UNIVERSITÄT KOBLENZ · LANDAU

Fachbereich 4: Informatik

IWVI

Institut für Wirtschafts- und Verwaltungsinformatik

Sicherheits- und Datenschutzaspekte von E-Partizipationsanwendungen

Masterarbeit

zur Erlangung des Grades eines Master of Science

im Studiengang Wirtschaftsinformatik

vorgelegt von

Patrick Schwirz

208110502

Betreuung und Begutachtung:

Prof. Dr. Maria A. Wimmer

Leiterin der Forschungsgruppe Verwaltungsinformatik, Institut für Wirtschafts- und Verwaltungsinformatik

Sabrina Scherer

Wissenschaftliche Mitarbeiterin in der Forschungsgruppe Verwaltungsinformatik, Institut für Wirtschafts- und Verwaltungsinformatik

Koblenz, im September 2010

Erklärung

Ich versichere, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe und dass die Arbeit in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegen hat und von dieser als Teil einer Prüfungsleistung angenommen wurde. Alle Ausführungen, die wörtlich oder sinngemäß übernommen wurden, sind als solche gekennzeichnet.

Die Richtlinien der Forschungsgruppe für Qualifikationsarbeiten habe ich gelesen und anerkannt, insbesondere die Regelung des Nutzungsrechts.

Mit der Einstellung dieser Arbeit in die Bibliothek bin ich einverstanden *Ja* [X] *Nein* [ ]

Der Veröffentlichung dieser Arbeit im Internet stimme ich zu. *Ja* [X] *Nein* [ ]

Koblenz, den 30.09.2010 *Unterschrift*

Zusammenfassung

Obwohl E-Partizipation immer mehr an Bedeutung gewinnt, werden Sicherheitsrisiken und -anforderungen bisher nur oberflächlich betrachtet. Diese Masterarbeit soll einen Beitrag zur Sicherheit und zum Datenschutz von E-Partizipationsanwendungen leisten.

Dabei befasst sich die Arbeit mit dem Nutzer von elektronischen Beteiligungsformen. Da dieser im E-Partizipationsprozess seine persönlichen Daten bereitstellt, müssen Vertrauenswürdigkeit, Vertraulichkeit, Transparenz, Verfügbarkeit und Rechtssicherheit zwischen öffentlicher Verwaltung und Nutzer geschaffen werden. Eine der wichtigsten Maßnahmen hierbei ist es, einen möglichst hohen Sicherheits- und Datenschutzstandard in der Informations- und Kommunikationstechnologie durch die Verwaltung zu gewährleisten und dem Bürger Sicherheit im Umgang mit E-Partizipationsanwendungen zu geben.

Die Masterarbeit untersucht verschiedene E Partizipationsangebote der Bereiche Bürgerhaushalte, E-Konsultationen, Parteiwebseiten und E-Petitionen und beleuchtet zunächst, welchen Einfluss sicherheitskritische E-Partizipationssysteme auf das politische System haben können. Anschließend wird der derzeitige Sicherheitsstandard der E-Partizipationsangebote erfasst. Hierzu wird ein Analyse-Framework verwendet, das für E-Partizipation relevante Sicherheits- und Datenschutzaspekte betrachtet. Darauf aufbauend werden Sicherheitslevels für verschiedenen Typen von E-Partizipationsanwendungen abgeleitet und Empfehlungen für die Gestaltung von E-Partizipation gegeben. Auf Grundlage dessen werden Handlungsempfehlungen gegeben, die helfen können, E-Partizipationsanwendungen zukünftig sicherer zu gestalten. Weiterhin werden zukünftige Technologien vorgestellt, die das Potential haben, die Sicherheit bei der Nutzung von Systemen zur elektronischen Bürgerbeteiligung zu erhöhen.

Abstract

Although e-participation is becoming more and more important, security risks and requirements are so far only superficially regarded. This master thesis aims at contribute to security and privacy of e-participation applications.

This paper deals with the users of electronic participation forms. Since personal data has to be transmitted in the e-participation process, systems require trustworthiness, privacy, transparency, availability and legal security between public administration and users. Therefore it is very important to ensure the most of security and privacy standards in information and communication technologies by the administration and the citizens to provide the necessary confidence in using e-participation applications.

This master thesis examines different e-participation platforms of the areas participatory budgeting, e-consultations, party websites, and e-petitions and explores at first which influence of sensitive e-participation systems on the political system they have. Subsequently, the current safety standard of the e-participation applications is determined. For this purpose an analysis framework is used, regarding on relevant security and privacy issues for e-participation. Based on the results safety levels are deduced from different types of e-participation applications. In addition recommendations for the constitution of e-participation are concluded, which helps to make e-participation applications more secure. Furthermore, future technologies with the potential to improve security in the use of electronic public participation are presented.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
BDSG	Bundesdatenschutzgesetz
BMI	Bundesministerium des Innern
BSI	Bundesamt für Sicherheit in der Informationstechnik
DDoS	Distributed Denial of Service
DoS	Denial of Service
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IKT	Informations- und Kommunikationstechnologie
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
PKI	Private Key Infrastructure
RSS	Really Simple Syndication (RSS 2.0)
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
XML	Extensible Markup Language

1. Einführung

1.1 Motivation

E-Partizipation ist der Einsatz von Informations- und Kommunikationstechnologien (IKT), der darauf abzielt, die politische Partizipation auszuweiten und zu vertiefen. Dabei soll es den Bürgerinnen und Bürgern ermöglicht werden, sich mit anderen Bürgern oder gewählten Repräsentanten in Verbindung zu setzen. Diese Definition umfasst alle Akteure in demokratischen Entscheidungsprozessen und enthält sowohl Aktivitäten, die politikseitig veranlasst werden, als auch Bürgerinitiativen, die sich an Verwaltung und Politik richten [Macintosh, 2006]. E-Demokratie ist die Verwendung von IKT in Regierungen durch gewählte Offizielle, Medien, politische Parteien, Interessensvertretungen usw. [Clift, 2003]. Daher kann E-Partizipation als Teil von E-Demokratie (neben E-Voting) betrachtet werden.

Obwohl E-Partizipation innerhalb der EU durch die Förderung zahlreicher Projekte[1] und auch auf nationaler Ebene (wie die aktuelle Studie im Auftrag des Bundesministeriums des Innern zeigt [Albrecht, et al., 2008]) immer mehr an Bedeutung gewinnt, werden Sicherheitsrisiken und -anforderungen bisher nur oberflächlich betrachtet. Mehrheitlich beruhen Analysen auf der Tatsache, dass eine Vielzahl von E-Partizipationsangeboten auf Systemen basiert, die schon in anderen Anwendungsbereichen erfolgreich eingesetzt wurden, wie z.B. Diskussionsforen, Chaträume etc. [Fraser, et al., 2006]. Dabei werden aber die neuen Anforderungen an die Software durch die Verwendung im Anwendungsbereich E-Partizipation nicht ausreichend berücksichtigt. Ein Beispiel ist die Diskussion eines Stadt-Haushaltsplanes mittels eines Forums und die darauf beruhende Entscheidungsfindung[2]. Eine Fragestellung in dem Zusammenhang könnte sein, wie hier sichergestellt werden kann, dass die Teilnehmer auch wirklich aus der entsprechenden Region stammen und bspw. nicht die Interessen von Nachbarregionen vertreten. Zusätzlich bestehen aber auch die Risiken von weiteren gezielten Angriffen auf E-Partizipationsangebote über das Internet, wie sie beispielweise in [Janowicz, 2007] allgemein erläutert werden.

1.2 Ziele

Diese Arbeit soll einen Beitrag zur Sicherheit und zum Datenschutz von E-Partizipationsanwendungen leisten und aufzeigen, warum die Sicherheit in diesen Angeboten so wichtig ist. Dazu werden aktuelle E-Partizipationsangebote mit Hilfe einer Sicherheitsanalyse auf verschiedene Sicherheitsaspekte untersucht.

***Forschungsfrage 1**: Welchen Einfluss können sicherheitskritische E-Partizipationssysteme auf das politische System haben?*

[1] Beispielsweise die eParticipation Preparatory Action http://www.eu-participation.eu/

[2] Beispielsweise die Aktionen „Bürgerhaushalt Berlin“ unter http://www.buergerhaushalt-berlin.de/ oder „Bürgerhaushalt Köln“ https://buergerhaushalt.stadt-koeln.de/

Zunächst werden mögliche Angriffsszenarien auf verschiedene E-Partizipationsanwendungen der Gebiete Bürgerhaushalte, E-Konsultationen, Parteiwebseiten und E-Petitionen thematisiert. Hierbei wird untersucht, welche speziellen Gefahren für die Partizipationsgebiete gelten und welche Sicherheits- und Datenschutzaspekte wichtig sind.

Forschungsfrage 2*: Wie sieht der momentane Sicherheitsstand bei E-Partizipationsangeboten aus?*

Hierfür wird ein Analyserahmen entwickelt, der die Grundlage der Untersuchung darstellt. Mit dessen Hilfe werden die Beteiligungsplattformen auf Sicherheitsaspekte verschiedener Sicherheitsbereiche einheitlich untersucht und bewertet. Ein Sicherheitsbereich ist z.B. der Datenschutz, der als Sicherheitsaspekte alle Maßnahmen, die zum Schutz von personenbezogenen Daten ergriffen werden können, umfasst. Anschließend werden für die E-Partizipationsanwendungen Sicherheitslevel abgeleitet, die einen Überblick über die Sicherheitsanforderungen der einzelnen Anwendungen geben.

Forschungsfrage 3: *Welche sicherheitsrelevanten Anforderungen bestehen für E-Partizipationssysteme und w*ie *können E-Partizipationsangebote sicher(er) gestaltet werden?*

Es werden Handlungsempfehlungen auf Grundlage der Angriffsszenarien und des derzeitigen Sicherheitsstandards gefolgert. Zudem sollen zukünftige Technologien, wie der elektronische Personalausweis, Beachtung finden und einen Ausblick auf mögliche Veränderungen im Sicherheitsbereich von E-Partizipationsanwendungen geben. Damit soll aufzeigt werden, wie sich die Sicherheitslandschaft der elektronischen Bürgerbeteiligung mittelfristig verändern könnte.

1.3 Aufbau der Arbeit

Die vorliegende Masterarbeit gliedert sich in sieben Teile. Das Kapitel 2 beschäftigt sich mit den Grundlagen zum Thema E-Partizipation. Hier werden die wichtigsten zugehörigen Begriffe definiert und es wird erläutert, warum das Internet zu einer verstärkten Beteiligung in politischen Prozessen führen kann. Zudem werden die Gefahren von E-Partizipation aufgezeigt und einen Einblick in den aktuellen Stand von E-Partizipationsanwendungen in Deutschland gegeben. Abschließend werden die in der Arbeit betrachteten Anwendungen vorgestellt und erläutert.

Kapitel 3 beschäftigt sich mit den Grundlagen der Sicherheit. Es zeigt zunächst Gefahren im Internet auf und thematisiert verschiedene mögliche Angriffsszenarien. Ferner befasst sich das Kapitel mit dem Datenschutz, der sicheren Kommunikation im Internet und dem individuellen Sicherheitsbewusstsein der Bürger.

Nach diesen Grundlagen thematisiert Kapitel 4 die möglichen Angriffsszenarien auf die in Kapitel 2 vorgestellten E-Partizipationsanwendungen und zeigt die wichtigsten Gefahren der jeweiligen Anwendungen auf.

Anschließend behandelt Kapitel 5 die Untersuchung der Sicherheits- und Datenschutzaspekte und gibt einen Überblick über das erarbeitete und verwendete Analyse-Framework und die Vorgehens-

weise. Anschließend werden die Ergebnisse zusammengefasst und den untersuchten Online-Anwendungen Sicherheitslevel zugeordnet.

In Kapitel 6 werden Empfehlungen auf Grundlage der Untersuchungsergebnisse für die Betreiber der E-Partizipationsanwendungen abgegeben. Zudem betrachtet das Kapitel zukünftige Technologien, die das Potential haben, Online-Anwendungen zu verändern und sicherer zu gestalten.

Den Abschluss bildet Kapitel 7, in dem ein Fazit und ein Ausblick gegeben werden.

2. Grundlagen der E-Partizipation

Dieses Kapitel beschäftigt sich mit den Grundlagen der E-Partizipation. Zunächst werden die Begrifflichkeiten der Partizipation, des E-Governments, der E-Demokratie und der E-Partizipation erläutert. Im Folgenden wird auf die Internetnutzung in Deutschland eingegangen, die auch das Web 2.0 und damit verbundene neue Formen der Bürgerbeteiligung umfasst. Anschließend werden die Gefahren der E-Partizipation aufgegriffen und der aktuelle Stand der E-Partizipationsanwendungen erläutert.

2.1 Begriffsbestimmung

Um ein Verständnis für die Bürgerbeteiligung zu bekommen, muss zunächst erklärt werden, was die Partizipation an Verwaltungsprozessen eigentlich ist und welche Bedeutung sie in der Politik einnimmt. Danach wird auf Beteiligungsformen eingegangen, die durch moderne Informations- und Kommunikationstechnologien (IKT) unterstützt und die unter dem Oberbegriff E-Government zusammengefasst werden. Für die elektronisch gestützte Beteiligung sind zudem die Themen E-Demokratie und E-Partizipation wichtig, die in diesem Kapitel erläutert werden.

2.1.1 Partizipation

Grundlagen

Die Begriffe Partizipation (v. lat.: particeps = an etwas teilnehmend) und Bürgerbeteiligung werden in der Literatur oft synonym verwendet und bezeichnen die aktive Teilhabe und Mitbestimmung von Bürgern an Prozessen der öffentlichen Willensbildung, Entscheidungsfindung, Leistungserstellung und -erbringung [Albrecht, et al., 2008]. Ferner bezeichnet Partizipation alle Verhaltensweisen des Einzelnen oder einer Gruppe, freiwillig Einfluss auf politische Entscheidungen auf allen Ebenen des politischen Systems ausüben zu wollen [Berger-Lenz, 2007].

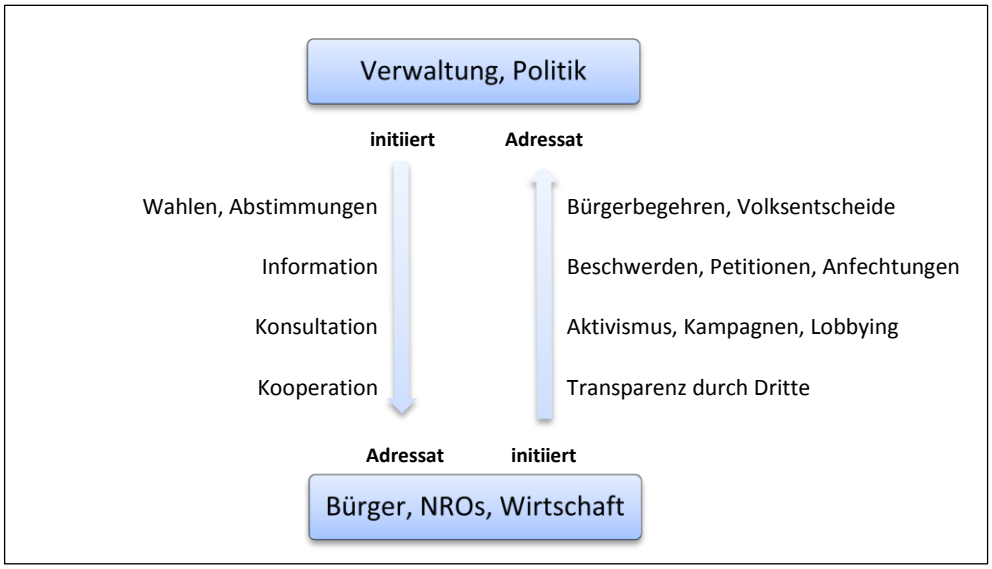

Abbildung 1. Formen politischer Partizipation[3]

Nach [Albrecht, et al., 2008] stehen sich in Partizipationsprozessen immer Verwaltung und Politik auf der einen Seite sowie Bürger, Nichtregierungsorganisationen (NRO) und die Wirtschaft auf der anderen Seite gegenüber. Dabei werden acht verschiedene Formen der politischen Partizipation unterschieden, die in Abbildung 1 aufgezeigt und im Folgenden kurz erklärt werden:

- **Wahlen und Abstimmungen** geben der Bevölkerung die Möglichkeit, ihren Willen auszudrücken und politischen Kandidaten ein Amt oder Gremium auf eine bestimmte Zeit anzuvertrauen.

- **Informationen** stellen eine wichtige Voraussetzung für die Partizipation dar. Die Bereitstellung von Informationen an Bürger stellt die Grundstufe der Bürgerbeteiligung dar. Informationen sollten hierzu bürgernah aufbereitet, leicht auffindbar sein und frühzeitig weitergegeben werden. Beispiele sind Bebauungspläne, Gemeinderatsprotokolle, Termine, Gesetzesinitiativen etc.

- Beteiligungsformen mit dem Ziel, Meinungen von Bürgen zu politischen Planungen und angesetzten Entscheidungen einzuholen, werden unter dem Begriff **Konsultation** zusammengefasst.

- **Kooperationen** bezeichnet die auf Einvernehmen ausgerichtete enge Zusammenarbeit von Verwaltung/Politik mit dem Bürger oder NROs über eine längere Zeit hinweg (z.B. Bürgerhaushalte).

- Unter direktdemokratische Instrumente fallen die **Bürgerbegehren und Volksentscheide**, wie sie beispielsweise in der Schweiz Verwendung finden. Hierbei geht die Macht direkt vom Volk aus, da politische Entscheidungen mit hoher Bürgerbeteiligung beschlossen werden.

[3] Quelle: [Albrecht, et al., 2008]

- Mittels **Beschwerden, Petitionen und Anfechtungen** können Bürger ihren Unmut über politische Entscheidungen an entsprechende Stellen der öffentlichen Verwaltung ausdrücken. Dies kann auf Bundes-, Länder- oder Kreisebene geschehen. Anfechtungen können in Form von Widersprüchen bis hin zur Klage vor Gericht reichen.

- Einzelpersonen oder organisierte Gruppen können mittels **Aktivismus, Kampagnen und Lobbying** Maßnahmen ergreifen, um Aufmerksamkeit oder Unterstützung für Themen und Positionen zu erhalten. Kampagnen zielen dabei auf die Mobilisierung der breiten Öffentlichkeit (z.B. gegen das BKA-Gesetz[4]). Mittels Lobbying wird versucht, seine Interessen bei einzelnen Stellen oder Personen durchzusetzen (z.B. über E-Mails an Abgeordnete).

- Unabhängige informelle Angebote (wie z.B. Abgeordnetenwatch[5]) ermöglichen die **Transparenz durch Dritte**. Sie informieren nutzerfreundlich über die Handlungen der öffentlichen Stellen und ermöglichen eine Kontrolle dieser Institutionen. Zudem zählen auch Angebote der politischen Bildung, wie z.B. der Wahl-O-Mat[6] der Bundeszentrale für politische Bildung, dazu.

Ziele von Partizipation

Bürgerbeteiligungsverfahren werden in erster Linie dazu eingesetzt, Entscheidungen stärker zu legitimieren und Bürger an Entscheidungsprozessen der Politik zu beteiligen [Schellong & Girrger, 2010]. Weiterhin soll den Bürgern die Möglichkeit gegeben werden, durch eigene Initiativen ihren Willen auszudrücken und die Politik zu beeinflussen. Partizipation soll das Zustandekommen von Entscheidungen transparenter, inklusiver und zugänglicher machen. Dem Bürger wird hierbei eine Einflussmöglichkeit in politische Geschehnisse eingeräumt, die er bei der repräsentativen Demokratie sonst nicht hat. Zudem soll es die Qualität der Kommunikation zwischen Politikern und Bürgern verbessern.

Bürgern wird ein stärkerer politischer Einfluss auf die Gestaltung ihres Umfeldes eingeräumt. Interessierte sollen auf die Entwicklung ihres Stadtteils oder bei der Verwendung von öffentlichen Geldern einwirken können. Somit wird die Demokratie begreifbarer und der Politikverdrossenheit in der Bevölkerung kann entgegengewirkt werden.

Zudem kann die Akzeptanz der Bürger für bestimmte Maßnahmen durch deren Beteiligung an den Planungen verbessert werden. So können mögliche Fehler frühzeitig durch die beteiligten Bürger erkannt werden. Anwohner betroffener Gebiete können ihre Bedenken, Ideen oder Verbesserungsvorschläge vor der Umsetzung bestimmter Pläne anbringen und somit kostspielige Nachbesserungen vermeiden. Somit wird die Planungsverantwortung auf mehrere Schultern verteilt.

Ein wichtiges Kriterium für die Partizipation von Bürgern ist die Motivation. Man muss dem Bürger erklären, warum es sich lohnt, sich an politischen Prozessen zu beteiligen. Ein Beispiel wäre die

[4] Siehe: http://wiki.vorratsdatenspeicherung.de/BKA-Petition_unterstützen (zuletzt Besucht: 09.04.2010)
[5] Siehe: http://www.abgeordnetenwatch.de/ (zuletzt Besucht: 09.04.2010)
[6] Siehe: http://www.wahl-o-mat.de (zuletzt Besucht: 09.04.2010)

mögliche Erhöhung der Lebensqualität in einem Stadtteil durch die Beteiligung an einem Bürgerhaushalt (siehe Kapitel 2.2.3.1).

Eine Studie von [Albrecht, et al., 2008] hat gezeigt, dass das Interesse an der Politik eher auf der Seite der formal besser Gebildeten liegt. Auch ältere Menschen und Bürger aus Großstädten haben ein höheres Interesse als junge Leute und Landbewohner. Zudem sind Männer eher an Politik interessiert als Frauen. Dieser Situation muss entgegengewirkt werden, um einen repräsentativen Durchschnitt der Bevölkerung einzubeziehen.

2.1.2 E-Government und E-Demokratie

Wie in der nachfolgenden Abbildung 2 veranschaulicht ist, wird klassisch das elektronische Regieren (E-Government) in verschiedene Untergruppen gegliedert [Wimmer, 2008]. Hierzu zählt die elektronische Verwaltung (E-Administration), die E-Demokratie (E-Democracy), die Vernetzung im Gesundheitssystem (E-Health) und viele weitere. Die internetgestützte, aktive Mitarbeit von Bürgern an politischen Prozessen fällt in die Kategorie E-Partizipation (E-Participation), die neben den elektronischen Wahlen (E-Voting) eine Untergruppe von E-Democracy darstellt.

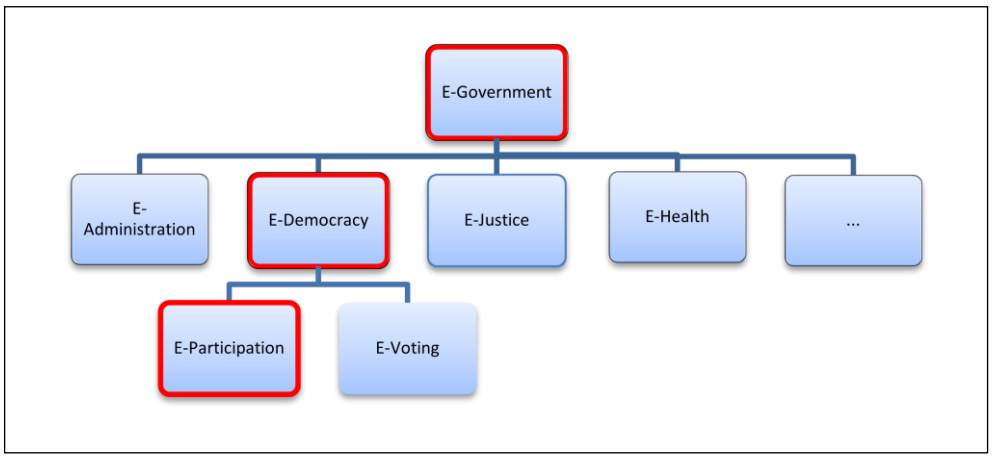

Abbildung 2. Einbettung von E-Partizipation in den Forschungskontext E-Government[7]

E-Government

Electronic Government oder E-Government steht für den Einsatz moderner Informations- und Kommunikationstechnologien im Bereich der Verwaltungs- und Regierungsaufgaben (engl. Government), also im gesamten öffentlichen Sektor, bestehend aus Legislative, Exekutive und Judikative, sowohl intern als auch im Behörden- bzw. Geschäftsverkehr mit Bürgern und Unternehmen. E-Government bezeichnet zum einen die Zielvorstellung, Verwaltungsleistungen bequem vom heimischen Computer aus in Anspruch zu nehmen und zum anderen den Veränderungsprozess dahin [Wimmer, 2008]. Dabei umfasst E-Government sowohl die lokale bzw. kommunale Ebene, die

[7] Quelle: [Wimmer, 2008]

regionale bzw. Landesebene, die nationale bzw. die Bundesebene sowie die supranationale bzw. globale Ebene [Lucke & Reinermann, 2000].

Die Akteure im Bereich des E-Government umfassen die Bürger (C), den Staat (G), die Wirtschaft (B) sowie Non-Profit und Non-Government Organisationen (N). Nach der „Speyerer Definition von Electronic Government“ [Lucke & Reinermann, 2000], die nur eine von vielen Definitionen zu E-Government darstellt, beinhaltet E-Government Prozesse innerhalb des öffentlichen Sektors (G2G), Prozesse zwischen diesem und der Bevölkerung (C2G und G2C), der Wirtschaft (B2G und G2B) sowie Non-Profit und Non-Government Organisationen (N2G und G2N). Tabelle 1 zeigt alle diese Beziehungen in einer Matrix, wobei die Bereiche des E-Government farblich hervorgehoben sind.

E-Government	Bevölkerung Bürger	Staat Verwaltung	Wirtschaft	NPO/NGO
Bevölkerung Bürger	C2C	**C2G**	C2B	C2N
Staat Verwaltung	**G2C**	**G2G**	**G2B**	**G2N**
Wirtschaft	B2C	**B2G**	B2B	B2N
NPO/NGO	N2C	**N2G**	N2B	N2N

Tabelle 1. Verknüpfung der Akteure im E-Government

E-Demokratie

Demokratie bedeutet im ursprünglichen Sinne die „Herrschaft des Volkes“. Der Begriff der elektronischen Demokratie (E-Demokratie) bezeichnet nach [Clift, 2003] die Verwendung von elektronischen Informations- und Kommunikationstechnologien durch demokratische Akteure wie Regierungen, gewählte Volksvertreter, Medien, politische Parteien, Bürgerorganisationen oder Wähler. [Trechsel, Kies, Mendez, & Schmitter, 2002] definieren E-Demokratie als alle Kommunikationsmittel, die den Bürger befähigen, die Regierenden für ihr Handeln im öffentlichen Raum zur Rechenschaft zu ziehen. Je nachdem, welcher Aspekt gefördert werden soll, stehen verschiedene Techniken zur Erhöhung der Transparenz, zur Verbesserung der direkten Beteiligung und Mitwirkung der Bürger und zur Verbesserung der Qualität der Meinungsbildung durch die Öffnung neuer Bereiche der Information und der Beratung zur Verfügung. Dies bezeichnet demnach den Einsatz von Partizipationsverfahren und Wahlen mit Hilfe von Informations- und Kommunikationstechnologien in öffentlichen Prozessen und soll den Diskurs zwischen Politik und Bürger fördern. E-Demokratie, als eine Unterkategorie des E-Government, kann als partizipative Ergänzung der gegenwärtigen Demokratie verstanden werden [E-Demokratie.org, 2010].

Neben der E-Partizipation umfasst E-Demokratie auch elektronische Wahlen als verbindlichste Form der Bürgerbeteiligung. Damit umfasst sie alle Bereiche, die die Information, die Diskussion, die Partizipation, die Interaktion und die Administration innerhalb einer Demokratie über das Internet fördern [Holznagel, 2001]. Politische Akteure stellen Informationen im Netz bereit und Bürger

informieren sich. Die Akteure der Demokratie können über das Internet politische Diskussionen führen und sich austauschen, gleichzeitig können Bürger an konkreten politischen Entscheidungen mitwirken und partizipieren. Über Meinungsumfragen oder Wahlen können Stimmungen eingefangen und verbindliche Entscheidungen getroffen werden.

2.1.3 E-Partizipation

Der Begriff E-Partizipation setzt sich aus den Begriffen „elektronisch“ und „Partizipation“ zusammen. E-Partizipation bezeichnet die Teilhabe von natürlichen und juristischen Personen (den sogenannten Stakeholdern) an politisch-administrativen Entscheidungs- und Willensbildungsprozessen mithilfe von Informations- und Kommunikationstechnologien [Albrecht, et al., 2008]. Durch die direkte Beteiligung von Bürgern in einer repräsentativen Demokratie wie in Deutschland können ganz neue Zielgruppen angesprochen und im politischen Entscheidungsprozess gehört werden. Mit Hilfe des Internets können Personen angesprochen werden, die nur wenig Interesse an Politik und klassischen Organisationen wie Parteien oder Verbänden zeigen [Wolff, 2006].

Durch die rasante Entwicklung des Internets Ende des 20. Jahrhunderts entstanden neben den klassischen Partizipationsmodellen auch neue Möglichkeiten der Bürgerbeteiligung. Das Internet, als neue Form elektronischer Medien, brachte einige Vorteile in der Beteiligung. So können Informationen rund um die Uhr und ohne räumliche Begrenzung abgerufen und bereitgestellt werden. Zudem werden durch das Internet die Eingriffs-, Auswahl-, Reaktions- und Steuerungsmöglichkeiten auf Informationen entscheidend erweitert und die mediengestützte interpersonelle Interaktion in einer neuen Qualität ermöglicht [Harth, 1999]. Diese neue Art der interaktiven Kommunikation, bei der man weder von Öffnungszeiten abhängig ist, noch zur einer Verwaltung fahren muss um teilzunehmen, prägt den Begriff der elektronischen Partizipation. Zudem verbleiben die Angebote über einen längeren Zeitraum im Netz, wodurch die Möglichkeit besteht, die entsprechenden Online-Angebote dann zu nutzen, wenn man die Zeit dazu hat. Zudem können Nutzer angesprochen und gehört werden, die in einer öffentlichen Veranstaltung, z.B. aufgrund eigener Beklommenheit, keine Wortbeiträge vor einem Publikum äußern würden [Wolff, 2006].

Abbildung 3. Vereinfachte Definition von E-Partizipation[8]

Abbildung 3 zeigt eine vereinfachte Form der Definition von E-Partizipation. Sie besteht aus der Beteiligung und der Nutzung von elektronischen Medien. Dabei beschränkt sich die Teilhabe nicht nur auf das Internet, sondern auch auf Medien wie Telefon und Fernsehen.

[8] Quelle: [E-Demokratie.org, 2010]

Neben der technischen Dimension beschäftigt sich E-Partizipation mit der Frage, wie man mithilfe der interaktiven Beteiligung zu konkreten Ergebnissen kommen kann, um den Bürger stärker einzubeziehen und seine Stimmung aufzunehmen. Eine Grundvoraussetzung für E-Partizipation ist die Transparenz. Sie entsteht durch E-Partizipation, ist aber auch Voraussetzung für diese. Eine Anforderung für Transparenz ist der kostenlose Zugang zu gut verständlichen Informationen. Zudem muss der Hintergrund für politische Entscheidungen bekannt sein. Es sollte der gesamte Entscheidungsprozess, also wer und wie involviert war und etwas beigetragen hat, klar und öffentlich zugänglich sein. Entscheidungs- und Gesetzesentwürfe sollten bereits im Vorfeld veröffentlicht werden [Wimmer, 2008]. Gute E-Partizipation basiert, wie klassische Beteiligungen, auf einem ausgewogenen Mix aus Information, Konsultation und Partizipation [E-Demokratie.org, 2010].

[Fraser, et al., 2006] unterscheidet auf Grundlage der Definition von Partizipation der OECD (vgl. [OECD, 2001]) und der Definition der „International Association for Public Participation“ (vgl. [IAP2, 2007]) vier Ebenen der E-Partizipation:

- **eInforming**: Eine einseitige Beziehung, in der die Regierung Informationen für die Bürger bereitstellt, um ein Verständnis für das Problem, Alternativen, Lösungen und Möglichkeiten zu erreichen.
- **eConsulting**: Eine beschränkte zweiseitige Beziehung, in der die Stakeholder eine Rückmeldung an die Regierung geben können und so ihre Meinung und Standpunkte zu speziellen Themen öffentlich oder geheim abgeben.
- **eCollaborating**: Eine erweiterte zweiseitige Beziehung, die auf einer Partnerschaft von Regierung und Bürger basiert, in der der Bürger aktiv an der Festlegung von politischen Entscheidungsfindungen beteiligt wird. Sie integriert den Bürger bei der Ausrichtung der Politik, die letzte Entscheidung liegt aber nach wie vor bei der Regierung.
- **eEmpowering**: Bezeichnet die höchste Stufe der Partizipation, in der die endgültigen Entscheidung in den Händen der Öffentlichkeit liegt.

Es gibt eine Vielzahl von Anwendungsbereichen der E-Partizipation in der öffentlichen Verwaltung. Tabelle 2 zeigt die wichtigsten Bereiche und erläutert diese kurz.

Kategorie	Beschreibung
Informationsbereitstellung (Information Provision)	IKT zur Bereitstellung, Strukturierung und Verwaltung von Informationen
Bildung von Communities / Kollaborativen Umgebungen (Community building / Collaborative Environments)	Einsatz von IKT zur Unterstützung von Individuen, um Gemeinschaften zu bilden und zu fördern und gemeinsame Ansichten zu entwickeln
Konsultation (Consultation)	IKT zur Ermöglichung eines Meinungsaustauschs über bestimmte Fragen zwischen privaten und/oder öffentlichen Beteiligten
Kampagnen (Campaigning)	Nutzung von IKT für kollektive Aktionen wie Protestaktionen, Lobbying oder Petitionen
Wahlkampf (Electioneering)	IKT zur Unterstützung von Politikern, Parteien und Lobbyisten im Rahmen des Wahlkampfes
Deliberation (Deliberation)	IKT zur Unterstützung von kleinen und großen virtuellen Gruppendiskussionen
Diskurs (Discourse)	IKT zur Unterstützung bei der Analyse und Darstellung von Diskursen
Mediation (Mediation)	IKT zur Beilegung von Streitigkeiten oder Konflikten in einem Online-Kontext
Raumplanung (Spatial planning)	IKT zur städtebaulichen und ökologischen Bewertung
Abstimmung (Polling)	IKT zur Messung der öffentlichen Meinung und Stimmung
Wahlen (Voting)	IKT im Rahmen der öffentlichen Stimmabgabe bei Wahlen, Referenden oder lokalen Volksabstimmungen

Tabelle 2. Zusammenfassung der E-Partizipations-Bereiche[9]

Die Gründe der Politik, sich die Meinungen der Bürger einzuholen, sind vielfältig. Politische Entscheidungsträger können Anregungen und Vorschläge von Bürgern aufnehmen und die Folgen von Alternativen ermitteln. Zudem können die Positionen und Präferenzen der Bürger festgestellt werden, um diese in die Entscheidungsfindung mit einfließen zu lassen, was zur größeren Akzeptanz der Bevölkerung für verschiedene Vorhaben führen kann. Durch die Bereitstellung von Hintergrundinformationen an die Bevölkerung können Problemlagen identifiziert und Alternativen kooperativ erarbeitet werden. Gerade wenn die Wissensbasis für Vorhaben unsicher, die Positionen unklar oder strittig und das Verständnis für dieses gestärkt werden soll, sind Online-Partizipationsvorhaben von Vorteil [Koop, 2010].

[9] Quelle: [Fraser, et al., 2006]

Für die Teilnahme an E-Partizipationsprozessen der öffentlichen Verwaltung sollte der Bürger einige Grundvoraussetzungen mitbringen [Wimmer, 2008]:

- Er benötigt eine Angebotskompetenz, d.h. er muss wissen, wo er Informationen finden und wie er mit technischen Hilfsmitteln des Internets wie E-Mail, Foren oder Suchmaschinen umzugehen hat.
- Es bedarf einer Anwendungskompetenz, d.h. er muss mit dem medienspezifischen Sprachgebrauch vertraut sein und über ein technisches Grundwissen verfügen.
- Zudem sollte eine Medienkompetenz vorhanden sein. Sie beinhaltet eine Reflexionsfähigkeit, um gefundene Informationen und die Vertrauenswürdigkeit von Quellen kritisch zu hinterfragen und zu wissen, ob man den Informationen trauen kann. Diese Medienkompetenz entwickelt sich meist durch eigene Erfahrungen, kann aber auch durch Weiterbildungs- und Förderprogramme geschult werden.

2.2 Das Internet als Instrument einer verstärkten Bürgerbeteiligung

> *„Demokratie lebt von gelingender Kommunikation. Kommunikationsbeziehungen zwischen politischen Führungsträgern und Bürgern, zwischen Bürgern untereinander oder zwischen Funktionsträgern und der (organisierten) Öffentlichkeit gehören zu den kulturellen Grundlagen der Demokratie. Wenn technische Entwicklungen Auswirkungen auf gesellschaftliche Kommunikationskulturen haben, sind sie daher von unmittelbarer Bedeutung für die Demokratie. Das Internet ist ohne Zweifel eine der gegenwärtig wichtigsten technischen Entwicklungen mit dem Potenzial zur Veränderung der kulturellen Grundlagen demokratischer Politik.“*
> [Grunwald, Banse, Coenen, & Hennen, 2006]

2.2.1 Internetnutzung in Deutschland

In den letzten Jahren hat sich das Internet als Leitmedium entwickelt und wird, gerade von der jüngeren Generation, mehr genutzt als alle anderen Medien. In Deutschland nutzten 2009, nach Daten der ARD/ZDF-Onlinestudie (vgl. [ARD/ZDF-Medienkommission, 2009]), 43,5 Millionen Bundesbürger ab 14 Jahren gelegentlich das Internet. Das entspricht 67,1 % der Bevölkerung. Im Vergleich zum Vorjahr war die Zahl der Internetnutzer leicht um 1,9 % angestiegen und gegenüber dem Jahr 2000 konnte ein Anstieg von rund 238 % verzeichnet werden. Während 2003 nur rund ein Viertel der Nutzer über einen Breitbandzugang verfügten, nutzten 2009 bereits 72 % diese schnelle Zugangsmöglichkeit in das Web, was eine enorme Steigerung gegenüber den Vorjahren darstellt. Abbildung 4 zeigt den Verlauf der Zugangsmöglichkeiten zum Internet.

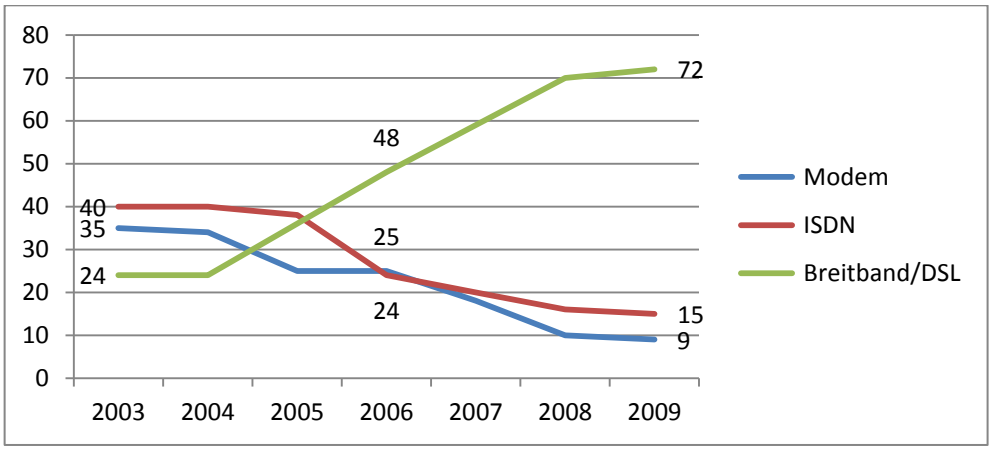

Abbildung 4. Internetzugang der Onlinenutzer ab 14 Jahre in Prozent[10]

Nach Abbildung 5 und Abbildung 6 sind innerhalb der Bevölkerung demographische und geschlechtsspezifische Unterschiede erkennbar. So nutzen ältere Menschen das Internet wesentlich seltener (über 60-jährige zu 27%) als junge Menschen (20-29-jährige zu 95%). Weibliche Personen nutzen das Internet seltener als Männer (60,1% zu 74,5%). Dennoch zeigen die Zahlen, dass eine Steigerung in allen Alters- und Geschlechtsklassen zu verzeichnen ist. Besonders bemerkenswert ist die Anzahl der jüngeren Internetnutzer, da in den Altersklassen von 14 bis 39 Jahren rund 90 % der Bürger online sind. Dies liegt vor allem daran, dass es für viele Menschen zur Normalität geworden ist, sich im World-Wide-Web zu informieren, Bankgeschäfte und Einkäufe zu erledigen, Anträge elektronisch auszufüllen und sich im Internet auszutauschen und zu kommunizieren [ARD/ZDF-Medienkommission, 2009].

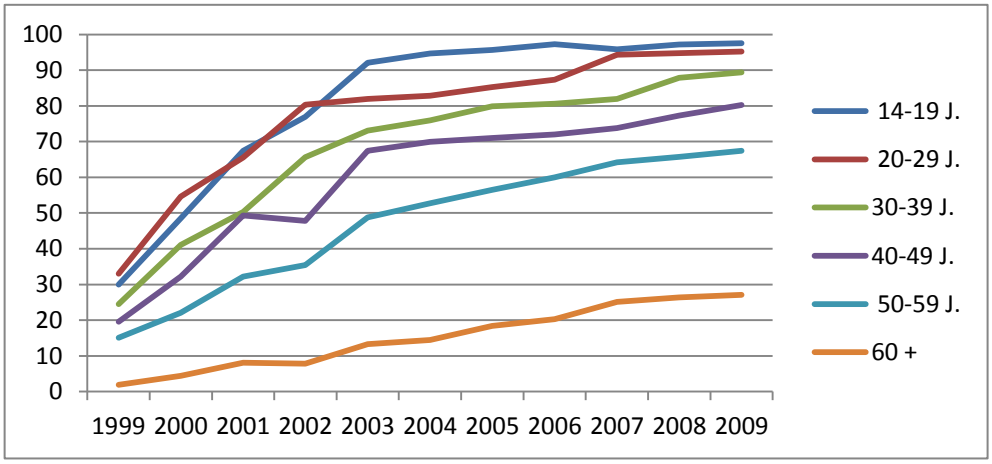

Abbildung 5. Entwicklung der gelegentlichen Onlinenutzung in Deutschland[11]

[10] Quelle: [ARD/ZDF-Medienkommission, 2009]
[11] Quelle: [ARD/ZDF-Medienkommission, 2009]

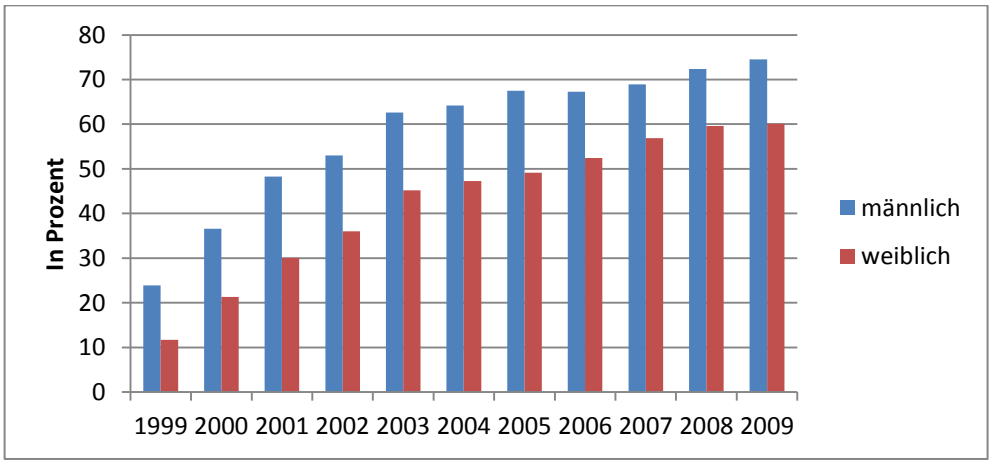

Abbildung 6. Entwicklung der gelegentlichen Onlinenutzung nach Männern und Frauen[12]

Nach der Studie „Monitoring Informationsgesellschaft“ des Bundesministeriums für Wirtschaft und Technologie konnten für das Jahr 2008 weitere Fakten abgeleitet werden [Bundesministerium für Wirtschaft und Technologie, 2009]. Demnach waren in Deutschland finanzschwächere Bürger weniger häufig online als wohlhabendere: Nur 41% der Bevölkerung mit einem Gehalt von unter 1000€ nutzten das Internet, dagegen waren Bürger mit einem durchschnittlichen Einkommen von über 3000€ zu 84 % vertreten. Zudem waren niedrigqualifizierte Personen weniger häufig online als hochqualifizierte: 87 % der Personen, die über Abitur oder einen Studienabschluss verfügten, hatten Zugang zu Web, Schüler sogar zu 95 %. Bei den Hauptschülern ohne Lehre fiel dieser Wert auf nur noch 33 %.

