Beobachtbarkeit der Wahl eine Schutzfunktion für die Korrektheit der Wahl darstellt. Ebenso besitzt die Öffentlichkeit der Wahl jedoch auch ein Gefährdungspotenzial hinsichtlich der Privatheit des Wählers. So ist für Personen im Wahllokal beispielsweise beobachtbar, ob und wenn ja, wann ein Bürger gewählt hat, oder ob und wie dieser Wähler mit anderen Personen interagiert hat. Darüber hinaus können bei nicht entsprechendem Umgang mit dem Wählerverzeichnis personenbezogene Daten über einen Wähler in Erfahrung gebracht werden.

2.2 Geheimheit, Privatheit und Öffentlichkeit bei der Briefwahl

Die Briefwahl ist eine Fernwahl. Somit erfolgt die Stimmabgabe dezentral im privaten Umfeld des Wählers. Dies ist ein zentraler Punkt für die nachfolgende Bewertung der Briefwahl, deren Ergebnisse in Tabelle 2 zusammengefasst sind.

Wie bereits eingangs erwähnt, verschiebt sich die Stimmabgabe bei der Briefwahl von eigens eingerichteten Wahllokalen in das private Umfeld des Wählers. Dies hat zur Konsequenz, dass sich die Stimmabgabe der Kontrolle des Wahlvorstandes und der Wahlöffentlichkeit entzieht. Bei der Briefwahl ist der Wähler selber verantwortlich für die geheime, persönliche und unverfälschte Stimmabgabe. Er muss für eine unbeobachtete und persönliche Stimmabgabe sowie eine unzugängliche Aufbewahrung der Briefwahlunterlagen vor und nach der Stimmabgabe Sorge tragen. Dem Wahlvorstand verbleibt lediglich die Möglichkeit, die Wählerauthentizität anhand der Unterschrift auf dem Wahlbrief

zu überprüfen. Diese Überprüfung der Unterschrift besitzt jedoch nur bedingte Aussagekraft darüber, ob die Stimme tatsächlich von dem Wähler und nur von dem Wähler abgegeben wurde (Fälschen der Unterschrift). Der Wahlbeobachter hat keine Kontrollmöglichkeit bezüglich der Stimmabgabe.

Die zeitliche Flexibilität der Briefwahl macht eine durchgängige Beobachtbarkeit der Stimmaufbewahrung durch die Wahlöffentlichkeit in der Praxis unmöglich. Somit obliegt die Verantwortung für die korrekte Stimmaufbewahrung einzig dem Wahlvorstand und allein dieser hat die Kontrolle über die korrekte und vollständige Aufbewahrung der eingegangenen Stimmen.

Der Einfluss der Wahlöffentlichkeit beschränkt sich somit auf die Ergebnisermittlung. Diese findet zu einem fest vorgegebenen Zeitpunkt statt. Wahlbeobachter können an der Ergebnisermittlung teilnehmen und sich so von der Korrektheit der Stimmauszählung überzeugen. D.h. sie können durch Beobachten nachvollziehen, dass alle in der Urne befindlichen Stimmen korrekt ausgezählt werden. Das korrekte Zustandekommen der Urne (verfälschen, entfernen oder hinzufügen von Stimmen) können sie jedoch nicht nachvollziehen.

Die dezentrale Stimmabgabe bei der Briefwahl verlagert somit die Verantwortung für die korrekte Stimmabgabe (geheim, persönlich, integer) vom Verantwortungsbereich des Wahlvorstandes in den Verantwortungsbereich des Wählers. Gleichzeitig entzieht sich die Stimmabgabe dem Blick der Wahlöffentlichkeit. Die Wahlöffentlichkeit hat somit weniger Kontrolle (im Sinne der Überprüfbarkeit) über den korrekten Ablauf der Wahl. Durch die zeitliche Flexibilität der Briefwahl wird darüber hinaus die Beobachtbarkeit der Stimmaufbewahrung durch die Wahlöffentlichkeit verhindert, so dass die Stimmaufbewahrung einzig in dem Verantwortungsbereich des Wahlvorstandes liegt und sich der Einfluss der Wahlöffentlichkeit auf die Ergebnisermittlung beschränkt.

