h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

fbi
FACHBEREICH INFORMATIK

Hochschule Darmstadt

- Fachbereich Informatik -

Voraussetzungen zum Vertrauensaufbau zur Preisgabe von sensiblen Daten im Web am Beispiel eines Online-Fragebogens

Abschlussarbeit zur Erlangung des akademischen Grades
Bachelor of Science (B.Sc.)

vorgelegt von
Andrea Cathrin Hendzel

Referent:	Prof. Dr. Klaus Wente
Korreferent:	Prof. Dr. Stephan Karczewski
Fachbetreuer:	Jörg Buchwitz
Kooperationsunternehmen:	ExperTeach Gesellschaft für Netzwerkkompetenz mbH

Eidesstattliche Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbständig erstellt und keine anderen als die angegebenen Hilfsmittel benutzt habe.

Soweit ich auf fremde Materialien, Texte oder Gedankengänge zurückgegriffen habe, enthalten meine Ausführungen vollständige und eindeutige Verweise auf die Urheber und Quellen.

Alle weiteren Inhalte der vorgelegten Arbeit stammen von mir im urheberrechtlichen Sinn, soweit keine Verweise und Zitate erfolgen.

Mir ist bekannt, dass ein Täuschungsversuch vorliegt, wenn die vorstehende Erklärung sich als unrichtig erweist.

Darmstadt, den 09.02.2010

Andrea Cathrin Hendzel

Abstract

Aktuell sind Fragebögen eine beliebte Methode, um Beurteilungen oder Informationen von Personen zu erhalten. Der Trend ist, dass ein Fragebogen nicht mehr in Papierform verteilt wird, sondern als Online-Fragebogen im Internet zur Verfügung gestellt wird.

Man muss sich hierbei jedoch die Frage stellen, wie man die Skepsis des Benutzers bezüglich Datenmissbrauchs mildern kann. Wie kann man es schaffen, dass der Benutzer Vertrauen in einen Online-Fragebogen bzw. die Institution dahinter aufbaut? Denn nur, wenn Vertrauen aufgebaut wird, wird der Benutzer bereit sein, seine ehrliche Meinung preiszugeben.

Die Ausarbeitung beschäftigt sich mit der Fragestellung, welche Empfehlungen für die Gestaltung eines Online-Fragebogens ausgesprochen werden können, damit ein Benutzer Vertrauen in einen Online-Fragebogen aufbaut. Es werden Möglichkeiten aufgezeigt, die dem Benutzer sichtbar machen, dass die eingegebenen Daten vertraulich behandelt werden.

Danksagung

Der schönste Dank ist jener, der vor lauter Freude vergessen wird.

(Walter Ludin)

In diesem Teil möchte ich all denjenigen danken, die mich während meines Studiums und insbesondere bei der Erstellung der Bachelorarbeit unterstützt haben.

Ich möchte mich bei meinem Partnerunternehmen der *ExperTeach Gesellschaft für Netzwerkkompetenz mbH* bedanken für das in mich gesetzte Vertrauen durch die Einstellung als KoSI-Studentin. Ich möchte mich bei allen Mitarbeitern des Unternehmens für das freundliche und angenehme Arbeitsklima bedanken. Vor allem bei Jörg Buchwitz, der in allen drei Praxisphasen mein Fachbetreuer war und mir immer freundlich und kompetent zur Seite stand. Auch beim Ausbildungsleiter Christoph Schramm möchte ich mich für seine Unterstützung und seine Ratschläge während des Studiums bedanken.

Ich bedanke mich bei Prof. Dr. Klaus Wente von der Hochschule Darmstadt für die gute Betreuung während der dritten Praxis- und der Schreibphase, den Begleitseminaren und den persönlichen Treffen. Er erklärte auf verständliche Weise die Techniken für eine wissenschaftliche Arbeit und unterstützte mich bei der Erarbeitung der Bachelorarbeit.

Vergessen möchte ich natürlich nicht meine Familie und Freunde, die mich während des ganzen Studiums und vor allem in der Endphase unterstützt haben. Ich bedanke mich bei meinen Korrekturlesern Matthias, Ngozi und Felix. Aber vor allem bedanke ich mich bei Benny und Anna, die mir stets beigestanden haben.

Inhaltsverzeichnis

Eidesstattliche Erklärung **2**

Abstract **3**

Danksagung **4**

Inhaltsverzeichnis **5**

1 Einleitung **8**

1.1 Motivation **8**

1.2 Problembeschreibung **9**

1.3 Zielsetzung **10**

1.4 Abgrenzung **11**

1.5 Struktur der Arbeit **12**

2 Grundlagen **14**

2.1 (Online-)Fragebogen **14**

2.1.1 Definition: Fragebogen 14

2.1.2 Definition: Online-Fragebogen 15

2.1.3 Nutzen von Fragebögen 15

2.2 Sicherheit im Web **17**

2.2.1 Definition: Sicherheit 17

2.2.2 Technologien zur sicheren Datenübertragung 18

2.2.2.1 Basic Authentication/Digest Access Authentication 19

2.2.2.2 Secure Hypertext Transfer Protocol (S-HTTP) 20

2.2.2.3 Secure Socket Layer (SSL)/Transport Layer Security (TLS) 21

2.2.3 JavaScript und Java Applets 23

2.2.4 Datenschutzerklärung eines Webseitenbetreibers 24

2.3 Benutzeroberfläche **26**

3 Vertrauen ... 28

3.1 Definition ... 28

3.2 Arten von Vertrauen ... 33

3.3 Modell zur Vertrauensbildung: Drei-Phasen-Modell ... 35

3.4 Verständnis des Begriffs „Vertrauen“ im Kontext dieser Arbeit ... 37

4 Aufbau des Vertrauens bei Online-Fragebögen ... 38

4.1 Bestimmung der Zielgruppe ... 38

4.2 Empfehlungen für die IT ... 40

4.3 Gestaltung der Benutzeroberfläche ... 49

4.3.1 Begleittext ... 50

4.3.2 Instruktionstext ... 52

4.3.3 Gestaltung ... 53

4.3.4 Benutzerfreundlichkeit ... 54

4.3.5 Sicherheitsmerkmale ... 57

4.4 Hinweise zur Fragenkonstruktion ... 62

4.4.1 Einleitungsfrage ... 62

4.4.2 Matrixfragen ... 63

4.4.3 Allgemeine Hinweise zur Fragenkonstruktion ... 65

5 Abschlussbemerkungen ... 68

5.1 Resümee ... 68

5.2 Ausblick und Forschungsdesiderata ... 70

5.3 Fazit ... 72

Literaturverzeichnis ... 73

Abbildungsverzeichnis ... 78

Abkürzungsverzeichnis ... 79

Glossar ... 80

Anlage 84

I. Leitfaden zur Erstellung des Online-Fragebogens 85

II. Checkliste 89

1 Einleitung

In der Einleitung wird zu Beginn die Motivation (Kap. 1.1) dieser Arbeit erläutert, worauf ein Überblick über das Problem (Kap. 1.2) geliefert wird. Darauf folgt das Ziel (Kap. 1.3) der Bachelorarbeit sowie eine Abgrenzung (Kap. 1.4) zu ähnlichen Themengebieten. Am Ende dieses Kapitels steht die Erläuterung zur Struktur der Abschlussarbeit (Kap. 1.5).

1.1 Motivation

Im Rahmen der dritten Praxisphase bei der *ExperTeach Gesellschaft für Netzwerkkompetenz mbH* hatte ich die Aufgabe, eine Webschnittstelle, die für den Datenaustausch zwischen Datenbanken zuständig sein sollte, zu definieren. Die durch die Schnittstelle erhaltenen Daten sollten in eine Datenbank integriert und Auswertungen erstellt werden. Die Daten stellten Fragen und Antworten von Beurteilungsbögen dar, die von Schulungsteilnehmern nach einer Veranstaltung abgegeben worden waren.

Vor Beginn des Projektes wurden die Befragungen mittels Fragebögen in Papierform durchgeführt, was eine komplexe Auswertung sehr aufwändig machte. Während der Projektphase wurde ein Web-Frontend erstellt, über das die Teilnehmer die Möglichkeit bekamen, ihre Antworten online abzugeben. Diese Daten werden in die interne Datenbank übertragen, in der unterschiedliche Auswertungsmechanismen angewandt und die Daten schließlich in aufbereiteter Form dargestellt werden.

Im Projektverlauf stellte sich immer wieder die Frage, wie man die Teilnehmer überzeugen kann, die Online-Fragebögen wahrheitsgemäß auszufüllen. In den Diskussionen mit meinen Fachbetreuern zeigte sich, dass Vertrauen womöglich ein entscheidender Faktor in diesem Bereich sein könnte. Aus dieser Fragestellung heraus entstand für mich die Motivation, diese Thematik im Rahmen meiner Abschlussarbeit näher zu beleuchten.

1.2 Problembeschreibung

Immer häufiger werden Daten über das Internet erhoben. Oftmals werden die Befragungen mittels Online-Fragebögen durchgeführt. Bei dieser Art der Befragung hat man die Möglichkeit, auf einfache Weise eine große Anzahl von Personen zu erreichen. Heutzutage sind bereits 67,1 % der deutschen Bevölkerung online, was 43,5 Mio. Personen entspricht (vgl. [ARDZDF09]).

Bei den meisten Online-Befragungen entstehen jedoch die Probleme, dass der Benutzer zum einen motiviert werden muss und zum anderen auch ein gewisses Vertrauen in den Fragenden bzw. die Institution, die hinter dem Datenerhebungsmittel steht, haben muss.

Es wird davon ausgegangen, dass der Befragte seine ehrliche Meinung nur dann preisgeben wird, wenn er eine Vertrauensbasis aufbauen kann. Alle Datenerhebungsmittel sind nur sinnvoll, wenn man davon ausgehen kann, dass die Ergebnisse unverfälscht und somit für weitere Auswertungen nutzbar sind.

Es stellt sich die Frage, welche Mittel existieren, damit der Benutzer Vertrauen in das internetbasierte Datenerhebungsmittel entwickeln kann. Schließlich besitzt das Internet keinen guten Ruf, wenn es um die sichere Übertragung von sensiblen Daten geht.

Am Beispiel des internetbasierten Datenerhebungsmittels Online-Fragebogen soll die dargestellte Problemstellung im Fokus dieser Arbeit stehen.

1.3 Zielsetzung

Ziel dieser Arbeit ist es, einen Leitfaden mit allen wichtigen Merkmalen zum Vertrauensaufbau zu einem Online-Fragebogen bzw. der dahinter befindlichen Institution zu erstellen und eine Checkliste[1] zu diesem Leitfaden anzufertigen.

Diese Arbeit erläutert die im Leitfaden zusammengefassten Hinweise genauer und liefert mindestens eine Begründung, inwiefern das beschriebene Merkmal den Aufbau von Vertrauen seitens des Benutzers unterstützt.

Im Leitfaden selber werden die in dieser Arbeit konkret erläuterten Möglichkeiten zum Vertrauensaufbau zusammengefasst. Er liefert einen Überblick über die wichtigsten Hinweise, die beim Aufbau eines Online-Fragebogens beachtet werden sollten, damit der Benutzer durch die Darstellung des Online-Fragebogens Vertrauen in diesen aufbauen kann.

Wichtig bei der Herangehensweise an die Ergebnisdokumente dieser Arbeit ist, dass der Leitfaden vor der Erstellung eines Online-Fragebogens beachtet werden sollte, da er Empfehlungen für unterschiedliche Gestaltungsaspekte enthält. Die Checkliste dient im Gegensatz dazu als Kontrollinstrument. In ihr werden alle wichtigen Hinweise übersichtlich aufgeführt und bieten z. B. dem Tester eines Online-Fragebogens die Möglichkeit abzuhaken, welche Merkmale des Leitfadens bei dem Online-Fragebogen beachtet worden sind.

[1] Der Begriff Checkliste besitzt unterschiedliche Definitionen. In dieser Arbeit soll er in folgender Form verstanden werden: Eine Checkliste ist eine Liste, die zur Kontrolle genutzt wird (vgl. Glossar – Checkliste).

