

Einfluss von Umgebungsfaktoren, Ergonomie und Systemgestaltung auf den sicheren mobilen Informationszugriff

Angela Frankfurth, Michael Knopp

ITeG - Forschungszentrum für Informationstechnik-Gestaltung

Universität Kassel

Wilhelmshöher Allee 64-66

34109 Kassel

frankfurth@wirtschaft.uni-kassel.de

michaelknopp@uni-kassel.de

Abstract: Im Zuge der Modernisierung wird die Verwaltung zunehmend mobile Endgeräte einsetzen, um den Außendienst effizient zu unterstützen. Informationszugriff und -gewinnung vor Ort finden jedoch unter anderen Bedingungen statt als im Büro, woraus sich andere Anforderungen an Datenschutz und -sicherheit ergeben, die durch die Technikgestaltung gelöst werden müssen. Der Beitrag beschreibt die sich ergebenden Herausforderungen beim mobilen Informationszugriff sowie die mobile Dokumentation am Beispiel der Gewerbeaufsicht.

1 Informationszugriff und Dokumentation in der Gewerbeaufsicht

Verwaltungshandeln ist insbesondere deshalb auf Information und Wissen angewiesen, weil für viele Entscheidungen Tatbestandsmerkmale einer Norm erfüllt sein müssen oder ein Ermessensspielraum besteht, zu dessen Ausübung Informationen über den gesamten Sachverhalt erforderlich sind. Information und Wissen stellen eine wesentliche Ressource der Arbeit eines Verwaltungsmitarbeiters dar, [WTL01] denn Verwaltungstätigkeit ist vor allem Informationsverarbeitung und ihre Prozesse sind hiervon stark geprägt [Le05, 43]. Wichtig für den vor Ort arbeitenden Verwaltungsmitarbeiter, z.B. einen Beamten der Gewerbeaufsicht, ist daher der Zugriff auf digital vorliegendes Wissen innerhalb der Verwaltung, wie Normen und Gesetze oder Angaben zu Betrieben. Außerdem werden kontinuierlich Informationen erhoben, verarbeitet und weitergegeben. Daher sind Produkt- und Prozessinnovationen in der Verwaltung sehr eng verknüpft. Das Zusammenwirken des Denkens in Geschäftsprozessen mit Potentialen der Informationstechnik und der Mobilisierung bietet die Möglichkeit, Verwaltungsverfahren hinsichtlich Qualität, Effektivität, Transparenz und Effizienz zu verbessern. Weitere Vorteile der Unterstützung der außendienstlichen Verwaltungstätigkeit durch mobile Endgeräte liegen im Wegfall von Mehrfacharbeiten (z.B. nachträgliche Digitalisierung erhobener Daten), der Fehlervermeidung bei Datenaufnahme, der Möglichkeit der unmittelbaren und abschließenden Beurteilung sowie der medienbruchfreien Bearbeitungsmöglichkeit. Vielfach führten jedoch Sicherheitsbedenken und praktische Hindernisse dazu, dass mobile

Lösungen bislang kaum umgesetzt wurden.¹

Mobile IuK-Technik führt zur Verlagerung des Informationszugriffs und der (elektronischen) Dokumentation aus dem Büro hin zum Betrieb vor Ort. Die Gewerbeaufsicht bspw. ist überwiegend eine kontrollierende Verwaltungstätigkeit (Aufsichtstätigkeit). Sie ist regelmäßig mit dem Zugriff auf das in der Verwaltung vorliegende Wissen hinsichtlich des Kontrollobjekts sowie der entsprechenden Vorgaben, Verordnungen und Gesetze, der Dokumentation eines vorgefundenen Sachverhalts (auch mit multimedialen Mitteln) sowie dem Treffen einer Entscheidung und oft mit einem Bescheiderlass oder dem Erstellen eines Revisions Schreibens verbunden. Mobile Endgeräte können die Entscheidungsfindung und -weiterleitung vor Ort unterstützen. Die Dokumentation der Aktivitäten kann direkt vor Ort elektronisch in den Fachanwendungen² erfolgen und muss nicht mehr später übertragen oder aus dem Gedächtnis und handschriftlichen Notizen rekonstruiert werden. Da die Dokumentation des Handelns und der angetroffenen Situation wesentlich für die Nachvollziehbarkeit und Überprüfbarkeit des Handelns der Verwaltung ist, hat sie einen hohen Anteil an der Verwaltungstätigkeit, gerade im Außendienst und in der Ordnungsverwaltung. In der Gewerbeaufsicht bedeutet dies, dass Betriebsdaten, personenbezogene Daten von Unternehmern und Beschäftigten sowie Geschäftsgeheimnisse betroffen sein können. Durch die Verlagerung der Verarbeitung auf Arbeitsumgebungen außerhalb der Behörden wächst die Gefahr, dass diese Informationen in unbefugte Hände gelangen. Der technische Schutzaufwand ist daher zu intensivieren.