Gleichzeitig hat aber die dezentrale Stimmabgabe zur Konsequenz, dass eben diese sowie viele mit ihr verbundenen Aktionen des Wählers für die Wahlöffentlichkeit nicht mehr beobachtbar sind. Sowohl Wahlöffentlichkeit als auch Wahlvorstand werden demnach in ihrer Möglichkeit beschränkt, private Informationen über den Wähler in Erfahrung zu bringen. Es ist zum Beispiel nicht mehr beobachtbar, wann ein Wähler gewählt hat (das ob ist anhand der Vermerke im Briefwählerverzeichnis feststellbar) oder mit wem ein Wähler wie interagiert hat.

Wert	**Anforderung**	**Sicherheitsmaßnahmen**	**Akteur**
Stimme	Unverknüpfbarkeit mit Wähleridentität	• Unmarkierte Stimmzettel	• Wahlvorstand (E) • Wähler (E)
		• Geheime Stimmabgabe	• Wähler (E)
Wähler	Authentizität	• Persönliche Stimm-	• Wähler (E)

		abgabe	
		• Unterschrift der eidesstattlichen Erklärung	• Wähler (E)
		• Überprüfung der Unterschrift auf eidesstattlicher Erklärung	• Wahlvorstand (E)
Wahlhandlung	Korrektheit	• Beobachtbarkeit von Stimmaufbewahrung	• Wahlvorstand (E)
Wahlergebnis	Korrektheit	• Mehraugenprinzip bei Auszählung	• Wahlvorstand (E) • Wahlbeobachter (Ü)
		• Öffentlichkeit bei Auszählung	• Wahlvorstand (E) • Wahlbeobachter (Ü)
	Vollständigkeit	• Verschlossene und versiegelte Urne	• Wahlvorstand (E)

Tabelle 2: Sicherheitsanforderungen und –maßnahmen für die Briefwahl im Überblick

Abschließend ist für die Briefwahl festzustellen, dass die dezentrale Stimmabgabe einen „Transport“ der Wahlbriefe vom privaten Umfeld des Wählers zur Urne bedingt. Dies erfolgt bei der Briefwahl auf dem Postwege. Entsprechend muss dieses „Transportmedium“ hinsichtlich Schwachstellen und Bedrohungen für die Sicherheitsanforderungen untersucht und bewertet werden. Bei der Briefwahl kann die Integrität und Vertraulichkeit der Briefwahlstimmen sowie deren Vollständigkeit bei der Übermittlung gefährdet werden. Dies kann sowohl durch Postangestellte sowie den Wahlvorstand erfolgen. Ein Postangestellter kann beispielsweise die Briefwahlunterlagen öffnen und deren Inhalt lesen (sowohl Stimme als auch Wähleridentität), die Briefwahlstimmen ändern, wegwerfen oder neue hinzufügen. Gleiches gilt für den Wahlvorstand bezüglich der Stimmaufbewahrung. Eingegangene Briefwahlstimmen können gelesen, verändert, entfernt oder neue Stimmen hinzugefügt werden. Hierbei sei angemerkt, dass derartige Manipulationen durch Postangestellte auf Grund der dezentralen Struktur der Briefwahlbezirke nicht ausreichend stark skalieren sowie Manipulationen durch den Wahlvorstand durch organisatorische Sicherheitsmaßnahmen hinreichend abgesichert werden/werden können. Somit ist das verbleibende Risiko[7] hinnehmbar.

[7] Risiko = Eintrittswahrscheinlichkeit * Schadenshöhe

2.3 Geheimheit, Privatheit und Öffentlichkeit bei der Internetwahl

In diesem Abschnitt wird der Einfluss der Internetwahl auf Geheimheit der Stimme, Privatheit des Wählers und Öffentlichkeit der Wahl untersucht. Das Vorgehen der Untersuchung ist analog zu den vorherigen Abschnitten. Die Ergebnisse sind in Tabelle 3 zusammengefasst.