Ein ähnliches Ergebnis zeigt die Studie in Bezug auf die E-Government-Nutzung. So waren die Unterschiede nach Bildungsabschlüssen besonders groß. Personen mit einer niedrigen formalen Bildung nutzten E-Government-Angebote zu 34 % seltener als der deutsche Durchschnitt. Zudem stellte die Studie fest, dass sich jüngere (16-24 Jahre) und ältere (65-75 Jahre) Personen zu 27 bzw. 30 % weniger beteiligen als der Durchschnitt. Auch im Vergleich nach der Besiedelungsdichte konnten signifikante Unterschiede ausgemacht werden. So nutzen Personen in dicht besiedelten Gebieten E-Government-Angebote wesentlich häufiger als in mitteldicht oder dünn besiedelten Gebieten. Lediglich bei der Unterscheidung nach dem Geschlecht konnte eine Gleichberechtigung der Nutzer festgestellt werden [Bundesministerium für Wirtschaft und Technologie, 2009].

In den letzten Jahren ist dennoch ein signifikanter Anstieg der Internetnutzer über alle Bevölkerungsgruppen hinweg zu erkennen. Konnten zwischen 1997 und 2000 jährliche Zuwachsraten von 60 bis 68 % erzielt werden, schwächte sich die Steigerung in den letzten Jahren immer weiter auf aktuell rund zwei Prozent ab. Ursache sind die Wachstumsraten bei den jüngeren Internetnutzern, die bereits weitestgehend ausgeschöpft sind. Lediglich bei den ab 60-Jährigen sind in den nächsten Jahren noch Wachstumsmöglichkeiten vorhanden, da Hard- und Software immer benutzerfreundlicher werden und die Anschaffungs- und Betriebskosten sinken. Zudem steigt die Technikkompetenz der älteren Generation. Durch die allgegenwärtige Präsenz des Internets in Fernsehen, Radio und

[12] Quelle: [ARD/ZDF-Medienkommission, 2009]

Zeitungen, die in ihren Berichten immer öfter auf Websites verweisen, verändert sich die Einstellung der „Offliner“ zum Medium Internet. Ein weiterer -wenn auch schwächerer- Anstieg der Nutzerraten ist in den nächsten Jahren zu erwarten, was auch zu einer erhöhten Nutzung von E-Partizipationsanwendungen führen kann [ARD/ZDF-Medienkommission, 2009].

Inklusives E-Government hat das Ziel, alle Bevölkerungsschichten gleichermaßen zu erreichen. Unabhängig von demographischen oder sozioökonomischen Merkmalen sollen sich alle Bürger an E-Government-Angeboten beteiligen können. Mit Hilfe der vorgestellten Studien können die Gruppen der Bürger, die diese Angebote nur unterdurchschnittlich nutzen, erkannt werden. Hierzu zählen niedrige Bildungsschichten, die sehr junge und sehr alte Bevölkerung sowie Personen aus mittel und leicht besiedelten Gebieten. Die Politik sollte diese Gruppen gezielt fördern und Maßnahmen erarbeiten, um E-Government für sie attraktiver zu gestalten [Bundesministerium für Wirtschaft und Technologie, 2009].

2.2.2 Web 2.0

> *„Web 2.0 ist ... ein Medium, das durch mehr Nutzerbeteiligung, Offenheit und Vernetzungseffekte gekennzeichnet ist.“*
> [O'Reilly, 2005]

Seit Anfang der 1990er Jahre entwickelte sich das Internet zu einem immer wichtiger werdenden Werkzeug des Alltags, zunächst nur als Informationsplattform, über das man sich zu bestimmten Themen informieren und Unterlagen in elektronischer Form herunter laden konnte. Nach und nach drang dieses Medium in immer mehr Bereiche des öffentlichen Lebens vor und ist heute nicht mehr wegzudenken.

Das „alte“ Web 1.0 ist ein Massenmedienmodell, d.h. ein aktiver Anbieter erstellt einen Inhalt, viele passive Nutzer rufen diesen ab. Im Vordergrund steht die Informationsbereitstellung und Kommunikation vom Anbieter zu den Nutzern (Top-down). Zwischen Anbieter und Nutzer besteht eine „One-to-Many“ Beziehung (siehe Abbildung 7). Der Internetnutzer gilt in diesem Modell nur als passiver Zuschauer, der überwiegend auf einfache Homepages zugreift, aber keine oder wenige Möglichkeiten der Interaktion besitz. Echte Kommunikation aller Beteiligten ist hier eher die Ausnahme. Der komplette Inhalt wird durch Medien und nicht durch die Nutzer geprägt. Das Erstellen von Webseiten ist im Web 1.0 noch äußerst aufwendig, jeder Webmaster benötigt fundierte Kenntnisse in den Bereichen HTML, CSS und PHP, um selbst einfache Seiten zu erzeugen.

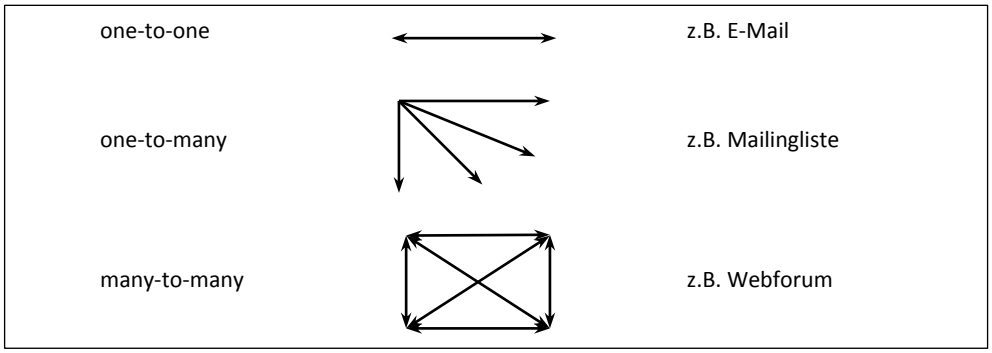

Abbildung 7. Definition von Kommunikationsformen[13]

Durch den Hype des „Web 2.0“ oder des sogenannten „Mitmach-Internets“ wurde Anfang 2004 ein neues Kapitel des weltweiten Netzes geschrieben. Von da an wurde das Internet neu aufgefasst und mehr als eine Kommunikationsplattform wahrgenommen. Der Nutzer wurde nicht mehr nur als Konsument, sondern als aktiver Part gesehen, der nun eigenständig Inhalte erstellt, bearbeitet und verteilt. Er bekam eine neue Rolle in dem bislang passiven Netz. Die Inhalte werden nicht mehr ausschließlich von großen Medienunternehmen erstellt, sondern von einer Vielzahl von Nutzern, die sich beispielsweise in sozialen Netzen vernetzen und gemeinsam Inhalte kreieren, ihr Leben in (Mikro-)Blogs veröffentlichen oder dabei helfen, das Web zu gestalten. Im Vordergrund stehen die Konversation und der Dialog der Beteiligten in einer „Many-to-Many“ Beziehung (siehe Abbildung 7). Viele Mitgestalter erstellen Inhalte („user generated content“), die von vielen Nutzern abgerufen, bearbeitet oder kommentiert werden können. Der gemeine Web 2.0-Nutzer braucht für dieses Konzept keine Programmierkenntnisse mehr. Er kann seine Meinungen in vorgefertigten Blogs äußern, seine Bilder auf Portalen wie z.B. Flickr.com und seine Videos auf z.B. YouTube.com bereitstellen. Web 2.0 Anwendungen setzen zudem oftmals auf die „Weisheit der Vielen“, wie zum Beispiel in diversen Wikis, die jeder Nutzer mit seinem speziellen Wissen füllen kann. Mittels einer einfachen Bedienoberfläche können z.B. in sozialen Netzwerken leicht persönliche Seiten erstellt werden, an denen andere Nutzer teilhaben und mitwirken können. Anstelle des „Top-down“ Prinzips wird im Web 2.0 „Bottom-up“, also von der Basis aus, gestaltet.

Dabei lassen sich verschiedene Stufen differenzieren [Bitkom, 2008]:

- Einmalige Bereitstellung von Inhalten (z.B. in YouTube oder Flickr)
- Dauerhafte Zusammenarbeit und Veränderung von bestehenden Inhalten von verschiedenen Nutzern (z.B. Mitarbeit in Wikis)
- Monolog, Dialog, Konferenzen (z.B. Erstellen von Blogs, Kommentare zu Blogs verfassen)

[13] Vgl.: [Sass, 2007]

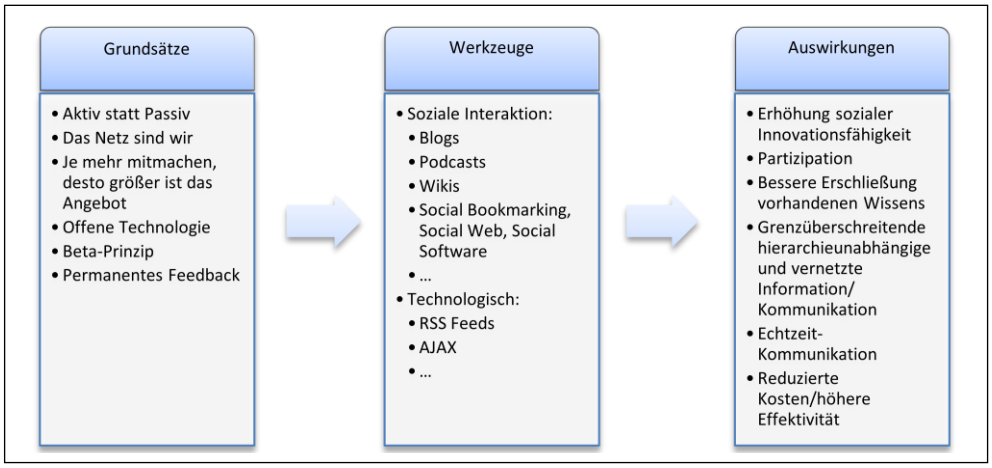

Abbildung 8. Grundsätze, Werkzeuge und Auswirkungen vom Web 2.0[14]

Zusammenfassend lässt sich sagen, dass das Web 2.0 das Internet nun stärker als Werkzeug des Austausches und der Kommunikation zwischen allen beteiligten Akteuren begreift. Durch diese Benutzer-Komponente im Internet wird Web 2.0 auch oftmals als Social-Web bezeichnet. Abbildung 8 zeigt noch mal zusammenfassend die Grundsätze, Werkzeuge und Auswirkungen vom Web 2.0.

Es gibt eine Vielzahl verschiedener Web 2.0 Angebote. Die folgende Aufzählung zeigt einige wichtige Angebote auf und erläutert diese kurz:

- **Wiki**: Ein Wiki (Hawaiianisch für „schnell“) stellt eine kollaborative Webseite dar, die aus Artikeln besteht, die alle Nutzer lesen und bearbeiten können. Jeder, der etwas zu einem bestimmten Thema weiß, kann dieses Wissen in Wiki-Artikeln veröffentlichen. Diese Artikel können von anderen Nutzern abgerufen, überprüft und korrigiert werden. Zu jedem Artikel gehört eine eigene Diskussionsseite, in der nicht selten weitere Fragestellungen entstehen, die sich gemeinsam mit anderen Nutzern lösen lassen. Durch eine große Zahl an Mitgliedern werden Falscheinträge meist sehr schnell erkannt und beseitigt. Durch ein komplexes Versionierungssystem können alle Änderungen nachvollzogen und notfalls rückgängig gemacht werden. Wikis zeichnen sich zudem durch eine hohe Zahl von Verlinkungen, sowohl zu externen Ressourcen, aber insbesondere auch zu anderen internen Artikeln, aus. Mit Wikis ist es möglich, durch die Beteiligung von vielen Akteuren schnell eine umfassende Wissenssammlung aufzubauen. Wikis haben eine eigene Syntax, um auf einfache und effektive Art und Weise Texte zu formatieren und Überschriften oder Listen zu erstellen.

- **Blog**: Ein Blog oder Weblog entspricht einem öffentlichen Online-Tagebuch oder Online-Journal. Ein Nutzer kann Einträge in Form von Texten, Bildern und Links für die Leser hinterlegen. Diese können anschließend für einzelne Artikel Kommentare verfassen oder diese bewerten. Besucher bekommen diese Einträge in umgekehrter chronologischer Reihenfolge präsentiert, dadurch haben Blogs meist einen endlosen Charakter. Blogs unterstützen oftmals RSS Feeds, mit denen man sich über neue Artikel oder Kommentare informieren lassen

[14] Quelle: [Bitkom, 2008, S. 9]

kann. In Unternehmen können Blogs sowohl zur internen als auch externen Kommunikation eingesetzt werden.

- **Microblog**: Relativ neu und sehr erfolgreich sind die Microblogs, als eine spezielle Form der Blogs. Bekanntestes Beispiel hierfür ist Twitter mit einer ungefähren Mitgliederzahl von 75 Millionen Menschen (im Januar 2010). Der Nutzer kann kurze SMS-ähnliche Texte mit einer maximalen Länge von 140 Zeichen schreiben, daher der Namenszusatz „Micro“ (griech. mikrós = klein). Nachrichten werden als "Tweets" (engl. tweet = zwitschern) bezeichnet. Die Nutzer-Accounts können von anderen Nutzern abonniert werden, diese Abonnenten nennen sich bei Twitter "Follower" (engl. follow = folgen). Sie bekommen auf der Startseite die neuesten Nachrichten der Nutzer, denen sie folgen, in chronologischer Reihenfolge angezeigt. Dort kann der Nutzer dann auch eigene Nachrichten verfassen, die wiederum den eigenen "Followern" angezeigt werden.

- **Soziale Netzwerke**: Soziale Netzwerke bauen auf das Kennenlernen oder Wiederfinden anderer Menschen im Netz. Sie haben alle dieselbe Vorgehensweise: Ein Benutzerprofil anlegen, persönliche Informationen hinterlegen und sich mit anderen Nutzern verknüpfen. In [Sass, 2007] werden dabei vier Typen von sozialen Netzwerken unterschieden.

    - *Friend-Networking***:** Man verknüpft sich mit bekannten Personen, meist aus dem Privatleben, tauscht Nachrichten aus und markiert sich und andere auf Bildern (z.B. StudiVZ.de, Facebook.com). Neu sind kleine Applikationen (sog. Apps), die ein User in seinem Nutzerprofil hinzufügen kann. Hierbei erfreuen sich insbesondere die Social Games (z.B. Farmville, Tetris oder Poker) großer Beliebtheit, die über die Netzwerke gespielt werden können.

    - *Hobbies/Interessen*: Nutzer mit gleichen Interessen verbinden sich und tauschen Informationen aus (z.B. 43things.com).

    - *Dating***:** Hierbei geht es vornehmlich um das Finden von Partnern für feste Beziehungen (z.B. FriendScout24.de, Elitepartner.de). Nutzer können ihr Aussehen, Interessen und Partnerwünsche hinterlegen und gezielt nach potentiellen Partnern suchen. Hier spielen auch Bilder eine große Rolle, anhand derer man die Attraktivität des Anderen beurteilen kann.

    - *Business***:** Das Finden von Geschäftsbeziehungen und das Anbieten oder Suchen von Stellenangeboten (z.B. XING.com) steht hier im Vordergrund.

  Innerhalb von Unternehmen können soziale Netzwerke genutzt werden, um die Teamdynamik zu erhöhen. Da die Produktivität in der Gruppe immer höher ist als die des Einzelnen, können im Internet ortsungebunden Kollegen oder Experten konsultiert werden, um schneller Lösungen für Probleme zu finden.

- **Videoplattformen**: Videoplattformen wie YouTube oder MyVideo erlauben es Nutzern, Videos bereitzustellen. Andere Nutzer können nach diesen Filmen suchen, sie ansehen und kommentieren. Meist ist das Einbinden von Videos in andere Webseiten möglich.

- **Social Tagging**: Tags sind Daten, die Informationen über andere Daten enthalten, sogenannte Metadaten. Nutzer können diese Schlagworte ohne spezielle Regeln Inhalten zuordnen und diese damit beschreiben, um so anderen Nutzern das Auffinden dieser Inhalte zu erleichtern. Mehrere Tags können in einer „Tag Cloud" visualisiert werden, wobei Schlagworte, die häufiger aufgerufen werden, größer dargestellt sind.

- **RSS**: RSS dient der einfachen und strukturierten Veröffentlichung von Änderungen auf Websites. Dabei wird ein standardisiertes Format (XML) verwendet. Ein Nutzer wird direkt bei der Veröffentlichung von neuen Inhalten ähnlich eines Nachrichtentickers mit kurzen Informationsblöcken versorgt, die eine Überschrift, einen kurzen Text und den Link zur Originalseite enthalten. Zum Lesen dieser sogenannten Feeds können Feedreader verwendet werden.

- **Mashup**: Mashup bezeichnet die Erstellung neuer Medieninhalte durch Kombination von bestehenden Inhalten des Webs, wie Texten, Daten, Bildern, Tönen oder Videos. Ein Beispiel ist die Verknüpfung von geographischen Daten auf einer Landkarte (z.B. Google Maps) mit dem Aufnahmeort von Fotos (z.B. Flickr) oder der Lage von z.B. Immobilienanzeigen.

Die Nutzung von Web 2.0 Anwendungen nimmt unter den Internetnutzern nach der ARD/ZDF-Onlinestudie 2009 immer weiter zu [ARD/ZDF-Medienkommission, 2009]. So wurden beispielsweise soziale Netzwerke 2009 vier Mal so häufig regelmäßig genutzt wie noch 2007. Aber auch Videoportale oder die Webseite Wikipedia verzeichnen in diesem Zeitraum Zuwachsraten von rund 40 bis 90 %. Eine Übersicht über die Nutzungshäufigkeit von Web 2.0 Anwendungen gibt die nachfolgende Tabelle 3.

	Gelegentliche Nutzung (zumindest selten)			Regelmäßige Nutzung (zumindest wöchentlich)		
	2007	2008	2009	2007	2008	2009
Wikipedia	47	60	65	20	25	28
Videoportale	34	51	52	14	21	26
Private Netzwerke	15	25	34	6	18*	24*
Fotosammlungen	15	23	25	2	4	7
Berufliche Netzwerke	10	6	9	4	2*	5*
Weblogs	11	6	8	3	2	3
Lesezeichensammlungen	3	3	4	0	1	2
Virtuelle Spielewelten	3	5	-	2	2	-

Tabelle 3. Nutzungshäufigkeit von Web 2.0 Angeboten 2009 (in Prozent) (* Nutzer mit eigenem Profil)[15]

Nachdem das Social Web in den vergangenen Jahren das Internet immer mehr erobert hat und derzeit knapp 40 % der Internetuser private Netzwerke und Communitys und knapp 60 % Videoportale nutzen, wird klar, dass auch Politiker und Parteien in diesen Netzen vertreten sein sollten. Das Social Web ist das Internet, so wie es heutzutage existiert. Es fördert die Kommunikation seiner Nutzer und gibt ihnen neue Werkzeuge an die Hand, um sich auf immer neue Art und Weise zu

[15] Quelle: [ARD/ZDF-Medienkommission, 2009]

organisieren. Gerade Jugendliche nutzen das soziale Netz meist, um sich im Internet zu präsentieren, ihre Vorlieben auf einer Pinnwand niederzuschreiben, sich mit ihren Freunden zu vernetzen und Gruppen zu bestimmten Themen beizutreten. Hierzu zählen beispielsweise Webseiten wie StudiVZ, Wer-Kennt-Wen oder Facebook.

Soziale Medien sind bereits aus dem Alltag nicht mehr wegzudenken. Sie werden in den nächsten Jahren noch enorm an Bedeutung gewinnen. Dies zeigen nicht zuletzt deren immense Zuwachsraten. So verzeichnete Facebook beispielsweise im Februar 2010 alleine in Deutschland 550.000 neue Mitglieder, was einer Steigerungsrate von 7,1% entspricht [Morrison, 2010]. In Twitter wurden im Januar 2010 ca. 39 Millionen Kurznachrichten pro Tag versendet, in 2008 waren es noch 300.000 und in 2007 lediglich 5.000 Tweets [Twitter Blog, 2010]. Twitter hatte im Januar 2010 ca. 75 Millionen Nutzer, wovon allerdings nur 15 Millionen Benutzer aktive Nutzer sind, die auch Inhalte einstellen [Evans, 2010]. Der Rest konsumiert lediglich Inhalte und informiert sich über Neuigkeiten. Flickr enthielt Ende 2009 bereits mehr als vier Milliarden Bilder [Champ, 2009]. Auf YouTube werden pro Minute 20 Stunden Videomaterial hochgeladen [Junee, 2009] und pro Tag eine Milliarde Videos angeschaut [The Sydney Morning Herald, 2009].

Aber auch private Organisationen wie Greenpeace setzen zur verbesserten Kommunikation ihrer Mitglieder verstärkt auf das Internet. So hat Greenpeace ein eigenes Portal eingerichtet, das ein internes soziales Netzwerk darstellt, in dem sich die ehrenamtlichen Mitglieder vernetzen können. Jedes Mitglied hat ein eigenes Profil, über das es Nachrichten austauschen, Leute kennenlernen und wiederfinden oder die eigenen Fähigkeiten einbringen kann. So kann die Kampagnenkommunikation schneller und direkter werden, was eine erhöhte Effizienz zur Folge hat. Darüber hinaus kann jedes Mitglied einen eigenen Blog einstellen, Rundbriefe versenden und gemeinsame Kalender sowie Wikis benutzen, was die Zusammenarbeit unterstützt [Schulzki-Haddouti, 2010]. Aber auch der Arbeitskreis Vorratsdatenspeicherung oder die Free Software Foundation nutzen Social Web-Dienste, um ihre Mitglieder und Kampagnen weltweit zu koordinieren und Kontakt unter ihren Mitgliedern herzustellen.

2.2.3 Bürgerbeteiligung 2.0

Immer mehr Bürger engagieren sich im Internet, insbesondere die jüngere Generation, die mit dem World-Wide-Web aufgewachsen ist. Sie sehen das Internet als einen Fortschritt des täglichen Lebens an. Laut einer Umfrage von BITKOM sehen 96 % der Befragten das Internet als einen Gewinn an nützlichen Informationen und 90 % als Verbesserung der Lebensqualität an [Bitkom, 2010]. Gerade das Web 2.0 ist darauf ausgerichtet, jedem Nutzer eine Teilnahme mit geringem Aufwand zu ermöglichen. Die neuen Freiheiten des Internets führen dazu, dass sich das Kommunikationsverhalten der Bürger verändert. Die Bürger informieren sich im Web, beteiligen sich an Foren oder wickeln ihre Bankgeschäfte und Einkäufe elektronisch ab. Es wartet keiner mehr ausschließlich auf den Briefträger, der einmal am Tag kommt und die Post bringt, die elektronischen Postfächer der E-Mails werden täglich mehrfach geleert. Die Transparenz, die ein Kunde von einem Paketdienst bekommt, wenn er weltweit den Versandweg seiner Pakete verfolgen kann, erwartet er in einem entsprechenden transparenten Arbeitsablauf auch von seiner Verwaltung. Es sinkt die Bereitschaft, sich zeitlichen

und örtlichen Einschränkungen zu unterwerfen und sich zu festgesetzten Zeiten an bestimmten Orten zu treffen, um an Politikprozessen teilzunehmen. Hinzu kommt, dass sich Bürger in klassischen Organisationen, wie Parteien und Verbänden, immer weniger engagieren. Gleichzeitig steigt die Bereitwilligkeit, sich öffentlich mitzuteilen [Bitkom, 2008]. Die Bürger gewöhnen sich daran, sich rund um die Uhr öffentlich (z.B. in Foren) äußern zu können. Sie sind immer vernetzter, was ihnen ebenso neue Formen der politischen Mobilisierung ermöglicht [Koop, 2010]. Daher ist es eine Aufgabe der Politik, sich an diesem Dialog zu beteiligen. Inzwischen nutzen Politiker immer öfter das Internet, um Bürger zu informieren und um ihre Zustimmung zu werben. Gerade in Wahlkampfzeiten wird mit Hilfe von Videokanälen, Chats und Blogs um Stimmen geworben.

Im „alten" Web 1.0 Modell ist noch keine Diskussion zwischen Bürgern und Verwaltungen möglich. Die eine Seite fragt, die andere antwortet, wenn z.B. die Verwaltung den Bürger per Webformular befragt. Die Möglichkeit der Bürger, der Politik eine Rückmeldung zu geben, ist stark begrenzt. Der Austausch von Argumenten sowie ein transparentes Verfahren sind nicht möglich. Probleme werden hier meist nur isoliert behandelt, ein ganzheitlicher Ansatz ist so nicht denkbar. Dabei wollen Bürger nicht nur angesprochen und informiert werden, sondern auch mitreden.

Die neue Betrachtungsweise vom Web 2.0 bietet hervorragende Bedingungen für Beteiligungsprozesse der Politik, da die Grundsätze wie Mitmachen, Mitbestimmen oder Selbstverwaltung eine Schnittmenge beider Welten darstellt. Sie machen es dem Bürger möglich, sich in einer Diskussion an konkreten Projekten zu beteiligen und diese mit zu gestalten. Behörden leiten und strukturieren die Diskussion, stellen zu bestimmten Themen gezielt Hintergrundinformationen bereit und fixieren Zwischenergebnisse. Im Web 2.0 ist es üblich, permanent öffentliche Feedbacks zu geben. Hierdurch werden Webinhalte und Meinungen anderer Nutzer kontinuierlich bewertet und kommentiert. Diese „Ratings" oder „Peer-Reviews" eigenen sich auch hervorragend für die Bewertung von Planungsvorhaben mit öffentlichem Interesse, wenn Bürger ihre Kommentare, Anregungen oder Kritiken zu bestimmten Sachverhalten äußern können.

Die in der Privatwirtschaft schon lange genutzten Web 2.0 Technologien, wie beispielsweise in Online-Shops oder auf Firmen-Webseiten, haben auch im Bereich der Bürgerbeteiligung ein großes Potential. Printmedien, Hörfunk und das Fernsehen arbeiten ausschließlich in eine Richtung und definieren damit unabänderlich die Rolle von Sender und Empfänger. Das Internet und insbesondere das Web 2.0 hingegen arbeitet mit einer bidirektionalen Kommunikation und ist durch eine zweiseitige Kommunikation gekennzeichnet [Kleinsteuber, 2001]. Durch die Auflösung der Passivität der Adressaten kann das Internet sowohl zur Kommunikation zwischen Bürgern untereinander, als auch zwischen Bürgern und Politikern genutzt werden. Durch die neuen Konzepte des Internets kann es den Bürgern in Zukunft möglich sein, sich einfach, zeit- und ortsunabhängig zu bestimmten Verfahren zu äußern und mit anderen Bürgern zu diskutieren. Außerdem wird durch das Internet eine wesentlich jüngere Zielgruppe angesprochen, die durch eine vertraute Technik ermuntert werden kann, sich in die lokale Politik einzuschalten und zu partizipieren. Jeder Bürger kann seine eigene Position veröffentlichen und Stellungnahmen anderer Bürger sowie politischer Akteure einsehen und bewerten. Gleichzeitig erhöht sich die Transparenz und Nachvollziehbarkeit von öffentlichen Entscheidungen.

In der Verwaltung kann der Einsatz von Web 2.0 Anwendungen die Kommunikation und Diskussion erhöhen. So können gezielte Informationen und die Förderung des Dialogs zwischen Verwaltung, Bürgern und Politik dazu führen, dass der Bürger ein verstärktes Interesse an der Politik bekommt, sich eher beteiligt und sich dadurch die Anzahl der Teilnehmer erhöht. Die Politik kann so Unterstützer für ihre Vorhaben gewinnen und das Vorgehen besser legitimieren. Außerdem schafft Partizipation eine Identifikation des Bürgers mit beispielsweise bestimmten Projekten die ihn direkt betreffen. Zusätzlich erhöht sich das Vertrauen in die Politik durch ein tiefergehendes Verständnis der Bürger für politische Prozesse [Schellong & Girrger, 2010].

Voraussetzung für diese Möglichkeiten der Partizipation sind zum einen der flächendeckende Zugang der Bürger zu einem schnellen Internet und zum anderen eine gewisse Medienkompetenz der Nutzer. Das bedeutet, dass die Nutzer wissen müssen, wo sie Informationen im Netz finden und wie sie damit umzugehen haben (z.B. technisches Grundwissen). Zudem sollten sie Angebote immer kritisch nach der Zuverlässigkeit der Quelle hinterfragen und ob die Inhalte Meinungen manipulieren. Um dies zu fördern, könnte man die Bürger im Umgang mit Computern und Inhalten schulen. Außerdem sollte die Benutzerfreundlichkeit und Sicherheit bei den Angeboten im Vordergrund stehen. Eine Studie der Universität Mannheim untersuchte die Einflussfaktoren, die eine Nutzungswahrscheinlichkeit von E-Partizipationsanwendungen verbessern. Demnach führte die Einfachheit und Nutzbarkeit eines Angebots zu einer erhöhten Bereitschaft, dieses zu nutzen [Schoppé, Parasie, & Veit, 2009]. Da dies mit den bekannten Web 2.0-Technologien möglich ist und sie von Online-Nutzern regelmäßig verwendet werden können, könnte der Einsatz dieser Technologien im Bereich der Partizipation helfen, die Nutzungsbereitschaft zu erhöhen.

Neue Techniken bringen immer ein gewisses Risiko mit sich. Daher muss hinterfragt werden, wie sicher die Technik ist und welche Wagnisse mit politischen Informationen im Internet eingegangen werden. Außerdem muss ein Missbrauch personenbezogener Daten und die Manipulation der Meinungsäußerungen verhindert werden. Hierbei kann als positiver Aspekt die mittlerweile jahrelange Nutzung und Erprobung von Web 2.0 Techniken im kommerziellen Umfeld gesehen werden. Viele Gefahrenquellen sind bereits identifiziert und können mittels technischer und/oder organisatorischer Maßnahmen begegnet werden.

Dennoch bedarf es der Aktivität des Bürgers, sich in der Politik einzubringen. Die Politik kann die Rahmenbedingungen schaffen, um eine Beteiligung der Bürger einfach und komfortabel zu ermöglichen. Der Bürger jedoch muss von sich aus tätig werden und die neuartigen Möglichkeiten auch annehmen und nutzen. Hierbei spielen auch Gesichtspunkte der Sicherheit eine große Rolle. Zum Beispiel will der Nutzer wissen, wer seine Daten bekommt und was damit gemacht wird.

Nachfolgend werden einige Beispiele für E-Partizipationsangebote vorgestellt, die im weiteren Kontext der Arbeit relevant sind.

2.2.3.1 Bürgerhaushalte

Die Idee, den Bürger bei der Haushaltsplanung einzubeziehen, wurde erstmals in der brasilianischen Stadt Porto Alegre und in Neuseeland im Jahr 1989 umgesetzt. Seitdem gewinnt der kommunale

Bürgerhaushalt weltweit immer mehr an Bedeutung und wird inzwischen in hunderten von Kommunen eingesetzt [Schwartig & Vorwerk, 2010].

Der Unmut der Bürger bei politischen Fehlentscheidungen bekommt durch die Onlinewelt immer größere Dimensionen, gerade wenn öffentliche Einrichtungen wie Schwimmbäder oder Schulen geschlossen werden. Zudem wollen Verwaltungen, wenn es darum geht Einsparungen aufgrund einer angespannten Finanzlage umzusetzen, den Bürger in die Entscheidungen miteinbeziehen [Stadt Solingen, 2010]. Daher geht die Politik in einigen Städten den kooperativen Weg. Sie lassen die Bürger über die Verwendung öffentlicher Gelder über die Bürgerhaushalte mitentscheiden. Diese Online-Dialoge verändern die politische Kultur in einer Kommune, indem Bürger intensiver eingebunden werden. Neben den Vorteilen kann dies aber auch zu Enttäuschungen auf beiden Seiten führen. Der Rat hat nach wie vor die Entscheidungsgewalt, nicht die Bürger. Trotzdem sind die Vorschläge der Bevölkerung prägend für die Ratsentscheidung [Schwartig & Vorwerk, 2010]. Bürgerhaushalte können zur inhaltlichen Verbesserung eines Vorhabens genutzt werden, denn sie können Probleme identifizieren und mögliche Lösungswege und Alternativen ermitteln. Im Gegensatz zu Studien oder Gutachten erlauben Bürgerhaushalte ein breit verteiltes Wissen und vielfältige Erfahrungen unterschiedlicher Experten sowie Betroffener und Interessierter aufzunehmen. Durch die Mitwirkung verschiedener Interessengruppen werden zusätzlich die Entscheidungsfindung und die Umsetzung von Vorhaben durch eine größere Akzeptanz und Legitimität erleichtert [Koop, 2010].

In Bürgerhaushalten ist die bislang höchste Partizipationsebene realisiert, in der die Beteiligung über das Informieren und Konsultieren hinaus geht, die Bürger aktiv über den Haushalt ihrer Stadt mitentscheiden dürfen und in den Entscheidungsprozess involviert werden. Dabei verfolgen Bürgerhaushalte in erster Linie die Ziele, dem Bürger die Haushaltsplanung der Stadt verständlicher zu machen, eine Beteiligung zu ermöglichen und so den Dialog zwischen Politik und Bürger zu intensivieren. Leider konnte sich dieses Instrument der Bürgerbeteiligung in Deutschland noch nicht flächendeckend durchsetzen. Von den 50 bevölkerungsreichsten Städten Deutschlands nutzen bislang nur 20% die Möglichkeit des Bürgerhaushalts (vgl. Kapitel 2.4).

Ein Bürgerhaushalt besteht meist aus drei Bausteinen: Der Bevölkerung Information zur Verfügung zu stellen, einen Dialog mit dem Bürger über verschiedene elektronische Medien zu führen und die Entscheidung des Rats mit einem Rechenschaftsbericht an den Bürger zu begründen [Stadt Köln, 2009]. Dabei gliedert sich ein Bürgerhaushalt meist in drei Phasen: In der ersten Phase werden Vorschläge gesammelt, die kommentiert und diskutiert werden können. In der zweiten Phase werden die vorhandenen Vorschläge von den Bürgern positiv oder negativ bewertet, hier können keine neuen Vorschläge mehr angegeben werden. In der letzten Phase werden die bestbewerteten Vorschläge von der Verwaltung diskutiert, über ihre Umsetzung entschieden und die Entscheidung vor dem Bürger begründet.

In dieser Arbeit wird eine Auswahl verschiedener Bürgerhaushalte untersucht: Die Bürgerhaushalte Köln, Hamburg, Trier, Lichtenberg und Solingen, die alle relativ fortgeschrittene Online-Lösungen darstellen und sich einer Vielzahl von E-Partizipations-Tools bedienen. Zudem werden die meisten der gewählten Angebote wiederholt durchgeführt, was für die Ernsthaftigkeit der Bürgerhaushalte spricht. Im Folgenden werden die einzelnen Haushalte kurz vorgestellt:

Der **Bürgerhaushalt Köln** wurde erstmals 2007 unter dem Motto „Deine Stadt, Dein Geld“ durchgeführt. Dabei haben mehr als 10.000 Bürger über 5.000 Vorschläge auf der Webseite https://buergerhaushalt.stadt-koeln.de eingebracht. Der aktuelle Bürgerhaushalt 2010 beschäftigt sich schwerpunktmäßig mit den Themen Bildung/Schule und Umweltschutz. Bürger können ihre Vorschläge und Anregungen schriftlich, telefonisch oder über das Internet einbringen. Der Bürgerhaushalt in Köln konnte 2009 den European Public Sector Award des Europäischen Instituts für öffentliche Verwaltung (European Institute of Public Administration) gewinnen [Stadt Köln].

Bei dem **Bürgerhaushalt Hamburg** können Bürger ihren eigenen, nach persönlichen Schwerpunkten ausgerichteten Haushaltsplan unter www.buergerhaushalt-hamburg.de aufstellen. Dazu wird der Bürger mit Kennzahlen und Hintergrundinformationen zu den 12 Hamburger Haushaltsbereichen informiert. Mit Hilfe eines Schiebereglers können die Nutzer die einzelnen Budgets erhöhen oder verringern. Zusätzlich können Bürger Begründungen angeben und in einem gesonderten Forum über die Haushaltsplanung diskutieren. Insgesamt besuchten bei der erstmaligen Durchführung des Bürgerhaushaltes in 2009 knapp 3.800 Bürger und Bürgerinnen den Bürgerhaushalt und 552 Nutzer registrierten sich auf der Webseite [Stadt Hamburg, 2010].

Der **Bürgerhaushalt Trier** wurde im Jahr 2009 zum ersten Mal unter www.buergerhaushalt-trier.de durchgeführt. Dabei wurden 512 Vorschläge abgegeben, von denen 143 Vorschläge, die von den Bürgern eine positive Bewertung bekamen, durch Verwaltung und Rat geprüft wurden. Insgesamt konnten im Jahr 2009 49 Sparideen, 43 Einnahmevorschläge und 51 kostenneutrale Vorschläge betrachtet werden. Es beteiligten sich über 1.500 Personen, die 628 Kommentare formulierten und 57.538 Einzelbewertungen abgaben. Teilnahmeberechtigt an dem Bürgerhaushalt sind ausschließlich Bürger mit Wohnsitz in Trier [Stadt Trier, 2010].

Der **Bürgerhaushalt Lichtenberg** führte 2009 die fünfte Beteiligung unter der Webadresse www.buergerhaushalt-lichtenberg.de durch. Dabei werden Vorschläge für die Haushalte im übernächsten Jahr abgegeben, so stimmten die Bürger in 2009 für den Haushalt 2011 ab. Es registrierten sich auf der Online-Plattform insgesamt 2.679 Personen, die 83 Vorschläge verfassten. Dazu kamen noch 158 Vorschläge, die bei 14 Stadtteilkonferenzen mit 1066 Teilnehmern offline formuliert wurden. An einem Votierungstag stimmten 256 Personen Online und 2.536 Personen an 26 Standorten über die Vorschläge ab [Stadt Lichtenberg, 2010].

Die Stadt **Solingen** in Nordrhein-Westfalen führt 2010 den ersten Bürgerhaushalt unter www.solingen-spart.de durch. Ausgangslage für die Einführung des Bürgerhaushalts ist die schlechte Finanzlage der Kommune. Daher wird er hier als Instrument verstanden, die Bürgerinnen und Bürger beim Sparen als Ratgeber und zur Prioritätensetzung einzubeziehen, um Einsparungen vor dem Bürger besser legitimieren zu können. Während der Beteiligungsphase vom 4. bis zum 26. März hatten sich 3.595 Teilnehmer in dem Portal registriert. Diese gaben rund 4.750 Kommentare und mehr als 150.000 Pro- und Contra-Stimmen ab. Insgesamt wurden der Verwaltung 78 Vorschläge vorgelegt [Stadt Solingen, 2010].

2.2.3.2 Parteiwebseiten/Politische Netzwerke

Was zu Zeiten von John F. Kennedy das Fernsehen war, ist heute das Internet. Kennedy wusste zu seiner Zeit schon, im Wahlkampf moderne Medien wie das Fernsehen für sich zu nutzen und erfolgreich einzusetzen, was Barak Obama aufnahm und im Wahlkampf 2008 mit dem Internet fortsetzte. So waren soziale Netzwerke für Obama die Königsdisziplin der Online-Kommunikation. Er erstellte früh eine Wahlkampf-Homepage, mit dessen Hilfe er hunderte von Millionen Dollar Spenden sammelte und knapp zwei Millionen freiwillige Helfer rekrutieren konnte. Jeder Bürger konnte Obama, mit nur wenigen Klicks über ein Online-Formular, eine Wahlkampfspende zukommen lassen. Zwei Tage nach der Wahl Obamas öffnete sein Team die Webseite change.gov. Darauf können sich Amerikaner in einem Blog über aktuelle Neuigkeiten informieren, sich um Arbeitsplätze in der Regierung bewerben oder sich als freiwillige Helfer in Schulen oder im Gesundheitswesen melden.

Inzwischen haben auch alle wichtigen Parteien in Deutschland zur Mitgliedergewinnung und für den Wahlkampf das Web 2.0 entdeckt. Neben Facebook, Twitter und Co. rücken auch parteiinterne soziale Netzwerke immer stärker in den Mittelpunkt der Online-Strategie von Parteien. Ziel der politischen sozialen Netze ist es, möglichst viele Kontakte zu knüpfen und den Adresspool der eigenen aktiven Anhänger zu vergrößern. So können lang andauernde Bindungen aufgebaut und der Bestand an aktiven Unterstützern erhöht werden. Was Obama vorgemacht hat, wollen nun die deutschen Parteien wiederholen [Brauckmann, Webwahlkampf: Was die Parteien wollen - und können, 2009].

Diese Arbeit betrachtet zwei große Parteiwebseiten von der SPD (meineSPD) und der FDP (my.FDP), die beide als soziale Netzwerke aufgebaut sind. Sie sollen den Dialog der Mitglieder fördern und kommende Wahlen unterstützen. Dabei darf jeder Internet-Nutzer grundsätzlich an den Angeboten teilnehmen. Mitglieder der jeweiligen Parteien können sich zusätzlich mit ihrer Mitgliedsnummer ausweisen. Sie bekommen so Zugang zu internen Bereichen und werden in ihrem Profil als „verifiziert“ markiert. Bei dem Angebot der SPD steht die Einbindung von Parteimitgliedern in laufende Debatten und Themendiskussionen im Vordergrund. Zudem soll die Plattform bestehende Mitglieder aktivieren sowie Unterstützer untereinander organisieren und vernetzen [SPD, 2010]. Die FDP stellt mit ihrem Angebot eines der ältesten politischen sozialen Netzwerke dar. Das Netzwerk my.fdp.de soll FDP Mitglieder vernetzen und eine Diskussion untereinander erlauben. Auch Aktionsplanungen oder Online-Kampagnen können hierüber koordiniert und umgesetzt werden. Mit einem Messenger, der auf dem heimischen PC installiert werden kann, wird der Online-Status eigener Kontakte angezeigt und man kann mit anderen Mitgliedern chatten. Für Wahlkämpfe ist die Seite um die Plattform mitmachen.fdp.de ergänzt, die auf Aktionen und Kampagnen ausgelegt ist und diese über das Netz organisiert [FDP-Bundespartei, 2010].

2.2.3.3 E-Konsultation

Online-Konsultationen haben das Ziel, mit Hilfe der Bürger ein Vorhaben zu verbessern oder Befindlichkeiten aufzunehmen. Dabei sollen Erfahrungen erfasst und Positionen und Präferenzen

festgestellt werden. Über eine gemeinsame Diskussion sollen Standpunkte und eine Marschrichtung, die aus einem größtmöglichen Konsens besteht, festgelegt werden.

