

Bundesamt für Sicherheit in der Informationstechnik



Phasenplan E-Government

Phase 3 “Analyse”

Der hier vorliegende Text ist ein Modul aus dem

E-Government-Handbuch

<http://www.e-government-handbuch.de>

Redaktion: Projektgruppe E-Government im
**Bundesamt für Sicherheit in der
Informationstechnik (BSI)**

Kontakt: egov@bsi.bund.de



Inhaltsverzeichnis

3	Phase 3 – „Analyse“	4
3.1	Aktivität „Systematische Prozessaufnahme“	5
3.2	Aktivität „Festlegung behördenkritischer Prozesse“, „erweiterte Prozessaufnahme“	11
3.3	Aktivität „Prozessoptimierung“	13
3.4	Aktivität „E-Government-spezifische Schutzbedarfsfeststellung“	16
3.5	Aktivität „Ableiten der Sicherheitsanforderungen“	24
3.6	Aktivität "Gestaltung des Online-Prozesses"	27
3.7	Aktivität "Vorabprüfung rechtlicher Rahmenbedingungen"	30
3.8	Aktivität „Überprüfung der Bewertungen aus Phase 2 hinsichtlich Aufwand und Nutzen“	32
3.9	Aktivität „Aktualisierung der E-Government-Strategie“	34
3.10	Aktivität "Information aller Betroffenen"	36
7	Checklisten	38
7.3	Checkliste für Phase 3	38
9	Autorendarstellung	39

Informationen zum Modul

Status	BSI-Beitrag
Autor	Belz, Dr. Mrugalla u. a. (BSI)
Ansprechpartner / Kontakt	Herr Belz (BSI), egov@bsi.bund.de

Änderungsverzeichnis

Datum	Name	Änderung
07.07.2005	Belz	Geringfügige Aktualisierung
14.02.2005	Herbolsheimer	Redaktionelle Überarbeitung
26.10.2004	Dr. Hauschild	Anpassung im Zuge der Veröffentlichung des Moduls „Sichere Kommunikation im E-Government“
08.10.2004	Dr. Hauschild	Geringfügige Anpassung im Zuge der Veröffentlichung der Module „Sichere Zahlungsverfahren im E-Government“ (noch nicht abgeschlossen) und „Vorgangsbearbeitungssysteme als Basistechnologie für E-Government“
18.03.2004	Horn	Geringfügige Anpassung im Zuge der Veröffentlichung des Moduls „Barrierefreies E-Government“
16.12.2002	Dr. Hauschild	Einarbeitung von Änderungsvorschlägen der Autoren des Moduls „Authentisierung im E-Government“ – weitere Überarbeitung folgt im Zusammenhang mit der Veröffentlichung von Phase 5 oder 6.
13.02.2002	Horn	Redaktionelle Überarbeitung
19.12.2001	Belz, Dr. Mrugalla u. a.	Erstellung erste Version

Das Werk einschließlich aller Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urhebergesetzes ist ohne Zustimmung des Bundesamtes für Sicherheit in der Informationstechnik unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

© 2005

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn

3 Phase 3 – „Analyse“

Die Phase 3 des E-Government-Einführungsprozesses wird durch die inhaltlich-organisatorische Aufbereitung der identifizierten online-fähigen Dienstleistungen bestimmt. Der Schwerpunkt der Aktivitäten liegt auf der Erfassung und Optimierung der Tätigkeiten in einer Geschäftsprozess-Analyse. Danach werden Randbedingungen, wie der Schutzbedarf und die Sicherheitsanforderungen für die geplanten Dienstleistungen bestimmt. Die präsentierte Vorgehensweise enthält außerdem unverzichtbare Elemente einer Gemeinkostenwert-Analyse. Alle Arbeitsvorgänge werden hierbei im Hinblick auf die spätere Abbildung in IT-Verfahren untersucht.

Darüber hinaus erfolgt eine Überprüfung der in Phase 2 begonnenen Machbarkeits- sowie Wirtschaftlichkeitsbetrachtungen sowie eine vorläufige rechtliche Prüfung. Abschließend ist geplant, die gewählte E-Government-Strategie zu überarbeiten und zu ergänzen.

Um die spätere Umsetzung der Innovationen zu garantieren, werden die Soll-Konzepte zusammen mit den betroffenen Mitarbeitern erarbeitet. Die Vorgehensweise erfordert eine enge Zusammenarbeit zwischen Organisations- und IT-Referaten, die ihre Arbeitsergebnisse der Behördenleitung zur Entscheidung vorlegen. Eine offene Informationspolitik soll die behördeninterne Akzeptanz der mit der Einführung von E-Government verbundenen Veränderungen sicherstellen.

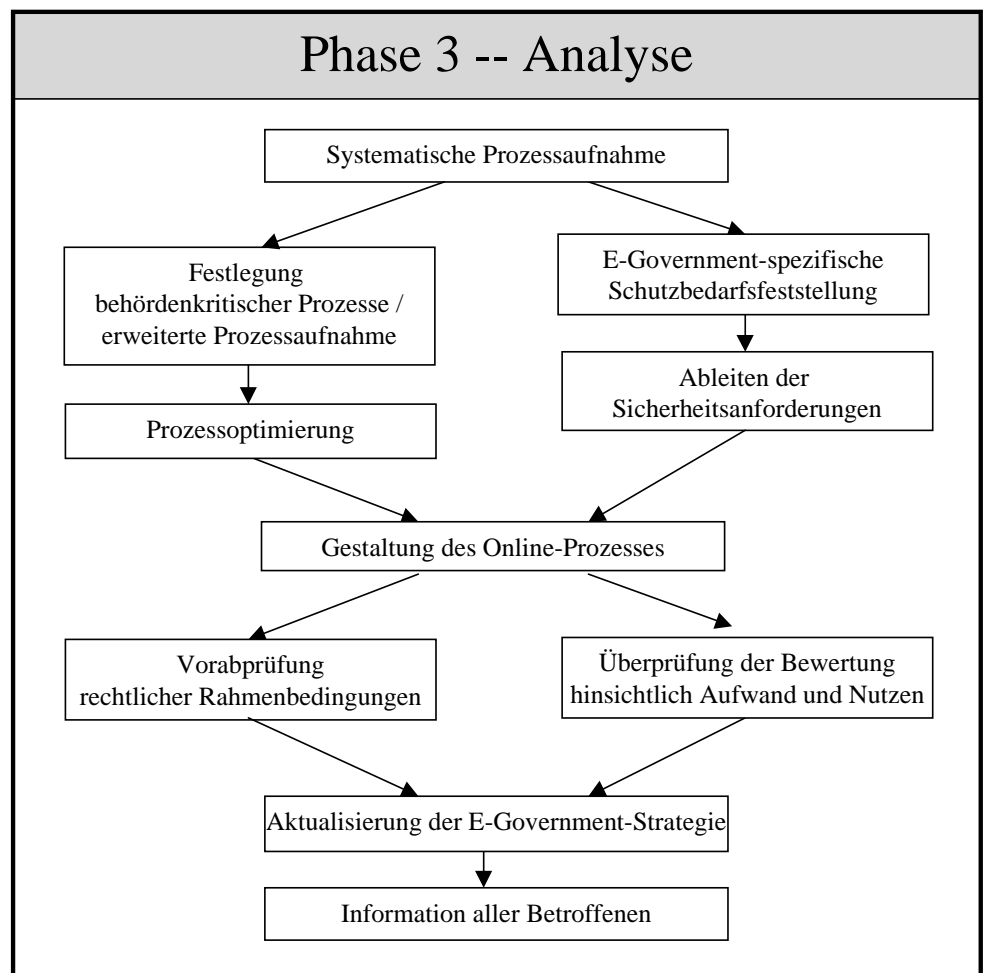


Abbildung 1: Ablaufplan Phase 3 – Analyse

3.1 Aktivität „Systematische Prozessaufnahme“

Initiierung: Teamleiter

Durchführung: Kernteam, Organisationsreferat, Personalvertretung
(Begleitung)

Prozessaufnahme im E-Government

Im öffentlichen Bereich wird der Handlungsrahmen für die Gestaltung der Behördenziele in der Regel durch die bestehenden Gesetze und den konkreten Behördenauftrag definiert. Zudem ist der finanzielle Rahmen durch den öffentlichen Haushalt geregelt. Im Gegensatz zu Wirtschaft und Industrie ist es systembedingt nicht möglich, durch eine Steigerung der Kundennähe und -akzeptanz gewinnorientiert bestehende Verfahren zu optimieren.

Gestaltungsrahmen, Schwerpunkte

Unterstellt man zudem, dass der Bürger als Kunde der öffentlichen Hand in erster Linie erwartet, dass die ihm gesetzlich zustehenden Leistungen schnell, kostengünstig und zuverlässig angeboten werden, so wird klar, dass die notwendige E-Government-Analyse in erster Linie auf eine Effizienzsteigerung abzielen wird; eine mehr oder weniger umfangreiche Prozessanalyse und -optimierung ist in aller Regel unumgänglich.

Die Erhebung potenziell online-fähiger Dienstleistungen in Phase 2 wurde auf der Grundlage existierender Arbeitspapiere aus der bestehenden Aufbau- und Ablauforganisation der Behörde durchgeführt. Um den o. g. Anforderungen von E-Government gerecht zu werden, ist jedoch eine prozessorientierte Betrachtungsweise notwendig. Dafür wird eine Beschreibung der Arbeitsabläufe (einschließlich Informationsfluss) benötigt, die es ermöglicht, Schwachstellen und Verbesserungspotentiale des herkömmlichen Verfahrens sowie Einsatzmöglichkeiten einer elektronischen Vorgangsbearbeitung zu identifizieren. Außerdem ist es Zweck dieser Prozessdokumentation, Medienbrüche zu erkennen und zu eliminieren.

Betrachtungsweise

Steht bereits zum Abschluss der Phase 2 fest, dass behördenweit ein Workflow-Verfahren eingesetzt werden soll, ist es vorteilhaft, den Aufwand für die „klassische“ Prozessaufnahme zugunsten der erwünschten Optimierung für ein IT-Verfahren in Phase 4 gering zu halten. Unter „klassische“ Prozessaufnahme ist hier insbesondere der Teil der Beschreibung und Optimierung der papiergestützten Bearbeitung und des Transports innerhalb der erforderlichen Teilprozesse zu verstehen.

Hierbei ist von Anfang an die Einbindung der zuständigen Personalvertretung geboten, da die Ergebnisse geeignet sind, Rückschlüsse auf die betroffenen Arbeitsplatzinhaber (Möglichkeit der Leistungs- und Verhaltenskontrolle) zu ziehen. Dies gilt unabhängig davon, mit welchem Aufnahmeverfahren die Untersuchung durchgeführt wird (Interviewtechnik, Beobachtungen am Arbeitsplatz, Durchlaufzettel, Fragebogen, Workshops). Bei automatisierten

Beteiligung der Personalvertretung

Erhebungsweisen ist die frühzeitige Beteiligung der Personalvertretungen stets erforderlich.

Prozessorientierte Analysen eröffnen im Gegensatz zu funktions- oder aufgabenorientierten Analysen gute Möglichkeiten für ein kontinuierliches Verbesserungswesen. Der Mitarbeiter wird aktiv in das Verfahren zur Gestaltung und Optimierung der Prozesse eingebunden. Dadurch dass der Mitarbeiter angehalten wird, seine Arbeit aus Sicht des internen oder externen Kunden zu betrachten, entsteht mehr gegenseitiges Verständnis und langfristig auch mehr Mitarbeiterzufriedenheit. Durch die Grundidee passende Objektgrößen zu modellieren, die ein Prozessverantwortlicher im Überblick hat, bilden Prozessanalysen zudem die Grundlage für eine Aufgabenbewältigung in flachen Hierarchien. Dies entspricht im allgemeinen auch den Kunden-/Bürgerwünschen für eine schlanke, effiziente und kostengünstige Verwaltungsstruktur.