Initial ist festzuhalten, dass kein konkretes Internetwahlsystem analysiert wird. Stattdessen wird ein Internetwahlsystem derart abstrahiert, dass die nachfolgenden Erörterungen möglichst allgemeingültig auf Internetwahlen anwendbar sind. Abbildung 1 zeigt eine schematische Darstellung eines solchen Internetwahlsystems. Es lässt sich jedoch nicht vermeiden, an einigen Stellen Annahmen zu treffen, die bestimmte Internetwahlsysteme ausschließen. Im Folgenden wird davon ausgegangen, dass das betrachtete Internetwahlsystem aus Sicherheitsgründen das Separation-of-Duty-Prinzip realisiert und das Internetwahlsystem serverseitig aus zwei getrennt geführten Server besteht. Davon realisiert einer die *Wahlurne* und der andere das *Wählerverzeichnis*. Der Wähler gibt seine Stimme über sein persönliches Endgerät, dem sogenannten *Wahlclient*, ab. Dazu muss sich der Wähler zunächst gegenüber dem Wählerverzeichnis authentifizieren. War die Authentifizierung erfolgreich, bekommt der Wähler den Stimmzettel auf seinem Wahlclient angezeigt und trifft seine Wahlentscheidung. Anschließend wird die Stimme verschlüsselt und verschlüsselt vom Wahlclient an die Wahlurne übertragen. Dort wird die verschlüsselte Stimme bis zum Ende der Stimmabgabephase gespeichert. Anschließend werden alle Stimmen entschlüsselt und ausgezählt[8]. Wählerverzeichnis und Wahlurne kommunizieren derart miteinander, dass die Stimmberechtigung des Wählers abgesichert ist, aber einer Verknüpfung der Wähleridentität mit der Stimme nicht möglich ist, z.B. über ein anonymisierendes Wahltoken nach [Cha81] oder der restrictedID des elektronischen Personalausweises nach [BGKVJ11]. Weiterhin wird die Annahme getroffen, dass ein sogenanntes *Bulletin Board* existiert. Ein Bulletin Board [Be87] ist ein öffentlicher Kanal wie etwa eine Webseite, auf die jeder lesend zugreifen kann, aber nur berechtigte Parteien Daten schreiben können. Zudem können bereits geschriebene Daten weder gelöscht noch verändert werden. Im Folgenden wird davon ausgegangen, dass Wählerverzeichnis und Urne Daten auf dem Bulletin Board veröffentlichen, welche von der Wahlöffentlichkeit gelesen werden können. Art und Umfang der veröffentlichten Daten variieren von Internetwahlsystem zu Internetwahlsystem und werden daher hier nicht weiter spezifiziert. Es wird jedoch im Folgenden davon ausgegangen, dass diese Daten eine sogenannte *Ende-zu-Ende-Verifizierbarkeit* (E2E-Verifizierbarkeit) [AN06], [LGTKI03], [RLHVB10] erlauben und somit alle der folgenden Teilkonzepte umsetzen:

- *Cast-as-Intended:* Der Wähler kann sich davon überzeugen, dass sein Stimmzettel korrekt verschlüsselt wird und dass die verschlüsselte Stimme seine Wahlentscheidung korrekt repräsentiert. Zum Schutze des Wahlgeheimnisses kann Cast-as-Intended nur durch den Wähler selber und nur vor der Stimmabgabe verifiziert werden. Ansonsten könnte Cast-as-Intended genutzt werden, um die Wahlentscheidung eines Wählers aufzudecken.

[8] Das hier beschriebene Verfahren berücksichtigt keine Internetwalsysteme mit homomorpher Verschlüsselung. Allerdings können die Ergebnisse der hier durchgeführten Untersuchung leicht für homomorphe Verfahren angepasst werden.

- *Recorded-as-Cast:* Der Wähler kann nachvollziehen, dass seine (verschlüsselte) Stimme korrekt vom Wahlclient an den Wahlserver übertragen und dort gespeichert wird. Grundsätzlich ist es möglich, Recorded-as-Cast unmittelbar nach der Stimmabgabe oder erst nach Abschluss der Stimmabgabephase zu erlauben.

- *Counted-as-Recorded:* Der Wähler wie auch die Wahlöffentlichkeit können die Ergebnisermittlung nachvollziehen. Dies betrifft zum einen die korrekte Entschlüsselung der Stimmen sowie die Vollständigkeit und Korrektheit des Ergebnisses. Dabei muss die Korrektheit der Entschlüsselung derart implementiert sein, dass dadurch das Wahlgeheimnis nicht gefährdet ist[9]. Die Korrektheit der Auszählung kann im einfachsten Fall durch Veröffentlichung der Klartextstimmen auf dem Bulletin Board[10] sowie Nachzählen der Klartextstimmen verifizierbar gemacht werden. Die Vollständigkeit des Wahlergebnisses ergibt sich aus der Beweiskette von Cast-as-Intended, Recorded-as-Cast und Counted-as-Recorded.