1.4 Abgrenzung

In dieser Arbeit soll nicht erläutert werden, wie die korrekte Struktur eines Fragebogens aussehen bzw. wie die Fragen formuliert werden sollten. Es werden lediglich einige allgemeine Ratschläge zu diesem Bereich gegeben, welche hinsichtlich des Vertrauensaufbaus wichtig sind. Eine genaue Betrachtung der Formulierungsarten von Online-Fragebögen würde den Rahmen dieser Ausarbeitung sprengen.

Der Online-Fragebogen wird hier als Instrument zur Datenerhebung genutzt. Davon zu unterscheiden sind Fragebögen für Intelligenz- oder Wissenstests. Für diese Art von Tests sind die Empfehlungen nicht ausgelegt.

Wichtig in dieser Ausarbeitung ist der erste Eindruck beim Blick auf den Online-Fragebogen als Datenerhebungsmittel. Im Mittelpunkt steht die Frage danach, welche Merkmale in der Darstellung entscheidend sind, damit der Benutzer eine Vertrauensbasis aufbaut und beim Online-Fragebogen bereit ist, ehrliche Antworten zu geben.

1.5 Struktur der Arbeit

Die Bachelorarbeit beginnt mit einer Einleitung, in der die Motivation, die Problemstellung, die Zielsetzung, die Abgrenzung und die Struktur der Arbeit erläutert werden.

Auf den Einleitungsteil folgt der Grundlagenabschnitt, der sich in drei Teile unterteilt. Zu Beginn wird vorgestellt, was ein Fragebogen und ein Online-Fragebogen ist und welchen Nutzen Fragebögen haben. Darauf folgt das Kapitel „Sicherheit im Web“, in dem zunächst der Begriff „Sicherheit“ definiert wird. Danach werden unterschiedliche Techniken vorgestellt. Zum einen solche, die für die sichere Datenübertragung im Internet genutzt werden können und zum anderen solche, die für eine interaktive Gestaltung nötig sind. Das Sicherheits-Kapitel endet mit einer Erläuterung des Begriffs „Datenschutzerklärung“. Das dritte Kapitel und somit das letzte des Grundlagenabschnitts nennt sich „Benutzeroberfläche“ und erläutert diesen Begriff, sowie dessen Nutzen.

Nach den Grundlagen folgt das Kapitel „Vertrauen“, das eigentlich in den Grundlagenabschnitt gehört. Der Komplexität und Wichtigkeit dieses Themas muss aber mit einem eigenen Abschnitt Genüge getan werden. In diesem werden einige wichtige Informationen zum Thema „Vertrauen“ geliefert. Es werden zum einen Definitionen behandelt, aber auch Arten von Vertrauen dargestellt. Darauf folgt das Drei-Phasen-Modell, welches den Aufbau von Vertrauen aus psychologischer Sicht darstellt. Am Ende wird geklärt, wie Vertrauen in dieser Ausarbeitung zu verstehen ist.

Der Hauptteil dieser Arbeit beginnt nach dem Vertrauenskapitel. Es beginnt mit einer Erläuterung zur Bestimmung der Zielgruppe und geht weiter mit der Aufzählung von Mechanismen zur sicheren Datenübertragung, um dem Benutzer das Vertrauen in einen Online-Fragebogen näher zu bringen. Darauf folgen fünf Ratschläge zur Gestaltung der Benutzeroberfläche, sowie drei sinnvolle Merkmale zu der Fragenformulierung eines Online-Fragebogens. Diese drei Hinweise zur Fragenformulierung sind für den Vertrauensaufbau relevant und werden aus diesem Grund erwähnt.

Beendet wird die Bachelorarbeit mit den Abschlussbemerkungen. Dazu gehören die Unterkapitel „Resümee“, „Ausblick und Forschungsdesiderata“ sowie das „Fazit“. Im Resümee wird das Ergebnis der Ausarbeitung zusammengefasst. Das Kapitel Ausblick und Forschungsdesiderata gibt Auskunft über die zukünftige Nutzung von Online-Fragebögen und zeigt mögliche fortführende Projekte auf. Beendet werden die Abschlussbemerkungen mit einem persönlichen Fazit.

Im Anhang werden der Leitfaden und die Checkliste, die die Ergebnisse dieser Ausarbeitung darstellen, gezeigt.

2 Grundlagen

Das Grundlagenkapitel enthält drei Unterkapitel. Das erste davon „(Online-)Fragebogen“ (Kap. 2.1) erklärt die unterschiedlichen Fragebögen sowie die Befragungsarten. Das darauffolgende Kapitel nennt sich „Sicherheit im Web“ (Kap. 2.2) und erläutert einige technische Aspekte, die für Übermittlung und Darstellung von Online-Fragebögen wichtig sind. Das letzte Kapitel in diesem Grundlagenteil beschäftigt sich mit der Beleuchtung des Themas Benutzeroberfläche (Kap. 2.3).

2.1 (Online-)Fragebogen

Im folgenden Abschnitt wird eine Definition zum (papiergebundenen) Fragebogen (Kap. 2.1.1) und zum Online-Fragebogen (Kap. 2.1.2) geliefert. Außerdem wird der Nutzen (Kap. 2.1.3) von Fragebögen jeglicher Art beschrieben.

2.1.1 Definition: Fragebogen

Der Fragebogen ist mit großem Abstand das meistverwendete Mittel zur Erhebung von Daten (vgl. [Döring03], S. 229). Man unterscheidet zwischen Papier-Fragebögen, und elektronischen Fragebögen[2]. Ein Fragebogen besteht aus einer Reihe von Fragen mit Antwortmöglichkeiten. Eine solche Frage-Antwort-Kombination wird meist *Item* genannt (vgl. [Stangl09]).

Die Befragung, die mittels Fragebogen durchgeführt wird, kann in drei Formen stattfinden. Die älteste Form ist der papiergebundene Fragebogen. Bei diesem Befragungstyp erhält jeder Befragte einen Stift und den Fragebogen in Papierform und ist angehalten, diesen selbstständig zu beantworten.

Eine weitere Form der Befragung ist das Interview. Es kann auf zwei Weisen durchgeführt werden: telefonisch oder in einem persönlichen Gespräch. Bei einem persönlichen Gespräch sitzen der Fragende und der Befragte beieinander und der Fragende stellt seinem Gegenüber die Fragen, die in einem Fragebogen zusammengefasst sind. Dieser Fragebogen kann auch Gesprächsleitfaden genannt werden, da

[2] In dieser Arbeit immer Online-Fragebogen genannt.

er dem Fragenden die Richtung des Gesprächs anzeigt. Beim telefonischen Interview wird das Gespräch mithilfe des Mediums Telefon durchgeführt. Wichtig für beide Arten ist, dass die Unterhaltung für Fragenden und Befragten mühelos und frei von Peinlichkeiten verläuft (vgl. [Stangl09]).

In dieser Arbeit wird das Augenmerk auf die dritte Form der Befragungsart mittels Fragebogen gelegt. Dabei handelt es sich um elektronische, d. h. Online-Fragebögen, welche im folgenden Kapitel erläutert werden.

2.1.2 Definition: Online-Fragebogen

Der Online-Fragebogen, welcher auch elektronischer Fragebogen genannt wird, ist eine Form der Befragung. Er hat einen ähnlichen Aufbau wie ein Fragebogen, nur wird dieser mithilfe von interaktiven Online-Formularen dargestellt oder via E-Mail versendet (vgl. [Döring03], S. 230). Er unterscheidet sich von einem Papier-Fragebogen in erster Linie dadurch, dass er mithilfe von Diensten im Internet zur Verfügung gestellt wird. Das bedeutet, die Befragung setzt voraus, dass der Befragte nicht nur einen Computer besitzt, sondern dieser auch einen Zugang ins Internet hat, um die E-Mail bzw. das Webformular abrufen zu können.

Neben dieser Schwierigkeit existieren noch weitere, z. B. dass der Benutzer auf sich selbst gestellt ist (vgl. [Pratzner01a]). Er hat keine Möglichkeit, sich persönlich nach dem Zweck der Umfrage zu erkundigen, wenn dieser nicht erläutert wird. Folglich kann keine persönliche Vertrauensbasis erzeugt werden. Diese und ähnliche Schwierigkeiten führen dazu, dass die Voraussetzungen ganz bewusst so geschaffen werden müssen, dass der Fragebogen vollständig und korrekt ausgefüllt wird.

2.1.3 Nutzen von Fragebögen

Der Hauptnutzen von Fragebögen besteht darin, Daten zu erheben. Aus den so gewonnenen Daten können wiederum Statistiken o. ä. erzeugt werden.

Friepoertner beschreibt auf seiner Webseite online-fragebogen.com folgende Einsatzgebiete von Online-Fragebögen:

- *Kundenbefragung*
- *Mitarbeiterbefragung*
- *Website-Befragung*
- *Produkttest, Covertest*
- *Feedback-Befragung*
- *Studien und Experimente*
- *Qualitätsmanagement*
- *Beschwerdemanagement*

[Friepoertner09]

Der durch die Befragung über das Web entstehende Vorteil ist, „dass die Daten sofort digital vorliegen und entsprechend komfortabel mit Statistik-Programmen weiterverarbeitet werden können“ ([Döring03], S. 230). Außerdem können via Online-Befragungen spezialisierte und/oder sehr große Zielgruppen erreicht werden (vgl. [Döring03], S. 230). Dies lässt sich dadurch begründen, dass 67,1% der deutschen Bevölkerung bereits im Internet präsent ist. Dabei handelt es sich nicht nur um Jugendliche oder Erwachsene, sondern auch die Generation ab 60 findet immer mehr Interesse am Internet (vgl. [ARDZDF09]).

2.2 Sicherheit im Web

Im folgenden Kapitel wird der Begriff „Sicherheit“ (Kap. 2.2.1) definiert und Techniken aufgezeigt, mit denen man eine sichere Datenübertragung (Kap. 2.2.2) realisieren kann. Darauf folgt ein Abschnitt, der die Begriffe JavaScript und Java Applets (Kap. 2.2.3) genauer erklärt. Der letzte Abschnitt in diesem Kapitel erläutert, was die Datenschutzerklärung eines Webseitenbetreibers (Kap. 2.2.4) ist.

2.2.1 Definition: Sicherheit

Der Begriff „Sicherheit“ wird in der freien Enzyklopädie Wikipedia wie folgt beschrieben:

> *Sicherheit bezeichnet einen Zustand, der frei von unvertretbaren Risiken der Beeinträchtigung ist oder als gefahrenfrei angesehen wird. Mit dieser Definition ist Sicherheit sowohl auf ein einzelnes Individuum als auch auf andere Lebewesen, auf unbelebte reale Objekte oder Systeme wie auch auf abstrakte Gegenstände bezogen.*
>
> *[Wiki09s2]*

Die nachfolgende Erläuterung stellt dar, wie Sicherheit umzusetzen ist. Es erklärt die wichtige Eigenschaft von Sicherheit im Netz.

> *"Sicherheit" ist kein Handbuch, Gerät oder Software-Programm, das man kaufen und sofort erfolgreich einsetzen kann. Sicherheit ist in der vernetzten Computerwelt ein Konzept, welches geplant, umgesetzt und überwacht werden muss, um gegenüber vorhersehbaren und unvorhersehbaren Problemen gewappnet zu sein.*
>
> *[Karadeniz09]*

In dieser Ausarbeitung muss eine Spezialisierung der Sicherheit erfolgen. Es muss speziell die IT-Sicherheit[3] definiert werden. Eine solche Definition der IT-Sicherheit liefert die Webseite des schweizerischen Bildungsservers:

> *Im Bereich der IT-Sicherheit haben wir es jedoch nicht mit Sicherheit im mathematischen Sinne (p=1) zu tun, sondern eher mit einer subjektiven und nur sehr schwer messbaren Sicherheit. In unserem Falle könnte man Sicherheit definieren als "In Erfahrung gegründetes und sich bestätigendes Gefühl, von gewissen Gefahren nicht vorrangig getroffen zu werden". Sicherheit kann nicht umfassend und ohne Doppeldeutigkeit definiert werden.*
>
> *[educa09]*

Als Gefahren sieht der Benutzer den Missbrauch seiner Daten, einen Angriff durch einen Hacker oder den Befall von Viren auf seinem Computer. Genauere Erläuterungen der genannten Gefahren folgen im nächsten Kapitel bzw. im Kapitel 4.2.