In dieser Arbeit wird das Konsultationsangebot „Perspektiven deutscher Netzpolitik“ des Bundesministeriums des Innern (BMI) untersucht. Bei diesem Angebot diskutiert der Bundesminister des Inneren Dr. Thomas de Maizière mit Onlinenutzern in einem offenen Dialog über Meinungen und Ideen zu dem Thema. Es umfasst dabei die vier Schwerpunkte „Datenschutz und Datensicherheit im Internet“, „Das Internet als Mehrwert erhalten“, „Staatliche Angebote im Internet“ sowie „Schutz der Bürger vor Identitätsdiebstahl und sonstiger Kriminalität im Internet“. Neben dem Online-Dialog umfasst das Angebot auch vier offline Veranstaltungen zu den einzelnen Schwerpunkten. Die Ergebnisse des Dialoges sollen in die Netzpolitik des Bundesinnenministeriums einfließen und die zukünftige Gesamtstrategie „Deutschland Digital 2015“ der Bundesregierung beeinflussen [Bundesministerium des Innern, 2010].

2.2.3.4 E-Petitionen

Seit Gründung der Bundesrepublik Deutschland im Jahr 1949 kann sich jeder Bürger mit einer Petition an den Bundestag wenden. Lange ging das nur per Brief, Postkarte oder Fax und vor allem unter Ausschluss der Öffentlichkeit. Seit 2005 gibt der Deutsche Bundestag seinen Bürgern die Möglichkeit, Petitionen über das Internet einzureichen – einfach und schnell. So ist es möglich, Einzel- oder öffentliche Petitionen auf einer Online-Plattform zu verfassen und öffentlich Mitstreiter zu suchen. Kommen innerhalb von sechs Wochen mindestens 50.000 Unterschriften zusammen, muss sich der Petitionsausschuss mit diesem Anliegen in einer öffentlichen Sitzung befassen.

Einzelpetitionen enthalten individuelle Bitten oder Beschwerden und werden anonym an den zuständigen Ausschuss übermittelt. Bei öffentlichen Petitionen werden das Anliegen und die Begründung zusammen mit dem vollständigen Namen des Einreichenden für sechs Wochen im Internet veröffentlicht. Andere Personen können die Petition in diesem Zeitraum durch eine „Mitzeichnung“ unterstützten. Auch diese Personen erscheinen öffentlich auf der Online-Plattform. Daneben haben die Benutzer die Möglichkeit, über die Petitionen in einem Forum zu diskutieren [Deutscher Bundestag, 2010].

2.3 Gefahren

Da die positiven Erwartungen an eine verstärkte und bessere Politikbeteiligung durch das Internet sehr hoch sind, ist es wichtig, auch die negativen Folgen zu diskutieren.

2.3.1 Gefahren der E-Partizipation

Ein großes Problem der direkten Beteiligung ist das sogenannte „Digital Divide“, also einer Zweiklassengesellschaft innerhalb der E-Partizipation. So besteht die Gefahr, dass Bürger, die keine Zugangsmöglichkeit zu elektronischen Inhalten haben, weil sie nicht über die Kompetenz verfügen mit neuen

Internet-Technologien umzugehen, es sich nicht leisten können oder regional ausgegrenzt sind, nicht an den Beteiligungsprozessen über das Internet teilnehmen können [Wimmer, 2008]. Dies bedeutet den dauerhaften Ausschluss ganzer Bevölkerungsschichten von wichtigen neuen Formen der politischen Information, Kommunikation sowie Partizipation.

Zudem könnten, gerade ältere Bürger, durch die Informationsüberflutung des Internets überfordert werden [Grunwald, Banse, Coenen, & Hennen, 2006, S. 67]. Wenn eine qualifizierte Qualitätsprüfung der Daten fehlt, wären Bürger wie auch Politiker mit einer Trennung zwischen relevanten und irrelevanten Informationen konfrontiert. Die Beurteilung der Vertrauenswürdigkeit der Daten würde auf Seiten der Nutzer geschehen, womit diese, gerade bei einer geringen Medienkompetenz, oftmals überfordert wären. Dies führt zu einer Abhängigkeit von technischen Hilfsmitteln wie z.B. Suchmaschinen, was wiederum eine Abhängigkeit von Dritten hervorruft.

Auch die Frage, wer an der Partizipation über das Internet teilnimmt, ist noch weitestgehend offen. So ist nicht ganz klar, ob bei E-Partizipationsprozessen dieselben Gruppen, Personen oder Lobbys vertreten sind, die sich auch in den klassischen Beteiligungsformen einbringen. Sie könnten, wenn keine ausreichende Steuerung oder Kontrolle durch Moderatoren vorhanden ist, Einfluss auf die restlichen Teilnehmer nehmen, indem sie sie unter Druck setzten und so die Beteiligung in ihrem Sinne beeinflussen [Wolff, 2006].

2.3.2 Gefahren im Social Web

Soziale Netze sind ein durchaus probates Mittel, um dem Bürger eine Möglichkeit der Partizipation zu geben. Das Web 2.0 zählt mit seinen vielfältigen Kommunikationsmitteln wie (Micro-) Blogs, Wikis oder Tagging zu den modernen Mitteln politischer Arbeit. Aber es sind auch vielfältige Gefahren damit verbunden. Deshalb ist es wichtig, den Nutzern sowohl auf der Bürger- als auch auf der Politikerseite Leitlinien über bestimmte Verhaltensweisen mit an die Hand zu geben. So sollte verhindert werden, dass zum Beispiel in geheimen Abstimmungen Informationen vor der offiziellen Verkündigung öffentlich gemacht werden. Dies geschah beispielweise bei der Wahl des Bundespräsidenten am 23.05.2009. Noch vor der offiziellen Verkündigung des Wahlausgangs twitterten zwei Abgeordnete das Wahlergebnis, darunter ein Mitglied, das bei der Stimmenauszählung persönlich beteiligt war. Dies kann auch zu rechtlichen Folgen für die Mitarbeiter führen, in diesem Fall insbesondere wegen der Verletzung des Wahlgeheimnisses [Heise Online, 2009].

In den meisten Verwaltungen existieren bereits seit vielen Jahren Regeln, wie beispielsweise eine E-Mail auszusehen hat oder welches Format Briefe haben sollen. Was allerdings in den meisten Verwaltungen (aber auch in privatwirtschaftlichen Unternehmen) fehlt, sind Handlungsempfehlungen für den Umgang mit sozialen Medien. Hier müssen neue Leitlinien geschaffen werden, die den Nutzern die Möglichkeiten und Gefahren des sozialen Netzes aufzeigen und ihnen eine Medienkompetenz oder eine Social Media Kompetenz vermitteln.

So sollte jedes Mitglied der öffentlichen Verwaltung, der ein Web 2.0 Angebot wie Twitter, Skype oder Facebook nutzen will, vor der Nutzung dieser Dienste geschult werden, wie dies heutzutage schon in vielen privaten Firmen geschieht. Diese Schulung sollte sowohl Richtlinien, Vorgaben und

Handlungsempfehlungen an die Mitarbeiter zur Nutzung der sozialen Medien, aber auch die Aufklärung über rechtliche Folgen von bestimmten Verhaltensweisen beinhalten. Solche Maßnahmen können nicht nur helfen Gefahren abzuwenden, sondern auch die Chance bieten, die Vorteile, die diese neuen Dienste bieten, im Sinne der öffentlichen Verwaltung zu steuern und so positiv einzusetzen. So können soziale Netze für einen verstärkten Kontakt zum Bürger und zur Kollaborationsmöglichkeit genutzt werden. Sie können aber auch dazu dienen, das Image von Verwaltungen oder einzelnen Politikern zu stärken.

Als Beispiel für solche Richtlinien können die „Social Media Guidelines“ von SAP angeführt werden, in denen das Unternehmen seinen Mitarbeitern Grundsätze im Umgang mit sozialen Medien vermittelt. Diese hat das Unternehmen auf einer eigens dafür eingerichteten Webseite veröffentlicht. Es wird erwartet, dass ein Mitarbeiter transparent, ehrlich und respektvoll agiert. Außerdem soll er sich mit seinem richtigen Namen identifizieren, was Vertrauen schaffen kann. Zudem sollen die verfassten Beiträge einen Mehrwert bieten, indem sie informativ und interessant sind. Ziel soll immer die Qualität und nicht die Quantität sein. Die Mitarbeiter werden auch darauf hingewiesen, dass sie selbst die Verantwortung für ihr Geschriebenes haben und als SAP Mitarbeiter keine falschen oder nachteiligen Aussagen über ihr Unternehmen treffen sollten. Offenbar hat SAP ein großes Vertrauen in seine Mitarbeiter, da in den Guidelines keine Verbote ausgesprochen werden [Elliott, 2009].

Wenn ein Unternehmen sein Personal als mündige und verantwortungsbewusste Mitarbeiter auffasst, können soziale Medien einen großen Mehrwert für das Unternehmen bringen.

2.4 Entwicklung und aktueller Stand von E-Partizipation und Web 2.0

Die ersten Versuche zur Partizipation über elektrische Medien stammen aus den 1970er Jahren. Hier wurde mittels Teledemokratie über Fernsehen und Telefon erstmals versucht, den Bürger über elektrische Medien zu beteiligen [Krauch, 1972]. Aber erst mit der zunehmenden Verbreitung des Internets ab den 1990er Jahren und den damit verbundenen Möglichkeiten der weltweiten Kommunikation ohne räumliche und zeitliche Beschränkungen wurde die E-Partizipation für die Verwaltungen interessant. Zunächst nur im Rahmen von Forschungsprojekten, später dann auch in kleinen Projekten auf kommunaler Ebene.

Nach einer Befragung des Instituts für Informationsmanagement Bremen GmbH im Auftrag des Bundesministeriums des Innern aus dem Jahr 2008 gaben rund drei Viertel der befragten wahlberechtigten Personen über 18 Jahren an, sich sehr stark (8,2%), stark (26,8%) bzw. etwas (41,6%) für Politik zu interessieren [Albrecht, et al., 2008]. Mehr als 20% der Befragten nutzen Webseiten des Bundes, um sich zu informieren, knapp 14% nutzen Webangebote, um sich Informationen herunterzuladen oder zu bestellen und nochmal genauso viele besuchten Webseiten von Politikern. Die Motivation zur Nutzung von E-Partizipationsangeboten differiert zwischen der kommunalen und der Bundesebene. Personen, die kommunal teilnehmen, sind meistens Betroffene, die etwas für ihre Gemeinde bewirken wollen. Auf Bundesebene beteiligen sich meist Personen, die ein erhöhtes Interesse für das entsprechende Thema haben.

Eine aktuelle Untersuchung der Computer Sciences Corporation (CSC), eines Beratungs- und Dienstleistungsunternehmens im Bereich der Informationstechnologie, vom Juni 2010 betrachtete den Stand von E-Partizipations- und Web 2.0 Anwendungen der 50 größten Städte und der Bundesländer in Deutschland [Schellong & Girrger, 2010]. Die Untersuchung bezog sich auf Daten des Zeitraums April - Mai 2010 und befasste sich mit den Bereichen der Stadtplanung, Finanzplanung, Beschwerden/Vorschlägen und Bürgerdiensten.

Als Ergebnis stellte die Studie fest, dass sich Bürger in 58 % der untersuchten Städte im Bereich der *Stadtplanung* über das Internet mit Meinungen zu Vorlagen und Konzepten beteiligen konnten. Virtuelle Abstimmungen gab es lediglich auf 5 % der untersuchten Webseiten. Ein genauer Einblick in bestimmte Projekte war teilweise nur offline durch einen Amtsbesuch möglich.

Im Bereich der *Finanzplanung* stellten 40 % der Kommunen und 8 % der Länder Informationen über laufende Haushalte zur Verfügung. Bürger hatten bei 60 % der städtischen Angebote die Gelegenheit, ihre Meinung an die zuständigen Stellen zu übermitteln, meist per E-Mail. Bürgerhaushalte der Länder gab es nicht.

Insgesamt 60 % der Städte und 31 % der Bundesländer boten den Bürgern die Möglichkeit an, *Beschwerden und Vorschläge* im Internet vorzutragen. Über die Auswirkungen der Beschwerden und Vorschläge informierten weniger als 10 % der untersuchten Plattformen. 50 % der Bundesländer und 30 % der Städte boten die Option der Petition an. Web 2.0 Anwendungen fanden in diesem Bereich keinen Einsatz.

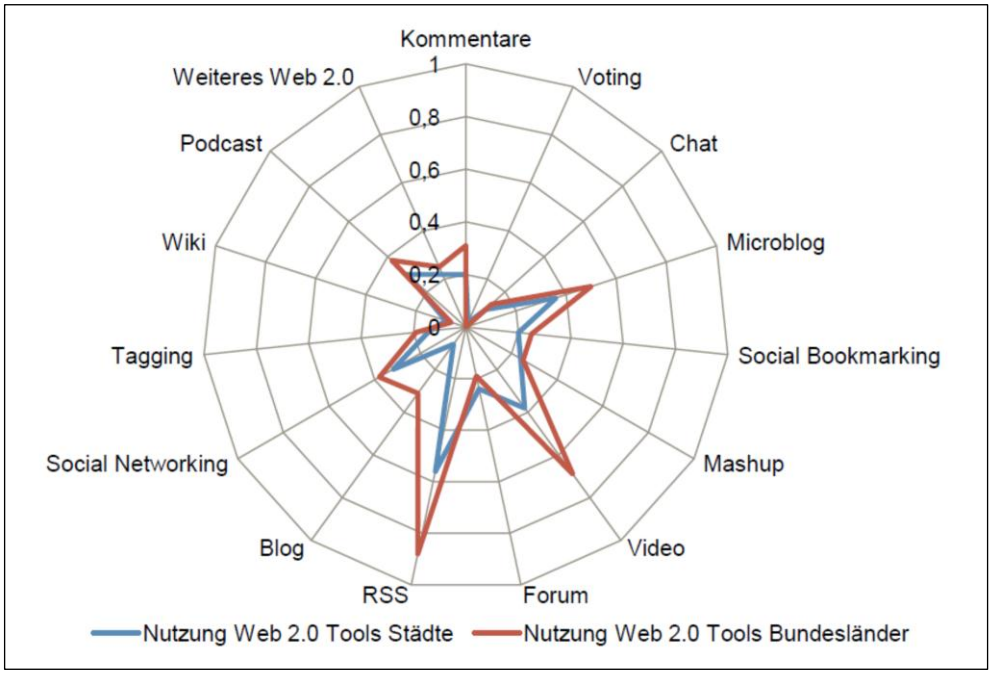

Abbildung 9. Eingesetzte Web 2.0 Anwendungen nach Städten und Bundesländer[16]

[16] Quelle: [Schellong & Girrger, 2010, S. 11]

Im Bereich der *Bürgerdienste* wurde untersucht, in welchem Maße Web 2.0 Anwendungen Verwendung fanden. Dabei wurden die 14 gängigsten Web 2.0 Anwendungen ausgewählt und untersucht, auf welchen Webseiten von Städten und Ländern diese eingesetzt wurden. Abbildung 9 zeigt ein Netzdiagramm mit der prozentualen Verteilung der untersuchten Web 2.0 Anwendungen. Es ist zu erkennen, dass sich RSS als Web 2.0 Anwendung am weitesten durchgesetzt hat. 14 der 16 Bundesländer und 28 der 50 Städte nutzen dieses Feature, gefolgt von Videofunktionen, die in 68 % der Bundesländer und 36 % der Städte anzufinden waren. Danach folgten Microbloggingdienste, die von 36 % der Städte und 50 % der Bundesländer angeboten wurden, leider fehlte aber oftmals der direkte Verweis auf diese Kanäle, sodass sie nur durch eine Webrecherche gefunden werden konnten. Tagging, Voting, Wikis, Blogs und Chats wurden kaum für die Kommunikation zwischen Verwaltung und Bürgern eingesetzt. Die Analyse zeigt somit, dass der Bürger immer noch eher als passiver Informationsempfänger an den Prozessen der öffentlichen Verwaltung beteilig wird. Eine aktive Aufforderung zum Teilnehmen, wie in Bürgerhaushalten, fehlt in weiten Teilen. Zudem werden alle Informationen immer noch nicht zentral zu Verfügung gestellt und bei längerfristigen oder abgeschlossenen Vorhaben mangelt es häufig an aktuellen Informationen. Die Beteiligung erfordert oftmals immer noch den Besuch bei der zuständigen Stelle in der Verwaltung.

Gerade im Bereich der Beschwerden und Vorschläge werden nur vereinzelt kooperative Web 2.0 Tools eingesetzt. Somit wird hier auf eine zweiseitige Kommunikation und damit eine aktive Diskussion verzichtet. Daran merkt man deutlich, dass sich die Verwaltung hier noch in der Anfangsphase befindet. Die Beteiligung beschränkt sich insgesamt vorrangig auf die Informationsbereitstellung der Verwaltung und nicht auf eine Diskussion mit dem Bürger. Virtuelle Abstimmungen sind so gut wie gar nicht vorzufinden, somit kann auch die Stimmung der Bevölkerung nicht aufgefangen werden. In 60% der Städte und 31% der Länder können Bürger ihre Beschwerden einreichen. Über deren Auswirkung und Umsetzung Informieren weniger als 10% der Stellen. Ein fehlendes Feedback führt oft zu Unmut unter den Bürgern und verringert die Bereitschaft, sich einzubringen. Nur wenn der Anwender das Gefühl hat, dass die Nutzung des Angebots das politische Handeln beeinflusst, erhöht sich die Nutzungsabsicht des Bürgers [Schoppé, Parasie, & Veit, 2009].

Ein großes Problem sind die oft unübersichtlich gestalteten Webseiten der Verwaltungen. Zu viele Ebenen sorgen dafür, dass interessierte Bürger die Angebote der Partizipation erst gar nicht finden. Der Wille zur E-Partizipation in Deutschland ist vorhanden, er wird allerdings nicht konsequent und ohne ganzheitliches Konzept umgesetzt, sodass viele Insellösungen, selbst innerhalb einer Verwaltung, erkennbar sind [Kubicek H. e., 2008].

Deutschland spielt bislang, im Vergleich mit anderen Ländern, noch keine große Rolle im Bereich der E-Partizipation. In den westlichen Industriestaaten nehmen laut [Albrecht, et al., 2008] USA, Kanada, Neuseeland, Großbritannien, Dänemark und Estland eine Vorreiterrolle in der E-Partizipation ein.

Ausblickend kann das Grundproblem der großen Distanz und des geringen Vertrauens nicht kurzfristig und nicht nur durch technische Einzelmaßnahmen gelöst werden, sondern nur durch ein langfristiges Programm, das möglichst viele Verwaltungsbereiche umfasst. Ein vereinfachter Zugang durch bereichsübergreifende One-Stop Angebote ist überaus wichtig. Hoch entwickelte Tools sind zwar eine notwendige, aber keinesfalls eine hinreichenden Bedingung für einen erfolgreichen

Partizipationsprozess. Transparenz und Glaubwürdigkeit sind essentiell, um den skeptischen Bürger und unsichere Verwaltungsmitarbeiter auf Kurs zu bringen. Daher müssen alle Dokumente und Beiträge, wo immer es geht, veröffentlicht werden. Dem Teilnehmer sollte ein Feedback mittels Tracking und Tracing gegeben werden, er muss wissen, was mit seinem Beitrag geschieht und was seine Partizipation bewirkt. Zudem ist es wichtig, die Stimmung der Bürger durch Wahlen und Abstimmungen aufzunehmen und dementsprechend das politische Handeln anzupassen. Dies kann auch dazu führen, dass sich weitere Kreise beteiligen, die keine eigenen Beiträge verfassen, sich aber durch die Zustimmung, Ablehnung oder Bewertung von Fragestellungen einbringen möchten. Die Beiträge der Bürger müssen ausgewertet und bewertet werden, um die Stimmung des Volkes korrekt zu erfassen. Wichtig ist, dass der E-Partizipationsprozess als ganzheitliches Programm angesehen wird, das von zentraler Stelle koordiniert, eingeführt und entwickelt wird [Albrecht, et al., 2008].

3. Grundlagen der Sicherheit

Dieses Kapitel befasst sich mit den für die Arbeit relevanten Grundlagen der Sicherheit und des Datenschutzes. Zunächst werden die Gefahren des Internets aufgeführt und einige für E-Partizipationsanwendungen relevante Angriffsszenarien kurz erläutert. Danach beschäftigt sich das Kapitel mit den Sicherheitsanforderungen bezüglich des Datenschutzes. Anschließend wird die sichere Datenübertragung behandelt und sich mit der symmetrischen und asymmetrischen Verschlüsselung, den digitalen Signaturen, der Verschlüsselung der Kommunikationsverbindungen mittels HTTPS sowie mit Sicherheitsaspekten im Umgang mit E-Mails befasst. Der letzte Abschnitt thematisiert den Bürger und sein Sicherheitsbewusstsein und umfasst die Themenbereiche Benutzeraccounts und Passwörter, Sicherheitsaspekte in Netzwerken sowie Sicherheitsaspekte, die beim Surfen im Internet beachtet werden sollten.

3.1 Gefahren im Internet

Wenn der Nutzer sich in dem weltumspannenden World-Wide-Web bewegt, muss dieser sich immer bewusst sein, dass das nicht anonym erfolgt. Im Internet findet immer eine Interaktion zwischen mehreren Parteien statt. Jeder Teilnehmer kann Daten abrufen, stellt aber gleichzeitig seine Ressourcen dem anderen auch zur Verfügung. Ein passives Konsumieren ist nicht möglich, der Nutzer gibt immer einen Teil seiner Daten und Interessen preis. Dieser Tatsache müssen sich Internetnutzer zu jeder Zeit bewusst sein. Da das Internet weltumspannend ist, kommt hinzu, dass eine Abgrenzung der Rechtsräume schwierig ist. Was in anderen Teilen der Welt erlaubt ist, kann in Deutschland verboten sein und umgekehrt [Janowicz, 2007].

Angetrieben von immer neuen Möglichkeiten, die das Internet bietet, werden auch häufig die Anbieter von Web-Anwendungen mit den Risiken konfrontiert, die im Word-Wide-Web lauern. Da immer mehr Geschäftsprozesse vereinfacht, beschleunigt und deren Produktivität gesteigert werden, wird oftmals aus Zeit- oder Kostengründen der Schwerpunkt auf die Funktionalität dieser Systeme und nicht auf die Sicherheit gelegt [Bundesamt für Sicherheit in der Informationstechnik, 2006]. Methoden, die sich in anderen Bereichen der Informationstechnik bewährt haben, werden allzu oft ohne die Sicherheit zu hinterfragen in die Online-Welt übertragen. Das führt letztendlich dazu, dass hier sensible Backend-Daten und Kommunikationsverbindungen ohne zusätzliche Sicherung und ohne kritische Qualitätskontrollen in Bezug auf die Sicherheit online gestellt werden.

Im Zentrum der Sicherheit im Internet stehen die Kernthemen: Vertraulichkeit, Integrität, Verfügbarkeit, Verbindlichkeit und Authentizität der Daten. Vertraulichkeit bezeichnet den Schutz der Daten vor unbefugtem Zugriff und Integrität beschreibt den Schutz vor unbefugter Manipulation. Verfügbarkeit erfordert die Bereitstellung der Informationen zur erforderlichen Zeit und die Verbindlichkeit bezeichnet die Nichtabstreitbarkeit des Senden und Empfangs von Nachrichten. Alles zusammen stellt die Authentizität dar, also die Sicherstellung der Echtheit der Kommunikation in Bezug auf Inhalt und Partner [Wimmer, 2008].

3.2 Angriffsszenarien

Die Seriosität von Internetanbietern ist im Web von zentraler Bedeutung, nicht nur bezüglich des Wahrheitsgehalts der bereitgestellten Informationen, sondern insbesondere auch bei der Frage nach der Sicherheit des eigenen Rechners und persönlicher Daten [Janowicz, 2007]: Welche Gefahren drohen bei dem Besuch einer Webseite, wo kann man seine persönlichen Daten unbedenklich eingeben und wo sollte man es lieber lassen? Grundlage zur Beantwortung dieser Frage stellt die Kenntnis über die verschieden Angriffsformen dar, die im Folgenden erläutert werden. Grundsätzlich sind alle vorgestellten Angriffsszenarien dazu geeignet, E-Partizipationsanwendungen zu bedrohen.

Social Engineering

Social Engineering ist eine sehr gefährliche Angriffsmethode mit dem Ziel, an Account-Daten von Nutzern zu gelangen. Dieser Angriff zielt weniger auf den Computer selbst ab, sondern vielmehr auf dessen Benutzer. Dieser soll dazu gebracht werden Informationen und Passwörter freiwillig herauszugeben, um dem Angreifer damit Zugriff auf den Benutzer-Account des Opfers zu geben. Dabei wird meist die Unwissenheit des Nutzers ausgenutzt, der meist das schwächste Glied der Sicherheitskette darstellt. Er bekommt beispielsweise eine E-Mail von dem Angreifer, der sich als Helpdesk Mitarbeiter ausgibt und ihn auffordert, seine Benutzerdaten aus „Sicherheitsgründen“ in ein vorgegebenes Wortpaar zu ändern oder gleich um die Rücksendung des Benutzernamens und Passworts bittet. Das Opfer übergibt somit die volle Kontrolle des betroffenen Accounts an den Angreifer. Es gibt keine technischen Schutzmaßnahmen gegen solche Attacken, lediglich Schulungen und Sensibilisierung der Internetnutzer können solche Angriffe verhindern [Janowicz, 2007].

Viren und Würmer

Computerviren werden an ausführbare Programme angehängt und aktivieren sich, sobald das Wirtsprogramm gestartet wird. Es kann vom Anwender unkontrollierbare Veränderungen an dem Betriebssystem, der Hard- oder Software durchführen und so im schlimmsten Fall ganze Systeme lahmlegen. Würmer funktionieren ähnlich wie Viren, sind aber eigenständige Programme, die sich oft als ungefährliche Dateien wie Bilder oder Textdokumente tarnen. Sie können den gleichen Schaden wie Viren anrichten sind aber nicht dafür programmiert, einzelne Programme oder Dokumente zu befallen, sondern das gesamte System zu kompromittieren. Sie verbreiten sich nicht von Datei zu Datei, sondern von System zu System. Zudem sind Würmer, im Unterschied zu Viren, nach einer Infizierung nicht auf die Interaktion mit dem Benutzer angewiesen und können sich viel schneller ausbreiten [Janowicz, 2007].

Voraussetzung für den Befall von Systemen mit Viren oder Würmern ist ein unsicheres System, das über offene Sicherheitslücken im Betriebssystem oder den verwendeten Programmen verfügt und auf dem kein aktueller Virenscanner und Firewall installiert sind [Janowicz, 2007]. Im Jahr 2009 wurden die meisten Systeme durch den bloßen Besuch von Internetseiten ("drive-by-infection") und präparierten PDF-Dokumenten angegriffen [Klostermeier, 2010].

Viren und andere Schadprogramme stellen die häufigste Gefahr der Online-Kriminalität dar. Im Jahr 2010 gaben 22 Millionen Internetnutzer ab 14 Jahre an, dass ihr Computer schon einmal infiziert wurde, was einer Quote von 43 % entspricht [Bundeskriminalamt, 2010].

Denial-of-Service-Angriff

Ein Denial-of-Service-Angriff (DoS) zielt auf die Verfügbarkeit eines Servers ab, indem dieser mit einer Flut meist sinnloser Anfragen überzogen wird. Dabei werden die Anzahl an möglichen Verbindungen, die Rechenzeit und die Bandbreite des Zielsystems voll ausgeschöpft, wodurch es oftmals zu einem Absturz des Servers kommt. Eine verschärfte Form der Dos-Attacken stellt der Distributed-Denial-of-Service-Angriff (DDoS) dar, bei dem der Angriff nicht von einem sondern von mehreren Systemen ausgeführt wird und so die Schlagkraft erhöht wird. Die angreifenden Computer sind meist durch einen Trojaner infiziert und werden von dem Angreifer ferngesteuert, wodurch die Besitzer meist gar nicht merken, dass ihr System an einem Angriff beteiligt war [Janowicz, 2007].

Trojanische Pferde

Der Begriff Trojanisches Pferd stammt aus der antiken Mythologie. In einem riesigen Holzpferd, angeblich einem Geschenk, schmuggelten sich Kämpfer in die Stadt Troja ein, verließen es in der Nacht und nahmen die Stadt ein. Da der Angriffsvorgang der Schadprogramme ähnlich funktioniert, wurde der Name für diese übernommen. In einem vermeintlich harmlosen Programm, das der Nutzer beispielsweise aus dem Internet herunterlädt, versteckt sich ein weiteres Programm, der Trojaner. Der Nutzer merkt von diesem zusätzlichen Programm im ersten Moment meist nichts. Ein Angreifer kann nun Informationen über das Verhalten des Users sammeln oder den befallenen Rechner fernsteuern und beispielsweise DDoS Angriffe auf andere Systeme durchführen. Eine weitere typische Form des Trojaners ist der Keylogger (Tastaturspion), der sämtliche Tastatureingaben des Benutzers überwacht und aufzeichnet. Meist werden Keylogger von Angreifern genutzt, um an vertrauliche Daten wie Passwörter oder PINs zu gelangen [Janowicz, 2007].

Sniffing

Unter Sniffing versteht man das Abhören und Mitlesen von Kommunikationsinhalten zwischen zwei Systemen oder Web Services. Dabei fängt der angreifende Computer meist den gesamten Datenverkehr ab und analysiert diesen. So kann ein Angreifer bei unverschlüsselten Verbindungen Passwörter abfangen, Informationen über die Netzwerkstruktur sammeln oder sonstige sensible Daten auslesen [Janowicz, 2007]. Als Beispiel für ein Sniffing Tool kann das leicht zu bedienende und frei verfügbare Programm Wireshark[17] genannt werden.

Spoofing

Spoofing ist im Allgemeinen eine Angriffsmethode, die eine falsche Identität bzw. IP-Adresse vortäuscht. Beim Web-Spoofing fälscht ein Angreifer eine Webseite, indem er diese meist bis ins Detail nachbildet. Ein Besucher ist der Meinung, dass er sich auf der Originalseite befindet. Erkennen

[17] Verfügbar unter http://www.wireshark.org/

lassen sich solche Webseiten meist nur an der Adressleiste, die den Originaladressen allerdings größtenteils ähneln und sich oft nur durch einen Buchstabendreher oder einen Bindestrich unterscheiden. Als Beispiel könnte die XY Bank unter der Adresse `www.xy-bank.de` erreichbar sein. Ein Angreifer könnte sich jetzt z.B. die Adresse `www.xybank.de` oder `www.xy-bank.com` registrieren lassen und auf dieser Seite die Originalseite der XY Bank bis ins Detail nachahmen. Zudem versucht er die Webseite über Suchmaschinen wie Google bekannt zu machen, indem er Stichworte wählt, nach denen die Kunden der XY Bank suchen könnten. Durch die Unwissenheit der Nutzer, die die Web-Adresse der Seite nicht überprüfen und annehmen, sie seien auf der Originalseite, kann der Angreifer mit dieser Methode persönlich Daten, Passwörter oder PINs, die die Nutzer eingeben, ausspähen [Dopatka, 2005] [Microsoft, 2006].

Phishing

Angriffe, bei denen der Angreifer versucht, mit Hilfe von gefälschten E-Mails vertrauliche Zugangs- und Identifikationsdaten zu erlangen, nennt man Phishing. Diese Angriffstechnik zählt aktuell zu den größten Bedrohungen im Internet. Dabei beginnt der Angriff grundsätzlich mit einem Social Engineering Angriff, bei dem der Nutzer eine E-Mail bekommt, die ihm eine glaubwürdige Quelle vorspielt. Darin wird er beispielsweise aufgefordert, seine Nutzerdaten aus bestimmten Gründen auf der Internetseite des Absenders einzugeben. Der Link zu der vermeintlichen Webseite des Absenders ist auch in der E-Mail enthalten, führt den Nutzer aber auf die gespoofte Seite des Täters, die der Originalseite, z.B. einer Bankenwebseite, meist bis ins Detail ähnelt. Fällt ein Kunde darauf herein, gibt er seine Benutzerdaten auf der Webseite des Angreifers ein, der die Daten anschließend missbrauchen kann. Der Nutzer wird auf die Originalseite weitergeleitet und schöpft so meist im ersten Moment keinen Verdacht [Borges, Arbeitsgruppe Identitätsschutz im Internet e.V., 2010].

Laut einer Forsa-Umfrage wurden sieben Prozent der Internetnutzer ab 14 Jahren bereits einmal Zugangsdaten für das Internet gestohlen, was 3,5 Millionen Deutschen entspricht. Dabei haben es Betrüger meist auf Benutzernamen und Codes für Shops und Auktionshäuser sowie Communities, Foren und E-Mail-Konten abgesehen [Bundeskriminalamt, 2010].

Man-in-the-Middle Angriff

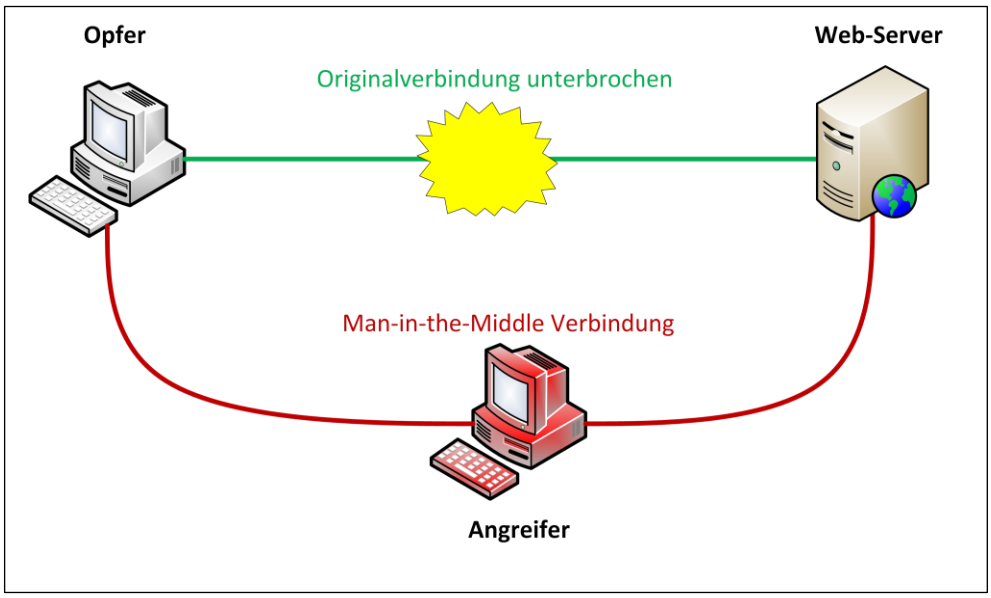

Abbildung 10. Illustration eines Man-in-the-Middle-Angriffs

Bei einem Man-in-the-Middle Angriff steht der Angreifer zwischen zwei Kommunikationspartnern, z.B. einem privaten PC und dem Server einer Bank (siehe Abbildung 10). Er spielt dabei beiden Seiten vor, der jeweils andere zu sein und lässt die gesamte Kommunikation über den eigenen Rechner laufen. So kann der Angreifer („man in the middle“) ausgetauschte Nachrichten abfangen, diese gelesen oder verändert an den Empfänger weiterleiten, ohne dass die Kommunikationspartner dies merken [Fuhrberg, 2000].

Identitätsdiebstahl

Identitätsdiebstahl bezeichnet die missbräuchliche Verwendung von nicht geheimen Identifizierungsdaten wie dem Namen und der Anschrift von natürlichen Personen durch Dritte. Ziel ist in der Regel der Verkauf dieser Daten an interessierte (illegal arbeitende) Kreise oder den rechtmäßigen Inhaber in Misskredit zu bringen. Oftmals wird Identitätsdiebstahl auch genutzt, um sich auf Kosten eines anderen zu bereichern. Der Identitätsdiebstahl ist eine Steigerungsform des Phishings, bei dem nun nicht nur einzelne Zugangsdaten gestohlen werden, sondern die komplette digitale Identität des Nutzers, beispielsweise in sozialen Netzen, E-Mail-Diensten oder Handelsplattformen. Angriffe werde meist über Schadprogramme wie trojanische Pferde durchgeführt, die zudem in der Lage sind, aktive technische Abwehrmaßnahmen zu umgehen [Klostermeier, 2010].

Um auf beispielsweise E-Commerce Webseiten Identitätsdiebstähle durchzuführen benötigen Angreifer meist lediglich Namen und Geburtstag des Opfers, um sich Waren zu bestellen. Die E-Mail und die postalische Adresse werden in solchen Fällen gefälscht. Bestellt wird auf Rechnung unter Angabe der falschen Adresse. Erst wenn von dem E-Commerce Unternehmen ein Inkassounternehmen eingeschaltet wird und herausfindet, dass die angegebene Adresse nicht korrekt ist, werden die

Personen angeschrieben, deren Identität gestohlen wurde. Die Opfer haben dann meist das Problem, dass die Firmen den Rechnungsbetrag von ihnen beglichen haben wollen, was oft in einem langen Rechtsstreit endet [Groll, 2010].

Sieben Prozent der deutschen Internetnutzer (rund 3,5 Millionen Nutzer) gaben im Jahr 2010 an, dass ihnen schon einmal persönliche Zugangsdaten für Online-Dienste und somit ihre Identität gestohlen wurde. Insgesamt fünf Prozent der Nutzer haben darüber hinaus einen finanziellen Schaden durch Datendiebstähle oder Schadprogramme erlitten [Bundeskriminalamt, 2010].

Cross-Site Scripting

Cross-Site Scripting bezeichnet das Ausführen von Code aus einem nicht vertrauenswürdigen Kontext auf einer vertrauenswürdigen Webseite. Das bedeutet, dass auf einer Webseite ein Programmiercode ausgeführt wird, den der Nutzer nicht erkennt und der ihm schaden kann. Diese Angriffe entstehen durch Fehler in der Programmierung von Webanwendungen, wenn diese Eingaben von Nutzer annehmen, ohne diese vor der Verarbeitung zu überprüfen. Die Möglichkeit des Einschleusens von fremden Codes befindet sich meist in Formularfeldern, URL-Parametern oder Cookie-Werten. Der eingeschleuste Code erzeugt hauptsächlich zwei Angriffsszenarien: Das Defacement (Umgestaltung) der Webseite oder der Diebstahl des Authentifizierungs-Cookies.

```
http://www.server.de/datei.php?wahl=<script>document.write('<img
src="http://angreifer.de/cookie.php?'+ document.cookie + '">');</script>
```

Abbildung 11. Beispiel für einen Aufruf zum Entwenden eines Cookies über die URL

Abbildung 11 zeigt ein Beispiel für eine präparierte URL in einem PHP Aufruf, die ein Cookie auslesen kann. Es wird ein neuer IMG-Tag auf der Webseite erzeugt, welcher normalerweise für die Anzeige von Bildern verwendet wird. In diesem Fall wird allerdings ein PHP-Script auf einem fremden Server (`angreifer.de`) aufgerufen und der Code von diesem fremden, nicht vertrauenswürdigem Server ausgeführt. Dabei sendet der Browser die Cookie-Informationen des Nutzers (`document.cookie`) an den Angreifer. Dieses Script kann nun z.B. in einem Beitrag eines unsicheren Web-Forums eingesetzt werden und zeichnet die Cookies aller Nutzer, die den Beitrag abrufen, auf.

Eine zusätzliche Gefahr besteht darin, dass Cross-Site Scripting auch mit einer per SSL verschlüsselten Seite funktioniert. Der Nutzer hat ein hohes Sicherheitsempfinden durch die sichere HTTPS Seite (vgl. Kapitel 3.4.3), kann aber trotzdem Opfer dieses Angriffs werden. Auch Weiterleitungsdienste wie tinyurl.com, die eigentlich dafür gedacht sind URLs zu verkleinern, um sie auf Microblogging Seiten platzsparend zu platzieren, können verwendet werden, um URL-Angriffe zu maskieren. Sie erzeugen aus einer langen URL eine sehr kurze, so wird aus der Adresse `http://www.uni-koblenz-landau.de/koblenz/fb4/institute/iwvi/agvinf` die URL `http://tinyurl.com/35drmcw`, die auf dieselbe Webseite führen. Dadurch ist nicht ersichtlich, auf welche Webseite mit welchen Parametern die kurze URL den Nutzer umleitet [Kachel, 2008].

Session-Hijacking

Ein Nutzer einer Webseite bekommt meist eine eindeutige Session-ID. Diese ID ist die einzige Möglichkeit, im zustandslosen HTTP Protokoll einen Nutzer über eine gesamte Sitzung hinweg wiederzuerkennen. Mit Hilfe der Session-ID können Webanwendungen mehrere zusammengehörige Anfragen eines Benutzers erkennen und einer Sitzung zuordnen. Die Session-ID wird dabei meist in einem Cookie auf dem Rechner des Benutzers gespeichert und bei jedem neuen Aufruf der Webseite neu ausgelesen.

Da die Session-ID nur zwischen Client und Server ausgetauscht wird, werden Angriffstechniken wie Cross-Side-Scripting genutzt, um die Session-ID auszulesen und an den Angreifer weiterzuleiten. Dieser kann das entwendete Cookie auf seinem Browser installieren und wird ab diesem Zeitpunkt von der Webanwendung als der Nutzer erkannt, dessen Cookie verwendet wird. Von da an kann der Angreifer im Namen des Opfers Schaden anrichten oder Daten auslesen.

Brute-Force-Angriff

Ein Angriff mit einem Computerprogramm, bei dem versucht wird, ein Passwort eines anderen Programms oder einer Webseite zu „knacken“, nennt man Brute-Force-Angriff. Dabei versucht das Programm des Angreifers alle möglichen Kombinationen von Buchstaben, Zahlen und Zeichen auszuprobieren, um so das Passwort zu entschlüsseln. Zunächst werden dabei alle einzelnen Zeichen durchprobiert, danach alle Kombinationen von zwei Zeichen, dann drei und so weiter. Eine Weiterentwicklung ist der sogenannte Dictionary Angriff, bei dem Begriffe aus dem Wörterbuch genutzt werden, um ein Passwort zu erraten. Von dieser Angriffsmethode sind sehr kurze Passwörter, die aus wenigen unterschiedlichen Zeichen bestehen, besonders gefährdet [Panko, 2006].

3.3 Datenschutz

> *Die Währung im Internet sind nicht Dollar oder Euro – sondern Ihre Daten!*
> [Roßnagel, 2009]

Dieses Kapitel beschäftigt sich mit dem Datenschutz, also dem Schutz von personenbezogenen Daten im Internet. Der Datenschutz ist ein Teilbereich der Datensicherheit, der außer den personenbezogenen Daten zusätzlich die sonstigen Daten, wie Unternehmensdaten oder Produktdaten, mit einbezieht. Die Datensicherheit ist wiederum ein Teilgebiet der IT-Sicherheit, die das gesamte Spektrum der Sicherheit von IT-Systemen mit den Daten, der Hard- und Software sowie der Kommunikationsnetzen umfasst. Diese drei Sicherheitsaspekte sind zwiebelförmig aufgebaut (siehe Abbildung 12), so umfasst die Datensicherheit auch den Datenschutz und die IT-Sicherheit auch die Datensicherheit [Möhring, 2009].