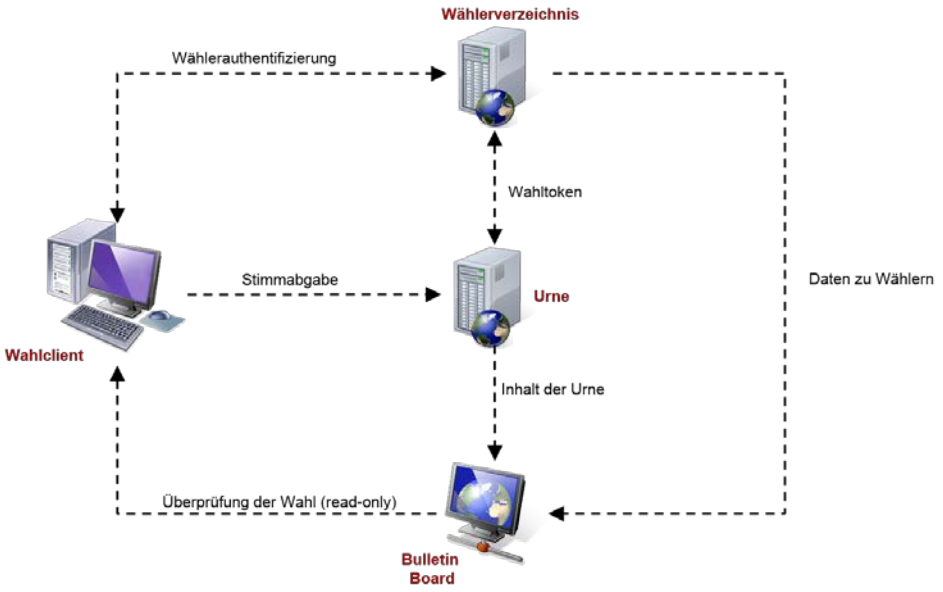

Abbildung 1: Schematische Darstellung eines Internetwahlsystems mit E2E-Veriifzierbarkeit mittels Bulletin Board

Wie auch die Briefwahl ist die Internetwahl eine Fernwahl mit einer dezentralen Stimmabgabe im privaten Umfeld des Wählers. Analog dazu entzieht sich die Stimmabgabe somit aus dem Kontrollbereich von Wahlvorstand und Wahlöffentlichkeit. Entsprechend

[9] Die Umsetzung erfolgt zumeist durch kryptographische Verfahren unter Verwendung von Mix-Netzen [Cha81] und Beweistechniken wie Zero-Knowledge-Proofs [FFS88] oder Randomized-Partial-Cecking [JJR02]

[10] In diesem Fall darf es nicht möglich sein, eine Verbindung zwischen den Klartextstimmen auf dem Bulletin Board und der dazugehörigen Wähleridentität herzustellen.

obliegt die geheime, persönliche und unverfälschte Stimmabgabe der Verantwortung des Wählers. D.h. der Wähler muss dafür Sorge tragen, dass er seine Stimme unbeobachtet (geheim) abgibt. Weiterhin muss der Wähler durch einen sorgsamen Umgang mit dem Authentifizierungsmerkmal[11] die persönliche Stimmabgabe sowie die Integrität der Stimmabgabe sicherstellen.

Während bei der Briefwahl zwischen Absenden des Wahlbriefes und Ergebnisermittlung eine Art „Black-Box" besteht, stehen bei der Internetwahl Verifikationsmechanismen zur Verfügung, die diese Lücke schließen. Mittels Verifikationsmechanismen für Cast-as-Intended kann sich der Wähler davon überzeugen, dass seine verschlüsselte Stimme seine Wahlentscheidung korrekt kodiert. Die Verifikation von Recorded-as-Cast erlaubt es dem Wähler, sich davon zu überzeugen, dass seine verschlüsselte Stimme korrekt von Wahlclient an Wahlserver übertragen und dort gespeichert wird. Die Verifikation von Counted-as-Recorded belegt die korrekte Auszählung aller eingegangenen Stimmen. Somit kann der Wähler die Verarbeitung seiner individuellen Stimme von Stimmabgabe über Stimmübertragung und –speicherung bis hin zur Stimmauszählung nachverfolgen.[12]