Die Definition der IT-Sicherheit sagt aus, dass man die Sicherheit nur schwer erläutern bzw. greifbar machen kann. Die Sicherheit kann man als Konzept sehen, das einem ein Gefühl gibt, vor Gefahren geschützt zu werden. Jedoch muss man die Schutzmechanismen weiterentwickeln, damit dieses Gefühl auch weiterhin bestehen bleibt.

2.2.2 Technologien zur sicheren Datenübertragung

Bei einer Datenerhebung über das Medium Internet ist es wichtig, dass die eingegebenen Daten korrekt übermittelt werden. Zusätzlich muss sichergestellt werden, dass die Daten durch Hacker nicht ausspioniert bzw. manipuliert werden können.

Der Begriff des Hackers kann positiv oder negativ dargestellt werden. Bei der positiven Betrachtung bedeutet der Begriff, dass ein Hacker eine Person mit tiefen Fachkenntnissen ist, die Sicherheitslücken aufzeigt und zu beseitigen versucht oder sie

[3] IT-Sicherheit bedeutet Sicherheit in der Informationstechnologie.

den zuständigen Personen mitteilt, damit sie geschlossen werden können. Oftmals wird der Begriff in negativer Weise verwendet und meint damit eine Person, die unbefugt Sicherheitsbarrieren umgeht und die Sicherheitslücken ausnutzt (vgl. [Wiki09h1]). Diese negative Definition soll verwendet werden.

Damit eine Datenmanipulation erschwert bzw. verhindert wird, gibt es verschiedene Verfahren zur Authentifizierung[4] und sicheren Datenübertragung mittels Webbrowser. Drei solcher Methoden sollen in den nächsten Abschnitten erläutert werden. Dabei handelt es sich um folgende Methoden: Basic Authentication/Digest Access Authentication (Kap. 2.2.2.1), Secure Hypertext Transfer Protocol (Kap. 2.2.2.2) und Secure Socket Layer (Kap. 2.2.2.3).

2.2.2.1 Basic Authentication/Digest Access Authentication

Die Basic Authentication ist ein standardisiertes Verfahren, mit dem sich ein Nutzer mittels Webbrowser bei einem Server als Benutzer authentifizieren kann. Dieses Verfahren ist – wie es der Name „Basic“ ausdrückt – in jedem gängigen Browser implementiert. Es schützt Dokumente oder Verzeichnisse vor unerlaubtem Zugriff. Jedoch garantiert es nur die Authentifizierung, d. h. kryptografische Verschlüsselung[5] der Dateien wird bei diesem Verfahren nicht unterstützt (vgl. [Zahn98]).

Die Authentifizierung durchläuft folgende Schritte (vgl. [Wiki09h2]):

1. Der Webserver fordert eine Authentifizierung für die geschützte Datei an.
2. Daraufhin sucht der Browser nach Benutzername und Passwort für diese Datei. Findet er keine Informationen, so wird der Benutzer gefragt.
3. Anschließend sendet der Browser die Daten mit dem Authorization-Header an den Server.
4. Wenn die Authentifizierung erfolgreich war, wird die Datei an den Benutzer gesendet. Ist das nicht der Fall, so wird der Vorgang abgebrochen.

[4] Die Authentifizierung weist eine behauptete Eigenschaft z. B. eines Gerätes o. ä. nach (vgl. Glossar – Authentifizierung).
[5] Die Verschlüsselung ist ein Vorgang, der einen lesbaren Text in einen nichtlesbaren Text umwandelt (vgl. Glossar – Chiffrierung)

Bei der Digest Access Authentication verläuft die Authentifizierung ähnlich der Basic Authentication. Der Unterschied zwischen den beiden Verfahren ist, dass beim Basic Authentication das Passwort und der Benutzername im Klartext über das Web transportiert werden, was beim Digest Access Authentication nicht der Fall ist.

Bei dieser Methode sendet der Server neben der Forderung einer Authentifizierung (Punkt 1) noch eine zufällig erzeugte Zeichenfolge an den Benutzer. Der Browser berechnet dann den Hashcode[6], d. h. eine Kombination aus Benutzername, Passwort, erhaltener Zeichenfolge, http-Methode[7] und angeforderter URL[8] (Uniform Resource Locator) welche dann mit dem Benutzernamen an den Server gesendet wird (Punkt 3). Der Server berechnet anschließend eine Prüfsumme und entscheidet, ob die Authentifizierung erfolgreich ist oder nicht (Punkt 4). Wichtig ist hierbei zu bedenken, dass die restliche Datenübertragung nicht weiter gesichert ist (vgl. [Wiki09h2]). Dies wird erst mittels S-HTTP möglich, welches im folgenden Kapitel erläutert wird.

2.2.2.2 Secure Hypertext Transfer Protocol (S-HTTP)

S-HTTP (Secure HTTP) ist eine Erweiterung des Protokolls HTTP (Hypertext Transfer Protocol), welches für die sichere Übertragung von Daten in einem Netzwerk genutzt wird. Der Name lässt darauf schließen, dass dieses Protokoll durch das *https* in der Adressleiste angezeigt wird, dies ist allerdings nicht der Fall. Das S-HTTP baut auf drei Arten von Sicherheit auf: Unterschrift[9], Authentifizierung und Verschlüsselung, welche sich alle auf den Benutzer beziehen. Es „kapselt gewöhnliche HTTP-Nachrichten“ [Zahn98]. Die in der Nachricht enthaltenen Nutzdaten werden wie folgt verschlüsselt:

- *Chiffriert*
- *Signiert*
- *Chiffriert und signiert*

[Zahn98]

[6] Der Hashcode ist eine Zeichenfolge, die aus einer Kombination von unterschiedlichen Werten gebildet wird (vgl. Glossar – Hashcode).
[7] Diese Methode bestimmt die Aktion der Client-Anforderung (vgl. Glossar – http-Methode).
[8] Die URL identifiziert bzw. lokalisiert eine Ressource im Netzwerk (vgl. Glossar – URL).
[9] Die digitale Unterschrift ist ein kryptografisches Verfahren (vgl. Glossar – Digitale Unterschrift).

Der Unterschied zwischen signieren und chiffrieren, d. h. verschlüsseln, ist folgender: Signierte Nachrichten bieten dem Empfänger die Möglichkeit, die Identität des Absenders zu überprüfen und davon auszugehen, dass die Datei während der Übertragung nicht manipuliert wurde. Hierbei muss nur der Sender die Nachricht signieren. Verschlüsselte Nachrichten sind sicherer als nur signierte. Diese arbeiten mit Zertifikaten des Senders und Empfängers einer Nachricht, d. h. nur wenn der Sender den *öffentlichen Schlüssel* des Empfängers besitzt, kann eine Nachricht chiffriert werden (vgl. [Apple09]).

Das bedeutet, dass das S-HTTP eine Reihe von Verfahren „für das Handshake[10], für Chiffrierung[11], digitale Unterschrift und mehr“ [Zahn98] unterstützt, sodass sich Dokumente vertraulich austauschen und leicht signieren lassen (vgl. [Zahn98]).

Dieses Verfahren definiert einen sicheren Datenaustausch zwischen Webserver und Webbrowser, indem es die Nutzdaten kapselt. Der Header ist bei diesem Verfahren nicht verschlüsselt. Daher ist es ratsam, das SSL zu verwenden, was eine komplett sichere Verbindung aufbaut (vgl. [Wiki09s1]). Das SSL-Verfahren wird im folgenden Kapitel erläutert.

2.2.2.3 Secure Socket Layer (SSL)/Transport Layer Security (TLS)

In der Literatur findet man oft die Bezeichnung SSL (Secure Socket Layer), welches das Vorgängermodell des TLS (Transport Layer Security) ist (vgl. [Wiki09t1]). Auf Grund des häufigen Vorkommens von SSL in der Literatur wird in dieser Ausarbeitung das Verfahren auch weiterhin unter dem Begriff SSL geführt.

Das SSL ist ein hybrides Verschlüsselungsprotokoll, das zur sicheren Datenübertragung im Internet genutzt wird (vgl. [Wiki09t1]). Es liegt funktional zwischen dem Aufgabenbereich von TCP/IP[12] und den Anwendungen. Jedoch wird es weder von den Transportprotokollen noch von den Applikationen bemerkt, da es transparent

[10] Das Handshake ist ein Verfahren, das eine verlustfreie Datenübertragung zwischen zwei Instanzen aufbaut (vgl. Glossar – Handshake).
[11] Die Chiffrierung ist ein Vorgang, der einen lesbaren Text in einen nichtlesbaren Text umwandelt (vgl. Glossar – Chiffrierung).
[12] TCP/IP ist ein Netzwerkprotokoll. Es regelt im Netzwerk den Datentransport, Datenfluss und die Leitungswege (vgl. Glossar – TCP/IP).

arbeitet, d. h. es müssen keine zusätzlichen Änderungen getätigt werden, damit SSL genutzt werden kann. Während einer sicheren Verbindung kommunizieren die Rechner ausschließlich über den Mechanismus, der von SSL bereitgestellt wird. Soll keine sichere Verbindung hergestellt werden, schaltet sich das SSL-Protokoll selbstständig aus.

Das SSL-Protokoll wird gestartet, indem das bekannte *http* (in der Adressleiste des Webbrowsers) um ein „s“ erweitert wird, d. h. *https*. Folgende Schritte werden dann von dem Browser und Server abgearbeitet (vgl. [Rojahn07]):

1. Der Browser fordert vom angesprochenen Server ein Zertifikat und seinen öffentlichen Schlüssel an.
2. An den Browser wird der Schlüssel mit einer Prüfsumme und einer ID zurückgeliefert[13].
3. Der Browser prüft anhand der übermittelten Daten, ob er wirklich mit dem Server verbunden ist, der in der URL angegeben ist. Ob das der Fall ist, wird auf unterschiedliche Weise dargestellt (siehe „Empfehlungen für die IT“ im Kapitel 4.2).
4. Beide Rechner verständigen sich auf einen symmetrischen Schlüssel, der *Session Key* genannt wird. Da die Absprache in asymmetrischer Verschlüsselung[14] vollzogen wird, ist die Sicherheit gegeben.
5. Vom Browser werden vor dem Datenaustausch Testnachrichten versendet, die nur der Server beantworten kann, wenn es wirklich der Server ist, der er zu sein vorgibt.

Nachdem alle fünf Schritte erfolgreich absolviert worden sind, können die Daten von beiden Parteien mit dem *Session Key* verschlüsselt, übertragen und entschlüsselt werden (vgl. [Rojahn07]).

Neben den bekannten SSL-Zertifikaten gibt es seit 2006 eine Erweiterung, nämlich die *Extended Validation SSL-Zertifikate* (EV-SSL). Diese Zertifikate bieten „in hochsicheren Webbrowsern Informationen zur eindeutigen Identifizierung des Unterneh-

[13] „Diese Informationen werden von einigen wenigen Zertifizierungsfirmen errechnet“ [Rojahn07].
[14] Die Asymmetrische Verschlüsselung ist ein Verschlüsselungsverfahren, das mit öffentlichen Schlüsseln arbeitet (vgl. Glossar – Asymmetrische Verschlüsselung).

mens, das hinter einer Website steht“ [VeriSign09]. Wie sich die EV-Zertifikate „sichtbar“ machen lassen, wird ebenfalls im Kapitel 4.2 „Empfehlungen für die IT“ genauer beschrieben.

2.2.3 JavaScript und Java Applets

Java Applets und die Skriptsprache JavaScript werden in diesem Abschnitt vorgestellt, da sie für die Gestaltung von Online-Fragebögen genutzt werden können. Es wird das Grundlagenverständnis zu diesen zwei Begriffen geliefert.

JavaScript und Java Applets haben trotz der Namens- und syntaktischen Ähnlichkeit nur geringe Gemeinsamkeiten.