Der Informationszugriff und die Informationsbearbeitung werden durch unterschiedliche Faktoren beeinflusst. Bestimmt sind sie vor allem durch Verfahrensvorschriften oder die Tatbestandsmerkmale des materiellen Rechts, die bestimmte Dokumentationsinhalte und deren Bearbeitungsreihenfolge vorgeben, und den Zugriff auf aktuelle Vorschriften und individuelle Regelungsmöglichkeiten erforderlich machen. Rechtliche Anforderungen, auch der Datenschutz, sind aber nur ein Teil der zu beachtenden Faktoren bei der Einführung mobiler Datenverwendung. Weitere Faktoren eher praktischer Art ergeben sich aus den Umweltkontexten, der bereits vorhandenen Verwaltungsinfrastruktur und Software sowie aus den Arbeitsbedingungen vor Ort.

2 Umgebungsfaktoren und Ergonomie

Die mobile Dokumentation in der Gewerbeaufsicht findet im Betrieb statt. Die ergonomischen Bedingungen, unter denen die Dokumentation stattfindet, unterscheiden sich grundsätzlich von Dateneingabe und -abruf an einem Büroarbeitsplatz. In Verbindung

¹ Eine empirische Untersuchung unter Unternehmen mit einem hohen Anteil an Außendienstmitarbeitern hat ebenfalls ergeben, dass eine nicht ausgereifte Technik, insbesondere offene technische Sicherheitsfragen und unzureichende Qualität der Dienste, der Hauptgrund für das Nicht-Einsetzen sowie den rückgängigen Einsatz mobiler Technologien im Außendienst sind. [Fa06, 62 und 67] Auch offene nicht-technische Sicherheitsfragen sowie ungeklärte rechtliche Aspekte können den Umfang des Einsatzes bzw. die Entscheidung über den Einsatz negativ beeinflussen. [Fa06, 63]

² In der Gewerbeaufsicht wird beispielsweise seit mehreren Jahren und bereits in 12 Bundesländern für den Arbeitsschutz die Fachanwendung IFAS (Informationssystem für die Arbeitsschutzaufsicht) der Kisters AG eingesetzt.

mit der Ergonomie der Endgeräte können Umgebungsfaktoren die Nutzung bestimmter Ein- und Ausgabemöglichkeiten wesentlich beeinflussen. Zu den Umgebungsfaktoren gehören u.a. das (Nicht-)Vorhandensein von Ablagemöglichkeiten für mobile Endgeräte, Lärm, Unruhe sowie wechselnde Lichtverhältnisse. Fehlende Ablagemöglichkeiten und die geringe Endgerätegröße³ erfordern alternative Eingabe- und Steuerungsmöglichkeiten neben der Eingabe über die Tastatur. Denkbar sind Spracheingabe und -steuerung oder Handschrifterkennung. Auf den ungeschützten Endgeräten kann die Displayanzeige, die auch wechselnde Sichtbedingungen kompensieren muss, leicht durch Dritte eingesehen werden. Die Ausgabe von Informationen durch Sprachausgabe kann problematisch sein, wenn z.B. Maschinengeräusche das Verfolgen der Sprachausgabe erschweren. Auch die Anwesenheit Dritter kann aufgrund des potentiellen Mithörens interner Informationen ebenfalls der Sprachausgabe entgegenstehen [FGK06]. Dies könnte jedoch durch den Einsatz von Kopfhörern reduziert werden.