**Prozessanalyse
für Modernen
Staat**

Für die Prozessanalyse und Prozessoptimierung können Ergebnisse der Organisationsreferate aus vergangenen Untersuchungen mit ähnlicher Zielsetzung genutzt werden. Es könnte beispielsweise der Fall sein, dass Teilbereiche der Behörde bereits nach Vorgaben und Methoden der REFA-Analyse untersucht wurden oder dass für die Realisierung eines effektiven Controlling bereits Standardisierungsansätze ähnlich der DIN-/ISO-Normen (9000, 9001 ff.) erarbeitet wurden. In der Regel ist es sinnvoll, auch auf das Know-how der Mitarbeiter vorangegangener Analysen zurückzugreifen.

**Synergieeffekte
nutzen**

Vor der Prozessaufnahme ist zu klären, welche Gestaltungsziele in der Vergangenheit zu Organisationsänderungen geführt haben. Interessenkonflikte könnten beispielsweise durch die in Phase 2 ermittelten Prioritäten für die Umsetzung der Behördenziele in Bezug auf Haushaltsmittel und Personalressourcen entstehen, falls gleichzeitig Maßnahmen für die Steigerung der Mitarbeitermotivation oder für Controlling vorgesehen sind.

**Berücksichtigung
neuer
Steuerungsinstru-
mente**

In aller Regel dürften sich die E-Government-Analyse und die Anwendung neuer Steuerungsinstrumente (Instrumente zu Effizienzsteigerung und Qualitätskontrolle z. B. Kosten- und Leistungsrechnung, Controlling, Zielvereinbarungen, Vorschlagswesen, Konzepte zur Kompetenzsteigerung) gegenseitig ergänzen. Die neuen Steuerungsinstrumente, auf der einen Seite, dienen vorrangig der Optimierung der reinen Entscheidungsprozesse. Die E-Government-Analyse, auf der anderen Seite, strebt in erster Linie Effizienzsteigerungen innerhalb der einzelnen Dienstleistungen an und dient somit als Voraussetzung für die Online-Bereitstellung von Dienstleistungen. Falls behördenintern bereits IT-Verfahren für den Einsatz neuer Steuerungsinstrumente implementiert wurden, ist bei der Modellierung der E-Government-Dienstleistungen darauf zu achten, dass Schnittstellen zu diesen Verfahren eröffnet werden, damit keine inkompatiblen oder für den Benutzer schwierig zu handhabenden Verfahren geplant werden.

Sollten dennoch Zielkonflikte zwischen E-Government und neuen Steuerungsinstrumenten zu erkennen sein, so ist es dringend ratsam, diese vor Beginn der Prozessaufnahme zu diskutieren und auszuräumen.

Selbst wenn bereits in der Vergangenheit Organisationsanalysen durchgeführt wurden, die die Grundlage für einen schnellen Einstieg in die Problematik bilden, ist der Zeit- und Personalaufwand, sowie die Dauer einer Analyse auf

**Faktoren für den
Analyseumfang**

Prozessebene nicht zu verkennen. Projekte, die eine umfassende Restrukturierung und Optimierung zum Ziel haben, dauern in der Regel mehrere Jahre und sind sehr personalintensiv. Der Umfang der Untersuchungen ist stark abhängig von dem bereits vorhandenen IT-Durchdringungsgrad in Relation zur Zahl der geplanten Online-Dienstleistungen. Der benötigte Aufwand der Analyse hängt entscheidend von der vorgesehenen Detailtiefe ab. Die im weiteren beschriebene Vorgehensweise ist tragfähig für Analysen mittlerer Detailtiefe. Soweit aus strategischen Vorgaben eine Analyse mit hohem Detaillierungsgrad notwendig ist, ist die Vorgehensweise anzupassen. Hierauf wird in der nachfolgenden Aktivität „Identifizierung behördenkritischer Prozesse, erweiterte Prozessaufnahme“ eingegangen.

Auch Analysen mittleren Volumens sollten dabei in der Regel nicht ohne Unterstützung einschlägiger Software-Produkte durchgeführt werden, da sonst der Aufwand für das spätere IT-Design kaum zu leisten ist. Sollte der Gesamtaufwand die Beschaffung spezieller Analyse-Software nicht rechtfertigen, ist mindestens der Einsatz einer Projekt-Ablauf-Software empfehlenswert. Falls ein Re-Design der Abläufe für Behördenteile (insbesondere Personalverwaltung und Kostenmanagement) bereits mit speziellen Modulen oder Programm-Paketen realisiert wurde, ist unter Wirtschaftlichkeitsgesichtspunkten der Einsatz dieser Produkte auch für die E-Government-Analyse zu prüfen.

**Projektmanagem
ent mit Software-
Unterstützung**

Zuordnung von Dienstleistungen zu Prozessen

Die in Phase 2 ausgewählten online-fähigen Dienstleistungen werden in dieser Aktivität den übergeordneten Behördenaufgaben als Prozesse zugeordnet. In Abgrenzung zu der in Phase 2 durchgeführten Aktivität „Identifikation notwendiger Infrastruktur-Verfahren“ geht es hierbei um die Bündelung von Dienstleistungen, die ähnliche Abläufe haben (z. B. sämtliche Beratungsanfragen). Ziel ist es, Tätigkeitsketten (Prozesse) zu identifizieren, die *ein* Bearbeiter (Prozessverantwortlicher) möglichst von Anfang bis Ende alleine bearbeiten kann. Die innerhalb eines solchen Prozesses erzielten Arbeitsergebnisse sollten also nicht durch mehrere Sachbearbeiter erreicht und anschließend von einem Vorgesetzten unterschrieben werden; die Verantwortung für das Resultat, für das Ergebnis der Abarbeitung des Prozesses, soll bei nur einer Person liegen.

Prozesse

Ziel der Identifikation von Prozessen ist es, eine grundsätzlich objektorientierte Organisation zu etablieren. Dadurch soll eine qualitative Verbesserung der Dienstleistungen erreicht werden. Ein externer Kunde findet einen eindeutigen Ansprechpartner vor; Vorgesetzte werden von Routinearbeiten entlastet und können sich voll auf ihre Leitungs- und Koordinierungsfunktion konzentrieren.

Werden im Zuge der Prozess-Modellierung Delegationsmöglichkeiten ausgeschöpft, können Effizienzsteigerungen erreicht werden. Verrichtungsspezialisierte Dienstleistungs-Pools sollten nicht grundsätzlich ausgeschlossen werden, aber deren Wirtschaftlichkeit muss eingehend geprüft werden.

Im Zuge der Identifikation von Prozessen sollte, ohne viel Aufwand zu betreiben, eine Zuordnung der bestehenden Tätigkeiten zu „virtuellen Funktionseinheiten“ vorgenommen werden. Dies ermöglicht, sich losgelöst von bestehenden

hierarchischen Strukturen über die theoretischen Möglichkeiten einer Restrukturierung bewusst zu werden. In der Realität wird sich ein so radikales Re-Design der Hierarchien innerhalb einer Behörde in der Regel nicht umsetzen lassen.

1. Jede online-fähige Dienstleistung wird auf Tätigkeitsebene zerlegt. Tätigkeiten sind z. B. Beraten, Prüfen, Analysieren, Recherchieren, Entscheiden. (Subprozesse bilden)
2. Zusammenfassung der in Schritt 1 erhaltenen Tätigkeiten in Gruppen mit gleichem Tätigkeitsinhalt, unabhängig von der Organisationseinheit (Referat), die die Dienstleistung erbringt. Funktionsinhalte richten sich nach dem Adressaten der Dienstleistung (Output an Bürger, Behörden, Wirtschaft).

Beispiel: Alle Beratungsdienstleistungen der Behörde, in denen der Bürger beraten wird, bilden eine Gruppe. (Fachthema 1, ..., n). Alle Dienstleistungen, in denen dem Bürger nur fertige Arbeitsergebnisse als Information vermittelt werden, werden der Gruppe Öffentlichkeitsarbeit zugewiesen.

Sofern die output-bezogene Gruppierung nicht möglich ist, sollte nach inhaltlich-logischen Bezügen gruppiert werden.

Beispiel: Alle Dienstleistungen der Behörde, die Kontakt mit ordentlichen Gerichten erfordern, werden der Gruppe Justitiariat zugeordnet.

Die Prozesse der Behörde werden klassifiziert in:

- Kernprozesse (Hauptaufgaben der Behörde)
- Unterstützungsprozesse (interne Verwaltungsaufgaben)

Eine weitere Aufgliederung, etwa in Lenkungsprozesse (Aufgaben der Entscheider, wie z. B. Personalführung) oder nach Kundenrollen ist aus hiesiger Sichtweise für die Ziele der E-Government-Analyse nicht erforderlich. Unterstützungsprozesse dürften nur im Einzelfall zu untersuchen sein, da sie nicht im Vordergrund der E-Government-Initiative stehen. Deren Untersuchung kann trotzdem sinnvoll und notwendig sein, falls es sich abzeichnet, dass ein behördenweit einheitliches Workflow-System eingesetzt werden soll.

Prozessarten

Abgrenzung zur umfassenden Prozessanalyse

Visualisierung der Prozesse

Gleichzeitig mit der inhaltlichen Aufnahme der Prozesse und Teilprozesse ist es sinnvoll, deren logische Verknüpfungen zu visualisieren. Diese Visualisierung erlaubt es, die wichtigen Abläufe und Verknüpfungen der Handlungen mit einem Blick zu erfassen. Es sollte modellhaft nachvollziehbar sein, welche Entscheidungen getroffen werden und welche Aktionen auf diese Entscheidungen folgen (müssen).

Verzweigungen entstehen insbesondere dann, wenn Ja-Nein- bzw. Oder-Entscheidungen vorliegen, die unterschiedliche Aktionen nach sich ziehen. Um später Optimierungsansätze zu ermitteln, sollte auch erkennbar sein, wann

Visualisierung in Flussdiagramm

Entscheidungsträger wechseln und wie der Transport der Informationen erfolgt. Anfang und Ende einer visualisierten Ereigniskette sollten durch identifizierte Teilprozesse abzugrenzen sein. Schnittstellen zwischen Prozessen sollten inhaltlich erläutert werden.

In der Regel sind mindestens die Teilprozesse zu markieren, die zwingend notwendig sind, um den Folgeprozess zu initialisieren.

Beispiel für einen Prozess / Definition Teilprozess

Produktzertifizierung

Prozess –
Teilprozess

Teilprozesse des Prozesses **Produktzertifizierung**:

Auftragsbestätigung

Funktionale Prüfung

Prüfung auf Einhaltung der Toleranzwerte

Patentrecherche

Gutachtenerstellung

Zertifikatserstellung

Veröffentlichung

Teilprozesse werden auf der Ebene von „Meilensteinen“ für die Erreichung des Prozessziels dargestellt, nicht auf einem Detaillierungsgrad, der sich der Tätigkeitsebene (Tätigkeit im Sinne von einzelnen Verrichtungen, Handgriffen) nähert. Teilprozesse sind durch den Ersteller abgrenzbare Vorgänge, die einen sinnvoll abzugrenzenden In- und Output haben. Aus den einzelnen Teilprozessen muss sich ableiten lassen:

Inhalt der
Teilprozesse,
Definition

- Name des Teilprozesses. Z. B. **Auftragsbestätigung**
- Kurze Ablaufbeschreibung der Arbeitsschritte. Wo findet ein Medienbruch statt?
- Wer ist für die Erstellung verantwortlich, Eigentümer des Teilprozesses? Hier sollte eine Rolle, nicht eine Person zugeordnet werden. Z. B. technischer Sachbearbeiter, Informatiker oder Jurist.
- Verwendete Arbeitsmittel/Medium für den Output. Z. B. Textverarbeitungsprogramm xy, Tabellenkalkulation xy oder Papier/Bleistift
- Benötigte Hilfsmittel/Medium. Z. B. Gesetz/Vorschriftensammlung xy (Papierform), Adressenverzeichnis xy (Datei/Tabellenformat xy), Kurstabelle (HTML-Internet), Telefon oder Fax
- Bestimmung des Aufwands für den Teilprozess. Z. B.: Mittlere Bearbeitungsdauer des Teilprozesses/Häufigkeit. Gegebenenfalls Zuordnung zu Kostenstellen.