Java Applets sind Computerprogramme, die mithilfe der Programmiersprache Java erzeugt worden sind. Sie lassen sich in Webseiten einbinden und werden clientseitig ausgeführt. Hierfür wird vom Webbrowser eine Java-Laufzeitumgebung benötigt, die entweder bereits im Browser vorhanden ist oder noch separat herunter geladen und installiert werden muss. Java Applets werden lokal auf dem Rechner ausgeführt, was ein Risiko sein kann. Man sollte diese daher nur ausführen, wenn man der Webseite, auf der das Applet zur Verfügung gestellt wird, vertraut (vgl. [Linke10]).

JavaScript ist eine Skriptsprache, die hauptsächlich zur Programmierung von dynamischem HTML im Webbrowser eingesetzt wird und direkt in einer HTML-Seite eingebunden ist. Sie ähnelt den C-Sprachen, wozu auch Java gehört (vgl. [Wiki10j1]). Mithilfe von JavaScript hat man die Möglichkeit, den Webauftritt um interaktive Komponenten zu erweitern. Ein Beispiel der interaktiven Nutzung von JavaScript ist die Eingabeüberprüfung in Webformularen, die dem Benutzer direkt eine Falscheingabe zeigt (vgl. [Linke10]) (z. B. die falsche Formatierung eines Datums).

Im Gegensatz zu Java Applets kann JavaScript nicht auf Dateien auf dem lokalen Rechner zugreifen. Die gängigen Webbrowser bieten dem Benutzer die Möglichkeit JavaScript bzw. einzelne Aktionen davon abzuschalten (vgl. [Wiki10j1]). Auch das direkte ausführen von Java Applets kann in Webbrowsern deaktiviert werden. Stattdessen fragt der Webbrowser den Benutzer vor dem Ausführen eines Java Applets, ob dieses gestartet werden soll.

2.2.4 Datenschutzerklärung eines Webseitenbetreibers

Die Datenschutzerklärung soll dem Benutzer einer Webseite die Information liefern, wie Datenschutz betrieben bzw. wie mit personenbezogenen Daten umgegangen wird.

Rechtliche Vorschriften legen fest, dass jede Webseite, die einen Teledienst darstellt, eine besondere Transparenz- und Aufklärungspflicht gegenüber dem Nutzer hat (vgl. [Trautmann05]). Im Telemediengesetz §2 ist ein Teledienst wie folgt charakterisiert:

> *Im Sinne des Gesetzes*
>
> 1. *ist Dienstanbieter jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt,*
> 2. *ist niedergelassener Dienstanbieter jeder Anbieter, der mittels einer festen Einrichtung auf bestimmte Zeit Telemedien geschäftsmäßig anbietet oder erbringt; der Standort der technischen Einrichtung alleine begründet keine Niederlassung des Anbieters,*
> 3. *ist Nutzer jede natürliche oder juristische Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen,*
> 4. *[...]*
>
> *[Telemediengesetz07]*

Somit sind alle gängigen Unternehmenspräsentationen wie Shops, Foren o. ä. im Internet Teledienste und so lässt sich auf jeden Webauftritt §4 Absatz 13 des Telemediengesetzes anwenden, welches einen Datenschutzhinweis in diesen Systemen anordnet (vgl. [Trautmann05]). §4 Absatz 13 des Telemediengesetzes sagt Folgendes aus:

> *(1) Der Dienstanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten [...] zu*

> *unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. [...] Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.*
>
> *[Telemediengesetz07]*

Das bedeutet, dass das Gesetz, dass am 17. Januar 2007 verabschiedet wurde, jeden Teledienst zur Abgabe einer Datenschutzerklärung verpflichtet. Verstöße gegen die Transparenz- und Aufklärungspflicht können mit Strafen bis zu 50.000 Euro geahndet werden (vgl. [Thon07]).

Das Telemediengesetzt wird umgangssprachlich oftmals als „Internetgesetz“ bezeichnet (vgl. [Thon07]).

2.3 Benutzeroberfläche

Die Art und Weise, wie Befehle und Daten in den Computer eingegeben werden, hängt von der Benutzeroberfläche bzw. Benutzerschnittstelle (*User Interface*, kurz UI) ab (vgl. [Mekelburg03]). Die Benutzeroberfläche wird als „Schnittstelle zwischen Computer und Mensch“ [ITWissen09] definiert, da sie der „für den Benutzer sichtbare Teil der Interaktionsschnittstelle eines Softwareprodukts“ [Mekelburg03] o. ä. ist.

Es gibt zwei Arten von Benutzerschnittstellen: die zuerst entwickelte Benutzerschnittstelle ist das textbasierte *Character User Interface* (CUI). Dieses wird beispielsweise im DOS-Betriebssystem benutzt. Die Eingabe kann nur durch Texteingaben oder Tastenkombinationen erfolgen, welche man kennt oder aus Tabellen ablesen muss (vgl. [ITWissen09]).

Der Nachfolger dieser Schnittstelle nennt sich *Graphical User Interface* (GUI), d. h. grafische Benutzeroberfläche. Bei dieser zweiten Art der Benutzerschnittstelle werden Menüs, Schaltflächen u. ä. für die Funktionseingabe und Programmauswahl verwendet, welche mithilfe der Maus oder Tastenkombinationen aktiviert werden (vgl. [ITWissen09]).

Die Benutzeroberfläche wird von Anwendungsprogrammen oder dem Betriebssystem bereitgestellt und „soll dem Benutzer das Arbeiten mit dem Computer erleichtern“ [ITWissen09]. Diese Kommunikation ist ein „wechselseitiger Informationsaustausch zwischen Benutzer und dem System“ [Mekelburg03], welcher bestimmten Regeln folgt. Jedoch liegt die Kontrolle in den meisten modernen interaktiven Systemen beim Benutzer.

Dieser Kommunikationsprozess lässt sich in folgende drei Abschnitte einteilen, in denen jeweils das System oder der Benutzer beschäftigt ist:

1. *Das System wartet auf die Auslösung einer Funktion durch den Benutzer oder fordert dazu auf.*
2. *Der Benutzer löst eine der zur Verfügung stehenden Funktionen aus.*

3. *Die Ausführung der Funktion und die Ausgabe des Ergebnisses durch das System (inkl. Fehlermeldungen, Hilfen und Erklärungen).*

[Mekelburg03]

Wie beschrieben, ist die Benutzerschnittstelle bzw. Benutzeroberfläche ein wichtiger Punkt für die Interaktion zwischen Benutzer und dem System, sodass dieser Aspekt für den Vertrauensaufbau von großer Bedeutung ist.

3 Vertrauen

Wie der Titel verdeutlicht, steht das „Vertrauen“ im Fokus dieser Arbeit. Aus diesem Grund wird es nicht im Rahmen der Grundlagen betrachtet, stattdessen wird ihm ein eigenes Kapitel gewidmet. Dieses Kapitel beginnt damit, dass Definitionen den Begriff „Vertrauen“ genauer erläutern (Kap. 3.1). Darauf folgt eine Aufzählung von Vertrauensarten (Kap. 3.2) und ein Modell (Kap. 3.3), das zeigt, wie der Vertrauensaufbau zwischen zwei Personen vollzogen wird. Zuletzt wird eine Zusammenfassung (Kap. 3.4) zum Themengebiet „Vertrauen“ gegeben, in der beschrieben wird, wie Vertrauen in dieser Arbeit verstanden wird.

3.1 Definition

> *Unser Alltag ist überwiegend von Vertrauen geprägt, […].*
>
> *[Ulrich08], S. 54*

Diese Zitat sagt aus, dass der Mensch sein Handeln im Alltag auf sein Wissen, Vorhersagen oder Erwartungen stützt und in diese Vertrauen setzt, da auf der Grundlage von Misstrauen das individuelle Leben und Zusammenleben nur schlecht funktionieren könnte (vgl. [Ulrich08], S. 55). Er traut den Empfehlungen, deren Richtigkeit nicht immer bewiesen wird (z. B. Befragung von Horoskop oder Astrologie), da der Entscheidungs- und Handlungsdruck im Alltag sonst ins Unermessliche wachsen würde, was das alltägliche Handeln und Leben nicht praktikabel machen würde (vgl. [Ulrich08], S. 54).

Zusammengefasst sagt das Zitat aus, wie wichtig Vertrauen im Alltag und somit im Umgang miteinander ist. Eine einheitliche und feststehende Definition von Vertrauen gibt es jedoch nicht, da es „eine Ausweitung des Bedeutungsfeldes auf alle nur denkbaren Gebiete gibt“ ([Petermann85], S. 9).

Im Folgenden werden verschiedene Definitionen geliefert, die der Psychologie entstammen. Die für die „empirische Vertrauensforschung wohl bedeutsamste

Definition“ ([Kassebaum04], S. 8) ist von Rotter, welcher einer der wichtigsten Forscher im Gebiet der Vertrauens-Psychologie ist:

> *Vertrauen basiert auf der Erwartung einer Person oder einer Gruppe, sich auf ein mündlich oder schriftlich gegebenes Versprechen einer anderen Person bzw. Gruppe verlassen zu können.*
>
> *Rotter in [Petermann85], S. 12*

Eine weitere bekannte Definition von „Vertrauen“ gibt es von Luhmann, welche ebenfalls in ([Petermann85], S. 12) zu finden ist:

> *Vertrauen reduziert die Komplexität menschlichen Handelns und gibt Sicherheit.*
>
> *Luhmann in [Petermann85], S. 12*

Diese Definition, die Eigenschaften von Vertrauen aufzeigt, sagt aus, dass die Probleme bzw. Hindernisse, die beim menschlichen Handeln entstehen können durch Vertrauen verringert bzw. abgesichert werden und der Mensch dadurch wohl eher bereit ist, eine Entscheidung zu treffen.

Luhmann behandelt „das institutionelle bzw. Systemvertrauen und beschäftigt sich nicht mit der Entstehung, sondern mit der „Funktion des Vertrauens“ in den Systemen“ ([Kluck09], S. 36). In seiner Definition spiegelt sich außerdem noch wider, dass die Sicherheit ein wichtiger Bestandteil von Vertrauen ist. Aus diesem Grund wird in dieser Arbeit oftmals der Begriff Sicherheit im Zusammenhang mit „Vertrauen“ erwähnt.

Eine weitere Definition von Vertrauen, die man konkreter auf die IT (Informationstechnologie) beziehen kann, liefert Rüdiger Grimm in seiner Ausarbeitung „Vertrauen im Internet“:

Vertrauen ist die Gewissheit (d. h. eine innere Repräsentanz des Eintretens) einer erwünschten Zukunft. Es beruht

- *auf der Kontinuität des regelhaften und erwünschten Verhaltens der Umgebung*
- *oder auf der Hilfe vertrauter Menschen (auch in unwägbarer Lage)*
- *oder auf der eigenen Kenntnis und Beherrschung der Lage (einschließlich ihrer Unwägbarkeiten)*

Diese drei Elemente von Vertrauen schließen sich nicht aus, […] sie ergänzen sich in aller Regel.

[Grimm01], S. 69f

Die in dem Zitat genannten Punkte bieten die Möglichkeit, zu definieren, welches Vertrauen von wem geleistet wird.