In der Umgebung eines Betriebes und auf Mobilgeräten sind die Daten zudem viel stärker als in einem Büro verlustgefährdet, etwa durch Hinfallen des Notebooks oder das Eindringen von Feuchtigkeit, auch wenn Tough- oder Outdoor-Notebooks hier bereits Schutz bieten. Dies würde für einen Einsatz der Notebooks als reines Terminal mit permanenter Verbindung zum Verwaltungsserver oder zum Behördenarbeitsplatz sprechen.⁴ Andererseits stehen nicht zuletzt Produktionshallen mit Störquellen, eventuell starkem Mauerwerk und ähnlich ungünstigen Beschaffenheiten einer permanenten drahtlosen Konnektivität entgegen. Nicht zu vergessen ist die Gefahr des Datenverlusts oder der Datenverfälschung durch unerkannte Übertragungsfehler oder Systemabstürze, die eine entsprechende Prüfung verhindern. Dies schließt die bloße Terminalnutzung des Endgerätes schon aus praktischen Gründen aus und erfordert Synchronisierungsmechanismen. Auch die Übertragungssicherheit erfordert keine Terminallösung. Die Sicherung durch eine VPN-Verbindung mit einer starken Authentifizierungskomponente und an die Authentifizierung gebundenen Zugriffsrechten ist genauso in der Lage, die notwendige Sicherheit zu gewährleisten.⁵

Eine andere Frage betrifft die Informationsaufnahme und -weitergabe vor Ort, in eventuell unsicheren Kontexten. Die elektronische Verfügbarkeit vor Ort und das Ziel medienbruchfreier Informationsaufnahme legt es nahe, Schnittstellen zu schaffen, die es zulassen, Informationen gleich vor Ort elektronisch weiterzugeben oder Informationen von Zusatzgeräten wie Messgeräten, Fotoapparaten oder RFID Chips unmittelbar, am besten drahtlos aufzunehmen. Die damit verbundenen Geräteschnittstellen schaffen aber auch Angriffspunkte für den unbefugten Zugriff auf dort gespeicherte sensible Inhalte.

Die Anpassung der Geräte an die Einsatzumgebung und an ergonomische Erfordernisse hat damit unmittelbare Auswirkung auf die Art und Weise des Umgangs mit Informatio-

³ Um das Gewicht gering und das Gerät handlich zu halten, andererseits aber die Arbeit mit Fachanwendungen und vielfältige andere Nutzungsmöglichkeiten zu ermöglichen, dürften sich kleine 12“ Tablet PCs als am besten geeignet erweisen.

⁴ So das nach Auffassung des LfD Niedersachsen zumindest für mobile Telearbeit vorzugswürdige Modell. [[LfD03]

⁵ Siehe hierzu die sehr gut gesicherte VPN-Lösung des Informatikzentrum Niedersachsen, Sicherer Zugang in das Landesdatennetz. http://www.izn.niedersachsen.de/master/C6021088_N5557516_L20_D0_I3654280.html.

nen sowie auf Fragen der Datensicherheit.

3 Rechtliche Faktoren

Aus rechtlicher Sicht ergibt sich zudem, dass die einführenden Verwaltungsträger aus ihrer Fürsorgepflicht als Arbeitgeber, nach dem Arbeitsschutzgesetz⁶ und auch durch die Notwendigkeit, im Einvernehmen mit dem Personalrat zu handeln,⁷ ergonomische Belange berücksichtigen müssen. Damit gewinnen die bereits aufgezählten Faktoren teilweise eine nicht nur praktische sondern auch rechtliche Bedeutung.

Die Gewerbeaufsicht bzw. die ausführenden Beamten sind spezialgesetzlich durch § 23 Abs. 2 ArbSchG und § 139b GewO sowie als Verwaltungsbehörde allgemein durch § 30 VwVfG und § 5 BDSG⁸ zur Geheimhaltung der erlangten Informationen verpflichtet. Soweit es sich um personenbezogene Daten handelt, stellt außerdem § 9 BDSG samt Anhang konkrete technische und organisatorische Anforderungen auf. Diese sind auch für mobile Datenerhebung und -verarbeitung relevant. Die Aufzählung des Anhangs enthält ohne abschließend gemeint zu sein Maßnahmenvorschläge und -ziele. Dazu gehören die Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Auftrags-, Verfügbarkeits-, Eingabe- oder Verantwortungskontrolle sowie die Trennungsmöglichkeit der Daten nach Erhebungszwecken. Diese sind technisch auch für das mobile Endgerät und seinen Einsatz umzusetzen, wobei zu beachten ist, dass die erforderlichen Sicherheitsmaßnahmen möglichst gut mit den Anforderungen des mobilen Arbeitens harmonisieren sollten.