Erhebung der
Teilprozesse

- Empfänger von Kopien des Outputs. Z. B. Sachbearbeiter für Beschaffung, Justitiariat, Abteilungsarchiv Z
- Schwachstellen aus Sicht des Eigentümers des Teilprozesses. Z. B. häufige Verzögerungen durch Nichterreichbarkeit der Kunden-Hotline, (zu) langsamer Verbindungsaufbau der Internet-Verbindung.

Hilfsmittel im E-Government-Handbuch:

- Modul „Vorgangsbearbeitungssysteme als Basistechnologie für E-Government“

3.2 Aktivität „Festlegung behördenkritischer Prozesse“, „erweiterte Prozessaufnahme“

Initiierung: Teamleiter

Durchführung: Kernteam, Organisationsreferat, Behördenleitung

Für die Festlegung behördenkritischer Prozesse werden die in der Aktivität „Systematische Prozessaufnahme“ (Aktivität 3.1) erfassten Prozesse ausgewertet, um Prozesse zu identifizieren, die aus wirtschaftlicher oder strategischer Sicht von elementarer Bedeutung sind. Behördenkritische Prozesse sind individuell für jede Behörde festzustellen. Dies können Prozesse sein, die durch ihre Häufigkeit oder Komplexität einen hohen Anteil der Personalressourcen binden. Es können auch Prozesse sein, die aufgrund ihrer finanziellen oder politischen Bedeutung essentiell für die Existenz der Behörde sind. Behördenkritische Prozesse aufgrund ihrer quantitativen Bedeutung lassen sich aus der Prozessaufnahme ableiten (Aufwand für den Teilprozess, Bearbeitungsdauer).

**Feststellung
behördenkritischer
Prozesse**

Qualitative Bewertungskriterien sind ableitbar aus der Aktivität "Festlegung der Qualitätsanforderungen für Online-Dienstleistungen" (Phase 2), z. B. die Festlegung eines sehr kurzen Antwort-Zeitverhaltens. Zusätzliche Anhaltspunkte für die qualitative Bewertung behördenkritischer Prozesse lassen sich auch aus der parallel angesetzten Aktivität „E-Government-spezifische Schutzbedarfsfeststellung“ (Aktivität 3.4) entnehmen (z. B. hohe oder sehr hohe Anforderungen an Vertraulichkeit, Integrität, Verfügbarkeit).

Es ist zu entscheiden, ob für die identifizierten behördenkritischen Prozesse eine gegenüber der Aktivität „Systematische Prozessaufnahme“ (Aktivität 3.1) erweiterte Prozessaufnahme mit höherem Detaillierungsgrad anzuwenden ist. Eine höhere Detailtiefe ist insbesondere für die Beschreibung der Arbeitsabläufe sowie für die Bearbeitungsdauer und -häufigkeit innerhalb der Teilprozesse denkbar. Je kritischer die Bedeutung des Prozesses, desto höher sollte die anzuwendende Detailtiefe sein.

**Detailanalyse
erforderlich?**

Für die Anwendung eines höheren Detaillierungsgrades ist es erforderlich, innerhalb der Teilprozesse die *Arbeitsvorgänge* zu identifizieren, die für die Bewertung als behördenkritischer Prozess (Kritikalität) entscheidend sind, sei es durch Häufigkeit oder durch ihre qualitative Bedeutung für den Prozess. Unter Arbeitsvorgängen sind einzelne Bearbeitungsschritte (Ablaufbeschreibung der Arbeitsvorgänge ist Bestandteil jedes Teilprozesses in der Prozessaufnahme) innerhalb der Teilprozesse zu verstehen.

Kritikalität

Quantitativ bedeutende Arbeitsabläufe lassen sich durch organisatorische Erhebungsmethoden/Beobachtungstechniken messen. Dazu zählen Techniken wie die Multi-Moment-Aufnahme. Die Anwendung dieser Techniken sollte nicht ohne theoretische und praktische Kenntnisse geeigneter Vorgehensweisen erfolgen (z. B. REFA-Methoden, näheres unter <http://www.refa.de>). Gegebenenfalls lassen

Erhebungstechniken

sich durch diese Methoden Kennzahlen ermitteln, die für ein späteres Benchmarking genutzt werden können.

Beispiele

Der Prozess „Produktzertifizierung“ besteht aus sieben Teilprozessen. Die Häufigkeit der Geschäftsvorfälle liegt bei 60 Stück pro Jahr. Die Summe der Bearbeitungszeiten für die Teilprozesse liegt bei 2 Millionen Arbeitsminuten pro Jahr. Dadurch werden derzeit 33 Mitarbeiter (von insgesamt 120 Mitarbeitern der Behörde) in verschiedenen Hierarchieebenen für die Erledigung des Prozesses eingesetzt. Aufgrund der quantitativen Bedeutung entscheidet die Behördenleitung, den Prozess als behördenkritischen Prozess zu klassifizieren. Eines der Behördenziele aus Phase 2 ist es Rationalisierungspotentiale zu entfalten. Zwei der Teilprozesse binden über 50 Prozent der Bearbeitungsdauer für den Gesamtprozess. Diese Teilprozesse werden zusätzlich zu dem durchgeführten Mitarbeiterinterview noch weiter untersucht. Es wird entschieden, diese Arbeitsabläufe genau zu beschreiben und einzeln durch die Erhebungstechnik Multi-Moment-Aufnahme zu bewerten, um so bei den Teiltätigkeiten detailgenauere Möglichkeiten für Optimierungsansätze zu erhalten.

1. **Behördenkritischer Prozess aufgrund qualitativer Bedeutung**

In der Behörde XY sind insgesamt 1.500 Mitarbeiter tätig. Die Behörde hat eine Abteilung, in der 400 Mitarbeiter Bürger-/Kundenanträge bearbeiten, 350 der 400 Mitarbeiter sind als Sachbearbeiter eingesetzt. Es werden 22.000 Anträge pro Jahr bearbeitet, die Kundendatei umfasst 130.000 Kunden. Die Kundenanträge betreffen alle das selbe Rechtsgebiet, *ein* Gesetz ist die Grundlage für die Bescheide, die erteilt werden. Die Bearbeitung der Anträge erfolgt mit einer Textverarbeitung, die durchschnittliche Bearbeitungsdauer liegt bei 28 Kalendertagen, von Eingang des Antrags bis zur Absendung des schriftlichen Bescheids per Post. Der Kunde erhält auch bei längerer Bearbeitungsdauer keinen Zwischenbescheid.

2. **Behördenkritischer Prozess aufgrund quantitativer Bedeutung**

In Phase 2 wurde entschieden, die Dienstleistung online zu stellen. Die Behördenleitung hat als Qualitätsmerkmal festgelegt, dass der Bürger spätestens innerhalb von fünf Kalendertagen eine Rückmeldung über den Eingang des Antrags erhalten soll. Die Gesamtbearbeitungsdauer soll 21 Kalendertage nicht überschreiten.

Aufgrund der quantitativen Bedeutung des Prozesses entscheidet die Behördenleitung, den Prozess als behördenkritischen Prozess zu klassifizieren. Zusätzlich wird entschieden, eine Detailanalyse der Arbeitsvorgänge durchzuführen. In Verbindung mit der „Elektronifizierung“ des Verfahrens soll auch eine inhaltliche Überarbeitung der Sacharbeit erfolgen, um die Qualität des Verfahrens zu steigern. Die getroffene Entscheidung soll dem Bürger transparenter gemacht werden. Die Inhalte sollen einheitlicher gestaltet werden.

3.3 Aktivität „Prozessoptimierung“

Initiierung: Teamleiter

Durchführung: Kernteam, Organisationsreferat, Personalreferat

Die Aktivität beginnt mit der Auswertung der Ergebnisse der Prozessaufnahme. Offensichtliche Ziele für Optimierungsansätze lassen sich aus den in Phase 2 durchgeführten Aktivitäten „Festlegung der Bewertungskriterien für online-fähige Dienstleistungen“ und „Festlegung der Qualitätsanforderungen für Online-Dienstleistungen“ ableiten.

**Generelle
Optimierungsansätze**

Aus den begrenzten Zielen der E-Government-Initiative dürfte unter dem bestehenden Zeit- und Kostendruck ein radikales Redesign der Prozesse in der Regel nicht in Frage kommen.

**Kein radikales
Redesign**

Es ist erfolgversprechend, zunächst durch einen fachkundigen Organisator zu markieren, wo Schwachstellen in den identifizierten Teilprozessen auftreten. Typische Schwachstellen sind beispielsweise:

Schwachstellenanalyse

- Lange Bearbeitungsdauer
- Lange Liegezeiten
- Häufiger Mitarbeiterwechsel innerhalb eines Prozesses
- Medienbrüche innerhalb der Prozesse

Im ersten Optimierungsschritt sollten grundsätzliche, überwiegend quantitative Verbesserungsmöglichkeiten durch IT-Einsatz berücksichtigt werden. Darunter fallen insbesondere zeitliche Beschleunigungen durch Wegfall von Transportzeiten, durch elektronische Weiterleitung und Verkürzung von Liegezeiten, durch zentrale Datenhaltung, Archive, Wiedervorlagen und Ablagen. Außerdem sollte, unter Berücksichtigung des jeweiligen Aufwands, die schrittweise Beseitigung von Medienbrüchen geprüft werden.

**Quantitative
Optimierungen
durch IT-Einsatz**

Mit Hilfe von Workshops oder Mitarbeiterbefragungen sollten die *Ursachen* für vermutete Schwachstellen herausgefunden werden. Workshops sind als moderne Kommunikationsplattform geeignet für die Untersuchung, weil durch den direkten Zugriff auf die Kompetenz und das Fachwissen der Mitarbeiter mit vergleichsweise geringem Aufwand sehr schnell Lösungsansätze erarbeitet werden können. Um hochwertige Ergebnisse zu erhalten, müssen Workshops gut vorbereitet und zielgerichtet moderiert werden. Sie sollten mit den faktisch handelnden Personen innerhalb der Teilprozesse und nicht mit den Prozessverantwortlichen durchgeführt werden. Die betroffenen Mitarbeiter erhalten so die Chance zur Äußerung. Dies ist zur Erhaltung der Motivation und für kreative Lösungsansätze als Basis für einen stetigen Verbesserungsprozess unumgänglich. Eine verordnete Prozesskritik und Restrukturierung ausschließlich durch Vorgesetzte oder „Sachverständige“ hat sich in der Praxis nicht bewährt. Die Mitarbeiter und die zuständige Personalvertretung sollte vorab darüber informiert werden, dass die Prozesskritik und die Aufdeckung von

**Partizipation der
Mitarbeiter in
Workshops**

Schwachstellen nur zu Zwecken der E-Government-Analyse und nicht zur Kontrolle der Mitarbeiter genutzt werden. Der Zugriff auf alle Erhebungsdaten ist entsprechend zu schützen, die Daten vertraulich zu behandeln.

Die Workshops sollten durch einen Organisator moderiert werden, der Potenziale von Lösungsansätzen der Mitarbeiter beurteilen kann. Seine Aufgabe besteht außerdem darin, Ansätze für Standardisierungen (Kundenkontakt, Anschreiben, Berichte, Statistiken) zu erkennen und darauf zielgerichtet hinzuweisen. Da das Ziel die Online-Bereitstellung der Dienstleistung ist, muss er in der Lage sein, den handelnden Personen die im ersten Schritt ermittelten grundsätzlichen Verbesserungsmöglichkeiten durch gezielten IT-Einsatz zu präsentieren. Langfristig ist das Ziel, möglichst viele Arbeits- und Hilfsmittel ohne Medienbruch zu integrieren.