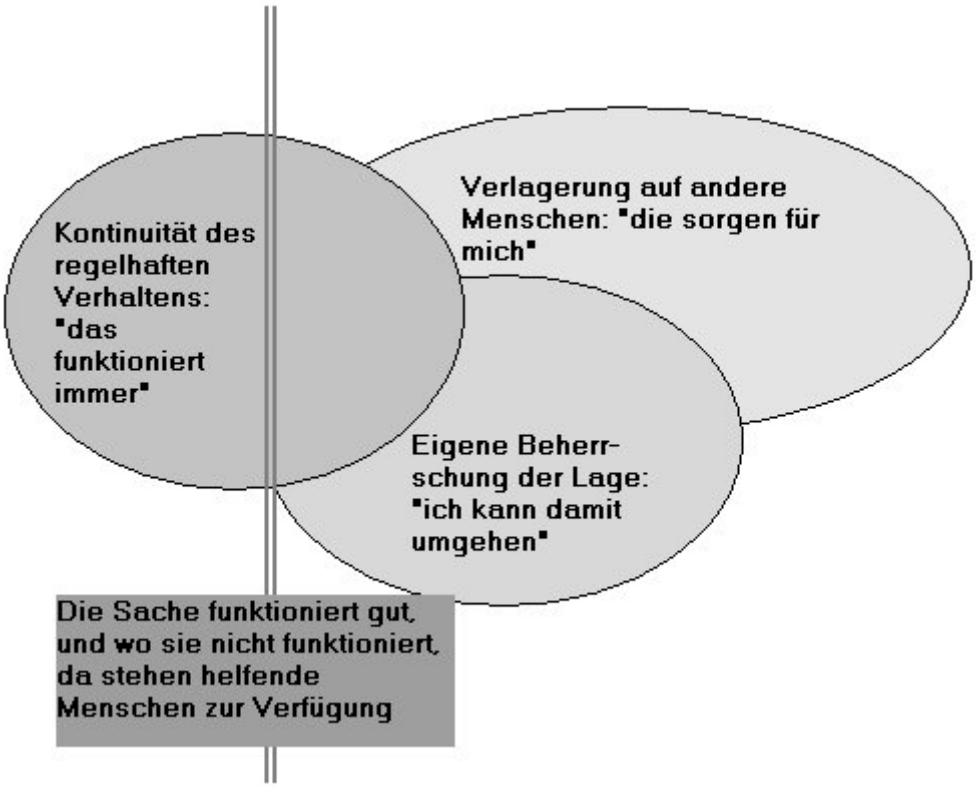

Abbildung 1: Grenzen zw. Mensch und (tech.) Funktionalität bei "Vertrauen"[15]

[15] Quelle: [Grimm01], S. 71.

Die Abbildung 1 stellt das Zusammenspiel der drei genannten Aspekte dar und es kann die Aussage getroffen werden, dass der erste Punkt, „*Kontinuität des regelhaften Verhaltens der Umgebung*“ auf der Funktionalität der Umgebung beruht und sich mithilfe technischer und organisatorischer Verfahren darstellen lässt. Die anderen zwei Punkte beziehen sich auf Menschen. Daher ist zwischen den drei zusammengehörenden Punkten eine Grenze abgebildet, die die Trennung zwischen Mensch und Technik darstellen soll (vgl. [Grimm01], S. 71f).

Wie bereits erwähnt, gibt es nicht die eine richtige und vollständige Definition von Vertrauen. Jedoch kann man aus der Mehrheit der Definitionen[16] gemeinsame Merkmale herleiten:

Wesentlich im Verständnis von Vertrauen ist:

- *Der Aspekt der Ungewissheit,*
- *Das Vorhandensein eines Risikos,*
- *die mangelnde Beeinflussung des Schicksals (freiwilliger oder erzwungener Kontrollverzicht) und*
- *die Zeitperspektive (auf die Zukunft ausgerichtet).*

[Petermann85], S. 13

Nachdem Definitionen von Vertrauen geliefert worden sind, stellt sich nun die Frage, wann Vertrauen wichtig wird. Im Allgemeinen kann man sagen, dass unter folgenden Bedingungen Vertrauen notwendig wird:

- *Es muss eine risikoreiche Situation vorhanden sein;*
- *Diese Situation muss auch erkannt und wahrgenommen werden;*
- *Dieser Situation kann nicht ausgewichen werden, sei es weil es nicht möglich ist oder man diese Möglichkeit nicht sieht.*

[Rohner04], S. 4

[16] Eine Zusammenfassung von Vertrauensdefinitionen liefert Petermann in seinem Buch „Psychologie des Vertrauens“ ab S. 12.

Vertrauen bildet sich also anhand eigener Erfahrungen oder Erfahrungen von Mitmenschen. Diese Erfahrungen werden erfragt, sobald eine risikoreiche Situation eintritt bzw. eine Entscheidung gefordert wird. Solch eine Entscheidung wird dann entsprechend der berichteten oder eigenen Erfahrungen getroffen, d. h. in diesem Moment wird der Akt des Vertrauens vollzogen. Dieser Sachverhalt verweist darauf, dass bei einer wissenschaftlichen Beurteilung einer Entscheidung, die auf Vertrauen basiert, auch andere Faktoren wie Herkunft, Wissensstand, etc. beachtet werden müssen, um der Komplexität menschlicher Entscheidungsprozesse adäquat zu begegnen (vgl. [Kluck09], S. 36).

3.2 Arten von Vertrauen

In der Literatur findet man verschiedene Ansichten über den Prozess der Vertrauensbildung. „Allgemein betrachtet sind bei dem Konstrukt des Vertrauens zwei Parteien involviert: Die eine Partei, die vertraut und die andere Partei, der Vertrauen entgegen gebracht wird“ ([Greschuchna06], S. 74). Eine Person oder Organisation kann dabei als Partei fungieren. Mithilfe dieser Grundaussage lassen sich vier Vertrauensarten beschreiben:

1. *Interpersonales Vertrauen*
2. *Personales Vertrauen in Systeme (organisationales Vertrauen)*
3. *Organisationsvertrauen in Personen*
4. *Interorganisationales Vertrauen*

[Greschuchna06], S. 74

Eine grafische Darstellung dieser Vertrauensarten wird ebenfalls in ([Greschuchna06], S. 75) geliefert:

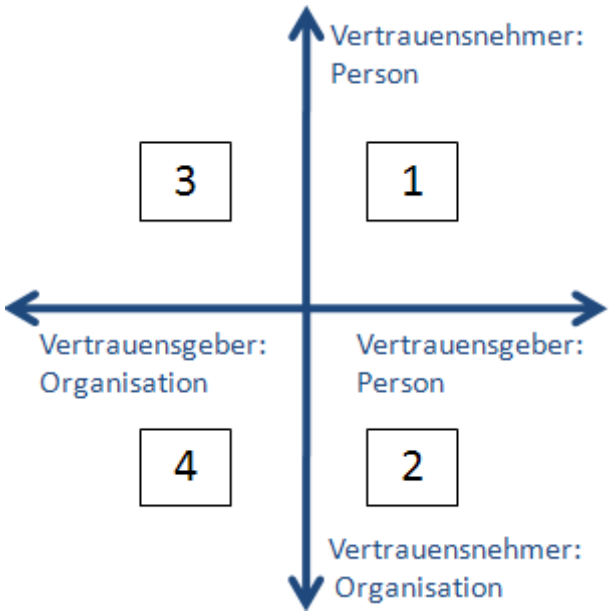

Abbildung 2: Arten von Vertrauen[17]

[17] Die Grafik ist in Anlehnung an [Greschuchna06], S. 75 erstellt.

Mit interpersonalem Vertrauen ist das Vertrauen gemeint, das sich zwischen Personen aufbaut (vgl. [Fladnitzer06], S. 147). Während beim personalen Vertrauen eine Person einer Institution vertraut (vgl. [Greschuchna06], S. 75).

Bei dem Organisationsvertrauen in Personen genießt eine Person das Vertrauen einer Organisation. Während bei der vierten Form von Vertrauen zwei Organisationen die Parteien sind und jeweils einer davon Vertrauensnehmer bzw. -geber ist.

Das personale Vertrauen in Systeme wird in der Literatur auch als Systemvertrauen bezeichnet. In „Kommunikation und Vertrauen in der Ethnomethologie[18]“ von Wenzel wird Systemvertrauen wie folgt beschrieben:

> *Systemvertrauen heißt Vertrauen gegenüber abstrakten Funktionssystemen und ist für Luhmann eine Form reflexiven Vertrauens, da soziale Funktionssysteme in der Regel soziale Beziehungen zu einem geringen Publikum nicht auf persönliche, emotionale Bindungen aufbauen, aber für die Bewältigung der Kontingenz[19] einer komplexen Welt trotzdem Vertrauen brauchen.*
>
> *[Wenzel01], S. 343*

Mit Systemvertrauen wird daher das Vertrauen in Systeme, also zum Bespiel auch das Vertrauen in Online-Fragebögen, bezeichnet.

Nachdem die Arten von Vertrauen erläutert worden sind, wird im nächsten Abschnitt ein einfaches Modell zur interpersonellen Vertrauensbildung gezeigt.

[18] Die Ethnomethologie ist die Soziologie des Alltäglichen (vgl. Glossar – Ethnomethologie).
[19] Die prinzipielle Offenheit und die Ungewissheit menschlicher Lebenserfahrung (vgl. Glossar – Kontingenz).

3.3 Modell zur Vertrauensbildung: Drei-Phasen-Modell

Das Drei-Phasen-Modell von Franz Petermann wird in seinem Buch „Psychologie des Vertrauens“ beschrieben und geht auf seine eigene Studie zur Arzt-Kind-Interaktion[20] zurück, was das interpersonale Vertrauen erklärt. Anhand seiner Studie formuliert Petermann, dass „man Vertrauen nur aufbauen kann, wenn keine Angst vorliegt und sich die Kinder sicher fühlen“ ([Petermann85], S. 118).

In diesem Modell wird deutlich, dass Vertrauen nur möglich ist, wenn ein Mindestmaß an Sicherheit gegeben ist und die Sicherheitssignale (in Petermanns Studie: Gesten, verbale Ankündigungen) „zu finden und zu entziffern sind“ ([Petermann85], S. 118). Aus dieser Erkenntnis baut Petermann das Drei-Phasen-Modell zur Vertrauensbildung auf:

1. *Phase: Herstellen einer verständnisvollen Kommunikation*
2. *Phase: Abbau bedrohlicher Handlungen*
3. *Phase: Gezielter Aufbau von Vertrauen*

[Petermann85], S. 120

In der ersten Phase muss „durch einen offenen und ehrlichen Austausch die verständnisvolle Kommunikation aufgebaut werden“ ([Kluck09], S. 41).

In der zweiten Phase muss diese Bedrohung durch „geplantes Verhalten abgebaut werden“ ([Petermann85], S. 120). Bedrohungen entstehen durch „Handlungen – vor allem gegenüber Partnern, die sich unterlegen fühlen“ ([Petermann85], S. 120).

In der dritten Phase findet der Vertrauensaufbau statt, d. h. „dass der Vertrauensgeber Vertrauen in die Kompetenz des Vertrauensnehmers“ ([Kluck09], S. 42) setzt und der Vertrauensnehmer durch gezielte Handlungen nun das volle Vertrauen gewinnen kann (vgl. [Petermann85], S. 122).

[20] Die Zielsetzung und das Vorgehen dieser Studie wird in [Petermann85] ab Seite 100 beschrieben.