Wie auch bei der Briefwahl entzieht sich die Stimmabgabe, -übertragung und –speicherung der Kontrolle der Wahlöffentlichkeit. Demnach wird die Kontrolle der Wahlöffentlichkeit auf die Ergebnisermittlung beschränkt. Der einzelne Wahlbeobachter kann auf dem Bulletin Board die korrekte Entschlüsselung der in der Urne befindlichen (verschlüsselten) Stimmen sowie deren korrekte Auszählung mittels Verifikation von Counted-as-Recorded nachvollziehen. Bezüglich des korrekten Zustandekommens der Urne muss er auf die Wahrnehmung der Verifikation von Cast-as-Intended und Recorded-as-Cast durch die individuellen Wähler vertrauen.

Zusammenfassend lässt sich für die Internetwahl sagen, dass sie bei gleichem Niveau an Geheimheit der Stimme und Privatheit des Wählers zusätzliche Sicherheitsmechanismen zur Umsetzung der Korrektheit der Wahlhandlung sowie der Korrektheit und Vollständigkeit der Ergebnisermittlung bereitstellt. Wie auch bei der Briefwahl obliegt die geheime und persönliche Stimmabgabe der Verantwortung des Wählers. Im Gegensatz zur Briefwahl ist der Wähler bei der Internetwahl jedoch mit zusätzlichen Sicherheitsmechanismen zur Wahrung der Integrität der Stimme ausgestattet (Cast-as-Intended und Recorded-as-Cast). Die Wahlöffentlichkeit ist bei der Internetwahl ebenfalls ausschließlich auf die Ergebnisermittlung beschränkt. Streng genommen, kommt dies der Briefwahl gleich. Durch die Beweiskette von Cast-as-Intended und Recorded-as-Cast für den individuellen Wähler im Zusammenspiel mit Counted-as-Recorded für die Wahlöffentlichkeit kann aber die Gewissheit der Wahlöffentlichkeit bezüglich des korrekten Zustandekommens der Urne als fundierter/besser bewertet werden. Letztlich bleibt anzumerken,

[11] Das Authentifizierungsmerkmal ist ein *„Merkmal, das jeder registrierte Wähler besitzt, um sich am EVG* [Anm.: EVG bezeichnet das Internetwahlsystem*] zu authentisieren."* [VV08] Das Authentisierungsmerkmal kann zum Beispiel eine TAN oder der private Schlüssel auf einer Smartcard wie dem elektronischen Personalausweis sein.

[12] Es ist hier anzumerken, dass zum Schutze des Wahlgeheimnisses meist die Verbindung zwischen verschlüsselter Stimme und Klartextstimme bei der Auszählung gelöscht wird. Dieser Schritt wird durch kryptographische Verfahren wie Mix-Netze in Verbindung mit Zero-Knowledge-Proofs oder Partialized-Random-Checking jedoch nachvollziehbar gemacht, und zwar für den individuellen Wähler wie auch die Wahlöffentlichkeit.

dass der Wahlvorstand in seinem Einflussbereich bei der Internetwahl am Stärksten beschränkt wird. Durch die Technik und die umfassenden Verifikationsmechanismen in Händen der Wähler bzw. der Wahlöffentlichkeit verbleibt dem Wahlvorstand die Aufgabe des Betriebs des Internetwahlsystems.

Die Privatheit des Wählers ist bei der Internetwahl in gleichem Maße realisiert wie bei der Briefwahl.