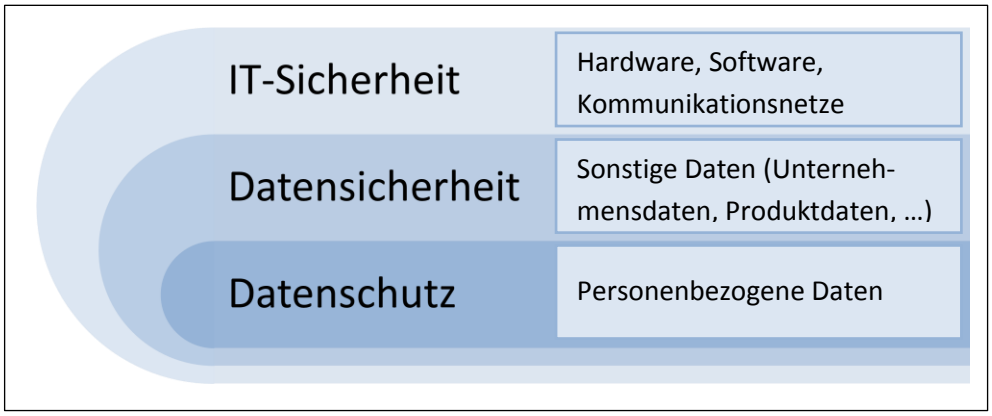

Abbildung 12. Datenschutz, Datensicherheit und IT-Sicherheit[18]

In Deutschland hat jede Person seit dem 15. Dezember 1983 ein Grundrecht auf informationelle Selbstbestimmung. Dieses wurde damals vom Bundesgerichtshof erstmals anerkannt: „Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf ‚informationelle Selbstbestimmung' sind nur im überwiegenden Allgemeininteresse zulässig." Die informelle Selbstbestimmung befähigt den Einzelnen, über die Verwendung seiner Daten in verschiedenen Rollen selbst zu bestimmen. Dementsprechend muss dieser befähigt sein, selbst zu entscheiden, welche Daten er über sich in welchen Rollen und in welcher Kommunikation freigibt [Roßnagel, 2009].

Der Datenschutz bezieht sich auf Regeln und Maßnahmen zum Schutz des Persönlichkeitsrechts von Individuen vor dem Missbrauch ihrer personenbezogenen Daten. Dazu gilt in Deutschland das Bundesdatenschutzgesetz (BDSG) sowie Datenschutzgesetze der einzelnen Länder. Das BDSG befasst sich mit der Datenverarbeitung durch öffentliche Stellen des Bundes sowie nichtöffentlicher Stellen. Die Datenschutzgesetze der Länder regeln im Wesentlichen die Verarbeitung der Daten in den jeweiligen Landesbehörden und Kommunalverwaltungen [Borges, Schwenk, Stuckenberg, & Wegener, 2010, S. 209]. Das Datenschutzrecht regelt umfassend den Umgang mit persönlichen Daten. Dabei bezeichnet das BDSG personenbezogene Daten als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person". Dies umfasst nicht nur die persönlichen Daten wie Name, Adresse oder Geburtsdatum, sondern auch Daten über vertragliche Beziehungen wie Ausweis-, Matrikel- oder Kreditkartennummern. Auch juristische Personen wie eine GmbH können sich auf ein Datenschutzrecht berufen.

Für alle Anwendungen, die im Internet Daten erheben, gilt die Verpflichtung nach §3a BDSG zur Datenvermeidung und Datensparsamkeit. Damit dürfen nur solche personenbezogenen Daten erhoben, verarbeitet und gespeichert werden, die für das jeweilige Verfahren unverzichtbar sind. Zudem sind nach dem BDSG „personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert" [Bundesministerium der Justiz, 2010].

[18] Vgl. [Möhring, 2009]

Ein vertrauensvoller Umgang von personenbezogenen Daten kann die Motivation zur Verwendung von elektronischen Beteiligungsformen, nach einer Studie der Universität Mannheim, signifikant steigern. Daher sollten Webangebote grundsätzlich einen hohen Stellenwert auf Datenschutz und sicherheitsrelevante Fragestellungen legen. Datenschutz sollte sich als Vertrauensfaktor etablieren. Folgende Punkte sollten Anbieter beachten [Schoppé, Parasie, & Veit, 2009] [Möhring, 2009]:

- **Datenschutzerklärung kommunizieren**: Die Daten, die gesammelt werden, sollten für den Nutzer immer transparent sein. Es sollte genau aufgezählt werden, welche Daten für welchen Zweck erhoben werden. Diese sollten übersichtlich und leicht auffindbar in den Datenschutzerklärung der Webseite hinterlegt werden.

- **Opt-in-Verfahren bei Übermittlung persönlicher Daten**: Es gibt grundsätzlich zwei Methoden, eine Einwilligung von dem Nutzer einzuholen: Opt-in und Opt-out. Bei der Opt-out Methode ist die Einwilligung bereits vorgegeben. Nur wer nicht will, dass seine Daten genutzt werden, muss ein Kästchen auf dem Formular ankreuzen oder einen Haken entfernen. Bei der Opt-in Regel muss ein Nutzer ein Kästchen aktiv ankreuzen und damit explizit der Nutzung seiner Daten zustimmen.
  Sobald persönliche Daten wie Name, Adresse, E-Mail-Adresse bei der Anmeldung gesammelt und gespeichert werden, sollte der Besucher um explizite Erlaubnis (Opt-in Verfahren) zur Speicherung dieser Daten gebeten werden. Zudem sollte er vor der Auswertung seiner Daten gefragt werden, inwiefern sie genutzt, weiterverarbeitet oder gar verkauft werden dürfen.

- **Ort der Datenspeicherung beachten**: Wenn Daten nicht intern gespeichert werden, sondern auf dem Server eines externen Anbieters, sollte man sich über den Standort des Datencenters im Klaren sein. Werden die Daten durch einen Drittanbieter innerhalb eines EU-Landes gespeichert, kann man davon ausgehen, dass der Anbieter durch die EU-weite Harmonisierung der Datenschutzregeln ein ähnlich hohes Schutzniveau wie in Deutschland aufweist. Im nichteuropäischen Ausland sollte man auf die Datenschutzregeln des jeweiligen Landes achten, so hat beispielweise die USA ein niedrigeres Schutzniveau als die EU.

- **Anonym per Voreinstellung**: Dem Nutzer sollte automatisch eine anonyme oder pseudonyme Nutzung von Webdiensten gestattet sein. Gerade unerfahrene Nutzer tun sich beispielsweise in sozialen Netzen oft schwer, die richtigen Einstellungen zu finden, um ihre persönlichen Daten im Profil zu deaktivieren. Der Nutzer sollte daher explizit seine persönliche Daten freischalten müssen, bevor diese öffentlich anzeigt werden.

- **Einsatz von Privacy Enhancing Technology**: Datenschutzfördernde Techniken (Privacy Enhancing Technology, PET) sollten so umfangreich wie möglich eingesetzt werden. Dazu gehören Grundsätze wie die Reduktion von personenbezogenen Daten, System- und Selbstdatenschutz, Transparenz, Pseudonymisierung, Anonymisierung und andere vertrauensbildende Maßnahmen.

- **Datensparsamkeit und -vermeidung**: Es sollten keine oder nur so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt werden. Betreiber von Webangeboten

sollten zudem wann immer möglich von einer Anonymisierung und Pseudonymisierung Gebrauch machen.

3.4 Sichere Datenübertragung

Dieses Kapitel beschäftigt sich mit Maßnahmen, die die Vertraulichkeit der elektronischen Kommunikation wahren, also dem Schutz vor unbefugter Preisgabe von Kommunikationsinhalten. Dies wird im Internet durch die Verschlüsselung der Kommunikation erreicht.

3.4.1 Symmetrische und asymmetrische Verschlüsselung

Eine Verschlüsselung besteht immer aus einem Verfahren, einem Schlüssel und einer Nachricht. Über das Verschlüsselungsverfahren wird mit dem Schlüssel die Originalnachricht in eine verschlüsselte Nachricht umgewandelt. Zur stark vereinfachten Darstellung könnte man sich als Verfahren das Erhöhen von jeder Zahl um einen festen Wert vorstellen und als Schlüssel den Wert der Erhöhung. Die Klartext-Nachricht wird dann um den Schlüsselwert erhöht. Die Entschlüsselung funktioniert mit demselben Verfahren, aber mit einem anderen Schlüssel [Leibniz-Rechenzentrum, 2005]. In der folgenden Abbildung 13 wird die vereinfachte Darstellung einer Verschlüsselung kurz dargestellt.

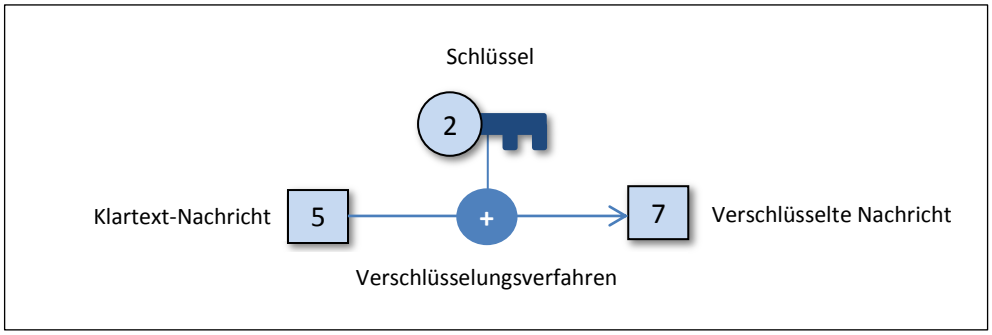

Abbildung 13. Stark vereinfachte Darstellung einer Verschlüsselung

Die **symmetrische Verschlüsselung** nutzt nur einen Schlüssel auf beiden Seiten der Kommunikation, um Daten zu ver- und entschlüsseln. Dieses Verfahren ist schnell und effizient. Da mit jedem Kommunikationspartner ein separater Schlüssel vereinbart werden muss, ist das Verfahren für die alltägliche Verschlüsselung der Kommunikation im Internet sehr unpraktisch. Jeder, der den Schlüssel kennt, kann die Kommunikationsinhalte mitlesen und verändern. Hierin liegt die Schwäche der Verschlüsselung, da der Schlüsselaustausch vertraulich geschehen muss und nicht von einem Angreifer belauscht werden darf. Populäre symmetrische Verschlüsselungsverfahren sind DES (Data Encryption Standard) und AES (Advanced Encryption Standard).

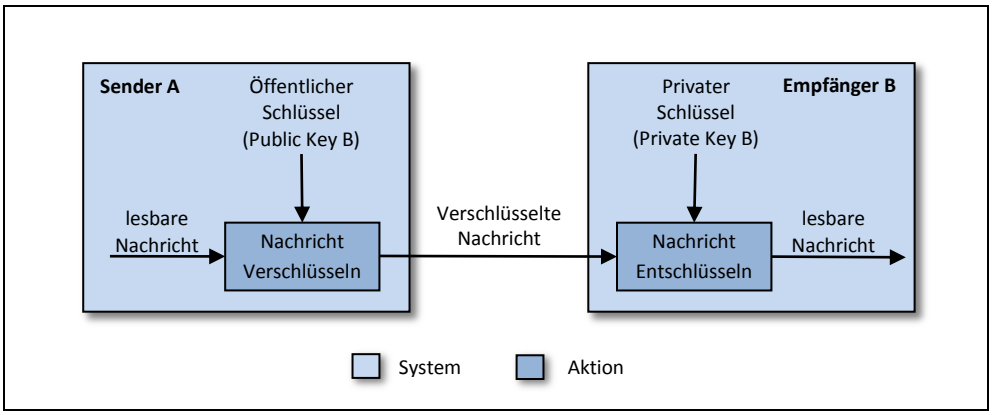

Abbildung 14. Asymmetrische Verschlüsselung[19]

Die **asymmetrische Verschlüsselung**, oder Public Key Infrastructure (PKI), nutzt zum Ver- und Entschlüsseln getrennte Schlüsselcodes. Hier reicht die Kenntnis der Verschlüsselung nicht zur Entschlüsselung aus und umgekehrt. Beide beteiligte Stellen verfügen über jeweils zwei Schlüssel, dem so genannten Schlüsselpaar. Zum Verschlüsseln einer Nachricht wird ein öffentlicher Schlüssel (oder auch Public Key) benötigt. Dieser kann und soll jedem bekannt sein und darf über beliebige unsichere Kanäle verteilt werden, da mit ihm nur verschlüsselt und keine Kommunikationsinhalte lesbar gemacht werden können. Zum Entschlüsseln einer Nachricht wird der private Schlüssel (oder Private Key) des Eigentümers genutzt, der immer geheim gehalten werden muss und nicht in fremde Hände fallen darf. Nur mit dem privaten Schlüssel können Nachrichten, die mit dem passenden öffentlichen Schlüssel kodiert wurden, entschlüsselt werden. Der Ablauf einer asymmetrischen Verschlüsselung wird in Abbildung 14 schematisch erklärt. Das bekannteste Public-Key Verfahren ist RSA (benannt nach den Entwicklern Rivest, Shamir und Adleman) [Panko, 2006].

3.4.2 Digitale Signatur

Mit Hilfe der PKI kann zu einer Nachricht eine digitale Signatur erstellt werden, wodurch die Urheberschaft und Zugehörigkeit der Nachricht überprüfbar gemacht wird. Die digitale Signatur wird aus dem Klartext der Nachricht mit Hilfe einer eindeutigen Rechenvorschrift berechnet. Dabei führen verschiedene Daten, selbst das Hinzufügen von einem einzelnen Leerzeichen, zu unterschiedlichen Signaturen.

Die asymmetrische Verschlüsselung wird nicht direkt auf die Nachricht angewendet, sondern auf deren Hash-Wert. Der Hash-Wert wird mit einer schnell zu berechnenden, kollisionsresistenten Einwegfunktion erstellt. Kollisionsresistent bedeutet, dass es möglichst keine zwei Datenstrukturen gibt, die denselben Hashwert erzeugen und zwei unterschiedliche (ähnliche) Eingaben immer zu unterschiedlichen Ergebnissen führen. Einwegfunktion beschreibt, dass die Berechnung des Hash-Wertes einfach ist, die Rückberechnung des Originalwertes dagegen nur sehr schwer möglich ist. Dabei wird üblicherweise der Speicherbedarf des Hash-Wertes wesentlich kleiner als der der Originalnachricht.

[19] Quelle: [Möhring, 2009]

Mit dem privaten Schlüssel des Absenders wird in der Regel aus dem Hash-Wert der Nachricht die digitale Signatur erstellt und ihr angehängt. Der Empfänger muss nach dem Eingang der E-Mail ebenfalls den Hash-Wert der Nachricht erstellen, die digitale Signatur mit Hilfe des öffentlichen Schlüssels des Absenders entschlüsseln und beide Werte vergleichen. Sind diese gleich, so weiß er, dass die Nachricht mit dem privaten Schlüssel des Absenders signiert und auf dem Transportweg nicht verändert wurde [Möhring, 2009].

3.4.3 Verschlüsselung mittels HTTPS

Der Standard für eine sichere Kommunikation über das Internet ist derzeit das Hypertext Transfer Protocol SSL (HTTPS). Dieses nutzt das klassische HTTP Protokoll, das über einen sicheren Kanal kommuniziert. Hierbei verschlüsselt, signiert und authentisiert das Verfahren „Secure Sockets Layer“ (SSL) oder der Nachfolger „Transport Layer Security“ (TLS) die gesamte Kommunikation. Es setzt dabei ein hybrides Verschlüsselungsverfahren ein, das aus symmetrischer und asymmetrischer Verschlüsselung besteht, um die Verbindung zwischen zwei Kommunikationspartnern abzusichern. Dieser Schutz führt bei heutigen Browsern soweit, dass auch bei einem Wechsel von einer per SSL geschützten Seite (HTTPS) zu einer ungeschützten Seite (HTTP) keine sensiblen Protokollinformationen weitergegeben werden.

Soll eine sichere Verbindung zwischen Server und Client aufgebaut werden, beginnt die Kommunikation mit einem sogenannten Handshake [Leibniz-Rechenzentrum, 2005]. Der Vorgang wird im Folgenden kurz erläutert:

1. Server und Client einigen sich über das zu benutzende Verschlüsselungsverfahren.
2. Der Client empfängt den öffentlichen, asymmetrischen Schlüssel (Zertifikat) des Servers und validiert ihn.
3. Der Client generiert einen symmetrischen „Hauptschlüssel“ und übermittelt ihn an den Server, und zwar verschlüsselt mit dessen öffentlichem Schlüssel.
4. Anschließend wird dieser Schlüssel für die folgende symmetrisch verschlüsselte Kommunikation verwendet. Selbst wenn die Kommunikation abgehört wurde, kennt kein Dritter den verwendeten symmetrischen Schlüssel und die gesendeten Daten sind abhörsicher und vertrauenswürdig.

Neben der sicheren Verbindung ist zusätzlich eine Verifikation der Zusammengehörigkeit von öffentlichem Schlüssel und seinem Besitzer notwendig, da nur so die Echtheit der Kommunikationspartner gewährleistet ist. Diese müssen sich authentisieren, weil ein falscher oder unbekannter Schlüssel wie eine falsche Unterschrift wirkt. Hierfür existieren Zertifikate, die von einer als seriös geltenden Zertifizierungsstelle (Certificate Authority (CA)) ausgestellt werden und eine eindeutige Zuordnung von einem öffentlichen Schlüssel zu einer bestimmten Identität gewährleisten. Eine CA bescheinigt einem Computer seine Identität und erkennt ungültige oder gefälschte Zertifikate. Bevor die verschlüsselte Kommunikation beginnt, schickt der Server dem Client sein Zertifikat zu, mit dem

er dessen Echtheit überprüfen kann [Janowicz, 2007, S. 153]. Durch diese Überprüfung der Zertifikate von Client und Server schützt HTTPS vor *Man-in-the-middle-Attacken*, da der zwischengeschaltete Angreifer nicht über die notwendigen gültigen Zertifikate verfügt.

Nachdem ein Handshake abgeschlossen ist und eine gesicherte Verbindung besteht, wird die Kommunikation in diesem sicheren Kanal über das normale HTTP Protokoll durchgeführt. Ein Angreifer, der die Kommunikation abhört, liest aufgrund der Verschlüsselung nur unleserliche Datenfragmente, daher schützt HTTPS zusätzlich vor *Sniffing* [Knall, 2007].

Allerdings ist durch HTTPS nicht die Echtheit einer angezeigten Webseite garantiert. SSL bietet nur einen Schutz während der Datenübertragung von Sender zu Empfänger und gewährleistet die Korrektheit der Kommunikationspartner. Ist eine Webseite aber selbst mittels Cross-Site Scripting verändert oder durch Web-Spoofing überdeckt, so ist dies nicht mit einer Verletzung des Zertifikats verbunden [Bundesamt für Sicherheit in der Informationstechnik, 2006].

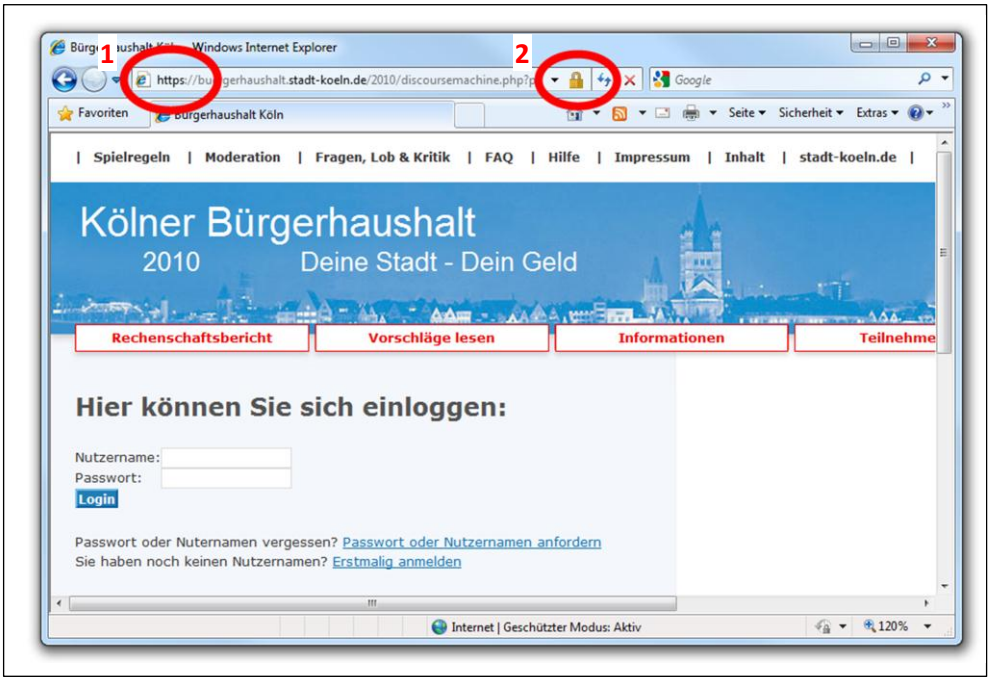

Abbildung 15. Kontrollmöglichkeiten für eine sichere Datenübertragung durch HTTPS

Abbildung 15 zeigt am Beispiel des Internet Explorers 8 die Merkmale, mit denen ein Nutzer erkennen kann, dass die Verbindung verschlüsselt stattfindet. Zum einen steht am Anfang der Adressleiste immer das Kürzel „https://“ (1), zum anderen wird zusätzlich ein Vorhängeschloss angezeigt (2). Ist das Schloss geschlossen, werden die eingegebenen Daten auf dem Weg von Browser zur Webseite verschlüsselt.

Neuere Versionen der SSL- und TLS-Verschlüsselung gelten als sicher. Probleme liegen hier nicht in der Technik, sondern bei dem Benutzer. Ein durchschnittlicher Benutzer hat oftmals keine Erfahrung im Umgang mit Zertifikaten und Verschlüsselungen. Meist klickt er, wenn sich ein Fenster mit einem Zertifikat öffnet, einfach auf „weiter“ ohne die Webseite zu überprüfen, um mit seiner Arbeit

fortzufahren. Da Zertifikate eng mit dem Domainnamen verknüpft sind, ist ein Blick auf die Domain aber äußerst wichtig. So kann die URL

`www.meine-bank.de`

auf die Webpräsenz der Bank führen, während

`www.meinebank.de`

eine gefälschte Seite öffnen kann, die vorgibt die Bankseite zu sein, um an die sensiblen Daten des Nutzers zu gelangen. Besitzt ein Angreifer ein gültiges SSL-Zertifikat für seine Domain, gibt es nicht einmal eine Warnung vom Browser [Knall, 2007].

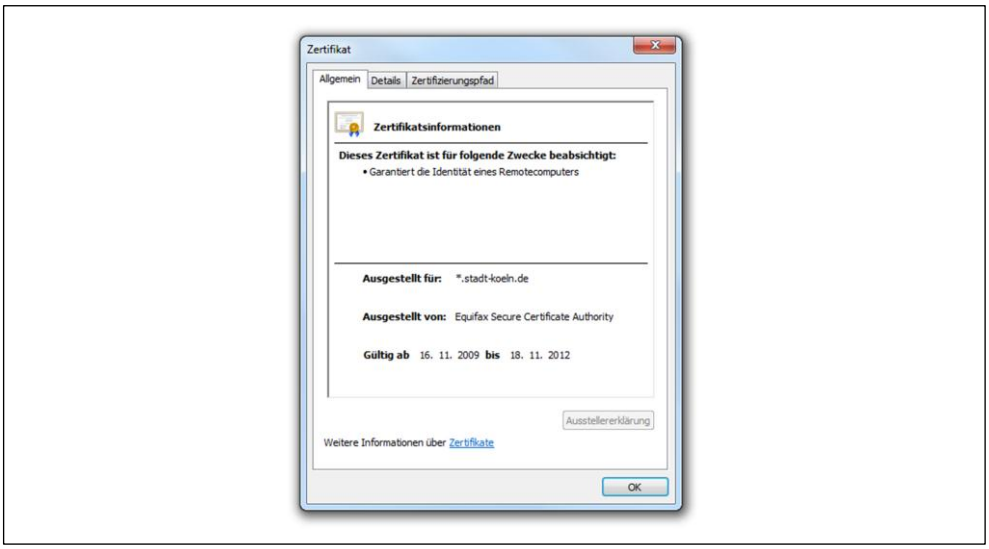

Abbildung 16. Zertifikat von stadt-koeln.de

Durch einen Doppelklick auf das Vorhängeschloss (2) aus Abbildung 15 kann man sich das Sicherheitszertifikat der Seite anzeigen lassen. Dieses Zertifikat entspricht dem Identitätsnachweis der Webseite. Abbildung 16 zeigt das Zertifikat der Stadt Köln. Nur wenn der unter „Ausgestellt für“ angegebene Domänennamen (`stadt-koeln.de`) exakt dem Domänennamen der Webseite entspricht, den man auch wirklich aufrufen wollte (auch `stadt-koeln.de`), kann sich ein Nutzer sicher sein, dass er auf der richtigen Webseite ist und seine Daten sicher im Internet übertragen werden [Microsoft, 2006].

Datenverschlüsselung ist besonders im Zusammenhang mit dem Schutz personenbezogener Daten wichtig. Auch wenn eine Anwendung selbst als nicht schutzbedürftig durch SSL eingestuft wird, so sollten doch Registrierung, Login, Zugriff auf persönliche Daten, Passwort-Änderung und die „Passwort vergessen“-Funktion verschlüsselt ablaufen [Bundesamt für Sicherheit in der Informationstechnik, 2006]. Aber auch weniger wichtige Seiten können komplett mittels SSL verschlüsselt werden, um einen optimalen Schutz der Identität vor Datensammlern im Netz zu gewährleisten. Die Länge der asymmetrischen Schlüssel sollte mindesten 1024 Bit, die der symmetri-

schen mindesten 128 Bit betragen, da die Sicherheit des Verfahrens auf der Schlüssellänge beruht. Schlüssel mit einer geringeren Länge gelten als unsicher [Janowicz, 2007].

3.4.4 Sicherheit von E-Mails

> *Jede unverschlüsselte E-Mail ist wie eine Postkarte. Jeder der sie zu sehen bekommt, kann sie sofort lesen.*
> [Spooren & Pohlmann, 2010]

Da eine E-Mail in der Regel unverschlüsselt gesendet wird, ist es ein leichtes für Angreifer, eine E-Mail mitzulesen. Aus diesem Grund ist die E-Mail zu unsicher für den Versand von rechtsverbindlichen Dokumenten wie etwa Verträgen oder personenbezogenen Daten. Solche sensible Informationen sollten stets verschlüsselt ausgetauscht werden. Jede E-Mail wandert über mehrere Stationen vom Absender zum Empfänger. Diese Stationen sind allesamt Gefahrenquellen des unbefugten Lesens. Damit schützenswerte Informationen nicht in falsche Hände gelangen, sollten E-Mails nicht wie eine offene Postkarte, sondern in einem Umschlag verschickt werden. Dieser Umschlag kann durch eine asymmetrische Verschlüsselung (oder Public Key Infrastructure, vgl. Kapitel 3.4.1) erzeugt werden. Ein Absender verschlüsselt die E-Mail mit dem öffentlichen Schlüssel des Empfängers, wodurch nur noch der Empfänger die elektronische Nachricht mit seinem privaten Schlüssel entschlüsseln kann [Spooren & Pohlmann, 2010].

Auch der Absender einer E-Mail ist beliebig manipulierbar. Dies ist in der unsicheren Konzeption des SMTP-Protokolls begründet, über das E-Mails verschickt werden. SMTP-Server verfügen über keinerlei Sicherheits- oder Authentifizierungsmechanismen. Ein Angreifer kann einen frei wählbaren Namen und eine beliebige E-Mail Adresse angeben, die in der E-Mail als Absender angezeigt wird. Daher ist die Authentizität des Absenders nicht gewährleistet [Janowicz, 2007]. Mit Hilfe der PKI kann eine E-Mail neben der Verschlüsselung auch digital signiert werden (vgl. Kapitel 3.4.2). Somit kann der Empfänger überprüfen, ob die Nachricht auf dem Transportweg verändert wurde und ob die Nachricht auch wirklich von dem angegebenen Absender stammt. Hierfür bieten sich Programme wie GNU Privacy Guard (GnuPG) oder Pretty Good Privacy (PGP) an. Diese Programme bieten die Möglichkeit, E-Mail Inhalte zu ver- und entschlüsseln und darüber hinaus elektronische Signaturen zu erzeugen und zu prüfen.

Um seinen Benutzernamen und sein Passwort sowie die E-Mail Inhalte in unsicheren Netzwerken zu schützen, sollte ein Nutzer die TLS/SSL Verschlüsselung, die auch bei HTTPS (vgl. Kapitel 3.4.2) verwendet wird, nutzen. Mittels der Verschlüsselung kann ein Nutzer seine E-Mails sicher senden und von einem Webserver abrufen. Dazu wird eine verschlüsselte Verbindung zum Server aufgebaut mit einer gegenseitigen Zertifizierung der Teilnehmer. Dies sichert den Weg der Nachricht vom Sender zu seinem E-Mail Server, ist aber kein Garant für eine sichere End-zu-End Übertragung, da der Weg der Gegenseite, also vom E-Mail Server zum Empfänger, trotzdem unverschlüsselt stattfinden kann und somit als unsicher einzustufen ist. Trotzdem ist die SSL Verschlüsselung für eine sichere E-Mail Kommunikation Pflicht, da nur so Nachrichten und Zugangsdaten ohne Gefahr des Abhörens übertragen werden können.

Über die weitere, zukünftige Entwicklung von dem sicheren und rechtsverbindlichen Versand von elektronischen Dokumenten Informiert Kapitel 6.2.2.

3.5 Sicherheitsbewusstsein der Bürger

Zu dem Thema Sicherheit in der Onlinewelt gehört neben den Sicherheitsaspekten, die Betreiber von Onlineangeboten auf ihren Webseiten umsetzen können, auch ein hohes Sicherheitsbewusstsein der Bürger. Die besten Sicherheitsmaßnahmen sind nutzlos, wenn der Nutzer nicht weiß, worauf man im World-Wide-Web achten muss und er nicht sensibel mit seinen persönlichen Daten umgeht. Daher beschäftigt sich dieses Kapitel zunächst mit Benutzer-Accounts von Online-Nutzern und den dazugehörigen Passwörtern, mit der Sicherheit in Netzwerken sowie mit Verhaltensweisen, die das Surfen im Netz sicherer machen können.

3.5.1 Benutzer-Accounts und Passwörter

Die einfachste Art der wissensbasierten Identifikation ist die Identifikation über ein unveränderliches Geheimnis. Dieses kann ein Passwort, eine Passphrase oder eine Persönliche Identifikationsnummer (PIN) sein. Passwörter sind der zentrale Sicherheitsmechanismus im Internet. Fast alle Seiten, bei denen sich ein Nutzer anmelden kann, nutzen zur Identifikation und Authentifikation einen Benutzernamen und ein Passwort, den sogenannten Benutzer-Account. In diesem Benutzer-Account werden zusätzlich beispielweise auf Online-Shopping-Seiten Profildaten des Kunden und seine Historie gespeichert. Gelingt es einem Fremden, an den Benutzernamen und das dazugehörige Passwort zu gelangen, kann er sich auf Rechnung des Betroffenen Waren bestellen, seine persönlichen Daten ausspähen oder sonstigen Unfug damit anstellen. Die größten Gefahren für Passwörter sind Keylogger, Sniffing, Web Spoofing und Phishing.

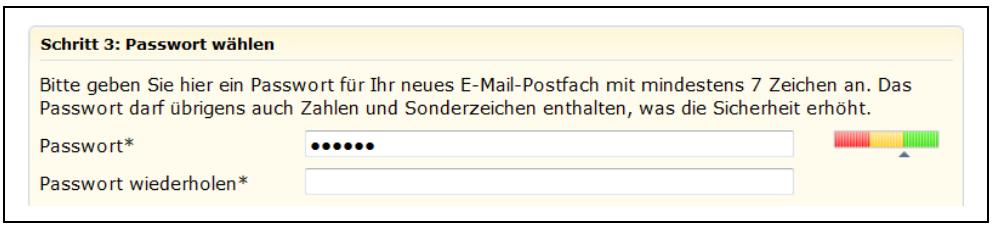

Abbildung 17. Überprüfung der Passwortstärke bei Web.de

Ein Problem bei Benutzer-Accounts stellen schwache Passwörter dar, die von Nutzern gewählt werden. Oft werden Begriffe die im Wörterbuch stehen, Namen von Familienangehörigen, Tieren oder Sportmannschaften genutzt. Solche Passwörter können schon fast durch einfaches Ausprobieren der Angreifer geknackt werden. Benutzer sollten daher immer aufgefordert werden sichere Passwörter zu verwenden. Hierzu könnte auf einer Webseite eine Anzeige neben der Passwortbox dienen, die den Benutzer über die Passwortstärke informiert, wie es beispielsweise bei Web.de vorzufinden ist (siehe Abbildung 17). Zudem sollten Nutzer immer bestärkt werden, ein langes Passwort von ungefähr 8-12 Zeichen einzugeben, große und kleine Buchstaben sowie Sonderzeichen

wie beispielsweise „!“, „§“ oder „$“ zu verwenden. Außerdem sollte das Passwort keinem Wort aus dem Wörterbuch entsprechen und keinen persönlichen Bezug zu dem Nutzer (wie z.B. ein Geburtsdatum) aufweisen. Einem Nutzer sollte zudem der Hinweis gegeben werden, das gleiche Passwort nicht auch an anderer Stelle zu verwenden [Janowicz, 2007].

Die Zeichenlänge begründet sich in der Dauer, die ein Brute-Force-Angriff (vgl. Kapitel 3.2) benötigt, um ein Passwort zu knacken. Würde ein Passwort ausschließlich aus Kleinbuchstaben bestehen, so kann es bei einer Stelle aus 26 verschiedenen Zeichen bestehen. Bei einer Länge von sechs Zeichen lässt dieses Passwort knapp 309 Millionen Kombinationen (26^6) zu. Ein übertakteter Core 2 Quad Q6600 Prozessor schafft rund 45 Millionen Tastenanschläge pro Sekunde. Also schafft es dieser Prozessor theoretisch, alle 309 Mio. möglichen Kombinationen innerhalb von 6,8 Sekunden auszuprobieren (309 Mio. Kombinationen / 45 Mio. Kombinationen/s). Das bedeutet, dass dieses Passwort innerhalb von knapp sieben Sekunden geknackt wäre. Besteht das sechs Zeichen umfassende Passwort aus Klein- und Großbuchstaben sowie aus Zahlen, erhöht sich die Zahl der Kombinationen auf knapp 56,8 Milliarden (62^6). Dies entspräche schon einer Dauer von rund 21 Minuten. Für ein Passwort mit acht Zeichen würde dieser Prozessor rund zwei Monate benötigen. Daher kann diese Zeichenlänge mit den derzeitigen technischen Möglichkeiten als recht sicher bezeichnet werden. Das bedeutet, dass die Passwortlänge die Sicherheit des Passwortes direkt bestimmt: Je länger das Passwort, desto geringer die Chance, ein Passwort zu entschlüsseln [PC Welt, 2010].

Ein häufiges Problem, welches Nutzer mit der Passwortwahl haben, ist die Vereinbarkeit eines möglichst sicheren Passwortes mit der Einprägbarkeit der Zeichenfolge. Daher wählen viele Nutzer den Namen von Familienangehörigen oder Geburtstage als Passwort. Diese sind, wenn man die Brute-Force Dauer betrachtet, sehr unsicher. Eine gute Methode ist es daher, sich aus den Anfangsbuchstaben eines leicht zu merkenden Satzes eine Eselsbrücke zu bauen. Beispielsweise kann mit den ersten Buchstaben aus dem Satz „Für ein sicheres Passwort benötige ich 10 Zeichen!“ das sehr sichere Passwort „FesPbi10Z!“ gebildet werden. Es enthält kleine und große Buchstaben, Zahlen, Sonderzeichen und besteht aus einer akzeptablen Länge [Janowicz, 2007] [Freenet, 2010].

Um die Passwortsicherheit zu erhöhen, können verschiedene organisatorische Maßnahmen erfolgversprechend sein. So können feste Regeln der Passworteingabe helfen, den Sicherheitsgrad des gewählten Passworts zu erhöhen. Eine feste Passwortlänge und die Mindestzahl von enthaltenen Sonderzeichen können schon ausreichend sein, um sichere Passwörter zu erzwingen, ohne den Nutzer zu stark einzuschränken [Bundesamt für Sicherheit in der Informationstechnik, 2006]. Zudem sollten Nutzer bereits während der Registrierung informiert werden, ihr Passwort niemals an andere Personen herauszugeben. Beispielsweise sollten unter keinen Umständen Passwörter von Kunden per Telefon oder E-Mail abgefragt werden.

Gerade für sensible Webangebote wie z.B. Online-Banking sollten Internetnutzer möglichst starke Passwörter benutzen. Zusammenfassend sollten diese sinnfrei zusammengesetzt werden und keine Namen oder Geburtsdaten enthalten. Grundsätzlich sollten starke Passwörter aus mindestens acht, besser aus 12 Zeichen und Ziffern bestehen, Sonderzeichen sowie Groß- und Kleinschreibung beinhalten und nicht aus Wörtern des Wörterbuchs bestehen. Zudem sollte für jedes Benutzerkonto ein anderes Passwort verwendet werden. Es tauchen immer wieder Datenskandale auf, bei denen

Tausende von Benutzerdaten gestohlen werden. Wenn man nur ein Passwort für mehrere Dienste verwendet, könnte ein Angreifer, der ein Passwort kennt, gleich auf mehrere Konten damit zugreifen [Spooren & Pohlmann, 2010].

3.5.2 Sicherheit in Netzwerken

Es können sich mittlerweile viele Computer, insbesondere Laptops, aber auch immer mehr Mobiltelefone wie Smartphones, über Funk in das Internet einwählen. Daher sollten Nutzer sich der Gefahren, die die WLAN-Technologie – neben dem Komfort – birgt, bewusst sein. So kann man in einem öffentlichen WLAN immer abgehört werden und andere Nutzer können auf die freigegebenen Ordner des Dateisystems zugreifen.

Ein Betreiber eines drahtlosen Netzwerkes muss dieses immer vor unbefugtem Zugriff schützen. Hier bieten sich die Verschlüsselung WPA (Wi-Fi Protected Access) oder der Nachfolger WPA2 an, die einen hohen Sicherheitsstandard gewährleisten. Die WEP (Wired Equivalent Privacy) Verschlüsselung, ein Vorläufer von WPA, sollte auf keinen Fall verwendet werden, da sie mittlerweile als unsicher gilt und innerhalb weniger Minuten geknackt werden kann. Auch der WLAN Schlüssel sollte sicher gewählt werden und sicher verwahrt bleiben, da mit diesem Schlüssel ein Zugang zu dem Netzwerk möglich ist. Wenn ein Angreifer in einem fremden Netz surft und sich strafbare Seiten ansieht oder sich illegal Software, Filme oder Musik herunterlädt, ist meist der Betreiber des drahtlosen Netzes in der Haftung für diese Rechtsverletzungen. Eine Nachverfolgung, wer das Netz zu welchem Zeitpunkt genutzt hat, ist im privaten Bereich so gut wie unmöglich. Hierzu gibt es bereits viele Urteilssprüche, die die Betreiber für Urheberrechtsverletzungen verantwortlich machen.

Der Anteil der Deutschen, die zur Nutzung des Internets mobile Endgeräte wie Laptops oder Smartphones verwenden, erhöht sich stetig [Bundesministerium für Wirtschaft und Technologie, 2009]. Dies führt dazu, dass sich eine zunehmende Zahl der Bürger an öffentlichen drahtlosen Netzwerken, wie an Flughäfen oder in Biergärten, in das World-Wide-Web einloggen. Dabei sollten einige Vorsichtsmaßnahmen beachtet werden, da sich andernfalls Angreifer leicht in den Funkverkehr einklinken können. Der Nutzer sollte unbedingt darauf achten, keine Passwörter auf Webseiten einzugeben, die nicht mittels HTTPS gesichert sind. Wenn man seine Login-Daten in ungesicherten, öffentlichen Netzwerken ohne eine Verschlüsselung versendet, können diese Daten leicht von einem Angreifer mittels Sniffing (vgl. Kapitel 3.1) aufgezeichnet und verwendet werden. In heimischen und mittels WPA gesicherten Netzen ist diese Gefahr geringer, da ein Angreifer erst die Verschlüsselung knacken muss, um den Internetverkehr des WLAN auslesen zu können.

Eine weitere wirksame Methode der Datenverschlüsselung während der Übertragung ist, neben dem HTTPS, die Verwendung eines VPN (Virtual Private Network). Bei solchen Netzwerken wird ein virtueller Tunnel zwischen dem Client-Computer (z.B. Laptop) und einem Netzwerk oder Server aufgebaut. Der Nutzer muss sich klassisch mit einem Benutzernamen und Passwort in dem Zielsystem einloggen. Der Datenverkehr zwischen den beiden Stellen erfolgt fortan in verschlüsselter Form, wodurch mögliche Angreifer die Datenpakete nicht mehr lesen können. Das Netzwerk oder der Server, mit dem man sich verbindet, muss dabei vertrauenswürdig sein, da die Anfragen des Client-

Systems unverschlüsselt an das Internet übermittelt werden. Die gewünschten Inhalte werden anschließend verschlüsselt an den Nutzer zurück gesendet [Universität Koblenz, 2010].

3.5.3 Bewusstes Surfen

Wenn man im Internet aktiv ist, sollte man immer für einen gewissen Basisschutz seines Computersystems sorgen, denn ein nicht gepatchtes System stellt ein erhebliches Sicherheitsrisiko dar und ist enorm anfällig für Schadprogramme wie Trojaner. Klickt man ein Programm, eine PDF oder eine Bilddatei, die infiziert ist, in einer E-Mail an, kann sich das Schadprogramm auf unsicheren Systemen unbemerkt installieren. Daher sollte man immer ein Virenprogramm und eine Firewall nutzen, die über aktuelle Updates verfügen, um das System zu schützen. Darüber hinaus sollten alle genutzten Programme wie das Betriebssystem, PDF-Reader, Flash-Player oder die Java-Software über die aktuellsten Sicherheitsupdates verfügen [Spooren & Pohlmann, 2010]. Programme wie der Heise Security Scan[20] können den Nutzer dabei unterstützen, veraltete Software zu identifizieren. Sie scannen das System auf unsichere Programme oder fehlende Sicherheitspatches und bieten meist direkt einen Downloadlink zu den Programmupdates an. Für viele Nutzer ist das Installieren von Sicherheitsupdates ein lästiges Thema, da sich das Betriebssystem oder Programme teilweise recht häufig melden und neue Updates anbieten. Dem Benutzer sind die Verbesserungen meist nicht ersichtlich, weshalb diese oft nur sehr widerwillig die Updates installieren. Sie sind aber wichtig, um Sicherheitslücken zu schließen und so das System vor Angriffen zu schützen.

Zugangsdaten zu verschiedenen Accounts sollten von den Nutzern stets sicher und verantwortungsvoll verwahrt werden, da sie bei einem Missbrauch zu großem Schaden und viel Ärger führen können. Gelingt es beispielsweise einem Angreifer, an die Internet Zugangsdaten eines Nutzers zu gelangen, so kann er auf fremde Kosten surfen. Wenn er an Zugangsdaten zu E-Commerce Seiten wie eBay gelangt, kann er leicht großen Schaden durch den Erwerb von teuren Gegenständen anrichten.

Wird zur E-Mail Verschlüsselung das PKI Verfahren genutzt, darf der private Schlüssel nie in fremde Hände gelangen. Ein Angreifer kann mit dem privaten Key alle Kommunikationsinhalte entschlüsseln und damit vertrauliche Inhalte einsehen. Darüber hinaus kann er E-Mails im Namen des Betroffenen verfassen und diese mit seinem Namen elektronisch signieren, was in einer rechtsverbindlichen Kommunikation wie eine Unterschrift gilt. Daher sollten private Schlüssel immer an einem sicheren Ort aufbewahrt werden. Gelangt der Schlüssel trotzdem in fremde Hände, so muss er möglichst zeitnah für ungültig erklärt werden, wodurch der öffentliche Schlüssel aus den Verzeichnisdiensten gelöscht wird und damit keine Kommunikation mehr stattfinden kann [Spooren & Pohlmann, 2010].