Das Drei-Phasen-Modell wird in der unten dargestellten Grafik gezeigt (vgl. [Petermann85], S. 121)

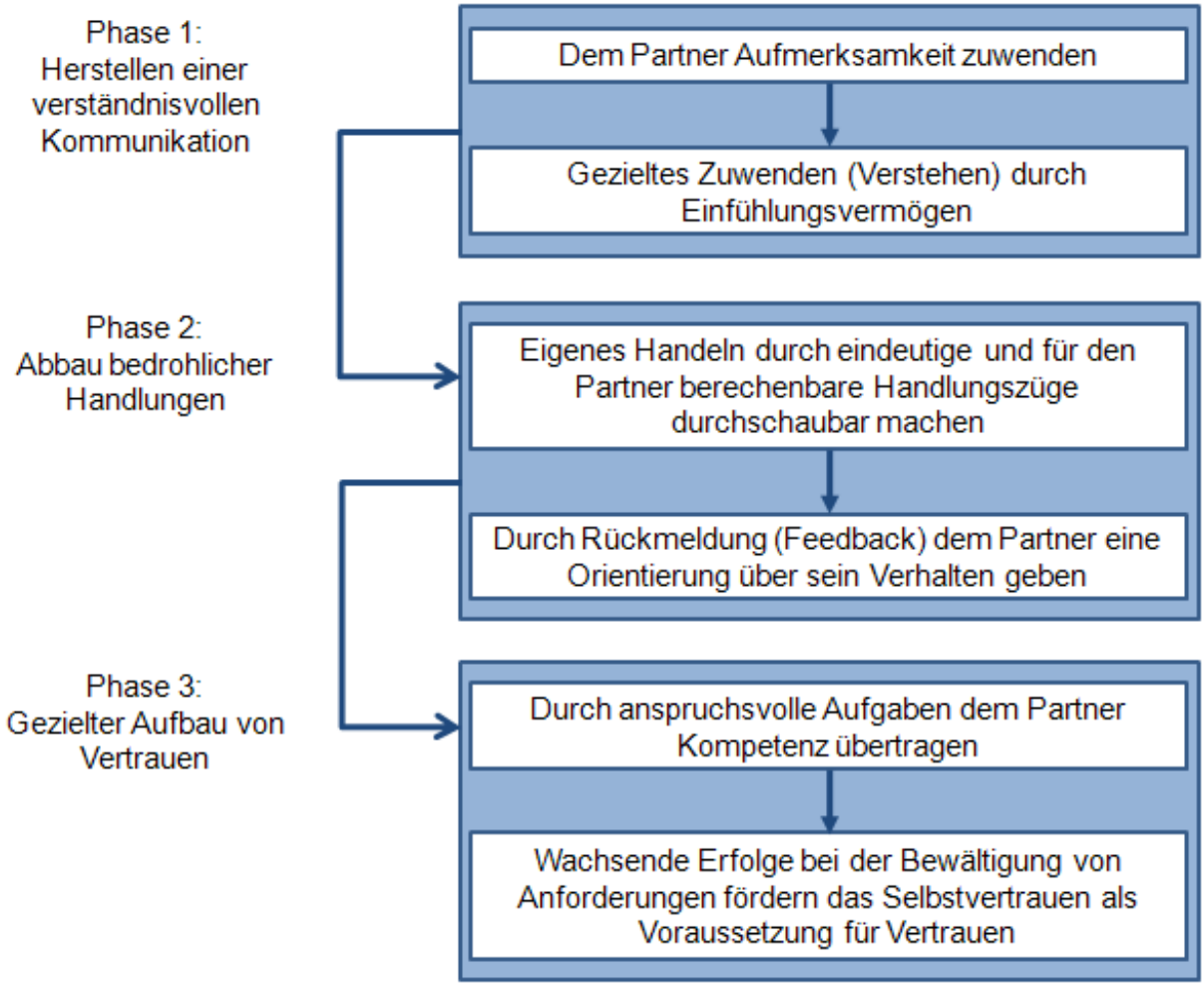

Abbildung 3: Drei-Phasen-Modell des Vertrauensaufbaus

Petermann fasst Vertrauen somit als aktiven Prozess auf, „der entscheidend vom Ausmaß des empfundenen eigenen Kompetenzgefühls (Selbstvertrauen) abhängt“ ([Petermann85], S. 125).

3.4 Verständnis des Begriffs „Vertrauen“ im Kontext dieser Arbeit

In dieser Arbeit wird dargelegt, welche Kriterien wichtig sind, um Vertrauen zu einem Online-Fragebogen aufzubauen. Diese Merkmale können als Sicherheitsmerkmale, die laut Petermann gegeben werden müssen, damit Vertrauen entsteht (vgl. [Petermann85], S. 118), gesehen werden und sollen dem Befragten eines Online-Fragebogens helfen, das Vertrauen aufzubauen.

Der Hauptteil beschäftigt sich damit, wie das Systemvertrauen einer Person zu einem System, d. h. dem Online-Fragebogen, erzeugt werden kann. Dieses Vertrauen soll mittels der nachfolgenden Empfehlungen aufgebaut werden.

Das Drei-Phasen-Modell für das interpersonale Vertrauen soll in dieser Arbeit darstellen, dass lediglich die erste Phase des Vertrauensaufbaus durch technische Möglichkeiten erreicht werden kann. Wie bereits in der Grafik auf Seite 30 angedeutet, kann man mit der heutigen Technik nicht den gesamten Vertrauensaufbau mittels technischer Objekte erzeugen.

4 Aufbau des Vertrauens bei Online-Fragebögen

Das folgende Kapitel stellt den Hauptteil der Bachelorarbeit dar. Es besteht aus einer Erklärung zur Zielgruppenbestimmung (Kap. 4.1), einer Empfehlungen für die IT (Kap. 4.2), einigen Gestaltungshinweisen für die Benutzeroberfläche (Kap. 4.3) und Hinweisen zur Fragenkonstruktion (Kap. 4.4) eines Online-Fragebogens.

4.1 Bestimmung der Zielgruppe

Eine Zielgruppe ist eine Gruppe von Marktteilnehmern, an die sich eine bestimmte Werbung oder ein bestimmtes Angebot richtet. Der Sinn einer Zielgruppenbestimmung ist, sein Angebot auf die bestimmte Zielgruppe anpassen zu können (vgl. [Bless08], S. 12) und somit z. B. bei einer konkreten Werbemaßnahme mehr Gewinn zu erwirtschaften.

Zielgruppen lassen sich nach zwei Arten von Merkmalen unterscheiden. Zum einen kann man Personen hinsichtlich soziodemographischer Eigenschaften unterteilen, d. h. man betrachtet z. B. die Altersgruppen oder den Wohnort. Zum anderen gibt es noch psychografische Merkmale, wie das Konsumverhalten, die Vorlieben, etc. von Personen (vgl. [Bless08], S. 12).

Für alle in den folgenden Kapiteln beschriebenen Empfehlungen gilt, dass die Maßnahmen zur Vertrauensbildung zielgruppengerecht ausgewählt werden sollte. Nicht alle Zielgruppen haben das gleiche Vorwissen im Bereich der Informationstechnologie, was dazu führen kann, dass nicht alle Merkmale sofort richtig erkannt bzw. verstanden werden und in der Konsequenz der Vertrauensaufbau nicht gelingt.

Der gelernte Informatiker beschäftigt sich wahrscheinlich stärker mit dem Medium Internet und kennt daher eher die Anzeichen für eine sichere Datenübertragung als eine Sekretärin, die nur ihre Aufgaben am Computer erledigt und ab und zu im Internet etwas recherchiert.

Aus diesem Grund ist es von zentraler Bedeutung, vor der Erstellung des Online-Fragebogens folgende Fragen zu beantworten, die für die Findung der Zielgruppe behilflich sind:

- Was ist Untersuchungsgegenstand des Online-Fragebogens?
- Welcher Personenkreis soll die Fragen beantworten?
- Können die gewünschten Personen die Fragen beantworten?
- Werden alle Personen über den Online-Fragebogen erreicht?

4.2 Empfehlungen für die IT

Durch die Verbreitung von IT-gestützten Kommunikationssystemen ist die Forderung der Sicherheit seitens der Nutzer immer größer geworden. Wie bereits beschrieben, kann der Benutzer erst Vertrauen aufbauen, wenn er sich sicher fühlt[21]. Man muss daher bei der Erstellung des Online-Fragebogens beachten, wie der Benutzer ein Sicherheitsgefühl aufbauen kann.

Der Benutzer hat mittels unterschiedlicher Schutzfunktionen die Möglichkeit, sein Sicherheitsbedürfnis selbst zu bestimmen (vgl. [EggMüller01], S. 31). Dazu gehört beispielsweise die Installation von Antiviren-Programmen o. ä.

Ein Antiviren-Programm schützt Computer vor Viren. Viren sind Programme, die z. B. via E-Mail versendet werden oder mit Downloads ungewollt aus dem Internet heruntergeladen werden und unbemerkt Schaden auf dem Computer anrichten können. Ein Antivirenprogramm soll Viren auffinden, anzeigen und beseitigen (vgl. [Groß09], S. 3).

Aus dem Buchabschnitt von Egg und Müller „Sicherheit und Vertrauen: Mehrwert im E-Commerce“ lassen sich folgende Klassifikationen von Schutzzielen nennen, die dem Benutzer helfen sollen, die erwünschte Sicherheit zu formulieren ([EggMüller01], S. 31):

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Zurechenbarkeit

Die Begriffe Integrität, Verfügbarkeit und Zurechenbarkeit sollen darauf hinweisen, dass man möchte, dass das System nicht manipuliert werden kann und immer zur Verfügung steht. Zusätzlich möchte der Benutzer immer vom System wissen, was es während der unterschiedlichen Vorgänge tut. Die Vertraulichkeit in der Aufzählung weist darauf hin, dass das Vertrauen von Benutzern darauf basiert, dass es funktionierende Sicherheitssysteme gibt.

[21] Vgl. Kap. 3.3 und [Petermann85], S. 181.

Im Folgenden wird nun beschrieben, welche Sicherheitsmaßnahmen für Online-Fragebögen sinnvoll sind und wie der gewählte Sicherheitsmechanismus dem Benutzer verständlich und in der Folge vertrauensbildend präsentiert werden kann. Denn im Internet muss der Benutzer dem Betreiber vertrauen, zumal er nicht immer die Option hat, eigene Schutzfunktionen zu implementieren. Aus diesem Grund muss der Betreiber versuchen, dem Benutzer die Sicherheitsmechanismen entsprechend zu kommunizieren und so das Vertrauen aufzubauen.

Von den in Kapitel 2.2.2 „Technologien zur sicheren Datenübertragung“ vorgestellten Sicherheitsmethoden ist das SSL-Protokoll das Verfahren, das in Verbindung mit Online-Fragebögen verwendet werden sollte. Dieses Verfahren schafft nämlich unter folgenden Gesichtspunkten eine sichere Verbindung:

1. *Die Verbindung ist im besten Sinne privat, weil ihr Inhalt nur verschlüsselt über das Netz geht.*
2. *Die Identität des Servers steht fest.*
3. *Wirkungsvolle Algorithmen prüfen, ob die Daten vollständig und unverändert ihren jeweiligen Empfänger erreichen.*

[Rojahn07]

Außerdem besitzt dieses Verfahren einige sichtbare Merkmale, welche nachfolgend beschrieben werden.

Das erste sichtbare Merkmal einer sicheren Verbindung, das dem Benutzer auffallen könnte, ist die Erweiterung der Webadresse um ein „*s*“, von *http* auf *https*. Wie bereits beschrieben, bedeutet dies, dass die SSL-Verbindung gestartet wird. Darüber hinaus ist es auch ein – wenn auch eher unauffälliges – optisches Merkmal für den Benutzer.

Zusätzlich zu dem „s“ zeigen die bekannten Webbrowser bei einer SSL-Verbindung ein Symbol o. ä. an, das dem Benutzer das Erkennen einer sicheren Verbindung erleichtert (vgl. [Groß09], S. 1).

Die nun folgenden Abbildungen wurden mit dem Internet Explorer 7 von Microsoft®[22] unter dem Betriebssystem Windows XP erstellt bzw. mit dem Firefox® 3 von Mozilla unter dem Betriebssystem Windows XP, da sie die am meisten genutzten Webbrowser sind (vgl. [Zimmermann09]).

Abbildung 4: Darstellung von SSL beim Internet Explorer

Die Abbildung 4 zeigt die Darstellung des SSL-Verfahrens beim Internet Explorer. Mithilfe des Schlosses neben der Navigationsleiste wird darauf hingewiesen, dass es sich um eine sichere SSL-Verbindung handelt.

In Abbildung 5 wird die Darstellung der sicheren SSL-Verbindung beim Firefox präsentiert. Bei diesem Browser zeigt das Schloss am unteren Fensterrand an, dass über den Link eine sichere SSL-Verbindung hergestellt ist und die Daten verschlüsselt übermittelt werden.