Qualifikation des Moderators

Die in den Teilprozessen handelnden Personen entwickeln über die Prozesskritik verbesserte Soll-Konzepte für die künftige Aufgabenbewältigung. In der Prozesskritik werden insbesondere die erfassten Arbeitsabläufe innerhalb der Teilprozesse und die Schwachstellen aus Sicht des Anwenders diskutiert. Die Fragestellungen sollten berücksichtigen:

Prozesskritik unverzichtbar

- Wie kann ein Teilprozess vereinfacht (Formulare, Textbausteine) oder standardisiert werden?
- Wo finden Doppelarbeiten (Mehrfacherfassung) statt?
- Werden Delegationspotentiale (Zeichnungsbefugnis) ausgeschöpft?
- Welche Fehler sind in der Praxis aufgetreten?
- Bestehen einheitliche Verfahrensvorgaben? Können bei einheitlicher Ausgangssituation unterschiedliche Ergebnisse entstehen, insbesondere durch unklare, fehlende oder widersprüchliche Verfahrensanweisungen? Entsteht dadurch eine Ungleichbehandlung, insbesondere im juristisch relevanten Sinne?
- Wie viel Zeit wird für Vorbereitungsarbeiten investiert? Sind alle Hilfs- und Arbeitsmittel lokal und zeitgerecht verfügbar?
- Ist der Bearbeiter mit dem Verfahren und dem Arbeitsergebnis zufrieden?

Bei der Generierung der Soll-Konzepte ist die Qualifikation und Leistungsfähigkeit der Mitarbeiter zu berücksichtigen. Der Moderator des Workshops sollte qualitative Verbesserungsinhalte und Erweiterungen durch organisatorische oder elektronische Verfahren initiieren:

Soll-Konzept

- Poolbildung für Wissen und Kompetenz
- Benchmarking für gleiche Tätigkeiten
- Vorstellung von Möglichkeiten für Reporting, Monitoring, Controlling. Festlegung des Prozessverantwortlichen
- Verfahrensbeschleunigung durch parallele Teilprozesse
- Einsatzmöglichkeiten für Projektarbeit
- Entlastung von Routinearbeiten durch IT-Einsatz

Wenn möglich sollten alle Änderungen bzw. Änderungsvorschläge bereits im Workshop aufgenommen werden. Gegebenenfalls können Stichworte notiert werden, die später inhaltlich ausgestaltet werden.

Nachdem so ein Soll-Konzept für die optimierten Teilprozesse erstellt wurde, ist zu klären, ob sich die Rolle des Bearbeiters entscheidend geändert hat. Falls das erarbeitete Profil nicht mit der Qualifikation der Mitarbeiter übereinstimmt, ist ein Qualifizierungskonzept vorzubereiten, welches im Verlauf der E-Government-Analyse erweitert und verfeinert werden sollte. Hierzu ist eine Abstimmung zwischen Organisations- und Personalreferat sinnvoll. Gegebenenfalls sind Möglichkeiten für Outsourcing zu prüfen, z. B. falls exotische Kenntnisse oder Fähigkeiten in geringem Umfang benötigt werden.

Qualifizierungskonzept

Alle messbaren Differenzen, z. B. bei Verfahrensbeschleunigungen (Zeitgewinn), sollten dokumentiert und bewertet werden. Gleiches gilt für erwartete Zeitaufwände für Verfahrensoptimierungen.

3.4 Aktivität „E-Government-spezifische Schutzbedarfsfeststellung“

Initiierung: Leiter E-Government-Team

Durchführung: Kernteam, IT-Sicherheitsbeauftragter, Datenschutzbeauftragter, Justitiariat

Im Zuge der Einführung von E-Government sollen bestehende Dienstleistungen so umgesetzt werden, dass ein bedeutender Anteil der notwendigen Kommunikation zwischen Kunden und Behörde über das Internet abläuft. Ziel dieser Aktivität ist es, für jede in Phase 2 identifizierte online-fähige Dienstleistung zu definieren, welchen Schutzbedarf die ihr zu Grunde liegende Kommunikation induziert. Die herausragenden zu betrachtenden Sicherheitsziele sind die Vertraulichkeit und Verbindlichkeit (Authentizität, Integrität und und Nicht-Abstreitbarkeit). Unverzichtbare Voraussetzung für das Funktionieren von E-Government ist ferner die Verfügbarkeit der technischen Systeme auf Behördenseite (z. B. Web-Server). Für rechtsverbindliche Transaktionen ist zudem der Aspekt des Schriftformerfordernisses zu berücksichtigen.

Einführung
Schutzbedarf

Das hier dargestellte Vorgehen, die so genannte E-Government-spezifische Schutzbedarfsfeststellung, betrachtet ausschließlich die *Kommunikation* zwischen Kunden und Behörde und damit die Schnittstellen der Online-Dienstleistung. Eine umfassende Schutzbedarfsfeststellung, z. B. nach IT-Grundschutz (IT-Grundschutzhandbuch, <http://www.bsi.bund.de/gshb>, Kapitel 2.2), die von der eingesetzten IT ausgeht und dabei sowohl den Kunden-PC, die technische Realisierung des Kommunikationskanals als auch die Behörden-IT (Web-Server, Hintergrundsystem) berücksichtigt, wird in Phase 4 vorgenommen.

Als Orientierungshilfe werden im Folgenden Schutzbedarfsklassen definiert. Da der Schutzbedarf meist nicht unmittelbar quantifizierbar ist, beschränkt sich die Definition auf eine qualitative Aussage. In Anlehnung an das IT-Grundschutzhandbuch werden fünf¹ Schutzbedarfsklassen definiert, in die sich der Schutzbedarf einordnen lässt:

Schutzbedarfs-
klassen

Schutzbedarfsklasse	Ausprägung der Schutzbedarfsklasse
kein	Ein besonderer Schutz ist nicht notwendig, da keine Schadensauswirkungen zu erwarten sind.
niedrig	Die Schadensauswirkungen sind eng begrenzt.
mittel	Die Schadensauswirkungen sind begrenzt und überschaubar.
hoch	Die Schadensauswirkungen können beträchtlich sein.
sehr hoch	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Tabelle 1: Schutzbedarfsklassen

¹ Im IT-Grundschutzhandbuch wird nicht zwischen „niedrig“ und „mittel“ unterschieden, daher sind dort lediglich vier Klassen definiert. Durch die Vielzahl möglicher Authentisierungs-Mechanismen ist insbesondere bei diesem Schutzziel eine feinere Unterteilung sinnvoll.

Unter Schadensauswirkungen sind hier auf Kundenseite insbesondere Auswirkungen auf die **gesellschaftliche Stellung** oder auf die **wirtschaftlichen Verhältnisse des Kunden** (z. B. Beeinträchtigung des informationellen Selbstbestimmungsrechts, Beeinträchtigung der persönlichen Unversehrtheit, finanzielle Auswirkungen) zu verstehen.

Schadensauswirkungen

Auf Behördenseite stehen das **gesetzmäßige Verwaltungshandeln** (z. B. Verstoß gegen Gesetze/Vorschriften/Verträge) und ein damit verbundener **Imageverlust** (z. B. negative Außenwirkungen) im Vordergrund. Andere Auswirkungen (z. B. **Beeinträchtigung der Aufgabenerfüllung, finanzielle Auswirkungen**) sind denkbar. Dabei sind insbesondere die finanziellen Auswirkungen nicht generell in absoluten Zahlen zu quantifizieren.

Zur Schutzbedarfsfeststellung für die Kommunikation in einem Fachverfahren werden zunächst die möglichen Schadensszenarien analysiert und die potenziellen Schadensauswirkungen den einzelnen Schutzbedarfsklassen zugeordnet (Tabelle 2, für eine genauere Erläuterung siehe auch das Modul „Authentisierung im E-Government“). Je höher die Schutzbedarfsklasse, desto wichtiger ist der Schutz vor dem jeweiligen Schadensszenario.

Schutzbedarfsfeststellung

Schutzbedarfsklasse	kein	niedrig	mittel	hoch	sehr hoch
Schadensauswirkungen					
beim Kunden:					
„gesellschaftliche Stellung“					
„wirtschaftliche Verhältnisse“					
bei der Behörde:					
„gesetzmäßiges Verwaltungshandeln“					
„Imageverlust“					
„Beeinträchtigung der Aufgabenerfüllung“					
„finanzielle Auswirkungen“					

Tabelle 2: Schutzbedarfsfeststellung

Im Folgenden werden für die relevanten Sicherheitsziele Hinweise und Beispiele gegeben, wie für Online-Dienstleistungen eine adäquate Schutzbedarfsklasse ermittelt werden kann. Bei einer komplexen Dienstleistung können durchaus mehrere Übertragungen in jede Richtung stattfinden. Die Schutzbedarfsfeststellung sollte in einem ersten Schritt für jede solche Übertragung getrennt durchgeführt werden, da oft ein unterschiedlich hoher

Schutzbedarf umzusetzen ist. Insbesondere wird es in der Regel einen Unterschied der Anforderungen zwischen Input- und Output-Phase geben.

Verfügbarkeit (der technischen Systeme auf Behördenseite)

Online-Dienstleistungen können nur genutzt werden, wenn die technischen Systeme auf Behördenseite verfügbar sind. Es ist für jede Dienstleistung zu prüfen, in welcher Zeit-Größenordnung ein Ausfall der Systeme akzeptabel ist. Dabei bietet sich folgende Einteilung an:

niedrig bis mittel: Eine Ausfallzeit der Online-Dienstleistung von mehr als 24 Stunden kann toleriert werden.

hoch: Eine Ausfallzeit der Online-Dienstleistung zwischen einer und 24 Stunden wird als tolerabel eingeschätzt.

sehr hoch: Die maximal tolerierbare Ausfallzeit der Online-Dienstleistung liegt unter einer Stunde.

Vertraulichkeit

Werden Daten zwischen Kunden und Behörde ausgetauscht, so ist es in vielen Fällen notwendig, sicherzustellen, dass diese nicht von unberechtigten Dritten mitgelesen werden; die *Vertraulichkeit* der übertragenen Daten muss geschützt werden. Im herkömmlichen papiergestützten Verfahren wird dies in der Regel durch die Verwendung von Briefumschlägen sichergestellt.

Folgende Beispiele erläutern die vorzunehmende Einordnung:

kein: Allgemeine Informationen; konventionelle Übermittlung durch Veröffentlichung in Broschüren / Zeitungen / allgemein zugänglichen Medien oder Versand per Postkarte.

niedrig: Gering schützenswerte personenbezogene bzw. firmenvertrauliche Daten (z. B. Familienstand, Geburtsdaten); konventionelle Übermittlung durch Versand per Postkarte oder Brief.

mittel: Eingeschränkt schützenswerte personenbezogene bzw. firmenvertrauliche Daten (z. B. Daten zur Lebenshaltung); konventionelle Übermittlung durch Versand per verschlossenem Brief.

hoch: Personenbezogene bzw. firmenvertrauliche Daten (z. B. Steuerangelegenheiten, Mahnbescheide); konventionelle Übermittlung durch Versand per verschlossenem Brief.

sehr hoch: Besonders schützenswerte personenbezogene bzw. firmenvertrauliche Daten (z. B. medizinische Daten über Patienten, Schriftverkehr rund um Konkurs, Pfändung); konventionelle Übermittlung üblicherweise durch Versand per Postzustellungsurkunde oder persönliche Übergabe.

Neben der Festlegung der Schutzbedarfsklasse sollte aber auch geklärt werden, wer innerhalb der Behörde die Daten sehen darf. Oder anders formuliert: müssen die Daten vertraulich bis zu einem bestimmten Mitarbeiter gelangen? Dies würde automatisch bedeuten, dass eine Ende-zu-Ende-Verschlüsselung vorgenommen

werden muss, eine Ende-zu-Organisation-Kommunikation also nicht möglich ist. Siehe hierzu auch das Modul „Sichere Kommunikation im E-Government“.