Um sich als Nutzer möglichst sicher im Web zu bewegen, bedarf es eines hohen Maßes an Sensibilität für das Thema Sicherheit. Dies kann ein Nutzer durch langjährige Erfahrungen und ein gleichzeitig hohes Maß an Misstrauen gegenüber den Online-Angeboten bekommen oder durch Schulungen und Weiterbildungen entwickeln. Da immer mehr Jugendliche in sozialen Netzwerken angemeldet sind und dort ihr Profile mit personenbezogenen Daten hinterlegen, sich auf Bilder verlinken und ihre Meinungen preisgeben, sollte schon in der Schule eine gewisse Medienkompetenz vermittelt

[20] Verfügbar unter http://www.heise.de/security/dienste/Der-Scan-869077.html

werden. Kinder und Jugendliche müssen für das Thema sensibilisiert und mit den Gefahren des Internets vertraut gemacht werden. Zwar sollte dies eigentlich Aufgabe der Eltern in der Erziehung sein, da sich aber Heranwachsende im Internet oftmals besser auskennen als ihre Eltern und viele Erwachsene selbst nicht mit den Gefahren des Webs vertraut sind, sollte die Schule hierfür eine Mitverantwortung übernehmen.

Um das Vertrauen der Nutzer zu stärken, sollten Webangebote freiwillig für mehr Datenschutz eintreten. So könnten restriktive Profil-Voreinstellungen neue, unerfahrene Nutzer besser schützen. Die allgemeinen Geschäfts- und Datenschutzbedingungen sollten in einer nutzerfreundlichen Sprache verfasst sein, damit diese für jede Nutzergruppe leicht verständlich und nachvollziehbar sind. Auch in technischer Hinsicht sollten Betreiber stets auf dem neuestem Stand der Sicherheitstechnik bleiben, um Datendiebstähle und Systemeinbrüche zu verhindern und einen möglichst hohen Daten- und Verbraucherschutz zu gewährleisten. Zudem muss der Identitätsdiebstahl aktiv bekämpft werden. Wenn Webangebote solche vertrauensbildenden Maßnahmen durchführen, wäre es eine sinnvolle Maßnahme der Politik, diese Seiten mit einer offiziellen Auszeichnung zu würdigen. Diese Datenschutz-Siegel könnten Nutzern Vertrauen geben, da sie wissen, dass diese Angebote sicher sind. Zudem kann es ein Anreiz für die Anbieter sein, ihre Angebote sicherer zu gestalten, um die Auszeichnung für Marketingzwecke zu nutzen.

Auch das Phishing zeigt, dass die Aufklärung und Sensibilisierung der Nutzer wichtig ist. Phishing ist gefährlich, solange ein Nutzer nicht aufgeklärt wurde, dass gefälschte E-Mails im Umlauf sind und er nicht weiß, wie er damit umzugehen hat. Daher müssen Unternehmen und Behörden darauf hinweisen, dass sie beispielsweise nie einen Nutzer dazu auffordern, sein Passwort in einem Online-Formular einzugeben oder es per E-Mail abfragen.

4. Mögliche Angriffsszenarien auf E-Partizipations-anwendungen

Dieses Kapitel beschäftigt sich mit der Untersuchung verschiedener Angriffsszenarien auf E-Partizipationsanwendungen (vgl. Abschnitt 2.2.3). Neben allgemeinen Gefahren, wie sie in Kapitel 2.3 geschildert wurden, werden hier unterschiedliche Anwendungen direkt untersucht. Dadurch sollen die Risiken unsicherer E-Partizipationsanwendungen abgeschätzt werden. Von den in Kapitel 3.1 aufgezählten Risiken kommen prinzipiell alle für die untersuchten Anwendungen in Betracht.

4.1 Bürgerhaushalte

Wie in Kapitel 2.2.3.1 erläutert, ist ein Bürgerhaushalt ein wichtiges Instrument der heutigen E-Partizipation. Neben der Möglichkeit Schadsoftware auszuführen könnte es zu folgenden sicherheitsrelevanten Ereignissen kommen:

1. Eine einzelne Person meldet sich mehrmals mit verschiedenen Benutzernamen bei einem Bürgerhaushalt an und versucht das Ergebnis des Haushalts in Richtung der eigenen Interessen zu beeinflussen. Eine Gruppe von Personen könnte sich auch zu diesem Vorgehen zusammenschließen, wodurch die Gruppe eine weitaus höhere Macht bekäme.

2. Durch einen Identitätsdiebstahl würde die Möglichkeit bestehen, Aussagen im Namen eines hochangesehenen Bürgers oder Politikers zu verbreiten, die die Meinung der anderen Teilnehmer beeinflussen könnte. Mögliche Angriffsszenarien sind der Passwortdiebstahl mittels Sniffing, Spoofing oder Phishing.

3. Denial-of-Service Angriffe können die Verfügbarkeit des Angebots beeinträchtigen, wodurch die Bürger das Interesse verlieren könnten, die nicht erreichbare Anwendung zu nutzen. Bei Umfragen, könnte die Nichtverfügbarkeit zu einer Verzerrung des Abstimmungsergebnisses führen, da nicht alle Bürger gehört werden.

4. Es könnten Angriffe auf den Server durchgeführt werden um (Hintergrund-) Informationen, die die Politik bereitstellt, um für mehr Transparenz zu sorgen, zum eigenen Vorteil zu fälschen. Dies kann dazu führen, dass die Bürger ihre Äußerungen auf Grundlage von Falschinformationen treffen. Hierdurch können Stimmungen manipuliert werden, ohne dass dies die Teilnehmer bemerken.

5. Auch Angriffe auf den Server mit dem Ziel, Ergebnisse unbemerkt zu löschen oder Abstimmungen zu manipulieren, können große Auswirkungen auf das Endergebnis haben. Hierbei wird die Meinung der Bürger komplett umgangen und die Ergebnisse fallen immer im Interesse der Angreifer aus.

6. Nutzer aus umliegenden Städten, Gemeinden oder Landkreisen könnten das Ergebnis des Bürgerhaushalts zum eigenen Vorteil (z.B. Lärmberuhigung in angrenzenden Ortsteilen) beeinflussen, wenn nicht sichergestellt wird, woher die Nutzer kommen.

7. Ein Datendiebstahl birgt die Gefahr, dass Bürger, die entgegen der Meinung, die sie in der Öffentlichkeit vertreten, eine andere Meinung bei Abstimmungen im Bürgerhaushalt äußern, erkannt und öffentlich vorgeführt werden. Dies kann zu einem Image- und Vertrauensverlust der Bürger in die Anwendungen führen.

4.2 Parteiwebseiten/Politische Netzwerke

Kapitel 2.2.3.2 beschreibt das Wesen der hier untersuchten politischen Webseiten. Da sie wie soziale Netzwerke aufgebaut sind, sind die bedeutsamsten Gefahren die folgenden:

1. Die größte Gefahr geht bei den politischen Netzwerken von dem Identitätsdiebstahl aus, gerade für verifizierte Nutzer. Beispielsweise könnte ein Angreifer, nach einem erfolgreichen Identitätsdiebstahl, Meinungen im Namen von hochrangigen Politikern verbreiten, die ihnen schaden und ihr Ansehen beschädigen oder andere Nutzer in ihrer Meinungsbildung beeinflussen.

2. Wie auch bei den Bürgerhaushalten können Phishing oder Spoofing dazu führen, dass der Nutzer seine Zugangsdaten auf der Webseite eines Angreifers eingibt, der diese anschließend nutzen kann um einen Identitätsdiebstahl zu begehen.

3. Da diese Angebote (wie soziale Netzwerke) darauf angewiesen sind, dass Nutzer persönliche Daten sowie ihre Vorlieben oder Präferenzen angeben, besteht hier eine Gefahr für den Datenschutz. So kann der falsche Umgang mit den Daten durch die Anwendung selbst oder durch einen Datendiebstahl über Sicherheitslecks, wie z.B. bei Cross-Side Scripting, dazu führen, dass sensible Daten zweckfremd missbraucht werden.

4. Falschmeldungen (Hoax), die über das Internet verbreitet werden, könnten über E-Partizipationssysteme wie z.B. politische Netzwerke (weiter-)verbreitet werden. Dies könnte zu einer Verunsicherung bei den Empfängern und durch die kettenbriefartige Verbreitung zu Netzüberlastungen (wie bei einem DDoS-Angriff) führen.

5. Durch Angriffe auf den Server von Parteiwebseiten könnten gezielt Falschmeldungen auf der Webseite verbreitet werden, um beispielsweise politische Entscheidungen zu beeinflussen oder für Unmut unter den Mitglieder zu sorgen.

4.3 E-Konsultation

Wie in Kapitel 2.2.3.3 aufgezeigt wurde, ähnelt das untersuchte E-Konsultationsangebot stark einem Forum, in dem der Bürger mit der Politik diskutieren kann, um gemeinsame Entscheidungen zu erreichen. Daher gelten für diese Art der E-Partizipation insbesondere die folgenden Gefahren:

1. Wenn E-Konsultationsangebote das Ausführen von unsicherem Code (z.B. JavaScript) nicht verhindern, besteht hier die Gefahr des Cross-Side Scripting, was zu einer Umgestaltung der Webseite oder zum Diebstahl des Authentifizierungs-Cookies führen kann. Dadurch kann es zu einem Session-Hijacking kommen und Angreifer können gezielte Falschmeldungen über registrierte Nutzer verbreiten.

2. Ein Denial-of-Service Angriff kann dazu führen, dass die Anwendung nicht mehr erreichbar ist. Dies könnte bewirken, dass die dadurch verärgerten Nutzer dazu gebracht werden, das Angebot nicht mehr zu nutzen. Darüber hinaus kann es zu einer Verzerrung des Abstimmungsergebnisses führen.

3. Angriffe auf den Server, mit dem Ziel Ergebnisse unbemerkt zu löschen oder zu verändern, können bewirken, dass die gemeinsamen Entscheidungen von Politik und Bürgern nicht der Mehrheitsmeinung entsprechen und der dadurch erreichte politische Konsens von dem Angreifer bestimmt wird.

4.4 E-Petitionen

Ein wichtiger E-Partizipationsbaustein des Deutschen Bundestags stellt das E-Petitionsangebot dar, das in Kapitel 2.2.3.4 erläutert wird. Die größten Bedrohungen stellen die folgenden Punkte dar:

1. Da die Einreichung einer elektronischen Petition die gleiche Relevanz wie eine klassische, unterschriebene Petition hat und diese somit gleichzusetzen sind, ist der Identitätsdiebstahl hier besonders gefährlich. Eine gestohlene Identität hat dieselbe Auswirkung wie beispielsweise ein blanko unterschriebenes Petitionspapier, daher sind hier die Sicherheitsanforderungen besonders hoch.

2. Ein weiteres Problem sind Denial-of-Service Angriffe, die dazu führen können, dass nicht alle Bürger, die eine Petition einreichen oder ihre Stimme für eine Petition abgeben wollen, dieses auch tun können. Das kann bewirken, dass dadurch Petitionen wegen zu wenigen Unterstützern scheitern. Diese Ausfälle können auch ohne explizite Angriffe auftreten, beispielsweise wenn sehr viele Nutzer gleichzeitig für eine bestimmte Petition stimmen wollen [heise online, 2009]. Daher ist auch dieser Punkt als besonders kritisch für die E-Petition anzusehen.

3. Angriffe auf die Server von E-Petitionen können dazu führen, dass falsche Daten, wie z.B. die Anzahl der Unterschriften, angezeigt werden. Dadurch können bestimmte Themen, die den Angreifer wichtig sind, die erforderliche Anzahl der Stimmen (50.000) bekommen, wodurch

diese vom Petitionsausschuss beraten werden müssen oder bestimmte Petitionen an Bedeutung gewinnen.

4.5 Zusammenfassung

Wie die Untersuchung der möglichen Angriffsszenarien zeigt, gibt es eine Vielzahl von Angriffsformen, die für E-Partizipationsanwendungen gefährlich sind. Um diesen zu begegnen, müssen einige Gegenmaßnahmen getroffen werden. Hierzu zählt der Schutz vor unbefugter Nutzung der Dienste, Maßnahmen, um die personenbezogenen Daten der Nutzer zu schützen, die sichere Registrierung sowie der Schutz von sensiblen Daten wie Benutzername und Passwort während der Kommunikation. Diese Angriffsszenarien bilden die Grundlage für die Entwicklung eines Analyseframeworks in Kapitel 5 und lassen sich zu den Sicherheitsaspekten Identitätsschutz, Datenschutz, Registrierung und sichere Kommunikation zusammenfassen.

5. Sicherheits- und Datenschutzaspekte von E-Partizipationsanwendungen

Dieses Kapitel beschäftigt sich mit der Untersuchung der Sicherheitsaspekte von E-Partizipationsanwendungen. Zunächst wird das Analyse-Framework vorgestellt, die einzelnen Sicherheitsbereiche und Sicherheitsaspekte erläutert und auf die Methodik bei der Auswertung kurz eingegangen. Danach werden die Ergebnisse der Untersuchung nach den einzelnen Sicherheitsbereichen vorgestellt und den Anwendungen Sicherheitslevel zugeordnet.

5.1 Analyse-Framework

Um den aktuellen Sicherheits- und Datenschutzstand von E-Partizipationsanwendungen zu erfassen, wird zunächst ein Analyse-Framework erarbeitet, mit dessen Hilfe die Anwendungen auf verschiedene Sicherheitsaspekte hin untersucht werden können. Das Framework ist auf alle zu betrachtenden E-Partizipationsplattformen anwendbar und stellt eine einheitliche Untersuchungsgrundlage dar.

Aufgrund der möglichen Angriffsszenarien aus Kapitel 4 und der Gefahrenlage für E-Partizipationsanwendungen aus Kapitel 2.3 und 3.1 werden vier verschiedene Sicherheitsbereiche definiert:

- Der Sicherheitsbereich des Datenschutzes untersucht, wie die Angebote mit personenbezogenen Daten der Nutzer umgehen. Grundlage der Untersuchung stellen verschiedene Bedrohungen des Datenschutzes (vgl. Kapitel 3.3), wie die zweckfremde Weitergabe von persönlichen Daten, dar.

- Der Sicherheitsbereich des Identitätsmanagements betrachtet wichtige Aspekte, die mit dem Identitätsdiebstahl zusammenhängen. Dabei wird untersucht, wie die Angebote mit den Identitäten ihrer Nutzer umgehen. Hier ist die Angriffsform des Identitätsdiebstahls von zentraler Bedeutung, auf dessen Grundlage die Sicherheitsaspekte entwickelt wurden.

- Da die Anwendungen aus Nutzersicht untersucht werden und schon die Registrierung die ersten Grundlage für die sichere Nutzung der Angebote darstellt, wird dies im Sicherheitsbereich der Registrierung zusammengefasst. Wie schon in Kapitel 3.5 aufzeigt sind beispielsweise ein sicheres Passwort und die Aufklärung der Nutzer über den Umgang mit ihren Daten schon von Beginn an wichtig und müssen konsequent umgesetzt werden. Gibt der Nutzer beispielsweise während der Registrierung ein sehr unsicheres Passwort ein, das leicht erraten werden kann, so werden die anderen Sicherheitsmaßnahmen wie z.B. die HTTPS-Verschlüsselung, ausgehebelt und der Schutz vor Angriffen oder Identitätsdiebstählen ist nicht mehr gewährleistet.

- Der Sicherheitsbereich „Sichere Kommunikation“ umfasst abschließend alle Sicherheitsfragen, die mit der sicheren Datenübertragung und dem Schutz vor Bedrohungen wie Sniffing oder Brute-Force-Angriffen zusammenhängen.

Insgesamt stellen die herausgestellten Sicherheitsaspekte Datenschutz, Registrierung, Identitätsmanagement und sichere elektronische Kommunikation wichtige Bereiche des Analyse-Frameworks dar, die in diesem Kontext zwar einzeln betrachtet werden, aber teilweise ineinandergreifen und ein Gesamtpaket der Untersuchung darstellen (vgl. Abbildung 18).

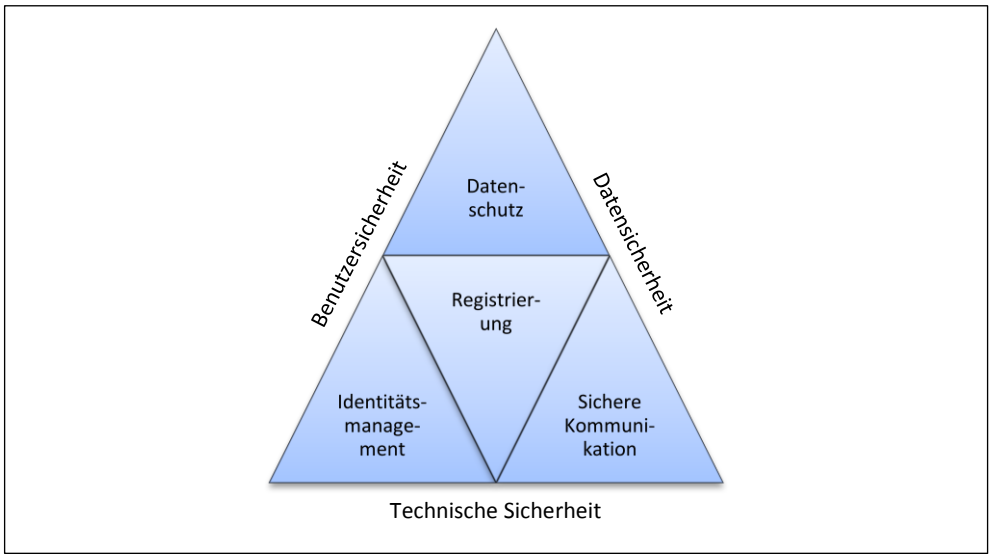

Abbildung 18. Untersuchte Bereiche des Sicherheits- und Datenschutz-Analyse-Frameworks

Im Folgenden werden die verschiedenen Sicherheitsbereiche mit den zugehörigen Sicherheitsaspekten kurz vorgestellt:

Der Bereich des **Datenschutzes** umfasst alle Maßnahmen, die mit dem Schutz von personenbezogenen Daten zusammenhängen. Hierzu zählen die Transparenz und sonstige vertrauensbildende Maßnahmen der Angebote, die Datenschutzaspekte kommunizieren und Vertrauen schaffen. Hinzu kommen die Sicherheitsaspekte Zweckbindung, Weitergabe und Auswertung der Daten, Datensparsamkeit und Datenvermeidung. Sie prüfen, wie mit den sensiblen Daten der Nutzer umgegangen wird und wie hoch die Anzahl der erhobenen Daten ist. Der Aspekt Nutzerkontrolle betrachtet, ob der Nutzer die volle Kontrolle und Transparenz über seine Daten behält.

Der Sicherheitsbereich **Registrierung** umfasst den Registriervorgang und beschreibt, wie Nutzer durch Aufklärung und Information unterstützt werden. Zudem wird die Anzahl der erhobenen Pflichtdaten, also die Datensparsamkeit, untersucht und betrachtet, ob die Datenschutzerklärung deutlich ist und der Nutzer weiß, was mit seinen Daten weiterhin geschieht. Ferner wird untersucht, ob es Maßnahmen für die Unterstützung bei der Erstellung von sicheren Passwörtern gibt und wie die Einwilligung in Sonderdienste wie Newsletter umgesetzt ist.

Der Bereich des **Identitätsmanagements** beschäftigt sich mit dem Benutzeraccount. Er untersucht, ob Nutzer die Möglichkeit einer anonymen oder pseudonymen Nutzung erhalten und wie die Identifikation und Authentifikation von Nutzern stattfindet. Ferner wird betrachtet, ob ein automatischer Logout nach einer gewissen Zeit der Inaktivität umgesetzt ist und ob eine Identitätsprüfung vorhanden ist. Zudem wird untersucht, ob Passwörter per E-Mail verschickt werden.

Die Verwendung von TLS/SSL zur sicheren Übertragung von Daten und die Frage ob dadurch sensible Informationen wie Passwörter im Klartext gesendet werden, umfasst der Sicherheitsbereich **Sichere Kommunikation**. Zusätzlich wird untersucht, wie viele Informationen bei einer Fehlanmeldung preisgegeben werden.

In der nachfolgenden Tabelle werden die einzelnen Sicherheitskriterien übersichtlich aufgeführt. Zusätzlich werden die Fragestellungen, die die einzelnen Aspekte beantworten sollen, aufgezeigt:

Bereich	Kriterium	Fragestellung
Datenschutz	Transparenz	Werden Regeln und Datenschutzbestimmungen übersichtlich und benutzerfreundlich erklärt?
	Zweckbindung	Werden Daten für andere Zwecke verarbeitet?
	Vertrauensbildende Maßnahmen	Gibt es besondere Maßnahmen, die helfen Vertrauen bei den Nutzern zu schaffen und die Sicherheit zu erhöhen?
	Datensparsamkeit/-vermeidung	Werden Daten sparsam und zweckdienlich erhoben?
	Nutzerkontrolle	Hat der Nutzer volle Kontrolle seiner Daten (verändern oder löschen)?
	Weitergabe der Daten	Werden persönliche Daten an Dritte weitergegeben?
	Auswertung der Daten	Wie werden die Daten der Nutzer ausgewertet?
Registrierung	Sicheres Passwort	Wird die Sicherheitsstärke des Passwortes überprüft und gibt es eine Anzeige für die Passwortstärke?
	Datenschutzerklärung deutlich	Sind die Datenschutzerklärungen deutlich und müssen diese akzeptiert werden?
	Einwilligung in Sonderdienste	Werden Sonderdienste wie z.B. Newsletter per Opt-in oder Opt-out angeboten?
	Anzahl der erhobenen Pflichtdaten	Wie hoch ist die Anzahl der Pflichtfelder an persönlichen Daten?
	Aufklärung und Information	Sind die Nutzungsbedingungen deutlich und nutzerfreundlich verfasst?
Identitätsmanagement	Anonymisierung / Pseudonymisierung	Ist eine anonyme oder pseudonyme Nutzung der Dienste möglich?
	Identifikation / Authentifikation	Wie identifiziert und authentifiziert sich ein Nutzer?
	Verifikation	Wie werden die Angaben des Benutzer-Accounts oder der E-Mail Adresse überprüft?
	Passwort per E-Mail verschickt	Werden Passwörter per E-Mail verschickt?
	Automatischer Logout	Wird ein Benutzer nach einer bestimmten Zeit der Inaktivität automatisch abgemeldet?

Sichere Kommunikation	Verwendung von TLS/SSL	Wird SSL oder TLS (HTTPS) auf den Webseiten verwendet?
	Passwörter werden im Klartext gesendet	Werden Passwörter im Klartext über das Netz versendet?
	Minimale Informationen bei Fehlanmeldung	Wie viele Informationen werden preisgegeben, wenn falsche Benutzerdaten eingegeben werden („Passwort falsch“ vs. „Benutzername oder Passwort falsch“)?

Tabelle 4. Untersuchte Bereiche des Analyse-Frameworks

5.2 Methodik bei der Auswertung

Zunächst stand die Informationsbeschaffung über die verfügbaren Angebote der öffentlichen Verwaltung im Vordergrund. Hierbei halfen Webseiten wie `www.e-participation.net`, das „European eParticipation Portal“ (`www.islab.uom.gr/eP`) und `www.buergerhaushalt.org`, die Informationen über E-Partizipationsanwendungen sammeln und eine Vielzahl von Links zu verschiedenen Angeboten bereitstellen. Für die Untersuchung wurden bekannte Online-Angebote aus verschiedenen Bereichen der E-Partizipation gewählt. Es wurde versucht, einen möglichst großen Querschnitt der zurzeit vorhandenen E-Partizipationsanwendungen aus Deutschland abzudecken. Dazu zählen Bürgerhaushalte, politischen Netzwerke von Parteien, das Konsultationsangebot des BMI und die E-Petitionen des Bundestages (vgl. Kapitel 2.2.3).

Mit Hilfe des Kriterienkataloges aus Tabelle 4 wurden diese E-Partizipationsanwendungen anschließend untersucht. Die Betrachtung erfolgte aus Sicht der Bürger, die diese Angebote nutzen. Zunächst fand eine Registrierung auf den Webseiten statt, während zur gleichen Zeit der gleichnamige Sicherheitsbereich „Registrierung“ untersucht wurde. Anschließend erfolgte eine Anmeldung in den Angeboten und die Sicherheitsaspekte der Sicherheitsbereiche „Identitätsmanagement“, „Datenschutz“ sowie „Sichere Kommunikation“ wurden überprüft.

5.3 Ergebnisse

In diesem Kapitel werden die Ergebnisse der Untersuchung vorgestellt. Zunächst wird eine Übersicht über die untersuchten Angebote mit den wichtigsten Ergebnissen gegeben. Anschließend erfolgt eine Auswertung der einzelnen Sicherheits- und Datenschutzkriterien, die in Kapitel 5.1 eingeführt wurden.

5.3.1 Übersicht über die untersuchten Angebote

Die Tabelle mit den Ergebnissen des Analyse-Frameworks ist im Anhang abgelegt. Die unterschiedlichen Farben zeigen positive (grün), neutrale (orange) oder negative (rot) Aspekte der jeweiligen Sicherheitskriterien an.

Das Angebot des Bundes für **E-Petitionen** gibt insgesamt das beste Bild aller untersuchten E-Partizipationsangebote ab. Sehr positiv fällt auf, dass es eine sehr transparente Übersicht über die veröffentlichten Daten während des Petitionsprozesses gibt. Zudem wird empfohlen, für vertrauliche Nachrichten den Postweg anstatt der elektronischen Übermittlung zu wählen. Die gesamte Kommunikation erfolgt über HTTPS und selbst die E-Mails, die die Anwendung an Anschlussdienste sendet, werden SSL-verschlüsselt übertragen. Auch die Adresse, an die man sich für eine Auskunft über seine gespeicherten Daten wenden muss, kann in den übersichtlichen Datenschutzerklärungen leicht gefunden werden. Während der Passworterstellung wird zwar nicht die Passwortstärke angezeigt, jedoch muss ein Begriff gewählt werden, der nicht aus Teilen der E-Mail oder des Benutzernamens besteht und mindestens acht Zeichen umfasst. Zudem ist die Sitzungslänge, also die Zeitspanne bis zur automatischen Abmeldung des Nutzers vom System, einstellbar. Ein Nachteil ist die Vielzahl der erhobenen Daten, die sich allerdings mit dem Petitionsprozess erklären lassen, der ohne die Angaben nicht möglich wäre. Zudem wird die öffentliche Anzeige der E-Mail Adresse im Benutzerprofil mittels Opt-out angeboten. Die Vorgabe eines festen Benutzernamens, der aus dem Wort „Nutzer“ gefolgt von einer sechsstelligen Zahl besteht, schränkt die Nutzerfreundlichkeit des Angebots etwas ein.

Bei **my.FDP** ist positiv hervorzuheben, dass die Datenschutzerklärung sehr übersichtlich und verständlich ist und der Nutzer volle Kontrolle über seine Daten erhält. Ein sicheres Passwort wird automatisch erzeugt und eine SSL Verschlüsselung, zum Schutz der Kommunikation, findet statt. Negative anzumerken ist der E-Mail-Versand des Passwortes an die Nutzer, die fehlende pseudonyme Nutzung im Mitgliederbereich und die öffentliche Anzeige des Vor- und Nachnamens im Benutzerprofil, das im Opt-out-Verfahren abgestellt werden kann.

Der **Bürgerhaushalt Köln** erhebt als Pflichtdaten nur ein frei wählbares Pseudonym sowie die E-Mail-Adresse, persönliche Angaben wie der Vor-und Nachname sind optional. Ein relativ sicheres Passwort wird während der Registrierung automatisch erzeugt und die gesamte Kommunikation erfolgt SSL-verschlüsselt. Das erzeugte sichere Passwort wird per E-Mail verschickt, was ein Sicherheitsrisiko darstellt. Zudem sind die Informationen zu dem Angebot sehr unübersichtlich dargestellt. In die Datenschutzerklärungen muss nicht aktiv eingewilligt werden und sie sind nur über die Spielregeln auffindbar. Alle geschriebenen Beiträge werden zudem unter der Creative-Common Lizenz veröffentlicht, was bedeutet, dass die Einträge unter bestimmten Bedingungen weiterverwendet werden können.

Ein sehr transparentes Angebot stellt der **Bürgerhaushalt Lichtenberg** dar. Es wird übersichtlich und ausführlich erklärt, welche Daten für welchen Zweck erhoben werden. Zudem wird eine Einführung in das Thema geboten. Während der Registrierung sind nur Benutzername, Passwort und E-Mail Pflicht, die restlichen Angaben können optional angegeben werden, sind aber für eine Teilnahme an Abstimmungen notwendigerweise anzugeben. Zudem hat man eine sehr gute Kontrolle über seine Daten und kann diese einfach ändern. Das Löschen des Accounts ist nur durch eine E-Mail an den Betreiber möglich. In den Regeln und den Datenschutzerklärungen wird nicht eindeutig aufgeklärt, ob und wie die persönlichen Daten geprüft werden und man muss während der Registrierung nicht in die Datenschutzerklärungen einwilligen. Außerdem wird von dem Angebot keine SSL-Verschlüsselung verwendet, wodurch die gesendeten Daten, inklusive der Login-Daten, im Klartext über das Internet

versendet werden. Ein weiterer negativer Punkt ist das Verschicken des automatisch erstellten Passwortes per E-Mail an den Nutzer.

Auch im **Bürgerhaushalt Solingen** werden die Spielregeln und Datenschutzerklärungen sehr übersichtlich und äußerst ausführlich behandelt. Es werden nur ein Benutzername und die E-Mail während des Registriervorgangs verlangt, der Rest ist optional. Das Auskunftsrecht über die von ihm gesicherten Daten kann ein Nutzer über die Moderatoren einfordern. Wurden vom Nutzer Kommentare geschrieben, können Nutzerkonten nicht mehr gelöscht werden, allerdings ist eine spätere Anonymisierung der Inhalte durch die Moderatoren auf Anfrage möglich. Der Bürgerhaushalt verwendet keine Verschlüsselung der Kommunikation und bietet keinerlei Hilfestellung bei der Passwortwahl, ansonsten würde er bezüglich der Sicherheitsaspekte sehr gut abschneiden.

Äußerst positiv beim **Bürgerhaushalt Trier** ist die Anzeige der Passwortstärke während der Passwortänderung, was sich nur bei sehr wenigen der untersuchten Angebote findet. Zudem erfolgt die Kommunikation SSL-verschlüsselt und die Nutzer kommunizieren ausschließlich über Pseudonyme. Allerdings werden von dem Angebot eine Vielzahl von persönlichen Daten wie Name, Adresse und Wohnort bei der Registrierung verlangt, ohne genaue Informationen, für welchen Zweck die persönlichen Pflichtangaben verwendet werden. Den Datenschutzerklärungen ist lediglich zu entnehmen, dass eine Überprüfung bei dem Verdacht auf Missbrauch stattfinden kann. Zudem werden in Trier Texte und Bilder, die von Nutzern bereitgestellt werden, unter der Creative-Common Lizenz veröffentlicht, ohne den Nutzer nach einer Einwilligung zu fragen. Zu Beginn der Untersuchungen stellte der Ort der Datenschutzerklärungen ein Problem dar, die nicht wie gewohnt unter „Datenschutz“ sondern im Impressum abgelegt und somit für einen Nutzer nur sehr schwer auffindbar waren. Dies änderte sich aber im Verlauf der Arbeit, mittlerweile gibt es einen eigenen Punkt „Regeln und Datenschutz“, der genauestens über die Verwendung der personenbezogenen Daten informiert. Hieran ist erkennbar, dass sich die Angebote noch in der Entwicklungsphase befinden und sich kontinuierlich weiterentwickeln.

Die **E-Konsultation** des BMI fördert sichere Passwörter durch die Anzeige der Passwortstärke während der Eingabe. Weitere positive Punkte sind die übersichtliche Datenschutzerklärung, die geringe Anzahl der personenbezogenen Daten (Benutzername und E-Mail) sowie die Möglichkeit der pseudonymen oder anonymen Nutzung des Angebots. Als negative Aspekte sind zu nennen, dass man in die Datenschutzerklärung nicht einwilligen muss, dass ein automatisch generiertes Passwort per E-Mail zugeschickt wird und im Besonderen, dass eine Verschlüsselung der Kommunikation fehlt. Zudem kann ein Nutzer sein Konto nur deaktivieren, es muss von einem Moderator endgültig gelöscht werden. Ein einmal gesetztes Passwort kann nachträglich nicht mehr im Benutzerprofil geändert werden. Man muss sich ein neues Passwort über die Option „Passwort vergessen“ per E-Mail zuschicken lassen und kann anschließend über einen Link ein neues Passwort setzen.

Bei dem Angebot **meineSPD** hat der Nutzer volle Kontrolle über seine Daten und kann seinen Account einfach löschen. Alle wichtigen Einstellungen sind von Beginn an per Default deaktiviert, der Nutzer muss per Opt-in explizit freigeben, wenn er beispielsweise seine E-Mail oder die postalische Adresse im eigenen Profil öffentlich anzeigen oder er Statusmails zugesendet bekommen möchte. Dies ist sehr vorbildlich. Zudem sind die Nutzungsbedingungen und Datenschutzerklärungen

übersichtlich gestaltet und der Nutzer muss bei einer Registrierung in diese einwilligen. Das Angebot verwendet SSL, wodurch die Kommunikation in dem Netzwerk und die Account-Daten sicher übertragen werden. Ein Problem findet sich in den Datenschutzerklärungen, da hier angegeben ist, dass die eingegebenen persönlichen Daten für „parteiinterne Zwecke“ verwendet werden, eine Aufklärung über die genauen Zwecke wird nicht gegeben. Zudem gibt es keinerlei Hilfestellung für die Erzeugung von sicheren Passwörtern und es findet sich keine Möglichkeit, anonym oder pseudonym an dem Angebot teilzunehmen.

Der **Bürgerhaushalt Hamburg** klärt seine Nutzer in den Spielregeln, die auch die Datenschutzerklärungen beinhalten, sehr knapp über das Angebot auf. Es werden keine personenbezogenen Daten abgefragt, nur ein Pseudonym und die E-Mail-Adresse müssen bei einer Registrierung angegeben werden. Der gewichtigste negative Punkt ist die Verwendung von Google Analytics, mit dem der Betreiber die Nutzungsdaten der Besucher auswertet. Da hiermit die Daten an einen externen Dritten weitergegeben werden, der seinen Sitz in den USA hat, stellt dies ein erhebliches Sicherheitsrisiko dar. Zudem fehlt bei dem Bürgerhaushalt eine SSL-Verschlüsselung. Eine Datenschutzerklärung existiert nicht, einige Informationen hierzu können in dem Impressum und den Spielregeln gefunden werden. Außerdem lässt das Angebot den Nutzer komplett im Unklaren, wie er sein Profil löschen kann. Newsletter bezieht ein Nutzer automatisch, dies kann nur per Opt-out deaktiviert werden.

5.3.2 Auswertung der Sicherheits- und Datenschutzkriterien

Im Folgenden werden die Untersuchungsergebnisse der obigen E-Partizipationsangebote vorgestellt. Dabei werden die unterschiedlichen Sicherheitsbereiche mit ihren Sicherheitsaspekten einzeln betrachtet.

5.3.2.1 Datenschutz

Im Nachfolgenden werden die Untersuchungsergebnisse des Sicherheitsbereiches Datenschutz vorgestellt, die alle mit dem Schutz von personenbezogenen Daten im Zusammenhang stehen.

Transparenz

Bei der Untersuchung der Transparenz ist erkennbar, dass fast alle Angebote sehr übersichtlich und benutzerfreundlich die Teilnahmebedingungen und Datenschutzaspekte der erhobenen Daten erklären. Der Bürgerhaushalt in Hamburg hat keinen eigenen Unterpunkt mit den Datenschutzerklärungen auf der Webseite. Außerdem informiert das Angebot nicht über die weitere Verwendung von personenbezogenen Daten, klärt aber über die Verwendung von Google Analytics auf. Bei dem Bürgerhaushalt in Köln sind die Datenschutzerklärungen nur über den Umweg der „Spielregeln“ auffindbar. In Trier wird nicht deutlich gemacht, wozu die erhobenen personenbezogenen Daten, wie Name, Adresse und Geburtsdatum, verwendet werden. Im Angebot meineSPD enthält die Datenschutzerklärung eine Klausel, die besagt, dass Nutzerdaten für „interne Zwecke“ verarbeitet werden können, es wird nicht deutlich, für welche Zwecke die Daten genutzt werden.

Zweckbindung/Auswertung der Daten

Die Daten werden von den meisten Angeboten nur für den Zweck, für den sie erhoben wurden und für statistische oder Forschungszwecke verwendet. Dabei werden die Daten ausschließlich anonymisiert ausgewertet. So wird beispielsweise erfasst, wie das prozentuale Verhältnis der teilnehmenden Männer zu Frauen oder der Bildungsstand der Nutzer ist. Der Bürgerhaushalt Hamburg gibt seine Daten an Google Analytics weiter und die SPD verarbeitet Nutzerdaten für „interne Zwecke" weiter, die in der Datenschutzerklärung nicht weiter erläutert werden. Hier weiß der Nutzer nicht, was mit seinen Daten nach einer Registrierung geschieht.

Vertrauensbildende Maßnahmen

Der Hamburger Bürgerhaushalt nutzt Google Analytics, um die Zugriffe auf seine Webseite zu analysieren. Dabei speichert Google Daten wie IP-Adresse, Herkunft und Verweildauer der Besucher auf einem Server in den USA. Schon seit längerem ist dieses Tool datenschutzrechtlich umstritten, da Google mit Google Analytics praktisch ein umfassendes Nutzerprofil von den Webseiten-Besuchern anlegen kann. Dies stellt eine große Gefahr für Nutzer des Hamburger Bürgerhaushaltes dar.

Bei den Bürgerhaushalten Köln und Trier willigen Nutzer in den Teilnahmebedingungen ein, dass die von ihnen verfassten Beiträge und Bilder unter der Creative Commons Lizenz veröffentlicht werden dürfen. Dies gilt zwar nur für nicht kommerzielle Angelegenheiten und nur mit der Namensnennung des Urhebers, trotzdem kann der Nutzer dieses nicht einschränken. Bei dem Lichtenberger Bürgerhaushalt wird zudem nicht ganz klar, wie die (optionalen) persönlichen Daten vom Betreiber geprüft werden.

Bei dem Bürgerhaushalt in Trier ist die Nutzung auf Bürger, die in Trier wohnen, beschränkt. Leider wird aus den Datenschutzerklärungen nicht deutlich, wie und wann die personenbezogenen Adressdaten, die man während der Registrierung angeben muss, geprüft werden.

Das E-Konsultations-Angebot des BMI und die E-Petitionen gehen einen sehr guten Weg der Vertrauensbildung. Das BMI zeigt während der Eingabe eines Passwortes die Passwortstärke an und schult damit den Nutzer. Das Petitionsangebot empfiehlt dem Nutzer, für vertrauliche Nachrichten den Postweg zu wählen. Zudem läuft die gesamte Kommunikation über HTTPS und der E-Mail-Verkehr zwischen der Anwendung und den Anschlussdiensten erfolgt SSL verschlüsselt. Dies kann zu einem sehr hohen Vertrauen der Nutzer führen.

Das Angebot der FDP verwendet Pseudonyme im Forum. Leider ist dieser Pseudonym-Name als Link dargestellt, der zur Profilseite des Autors mit seinem kompletten Namen führt, wodurch die pseudonyme Nutzung mehr als fraglich wird.

MeineSPD deaktiviert von Beginn an alle wichtigen Einstellungen per Default. Hierzu zählen die öffentliche Anzeige von E-Mail und postalischer Adresse im eigenen Profil, das Empfangen von Statusbenachrichtigungen per E-Mail sowie die automatische Annahme von Kontaktanfragen. Alle diese Optionen müssen per Opt-in explizit aktiviert werden.

Datensparsamkeit/-vermeidung

Die Bürgerhaushalte aus Hamburg, Köln, Lichtenberg und Solingen sowie das Angebot des BMI fragen nur die dringend notwendigen Daten für eine Registrierung ab. Er werden nur ein pseudonymer Nutzername, ein Passwort und eine E-Mail Adresse für die Nutzung der Angebote benötigt. Der Bürgerhaushalt in Hamburg erhebt den Vor- und Nachnamen, Trier benötigt den kompletten Namen sowie die Adressdaten, da bei diesem Angebot nur Bürger aus Trier teilnehmen sollen und die Daten ggf. von den Betreibern überprüft werden. Die Webseiten my.FDP und meineSPD verlangen, neben Benutzernamen und E-Mail Adresse, den Vor- und Nachnamen der Nutzer. Dies ist allerdings für das Wesen der Angebote wichtig, da sie wie soziale Netzwerke aufgebaut sind und die Namen zum Finden von Personen und zum Netzwerken benötigt werden.

Nutzerkontrolle über eigene Daten

Die Bürgerhaushalte aus Hamburg und Trier enthalten keine Angaben, wie Nutzer ihr Profil löschen können. Köln und Solingen löschen keine Nutzerkonten, wenn schon Beiträge verfasst wurden, sie bieten aber die Möglichkeit, die geschriebenen Beiträge nachträglich zu anonymisieren. Bei dem E-Konsultationsangebot sowie den E-Petitionen können die Benutzerkonten von den Nutzern lediglich deaktiviert werden, die Löschung muss bei den Moderatoren beantragt werden.

Ein negativer Aspekt fällt bei dem Bürgerhaushalt in Trier auf. Hier dürfen Moderatoren Beiträge verändern, wenn Abkürzungen und Rechtschreibfehler vorhanden sind. Im schlimmsten Fall kann dies den ursprünglichen Sinn einer Nachricht verändern. Bei dem Angebot der FDP ist ein Profil automatisch öffentlich. Es muss erst per Opt-out abgeschaltet werden, wenn ein Nutzer anonym bleiben möchte. Dies führt dazu, dass das Profil anschließend auch bei einer Suche nicht mehr gefunden werden kann. Bei dem Angebot der SPD kann die Sichtbarkeit des eigenen Profils nicht abgeschaltet werden, somit ist der volle Name immer über die Suche auffindbar.

Das Ändern der eigenen Profildaten funktioniert bei den meisten der untersuchten Angeboten problemlos. Lediglich der Bürgerhaushalt in Solingen und das E-Konsultationsangebot geben ihren Nutzern im Nachhinein keine Möglichkeit mehr, ihr eigenes Profil, insbesondere das Passwort, zu ändern.

Weitergabe der Daten an Dritte

Bis auf den Bürgerhaushalt Hamburg, der Daten an Google Analytics sendet, gibt laut den Datenschutzerklärungen kein Angebot Nutzerdaten an dritte Stellen weiter.

5.3.2.2 Registrierung

Dieser Abschnitt befasst sich mit der Untersuchung des Sicherheitsbereiches Registrierung und stellt die Ergebnisse der verschiedenen Sicherheitsaspekte einzeln vor.

Sicheres Passwort

Ein sicheres Passwort ist essentiell, um die Gefahr von einem Identitätsdiebstahl möglichst gering zu halten.