Durch die Einführung mobiler Endgeräte, die den elektronischen Arbeitsplatz in den Betrieb verlagern, entstehen außerdem völlig neue Gefahrenlagen für Geheimnisschutz und Datensicherheit [LfD03]. Durch den Verlust des Endgeräts, den Einblick in gespeicherte Daten, den Zugriff auf Datensammlungen und Vorgangsbearbeitungssysteme und das Ausspionieren drahtloser Kommunikation bestehen zusätzliche Möglichkeiten für Dritte, sich unbefugten Zugang zu Verwaltungsdaten zu verschaffen und diese eventuell sogar zu manipulieren [RK07]. Teilweise stehen die potentiellen Gefahren im unmittelbaren Zusammenhang mit den praktischen oder ergonomischen Erfordernissen. Ein Beispiel bildet der oben geschilderte Umstand, dass ein reibungsloses mobiles Arbeiten mit Blick auf die nicht jederzeit gesicherte Konnektivität eine reine Terminallösung ohne Speicherung oder Verarbeitung auf dem Endgerät nicht erlaubt. Hierdurch müssen in größerem Umfang Daten auf dem Endgerät vorgehalten werden. Ein anderes Beispiel ist die Notwendigkeit, das Endgerät mit zahlreichen, vor allem drahtlosen Schnittstellenmöglichkeiten zu versehen, um eine schnelle Informationsaufnahme zu fördern.

⁶ Siehe die Grundpflichten nach §§ 3 f. ArbSchG.

⁷ Durch die Einführung mobiler Endgeräte und die Umgestaltung der Arbeitsweise können etwa das Ordnungsverhalten, die Gestaltung des Arbeitsplatzes oder die Leistungsüberwachung durch Geräte und damit die Mitbestimmungsrechte de § 75 Abs. 3 Nr. 15, 16 und 17 BPersVG, das hier stellvertretend für die entsprechenden Landesregelungen betrachtet wird, betroffen sein.

⁸ Die Nennung des Bundesrechts erfolgt hier wie auch im Weiteren stellvertretend für die weitgehend inhaltsgleichen Landesvorschriften.

Eine in Intervallen erforderliche Authentifizierung des Nutzers, ein Sich-Deaktivieren des Gerätes in längeren Nutzungspausen, Sicherungen gegen Dateneinblick bei abhanden gekommenen Geräten wie etwa Festplattenverschlüsselung, eine Sicherung der drahtlosen Übermittlung sowie ein gesonderter Zugangsschutz des Servers gehören zu den wichtigsten rechtlichen Anforderungen an die Technik. Hier ist zu beachten, dass einige der mobil vorzugswürdigen Eingabeformen, etwa Schrift- und Spracherkennung, durchaus auch als biometrische Merkmale und damit als Sicherheitsmechanismen eingesetzt werden können. Auf diese Weise könnte permanent festgestellt werden, ob die befugte Person das Endgerät bedient. Generell sind vor allem die Sicherungsmaßnahmen direkt am Endgerät zu verstärken. Vielfach sind die notwendigen Sicherheitsmechanismen bereits vorhanden und praktisch erprobt. Doch hinsichtlich des mobilen Einsatzes der Sicherheitsmittel, der Anpassung an den mobilen Arbeitskontext und der Besonderheiten mobiler Arbeit besteht weiterer Entwicklungsbedarf.

4 Gestaltung der Anwendungssysteme

Unter einem Anwendungssystem wird eine Kombination aus Hard- und Software verstanden, die zur Erfüllung bestimmter Aufgaben eingesetzt wird. Anwendungssysteme müssen aufgabenangemessen gestaltet sein. In der Gewerbeaufsicht gehören zu den Aufgaben eines Mitarbeiters neben der Überprüfung von Betrieben auch Beratungen, Gremienarbeiten sowie das persönliche Informations- und Wissensmanagement. Für den Mitarbeiter der Gewerbeaufsicht wird das mobile Endgerät daher ein wesentliches und sehr wichtiges Arbeitsgerät zur effizienten Erfüllung vielfältiger und unterschiedlicher Aufgaben.⁹ Er wird daher einerseits auf bereits bestehende Fachanwendungen zurückgreifen, aber auch nutzerspezifische Einstellungen und Dateien verwalten wollen.