Die zu beantwortenden Fragen lauten also:

- Wie hoch ist der Schutzbedarf in Bezug auf Vertraulichkeit?
- Wem dürfen im Rahmen der Dienstleistung verarbeitete sensitive Informationen zugänglich sein? Wem sind sie im Rahmen der traditionellen Abwicklung zugänglich?
- Wird eine Ende-zu-Ende-Verschlüsselung ausdrücklich benötigt?
 - Wenn nein: können die Daten nach eventueller zentraler Entschlüsselung innerhalb der Behörde unverschlüsselt an den Bearbeiter weitergeleitet werden oder müssen sie erneut verschlüsselt werden?
- Kenne ich die elektronische Anschrift des Kunden im Falle von E-Mail-Kommunikation (Adressierbarkeit)?

Verbindlichkeit

Unter dem Sammelbegriff Verbindlichkeit von Daten verstehen wir im E-Government eine Kombination aus Integrität, Authentizität und Nicht-Abstreitbarkeit. Im Rahmen der Schutzbedarfsfeststellung empfiehlt es sich, diese Aspekte zunächst getrennt voneinander zu betrachten und, falls sinnvoll, anschließend zusammenzufassen.

Verbindlichkeit als Sammelbegriff

Letztlich gilt es also zu beurteilen, wie wichtig es ist, dass die Daten vom angegebenen Absender bzw. Autor stammen, dass sie unterwegs nicht verändert wurden und dass nachweisbar ist, dass sie auch wirklich gesendet wurden. Erstrebenswert sind diese Ziele immer; es hängt jedoch in hohem Maße von dem möglichen Schaden ab, der im Falle eines Missbrauchs entstehen kann, ob Maßnahmen ergriffen werden müssen, um die Einhaltung der Schutzziele auch wirklich sicherzustellen oder zu überprüfen. Und hier greift die Schutzbedarfsfeststellung.

Folgende Fragen müssen daher beantwortet werden:

- Wie sicher müssen sich die Kommunikationspartner sein, dass die Daten unverändert und authentisch sind (Schutzbedarf bezüglich Authentizität und Integrität der Daten)?
- Ist es notwendig, dass einer der Kommunikationspartner gegenüber Dritten nachweisen kann, dass er die Daten gesendet oder erhalten hat (Schutzbedarf bezüglich Nicht-Abstreitbarkeit)? Siehe hierzu auch die späteren Ausführungen zum Schriftformerfordernis.
- Ist es notwendig, den Zeitpunkt des Erhalts oder des Versands einer Nachricht nachweisen zu können?
- Wie sicher müssen sich die Kommunikationspartner über die Identität des jeweils anderen sein (Schutzbedarf bezüglich Authentizität der Kommunikationspartner)?

- Ist es notwendig, dass die Authentizität des Kommunikationspartners vor Erbringung der Dienstleistung überprüft wird² (Ex-ante-Authentifizierung) oder reicht eine nachträgliche Überprüfungsmöglichkeit (Ex-post-Authentifizierung)?

Betrachten wir einige Aspekte ein wenig genauer:

Werden Daten übertragen, so ist sicherzustellen, dass diese nicht auf dem Übertragungsweg verändert werden; ihre *Integrität* bedarf eines gewissen Schutzes. Eine Veränderung kann hierbei sowohl durch technische Fehler (unbeabsichtigt) als auch durch gezielte Manipulation (beabsichtigt) entstehen. Erstere Veränderung ist zu erkennen, wenn die durch Übertragungsfehler veränderten Daten keinen Sinn mehr ergeben (z. B. beliebige Zeichenketten).

Integrität (der übertragenen Daten)

Streng genommen ist es immer wichtig, dass Daten nicht verändert werden³. Insofern sind hier einerseits die Auswirkungen bei einer Veränderung und andererseits die Wahrscheinlichkeit, dass diese Daten gezielt manipuliert werden, abzuschätzen.

Die Fragestellung der Datenintegrität spielt in den papiergestützten Verfahren nur eine sehr geringe Rolle, da eine Veränderung von auf Papier niedergeschriebenen Inhalten in der Regel nicht unbemerkt vorgenommen werden kann. Hier ergibt sich ein anderes Gefährdungspotenzial als bei den IT-gestützten Verfahren.

Alle Daten, die gerichtsverwertbar aufbewahrt werden sollen, müssen im Schutzbedarf „Integrität“ mindestens „hoch“ eingeordnet werden.

Folgende Beispiele mögen die Einordnung erläutern:

niedrig: Allgemeine Informationen (z. B. Verfahren der Dienstleistungserbringung, Öffnungszeiten).

mittel: Informationen für einen eingeschränkten Benutzerkreis (z. B. Terminänderungen von Versammlungen).

hoch: Steuererklärung, Steuerbescheid

sehr hoch: Daten, die zu automatischen Handlungen oder zu Hilfseinsätzen führen (Alarmierung Rettungsdienst/THW), Ermittlungsdaten der Polizeien.

Es ist ferner zu prüfen, inwieweit es notwendig ist, die übersandten Daten ihrem Absender zuzuordnen zu können. Dies betrifft sowohl die *Authentizität* der kommunizierten Daten, d. h. die für den Empfänger verlässliche Zuordnung zum vermeintlichen Absender, als auch die *Nicht-Abstreitbarkeit*, also die gegenüber Dritten beweisbare Zuordnung. Hierbei sind wiederum beide Kommunikationsrichtungen zu berücksichtigen, also sowohl vom Kunden zur

Authentizität und Nicht-Abstreitbarkeit (der übertragenen Daten)

² Dies ist insbesondere dann von Bedeutung, wenn bei der Erbringung der Dienstleistung ein irreparabler Schaden entstehen kann (z. B. Preisgabe von Informationen über schwerwiegende Erkrankungen oder Vorstrafen an Dritte).

³ Dies gilt nicht nur für die eigentliche Übertragung sondern auch für eine eventuelle Speicherung vor bzw. nach der Übertragung.

Behörde (Input, z. B. Kunden-Antrag, -Anfrage), als auch von der Behörde zum Kunden (Output, z. B. Bescheid, Antwort oder Anforderung der Behörde).

In papiergebundenen Verfahren werden die Authentizität und die Nicht-Abstreitbarkeit in der Regel durch Unterschrift bzw. Dienstsiegel sichergestellt.

Folgende Beispiele erläutern die Einordnung:

kein: Der Abruf allgemeiner Informationen (z. B. Verfahren der Dienstleistungserbringung, Öffnungszeiten) ist ohne Nennung des Namens möglich.

niedrig: Für die Vereinbarung eines persönlichen Beratungsgesprächs beim Bauamt ist das Themengebiet und ggf. die Telefonnummer des Gesprächspartners relevant.

mittel: Die Mitteilung über die Änderung der Bankverbindung, auf die eine monatliche geringe Förderung überwiesen wird, sollte nur der Förderberechtigte vornehmen können.

hoch: Die Mitteilung über die Änderung der Bankverbindung, auf die eine einmalige hohe Summe überwiesen wird, darf nur der Förderberechtigte vornehmen können.

sehr hoch: Bei der Aushändigung des Personalausweises ist persönliches Erscheinen unter Vorlage eines Dokuments zur Authentisierung erforderlich. Der Erhalt des Ausweises wird gegengezeichnet (Nicht-Abstreitbarkeit).

Die Nutzung von Online-Dienstleistungen setzt oft voraus, dass Behörde und Kunde sich „erkennen“ können. Einerseits möchte sich die Behörde vor der Übersendung von Dokumenten sicher sein, dass der Kunde ist, wer er vorgibt zu sein. Auf der anderen Seite muss es auch dem Kunden möglich sein, zu erkennen, dass sein Kommunikationspartner (E-Mail- oder Web-Adresse) wirklich die gewünschte Behörde ist.

Authentizität der
Kommunikationsp
artner

Auch diese Aufgabenstellung ist in der Papier-Welt weniger anspruchsvoll, da ein Großteil des Datenaustauschs per Post vorgenommen wird, Postadressen aber im Gegensatz zu Web- und E-Mail-Adressen in der Regel nicht frei wählbar und nicht beliebig schnell wechselbar sind.

Ist der *Vertraulichkeitsbedarf* der übertragenen Daten „hoch“ oder „sehr hoch“, so gilt diese Einstufung auch für die Authentizität der Behörde. Folgende Erläuterungen und Beispiele sollen die Einordnung erleichtern:

kein: Die Kommunikationspartner können ungenannt bleiben.

niedrig: Die Behauptung der Identität reicht aus, z. B. lediglich Angabe von Name und Adresse des Kommunikationspartners oder Abdruck eines Behördenlogos (allgemeine Informationen der Behörde, einfache Anfragen, die auch telefonisch vorgenommen werden könnten).

mittel: Die Identität lässt sich plausibel nachprüfen, z. B. durch Angabe weiter gehender Informationen wie Aktenzeichen, Bezug auf vorangegangene Kommunikation.

hoch: Die Identität der Kommunikationspartner lässt sich verbindlich nachprüfen.

sehr hoch: Die Identität der Kommunikationspartner wird vorab zweifelsfrei geprüft (z. B. durch Vorlage Personalausweis, bei Zustellung einer Postzustellungsurkunde).

Schriftformerfordernis

Erhoben werden muss an dieser Stelle auch, ob ein Schriftformerfordernis besteht, da dieses direkten Einfluss auf die einzusetzenden Sicherheitsmechanismen hat. Wichtig ist dabei festzuhalten, ob es eine ausdrückliche Abweichung gegenüber der Generalaussage im Verwaltungsverfahrensgesetz gibt, die Schriftform und elektronische Form (elektronische Kommunikation unter Verwendung einer qualifizierten elektronischen Signatur) gleichsetzt. Abweichungen hiervon sind nach oben wie nach unten möglich.

Die elektronische Umsetzung eines Schriftformerfordernisses ist rechtlich geregelt.

Gibt es keine solche rechtliche Grundlage, werden aber in der herkömmlichen Vorgehensweise Unterschriften gefordert, so ist der Zweck der Unterschriften zu hinterfragen. Gegebenenfalls kann auf die Unterschrift verzichtet werden.

Zu klärende Fragen:

- Wird für diesen Kommunikationsschritt die Schriftform gefordert? Ist diese rechtliche Vorgabe notwendig oder kann das Gesetz/die Verordnung kurzfristig geändert werden (Prozessoptimierung, Bürokratieabbau)?
- Gibt es in den zu Grunde liegenden Gesetzen und Verordnungen eine darüber hinausgehende Anforderung (z. B. dauerhafte Aufbewahrung)?
- Gibt es eine Abschwächung (z. B. durch das Wortpaar „schriftlich oder elektronisch“⁴)?
- Wenn keine Schriftform: Werden in diesem Kommunikationsschritt im konventionellen Verfahren Unterschriften eingesetzt? Wenn ja, zu welchem Zweck? Wodurch könnten sie ersetzt werden?

Sonstige Aspekte

Wenn auf Bestandsdaten zugegriffen werden soll oder muss, müssen Authentisierungs-Daten entweder direkt oder durch Kombination mit Identifikations-Daten geeignet sein, die Bestandsdaten ausfindig zu machen.

Eindeutigkeit der Abbildung auf die Bestandsdaten

Dies ist insbesondere dann von Bedeutung, wenn zur Erbringung der Dienstleistung ein Datenzugriff auf Kunden-Bestandsdaten erforderlich ist. Hierzu müssen die Identifikations- bzw. Authentisierungs-Daten eine eindeutige Zuordnung ermöglichen. Dabei ist zu beachten, dass

- es zu den Bestandsdaten ein Merkmal gibt, aufgrund dessen diese unterscheidbar sind (sog. *principal*),
- es eine Rechteprüfung (sog. *reference monitor*) geben muss, anhand der

⁴ Siehe Erläuterung in Abschnitt 4.2 des Moduls „Rechtliche Rahmenbedingungen“

entschieden wird, ob der Zugriffswunsch des Subjekts auf das Objekt (gemäß sog. *access control policy*) erlaubt ist; das ist aber keine Frage der Authentisierung im Sinne von Eindeutigkeit der Abbildung,

- der Zugriff erst nach erfolgreicher Authentisierung und Rechteprüfung gewährt wird.