Abbildung 19. Anzeige der Passwortstärke beim Bürgerhaushalt Trier

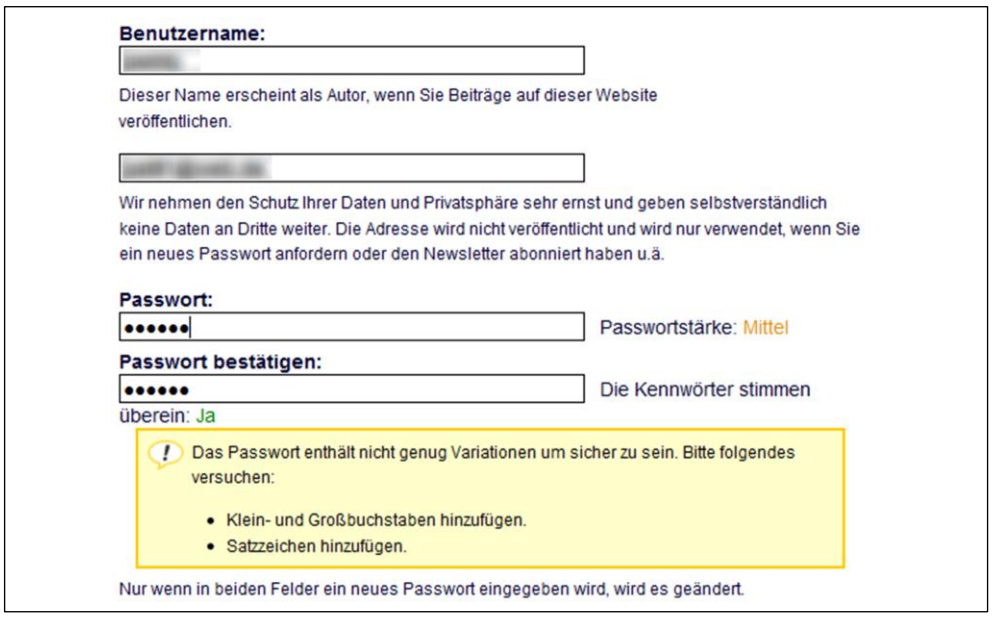

Abbildung 20. Anzeige der Passwortstärke beim E-Konsultationsangebot des BMI

Leider verfügen die wenigsten Seiten über Maßnahmen, die Passwortstärke anzuzeigen und dem Nutzer eine Hilfestellung für das Erstellen eines sicheren Passwortes zu geben. Der Bürgerhaushalt aus Trier (siehe Abbildung 19) sowie des E-Konsultationsangebot des BMI (siehe Abbildung 20) zeigen die Passwortstärke des eingegebenen Passwortes benutzerfreundlich an. Auf der Webseite der Online-Konsultation wird neben der Passwortstärke noch eine Hilfestellungen gegeben, wie das eingegebene Passwort sicherer gemacht werden kann.

Das E-Petitionsangebot gibt dem Nutzer eine Mindestlänge des verwendeten Passwortes von acht Zeichen vor, das zudem nicht aus Teilen der E-Mail bestehen darf. Dadurch wird eine gewisse Grundsicherheit hergestellt. Würde man den Nutzer zusätzlich noch animieren, ein zufälliges

Passwort ohne Begriffe aus dem Wörterbuch zu verwenden, das aus Groß- und Kleinbuchstaben sowie Zahlen und Sonderzeichen besteht, wäre das für ein sicheres Passwort ausreichend.

Die Bürgerhaushalte Köln, Trier und Lichtenberg, das E-Konsultationsangebot sowie my.FDP erzeugen automatisch ein sicheres zufälliges Passwort mit einer Länge zwischen sieben und zehn Zeichen und schicken es dem Nutzer zu. Sie können dies bei der ersten Anmeldung wieder (in ein unsicheres Passwort) ändern.

Die Angebote aus Hamburg, Solingen und der SPD bieten keinerlei Hilfestellung, um ein sicheres Passwort zu erzeugen.

Datenschutzerklärung deutlich

Die Datenschutzerklärungen werden von den meisten Angeboten deutlich angezeigt und benötigen eine explizite Zustimmung mittels Opt-in. Nur die Bürgerhaushalte in Köln und Trier sowie das Online-Konsultationsangebot klären den Nutzer nicht klar über die Datenschutzbedingungen auf. Der Nutzer muss bei diesen Angeboten meist in den „Regeln“ explizit nach den Datenschutzaspekten und der Verwendung seiner Daten suchen. Zudem muss er bei diesen Angeboten, während der Registrierung, nicht in die Datenschutzerklärung einwilligen.

Einwilligung in Sonderdienste

Bei dem Thema Sonderdienste gehen die Angebote weit auseinander. Die meisten Bürgerhaushalte nehmen ihre Nutzer, nachdem sie sich mit ihrer E-Mail Adresse registriert haben, automatisch in den Newsletter-Verteiler auf. Diese Nutzer erhalten so automatisch nach der Registrierung regelmäßig per E-Mail Neuigkeiten zugesandt, ohne sie vorher um Erlaubnis zu fragen. Die Newsletter sind später im Profil per Opt-out abbestellbar. Lediglich Nutzer des Bürgerhaushalts Köln müssen zusätzlichen Angeboten, wie dem Empfang von Newslettern oder von E-Mails anderer Nutzer, vorher explizit mittels Opt-in zustimmen. Denselben Weg gehen auch die Netzwerke von SPD und FDP und das E-Konsultationsangebot. Hier hat der Nutzer die Möglichkeit, seine Newsletter und andere Benachrichtigungsdienste frei zu konfigurieren. In der Grundeinstellung sind diese nach der Registrierung deaktiviert. Im E-Petitionsangebot muss die Anzeige der E-Mail Adresse auf der öffentlichen Benutzerseite mittels Opt-out deaktiviert werden, standardmäßig wird sie angezeigt.

Anzahl der erhobenen Pflichtdaten

Die meisten Angebote verlangen währen der Registrierung lediglich ein Pseudonym, ein Passwort und die E-Mail Adresse des Nutzers. Meist sind persönliche Angaben optional. Der Bürgerhaushalt Trier und das E-Petitionsangebot erheben die meisten Daten der untersuchten Anwendungen. Es werden, neben den Login-Daten, der Vor- und Nachname sowie die Anschrift abgefragt. Die politischen Seiten der SPD und FDP erheben, da sie soziale Netzwerke darstellen, neben den Login-Daten auch den vollen Namen, damit sich Bürger finden und vernetzen können.

Aufklärung und Informationen

Es findet keine durchgängig transparente Aufklärung über das Angebot und die Datenschutzaspekte während der Registrierung statt. Sehr gute und benutzerfreundliche Angaben sind bei den Bürgerhaushalten Hamburg und Lichtenberg sowie dem Angebot my.FDP zu finden. Übersichtlich und über einen Link erreichbar sind die Nutzungsbedingungen und Datenschutzerklärungen ebenso bei meineSPD und den E-Petitionen. Keine Informationen während der Registrierung finden sich hingegen bei den Bürgerhaushalten aus Köln und Solingen sowie dem E-Konsultationsangebot des BMI.

Der Bürgerhaushalt Trier bietet eine sehr nutzerfreundliche Übersicht über die Spielregeln und Datenschutzaspekte an. Dies war nicht immer so, da zu Beginn der Untersuchung für diese Arbeit die Datenschutzaspekte noch versteckt im Impressum der Seite zu finden waren und man nicht in die Datenschutzaspekte einwilligen musste. Das ist eine sehr positive Entwicklung des Angebots.

5.3.2.3 Identitätsmanagement

Nachfolgend werden die Untersuchungsergebnisse des Sicherheitsbereiches Identitätsmanagement präsentiert, die sich mit den Benutzeraccounts beschäftigen.

Anonymisierung/Pseudonymisierung

Alle Bürgerhaushalte bieten ausnahmslos eine pseudonyme Nutzung der Angebote an. Zwar müssen Nutzer des Bürgerhaushalts Trier persönliche Daten während der Registrierung angeben, diese werden aber nicht öffentlich im Rahmen der Beteiligung angezeigt. Das E-Konsultationsangebot bietet ebenfalls eine pseudonyme Nutzung für angemeldete Nutzer an, eine anonyme Nutzung als Gast ist ebenfalls möglich. Die Angebote der SPD und der FDP bieten keine anonyme oder pseudonyme Nutzung an, lediglich im Forum zu my.FDP kann über ein Pseudonym kommuniziert werden, wobei das Benutzerprofil, das den vollen Namen enthält, allerdings verlinkt ist. Auch die E-Petitionen bietet im Forum eine Nutzung mittels eines Pseudonyms an. Auf der Hauptseite werden, aufgrund der Notwendigkeit für den Online-Petitionsprozess, Vor- und Nachname des Hauptpetenten und der Mitzeichner angezeigt.

Identifikation und Authentifikation

Alle Angebote bieten ausnahmslos eine Identifikation mittels Benutzernamen und eine Authentifikation mittels Passwort an. Dies ist die einfachste Form der wissensbasierten Identifikation und zurzeit der zentrale Sicherheitsmechanismus im Internet. Lediglich bei den E-Petitionen bekommt der Nutzer einen Benutzernamen in der Form „Nutzer123456“ fest vorgegeben, in den restlichen Anwendungen kann der Benutzername frei gewählt werden. Die Angebote aus Köln, Trier und Lichtenberg, sowie die E-Konsultation und my.FDP erzeugen ein erstes Passwort selbst und schicken es dem Nutzer per E-Mail zu. Dieses kann nach dem erstmaligen Anmelden geändert werden.

In keiner der untersuchten Anwendungen gibt es ein System zur Feststellung, ob der Nutzer wirklich derjenige ist, für den er sich ausgibt. Lediglich der Bürgerhaushalt in Trier gibt in seinen Regeln an, dass sich jeder Nutzer einem Stadtteil zuordnen und seine Wohn- oder Dienstadresse angeben muss, um damit dem Missbrauch durch mehrfache Registrierungen vorzubeugen.

Verifikation

Alle Angebote verschicken zur Verifikation der Nutzer einen Aktivierungslink an die angegebene E-Mail Adresse, den die Nutzer anklicken müssen, um das Angebot nutzen zu können. Diese Vorgehensweise soll dafür sorgen, dass eine korrekte E-Mail Adresse eingetragen wurde.

Passwort per E-Mail verschickt

Die Angebote, die ein sicheres Passwort automatisch erzeugen (Köln, Trier, Lichtenberg, E-Konsultation und my.FDP), versenden dieses zusammen mit dem Benutzernamen in einer unverschlüsselten E-Mail an den Nutzer. Das erzeugte Passwort ist in allen Fällen relativ sicher, da es aus sieben bis zehn Zeichen und einer Kombination aus Zahlen sowie Groß- und Kleinbuchstaben besteht. Allerdings werden die E-Mails ohne Verschlüsselung oder Zertifikat versendet. Das Fehlen jeglicher Sicherheitsvorkehrungen bei unverschlüsselten E-Mails kann dazu führen, dass Angreifer die Nachrichten ohne großen Aufwand mitlesen und sich mit den Benutzerdaten unter falschen Namen in die Angebote einloggen können.

Automatischer Logout

Für diese Arbeit wurde untersucht, welches Angebot seinen Nutzer nach spätestens zehn Stunden automatisch vom System abmeldet. Dabei stellte sich heraus, dass fast keine Anwendung ein automatisches Logout nutzt. Lediglich in dem Angebot meineSPD wurde der Nutzer nach dem Zeitraum zwangsabgemeldet, bei den E-Petitionen ist die gewünschte Sitzungslänge, also die Zeit bis zum automatischen Logout, frei einstellbar. Standardwert sind hier 240 Minuten, die per Default eingetragen sind.

5.3.2.4 Sichere Kommunikation

Dieses Kapitel beschäftigt sich mit den Untersuchungsergebnissen zur Sicherheit während der Kommunikation und damit, wie (sensible) Daten geschützt werden.

Verwendung von TLS/SSL

Bei den Bürgerhaushalten nutzen lediglich die Angebote aus Köln und Trier SSL, um die Datenübertragung zwischen Server und Client zu verschlüsseln. Weitere Angebote, die dieses Verfahren nutzen, sind meineSPD, my.FDP und die E-Petitionen. Die Haushalte aus Hamburg, Lichtenberg und Solingen sowie das E-Konsultationsangebot verwenden keine Technologien, um die Übermittlung der Daten und somit auch des Benutzernamens und Passworts zu schützen. Ein sehr positives Beispiel stellt der Bürgerhaushalt Köln dar, da er die Verschlüsselung als Einziger für den gesamten Besuch auf der

Webseite anbietet und nicht erst ab dem Login-Vorgang. Somit ist hier die höchste Sicherheit der Kommunikation geboten.

Passwörter werden im Klartext gesendet

Da von den Bürgerhaushalten in Hamburg, Lichtenberg und Solingen sowie von dem E-Konsultationsangebot keine SSL-Verschlüsselung verwendet wird, werden hier auch die Anmeldedaten wie Benutzername und Passwort im Klartext übertragen. Somit können diese von einem Angreifer mit wenig Aufwand mittels Sniffing ausgelesen werden.

Minimale Informationen bei einer Fehlanmeldung

Fast alle untersuchten Angebote geben nur minimale Informationen preis und verraten bei einer Anmeldung mit falschem Benutzernamen oder Passwort nicht, welcher Part falsch eingegeben wurde. Lediglich der Bürgerhaushalt in Köln sowie das E-Petitionsangebot spezifizieren, ob ein Benutzername existiert und nur das Passwort falsch eingegeben wurde.

5.4 Zusammenfassung

Insgesamt ist das Sicherheitsniveau der untersuchten E-Partizipationsanwendungen relativ durchwachsen. Es wird der Datenschutz recht gut umgesetzt, die anonyme oder pseudonyme Nutzung ist fast durchgängig möglich und die Zweckbindung der Daten ist vorhanden. Allerdings gibt es noch Verbesserungspotential. Gerade die Sicherheitsmängel in Bezug auf die Verschlüsselung der Kommunikation und die Probleme mit dem Versenden von Passwörtern per E-Mail gehören dazu.

Positive Ergebnisse

Besonders positiv hervorzuheben sind einige Aspekte, die die Sicherheit der untersuchten Plattformen erhöhen:

- Eine sehr gute Maßnahme zur Förderung der Sicherheit der Benutzeraccounts findet sich bei dem Bürgerhaushalt Trier und dem E-Konsultationsangebot des BMI. Diese Seiten bieten dem Nutzer Hilfestellungen bei der Erstellung eines Passwortes an, indem sie die Passwortstärke anzeigen (schwach, mittel, hoch) und Tipps geben, wie das Passwort stärker gemacht werden kann. Besonders hervorzuheben ist das Angebot des BMI, da es besonders benutzerfreundlich Anweisungen und Tipps gibt.

- Ein hohes Maß an Sicherheit bietet das Angebot der E-Petitionen, da unter anderem darauf hingewiesen wird, dass der unverschlüsselte Nachrichtenversand über das Internet unsicher ist und für vertrauliche Nachrichten der Postweg empfohlen wird. Zudem werden E-Mails zwischen der Anwendung und Anschlussdiensten SSL-verschlüsselt übermittelt.

Negative Ergebnisse

Es können zwei Probleme festgestellt werden, die alle Anwendungen gleichermaßen betreffen:

- Es findet in allen untersuchten Anwendungen eine Anmeldung mittels Benutzername und Passwort statt. Eine Single-Sign-On Lösung wird von keinem der untersuchten Anwendungen unterstützt. Will ein Bürger an verschiedenen Angeboten partizipieren, so muss er sich für jedes Angebot einen neuen Nutzernamen und ein neues Passwort merken. Dies kann dazu führen, dass ein Nutzer die gleiche Benutzernamen/Passwort-Kombination für mehrere Anwendungen benutzt.

- Die verschiedenen Angebote haben nur beschränkte Möglichkeiten zu überprüfen, ob der Nutzer wirklich der ist, für den er sich ausgibt. Die meisten Angebote kontrollieren nicht, wer die Nutzer sind, da sie nur ein Pseudonym der Nutzer verwenden. Der einzige Bezug zum Nutzer stellt hier die E-Mail Adresse dar. Daher ist es bei diesen Angeboten möglich, dass sich ein Nutzer mit verschiedenen E-Mail-Adressen mehrmals registrieren kann. Die anderen Plattformen, die ihr Angebote nur für die eigenen Bürger bereitstellen wollen oder die Nutzer aufgrund des Wesens der Angebote identifizieren müssen, erheben diverse personenbezogene Daten, wie den Namen und die Adresse, um die Bürger gegebenenfalls überprüfen zu können. Dies könnte den Bürger von einer Beteiligung abschrecken.

Sicherheitsmängel

Bei der Untersuchung der E-Partizipationsangebote fallen drei gravierende Datenschutz- bzw. Sicherheitsmängel auf:

- Ein sehr großes Sicherheitsrisiko findet sich bei dem Bürgerhaushalt Hamburg, der Google Analytics nutzt, um Besucherdaten auszuwerten. Dieses Google-Programm steht schon seit langem in der Diskussion, da nicht sicher ist, in wieweit Datenschutzaspekte eingehalten werden. Zudem werden die Daten, inklusive der IP-Adresse, die in Deutschland ein personenbezogenes Datum darstellt, auf einen Server in den USA übermittelt und ausgewertet. Somit werden personenbezogene Daten an einen Dritten weitergegeben, der über kein adäquates Datenschutzniveau wie Deutschland verfügt [Möhring, 2009]. Außerdem hat der Nutzer keine Möglichkeit, die Beobachtungen durch Google aktiv abzulehnen (Opt-in oder Opt-out). Der Einsatz im Bürgerhaushalt Hamburg ist zudem verwunderlich, da der Landesdatenschutzbeauftragte aus Hamburg laut [Jakobs, 2009] das Tool Google Analytics nach deutschem Recht als unzulässig erachtet.

- Eine große Gefahr geht von dem Versand automatisch erzeugter Passwörter per E-Mail aus. Das ist ein Sicherheitsrisiko, da eine unverschlüsselte E-Mail ein unsicheres Kommunikationsmedium darstellt (vgl. Kapitel 3.4.4). Zwar können die Nutzer ihre Passwörter nach dem ersten Login direkt verändern, tun sie dies aber nicht, können Angreifer, die das Passwort aus der E-Mail ausgelesen haben, sich mit dem Account unbemerkt anmelden und im Namen des Betroffenen auf der Online-Plattform agieren.

- Der dritte große Sicherheitsmangel besteht in der fehlenden Umsetzung einer SSL Verschlüsselung in fast der Hälfte aller untersuchten E-Partizipationsanwendungen. Da dadurch Benutzernamen und Passwort im Klartext übertragen werden, besteht hier eine große Gefahr des Identitätsdiebstahls durch einfaches Mitlesen und Aufzeichnen der Kommunikationsinhalte, beispielsweise in einem offenen WLAN oder einem unverschlüsseltem Router.

Ranking der Angebote

Es gibt kein Angebot, das während der Untersuchung durchgängig alle Sicherheitsaspekte zufriedenstellend umgesetzt hat. Sehr positiv aufgefallen sind aber das Angebot my.FDP und das Online-Petitionsangebot der Bundesregierung, hier sind relativ wenige Beanstandungen zu finden. Im Mittelfeld liegen die Haushalte aus Köln, Lichtenberg, Solingen und Trier, das E-Konsultationsangebot des Innenministeriums sowie das Netzwerk meineSPD. Hier sind einzelne sicherheitsrelevante Risiken vorhanden. Einen großen Verbesserungsbedarf in Sicherheitsfragen hat der Bürgerhaushalt aus Hamburg. Bei diesem Angebot kommen gleich mehrere Beanstandungen zusammen, die behoben werden sollten. Ein Ranking der Beanstandungen findet sich in Tabelle 5.

Wenig Beanstandungen	- my.FDP - E-Petitionen
Einige Beanstandungen	- Bürgerhaushalt Köln - Bürgerhaushalt Lichtenberg - Bürgerhaushalt Solingen - Bürgerhaushalt Trier - E-Konsultationsangebot des BMI - meineSPD
Größere Beanstandungen	- Bürgerhaushalt Hamburg

Tabelle 5. Gruppierung nach den Beanstandungen der E-Partizipationsangebote

5.5 Sicherheitslevel

Auf Grundlage der Untersuchung werden den E-Partizipationsbereichen Bürgerhaushalt, E-Konsultation, Parteiwebseiten und E-Petitionen Sicherheitslevel zugeordnet. Die Vergabe der Sicherheitslevel ist auch immer im Kontext einer „traditionellen“ Lösung (ohne Internet) zu sehen. Die Zuordnung der Sicherheitslevel erfolgt auf Grundlage der möglichen Angriffsszenarien auf die E-Partizipationsanwendungen (vgl. Kapitel 4).

Neben den Angriffsszenarien spielt auch die Zielgruppe und die dadurch entstehende Nutzerzahl eine große Rolle, da eine größere Zielgruppe auch einen größeren Anreiz für den Angreifer darstellt. Lokale Angebote sind vermutlich eher für lokale Angreifer interessant.

Eine weitere Rolle für die Bewertung der Sicherheitslevel spielt die Perspektive der elektronischen Partizipation. Die Top-down-Perspektive schließt alle Formen der E-Partizipation, die verwaltungs- und politikseitig initiiert werden, ein. Die Bottom-up-Perspektive geht von der Bürgerschaft,

Nichtregierungsorganisationen oder der Wirtschaft aus und richten sich an Verwaltung und Politik als Adressaten [Märker & Wehner, 2008]. Die größere Gefahr geht von den Bottom-up-Anwendungen aus, da hier der Bürger mehr Freiheiten bei der Beteiligung hat und nicht so stark eingeschränkt wird. Die Mehrheit der in dieser Arbeit untersuchten E-Partizipationsanwendungen haben eine Top-down Perspektive.

Bürgerhaushalt

Bürgerhaushalte bieten die Funktionalität, sich in Foren austauschen, sich zu bestimmten politischen Themen zu informieren und Vorschläge für die Verwendung von Geldern oder für Sparmaßnahmen zu äußern. Somit werden bei den untersuchten Bürgerhaushalten derzeitig lediglich Vorschläge für eine zukünftige Finanzpolitik gesammelt, die endgültige Entscheidung liegt bei den verantwortlichen politischen Akteuren. Eine Gefahr besteht bei den Bürgerhaushalten insbesondere bei einem Daten- oder Identitätsdiebstahl, wenn beispielsweise ein Angreifer Daten ausliest oder den Account eines anderen verwendet, um in dessen Namen Beiträge zu verfassen. Dieses Problem ist umso größer, je mehr personenbezogene Daten von den Angeboten erhoben werden. Somit erreichen Bürgerhaushalte keine politischen Entscheidungen, sondern unterstützen lediglich die Politik und schaffen Transparenz. Daten- oder Identitätsdiebstahl wäre zwar gefährlich, jedoch ist das Risiko bei den meisten Haushalten, die nur wenige personenbezogene Daten erheben, eher gering. Daher haben Bürgerhaushalte insgesamt ein **mittleres Sicherheitslevel**.

Alle Bürgerhaushalte haben eine Top-down-Perspektive der Beteiligung. Die Sicherheitslevels der einzelnen Anwendungen werden nach der Art des Beteiligungsverfahrens sowie der Nutzerzahl ermittelt, wobei alle Bürgerhaushalte als Zielgruppe die Bürger der entsprechenden Stadt haben:

- Der Bürgerhaushalt Köln hat mit rund 10.000 Nutzern eine vergleichsweise sehr hohe Nutzerzahl und das Beteiligungsverfahren lässt viele Freiheiten zu. Daher hat er ein **hohes Sicherheitslevel**.
- Der Hamburger Bürgerhaushalt lässt seinen Bürgern Budgets für den Haushalt verteilen, die von der Stadt vorgegebenen werden. Zudem nutzten 2009 nur 552 Bürger dieses E-Partizipationsangebot, wodurch es ein **mittleres Sicherheitslevel** hat.
- In Trier und Lichtenberg nutzten nur rund 1.500 bzw. 2.700 Bürger das Angebot. Daher haben diese Haushalte ein **mittleres Sicherheitslevel**.
- Den Bürgerhaushalt in Solingen nutzten bislang rund 3.600 registrierte Bürger. Da dieser Bürgerhaushalt eine Beteiligung erlaubt, bei dem die Bürger über Vorschläge ihrer Verwaltung abstimmen, hat auch dieses Angebot ein **mittleres Sicherheitslevel**.

E-Konsultation

Das E-Konsultationsangebot des BMI hat das Ziel, Stimmen für bestimmte Themen zu sammeln und zu einem gemeinsamen Konsens zu kommen. Hierbei diskutiert das Innenministerium, vertreten durch den Innenminister de Maizière, mit Bürgern über die zukünftige Netzpolitik. Da diese Kommu-

nikation einem Forum entspricht, in dem moderiert und gelenkt über spezielle Themen diskutiert werden kann und auch Gasteinträge möglich sind, ist die Gefahr nicht besonders hoch einzuschätzen. Lediglich der Identitätsdiebstahl ist hier ein mögliches Angriffsszenario, das aber bei Einzelfällen keine große Auswirkung auf den Nutzer und die Diskussion haben sollte.

Die Thesen, über die diskutiert werden können, werden im Top-Down Verfahren vorgegeben. Die meistdiskutierte These zählte lediglich 327 Beiträge. Aufgrund der eher geringen Beteiligung, der Top-down Vorgaben der Thesen und geringen Gefahren durch den Identitätsdiebstahl haben solche E-Konsultationsangebote ein **niedriges Sicherheitslevel**.

Parteiwebseiten/Politische Netzwerke

Die hier untersuchten Parteiwebseiten von FDP und SPD sind wie soziale Netzwerke aufgebaut und erlauben es, sich mit anderen zu vernetzen und Freunde wiederzufinden. Zusätzlich kann man in Foren oder Blogs seine Meinung äußern, zu bestimmten politischen Themen Stellung beziehen und verschiedenen Gruppen beitreten. Ein bestimmter interner Bereich ist nur für Mitglieder, die sich mit ihrer Mitgliedsnummer verifiziert haben, zugänglich und beinhaltet zusätzliche Funktionen wie eine Stellenbörse.

Die größte Gefahr geht von einem Identitätsdiebstahl von verifizierten Nutzern aus (vgl. Kapitel 2.2.3.2), indem in ihrem Namen Falschaussagen in den Netzen verbreitet werden.

Die sozialen Netzwerke verfügen über eine hohe Zahl an registrierten Nutzern. So verzeichnet das Angebot my.FDP im September 2010 rund 45.400 Nutzer [FDP-Bundespartei, 2010], die SPD im Juni 2009 rund 30.000 Nutzer [Brauckmann, Politische Onlinemacher im Interview: Sebastian Reichel (SPD), 2009]. Zwar geht das Beteiligungsverfahren bei beiden Web-Seiten von den Anbietern im Top-Down Verfahren aus, da aber die Zielgruppe deutschlandweit angesprochen wird, haben beide Anwendungen eine **hohe Sicherheitsstufe**.

E-Petitionen

Da eine klassisch schriftlich eingereichte Petition immer unterschrieben sein muss, kann angenommen werden, dass man sowohl beim Erstellen einer Petition als auch beim Mitzeichnen im Internet eine Art digitale Unterschrift abgibt, die die handschriftliche Unterschrift ersetzt. Zudem werden der Einreichende sowie die Mitzeichner jeder Petition mit vollem Namen und Bundesland, also mit personenbezogenen Daten, im Internet veröffentlicht. Zwar kann auch hier nicht direkt politisch mitbestimmt werden, dennoch ist ein Identitätsdiebstahl wegen der Sensibilität der elektronischen Unterschrift und der Öffentlichkeit der Petitionen gefährlicher als in den restlichen Anwendungen.

Es nutzen rund 600.000 registriere Nutzer diese E-Partizipationsanwendung [Kerkmann, 2010], was der größten Nutzerzahl aller untersuchten Anwendungen entspricht. Das Angebot ist an alle BürgerInnen in Deutschland gerichtet und das Engagement geht von den Bürgern aus (Bottom-up). Daher haben E-Petitionen **hohe Sicherheitsanforderungen**.

Zusammenfassung

Die Sicherheitslevels sind in der nachfolgenden Tabelle 6 nochmals zusammengefasst aufgeführt. Dabei werden die E-Partizipationsanwendungen insgesamt und jede untersuchte Anwendung zusätzlich einzeln dargestellt.

Bürgerhaushalte	
Köln	**Hoch**
Hamburg	**Mittel**
Trier	**Mittel**
Lichtenberg	**Mittel**
Solingen	**Mittel**
Insgesamt	**Mittel**
Parteiwebseiten/Politische Netzwerke	
SPD	**Hoch**
FDP	**Hoch**
Insgesamt	**Hoch**
E-Konsultation	
E-Konsultation des BMI	**Niedrig**
Insgesamt	**Niedrig**
E-Petitionen	
Bundestag	**Hoch**
Insgesamt	**Hoch**

Tabelle 6. Übersicht über die Sicherheitslevels

6. Empfehlungen für Betreiber von E-Partizipations-anwendungen

Dieses Kapitel gibt Empfehlungen auf Grundlage der Untersuchungsergebnisse ab, die an die Betreiber von E-Partizipationsanwendungen gerichtet sind. Sie haben aber auch Gültigkeit für andere Anwendungen im Web. Zudem wird auf zukünftige Technologien eingegangen, die in nächster Zeit erscheinen werden und das Potential haben, die Nutzung und die Sicherheit von Online-Anwendungen zu verändern.

6.1 Empfehlungen

Im Folgenden werden Ratschläge auf Grundlage der Untersuchungsergebnisse abgegeben, die helfen können, die betrachteten Webanwendungen sicherer zu machen.

Google Analytics

Der Bürgerhaushalt in Hamburg nutzt Google Analytics, um eine Zugriffsanalyse der Webseite durchzuführen. Hierbei wird unter anderem die vollständige IP-Adresse des Seitenbesuchers an Google übermittelt, was einer Übermittlung eines personenbezogenen Datums an einen Dritten entspricht. Hierüber klärt der Bürgerhaushalt weder in seinen „Spielregeln“ ausreichend auf, noch werden die Nutzer gefragt, ob sie mit dieser Übermittlung einverstanden sind. Hier ist ein unbedingter Handlungsbedarf vorhanden, da laut [Ulbricht, 2007] ein solches Vorgehen gemäß Paragraf 16, Absatz 3 des Telemediengesetzes Bußgelder von bis zu 50.000 Euro nach sich ziehen kann, wenn der Seitenbetreiber die Nutzer nicht um Einwilligung bittet. Zudem ist die Sicherheit der Daten nicht gewährleistet, da es theoretisch möglich wäre, dass Nutzer, die über ein Google Benutzerkonto verfügen, während des Besuches der Seite identifiziert werden. Google hat die Möglichkeit die IP-Adresse von Analytics mit der IP-Adresse des Google Accounts zu verknüpfen und so den Nutzer hinter der IP-Adresse dem Account zuzuordnen. Das Unternehmen wäre damit in der Lage, genau nachzuvollziehen, wer sich wann auf welcher Webseite aufgehalten hat. Hamburg sollte auf ein Analyseprogramm umsteigen, das auf dem Webserver selbst läuft und die Daten hier analysiert. So müssen keine Daten an Dritte übertragen werden und die Sicherheit der personenbezogenen Daten bleibt gewahrt. Beispiele hierfür sind das Open Source Programm Piwik[21] oder SlimStat[22], die beide auf dem Webserver installiert werden können, kostenlos sind und eine eigene Webanalyse der Nutzerdaten ermöglichen. Den Bürgern kann generell nur empfohlen werden, Maßnahmen gegen die Datensammlung von Google Analytics zu ergreifen. So hat Google selbst Mitte 2010 ein Opt-Out-Plugin[23] für verschiedene Browser herausgebracht, das den Webanalysedienst Analytics abschaltet.

[21] http://de.piwik.org/
[22] http://slimstat.net/
[23] Verfügbar unter http://tools.google.com/dlpage/gaoptout?hl=de

SSL/TLS

Ein großes Sicherheitsrisiko bei verschiedenen E-Partizipationsangeboten ist das Fehlen einer Ende-zu-Ende Verschlüsselung zwischen Webbrowser und Server. Hier müssen einige Anbieter nachbessern, da alle Angebote, unabhängig von ihrem Sicherheitslevel, die Verbindung mittels SSL verschlüsseln sollten. Im günstigsten Fall für die Zeit der gesamten Sitzung, also vom Betreten einer Seite bis zum Verlassen, mindesten jedoch für den Login-Vorgang. Nur so kann sichergestellt werden, dass sensible Daten wie Benutzername und Passwort sicher über das Netz übertragen werden. Nicht nur um die Angebote selbst zu schützen, sondern auch vor dem Hintergrund, dass viele Nutzer nur ein Passwort für verschiedene Online-Anwendungen benutzen. Wenn ein Angreifer das Passwort während des Logins abfängt, kann er zwar auf dem Online-Angebot mit niedrigen Sicherheitsanforderungen nicht viel Schaden anrichten, der Angreifer hat dadurch aber eventuell Zugriff auf viel sensiblere Anwendungen wie z.B. Online-Banking. Die Verschlüsselung mittels SSL ist beispielsweise in den großen sozialen Netzwerken schon lange Standard. So zeigt eine Analyse mittels Wireshark, dass StudiVZ und Wer-Kennt-Wen.de den Login-Vorgang mittels SSL verschlüsseln, Facebook bietet die Verschlüsslung während der gesamten Sitzung an. Hier sollten sich die öffentlichen Angebote ein Vorbild nehmen, da die Angriffsszenarien schon lange bekannt sind (siehe Kapitel 3.1 Sniffing) und die Verschlüsselung ein seit längerer Zeit verwendetes und effektives Mittel für eine hohe Kommunikationssicherheit ist. Als Mindestanforderung sollte, wenn die Anwendung selbst als nicht schutzbedürftig durch SSL eingestuft wird, Registrierung, Login, Zugriff auf persönliche Daten, Passwort-Änderung und die „Passwort vergessen“-Funktion verschlüsselt ablaufen [Bundesamt für Sicherheit in der Informationstechnik, 2006]. Die öffentliche Verwaltung sollte keine Fehler machen, die schon lange bekannt sind und für die es bereits Best-Practice Lösungen aus der Privatwirtschaft gibt.

Ein weiteres Anwendungsfeld von SSL und TLS ist die Authentifizierung und Wiedererkennung von Clients und Servern im Internet. Voraussetzung hierfür ist, dass das SSL-Serverzertifikat niemals fehlerhaft sein darf und der Servername, der in der URL angezeigt wird, immer exakt mit dem im Zertifikat eingetragenen Namen übereinstimmt. So lassen sich Fehlermeldungen umgehen, die den Nutzer verunsichern können.

Passwort versenden

Ein großes Problem, das erstaunlicherweise bei vielen der untersuchten Webseiten auffiel, ist das Versenden eines automatisch erzeugten Passwortes per E-Mail an die Nutzer. Dies geschieht meist während der Registrierung oder wenn ein Passwort vergessen wurde und man ein neues anfordert. Wie in Kapitel 3.4.4 beschrieben wurde, stellt die klassische E-Mail ein sehr unsicheres Kommunikationsmittel dar und kann leicht mitgelesen werden. Ein Angreifer kann beispielsweise durch Sniffing das in der E-Mail enthaltene Passwort auslesen und so einen Identitätsdiebstahl begehen. Um für etwas mehr Sicherheit zu sorgen, sollte ein Nutzer sein Passwort beim ersten Einloggen direkt ändern müssen, bevor er das Angebot nutzen kann. Am besten sollte dieses überflüssige Sicherheitsrisiko abgestellt werden. Die Angebote sollten eher eine Hilfestellung für die Erstellung von sicheren Passwörtern geben (wie es in Kapitel 3.5.1 vorgestellt wurde) und keine Passwörter mehr über unsichere Kanäle verschicken.

E-Mail

Werden E-Mails von der Webanwendung an die Nutzer versendet, sollten diese immer von der gleichen Domain wie die Webanwendung kommen, wie z.B. `service@webanwendung.de`. Niemals sollten E-Mails von einem Dritt-Anbieter wie `noreply@maildienstleister.com` versendet werden, da der Nutzer sonst nicht mehr unterscheiden kann, ob die Nachricht vertrauenswürdig ist oder nicht. Bei der Untersuchung stellte sich allerdings heraus, dass bei den Bürgerhaushalten von Solingen und Köln sowie dem E-Konsultationsangebot die E-Mails von der Domain `zebralog.de` kommen, dem Dienstleister und verantwortlichem Unternehmen der drei E-Partizipationsanwendungen. Dieser ist zwar in diesem Fall ein vertrauenswürdiger Anbieter, dennoch sollte man hier nachbessern und den E-Mail Provider auf die URL der entsprechenden Webseiten, wie z.B. `info@solingen-spart.de` oder `buergerhaushalt@stadt-koeln.de` umstellen, da den wenigsten Nutzern die Zusammengehörigkeit von `zebralog.de` und der jeweiligen Webanwendung bekannt sein dürfte.

Single-Sign-On

In allen untersuchten E-Partizipationsanwendungen muss sich ein Nutzer mittels Benutzername und Passwort anmelden. Das bedeutet, dass er sich, wenn er mehrere E-Partizipationsanwendungen nutzt, eine Vielzahl von Benutzernamen und Passwörtern merken muss. Betrachtet man die Passwortsicherheit aus Kapitel 3.5.1, so wird empfohlen für jeden Benutzer-Account ein individuelles und sicheres Passwort zu wählen. Das bedeutet, für jede Anwendung muss im Idealfall ein Passwort aus kleinen und großen Buchstaben, Zahlen und Sonderzeichen generiert werden, das sich der Nutzer merken muss. Da dies bei einer Vielzahl von Diensten nur sehr schwer umsetzbar ist, wird der Großteil der Nutzer nur ein Passwort in verschiedenen Anwendungen einsetzen.

Ein einheitliches Single-Sign-On wäre ein probates Mittel, den vielen Problemen mit Passwörtern und Benutzeraccounts zu begegnen. Da jeder Internet-Nutzer immer mehr Identitätsdaten zu verwalten hat, wird die Verwendung einer einheitlichen Zugangsmöglichkeit immer mehr an Bedeutung gewinnen. So können auch die Schwierigkeiten im Zusammenhang mit dem Erstellen von sicheren Passwörtern, dem Versenden von Passwörtern per E-Mail usw. wirkungsvoll begegnet werden. Leichte Bedienbarkeit und der Schutz gegen einfache Phishing-Angriffe müssen dabei im Vordergrund der Entwicklungen stehen. In der Industrie werden zurzeit sogenannte Single-Sign-On-Protokolle als Standardlösung für die Login-Problematik entwickelt. Neben Protokollen wie OpenID[24], das eine niedrige Sicherheitsanforderung voraussetzt, oder dem Cardspace[25] von Microsoft, ist der offene Standard SAML[26] (Security Assertion Markup Language) zu nennen, der mittlerweile eine hohe technische Reife erlangt hat. Zudem ist es mit SAML problemlos möglich, die Authentisierung des neuen elektronischen Personalausweises (vgl. Kapitel 6.2.1) einzubinden [Borges, Arbeitsgruppe Identitätsschutz im Internet e.V., 2010].

[24] Siehe http://www.openid-center.de/
[25] Siehe http://www.microsoft.com/windows/products/winfamily/cardspace
[26] Siehe http://saml.xml.org/

Logout

Von fast keiner der untersuchten Anwendungen wurde ein automatischer Logout umgesetzt. Wenn ein Nutzer, der sich auf der Webanwendung angemeldet hat, seinen Browser einfach schließt ohne sich auszuloggen, kann ein Angreifer, der beispielsweise das Cookie von dem Nutzer ausgelesen hat, in dieser Session weiterarbeiten. Viele Nutzer wissen gar nicht, dass sie nicht ausgeloggt werden, wenn sie das Browserfenster einfach schließen. Daher sollte der Nutzer nach einer bestimmten inaktiven Zeit automatisch vom System abgemeldet werden. Zudem sollten Anwendungen den Benutzer darin trainieren, den Logout auch wirklich vorzunehmen und ihn andernfalls beim nächsten Anmelden darauf hinweisen, dass in Zukunft ein explizites Ausloggen erfolgen sollte [Bundesamt für Sicherheit in der Informationstechnik, 2006].

Schulung der Nutzer

Neben dem Technikeinsatz sind auch organisatorische Maßnahmen notwendig, um die Sicherheit von Webanwendungen zu erhöhen. Ein wichtiger Schritt ist die Schaffung eines Sicherheitsbewusstseins über Schulungen von Nutzern und/oder Mitarbeitern von E-Partizipationsanwendungen. Einer der wichtigsten Punkte bei Schulungen ist eine zielgruppengerechte Ansprache der Nutzer. Nur wenn der Nutzer die Inhalte auch versteht, ist ein Lernerfolg erreichbar [Borges, Arbeitsgruppe Identitätsschutz im Internet e.V., 2010].

Es besteht ein erheblicher Bedarf an Informationen und Aufklärungen in Bezug auf die Sicherheit, da Nutzer oft nur über ein sehr geringes Wissen im Zusammenhang mit dieser Thematik verfügen. Daher müssen die Gefahren des Internets, sowie die erforderlichen Gegenmaßnahmen, Gegenstand der Aufklärung sein. Gerade die rechtlichen Pflichten nach § 4 (Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung) BDSG und §§ 5 (Allgemeine Informationspflichten), 6 (Besondere Informationspflichten bei kommerziellen Kommunikationen) TMG (Telemediengesetz), die eine Mindestanforderung der Informationspflichten darstellen, müssen benutzerfreundlich umgesetzt werden. Zudem können Empfehlungen für das Nutzerverhalten, beispielsweise in den allgemeinen Geschäftsbedingungen, zu einer Erhöhung der Sicherheit beitragen.

Hier können Quellen von Instituten, wie der „Arbeitsgruppe Identitätsschutz im Internet“ e.V. oder „Deutschland sicher im Netz“ e.V., aber auch von staatlichen Stellen wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) oder verschiedener Polizeibehörden, unterstützend hinzugezogen werden. Sie Informieren Privatpersonen und Unternehmen in Sicherheitsfragen und bieten Checklisten für mehr Sicherheit an, um so das Sicherheitsbewusstsein zu erhöhen. Diese Institutionen und ihre sinnvollen Empfehlungen sind den meisten Nutzern oft nicht hinreichend bekannt. Das umfassende Know-How dieser Institute sollte zudem schon während der Entwicklung von Online-Projekten einbezogen werden. So können Fehler vermieden, ein hoher Grad an Sicherheit bei gleichzeitiger Nutzerfreundlichkeit erreicht und damit Vertrauen der Nutzer gewonnen werden.

Sichere Passwörter

Die Angebote sollten nicht jedes gewünschte Passwort der Nutzer akzeptieren, sondern Regeln vorgeben und diese prüfen. Ein gutes Mittel, um die Erstellung eines sicheren Passworts nutzerfreundlich zu unterstützen, ist die Anzeige der Stärke des eingegebenen Passwortes und die aktive Unterstützung bei der Eingabe. So könnte beispielsweise angegeben werden, dass noch Sonderzeichen oder zusätzliche Klein- und Großbuchstaben fehlen, um das Passwort sicherer zu machen. Auch Tipps für sichere Passwörter können den Nutzern eine nützliche Hilfestellung sein (vgl. Kapitel 3.5.1). Nur so kann unerfahrenen Nutzern ein Hilfsmittel angeboten werden, um die Sicherheit des Benutzer-Accounts zu erhöhen. Dies hat sich mittlerweile auf sehr vielen Webangeboten wie z.B. von E-Mail-Providern oder in sozialen Netzwerken durchgesetzt. Hier müssen sich die Angebote der Politik anschließen. Eine Umsetzung sollte sich, aufgrund der vielen Beispiele im Netz, nicht besonders schwierig gestalten.

Verifikation der E-Mail

Alle Angebote schicken zur Verifikation der E-Mail Adresse nach der Registrierung einen Link an die Adresse, die der Nutzer angegeben hat, um ein Minimum an Verbindlichkeit zu erzeugen. Erst nach dem Anklicken des Links wird sein Nutzerkonto als „Aktiv“ gekennzeichnet und kann genutzt werden. Mit sogenannten „Wegwerf-E-Mail-Adressen“ wie `trash-mail.com` oder `twinmail.de` können Nutzer dieses System unterlaufen, indem sie eine begrenzt gültige Adresse anlegen und sich mit dieser anmelden. Daher sollten Angebote diese E-Mail Anbieter grundsätzlich blocken und eine Registrierung mit deren Adresse nicht erlauben.