Für die sichere Gestaltung von Anwendungssystemen zur mobilen Arbeit innerhalb der Verwaltungen liegen bereits Checklisten der Landesbeauftragten für den Datenschutz (s. Niedersachsen) vor [LfD03]. Diese beinhalten zwar bereits wesentliche Aspekte, gehen aber immer noch stark von der Situation bei der Telearbeit aus. Ein wesentlicher Aspekt ist der, dass der Mitarbeiter keine Administratorrechte hat, so dass bestimmte Wartungs- und Konfigurationsmöglichkeiten nur durch einen zentralen Administrator vorgenommen werden können. Die zentrale Administration kann jedoch nur einige Sicherheitsaspekte berücksichtigen (Virens Scanner, Firewall, Passwörter, Konfiguration der Festplattenverschlüsselung, Verbindungsaufbau etc.). Auf der anderen Seite ist hier aber zu berücksichtigen, dass das Endgerät an persönliche Arbeitsweisen seines Besitzers anpassbar sein soll.

Für den Umgang mit Sicherheitsrisiken, die bei der mobilen Nutzung entstehen, könnte das mobile Endgerät den Kontext erkennen und auf der Grundlage von festgelegten Kontext-Regeln entsprechende Maßnahmen treffen, so bspw. Zugriffe erlauben oder

⁹ An dieser Stelle sollte auch bedacht werden, dass die Möglichkeit, ein derart optimierbares System einsetzen zu können, sich auch positiv auf die Motivation des Mitarbeiters auswirkt.

verbieten [Ec06, 28].¹⁰ Im Fall der Gewerbeaufsicht erscheint denkbar, bei dem Zugriff den Aufenthaltsort des Aufsichtsbeamten über die bei der Verbindung anfallenden Standortdaten zu bestimmen und nur an üblichen Arbeitsorten und im Bereich des überprüften Betriebes dessen Daten zugänglich zu machen.¹¹

Ein wesentliches Kriterium für die Gestaltung ist die Nutzerakzeptanz. Für eine mobile Umgebung ist zu vermeiden, dass die Anwendungssysteme durch lange Ladezeiten, Fehler oder falsche Reaktionen die Bearbeitung verzögern oder zu fehlerhafter Bearbeitung führen. Genauso ist darauf zu achten, dass nicht die Sicherheitsmechanismen (vom Virenschutzprogramm bis hin zur Festplattenverschlüsselung), vor allem in ihrem Zusammenwirken, die Arbeit mit dem Gerät behindern oder stark verlangsamen.

Als funktionale Anforderungen lassen sich die folgenden identifizieren: alternative Eingabemöglichkeiten (Schrift- und Spracherkennung), alternative Ausgabemöglichkeiten (Text, Sprache), Sprachsteuerung, Schnittstellen für den Datenaustausch mit anderen Geräten (z.B. drahtlose Übertragung durch RFID oder Bluetooth), Datensicherung (lokal, serverseitig), alternative Authentifizierungsmöglichkeiten sowie Synchronisationsmöglichkeiten. Nicht-funktionale (qualitative) Anforderungen leiten sich überwiegend aus den rechtlichen Aspekten sowie den Nutzerbedürfnissen ab. Folgende nicht-funktionale Anforderungen lassen sich identifizieren: geringe Ladezeiten, geringe Rechenzeiten, schnelles Antwortzeitverhalten und Dokumentationseignung.

4 Fazit

Die Entwicklung mobiler Anwendungen für die mobile Verwaltung weist große Potentiale, aber auch neue Risiken aufgrund der Einführung neuer Technologien und anderer Arbeitskontexte auf. Die Risiken ergeben sich aus den Umgebungsfaktoren, die im jeweiligen Kontext angetroffen werden, aus ergonomischen Gestaltungsanforderungen sowie aus weiteren Gefahren für die Datensicherheit, die im mobilen Umfeld entstehen. Die Informationstechnik muss zum einen die hohen Sicherheitsanforderungen, zum anderen auch die Bedürfnisse mobiler Arbeit erfüllen. Die Wahl und Gestaltung der Sicherheitskomponenten ist an die Arbeitskontexte anzupassen. Dies gilt nicht nur für das gewählte Beispiel der Gewerbeaufsicht, sondern kann auf sämtliche Kontrolltätigkeiten der Verwaltung sowie andere M-Government-Anwendungen übertragen werden.