In einigen Fachverfahren ist es zudem relevant,

- ob die Identität des Kunden „ex ante“, d. h. vor Erbringung der Dienstleistung, festgestellt werden kann (ggf. ist hier noch zu unterscheiden, ob die Feststellung der Identität nur möglich oder tatsächlich durchgeführt sein muss) oder
- ob es ausreicht, dass die Identität des Kunden erst „ex post“, d. h. im Nachhinein, feststellbar ist.

**Notwendigkeit
einer Ex-ante-
Authentifizierung**

Dies ist insbesondere dann von Bedeutung, wenn bei der Erbringung der Dienstleistung ein irreparabler Schaden entstehen kann (z.B. Preisgabe von Informationen über schwerwiegende Erkrankungen oder Vorstrafen an Dritte). Dieser Aspekt trifft de facto nur bei einem Schutzbedarf von „mittel“ bis „hoch“ zu. Bei einem Schutzbedarf von „kein“ bis „niedrig“ wird sich die Frage „vor Erbringung oder nach Erbringung“ nicht stellen – aus einem Schutzbedarf von „sehr hoch“ folgt zwangsläufig, dass die Identitätsfeststellung „ex ante“ erfolgen muss.

Hilfsmittel im E-Government-Handbuch:

- Modul „Sichere Kommunikation im E-Government“
- Modul „Hilfsmittel für E-Government – Werkzeugkasten“ (Erläuterung der Schutzbedarfsfeststellung im Kapitel 2.2 des IT-Grundschutzhandbuchs)
- Modul „Verschlüsselung und Signatur“
- Modul „Authentisierung im E-Government“
- „Handlungsleitfaden für die Einführung der elektronischen Signatur und Verschlüsselung in der Verwaltung“ (Werkzeugkasten)

3.5 Aktivität „Ableiten der Sicherheitsanforderungen“

Initiierung: Leiter E-Government-Team

Durchführung: Kernteam, IT-Sicherheitsbeauftragter, Datenschutzbeauftragter, Justitiariat

Im Ergebnis der vorangegangenen Aktivität liegt jetzt eine Erhebung über den Schutzbedarf der übertragenen Daten und der beteiligten Kommunikationspartner hinsichtlich der generischen Schutzziele der einzelnen Kommunikationsphasen vor. Diese steckt den Rahmen für das Maß an Sicherheit ab, das für eine sichere Kommunikation zwischen Kunde und Behörde erforderlich ist. Daran anschließend kommt es darauf an, diesen Schutzbedarf mündend in konkrete Sicherheitsanforderungen auf die beteiligten Partner und die dort erforderlichen Maßnahmen zu beziehen. Im Ergebnis werden die Anforderungen an die eingesetzten Verfahren, Datenformate oder organisatorischen Randbedingungen deutlich, die zu einer Kategorisierung der möglichen Lösungsmechanismen zur Umsetzung der Online-Dienstleistungen führen.

Für die einzelnen Dienstleistungen lassen sich mit folgenden Vorschlägen aus der Schutzbedarfsklasse die entsprechenden Sicherheitsanforderungen ableiten:

Vertraulichkeit

Vertraulichkeit lässt sich durch Verschlüsselung erreichen, je nach Schutzbedarf ist diese Verschlüsselung sinnvoll oder zwingend erforderlich, siehe nachfolgende Tabelle 3. Bei den verwendeten Algorithmen und Schlüssellängen sollen die Empfehlungen des BSI beachtet werden.

Schutzbedarf bzgl. Vertraulichkeit	Sicherheitsanforderung
kein	keine
niedrig bis mittel	Verschlüsselung sinnvoll, aber nicht zwingend erforderlich
hoch bis sehr hoch	Verschlüsselung zwingend erforderlich

Tabelle 3: Verschlüsselung in Abhängigkeit vom Schutzbedarf der Vertraulichkeit

Verbindlichkeit

Alle Teilaspekte der Verbindlichkeit lassen sich durch Signaturen absichern. Zur Authentisierung müssen diese jedoch mit fachverfahrensspezifischen Angaben kombiniert werden, was aber in einer sinnvoll gestalteten E-Government-Dienstleistung keine besondere Hürde darstellt.

Es gibt daneben auch noch andere Mechanismen zur Authentisierung (z. B. PIN-TAN-Verfahren), auf die hier nicht weiter eingegangen wird, bei Interesse siehe Modul „Authentisierung im E-Government“.

Bezogen auf den Schutzbedarf bzgl. der Integrität wird keine gesonderte Ableitung der Sicherheitsanforderungen vorgenommen, da die gleichen Schutzmechanismen (elektronische Signatur) wie zur Erfüllung der Authentizität der übertragenen Daten genutzt werden.

Ergeben sich für Input und Output unterschiedlich hohe Anforderungen an die Authentizität des Kunden, so kann es sinnvoll sein, schon für den Input die höhere Authentisierungsanforderung zu stellen, damit die Behörde für den Output darauf zurückgreifen kann.

Schutzbedarf bzgl. Verbindlichkeit	Sicherheitsanforderung
kein	keine
niedrig	Authentisierung: plausible Angaben genügen (z. B. E-Mail-Adresse, Wohnungsanschrift), Integrität, Nicht-Abstreitbarkeit: keine
mittel	Authentisierung, bei der die Identität des Kunden durch eine unabhängige Instanz bestätigt wurde, d. h. fortgeschrittene elektronische Signatur aus der Verwaltungs-PKI empfohlen, qualifizierte elektronische Signatur sinnvoll
hoch	Authentisierung, die eine zweifelsfreie Nachweisbarkeit der Identität des Kunden zulässt, d. h. qualifizierte elektronische Signatur zwingend erforderlich
sehr hoch	Authentisierung, die eine zweifelsfreie Nachweisbarkeit der Identität des Kunden bereits zum Zeitpunkt der Antragsbearbeitung zulässt, d. h. persönliches Erscheinen erforderlich, elektronisch nicht abbildbar

Tabelle 4: Einsatz von Signaturen in Abhängigkeit vom Schutzbedarf der Verbindlichkeit

Schriftformerfordernis

Wird aufgrund eines Gesetzes oder einer Verordnung die Schriftform gefordert und kann auf dieses Erfordernis nicht verzichtet werden, so kann diese Anforderung – sofern rechtlich keine Ausnahme formuliert wurde – technisch ausschließlich mithilfe einer qualifizierten elektronischen Signatur umgesetzt werden. Mit der qualifizierten elektronischen Signatur erreicht man en passant auch eine Mechanismenstärke bzgl. der Authentizität des Signierenden von mindestens „hoch“.

Schriftformerfordernis	Sicherheitsanforderung
nein	keine zusätzliche
ja	qualifizierte elektronische Signatur zwingend vorgeschrieben

Tabelle 5: Auswirkungen eines Schriftformerfordernisses auf den Einsatz von Signaturen

Verfügbarkeit

Die Ableitung der Sicherheitsanforderungen aus dem Schutzbedarf bzgl. der Verfügbarkeit ist lediglich für die Klassen „hoch“ und „sehr hoch“ erforderlich. Weitere Betrachtungen dieser Sicherheitsanforderungen sind nur in Kenntnis der Spezifika eines Fachverfahrens möglich.

Im Ergebnis sind für jede Online-Dienstleistung nun die Sicherheitsanforderungen an die Schnittstelle zwischen Kunde und Behörde bekannt, die bei der Realisierung beachtet werden müssen.

Hilfsmittel im E-Government-Handbuch:

- Modul „Sichere Kommunikation im E-Government“
- Modul „Verschlüsselung und Signatur“
- Modul „Authentisierung im E-Government“

3.6 Aktivität "Gestaltung des Online-Prozesses"

Initiierung: Teamleiter

Durchführung: Kernteam, Organisationsreferat, Leiter IT-Abteilung

Zweck dieser Aktivität ist es in erster Linie, die vorgesehenen Optimierungsmöglichkeiten innerhalb der einzelnen Prozesse aus den vorangegangenen Aktivitäten aufzubereiten und zu geplanten IT-Vorhaben zusammenzufassen. Zusätzlich sollte bereits jetzt eine grundsätzliche Prüfung auf Machbarkeit erfolgen.

Die im Soll-Konzept per Stichwort oder Umschreibung (Ergebnis Workshop) geänderten Arbeitsabläufe sind in eine Form zu bringen, die sich durch IT-Einsatz nachbilden lässt. Aufgabenblöcke für die Umsetzung, Verantwortlichkeiten und Zeitvorgaben sind entsprechend zuzuweisen. Für diese Vorgehensweise ist der Einsatz geeigneter Hilfsmittel (Formulare, To-do-Listen) dringend anzuraten. Um den Überblick zu behalten und den Bearbeitungsaufwand gering zu halten, ist bei größeren Projekten der Einsatz eines leistungsfähigen Tools geboten.

Die Flussdiagramme müssen entsprechend angepasst werden. Es ist zu klären, inwiefern geeignete Arbeitsvorgänge zu neuen Teilprozessen zusammengefasst und gegebenenfalls durch IT-Einsatz automatisiert werden können. Bei der Modellierung sollten kundenfreundliche Zusatzmöglichkeiten (automatisierte Eingangsmeldungen o. ä.) durch den IT-Einsatz berücksichtigt werden.

Die in Betrieb befindlichen IT-Verfahren sollten aufgelistet werden. Danach werden die Optimierungsansätze aus den Soll-Konzepten, die Schnittstellen zu bestehenden IT-Verfahren haben, oder neue IT-Verfahren erforderlich machen, gesammelt und entsprechend zusammengefasst.

Mit einem Workshop zwischen Beteiligten des Organisationsreferates und IT-Experten sollten folgende Punkte geklärt werden:

**Zu klärende
Fragestellungen**

- Online-Tauglichkeit von Altverfahren
- Anforderungsprofil für „neue“ IT-Verfahren unter Berücksichtigung der bereits zuvor identifizierten behördenweiten Infrastruktur-Verfahren (behördenweiter Einsatz elektronischer Signaturen, Verschlüsselung, Workflow, Dokumentenmanagement usw.)
- Identifikation der zu modellierenden zusätzlichen IT-Verfahren
- Grenzen der Machbarkeit neuer IT-Verfahren
 - Schätzung des Aufwandes für die IT-Modellierung, Programmierung
 - Vorgaben aus der Schutzbedarfsfeststellung und Sicherheitsanforderungen, die nicht oder nur mit unverhältnismäßig großem Aufwand abzubilden sind

- Nicht auf dem Markt existente Standardprodukte oder Lösungen für Teilumsetzungen, dadurch nicht kalkulierbare Kosten.