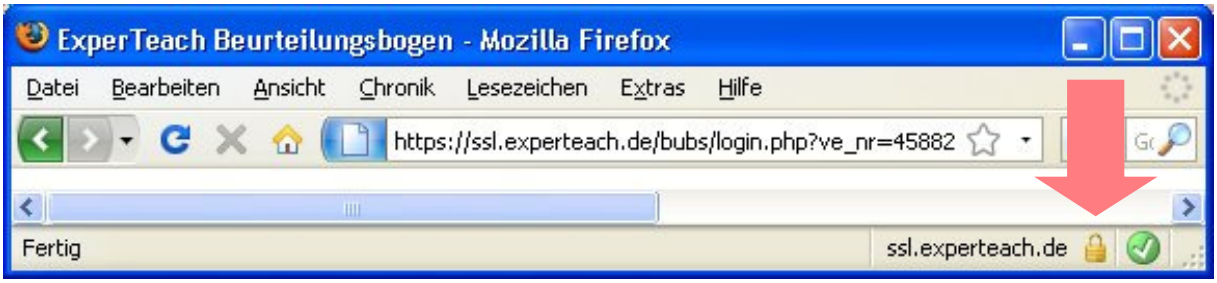

Abbildung 5: Darstellung von SSL beim Firefox

Neben den Symbolen, die die Webbrowser bei einer sicheren Verbindung anzeigen, gibt es noch ein weiteres Merkmal zur schnellen Erkennung einer SSL-Verbindung. Dieses Merkmal wird allerdings nur bei bestimmten Voraussetzungen dargestellt.

[22] Das Unternehmen Microsoft® und das Produkt Firefox® sind eingetragene Marken, welche in dieser Ausarbeitung fortwährend unter dem Begriff Microsoft bzw. Firefox geführt werden, um eine gute Lesbarkeit zu gewähren.

Bei Verwendung von EV-SSL-Zertifikaten[23] und neueren Webbrowser-Versionen (beim Internet Explorer bei bestimmten Voraussetzungen[24] ab Version 7, sonst ab Version 8) färbt sich sogar die Navigationsleiste bzw. der Registertabulator grün, wenn die Daten in verschlüsselter Form übertragen werden. Die Färbung der Adressleiste beim Firefox von Mozialla zeigt Abbildung 6.

Abbildung 6: Farbige Navigationsleiste beim Firefox

Damit die farbige Navigationsleiste beim Internet Explorer dargestellt werden kann, wurde die Abbildung 7 mit dem Internet Explorer 8 erstellt und nicht wie alle anderen Internet-Explorer-Grafik mit der Version 7.

Abbildung 7: Farbige Adressleiste beim Internet Explorer 8

Das SSL-Verfahren kann auch mithilfe unbekannter oder abgelaufener SSL-Zertifikate gestartet werden. In diesem Fall sollte der Benutzer keine sensiblen Daten preisgeben, da die Seriosität des Webseitenbetreibers angezweifelt werden kann. Solch ein unglaubwürdiges Zertifikat wird von den Browsern in besonderer Weise dargestellt, damit der Benutzer dies bemerkt und seine Daten schützen kann.

[23] Siehe Kap. 2.2.2.3 „Secure Socket Layer (SSL)/Transport Layer Security (TLS)“.

[24] „Browser erkennen die Authentizität von SSL-Zertifikaten, indem sie überprüfen, ob das Zertifikat mit einer gültigen SSL-Root auf dem Client-Rechner übereinstimmt. VeriSign signiert jedes EV-SSL-Zertifikat mit zwei Roots: einer EV-Root und einer herkömmlichen SSL-Root. Mit zwei Roots erkennt jeder Browser eine gültige SSL-Root, selbst ältere, die noch kein EV kennen. IE7 ist dafür vorgesehen, Extended Validation zu erkennen, was aber unter Windows XP eventuell nicht korrekt angezeigt wird, da die traditionelle SSL-Root eher erkannt wird als die EV-Root. Systeme mit Windows XP aktualisieren den Root Store nicht automatisch“ [VeriSign09].

Beim Firefox wird ein fehlerhaftes Zertifikat mit einem veränderten Schloss dargestellt. Das Schloss am unteren Bildschirmrand erhält einen roten Kreis mit einem Ausrufezeichen, das signalisieren soll, dass die Webseite nicht vertrauenswürdig ist, da z. B. der Inhaber des SSL-Zertifikates nicht angegeben ist (siehe Abbildung 8).

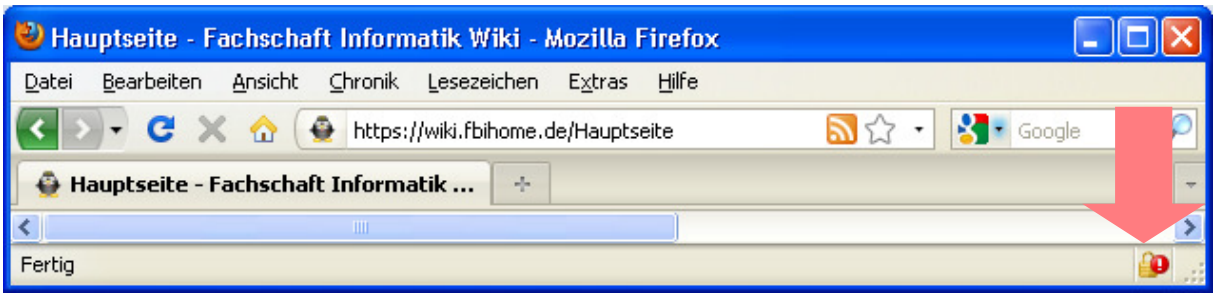

Abbildung 8: Fehlerhaftes SSL-Zertifikat beim Firefox

Weitere Hinweise erhält der Benutzer vom Firefox nur, wenn die dafür benötigten Einstellungen im Browser gesetzt worden sind. Ist das nicht der Fall, kann der Benutzer nur anhand des kleinen Symbols am Fensterrand ein ungültiges Zertifikat erkennen.

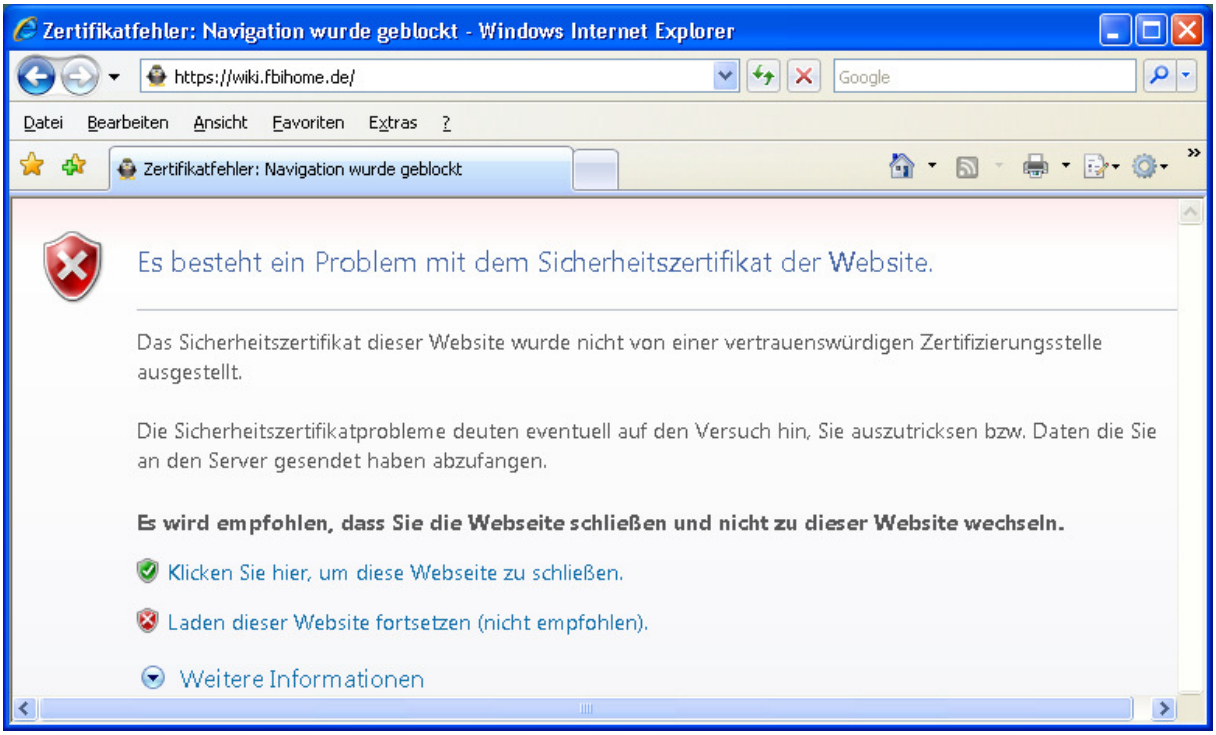

Abbildung 9: Hinweisseite beim Internet Explorer

Der Internet Explorer dagegen weist den Benutzer mittels einer Hinweisseite darauf hin, dass der Webseitenbetreiber kein gültiges Zertifikat nutzt. Diese Hinweisseite wird in Abbildung 9 dargestellt.

Hier wird explizit eine Entscheidung vom Benutzer gefordert. Er kann die Webseite schließen und besucht damit die Zieladresse nicht oder er fordert den Browser auf, die gewählte Webseite darzustellen, obwohl das Zertifikat unglaubwürdig erscheint. Bei Letzterem wird das Laden der geforderten Webseite fortgeführt und der Benutzer gelangt an sein Ziel.

Während der Benutzer die unglaubwürdige Webseite besucht, weist der Webbrowser von Microsoft den Benutzer allerdings weiterhin auf die Unsicherheit der Webseite hin, indem der Browser die Adressleiste rot einfärbt und daneben den Hinweis „Zertifikatfehler“ anzeigt.

Abbildung 10: Fehlerhaftes SSL-Zertifikat beim Internet Explorer

Prinzipiell hat der Benutzer jederzeit die Möglichkeit, sich weitere Informationen zu dem Zertifikat anzeigen zu lassen, wobei die Art und die Vertrauenswürdigkeit des SSL-Zertifikats irrelevant sind.

Die beschriebenen Zertifikatsinformationen erhält man, indem man auf das jeweilige Symbol klickt. Beim Internet Explorer ist das Symbol zum Aufrufen der Zertifikatsinformationen das Schloss in der Navigationsleiste (siehe Abbildung 4) bzw. der Hinweis „Zertifikatfehler“ (siehe Abbildung 10). Beim Firefox muss man auf das Schloss am unteren Fensterrand klicken (siehe Abbildung 5 bzw. Abbildung 8).

Die folgenden Abbildungen zeigen die Zertifikatsinformationen von vertrauenswürdigen SSL-Zertifikaten an.