Wert	**Anforderung**	**Sicherheitsmaßnahmen**	**Akteur**
Stimme	Unverknüpfbarkeit mit Wähleridentität	• Geheime Stimmabgabe	• Wähler (E)
	Integrität	• Individual Verifiability (=Cast-as-Intended und Recorded-as-Cast)	• Wähler (Ü)
Wähler	Authentizität	• Persönliche Stimmabgabe	• Wähler (E)
		• „guter Umgang“ mit Authentifizierungsmerkmale	• Wähler (E)
		• Validierung des Authentifizierungsmerkmals	• Wahlsystem
Wahlhandlung	Korrektheit	• Verifizierbarkeit von Cast-as-Intended	• Wähler (Ü)
		• Verifizierbarkeit von Recorded-as-Cast	• Wähler (Ü)
Wahlergebnis	Korrektheit	• Verifizierbarkeit von Counted-as-Recorded	• Wahlbeobachter (Ü)
	Vollständigkeit	• Verifizierbarkeit von Recorded-as-Cast	• Wähler (Ü)

Tabelle 3: Sicherheitsanforderungen und –maßnahmen für die Internetwahl im Überblick

Wie auch die Briefwahl ist die Internetwahl eine Fernwahl. Bei der Briefwahl werden die Stimmen per Post vom Wähler zur Briefwahlurne übermittelt. Wie im vorherigen Abschnitt erwähnt, macht dies eine Bewertung der Bedrohungen auf und durch das „Transportmedium“ notwendig. In Hinblick auf Internetwahlen ist festzustellen, dass die Internetwahltechnik sich nicht (wie die Briefwahltechnik) lediglich auf den Transport der Stimmen von Wahlclient an Wahlserver mittels Internettechnologie beschränkt. Vielmehr schließt sie die Stimmverarbeitung sowohl auf Client- als auch Server-Seite mit ein. Entsprechend komplexer ist auch eine Identifikation und Bewertung existierender Bedrohungen, da diese sowohl Manipulationen auf dem individuellen Endgerät der Wählers (zum Beispiel durch das sogenannte Secure-Platform-Problem [Riv01]), auf dem Übertragungsweg sowie auf dem Wahlserver inkludiert. Das Internetwahlsystem als solches sowie die dadurch notwendige Infrastruktur aus Internet-Service-Provider und Wahldiensteanbieter sowie Wahlorganisatoren müssen dabei Berücksichtigung finden. Da eine solche Sicherheitsanalyse ohne konkretes Internetwahlsystem sowie seiner organisatorischen Einbettung nicht möglich ist, wird an dieser Stelle keine umfassende Sicherheitsbewertung vorgenommen. Es sei lediglich festgestellt, dass die Integrität und Vollständigkeit der Stimmen mittels der oben erwähnten Verifikationsmechanismen innerhalb des Internetwahlsystems umgesetzt werden, dass die Geheimheit der Stimme auf dem Übertragungsweg durch hinreichend starke Verschlüsselung geschützt wird, aber die Geheimheit der Stimme durch das Secure-Platform-Problem auf dem Endgerät des Wählers gefährdet ist. Weiterhin sei angemerkt, dass bei einer tiefergehenden Bewertung zu berücksichtigen ist, dass Manipulationen bei Internetwahl stärker skalieren als bei Briefwahlen. Dies muss bei der Bewertung des Risikos Berücksichtigung finden.

3 Zusammenfassung, Fazit und Ausblick

Bei der Papier-Präsenzwahl erfolgt die Stimmabgabe in eigens eingerichteten und vom Wahlvorstand kontrollierten Wahllokalen statt. Der Wähler als solcher kommt dabei seiner Aufgabe der Stimmabgabe nach. Darüber hinaus hat er keine aktive Rolle bei der Durchführung/Durchsetzung der Wahl. Sowohl bei der Brief- als auch der Internetwahl verlagert sich die Stimmabgabe in das private Umfeld des Wählers. Das bringt ein mehr an Privatheit für den Wähler, indem die Stimmabgabe dem Blick des Wahlvorstandes und der Wahlöffentlichkeit entzogen wird. Dabei kann das Maß an Privatheit bei der Briefwahl und der Internetwahl als gleich bewertet werden. In der Umkehrung bedeutet dies aber auch, dass sich die Verantwortung für die geheime und persönliche Stimmabgabe vom Wahlvorstand in den Verantwortungsbereich des Wählers verschiebt. Bei der Briefwahl hat der Wähler keine Kontrolle über die Stimmübermittlung per Post und die Stimmaufbewahrung durch den Wahlvorstand. Eine Verletzung der Integrität, Vertraulichkeit und Vollständigkeit der Stimmen kann sowohl auf dem Übertragungsweg durch die Post als auch bei der Stimmaufbewahrung durch den Wahlvorstand erfolgen. Von Seiten des Wählers ist auf Grund der fehlenden Kontrolle daher Vertrauen in die Post sowie den Wahlvorstand notwendig. Im Gegensatz dazu ist der Wähler bei der Internetwahl mit Mechanismen zur E2E-Verifizierbarkeit ausgestattet, welche eine Nachverfolgung der Stimme von Stimmabgabe, -übermittlung, -speicherung bis hin zur -auszählung