Problematisierung durch Beispiel „Wegfall von Medienbruch“:

1. Innerhalb eines Teilprozesses werden Gesetze und Verordnungen in Papierform von 15 Bearbeitern genutzt. Es wurde festgestellt, dass ein hoher Aufwand für die Verwaltung und Aktualisierung dieser Papierform notwendig ist. Im Workshop zum Soll-Konzept wurde deshalb präferiert, den Medienbruch durch IT-Einsatz zu beseitigen. Da die zu betrachtenden Arbeitsplätze grundsätzlich mit der benötigten IT ausgestattet und vernetzt sind, ist die Umsetzung der Vorgabe nicht besonders aufwändig. In der Liste der benutzten Arbeitsmittel für *alle* betroffenen Teilprozesse (Prüfung) wird das Medienformat von Papierform auf Dateiform geändert. Es muss in der Aufgabenliste für die IT-Abteilung festgehalten werden, dass sie für die Bereitstellung und die Realisierung des Zugriffs zuständig ist. Die Verwaltungsabteilung ist für die geänderte Beschaffung und Benutzungsordnung zuständig. (Alle weiteren Details, wie Datenformat, Zugriffsrechte, Backup, Schnittstellen zu Datenbanken o. ä. werden in Phase 4 modelliert).
2. Zwischen zwei Teilprozessen wird das Arbeitsergebnis ausgedruckt und per Hausbote von Bearbeiter A zu Bearbeiter B transportiert. Durch den Ausdruck und Transport entsteht inklusive Liegezeit eine Verzögerung in der Bearbeitungskette von zwei Tagen. Im Workshop wurde festgestellt, dass die Bewältigung beider Teilprozesse durch einen Bearbeiter aufgrund unterschiedlicher Rollen nicht möglich ist. Alternativ wurde vereinbart, den Medienbruch durch elektronische Weiterleitung zu beseitigen. Ein eigenes IT-Verfahren wird nicht geprüft, da es sich nicht um einen behördenkritischen Prozess (Ressourcenbindung unter drei Prozent) handelt. Da von Teilprozess zu Teilprozess bislang Kundenunterlagen weitergegeben wurden, muss dies schon ab dem ersten Teilprozess berücksichtigt werden, bei dem die Kundenunterlagen eingehen. Es ist zu prüfen, ob in den behördenweiten infrastrukturellen Voraussetzungen ein zentrales Online-IT-Verfahren, etwa eine „Virtuelle Poststelle“ als Steuerungsinstrument für alle Online-Inputs/-Outputs geplant ist. Falls dies nicht der Fall ist, ist an erster Stelle in der Teilprozesskette ein neuer Teilprozess zu generieren, zur Prüfung auf Vollständigkeit, Digitalisierung und Weiterleitung an den ersten inhaltlichen Bearbeiter. Der Teilprozess ist als generischer IT-Prozess zu kennzeichnen. Es sollte eine behördenweite Liste angelegt werden für gleichartige Fälle der Dokumentendigitalisierung. Hinweis: Im Sinne der Initiative BundOnline 2005 wäre ein vollständiges Online-Verfahren vorzuziehen, da es sich bei dem Zwischenschritt der Digitalisierung von Dokumenten und Erteilung von Papierbescheiden wiederum um einen Medienbruch handelt. Gleichzeitig ist zu dokumentieren, wie die vom Kunden eingegangenen Dokumente archiviert und am Ende der Prozesskette mit dem Abschlussbescheid zusammengeführt werden. In der Aufgabenliste sind wiederum Zeitplan und Zuständigkeiten festzuhalten. Außerhalb der IT-Modellierung müssen noch einheitliche organisatorische Verfahrens- und Vorgehensweisen erstellt

werden (Geschäftsordnung IT: Mitzeichnung, Vertretung o. ä.) Alle Konnektoren zwischen den Teilprozessen sind entsprechend zu modifizieren (elektronischer Transport).

3.7 Aktivität "Vorabprüfung rechtlicher Rahmenbedingungen"

Initiierung: Teamleiter E-Government

Durchführung: Fachverantwortliche, Justitiariat, Datenschutzbeauftragte, Beauftragter für den Haushalt

Die Erbringung von E-Government-Dienstleistungen ist in noch viel stärkerem Maße als entsprechende Vorhaben in der freien Wirtschaft durch Gesetze, Verordnungen und andere Rechtsnormen reguliert. Die Möglichkeiten und Grenzen ihrer Bereitstellung werden wesentlich durch rechtliche Rahmenbedingungen abgesteckt. Durch eine Überprüfung der relevanten Rechtslage soll verhindert werden, dass die neugestaltete Dienstleistung rechtliche Vorgaben verletzt oder einen rechtlich vorhandenen Spielraum nicht in angemessenem Umfang nutzt. Eine solche *Vorabprüfung* muss am Ende des Einführungsprozesses durch eine abschließende und vollständige rechtliche Prüfung der neuen Dienstleistung unter Berücksichtigung der dann geltenden Rechtslage ergänzt werden.

Besondere Bedeutung von Rechtsnormen im E-Government

Die Vorabprüfung der rechtlichen Rahmenbedingungen sollte sowohl die für eine Dienstleistung maßgeblichen Fachgesetze (hier können die entsprechenden Angaben, die in der Aktivität „Erhebung online-fähiger Dienstleistungen“ erfasst wurden, als Grundlage dienen) als auch den allgemeinen Rahmen des Verwaltungshandelns erfassen. Unter die zu beachtenden allgemeinen Gesetze fallen typischerweise:

- **Bundesdatenschutzgesetz** (und entsprechende Vorschriften der Länder): Das BDSG fordert in zahlreichen Fällen eine ausreichende *Verschlüsselung* von personenbezogenen Daten bei elektronischer Speicherung, Verarbeitung und Übermittlung. Daneben werden Informationsrechte des Bürgers gegenüber der Verwaltung geregelt.
- **Formvorschriften:** Durch die Umsetzung der EU-Signaturrechtlinie 1999/93 EWG in deutsches Recht werden zahlreiche Formvorschriften sowohl im Privatrecht als auch im öffentlichen Recht dahin gehend novelliert, dass eine qualifizierte elektronische Signatur nach den Vorgaben des **Signaturgesetzes** die eigenhändige Unterschrift und damit die Schriftform ersetzen kann. Maßgeblich sind hier vor allem die Novellierungen im **BGB** und die Änderungen des **Verwaltungsverfahrensgesetzes**

Weiter zu beachten sind Regelungen wie Personalvertretungsrechte (z. B. im BPersVG bzw. BetrVG), Fernabsatzrichtlinie, Teledienstegesetz, Teledienstedatenschutzgesetz, Telekommunikationsgesetz, Mediendienstestaatsvertrag, Informations- und Kommunikationsdienste-Gesetz, TK-Überwachungsverordnung, Bundeshaushaltsordnung usw.

Gegenstand der Überprüfung der neugestalteten Dienstleistung sollten u. a. folgende Fragestellungen sein:

Standardfragen

- Ist der angestrebte Automatisierungsgrad der Dienstleistung mit den rechtlichen Vorgaben verträglich?
- Genügen die vorgesehenen Mechanismen zur Sicherstellung der Vertraulichkeit von (personenbezogenen) Daten den rechtlichen Anforderungen?
- Wird eine ausreichend langfristige und rechtssichere Archivierung der Daten erreicht?
- Sind die Informationsrechte des Bürgers über seine Daten gewährleistet?
- Schafft die Bereitstellung der Dienstleistung in elektronischer Form besondere Anforderungen an die Verschlüsselung und Authentisierung der kommunizierten Daten?
- Wie sind Verfahren zu bewerten, in denen sowohl elektronische als auch „klassische“ Kommunikationswege genutzt werden?
-

Bei der Beurteilung der rechtlichen Rahmenbedingungen sollte auf jeden Fall berücksichtigt werden, dass derzeit zahlreiche für E-Government relevante gesetzliche Vorschriften überarbeitet werden. Hieraus ergeben sich oft neue Möglichkeiten für E-Government-Dienstleistungen. Informationen über geplante und realisierte Gesetzgebungsnovellen können u. a. auf den Seiten <http://www.deutschland-online.de>, <http://www.bund.de>, und <http://www.staat-modern.de> abgerufen werden. Darüber hinaus kann auch eine Anfrage bei dem für ein bestimmtes Fachgesetz zuständigen Ministerium sinnvoll sein.

**Neues Recht für
E-Government**

Ferner ist zu beachten, dass es sich bei E-Government um verwaltungsrechtliche Themengebiete handelt, die weitestgehend noch nicht – oder nicht abschließend – durch Rechtsprechung bewertet sind. Um einem eventuellen Fehlverhalten der Behörde vorzubeugen, sollte daher regelmäßig und anlassbezogen überprüft werden, ob die rechtlichen Bewertungen aufrechterhalten werden können.

Zum Abschluss der rechtlichen Vorabprüfung sollte eine Genehmigung des Justitiariats der Behörde für die geplante Umsetzung der Dienstleistung eingeholt werden. So kann auch formal Planungssicherheit für die weiteren Schritte gewonnen werden.

**Justitiariat,
Personalvertretun
g**

Hilfsmittel im E-Government-Handbuch:

- Modul „Rechtliche Rahmenbedingungen für E-Government“
- Kapitel VII „Rechtsgrundlagen“ in der Lose-Blatt-Sammlung

3.8 Aktivität „Überprüfung der Bewertungen aus Phase 2 hinsichtlich Aufwand und Nutzen“

Initiierung: Teamleiter E-Government

Durchführung: Kernteam, Fachverantwortliche

Nachdem die Ausgestaltung des geplanten Online-Prozesses in der Aktivität "Gestaltung des Online-Prozesses" (Aktivität 3.6) vorläufig festgelegt wurde, sollte überprüft werden, inwieweit die so einzurichtende Dienstleistung noch den ursprünglich formulierten Behördenzielen gerecht wird und ob ihre Einführung in der geplanten Form unter „Aufwand-Nutzen-Aspekten“ gerechtfertigt ist.

Zielkonformität?

Zur Überprüfung der Zielkonformität sollten u. a. folgende Fragen beantwortet werden:

- Sind gerade die hoch priorisierten Dienstleistungen (am besten) geeignet, zur Erreichung der übergeordneten Behördenziele beizutragen?
- Haben sich die Annahmen, die Grundlage der Prioritätensetzung waren, im Laufe der konkreten Planungen bestätigt?
- Sind wesentliche Randbedingungen und Schwierigkeiten oder Chancen, die mit der Umsetzung der Online-Dienstleistung verbunden sind, unberücksichtigt geblieben?
- Können die geplanten Optimierungsschritte im vorgesehenen Zeitplan umgesetzt werden?
-

Ziel der (vorläufigen) Aufwand-Nutzen-Analyse ist es, herauszufinden, ob der vor dem Hintergrund der Behördenziele gesehene Nutzen der neuen Online-Dienstleistung die zu erwartenden Aufwände bei der Gestaltung der zugehörigen Online-Prozesse rechtfertigt.

Auf **Nutzenseite** sollte geprüft werden, ob die Festlegungen, die zur Prioritätensetzung der Dienstleistungen geführt haben vor dem Hintergrund der zwischenzeitlich gewonnenen Erkenntnisse und konkreteren Planungen noch Bestand haben und ob insbesondere durch die vorrangig zu bearbeitenden Dienstleistungen die in Phase 2 definierten Behördenziele tatsächlich erreicht werden. Sofern in Phase 2 Bewertungsbögen ausgefüllt wurden, bietet es sich an, die dort gemachten Eintragungen noch einmal kritisch zu überprüfen.

Nutzen

Aufgrund der in dieser Phase noch nicht erfolgten technischen Detailplanung der Online-Prozesse kann auf **Aufwandsseite** an dieser Stelle noch keine seriöse monetäre Analyse vorgenommen werden. Typische hier zu erfassende Aspekte wären aber:

Aufwand

- Ausmaß der erforderlichen Umgestaltungen (insbesondere organisatorisch, technisch nur soweit eine Beurteilung jetzt schon möglich ist) unter Berücksichtigung der in Phase 2 identifizierten Infrastruktur-Verfahren.
- Fortbildungsbedarf der betroffenen Mitarbeiter

- (größere) Komplexität der Dienstleistung auf Nutzerseite
- Abhängigkeit von zeitlich schwer bestimmbareren Gesetzgebungsverfahren
-

Hilfsmittel im E-Government-Handbuch:

- Modul „Bewertungskriterien für potenziell online-fähige Dienstleistungen“

3.9 Aktivität „Aktualisierung der E-Government-Strategie“

Initiierung: Leiter E-Government-Team

Durchführung: Kernteam, Behördenleitung

In Phase 2 des Phasenplans wurde durch Festlegung der E-Government-Behördenziele verbunden mit der Auswahl der geeigneten Dienstleistungen und dem Aufstellen einer groben Ressourcenplanung letztlich eine *E-Government-Strategie* der Behörde formuliert. Da diese jedoch nur auf den Ergebnissen der dort vorgenommenen Erhebungen beruht, kann sie weder funktionelle noch technische Einzelheiten der neu gestalteten Dienstleistungen berücksichtigen. Es bietet sich daher an, die Strategie am Ende dieser dritten Phase kritisch zu sichten und ggf. zu überarbeiten. Insbesondere sollten dabei die bei der Vorabprüfung der rechtlichen Rahmenbedingungen und der vorläufigen Aufwand-Nutzen-Analyse erzielten Ergebnisse einfließen.