Die Gefahrenpotentiale können durch eine optimale Technikgestaltung sowie durch Verhaltenshinweise reduziert werden. Technische Lösungen stehen teilweise schon bereit; die Herausforderung liegt in der Anpassung der Technologien an die besonderen Anforderungen mobiler Verwaltungsaußendiensttätigkeit und in der Zusammenführung der verschiedenen Technologien und Produkte, ohne gegenseitige Störungen und Zielkonflikte. Weiterhin müssen Methoden entwickelt werden, die die Definition von Sicherheitsrisiken und damit verbundenen Anforderungen an die mobilen Systeme verein-

¹⁰ Hierbei handelt es sich um ein Forschungsthema des Instituts Fraunhofer SIT.

¹¹ Eine offene Frage aus praktischer Sicht bleibt allerdings die Arbeit auf Reisen oder an unvorhergesehenen Orten, die nicht völlig ausgeschlossen werden soll.

fachen.

Anders als bei der computergestützten Bürotätigkeit muss für das mobile Arbeiten intensiv bei der Gestaltung des mobilen Endgerätes angesetzt werden. Dies betrifft neben Sicherheitsmechanismen auch die Individualisierung und aufgabenspezifische Anpassung des Endgerätes. Das Endgerät ersetzt die Mitnahme von Informationen, es authentifiziert den Mitarbeiter, es nimmt Informationen auf und seine Gestaltung beeinflusst das Verhalten der Mitarbeiter. Es ist der Vermittler zwischen Mitarbeiter und Verwaltung und wird unentbehrlicher Bestandteil des Außendienstes werden. Damit steigt aber auch die Abhängigkeit von dem Gerät. Somit ist Gestaltung mobiler Verwaltungsarbeit ganz wesentlich Gestaltung der Soft- und Hardware des mobilen Endgerätes.

Literaturverzeichnis

- [Ec06] Eckert, C.: Geschützter Datenverkehr. Gespräch mit Prof. Dr. habil. Claudia Eckert, Leiterin des Fraunhofer-Instituts für Sichere Informationstechnologie SIT in Darmstadt. Fraunhofer Magazin 2.2006. S. 28-30. http://www.fraunhofer.de/fhg/Images/magazin2-2006_28_tcm5-60879.pdf, Abruf am 07.07.2006.
- [Fa06] Faupel, T.: Hindernisse beim Datenzugriff mittels mobiler Kommunikationstechnologie – Eine empirische Analyse. In: Kiste, T.; König-Ries, B.; Pousttchi, K.; Turowski, K. (Hrsg.): Mobile Informationssysteme – Potentiale, Hindernisse, Einsatz. Proceedings 1. Fachtagung Mobilität und Mobile Informationssysteme (MMS). Passau, 20.-22. Februar 2006. S. 57-67
- [FGK06] Frankfurth, A.; Gerstheimer, O.; Knopp, M.: The Need for Suitable User Interfaces for Mobile Devices. Proceedings Euro mGov 2006, i.E.
- [Le05] Lenk, K.: Vielfalt der Geschäftsprozesse in der öffentlichen Verwaltung. In: Klichschewski, Ralf; Wimmer, Maria (Hrsg.): Wissensbasiertes Prozessmanagement im E-Government. In der Reihe: Lenk, Klaus; Brüggemeier, Martin; Reichard, Christoph: E-Government und die Erneuerung des öffentlichen Sektors. Band 4. LIT Verlag. Münster 2005. S. 43-55
- [RK07] Roßnagel, A.; Knopp, M.: Mobilisierte Verwaltung: Rechtliche Perspektiven und Gestaltungsbedarf, DÖV 07, i.E.
- [LfD03] Landesbeauftragter für den Datenschutz Niedersachsen, Mobiles Arbeiten - datenschutzgerecht gestaltet - Orientierungshilfe und Checkliste, 2003.
- [WTL01] Wimmer, M.; Traummüller, R.; Lenk, K.: Besonderheiten in der Gestaltung von e-Government Prozessen. 2001. <http://falcon.ifs.uni-linz.ac.at/lvas/ss/ppt-egov/wimmeretal.pdf>, Abruf am 2005-06-09.