Minimalitätsprinzip für Informationen

Es ist empfehlenswert, einem Nutzer nur die Informationen bereitzustellen, die er gerade benötigt. Zu viele davon können einem Angreifer wertvolle Hinweise liefern, die er für Angriffe nutzen kann. So gibt die Anmeldeinformation „Falsches Passwort eingegeben“ einem Angreifer zugleich den Hinweis „Eingegebener Benutzername ist richtig“. Besser wäre hier die Information „Benutzername oder Passwort wurden falsch eingegeben“. Auch bei der „Passwort vergessen“-Funktion sollte diese Art der Implementierung Verwendung finden. Wird der Nutzer aufgefordert, seinen Benutzernamen einzutragen lautet die Antwort meist: „Das Passwort wurde an die hinterlegte E-Mail Adresse geschickt“ oder „Der Benutzer existiert nicht, bitte überprüfen Sie Ihre Eingabe“. Hier wäre die bessere Umsetzung, wenn der Nutzer eine Information wie „Das Passwort wurde an die hinterlegte E-Mail Adresse verschickt, falls der eingegebene Nutzer existiert. Sollten Sie in Kürze keine E-Mail erhalten, so haben Sie eventuell einen falschen Nutzernamen eingegeben.“ bekommen würde. Zudem sollte eine Hilfeseite, die Informationen über Zusammenhänge von geschützten Anwendungen enthält, nur von angemeldeten Nutzern zugreifbar sein. Dabei sollte immer genau zwischen der Unterstützung des Nutzers und dem Schutz vor Angriffen abgewogen werden [Bundesamt für Sicherheit in der Informationstechnik, 2006].

Datenschutz

Die Datenschutzerklärung muss immer deutlich sein, da jede Webseite, die einen Teledienst darstellt, besonderen Transparenz- und Aufklärungspflichten gegenüber dem Nutzer unterliegt [Trautmann, 2005]. In der Regel erhebt eine Webseite schon bei dem ersten Besuch eines Nutzers personenbezogene Daten. So werden auf dem Server Logfiles erstellt, die die IP-Adressen, Browsertyp, verwendetes Betriebssystem, die vorhergehende Webseite und mehr erfassen. Hinzu kommt, dass viele Seiten automatisch Cookies setzen, bei denen es sich auch um personenbezogene Daten handelt. Auch bei der Nutzung der E-Partizipationswebseiten werden während der Registrierung mit Benutzername, Passwort und E-Mail Adresse persönliche Daten erfasst und abgespeichert. Dies führt dazu, dass in jedem Fall eine Datenschutzerklärung des Anbieters nötig ist, die den jeweiligen Bedürfnissen der Webseite angepasst sein sollte.

Die folgende Abbildung 21 zeigt ein anschauliches Beispiel für eine solche Datenschutzerklärung. Sie klärt den Nutzer über die Datenerhebung während der Nutzung auf und unterrichtet ihn, wie er Informationen über seine gespeicherten Daten einholen kann. In dem Beispiel ist die Aufklärung übersichtlich und die Sprache bleibt immer benutzerfreundlich und leicht verständlich.

Wir, die (Name und Anschrift der Anbieterin) nehmen den Schutz Ihrer persönlichen Daten sehr ernst und halten uns strikt an die Regeln der Datenschutzgesetze. Personenbezogene Daten werden auf dieser Webseite nur im technisch notwendigen Umfang erhoben. In keinem Fall werden die erhobenen Daten verkauft oder aus anderen Gründen an Dritte weitergegeben.

Die nachfolgende Erklärung gibt Ihnen einen Überblick darüber, wie wir diesen Schutz gewährleisten und welche Art von Daten zu welchem Zweck erhoben werden.

Datenverarbeitung auf dieser Internetseite

(Anbieterin) erhebt und speichert automatisch in ihren Server Log Files Informationen, die Ihr Browser an uns übermittelt. Dies sind:

- Browsertyp/ -version
- verwendetes Betriebssystem
- Referrer URL (die zuvor besuchte Seite)
- Hostname des zugreifenden Rechners (IP Adresse)
- Uhrzeit der Serveranfrage.

Diese Daten sind für (Anbieterin) nicht bestimmten Personen zuordenbar. Eine Zusammenführung dieser Daten mit anderen Datenquellen wird nicht vorgenommen, die Daten werden zudem nach einer statistischen Auswertung gelöscht.

Cookies

Die Internetseiten verwenden an mehreren Stellen so genannte Cookies. Sie dienen dazu, unser Angebot nutzerfreundlicher, effektiver und sicherer zu machen. Cookies sind kleine Textdateien, die auf Ihrem Rechner abgelegt werden und die Ihr Browser speichert. Die meisten der von uns verwendeten Cookies sind so genannte „Session-Cookies“. Sie werden nach Ende Ihres Besuchs automatisch gelöscht. Cookies richten auf Ihrem Rechner keinen Schaden an und enthalten keine Viren.

Newsletter

Wenn Sie den auf der Webseite angebotenen Newsletter empfangen möchten, benötigen wir von Ihnen eine valide Email-Adresse sowie Informationen, die uns die Überprüfung gestatten, dass Sie der Inhaber der angegebenen Email-Adresse sind bzw. deren Inhaber mit dem Empfang des Newsletters einverstanden ist. Weitere Daten werden nicht erhoben.

Ihre Einwilligung zur Speicherung der Daten, der Email-Adresse sowie deren Nutzung zum Versand des Newsletters können Sie jederzeit widerrufen.

Auskunftsrecht

Sie haben jederzeit das Recht auf Auskunft über die bezüglich Ihrer Person gespeicherten Daten, deren Herkunft und Empfänger sowie den Zweck der Speicherung. Auskunft über die gespeicherten Daten gibt der Datenschutzbeauftragte (der Anbieterin, als Email-Link ausführen).

Weitere Informationen

Ihr Vertrauen ist uns wichtig. Daher möchten wir Ihnen jederzeit Rede und Antwort bezüglich der Verarbeitung Ihrer personenbezogenen Daten stehen. Wenn Sie Fragen haben, die Ihnen diese Datenschutzerklärung nicht beantworten konnte oder wenn Sie zu einem Punkt vertiefte Informationen wünschen, wenden Sie sich bitte jederzeit an den Datenschutzbeauftragten (der Anbieterin, als Email-Link ausführen).

Abbildung 21. Beispiel für eine gute Datenschutzerklärung[27]

[27] Quelle: [Trautmann, 2005]

Verschiedenes

Schon während der Recherche ist aufgefallen, dass es in Deutschland keine einheitliche, benutzerfreundliche und übersichtliche Plattform gibt, die einen Bürger umfassend und aktuell über derzeitige E-Partizipationsangebote informiert. So sind zum Beispiel die Seiten `www.e-participation.net` und `www.islab.uom.gr/eP` sehr unübersichtlich gestaltet und enthalten viele veraltete Links. Dieser Umstand führt nicht dazu, dass sich das Vertrauen in öffentliche Online-Anwendungen weiter erhöht. Zudem ist die Gefahr groß, dass Bürger, die sich beteiligen wollen, die entsprechenden Angebote im Web nicht finden können. Da E-Partizipationsangebote ein sehr breites Spektrum von Bürgern ansprechen sollen, auch Bürger, die sich nicht sehr gut mit dem Internet auskennen, wie z.B. alte oder weniger gebildete Menschen, sollte hier ein einheitliches Portal geschaffen werden, dass benutzerfreundlich über E-Partizipationsanwendungen berichtet. Denkbar wäre eine partizipative Anwendung, die auf aktive Beteiligung der Nutzer baut und so zu einer größeren und aktuelleren Wissensbasis führen kann.

Wichtiges Akzeptanzkriterium für eine Webanwendung ist die Wahrung der Privatsphäre der Nutzer. Daher ist nicht nur aus Datenschutzgründen, sondern auch wegen der Akzeptanz einer solchen E-Government-Anwendung eine genaue Analyse der Notwendigkeit von persönlichen Daten vonnöten. Dennoch hat man teilweise den Eindruck, dass die Good-Practice Techniken aus der Privatwirtschaft nicht immer angenommen und umgesetzt werden. So haben sich bei den sozialen Netzwerken beispielsweise bereits einige Datenskandale negativ ausgewirkt. Solche Skandale im E-Government würden vermutlich zu einem größeren Image- und Vertrauensverlust führen. Für viele Probleme gibt es bereits erprobte und bewährte Lösungen, die aber auch genutzt werden müssen. Die bewährten Praktiken sollten angenommen und umgesetzt werden, die Verwaltung sollte bei dem Thema Sicherheit eine Vorreiterrolle einnehmen.

6.2 Ausblick auf zukünftige Technologien

Ein großes Problem der E-Partizipation ist die fehlende Möglichkeit der Bürger, sich im Netz rechtsverbindlich und benutzerfreundlich ausweisen und kommunizieren zu können. Dies erschwert beispielsweise die einfache und eindeutige Identifizierung und Authentifizierung der Nutzer im Web. Erst jetzt gibt es neue Technologien, die diese Lücke füllen können. Für die eindeutige Identifizierung im Netz wird der neue oder elektronische Personalausweis auf Bundesebene Ende 2010 eingeführt. Er ersetzt den bisherigen Personalausweis und verfügt über neue elektronische Funktionen. Einen etwas anderen Ansatz geht die Schweiz mit der SuisseID. Sie ersetzt nicht die Schweizer Identitätskarte, sondern wird ausschließlich als elektronischer Identitätsnachweis im Internet eingesetzt. Im Rahmen der authentischen Kommunikation werden demnächst der E-Postbrief der Deutschen Post sowie die De-Mail in Deutschland eingeführt. Sie ermöglichen eine sichere Kommunikation und erlauben den rechtsverbindlichen Versand von hoheitlichen Dokumenten. Ein weiterer Bereich der zukünftigen Technologien stellen die mobilen Applikationen dar, die in der Privatwirtschaft immer mehr an Bedeutung gewinnen. Daher wird diese Technologie in Zukunft auch im Bereich des E-Government eine zunehmend wichtigere Rolle erhalten.

6.2.1 Elektronische Ausweise

Im Folgenden wird der neue oder elektronische Personalausweis ausführlich mit seinen Funktionen vorgestellt. Anschließend wird der Schweizer Ansatz (SuisseID) kurz erläutert.

Elektronischer Personalausweis in Deutschland

Bürger verwenden Ihren Personalausweis sowohl zum Identitätsnachweis gegenüber Behörden aber auch im privaten Umfeld beispielsweise zum Altersnachweis oder für den Abschluss von Verträgen. Mittlerweile werden immer mehr Lebensbereiche in das Internet verlagert: Es wird sich online informiert, online eingekauft und Behördengänge online absolviert. Daher passt sich der neue oder elektronische Personalausweis diesem Trend an, indem er den herkömmlichen Ausweis mit elektronischen Funktionen vereint. Der elektronische Personalausweis wird am 01. November 2010 eingeführt und ist Bestandteil der E-Government-Strategie des Bundes. Er soll im Bereich der elektronischen Kommunikation eine Verbesserung der Identifikationssicherheit herbeiführen und einen wesentlichen Beitrag zur Modernisierung der Verwaltung leisten [Bundesministerium des Innern, 2008].

Abbildung 22. Der elektronische Personalausweis[28]

Der neue Personalausweis soll den bisherigen Bereich der Identifizierung von Mensch zu Mensch weiterhin abdecken und zudem eine Identifizierung in der Online-Welt ermöglichen. Dazu wird er mit zusätzlichen Funktionen ausgestattet: Der biometriegestützten Identitätsfunktion, dem elektronischen Identitätsnachweis und der elektronischen Signatur. Auf dem neuen Ausweis bleibt die Funktion des Sichtausweises, mit dem Lichtbild und den aufgedruckten Angaben, erhalten (siehe Abbildung 22). Neu hinzu kommt der Internetausweis, der in elektronischer Form Name, Anschrift, Geburtstag, Geburtsort und Ablaufdatum enthält. Optional kann der Ausweis um die biometriegestützte Identitätsfunktion, mit zwei digitalen Fingerabdrücken, erweitert werden, die dabei ausschließlich dem hoheitlichen Bereich (z.B. Polizei und Grenzschutz) vorbehalten ist und nicht für die

[28] Quelle: [Fraunhofer-Institut für Offene Kommunikationssysteme, 2010]

Online-Authentifizierung genutzt wird. Die elektronische Signatur, die als Zertifikat ebenfalls optional auf den Ausweis geladen werden kann, dient als elektronische Unterschrift. Hiermit können rechtssichere und medienbruchfreie Anträge, Bescheide und Verträge unterzeichnet werden, bei denen normalerweise eine eigenhändige Unterschrift erforderlich wäre. Die elektronische Signatur ist kein fester Bestandteil des neuen Ausweises.

Der elektronische Personalausweis ist mit einer eID-Funktion ausgestattet, mit dem Prozesse wie ein Login, eine Adressverifikation oder ein Altersnachweis realisiert werden können. Sicherheit wird durch zwei Mechanismen gewährt. Zum einen dürfen nur staatlich geprüfte Anbieter von Dienstleistungen Daten, die auf den konkreten Geschäftszweck beschränkt sind, von dem Personalausweis abfragen. Zum anderen muss sich der Dienstanbieter seinerseits vor dem Identifikationsprozess gegenüber dem Nutzer ausweisen. Dieser hat, durch ein auf Berechtigungszertifikaten basierendes Zugriffssystem, stets die volle Kontrolle darüber, welche seiner persönlichen Daten an den Anbieter gesendet werden dürfen. Der Nutzer kann die zu übermittelnden Daten selbst einschränken und nur solche freigeben, die für den jeweiligen Zweck notwendig sind. So kann er beispielweise ausschließlich den Name oder das Geburtsdatum für einen Dienst freigeben. Eine Transaktion muss anschließend mit einer sechsstelligen PIN vom Nutzer explizit bestätigt werden [Beauftragte der Bundesregierung für Informationstechnik, 2010]. Die Bundesregierung vergibt die Zertifikate, die für die für die eID-Funktionalität von Anwendungen nötig sind, an die Dienstanbieter und kann diese auch wiederrufen. Dabei wird nur ein Zugang zu solchen Daten gewährt, die für das Erbringen der jeweiligen Dienstleistung unbedingt notwendig sind. [Kubicek & Noack, 2010].

Wer den elektronischen Personalausweis im Internet nutzen möchte, braucht einen geeigneten Kartenleser und die Software „Bürgerclient“, die für die Kommunikation zwischen Kartenleser, Chipkarte und Dienstanbieter zuständig ist. Die Kommunikation erfolgt über einen RFID-Chip, der sich auf der Karte befindet und kontaktlos über das Lesegerät ausgelesen werden kann [Kubicek & Noack, 2010]. Bevor ein Datenaustausch zwischen Dienst und Ausweis stattfinden kann, müssen sich die Kommunikationspartner gegenseitig identifizieren. So wissen beide Seiten, mit wem sie sich verständigen [Beauftragte der Bundesregierung für Informationstechnik, 2009].

Nach einer Umfrage des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom) von Anfang 2010 würden 14 Millionen Deutsche, was rund 30% der Bevölkerung entspricht, ihren alten Personalausweis vor dessen Ablauf in einen neuen umtauschen. Die Zustimmung und Ablehnung verteilen sich in etwa gleich: 46 % der Bevölkerung begrüßen die Einführung, 45 % lehnen diese ab. Bei den Internetnutzern ist die Zahl der Befürworter noch größer, hier sind 52 % für und 32 % gegen den neuen Ausweis [Bitkom, 2010]. Diese Zahlen zeigen aber auch, dass es noch einige Vorbehalte der Bevölkerung gegen den elektronischen Personalausweis gibt, beispielsweise in den Bevölkerungsteilen, die nicht sehr technikaffin sind, wie bei den Senioren oder bei Bürgern, die den Schutz ihrer personenbezogenen Daten durch die neue Technik gefährdet sehen.

Um die Akzeptanz zu erhöhen und Möglichkeiten des neuen Personalausweises zu erkennen, findet vom 1. Oktober 2009 bis 30. Oktober 2010 ein großangelegter Anwendungstest unter Leitung des „Kompetenzzentrums elektronischer Personalausweis“ statt. Der Test soll die Praxistauglichkeit,

Handhabbarkeit und Akzeptanz untersuchen und die Einsatzmöglichkeiten testen. Er ist in zwei Abschnitte gegliedert: Zunächst nahmen 29 Unternehmen, Behörden und Konsortien als Dienstanbieter an einem zentral koordinierten Anwendungstest teil. Diese entwickelten in Abstimmung mit dem BMI Prozesse zur Integration des Ausweises in verschiedene Dienste und Anwendungen. In einem zweiten Abschnitt ab Februar 2010 können mehr als 150 Organisationen, die eigene Dienste anbieten möchten, teilnehmen und das System ausgiebig testen [Fraunhofer-Institut für Offene Kommunikationssysteme, 2010].

Die möglichen Einsatzszenarien des neuen Personalausweises im Bereich des E-Commerce liegen beim Handel (z.B. Alterskontrollen oder Onlineverkauf), bei Banken (z.B. Online Kontoeröffnung oder Onlinebanking) oder bei Versicherungen (z.B. Online-Antrag oder Online-Schadensmeldung). Im Bereich des E-Government könnte der Personalausweis beispielsweise dabei helfen, Anträge auf Sozialleistungen online abzuwickeln, sich bei einem Umzug rechtsverbindlich umzumelden oder die Einkommensteuererklärung elektronisch unterschrieben einzureichen. Zudem kann der Ausweis bei allen Online-Anwendungen ein einheitliches Single-Sign-On umsetzen und die Registrierung unterstützen. Der elektronische Personalausweis stellt für den Bereich der E-Partizipation eine einheitliche Möglichkeit dar, den Benutzer eindeutig zu identifizieren und Rechte individuell zu vergeben. So können beispielsweise Bürgerhaushalte ihre Angebote ausschließlich für Bürger ihrer Stadt freigeben.

Allerdings kann dies zu Hemmnissen für die Nutzer führen, die diese Angebote nur unter einem Pseudonym nutzen und ihre wahre Identität nicht preisgeben möchten. Daher wäre es vorstellbar eine unabhängige Behörde einzurichten, die die persönlichen Daten aufbewahrt und gleichzeitig für z.B. einen Bürgerhaushalt ein Pseudonym generiert, unter dem sich der Bürger anmelden kann. Die Stadt und andere Teilnehmer erfahren nur das Pseudonym, können den Bürger, der dahinter steht, aber nicht identifizieren. Lediglich zur Strafverfolgung kann die Behörde die Herausgabe der Identität verlangen. Zusätzlich könnte eine Stadt noch den Wohnort anfordern, wenn sie für eine Beteiligung nur eigene Bürger zulassen will [Preuss, 2009]. Diese Vorgehensweise kann die Akzeptanz der Bürger fördern und hat auch einen großen Vorteil in Sicherheitsfragen. Da das Pseudonym und die zugehörige Identität an verschiedenen Stellen aufbewahrt werden, müsste ein Angreifer in beide Stellen eindringen, um eine Verbindung herzustellen.

Die Entscheidung, eine Identifizierung über den elektronischen Personalausweis durchzuführen, sollte immer in Abhängigkeit vom Sicherheitslevel eines Angebots getroffen werden. Es macht vermutlich wenig Sinn, die Nutzung eines Personalausweises vorzuschreiben, wenn nur ein Pseudonym, eine E-Mail Adresse und ein Passwort für die Nutzung des Angebots notwendig sind. Daher sollte man zunächst die Funktionalität des elektronischen Personalausweises ausschließlich zusätzlich anbieten, um nicht unnötig die Hürden für eine Teilnahme zu erhöhen und so Bürger abzuschrecken. Für die Verwendung wird zusätzliche Hard- und Software benötigt, wie beispielsweise ein Kartenlesegerät, um den elektronischen Personalausweis auszulesen und die Software Bürgerclient, die die Verbindung zwischen Personalausweis, heimischem Rechner und Server herstellt. Dadurch sind die Hürden hier besonders hoch.

SuisseID

Die Schweiz geht einen etwas anderen Weg der eindeutigen Identifizierung im Internet. Hier gibt es seit Mai 2010 die SuisseID, einen elektronischen Identitätsnachweis, der nicht die Schweizer Identitätskarte ersetzt, sondern ausschließlich als Identitätsnachweis im Internet dient. Sie enthält neben dem elektronischen Identitätsnachweis eine qualifizierte elektronische Signatur und einen elektronischen Funktionsnachweis. Damit kann sich ein Kunde in einem Online-Angebot sicher authentisieren, ein Dokument rechtsverbindlich unterschreiben und im Funktionsregister des Ausweises Nachweise wie Handlungsvollmachten oder Verbandszugehörigkeiten hinterlegen. Mit dem System ist es zusätzlich möglich, E-Mails sicher und nachweisbar im Internet zu versenden und sich in verschiedenen Systemen im Single-Sign-On Verfahren anzumelden.

Die SuisseID enthält auf der Karte als Pflichtangaben Vorname, Nachname, E-Mail Adresse und eine spezielle SuisseID-Nummer und ist als Chipkarte oder USB-Stick erhältlich. Daher wird entweder ein Lesegerät oder ein USB-Port benötigt, um die Daten auszulesen. Auf die im Chip gespeicherten Daten kann nur zugegriffen werden, wenn der Inhaber des elektronischen Ausweises dies ausdrücklich erlaubt. Der Identifikationsnachweis kann beispielsweise in der Kommunikation mit Behörden genutzt werden, wenn offizielle Dokumente über das Internet „unterschrieben“ werden sollen oder man einen rechtverbindlichen Vertrag, z.B. einen Mobilfunkvertrag, über das Internet abschließen will.

6.2.2 E-Postbrief und De-Mail

E-Mails sind sehr unsicher, da sie über keinerlei Sicherheitsmechanismen in Bezug auf den Transport und die Identifizierung der Kommunikationspartner verfügen. Sie können mit wenig Aufwand abgefangen und gelesen werden, die Kommunikationspartner können sich nie sicher sein, mit wem sie gerade tatsächlich kommunizieren. Daher ist die klassische E-Mail zu unsicher für rechtsverbindliche Dokumente, wie etwa Verträge. Ein neuer Ansatz für eine sichere Kommunikation im Internet sind der E-Postbrief der Deutschen Post sowie die De-Mail. Sie sollen die geschäftliche oder behördliche Kommunikation, die bislang den Postweg erforderte, im Internet mit der gleichen Sicherheitsanforderung umsetzen und die Übermittlung von Nachrichten sicher und rechtsverbindlich machen. Da sich der Einsatz von Verschlüsselungsverfahren innerhalb der E-Mail-Kommunikation nicht etabliert hat und nur sehr geringe Akzeptanz findet, entstand die Notwendigkeit dieser Dienste. Lediglich fünf Prozent des gesamten E-Mail Verkehrs findet heute verschlüsselt statt [Beauftragte der Bundesregierung für Informationstechnik, 2010].

E-Postbrief

Die Deutsche Post versucht mit dem E-Postbrief einen Dienst zu etablieren, der ähnlich wie eine herkömmliche E-Mail funktioniert, aber gleichzeitig so „sicher und verbindlich wie ein Brief der Deutschen Post“ sein soll. Die Post verwendet zum Verschlüsseln der Nachrichten das Verschlüsselungsverfahren TLS (vgl. Kapitel 3.4.4). Zudem wird jeder E-Postbrief mit einer elektronischen Signatur versehen, die eine Integritätsprüfung der erhaltenen Daten ermöglicht. Mit diesen Maß-

nahmen wird die Integrität (Manipulation der Daten während des Transports) und Vertraulichkeit (Abhören der Daten während des Transports) der Nachrichten sichergestellt. Durch eine eindeutige Identifizierung der Nutzer wird die Authentizität (Echtheit) der Kommunikationspartner und die Rechtssicherheit der Kommunikation gewährleistet. Dazu muss sich ein Nutzer einmalig in einer Postfiliale mit dem Post-Ident-Verfahren ausweisen. Für die Registrierung an dem Dienst und die Ausführung bestimmter Aktionen wird ein HandyTAN-Verfahren genutzt. Dabei bekommt der Nutzer eine einmalige Transaktionsnummer auf das Handy geschickt, die er anschließend, zusammen mit seinem persönlichen Passwort, eingeben muss. So wird eine Identifikation mittels Wissen (persönliches Passwort) und Besitz (persönliches Handy) vorgenommen, ähnlich dem mTAN-Verfahren von Banken.

Um sich für den E-Postbrief registrieren zu können, muss ein Nutzer seinen Vor- und Nachnamen, Geburtstag und -ort, Adresse sowie Handynummer angeben. Die E-Postbrief-Adresse hat das Format `Vorname.Nachname@epost.de`. Wenn sich mehrere Personen mit demselben Namen registrieren, wird eine fortlaufende Nummer hinter den Nachnamen angefügt. Registrierte und verifizierte Nutzer können in einem Adressverzeichnis des E-Postbrief Portals gefunden werden. Soll ein Empfänger angeschrieben werden, der keine E-Postbriefadresse besitzt, so kann dieser Brief an eine Postanschrift adressiert werden und wird ausgedruckt in klassischer Briefform zugestellt.

Es gibt einige Kritik an dem E-Postbrief. So ist die Anmeldeprozedur sehr umständlich und kompliziert, die E-Briefe, die ausgedruckt werden, können theoretisch von Postmitarbeitern gelesen werden. Außerdem werden die E-Briefe nur vom Absender zum Postserver und vom Postserver zum Empfänger verschlüsselt. Auf dem Server wird die Nachricht kurz entschlüsselt, wodurch hier eine Sicherheitslücke im System entsteht. Wer eine End-zu-End Verschlüsselung nutzen will, muss zusätzlich ein persönliches Zertifikat beantragen. Diese Zertifikatnutzung sollte das Standardverfahren darstellen, um als zuverlässiger Dienst zu gelten. Negativ gesehen wird ebenso der hohe Preis für den Service: Ein E-Postbrief kostet mit 55 Cent genauso viel wie ein Papierbrief [Stiftung Warentest, 2010]. Auch die allgemeinen Geschäftsbedingungen (AGB) stehen in der Kritik. So wird ein Nutzer in den AGBs dazu verpflichtet, seine E-Mails täglich mindestens einmal aufzurufen, auch im Urlaub. Zudem behält sich die Post vor, die E-Postbriefadresse ihrer Nutzer an interessierte Geschäftskunden weiterzugeben, die der Post Name und Postanschrift des Empfängers mitteilen. Obwohl die Deutsche Post damit wirbt, dass die E-Postbriefe so sicher und verbindlich wie herkömmliche Briefe sein sollen, teilt sie in den AGBs unter VI.9.3 dennoch mit, dass sie als neuer Telekommunikationsanbieter den „gesetzlichen Vorgaben zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung“ zur unverschlüsselten Herausgabe von Nachrichten an die Verfassungsschutzbehörden verpflichtet ist. Damit wird kein vergleichbares Sicherheitsniveau zu einem klassischen Brief erreicht. Es gibt wesentlich mehr Überwachungsmöglichkeiten der Strafverfolgungsbehörden als bei dem Papierbrief, der unter das Postgeheimnis fällt. Außerdem werden elektronische Briefe, die von einem Nutzer gelöscht werden, zunächst nur gesperrt und mit einer zeitlichen Verzögerung entfernt, um „versehentlichen Löschungen oder evtl. vorsätzlichen Schädigungen vorzubeugen“ (IV.2.5). Damit wird einem User untersagt, seine Briefe endgültig zu löschen, er ist somit abhängig von dem Betreiber, der die Daten löschen muss [Deutsche Post, 2010] [Gutjahr, 2010].

De-Mail

Auch De-Mail wirbt damit, „so einfach wie E-Mail, so sicher wie die Papierpost“ zu sein. De-Mail ist dabei kein Dienst von einem einzelnen Anbieter, er kann von verschiedenen Unternehmen angeboten werden. Diese benötigen die BSI-Zertifikate für IT-Sicherheit, Interoperabilität und Funktionalität sowie einen Datenschutznachweis von einer unabhängigen Prüfstelle. Zu den Unternehmen, die De-Mail anbieten werden, gehören beispielweise GMX, Web.de und die Deutsche Telekom. Der Dienst soll 2011 gestartet werden.

De-Mail soll es Bürgerinnen und Bürgern, Wirtschaft und Verwaltung erlauben, zuverlässig und vertraulich elektronisch zu kommunizieren. Die Sicherheit basiert auf gegenseitiger Authentisierung und verschlüsselter Kommunikation. De-Mail Konten können von natürlichen wie auch juristischen Personen (z.B. Firmen, Organisationen oder Verwaltungen) eröffnet werden. Dazu müssen sich die Nutzer einmalig zuverlässig identifizieren lassen, beispielweise mit dem Post-Ident-Verfahren oder dem künftigen elektronischen Personalausweis. Natürliche Personen müssen persönliche Daten wie ihren Vor- und Nachnamen, Adresse und Geburtsdatum angeben. Bei juristischen Personen werden Daten zu der juristischen Person selbst und zu persönlichen Daten von vertragsberechtigten Personen abgefragt.

Der De-Mail Dienst bietet dem Nutzer zwei Versandarten an: Die De-Mail selbst schützt die Vertraulichkeit und Integrität der Nachrichteninhalte und der Metadaten. Bei dem De-Mail-Einschreiben erhält der Absender eine qualifiziert signierte Bestätigung, wann er die Nachricht verschickt hat und wann sie im Postfach des Empfängers angekommen ist.

Eine De-Mail Adresse setzt sich aus `Vorname.Nachname@Anbieter.de-mail.de` zusammen. Gibt es bei einem Anbieter mehrere Personen mit dem gleichen Namen, so wird eine fortlaufende Nummer hinter den Nachnamen gesetzt. Jedes De-Mail Konto kann aus mehreren Adressen bestehen. So kann ein Nutzer weitere Adressen mit frei wählbaren Pseudonymen anlegen. Diesen Adressen wird zur Kennzeichnung das Präfix „pn_“ vorangestellt. Juristische Personen bekommen eine eigene Domain in der Form `@Firmenname.de-mail.de` zugewiesen. Sie können den Teil vor dem @ dann frei vergeben, z.B. nach Organisationseinheiten oder Namen von Mitarbeitern.

De-Mail bietet neben den elektronischen Nachrichten zusätzlich zwei weitere Dienste an. Mit De-Ident ist es möglich, sich im Internet einfach zu identifizieren und sich damit z.B. in Online-Shops zu registrieren oder sein Alter zu verifizieren. Um die Korrektheit zu bestätigen, signiert der De-Mail-Provider die Daten mit einer qualifizierten Signatur, die der höchsten Sicherheitsstufe im Signaturgesetz entspricht. Der Dienst De-Safe soll elektronische Dokumente langfristig speichern und einen Schutz vor Verlust oder Manipulation bieten. Ein Kunde kann ein Dokument an den Dienst übergeben, das zum Schutz direkt verschlüsselt gespeichert wird.

Es werden zwei Authentifizierungsniveaus unterstützt. Das Niveau „Normal“ erfordert zur Identifizierung nur Wissen und entspricht damit einer Anmeldung mit Benutzername/Passwort. „Hoch“ fordert Wissen und Besitz, was bedeutet, dass neben dem Benutzernamen/Passwort zusätzlich entweder ein Mobiltelefon-basiertes Verfahren, eine Chipkarte oder der zukünftige elektronische Personalausweis

abgefragt wird. So wird sichergestellt, dass ein Angreifer zwar das Passwort abfangen kann, daneben aber noch greifbare Gegenstände des Nutzers benötigt. In diesem Zusammenhang stehen dem Absender vor dem Versand der Nachricht zwei optionale Auswahlmöglichkeiten zur Verfügung. Wenn ein Absender eine Nachricht als „persönlich“ kennzeichnet, so muss das Authentifizierungsniveau des Empfängers mindestens „hoch“ sein, um die Nachricht lesen zu können. Mit der Option „Absender-Bestätigt“ weist der Empfänger den Erhalt einer Nachricht mittels qualifizierter Signatur nach. Dieser muss sich dazu mit einem hohen Authentifizierungsniveau anmelden, da so die Bestätigungsnachricht eine höhere Beweiskraft bekommt.

Zum Versand der Nachrichten über einen Webbrowser wird der Nachrichtentext mittels HTTPS übertragen. Wird eine Nachricht über einen E-Mail-Client versendet, so wird die Nachricht auch hier ausschließlich TLS-Verschlüsselt über SMTP versendet [Beauftragte der Bundesregierung für Informationstechnik, 2010].

Auch De-Mail steht in der Kritik. So werden auch bei dem Dienst, wie bei dem E-Postbrief, die Nachrichten nach dem derzeitigen Stand auf dem Server kurz entschlüsselt und danach direkt wieder verschlüsselt. Wird eine De-Mail an einen anderen Anbieter verschickt, so muss sie sogar zweimal entschlüsselt werden. Hier ist es theoretisch möglich, die Nachrichten zu kopieren oder zu verändern, wenn es einem Angreifer gelingen sollte, einen De-Mail Server zu hacken [Schlandt, 2010]. Es stellt sich die Frage, warum Unternehmen über diesen Dienst vertrauliche Informationen austauschen sollten, die von den De-Mail-Providern (zum Beispiel der Deutschen Telekom) eingesehen werden können. Zudem stellt De-Mail eine Insellösung für Deutschland dar. Es gibt in der EU keine Pläne, ein vergleichbares E-Mail System einheitlich in allen Mitgliedsstaaten einzuführen. Auch die Zustellung steht in der Kritik, da laut dem Gesetzentwurf für die De-Mail eine Nachricht als zugestellt gilt, sobald sie im Postfach des Empfängers eingetroffen ist. Damit beginnen ab diesem Zeitpunkt auch die Rechtsfristen an zu verstreichen, wenn beispielsweise Behörden elektronische Briefe versenden. Bürger sind dadurch gezwungen, ihr Postfach regelmäßig zu kontrollieren. Experten fordern ein Verfahren, dass Briefe erst dann als zugestellt gelten, wenn sie aufgerufen wurden [Kafka, 2010].

Der Deutsche Anwaltsverein (DAV) bezweifelt den Bedarf eines solchen Dienstes, da es bereits heute eine Infrastruktur der elektronischen Signatur und bewährte Verschlüsselungsverfahren gibt. Ein neues System sollte, wenn es denn eingeführt wird, nur im öffentlichen Bereich eingesetzt werden, da der Einsatz in der Wirtschaft zu einer umfangreichen Datenspeicherung der Kommunikation führen würde. Auch die geplante Pseudonymisierung sieht der DAV kritisch, da dies im klaren Widerspruch zu einer eindeutigen Identifizierung der Nutzer steht. Zudem sollten die Daten der Dienste nicht für Strafverfolgungszwecke zur Verfügung stehen, da dies das Persönlichkeitsrecht der BürgerInnen beeinträchtige. Die De-Mail-Dienste dürfen die anonyme Kommunikation in keiner Weise beeinträchtigen, da dies ein „wichtiger Grundwert der Meinungs- und Informationsfreiheit“ darstellt. Ein weiterer Kritikpunkt ist das Wahlrecht von juristischen Personen, auch Zustellungen über den De-Mail-Dienst zu versenden. Hier fehlt die Hinweis- oder Warnwirkung von amtlichen Umschlägen der Briefpost. Löscht ein Nutzer die Nachricht, wenn er beispielsweise denkt, dass es sich um Spam handele, ergeben sich erhebliche Nachteile für ihn. Der Bürger muss zukünftig immer

die Wahl haben, ob er Dokumente in elektronischer oder Papierform zugestellt bekommen möchte und nicht dazu verpflichtet werden, den De-Mail-Dienst zu nutzen [Deutscher Anwaltverein, 2010].

6.2.3 Mobile Applikationen

Die Einsatzmöglichkeiten von Web 2.0 Anwendungen sind immer weniger an einen heimischen Internetzugang gekoppelt, die mobilen Einsatzmöglichkeiten sind weiter auf dem Vormarsch. Gerade durch den Hype des iPhones und der Android-basierten Telefone wird dieser Markt immer attraktiver für Anwendungen wie soziale Netzwerke, E-Commerce-Seiten oder Video-Communities. Der große Unterschied von mobilen zu „normalen" Anwendungen liegt in einem verkleinerten Bildschirm, einer meist langsameren Internetgeschwindigkeit und der Beschränktheit bei der Nutzung durch kleinere Tastaturen und Touch-Displays.

Der Einsatz mobiler Prozesse eröffnet Behörden die Möglichkeit, Geschäftsprozesse effektiver und effizienter zu gestalten und den Multi-Kanalzugang mit dieser Zugangsmöglichkeit weiter auszubauen. Das sogenannte M-Government stellt Behörden vor die Aufgabe, die Daten der Behörde sowie der Nutzer zu schützen. Hier ist das Sicherheitsrisiko etwas anders verteilt als bei normalen Webanwendungen, beispielweise durch eine leichte Ausspähbarkeit bei Unachtsamkeiten im mobilen Einsatz, ein erhöhtes Verlustrisiko der Endgeräte oder Probleme im Zusammenhang mit der Bluetooth-Nutzung. Zudem sind Virenscanner und regelmäßige Softwareupdates noch nicht bei allen Smartphones zu finden. Daher geht im mobilen Bereich in nächster Zeit eine immer größer werdende Gefahr von Viren und Schwachstellen in der Software aus. So wurden bereits Programme entdeckt, die sich als Spiele-Applikation ausgeben, in Wirklichkeit aber im Hintergrund teure Mehrwert-SMS verschicken [Bundeskriminalamt, 2010].

In dem Bereich des M-Government, der bislang noch keine größere Beachtung gefunden hat, sind noch sehr große Wachstumsmöglichkeiten vorhanden. Vor dem, was die Privatwirtschaft bisher vorexerziert, wird sich die öffentliche Verwaltung nicht verschließen können, um neue Nutzerkreise zu gewinnen. Allerdings sind hier ganz spezielle Sicherheitsaspekte zu beachten, die aufbauend auf der bisherigen Sicherheit von Webanwendungen noch einiges mehr umfassen.

6.2.4 Zusammenfassung

Wenn man zukünftig das Level der Beteiligung ausbauen und auf eine höhere Partizipationsstufe wie eCollaborating oder eEmpowering treten will, in denen der Bürger mehr mitbestimmen und politische Entscheidungen aktiv beeinflussen kann, wird es irgendwann zwingend notwendig, dass der Nutzer eindeutig identifiziert werden kann. Bei den derzeitigen E-Partizipationsangeboten ist dies nicht überall unbedingt erforderlich, da sich die politischen Akteure bislang auf eine Durchschnittsmeinung der Bürger stützen. Die Entscheidung liegt immer bei der Politik, die Rechenschaft für ihr Handeln ablegen muss. Wenn man einzelne Bürger oder Bürgergruppen autorisieren will, in bestimmten Bereichen aktiv mitzuwirken und politische Prozesse zu beeinflussen, ist es absolut wichtig, diese Bürger eindeutig erkennen zu können. Auch der Schutz vor einem möglichen Identitätsdiebstahl wird aufgrund der größeren Macht, die in dem Moment an die Bürger übergeht,

wichtiger. Nicht zuletzt, weil dadurch auch der Anreiz größer wird, diese Angebote anzugreifen oder auszuspionieren. Deshalb werden die Sicherheitsanforderungen in diesem Bereich in Zukunft noch wesentlich höher als bislang. Der elektronische Ausweis, der E-Postbrief sowie die De-Mail könnten mittelfristig die zentralen Themen für Sicherheitsfragen werden.

Der neue elektronische Personalausweis hat das Potential, die Sicherheit im Online-Umfeld zu erhöhen. Durch seine Funktion des elektronischen Identitätsnachweises können sich Bürger, ähnlich der Legitimation mittels Lichtbilddokument, im Internet ausweisen. Allerdings muss immer zwischen den Stärken und Schwächen solcher Techniken abgewogen werden. Für E-Partizipationsangebote mit einem niedrigen oder mittleren Sicherheitslevel macht der Ausweis keinen Sinn, da er eher abschreckend wirkt und die schon geringe Beteiligung noch weiter blockieren könnte. Angebote, die eine sehr hohe Sicherheit erfordern, können mit dem neuen Personalausweis überhaupt erst realisiert werden, da bislang noch kein allgemein akzeptiertes System für eine einheitliche und sichere Identifizierung und Authentifizierung auf Webseiten existiert. Zudem ist es möglich, sich mit einem einheitlichen Single-Sign-On an verschiedenen Plattformen anzumelden. Vergleichbar wäre dies mit den Angeboten von Google, bei denen man sich einmal anmeldet und anschließend verschiedene Tools mit nur einem Konto nutzen kann, wie z.B. YouTube, Picasa, Google Docs, Google Kalender oder Google Mail. Allerdings stellt sich hier -wie auch bei Google- wieder die Frage des Datenschutzes und ob man Informationen aus verschiedenen Quellen einem Anbieter zentral zur Verfügung stellen will.

Für eine sichere und rechtsverbindliche Kommunikation ist ein einheitliches und von allen Akteuren akzeptiertes System notwendig. Es wird dringend eine echte digitale Alternative zum Papierbrief benötigt. Trotz aller Bedenken können der E-Postbrief und De-Mail wichtige zukünftige Bausteine für Integrität, Vertraulichkeit und Authentizität elektronischer Kommunikation werden und Deutschland weltweit zum Vorreiter beim sicheren Mail-Verkehr zu positionieren. Gegenüber den bisherigen E-Mails bedeutet der E-Postbrief und De-Mail einen enormen Vorsprung in puncto Sicherheit. Derzeit sind nur diese Dienste in der Lage, die Sicherheit der Kommunikation flächendeckend zu erzielen. Zwar nutzen schon heute Bürger die Möglichkeit, sich über digitale Signaturen eindeutig zu identifizieren und den E-Mail Verkehr mittels Verschlüsselungsverfahren wie PGP sicherer zu machen, diese Verfahren benötigen aber alle ein größeres technisches Verständnis der Nutzer und erfordern einen erhöhten Aufwand in der Umsetzung [Beauftragte der Bundesregierung für Informationstechnik, 2010].

7. Fazit und Ausblick

Im theoretischen Teil der Arbeit wurden zunächst in Kapitel 2 die Grundlagen der elektronischen Partizipation gelegt. Hier mussten wichtige Partizipationsformen ausgewählt werden, die die Basis der Sicherheitsanalyse darstellen. Um sich zunächst einen Überblick über den derzeitigen Stand von E-Partizipationsanwendungen in Deutschland zu verschaffen, halfen Portale wie das „European eParticipation Portal“ (www.islab.uom.gr/eP), www.e-participation.net oder www.buergerhaushalt.org, die Informationen und weiterführende Links zu dem Thema beinhalten. Anschließend wurden die zentrale Anwendungen für diese Arbeit nach verschiedenen Gesichtspunkten (z.B. Anzahl der Nutzer, Alter des Angebots) ausgewählt. Hierbei wurde versucht, einen möglichst großen Querschnitt der zurzeit vorhandenen E-Partizipationsanwendungen abzudecken. In Kapitel 3 wurde das komplexe Thema der Sicherheit behandelt. Es wurden Angriffsformen ausgewählt, die besondere Relevanz in Bezug auf E-Partizipationsanwendungen haben und theoretische Konzepte behandelt, die untersuchten, wie die Sicherheit im Internet erhöht werden kann.

Der empirische Teil der Arbeit begann mit Kapitel 4, in dem zunächst die theoretischen Kapitel 2 und 3 zusammengeführt und die möglichen Angriffsszenarien, die für die zu untersuchenden E-Partizipationsanwendungen von Bedeutung sind, erläutert wurden. Ziel des Kapitels war es, die wichtigsten Angriffsformen herauszuarbeiten. Auf Basis dieser Angriffsformen wurde ein Analyse-Framework erstellt, das auf alle Plattformen anwendbar ist und verschiedene Sicherheitsaspekte aus den Bereichen Datenschutz, Registrierung, Identitätsmanagement und sichere elektronische Kommunikation umfasst. Mit dem Framework stand ein Werkzeug zur Verfügung, mit dessen Hilfe die E-Partizipationsanwendungen nach einheitlichen sicherheits- und datenschutzrelevanten Aspekten untersucht werden konnten. Mit Hilfe der gewonnenen Daten wurden den Anwendungen anschließend Sicherheitslevels zugeordnet, die verdeutlichen, welche Anwendungen besonders schützenswert sind. Hierbei ist anzumerken, dass diese Zuordnungen zwar auf den Untersuchungsergebnissen beruhen, aber dennoch subjektiv sind.