Besseres Wissen
führt zu einer
neuen Strategie

Als Resultat der Überlegungen wird typischerweise eine (oder mehrere) der folgenden Feststellungen getroffen werden:

Typische
Ergebnisse

- **Die in Phase 2 festgelegte Strategie bedarf keiner Modifikation.** Alle zu Grunde liegenden Annahmen haben sich in Phase 3 bestätigt. Der Zeitplan kann eingehalten werden.
- **Die zur Umsetzung der Online-Dienstleistung erforderlichen Prozessneugestaltungen führen zu einer Verzögerung im Projektverlauf.** In diesem Fall muss der zu erstellende Zeitplan entsprechend angepasst werden. Sollte eine schnelle Umsetzung der Online-Dienstleistung dennoch gewünscht sein, kann unter Berücksichtigung von Aufwand-Nutzen-Aspekten auch über die Implementierung von Übergangslösungen nachgedacht werden.
- **Bestimmte zur vorrangigen Umsetzung ausgewählte Dienstleistungen tragen nicht im erforderlichen Umfang zur Erreichung der Behördenziele bei oder erweisen sich dabei sogar als hinderlich.** Hier gibt es prinzipiell zwei Reaktionsmöglichkeiten:
 - Die entsprechenden Dienstleistungen werden im Umsetzungsplan niedriger priorisiert oder ganz gestrichen, oder
 - die Behördenziele müssen revidiert werden. Von dieser Option sollte jedoch nur im „Notfall“ Gebrauch gemacht werden, also wenn sich beispielsweise überhaupt keine wirklich zur Zielerreichung geeigneten online-fähigen Dienstleistungen finden lassen.
- **Einige geplante Online-Dienstleistungen sind mit zu hohem Umsetzungsaufwand verbunden.** Reaktionsmöglichkeiten:
 - Die entsprechenden Dienstleistungen werden im Umsetzungsplan niedriger priorisiert, z. B. so lange aufgeschoben, bis sich bestimmte ungünstige Rahmenbedingungen geändert haben, oder ganz gestrichen, oder

- es wird überprüft, inwieweit sich, ggf. zeitlich befristete, Übergangs- oder Teillösungen mit weniger Aufwand umsetzen lassen.
- **Einige geplante Dienstleistungen können aufgrund von rechtlichen Restriktionen gar nicht oder nur in begrenztem Umfang, z. B. mit vermindertem Automatisierungsgrad, umgesetzt werden.** Abhängig davon, ob in absehbarer Zeit mit Änderungen der gesetzlichen Rahmenbedingungen zu rechnen ist, müssen die betreffenden Dienstleistungen in ihrer Planung modifiziert, gestrichen oder vorläufig zurückgestellt werden. Auch hier sollte ggf. die Möglichkeit zur Realisierung von Übergangslösungen erwogen werden.
- **Durch eingetretene oder absehbare Änderungen der Rechtslage können bestimmte Online-Dienstleistungen zusätzlich oder in erweitertem Umfang angeboten werden.** Diese „neuen“ Dienstleistungen sind entsprechend den Vorschlägen in Phase 2 zu überprüfen und sollten, sofern dies mit den zur Verfügung stehenden Ressourcen möglich ist, in den Einführungsplan integriert werden.
- **Bestimmte Dienstleistungen können im funktionalen „Bündel“ mit anderen ohne großen Aufwand „miterledigt“ werden.** Im Sinne der Abrundung des Dienstleistungsportfolios der Behörde sollten diese Dienstleistungen in den Umsetzungsplan aufgenommen werden.

Das Ergebnis der Überprüfung der E-Government-Strategie ist der Behördenleitung zur Genehmigung vorzulegen. Sie muss dann entscheiden, ob und inwieweit die Veröffentlichung einer neuen E-Government-Leitlinie erforderlich und sinnvoll ist. Das E-Government-Team sollte hierzu einen Entscheidungsvorschlag formulieren.

Genehmigung
durch
Behördenleitung

Die Personalvertretung ist unbedingt in diese Aktivitäten einzubinden. Die Einbindung des Personalrates ergibt sich zum einen aus den Mitbestimmungsrechten nach BPersVG und BetrVG, sollte aber in jedem Falle rechtzeitig vor der Einführung neuer Techniken und Verfahren erfolgen, so dass keine unnötigen Hürden durch fehlende Informiertheit und Beteiligung entstehen.

3.10 Aktivität "Information aller Betroffenen"

Initiierung: Leiter E-Government-Team

Durchführung: Kernteam, Bereich Öffentlichkeitsarbeit, Behördenleitung

Durch die funktionale Konzeption der geplanten Online-Dienstleistungen und die damit verbundene Revision der E-Government-Strategie haben die E-Government-Pläne der Behörde im Vergleich zur Situation am Ende von Phase 2 erheblich an Verbindlichkeit gewonnen. Neben der erneuten Information der Mitarbeiter und der Personalvertretung über den erreichten Stand der Umsetzungsplanung sollte in dieser Phase auch erwogen werden, inwieweit eine breitere Information von betroffenen Kunden und Partnern erfolgen soll. Diese Aktivitäten sollten mit der allgemeinen Öffentlichkeitsarbeit koordiniert werden und müssen letztlich von der Amtsleitung gebilligt werden.

Im Gespräch
bleiben

Bei der Information breiterer Nutzerkreise muss gerade in dieser frühen Projektphase vermieden werden, durch vorzeitige Versprechungen oder allzu ehrgeizige Zeithorizonte eine Erwartungshaltung zu wecken, die hinterher möglicherweise enttäuscht wird und damit dem Image der Behörde mehr schadet als nützt. Dieser Negativ-Effekt sollte durch eine angemessene Zurückhaltung in Form und Inhalt vermieden werden. Dazu ist es hilfreich, wenn das E-Government-Team eine Einschätzung der verbleibenden Projektrisiken formuliert.

Realistische
Erwartungen

Mit einer Information der Betroffenen können mehrere Ziele verfolgt werden. Hierzu gehören u. a.

Ziele

- **„PR-Effekt“:** Die Behörde zeigt nach außen, dass sie sich den Anforderungen und Möglichkeiten der Internettechnologien offensiv stellt. Neben Pressemitteilungen oder Messe- und Vortragsauftritten bietet sich natürlich besonders auch der bestehende Web-Auftritt der Behörde für diese Form der Öffentlichkeitsarbeit an. Das Risiko eines Negativ-Effekts durch die Erweckung überzogener Erwartungshaltungen ist hier naturgemäß besonders hoch.
- **„Feedback“, aktive Partizipation von Externen:** Die Behörde sollte spätestens jetzt in der Lage sein, ihre E-Government-Pläne auch in intensiveren Diskussionen mit Betroffenen zu erörtern und deren Anregungen sinnvoll aufzunehmen und diese ggf. bei der weiteren Planung zu berücksichtigen. Je nach Umfang und Zusammensetzung des Kunden- und Partnerkreises bieten sich verschiedene Vorgehensweisen an. Während die Einrichtung von E-Mail- und Telefon-Hotlines die Beteiligung von breiten Bevölkerungskreisen ermöglicht, kann bei kleinen, der Behörde im wesentlichen bekannten Nutzerkreisen auch die Veranstaltung von Workshops oder die Einrichtung von entsprechenden Arbeitskreisen in einigen Fällen sinnvoll sein. Auch die Einbindung von Fachverbänden, politischen Gremien oder die Teilnahme an Fachkongressen u. ä. können wertvolle Informationen liefern. Die Internet-Seiten sollten auf ihre

Barrierefreiheit hin überprüft werden; Nutzertests sind auch von behinderten Nutzern durchzuführen.⁵

- **Planungssicherheit auf Nutzerseite:** In einigen Fällen wird sich für externe Nutzer der Wunsch oder sogar die Notwendigkeit ergeben, durch eigene technisch-organisatorische Maßnahmen den Mehrwert der neuen Dienstleistung zu vergrößern oder zu sichern (Bsp.: Beschaffung von Signaturchipkarten, Anmeldung bei Anbietern von Online-Bezahlverfahren, Anpassung interner IT-Prozesse oder -Formate auf Nutzerseite, ...). Durch frühzeitige Information der Kunden und Partner über die anstehenden Änderungen erhöht sich deren Planungssicherheit und damit letztlich auch deren Bereitschaft und Fähigkeit, diese Dienstleistungen online anzunehmen.

⁵ Siehe Modul „Barrierefreies E-Government“

7 Checklisten

Die nachfolgende Checkliste kann dazu benutzt werden nachzuhalten, ob alle unverzichtbaren Ergebnisse der aktuellen Phase vorliegen. Sie kann auch dann benutzt werden, wenn die oben vorgestellten Aktivitäten in anderer Reihenfolge oder in einer anderen Ausprägung durchgeführt wurden:

7.3 Checkliste für Phase 3

Ergebnis	Wer?	Wann?	Erledigt?
Prozesse sind aufgenommen			
Prozesse sind optimiert und gestaltet			
Schutzbedarf ist festgestellt			
Rechtliche Rahmenbedingungen sind geprüft			

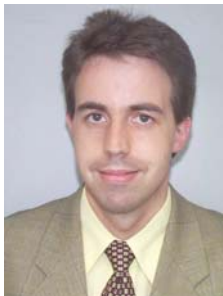
9 Autorendarstellung

Rainer Belz, BSI



Herr Belz wurde nach seinem Studium zum Diplom-Verwaltungswirt langjährig als Sachbearbeiter für Personal und Organisation beim Ausweichsitz der obersten Verfassungsorgane des Bundes (Regierungsbunker) eingesetzt. Aufgrund fundierter Kenntnisse auf dem Gebiet der Informatik erfüllte er auch zahlreiche Aufgaben in den Bereichen IT-Sicherheit und IT-Koordinierung. Die Einführung von IT innerhalb der Behörde, die zu treffenden technischen und organisatorischen Maßnahmen, sowie deren Planung und Umsetzung hatte er vor der obersten Bundesbehörde zu vertreten. Seit 1999 wird er beim Bundesamt für Sicherheit in der Informationstechnik als IT-Sicherheitsberater mit Aufgabenschwerpunkt in der technischen Infrastruktur und Kommunikationstechnik eingesetzt. Er zeichnet für IT-Sicherheitsanalysen bei Behörden mittlerer Größe verantwortlich und ist auch bei der Entwicklung neuer Methoden und Vorgehensweisen der Sicherheitsanalyse beteiligt. Er ist als Autor und Teilprojektleiter für das E-Government-Handbuch verantwortlich.

Dr. Christian Mrugalla, BSI



Nach Studium und Promotion in Physik an der TU Clausthal wechselte Dr. Christian Mrugalla 1998 als Referent ins Bundesamt für Sicherheit in der Informationstechnik. Neben der allgemeinen IT-Sicherheitsberatung von (Bundes-)Behörden und der Mitwirkung an der Fortentwicklung des IT-Grundschutzhandbuchs lag und liegt ein Schwerpunkt seiner Tätigkeit im BSI-Projektbüro „Digitale Signaturen“ und hier besonders in der Beratung von E-Government-Projekten, in denen diese Technologie zum Einsatz kommt. Als beratendes Mitglied des Arbeitskreises „Digitales Rathaus“ des Deutschen Städtetags begleitet Herr Dr. Mrugalla auch die Umsetzung von E-Government-Initiativen im kommunalen Umfeld.