erlaubt. Er besitzt somit bei der Internetwahl im Vergleich zur Briefwahl mehr Kontrollmöglichkeiten bei gleichem Niveau an Privatheit und Geheimheit. Jedoch bedingen die Bedrohungen auf und durch die Wahltechnik sowie die starken Auswirkungen solcher potenziellen Angriffe ein Vertrauen in das Internetwahlsystem, die verwendete Hardware, die Internetkommunikation sowie deren organisatorische Einbettung.

Während bei der Papier-Präsenzwahl eine durchgängige Beobachtbarkeit der Wahlhandlung von Stimmabgabe über Stimmeinwurf und –aufbewahrung bis hin zur Stimmauszählung gegeben ist, wird durch die Fernwahl (sowohl Brief- als auch Internetwahl) die Nachvollziehbarkeit der Wahlöffentlichkeit auf die Stimmauszählung beschränkt. Bei der Briefwahl muss der Wahlbeobachter darauf vertrauen, dass der Wähler seine Stimme geheim und persönlich abgibt und dass die Integrität, Vertraulichkeit und Vollständigkeit der Stimmen sowohl auf dem Postweg als auch bei der Aufbewahrung durch den Wahlvorstand gewahrt bleiben. Bei der Internetwahl verhält es sich ebenso. Allerdings kann das Vertrauen des Wahlbeobachters auf Grund der bestehenden Verifikationsmechanismen für den Wähler als fundierter bewertet werden.

Während der Wahlvorstand bei der Papier-Präsenzwahl als Hauptverantwortlicher für die korrekte Durchführung der Wahl zu identifizieren ist, wird sein Verantwortungsbereich bei der Fernwahl mit der Verlagerung der Stimmabgabe in das private Umfeld des Wählers stark beschränkt. Bei der Briefwahl beschränkt sich sein Verantwortungsbereich auf die Stimmaufbewahrung und -auszählung. Der Wahlvorstand muss entsprechend bei der Briefwahl auf die geheime und persönliche Stimmabgabe durch den Wähler sowie die Wahrung von Integrität, Vertraulichkeit und Vollständigkeit der Stimmen auf dem Postweg vertrauen. Seine Verantwortung wird bei der Internetwahl sogar noch weiter beschränkt, indem er keine direkte Kontrolle über die Stimmaufbewahrung und –auszählung mehr besitzt. Er ist lediglich für die Bereitstellung und den Betrieb der Technik verantwortlich.

Bezüglich der Frage, welchen Einfluss die Wahlform auf die Geheimheit der Stimme, Privatheit des Wählers und Öffentlichkeit der Wahl hat, lässt sich zusammenfassend feststellen, dass die Fernwahl die Stimmabgabe in das private Umfeld des Wählers verlagert und somit dessen Privatheit erhöht, ihn dabei auch gleichzeitig in die Verantwortung für die geheime, persönliche und unverfälschte Stimmabgabe nimmt. Die Wahlöffentlichkeit wird dadurch auf die Stimmauszählung beschränkt. Weiterhin bleibt zu berücksichtigen, dass dadurch Manipulationen auf dem Übertragungsweg möglich werden. Deren Auswirkungen sind sorgfältig gegen den Nutzen durch die Fernwahl abzuwägen.

Im Vergleich zwischen Brief- und Internetwahl konnte festgestellt werden, dass beide Wahltechniken ein äquivalentes Maß an Privatheit des Wählers und Geheimheit der Stimme realisieren. Im Gegensatz zur Briefwahl hat der Wähler bei der Internetwahl jedoch mehr Kontrolle und somit mehr Gewissheit in die korrekte Verarbeitung seiner individuellen Stimme und somit in die Korrektheit der gesamten Wahl. Jedoch bedingt die Internetwahltechnik noch eine detailliertere Betrachtung der existierenden Bedrohungen sowie einer Bewertung der Bedrohungen.