Eine Auswertung der Untersuchungsergebnisse, die zu Empfehlungen für Betreiber von E-Partizipationsanwendungen führte, wurde in Kapitel 6 vorgenommen. Zudem wurden wichtige zukünftige Technologien aufgegriffen, die nach der Meinung des Autors eine zentrale Rolle der sicheren Nutzung in Zukunft spielen werden.

Die Arbeit zeigt, dass das Sicherheitsniveau der untersuchten E-Partizipationsanwendungen sehr unterschiedlich ist. Einige der Anwendungen verfügen über ein sehr hohes Sicherheitslevel, bei anderen gibt es noch einige Beanstandungen, die behoben werden sollten. Gerade der Datenschutz wurde insgesamt recht gut umgesetzt, eine anonyme oder pseudonyme Nutzung ist fast durchgängig möglich und die Zweckbindung der Daten ist vorhanden. Allerdings findet sich kein Angebot, das alle untersuchten Sicherheitsaspekte zufriedenstellend umgesetzt hat. So verschlüsseln beispielsweise einige Angebote die Kommunikation mit den Nutzern nicht, wodurch Passwörter im Klartext im Internet übertragen werden. Zudem nutzt keines der Angebote eine einheitliche Single-Sign-On

Lösung und es wird von den meisten Angeboten nicht überprüft, wer die Nutzer sind, die sich beteiligen.

Von den untersuchten Anwendungen stellten das Angebot my.FDP und die E-Petitionen das beste Gesamtbild dar. Mehr Beanstandungen waren bei den Angeboten der Bürgerhaushalte in Köln, Lichtenberg, Solingen und Trier sowie bei dem E-Konsultationsangebot des BMI und meineSPD zu finden. Die Anwendung mit der größten Kritik war der Bürgerhaushalt Hamburg, bei dem diverse sicherheits- und datenschutzrelevante Risiken vorhanden waren.

Bei der Untersuchung der Sicherheitslevel wurden die E-Petitionen und die Parteiwebseiten als besonders schutzwürdig eingestuft, sie bekamen das Level „hoch“. Insgesamt betrachtet, verfügten die Bürgerhaushalte über ein mittleres Sicherheitslevel, lediglich dem Angebot aus Köln wurde, wegen der hohen Nutzerzahl, ein hohes Level zugeordnet. Die E-Konsultation wurde als einziges mit einem niedrigen Sicherheitslevel eingestuft, da die Gefahr, die von dem Angebot ausgeht, vergleichsweise gering ist.

Bereits während der theoretischen Betrachtung zu den Grundlagen der Sicherheit in Kapitel 3 zeigte sich die Komplexität dieser Arbeit. Hierbei stellte sich heraus, dass es für eine Masterarbeit zu umfangreich ist, alle Seiten der Sicherheit gleichermaßen zu betrachten. Daher beschränkt sich diese Arbeit auf die wichtigsten Aspekte der Themenbereiche Sicherheit und Datenschutz aus der Nutzersicht. Der Bereich der Sicherheit aus Anbietersicht bietet sich daher für weitere Forschungsaktivitäten an. Hierbei ist interessant, wie die Anbieter Sicherheitsaspekte serverseitig umsetzen und wie eine möglichst hohe Sicherheit gewährleistet wird. So könnte untersucht werden, wie die Daten- und IT-Sicherheit umgesetzt wird und welche Tools eingesetzt werden, um Angriffe zu verhindern. Zudem wäre eine Fragestellung, wie organisatorisch mit Angriffen umgegangen wird und ob beispielsweise ein „Computer Emergency Response Team“ (CERT) vorhanden ist. Auch die Umsetzung von Leitlinien im Umgang mit den Nutzerdaten wäre ein interessantes Thema. Hierfür könnten Umfragen an die entsprechenden Anbieter eingesetzt werden.

Ein weiteres Untersuchungsfeld wäre die Nutzung von sozialen Netzwerken in der E-Partizipation. Da immer mehr Firmen soziale Netzwerke als wichtiges Marketinginstrument sehen, werden diese in der Privatwirtschaft immer verstärkter eingesetzt [Online Marketing Podcast, 2010]. Daher bietet sich hier eine Untersuchung über die Gefahren und Möglichkeiten an, die durch die Nutzung von Plattformen wie StudiVZ, Facebook und Twitter entstehen. Insbesondere die Gefahren des Datenschutzes könnten betrachtet werden.

Zudem eignet sich für weitere wissenschaftliche Arbeiten die Sicherheitsbetrachtung von E-Partizipationsanwendungen nach der Einführung von E-Postbrief und De-Mail. Es ist interessant, welche Angebote auf ein sichereres System der Identifikation und der sicheren Kommunikation umsteigen und wie schnell sich neue Technologien im öffentlichen Umfeld umsetzen. Auch ob sich

doch eher alternative kommerzielle Produkte wie Regify[29] durchsetzen und ob sich nur eine oder beide Technologien etablieren können sind interessante Gesichtspunkte. Zudem bietet sich die Untersuchung der Online-Landschaft von E-Commerce und E-Government nach der Einführung des elektronischen Personalausweises für weitere Forschungsarbeit an. Hierbei könnte betrachtet werden, welche Angebote die Identifizierung mittels des neuen Ausweises umsetzen und wie die Kunden diese neue Technologie annehmen.

[29] http://www.regify.com/

Literaturverzeichnis

Achatz, L. (2009). *Möglichkeiten der ePartizipation für Jugendliche in Deutschland.* Magisterarbeit an der Kultur- und Gesellschaftswissenschaftlichen Fakultät der Universität Salzburg.

Albrecht, S., Kohlrausch, N., Kubicek, H., Lippa, B., Märker, O., Trénel, M., et al. (2008). *E-Partizipation - Elektronische Beteiligung von Bevölkerung und Wirtschaft am E-Government.* Bremen: Studie im Auftrag des Bundesministeriums des Innern, Ref. IT 1.

ARD/ZDF-Medienkommission. (2009). *ARD/ZDF-Onlinestudie 2009*. Abgerufen am 05. Mai 2010 von http://www.ard-zdf-onlinestudie.de

Beauftragte der Bundesregierung für Informationstechnik. (2010). *De-Mail - so einfach wie E-Mail und so sicher wie Papierpost.* Abgerufen am 31. 03 2009 von http://www.cio.bund.de/cln_102/sid_1D60D3BC661B7DFD76DEAE3A588324BC/DE/IT-Projekte/De-Mail/demail_node.html

Beauftragte der Bundesregierung für Informationstechnik. (2010). *Der neue Personalausweis* . Abgerufen am 27. Juli 2010 von http://www.cio.bund.de/cln_164/DE/IT-Projekte/Neuer_Personalausweis/neuer_personalausweis_node.html

Beauftragte der Bundesregierung für Informationstechnik. (2009). *Der neue Personalausweis Anwendungstest 2009 – 2010.* Abgerufen am 31. 03 2010 von http://www.bmi.bund.de/cae/servlet/contentblob/895702/publicationFile/55297/broschuere_neuer_perso.pdf

Berger-Lenz, M. (2007). *Bürgerinitiativen in Großbritannien und Deutschland- welchen Einfluss haben sie auf die Politik in ihren Staaten?* Norderstedt: GRIN Verlag.

Bertelsmann Stiftung. (2002). *Balanced E-Government - Elektronisches Regieren zwischen administrativer Effizienz und bürgernaher Demokratie.* Abgerufen am 31. 03 2010 von http://www.bertelsmann-stiftung.de/cps/rde/xbcr/SID-9A246CB2-85DD0E6E/bst/studie.pdf

Bitkom. (18. April 2010). *Internet ist großer Gewinn für die Lebensqualität*. Abgerufen am 26. Juni 2010 von http://www.bitkom.org/de/presse/8477_63364.aspx

Bitkom. (02. März 2010). *Internet-Nutzer begrüßen neuen Personalausweis*. Abgerufen am 27. Juli 2010 von http://www.bitkom.org/de/presse/8477_62642.aspx

Bitkom. (2008). *Web 2.0 für die öffentliche Verwaltung - Grundzüge, Chancen, Beispiele und Handlungsvorschläge.* Berlin: BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.

Borges, G. (2010). *Arbeitsgruppe Identitätsschutz im Internet e.V.* Abgerufen am 06. Juli 2010 von https://www.a-i3.org/

Borges, G., & Schwenk, J. (2006). Identitätsschutz: Eine zentrale Herausforderung für IT und E-Commerce. *Vortrag beim IT-Gipfel der Bundesregierung am 18.12.2006.* Potsdam.

Borges, G., Schwenk, J., Stuckenberg, C.-F., & Wegener, C. (2010). *Identitätsdiebstahl und Identitätsmissbrauch im Internet - Rechtliche und technische Aspekte .* Bonn: Bundesamt für Sicherheit in der Informationstechnik.

Brauckmann, P. (04. Juni 2009). *Politische Onlinemacher im Interview: Sebastian Reichel (SPD)*. Abgerufen am 17. September 2010 von http://politik-digital.de/politische-onlinemacher-im-interview-sebastian-reichel-spd

Brauckmann, P. (15. April 2009). *Webwahlkampf: Was die Parteien wollen - und können*. Abgerufen am 20. August 2010 von politik-digital.de: http://politik-digital.de/soziale-netzwerke-im-deutschen-wahlkampf

Bundesamt für Sicherheit in der Informationstechnik. (kein Datum). *CERT-Bund.* Abgerufen am 31. 03 2010 von https://www.bsi.bund.de/DE/Themen/CERTBund/certbund_node.html

Bundesamt für Sicherheit in der Informationstechnik. (2009). *IT-Grundschutz-Kataloge.* Abgerufen am 31. 03 2010 von https://www.bsi.bund.de/cln_156/DE/Themen/weitereThemen/ITGrundschutzKataloge/Inhalt/inhalt_node.html

Bundesamt für Sicherheit in der Informationstechnik. (2006). *Sicherheit von Webanwendungen - Maßnahmenkatalog und Best Practices.* Abgerufen am 06. Juli 2010 von https://www.bsi.bund.de/cae/servlet/contentblob/476464/publicationFile/30642/WebSec_pdf.pdf

Bundesamt für Sicherheit in der Informationstechnik. (2009). *SOA-Security-Kompendium - Sicherheit in Service-orientierten Architekturen.*

Bundeskriminalamt. (06. September 2010). *Online-Kriminelle gehen immer raffinierter vor*. Abgerufen am 07. September 2010 von http://www.bka.de/pressemitteilungen/2010/pm100906.html

Bundesministerium der Justiz. (2010). *Bundesdatenschutzgesetz*. Abgerufen am 25. Juli 2010 von http://www.gesetze-im-internet.de/bdsg_1990/

Bundesministerium der Justiz. (2001). *Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG).* Berlin: http://www.gesetze-im-internet.de/sigg_2001/.

Bundesministerium des Innern. (2009). *Der elektronische Personalausweis .* Abgerufen am 31. 03 2010 von http://www.bmi.bund.de/cae/servlet/contentblob/594848/publicationFile/33685/epa_broschuere_cebit.pdf

Bundesministerium des Innern. (2010). *e-konsultation.de.* Abgerufen am 31. 03 2010 von BMI Internetredaktion: http://www.e-konsultation.de/

Bundesministerium des Innern. (2008). *Umsetzungsplan 2008 - E-Government 2.0.* Berlin.

Bundesministerium für Wirtschaft und Technologie. (2009). *12. Faktenbericht Monitoring Informationswirtschaft.* Berlin.

Champ, H. (12. Oktober 2009). *4,000,000,000*. Abgerufen am 10. Juni 2010 von Flickr Blog: http://blog.flickr.net/en/2009/10/12/4000000000/

Clift, S. (September 2003). *E-Democracy, E-Governance and Public Net-Work (Government 2.0)*. Abgerufen am 19. Mai 2010 von http://stevenclift.com/?p=104

Das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag. (2007). Öffentliche Petitionen beim Deutschen Bundestag – Erste Ergebnisse der Evaluation des Modellversuchs. *Brief Nr. 32* , S. 35.

Das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag. (2008). Varianten Digitaler Demokratie – Eine Einführung in den Schwerpunkt. *Brief Nr. 34* , S. 5.

Department für Informationsverarbeitung & Prozessmanagement, Wirtschaftsuniversität Wien. (2009). *eDemocracy & eVoting Wiki*. Abgerufen am 31. 03 2010 von http://www.ocg.at/ak/edemocracy/wiki/doku.php

Deutsche Post. (2010). Abgerufen am 26. Juli 2010 von E-Postbrief - Allgemeine Geschäftsbedingungen: https://www.epost.de/adressreservierung/footer/rechtliches/agb.html#DatenschutzVertraulichkeit

Deutscher Anwaltverein. (Juli 2010). *Stellungnahme des Deutschen Anwaltvereins durch den Ausschuss Informationsrecht zum Referentenentwurf eines Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften (De-Mail-Gesetz).* Abgerufen am 27. Juli 2010 von http://anwaltverein.de/downloads/stellungnahmen/SN-10/SN-39.pdf

Deutscher Bundestag. (2010). *Petitionen*. Abgerufen am 15. September 2010 von https://epetitionen.bundestag.de/

Dopatka, A. (2005). *E-Voting in Deutschland? Zum Problem der Stimmabgabe über das Internet bei politischen Wahlen.* Universität Hildesheim: Magisterarbeit am Institut für Angewandte Sprachwissenschaft.

E-Demokratie.org. (2010). *E-Partizipation – Was ist elektronische Demokratie?* Abgerufen am 31. 03 2010 von http://www.eDemokratie.org

Elliott, T. (10. Juli 2009). *SAP Social Media Guidelines 2009*. Abgerufen am 16. Juni 2010 von SAP Web 2.0: http://www.sapweb20.com/blog/2009/07/sap-social-media-guidelines-2009/

E-Partizipation. (2007). Beteiligungsprojekte im Internet, Nummer 21. In *Beiträge zur Demokratieentwicklung.* Bonn: Stiftung Mitarbeit.

Evans, M. (26. Januar 2010). *75M Twitter Users But Growth Slowing*. Abgerufen am 17. Juni 2010 von Twitterrati: http://www.twitterrati.com/2010/01/26/75m-twitter-users-but-growth-slowing/

FDP-Bundespartei. (2010). *my.FDP - Die Liberale Kommunikationsplattform*. Abgerufen am 17. September 2010 von https://my.fdp.de/

Firesmith, D. G. (2003). Engineering Security Requirements. *Journal of Object Technology Vol. 2, No. 1, January-February 2003* .

Fraser, C., Liotas, N., Lippa, B., Mach, M., Macintosh, A., Marzano, F., et al. (2006). Report on current ICTs to enable Participation. *Deliverable 5.1, DEMO-net Consortium, www.demo-net.org* .

Fraunhofer eGovernment Zentrum. (2007). *Aktuelle Trends im E-Government und Vorschläge zum Programm "E-Government 2.0".* Abgerufen am 31. 03 2010 von http://www.egov-zentrum.fraunhofer.de/extra_files_filedownload.php3?sessionid=11163be3b9b16ed1b9936830721aa3c1&id=101

Fraunhofer-Institut für Offene Kommunikationssysteme. (2010). *Kompetenzzentrum neuer Personalausweis*. Abgerufen am 27. Juli 2010 von http://www.ccepa.de/public/index.htm

Freenet. (2010). *Sicheres Passwort*. Abgerufen am 15. September 2010 von freenet.de Kundenservice: http://kundenservice.freenet.de/hilfe/allgemeines/passwort/passwort-sicher/sicherespasswort/index.html

Fuhrberg, K. (2000). *Internet-Sicherheit - Browser, Firewalls und Verschlüsselung.* München: Carl Hanser Verlag.

Grimm, R. (2008). *Folien zur Vorlesung IT-Risk Management.* Universität Koblenz.

Groll, T. (11. Februar 2010). *Meine Identität gehört mir!* Abgerufen am 06. Juli 2010 von Zeit Online: http://www.zeit.de/digital/datenschutz/2010-01/identitaetsdiebstahl-selbsterfahrung?page=all

Grunwald, A., Banse, G., Coenen, C., & Hennen, L. (2006). *Netzöffentlichkeit und digitale Demokratie - Tendenzen politischer Kommunikation im Internet.* Berlin: edition sigma, ISBN: 3-89404-827-1.

Gutjahr, R. (23. Juli 2010). *Der E-Postbrief – Die Gelbe Gefahr?* Abgerufen am 26. Juli 2010 von G! – gutjahr's blog: http://gutjahr.biz/blog/2010/07/die-gelbe-gefahr/

Harth, T. (1999). Internet und Demokratie – neue Wege politischer Partizipation: Überblick, Potential, Perspektiv. (W. Woyke, Hrsg.) *Internet und Demokratie* , S. 8 - 24.

Heise Online. (24. Mai 2009). *Bundespräsidenten-Wahl: Ergebnis per SMS und Twitter verkündet*. Abgerufen am 18. Juli 2010 von http://www.heise.de/newsticker/meldung/Bundespraesidenten-Wahl-Ergebnis-per-SMS-und-Twitter-verkuendet-219939.html

heise online. (09. Februar 2009). *Online-Petitionssystem des Bundestags mit Ausfällen*. Abgerufen am 22. September 2010 von http://www.heise.de/newsticker/meldung/Online-Petitionssystem-des-Bundestags-mit-Ausfaellen-206844.html

Holznagel, B. (2001). *Elektronische Demokratie – Bürgerbeteiligung per Internet zwischen Wissenschaft und Praxis.* München: Verlag C.H.Beck oHG.

IAP2. (2007). *IAP2 Spectrum of Public Participation.* Abgerufen am 02. August 2010 von http://www.iap2.org/associations/4748/files/spectrum.pdf

Jakobs, J. (24. November 2009). *Datenschützer wollen Einsatz von Analytics verhindern*. Abgerufen am 16. Juli 2010 von Zeit Online: http://www.zeit.de/digital/datenschutz/2009-11/google-analytics-datenschutz

Janowicz, K. (2007). *Sicherheit im Internet.* 3. Auflage, ISBN 978-3-89721-715-7.

Junee, R. (20. Mai 2009). *Zoinks! 20 Hours of Video Uploaded Every Minute!* Abgerufen am 13. Juni 2010 von YouTube Blog: http://youtube-global.blogspot.com/2009/05/zoinks-20-hours-of-video-uploaded-every_20.html

Kachel, E. (24. August 2008). *CSS / XSS – Angriff (Cross Site Scripting) - eine Analyse*. Abgerufen am 08. Juni 2010 von PHP Application and Website Defense: http://www.erich-kachel.de/?p=181

Kafka, G. (11. August 2010). *Gesetzentwurf in der Kritik - De-Mail ist unsicher, teuer, unpraktisch*. Abgerufen am 12. August 2010 von Computerwoche: http://www.computerwoche.de/mittelstand/2351154/index2.html

Kerkmann, C. (21. Februar 2010). *Durchwachsene Bilanz bei Online-Petitionen*. Abgerufen am 17. September 2010 von heise online: http://www.heise.de/newsticker/meldung/Durchwachsene-Bilanz-bei-Online-Petitionen-936369.html

Kleinsteuber, H. J. (2001). Das Internet in der Demokratie. Euphorie und Ernüchterung. In B. Holznagel, A. Gründwald, & A. Hanßmann, *Elektronische Demokratie: Bürgerbeteiligung per Internet zwischen Wissenschaft und Praxis* (S. S. 7-27). München: Beck.

Klostermeier, J. (13. Juli 2010). *Identitätsmissbrauch bedroht Sicherheit*. Abgerufen am 13. Juli 2010 von Computerwoche: http://www.computerwoche.de/subnet/oracle-crm/2349033/

Knall, C. (2007). *Cross-Site-Scripting-Problem.* Berufsakademie Ravensburg.

Koop, A. (2010). *Leitfaden Online-Konsultation - Praxisempfehlungen für die Einbeziehung der Bürgerinnen und Bürger über das Internet.* Gütersloh: Bertelsmann Stiftung.

Krauch, H. (1972). *Computer-Demokratie.* Düsseldorf: VDI-Verlag.

Kubicek, H. e. (2008). *E-Konsultation Ergebnisse der elektronischen Konsultation zu den Gutachten E-Partizipation und E-Inclusion.* Abgerufen am 31. 03 2010 von http://www.e-konsultation.de/e-konsultation/site/pictures/IFIB_Zebralog_ERCIS_BMI_E_Konsultationsauswertung.pdf

Kubicek, H., & Noack, T. (10. April 2010). Identity in the Information Society Volume 3. *Special Issue: The Diversity of National E-IDs in Europe: Lessons From Comparative Research* , S. 111-153.

Leibniz-Rechenzentrum. (14. Juni 2005). *Verschlüsselung, digitale Signaturen, Zertifikate*. Abgerufen am 12. Juli 2010 von Leibniz-Rechenzentrum: http://www.lrz.de/services/pki/einf/

Lucke, J. v., & Reinermann, H. (2000). *Ergebnisse des Forschungsprojektes Regieren und Verwalten im Informationszeitalter.* Speyer: Forschungsinstitut für öffentliche Verwaltungbei der Deutschen Hochschule für Verwaltungswissenschaften Speyer.

Macintosh, A. (2006). eParticipation in Policy-making: the Research and the Challenges. In P. Cunningham, & M. Cunningham, *Exploiting the Knowledge Economy: Issues, Applications, Case Studies.* Amsterdam: IOS Press.

Magoutas, B., & Mentzas, G. (2007). The role of Adaptivity & Personalization technologies in eParticipation. *Deliverable 14.3, DEMO-net Consortium, www.demo-net.org* .

Märker, O., & Wehner, J. (18. Juli 2008). *E-Partizipation – ein Beratungsinstrument für Politik und Verwaltung.* Abgerufen am 22. September 2010 von Newsletter Wegweiser Bürgergesellschaft 14/2008: http://www.buergergesellschaft.de/fileadmin/pdf/gastbeitrag_maerker_wehner_080718_01.pdf

Microsoft. (26. Oktober 2006). *So erkennen Sie gefälschte Webseiten*. Abgerufen am 27. Juli 2010 von http://www.microsoft.com/germany/protect/yourself/phishing/spoof.mspx

Ministerium des Innern und für Sport Rheinland-Pfalz. (2010). *IT-Sicherheit*. Abgerufen am 07. Mai 2010 von http://www.zukunft.rlp.de/it-management/it-sicherheit/

Ministerium des Innern und für Sport Rheinland-Pfalz. (2010). *zukunft.rlp.de*. Abgerufen am 31. März 2010 von http://www.zukunft.rlp.de/

Möhring, M. (2009). *Folien zur Vorlesung Datenschutz WS 2009/2010.* Universität Koblenz.

Morrison, C. (8. April 2010). *Eastern Europe Rises as Facebook Continues Strong Regional Growth in March*. Abgerufen am 19. Juni 2010 von Inside Facebook: http://www.insidefacebook.com/2010/04/08/eastern-europe-rises-as-facebook-continues-strong-regional-growth-in-march/

OECD. (2001). *Citizens as Partners - Information, consultation and public participation in policy-making.* Paris: OECD.

Online Marketing Podcast. (23. September 2010). *Volkswagen und MTV präsentieren internationale Social-Media-Studie „MePublic“*. Abgerufen am 23. September 2010 von http://www.online-

marketing-podcast.de/2010/volkswagen-und-mtv-praesentieren-internationale-social-media-studie-mepublic/2929/

O'Reilly, T. (30. September 2005). *What Is Web 2.0?* Abgerufen am 26. Mai 2010 von http://www.oreilly.de/artikel/web20.html

Panko, R. R. (2006). *Business Data Networks and Telecommunications, 6. Edition.* Prentice Hall.

PC Welt. (06. Mai 2010). *Ratgeber - So knacken Sie Ihr vergessenes Passwort*. Abgerufen am 08. Juni 2010 von PC Welt: http://www.pcwelt.de/start/sicherheit/backup/praxis/197778/so_knacken_sie_ihr_vergessenes_passwort/index2.html

Perscheid, C. (2007). *Vergleichende Analyse verschiedener E-Partizipationsprojekte in Deutschland.* Masterarbeit am Institut für Wirtschafts- und Verwaltungsinformatik an der Universität Koblenz-Landau.

Preuss, T. (2009). *Anonymitäts- und Pseudonymitätskonzepte für Online-Bürgerbefragungen und Online-Diskussionen.* Masterarbeit am Institut für Wirtschafts- und Verwaltungsinformatik an der Universität Koblenz-Landau.

Rastetter, K. (kein Datum). *Aktionsplan 2009.* Abgerufen am 31. 03 2010 von Innenministerium NRW: http://www.im.nrw.de/pub/pdf/aktionsplan_2009.pdf

Roßnagel, A. (2009). *Preisrede zur "Modernisierung des Datenschutzes" .* Abgerufen am 31. 03 2010 von http://www.datenschutz.rlp.de/de/wissenschaftspreis/bisherige_arbeiten/2009_Preisrede_Prof_Rossnagel.pdf

Sass, L. (2007). *Moderne Webwerkzeuge, Informationsräume und kollaborative Projekte.* Seminararbeit im Rahmen des Seminars “Wissen in der modernen Gesellschaft” Universität Leipzig.

Sauerborn, M. (2008). *E-Participation in Germany: Analysis of the status quo and survey in Koblenz.* Masterarbeit am Institut für Wirtschafts- und Verwaltungsinformatik an der Universität Koblenz-Landau.

Schellong, A., & Girrger, P. (Juni 2010). *Government 2.0 in der Betaphase.* Abgerufen am 28. Juli 2010 von CSC: http://assets1.csc.com/de/downloads/CSC_policy_paper_series_06_2010_government_20_betaphase.pdf

Scherer, S., Liotas, N., Wimmer, M. A., Tambouris, E., & Tarabanis, K. (2010). Interoperability Requirements, Recommendations and Standards in E-Participation (Chapter 6). In *Charalabidis, Yannis: Interoperability in Digital Public Services and Administration: Bridging E-Government and E-Business.* IGI-Global book, ISBN: 978-1-61520-887-6.

Scherer, S., Wimmer, M. A., & Schneider, C. (2008). Investigating Information and Knowledge Management (IKM) in eDeliberation. In *Cunningham, Paul; Cunningham, Miriam: Collaboration and the Knowledge Economy: Issues, Applications, Case Studies* (S. 270-277). Amsterdam: IOS Press.

Schlandt, J. (21. Juli 2010). *De-Mail - Elektronischer Kuvertwechsel*. Abgerufen am 26. Juli 2010 von Frankfurter Rundschau: http://www.fr-online.de/in_und_ausland/wirtschaft/aktuell/2868446_De-Mail-Elektronischer-Kuvertwechsel.html

Schoppé, F., Parasie, N., & Veit, D. (18. August 2009). *Empirische Studie zur Identifikation von Einflussfaktoren auf die Akzeptanz von Innovationen E-Participation-Anwendungen.* Abgerufen am 30. Juni 2010 von Universität Mannheim: http://veit.bwl.uni-mannheim.de/fileadmin/files/Forschung/Fachberichte/Fachbericht_20090818.pdf

Schulzki-Haddouti, C. (03. April 2010). *futurezone.ORF.at*. Abgerufen am 14. April 2010 von http://futurezone.orf.at/stories/1642752/

Schwartig, G., & Vorwerk, V. (2010). Bürgerhaushalt und Internet - Auftakt zu einer interaktiven Politik? *Fachtagung Verwaltungsinformatik FTVI - Rechtsinformatik FTRI, Fachbereich Informatik 02/2010*, (S. 12-15). Koblenz.

SPD. (2010). *meineSPD*. Abgerufen am 25. September 2010 von http://www.meinespd.net/

Spooren, S., & Pohlmann, N. (2010). *Sicherer Dokumentenaustausch via E-Mail.* Fachhochschule Gelsenkirchen: Institut für Internet-Sicherheit.

Stadt Hamburg. (2010). *Bürgerhaushalt Hamburg*. Abgerufen am 31. März 2010 von http://www.buergerhaushalt-hamburg.de/

Stadt Köln. (kein Datum). Abgerufen am 22. Juli 2010 von Könler Bürgerhaushalt: https://buergerhaushalt.stadt-koeln.de/

Stadt Köln. (2009). *Broschüre Kölner Bürgerhaushalt.* Abgerufen am 22. Juli 2010 von http://www.stadt-koeln.de/mediaasset/content/pdf20/buergerhaushalt/broschuere_koelner_buergerhaushalt_2010.pdf

Stadt Lichtenberg. (2010). *Bürgerhaushalt Lichtenberg*. Abgerufen am 22. Juli 2010 von http://www.buergerhaushalt-lichtenberg.de

Stadt Solingen. (2010). *Solingen Spart!* Abgerufen am 20. August 2010 von http://www.solingen-spart.de

Stadt Trier. (2010). *Bürgerhaushalt Trier*. Abgerufen am 01. August 2010 von http://www.buergerhaushalt-trier.de/

Stiftung Warentest. (15. Juli 2010). *E-Postbrief: Briefe per Mail verschicken*. Abgerufen am 26. Juli 2010 von http://www.test.de/themen/freizeit-reise/schnelltest/E-Postbrief-Briefe-per-Mail-verschicken-4115841-4115843/

The Sydney Morning Herald. (12. Oktober 2009). *YouTube views over one billion a day*. Abgerufen am 14. Juni 2010 von http://www.smh.com.au/technology/biz-tech/youtube-views-over-one-billion-a-day-cofounder-20091012-gsva.html

Trautmann, A. (24. Oktober 2005). *Vorschlag für eine Muster-Datenschutzerklärung für Webseiten.* Abgerufen am 06. August 2010 von Law-Blog: http://www.law-blog.de/203/datenschutzerklaerung-webseite/

Trechsel, A. H., Kies, R., Mendez, F., & Schmitter, P. C. (2002). *Evaluation of the Use of Technologies in Order to Facilitate Democracy in Europe - E-Democratising the Parliaments and Parties of Europe.* Abgerufen am 02. August 2010 von CIES-ISCTE: http://www.cies.iscte.pt/destaques/pdf/1.pdf

TuTech Innovation GmbH, Rolf Lührs. (2009). *Ergebnisbericht zur Online-Diskussion „Bürgerhaushalt Hamburg 2009“.* Abgerufen am 31. 03 2010 von http://www.buergerhaushalt-hamburg.de/site/downloads/6400_32_090909_Abschlussbericht_Hamburger_Buergerhaushalt_2009_FINAL.pdf

Twitter Blog. (22. Februar 2010). *Measuring Tweets*. Abgerufen am 16. Juni 2010 von http://blog.twitter.com/2010/02/measuring-tweets.html

Ulbricht, C. (12. November 2007). *Ist die Nutzung von Google Analytics und Co rechtswidrig?* Abgerufen am 11. August 2010 von Web 2.0, Social Media & Recht: http://www.rechtzweinull.de/index.php?/archives/50-Ist-die-Nutzung-von-Google-Analytics-und-Co-rechtswidrig.html

Universität Koblenz. (2010). *Virtual Private Network (VPN)*. Abgerufen am 08. September 2010 von http://www.uni-koblenz-landau.de/koblenz/GHRKO/netzwerk/vpn

Wimmer, M. (2008). *Folien zur Vorlesung Grundlagen der Verwaltungsinformatik.* Universität Koblenz.

Wolff, V. (2006). *Diskursverständnis in E-Diskursen - Ein Instrumentarium für das Monitoring und die quantitative Analyse von moderierten E-Diskursen.* Doktorarbeit am Fachbereich Informatik an der Universität Koblenz-Landau.

Zielinski, M. P. (2007). Privacy protection in eParticipation: guiding the anonymisation of microdata. In A. Avdic, K. Hedström, J. Rose, & Å. Grönlund, *Understanding eParticipation - Contemporary PhD eParticipation research in Europe* (S. 57-68). Örebro: ISBN 978-91-7668-530-3.

Anhang

Analyse-Framework

Datenschutz

	Bürgerhaushalte				
	Hamburg	Köln	Trier	Lichtenberg	Solingen
Transparenz	Die "Spielregeln" und Datenschutz-erklärung sind sehr übersichtlich und äußerst ausführlich	Informationen recht unübersicht-lich, Datenschutz-erklärung nur über "Spielregeln" auffindbar	Es wird nicht erkenntlich, wann persönliche Daten (Name, Adresse etc.) verwendet werden, außer dass sie den Moderatoren bei dem Verdacht des Missbrauchs zur Verfügung stehen	Angebot ist sehr transparent	Die "Spielregeln" und Datenschut-zerklärung sind sehr übersichtlich und äußerst ausführlich
Verarbeitung der Daten für andere Zwecke (Zweckbindung)	Nur für Forschungszwecke	Nein	Nur für statistische Zwecke	Nur für statistische Zwecke	Nein
Vertrauensbilden-de Maßnahmen / Negative Datenschutzas-pekte	**Nutzt Google Analytics, Daten werden in den USA gespeichert**	Teilnehmende veröffentlichen ihre Texte und Bilder unter der Creative Commons Lizenz	Teilnehmende veröffentlichen ihre Texte und Bilder unter der Creative Commons Lizenz 3.0 by-nc	Es wird nicht klar, ob und wie die persönlichen Daten (Name, Adresse, etc.) geprüft werden Gute Kurzeinfüh-rung in das Thema	Keine
Datensparsam-keit / -vermeidung	Vor- und Nach-name, Pseudonym und E-Mail Pflicht, pers. Angaben optional	Keine persönlichen Daten werden abgefragt (Nur Pseudonym und E-Mail)	Persönliche Daten werden bei Verdacht eines Missbrauchs überprüft	Alle persönlichen Daten sind optional.	Nur Nutzernamen und E-Mail Pflicht, Rest optional
Nutzerkontrolle über eigene Daten	Keine Angaben, wie das Profil gelöscht werden kann, Beiträge können nur über Administratoren gelöscht werden	Wenn Beiträge geschrieben wurden, können Nutzerkonten nicht mehr gelöscht werden, eine spätere Anonymisierung ist möglich	Moderatoren verändern Einträge, die z.B. Abkürzungen oder Tippfehler enthalten Es gibt keine Informationen, wie das Benutzerprofil gelöscht werden kann	Sehr gute Kontrolle, alle Daten änderbar, Löschung durch eine E-Mail an die Moderation	Wenn Kommenta-re geschrieben wurden, können Nutzerkonten nicht mehr gelöscht werden, eine spätere Anonymisierung ist durch Moderatoren möglich
Weitergabe der Daten an Dritte	**Ja, an Google**	Nein	Nein	Nein	Nein
Auswertung der Daten	In anonymisierter Form	In anonymisierter Form	In anonymisierter Form	In anonymisierter Form	In anonymisierter Form

	E-Konsultation	**Parteiwebseiten**		**E-Petitionen**
	Netzpolitik	meineSPD	my.FDP	Bundestag
Transparenz	Sehr übersichtliche Datenschutzerklärung	Gute Datenschutzer-klärung, unklar wie die Daten für "interne" Zwecke verarbeitet werden	Sehr gut, verständliche und übersichtliche Datenschutzerklärung	Sehr transparente Angabe aller veröffentlichten Daten in den Datenschutzer-klärungen
Verarbeitung der Daten für andere Zwecke (Zweckbindung)	Nein	Daten können für (partei-)interne Zwecke verwendet werden	Nein	Daten werden nur im Rahmen der Petitionsverarbeitung weitergegeben
Vertrauensbildende Maßnahmen / Negative Daten-schutzaspekte	**Passwortstärke wird bei der Eingabe angezeigt**	Alle zusätzlichen Dienste wie Newsletter per Opt-in Anzeige der E-Mail und Adresse per Opt-in Alle Einstellungen zur Veröffentlichung von Angaben per Default deaktiviert	Im Forum werden nur Pseudonyme verwendet, per Link wird man auf die Profilseite der Person geführt -> Fragliche pseudonyme Nutzung	**Für vertrauliche Nachrichten wird der Postweg empfohlen, gesamte Kommunika-tion über https verschlüsselt, E-Mailverkehr zw. Anwendung und Ausschussdienst erfolgt SSL-verschlüsselt (erläutert in Datenschutzerklärung)**
Datensparsamkeit / -vermeidung	Nur Benutzername und E-Mail Pflicht	E-Mail, Vor- und Nachname Pflicht	E-Mail, Vor- und Nachname, Geschlecht	Alle sonstigen persönlichen Daten sind optional
Nutzerkontrolle über eigene Daten	Konto wird vom Nutzer nur deaktiviert, kann nur durch einen Moderator gelöscht werden, Passwort später nicht mehr änderbar	Nutzer hat volle Kontrolle, Profil einfach löschbar Die Sichtbarkeit des Profils ist einstellbar	Nutzer hat volle Kontrolle über seine Daten, Account löschbar, eigene Beiträge bleiben bestehen Vor- und Nachname wird im Profil immer öffentlich angezeigt, nicht abschaltbar	Konto kann von Nutzer nur deaktiviert werden, Löschung muss beantragt werden
Weitergabe der Daten an Dritte	Nein	Nein	Nein, nur wenn ausdrücklich gewollt	Nein
Auswertung der Daten	In anonymisierter Form	Daten werden für parteiinterne Zwecke verwendet	Nur netzwerkintern	Nutzung für den Petitionsprozess, sonst keine Auswertung

Registrierung

	Bürgerhaushalte				
	Hamburg	Köln	Trier	Lichtenberg	Solingen
Sicheres Passwort	Keine	Relativ sicheres Passwort, wird automatisch erzeugt (7 Zeichen, Klein- und Großbuchstaben, Zahlen), änderbar	Sicheres Passwort, wird zugeschickt (10 Zeichen, Klein- und Großbuchstaben, Zahlen), änderbar	Sicheres Passwort, wird automatisch generiert (7 Zeichen, Klein- und Großschreibung), änderbar	Keine
In Datenschutzerklärung einwilligen	Ja, Opt-in	Nein	Ja, Opt-in	Nein	Ja, Opt-in
Einwilligung in Sonderdienste	Benutzer bezieht automatisch den Newsletter und kann Nachrichten von anderen Nutzern empfangen, per Opt-out im Benutzerprofil abwählbar	Sehr gut, Nutzer muss für zusätzliche Angebote wie Newsletter oder Empfang von E-Mails anderer Nutzer mittels Opt-in explizit zustimmen	Ein Newsletter wird Opt-in, ein anderer Newsletter Opt-out angeboten	Newsletter Opt-out	Newsletter wird über Opt-out angeboten
Anzahl der erhobenen Pflichtdaten	Pseudonym, Passwort und E-Mail werden erfasst	Nur Nutzername, E-Mail Pflicht, Vor- und Nachname sowie persönliche Angaben optional	Sehr viele: Benutzername, E-Mail, Stadtteil, Vor-, Nachname, Straße und Hausnummer, PLZ, Ort	Nur Benutzername und Passwort, alle anderen Angaben sind freiwillig Persönliche Daten sind für die Abstimmung nötig	Nutzername, E-Mail Adresse und Passwort Pflicht Vor- und Nachname, Geschlecht, etc. freiwillig
Aufklärung und Informationen	Sehr gut, hier werden dem Nutzer die "Spielregeln" (incl. Datenschutzerklärung) verständlich erklärt	Keine	Alle Angaben übersichtlich und nutzerfreundlich verfasst	Alle Angaben sehr nutzerfreundlich verfasst Kurze Einführung in das Thema wird angeboten Datenschutzerklärungen nicht vorhanden, Verwendung der Daten nur über die „Regeln“ auffindbar	Keine

	E-Konsultation	**Parteiwebseiten**		**E-Petitionen**
	Netzpolitik	meineSPD	my.FDP	Bundestag
Sicheres Passwort	Sicheres Passwort wird automatisch generiert, änderbar, dabei wird die Passwortstärke angezeigt	Nein	Sicheres Passwort wird automatisch generiert, änderbar	Mindestens 8 Zeichen, darf nicht aus Teilen der E-Mail Adresse bestehen
In Datenschutz-erklärung einwilligen	Nein	Ja, Opt-in	Ja, Opt-in	Ja, Opt-in
Einwilligung in Sonderdienste	Newsletter: Opt-in	Alle Einstellungen per Default deaktiviert (E-Mail Anzeigen, Adresse anzeigen, Statusmail zusenden)	Newsletter per Opt-in	Anzeige der E-Mail-Adresse im Profil: Opt-out
Anzahl der erhobenen Pflichtdaten	Sehr gut, nur Benutzername und E-Mail Adresse	Vor- und Nachname, Benutzername, Passwort, E-Mail Adresse	Geschlecht, Vor- und Nachname, Benutzername, E-Mail Adresse	Viele Daten werden erfasst: E-Mail, Passwort, Vor-, Nachname, Adresse
Aufklärung und Informationen	Datenschutzerklärung verständlich	Nutzungsbedingungen und Datenschutzerklä-rung klar und verständlich	Datenschutzerklärung übersichtlich und klar	Datenschutzerklär-ungen und Richtlinien klar und verständlich

Identitätsmanagement

	Bürgerhaushalte				
	Hamburg	Köln	Trier	Lichtenberg	Solingen
Anonymisierung / Pseudonymisie-rung	- / Ja	- / Ja	- / Ja	- / Ja	- / Ja
Identifikation / Authentifikation	Benutzername / Passwort	Benutzername / Passwort	Benutzername / Passwort	Benutzername / Passwort	Benutzername / Passwort
Verifikation	Aktivierungslink per E-Mail	Aktivierungslink per E-Mail	Aktivierungslink und Passwort in E-Mail	Aktivierungslink und Passwort in E-Mail	Aktivierungslink per E-Mail
Passwort per E-Mail verschickt	Nein	Ja	Ja	Ja	Nein
Automatischer Logout	Nein	Nein	Nein	Nein	Nein

	E-Konsultation	Parteiwebseiten		E-Petitionen
	Netzpolitik	meineSPD	my.FDP	Bundestag
Anonymisierung / Pseudonymisierung	Ja / Ja	Nein	Mitgliederbereich: Nein	Petition: Nein
	Gastteilnahme möglich		Forum: Ja, Pseudonym	Forum: Ja, Pseudonym
Identifikation / Authentifikation	Benutzername / Passwort	Benutzername / Passwort	Benutzername / Passwort	Benutzername / Passwort
Verifikation	Passwort wird per E-Mail zugeschickt	Aktivierungslink per E-Mail	Passwort wird per E-Mail zugeschickt	Benutzername und Aktivierungslink wird per E-Mail zugeschickt
Passwort per E-Mail verschickt	Ja	Nein	Ja	Nein
Automatischer Logout	Nein	Nein	Nein	Sitzungslänge einstellbar

Sichere Kommunikation

	Bürgerhaushalte				
	Hamburg	Köln	Trier	Lichtenberg	Solingen
Verwendung von TLS/SSL	Nein	Ja, auch ohne Anmeldung	Ja	Nein	Nein
Passwörter werden im Klartext gesendet	Ja	Nein	Nein	Ja	Ja
Minimale Informationen bei Fehlanmeldung	Ja	Nein	Ja	Ja	Ja

	E-Konsultation	Parteiwebseiten		E-Petitionen
	Netzpolitik	meineSPD	my.FDP	Bundestag
Verwendung von TLS/SSL	Nein	Ja	Ja	Ja
Passwörter werden im Klartext gesendet	Ja	Nein	Nein	Nein
Minimale Informationen bei Fehlanmeldung	Ja	Ja	Ja	Nein

Danksagung

Zunächst einmal möchte ich Frau Prof. Dr. Maria A. Wimmer für die Bereitstellung dieses interessanten Themas danken. Darüber hinaus möchte ich mich nicht nur bei ihr, sondern auch bei Frau Sabrina Scherer für die tatkräftige Unterstützung und Betreuung bei der Entstehung dieser Arbeit bedanken. Ein weiterer Dank geht auch an meine Familie und meine Freunde, die mir während der Masterarbeit hilfreich zur Seite standen.