Dies ist ein Punkt für zukünftige Arbeiten. Vertrauen wird oftmals als fundamental für eine mögliche Akzeptanz von Internetwahlen genannt. Gemäß des Vertrauensmodells nach [MDS95] wird Vertrauen beeinflusst von dem wahrgenommenen Risiko in einer Vertrauensrelation (hier der Vertrauensrelation zwischen dem Wähler und der Internet- bzw. Briefwahltechnik). Im Kontext von Wahlen wäre es daher äußerst interessant, zu untersuchen, inwiefern das tatsächliche Risiko der untersuchten Fernwahltechniken mit dem wahrgenommenen Risiko korreliert und welche Maßnahmen vertrauenssteigernde Wirkung besitzen

Literaturverzeichnis

[AN06] Adida, B.; Neff: *Ballot casting assurance.* In EVT '06: Proceedings of the USENIX/ACCURATE Electronic Voting Technology Workshop, Berkeley, CA, USA, 2006. USENIX Association.

[Be87] Benaloh, J. D. C. (1987): *Verifiable secret-ballot elections*, Dissertation, Yale University, Department of Computer Science, Technical Report number 561.

[BGKVJ11] Bräunlich, K.; Grimm, R.; Kasten, A.; Vowé, S.; Jahn, N. (2011): *Der neue Personalausweis zur Authentifizierung von Wählern bei Onlinewahlen*. Institut für Wirtschafts- und Verwaltungsinformatik, Universität Koblenz-Landau. Nr. 11/2011. Arbeitsberichte aus dem Fachbereich Informatik, online verfügbar unter http://www.uni-koblenz.de/~fb4reports/2011/2011_11_Arbeitsberichte.pdf [zuletzt abgerufen am 24.07.2014]

[BVerfG09] Bundesverfassungsgericht (2009): 2 BvC 3/07 vom 3.3.2009, Absatz-Nr. (1 - 163), online verfügbar unter http://www.bverfg.de/entscheidungen/cs20090303_2bvc000307.html [zuletzt abgerufen am 17.07.2014]

[Cha81] Chaum, David L.: *Untraceable electronic mail, return addresses, and digital pseudonyms.* In: Communications of the ACM 24 (1981), Nr. 2, S. 84_90

[FFS88] U. Feige, A. Fiat und A. Shamir. *Zero Knowledge Proofs of Identity*. Journal of Cryptology, 1(1):77–94, 1988.

[JJR02] Jakobsson, M.; Juels, A.; Rivest, R.L.: *Making mix nets robust for electronic voting by randomized partial checking.* In USENIX Security Symposium, Seite 339353, 2002.

[LGTKI03]Lambrinoudakis, C.; Gritzalis, D.; Tsoumas, V.; Karyda, M., Ikonomopoulos, S.: *Secure electronic voting: The current landscape*, volume 7 of Advances in Information Security, chapter 7. Kluwer Academic Publishers, 2003.

[MDS95] Mayer, R.; Davis, J.; Schoorman, F. (1995): An Integrative Model of Organizational Trust, In: *The Academy of Management Review*, Vol. 20, No. 3 (Jul., 1995), pp. 709-734, online verfügbar unter: http://www.jstor.org/stable/258792 [zuletzt abgerufen am 29.07.2014]

[Ric10] Richter, P. (2010): Briefwahl für alle? - Die Freigabe der Fernwahl und der Grundsatz der Öffentlichkeit, In: DÖV 2010, 606

[Riv01] Rivest, R.L.: *Electronic Voting*. In Proc. Financial Cryptography ’01, volume 2339, pages 234–259. Laboratory for Computer Science Massachusetts Institute of Technology Cambridge, Springer, 2001.

[VV08] Volkamer, M.; Vogt, R. (2008): *Common criteria protection profile for basic set of security requirements for online voting products*. BSI-CC-PP-0037, Version 1.0, online verfügbar unter http://www.bsi.bund.de/ [zuletzt abgerufen am 24.07.2014]

Bisher erschienen (seit 2012)

Davor erschienene Arbeitsberichte, siehe

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

Arbeitsberichte aus dem Fachbereich Informatik

Katharina Bräunlich, Rüdiger Grimm, Einfluss von Wahlszenario auf Geheimheit, Privatheit und Öffentlichkeit der Wahl, Arbeitsberichts 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