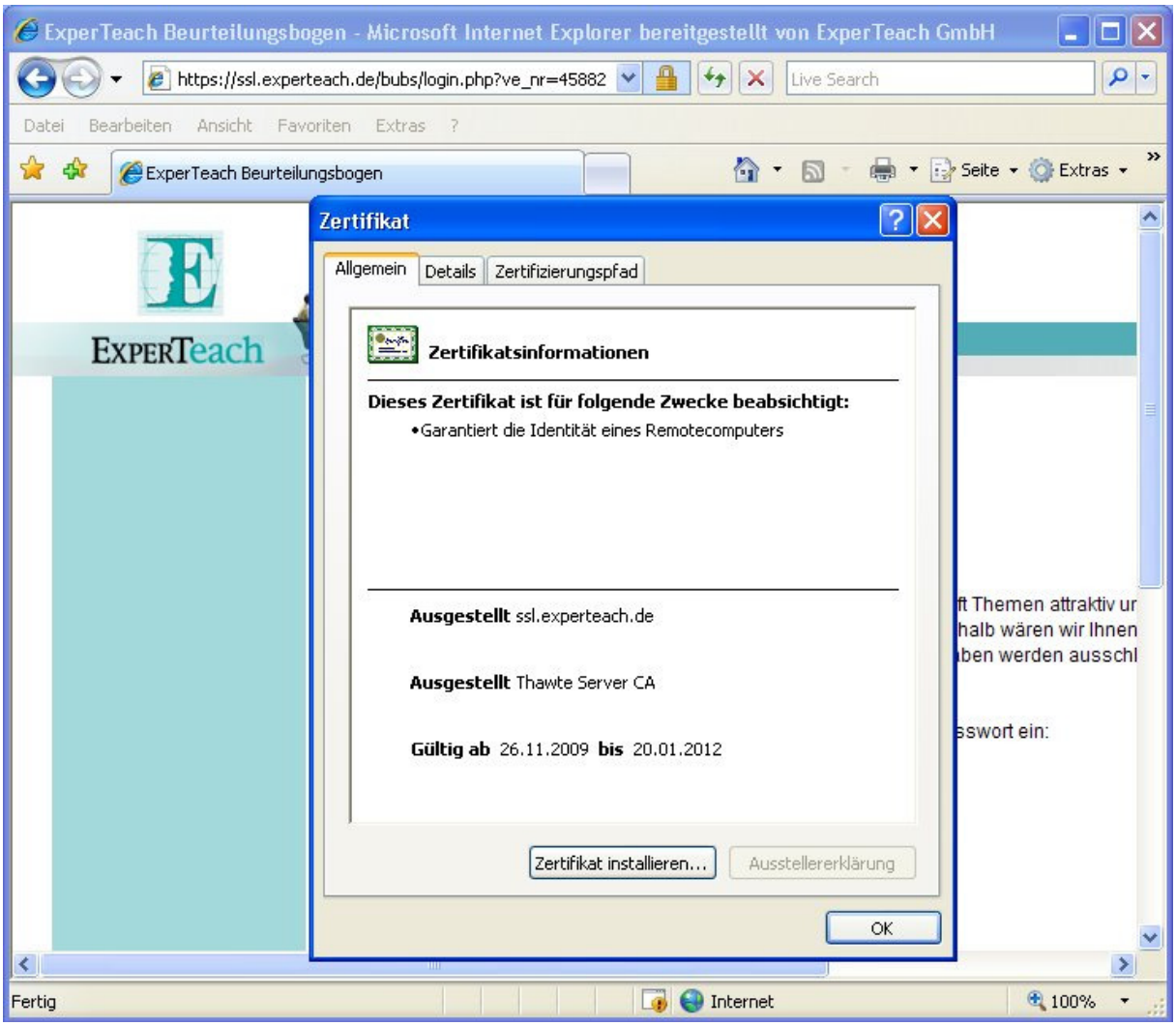

Abbildung 11: Zertifikatsinformationen beim Internet Explorer

Die Zertifikatsinformation, die beim Internet Explorer dargestellt wird (Abbildung 11), zeigt auf dem ersten Register eine garantierte Identität, den Zertifikatausteller und den Gültigkeitszeitraum. Detailliertere Informationen zum Zertifikat sind über die Registerkarte „Details“ und „Zertifizierungspfad“ erreichbar.

Beim Firefox von Mozilla sind die Zertifikatsinformationen auf der Seiteninformation angesiedelt, die über das Schloss am unteren Fensterrand aufgerufen wird. Diese Seite zeigt neben den drei bereits genannten Informationen noch Technische Details sowie Informationen zum Thema Datenschutz und Chronik an (Abbildung 12). Weitere Informationen zum SSL-Zertifikat kann der Benutzer über die Schaltflächen auf der Seiteninformation aufrufen.

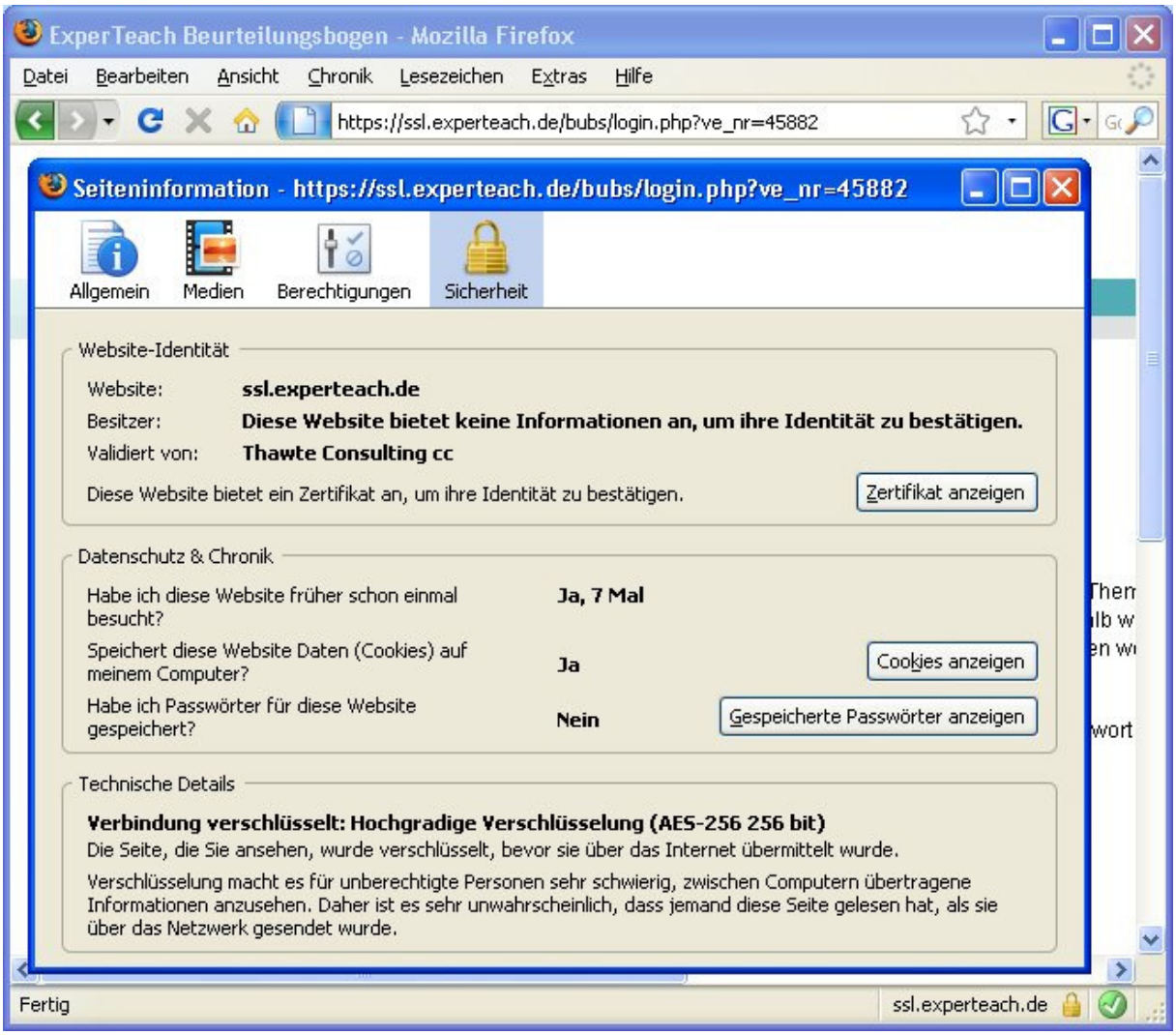

Abbildung 12: Zertifikatsinformationen beim Firefox

Zusammengefasst kann man sagen, dass SSL dem Benutzer dadurch Vertrauen gibt, dass das System, mit dem man kommunizieren möchte, authentifiziert wird. Zusätzlich wird die zur Verfügung stehende Sicherheit durch Symbole im Browser für den Benutzer sichtbar. Wie bereits im Vertrauenskapitel erläutert, benötigt der Mensch diese sichtbaren Sicherheitsmerkmale, um Vertrauen aufzubauen (vgl. [Petermann85], S. 118).

Die Authentifizierung wird aus der Sicht eines Benutzers wie folgt beschrieben:

> *Nur wenn ich sicher sein kann, dass der Absender auch wirklich der ist, für den er sich ausgibt, kann ich meine Daten mit gutem Gewissen herausgeben.*
>
> *[Friedemann01], S. 16*

Das bedeutet, dass der Benutzer erst seine Daten mit gutem Gewissen mitteilt, wenn er sich sicher ist, dass der Webserver der ist, für den er ihn hält. Diese Sicherheit bietet das SSL-Verfahren. Die anderen beiden Verfahren, die in Kapitel 2.2.2 beschrieben werden, sind daher für die Übermittlung von sensiblen Daten nicht geeignet, da die Daten von Dritten abgehört bzw. manipuliert werden können.

Ein weiterer technischer Aspekt, der bei der Erstellung eines Online-Fragebogens beachtet werden sollte, ist die Vermeidung von JavaScript und Java Applets (vgl. [Gräf99], S. 165).

„Sicherheitsbewusste Internetbenutzer haben die automatische Ausführung von Java Applets unterbunden“ [Pratzner01c], was den fehlerfreien Ablauf einer Online-Befragung verhindern könnte. Auch JavaScript lässt sich „in fast allen JavaScript-fähigen Browsern […] abschalten oder […] einzelne Aktionen, wie die Änderung des Textes in der Statusleiste oder die Manipulation von Browserfenstern“ [Wiki10j1], lassen sich deaktivieren. Aus diesem Grund sollte der Einsatz von Java Applets und JavaScript gut überlegt und wenn möglich nicht genutzt werden.

Allgemein lässt sich sagen, dass „die technischen Voraussetzungen […] sich […] am unteren Niveau der Möglichkeiten der Zielgruppe“ [Pratzner01c] des Online-Fragebogens orientieren sollten, damit jeder, der den Online-Fragebogen ausfüllen möchte bzw. soll, auch die Möglichkeit dazu hat.

Grundsätzlich ist bei den technischen Hinweisen zu bedenken, dass nicht jeder Benutzer die sichtbaren Merkmale erkennt. Diese sind oftmals erst erkennbar, wenn man auch das Wissen über sie besitzt. Daher ist es sinnvoll, wenn man nur auf Basis des Sichtbaren die Empfehlungen implementieren möchte, zu bedenken, wer die Zielgruppe des Online-Fragebogens ist.

4.3 Gestaltung der Benutzeroberfläche

Mekelburg sagt in seiner Erläuterung zum Design der Benutzeroberfläche Folgendes:

> *Die grafische Oberfläche ist heutzutage vom Computer gar nicht mehr wegzudenken. So können sich viele Heimanwender gar nicht vorstellen, mit einem Computer zu arbeiten, wenn dieser eine rein textorientierte Benutzerschnittstelle hätte. Wer heutzutage Software an den Benutzer bringen will, der muss auf das "graphical User Interface (gUI)" setzen und seine Software mit einer grafischen Oberfläche versehen. Aber auch dann kann ein schlechtes Design die gute Funktionalität einer Software so überdecken, dass eine Anwendung selbst dann nicht mit anderen Produkten konkurrieren kann, wenn es eine deutlich besser [sic!] Leistungsfähigkeit aufweist.*
>
> *[Mekelburg03]*

Diese Aussage ist nicht nur für Software gültig, sondern kann auch auf Anwendungen im Internet, d. h. zum Beispiel auf einen Online-Fragebogen, angewendet werden. Da die Benutzeroberfläche auch für den Online-Fragebogen wichtig ist, werden Empfehlungen für die Benutzeroberfläche vorgestellt. Es folgt eine Aufzählung relevanter Elemente, die ergänzt wird durch entsprechende Begründungen zu den unterschiedlichen Aussagen. Eine zusammenfassende Auflistung, die als Leitfaden gesehen werden kann, wird im Anhang geliefert.

Dieses Kapitel besteht aus fünf Unterkapiteln. Zu Beginn werden Formulierungshinweise zum Begleit- (Kap. 4.3.1) und Instruktionstext (Kap. 4.3.2) geliefert, die als Einleitung des Online-Fragebogens fungieren. Darauf folgen Gestaltungshinweise (Kap. 4.3.3), die den Vertrauensaufbau fördern und Hinweise zur Benutzerfreundlichkeit (Kap. 4.3.4). Zum Schluss dieses Kapitels werden Merkmale gezeigt, die das Sicherheitsgefühl steigern können (Kap. 4.3.5).

4.3.1 Begleittext

Der Begleittext steht am Anfang des Fragebogens und soll „die Motivation der Versuchsperson zum Ausfüllen des Fragebogens heben und den Kontext der Untersuchung transparent machen“ [Stangl09].

Bei der Formulierung des Textes muss darauf geachtet werden, dass keine Tatsachenbehauptungen „ohne entsprechenden Nachweis [...] enthalten sein sollten“ [Richter09]. Sie würden nur einen geringen Wert haben und bergen außerdem „(und zwar völlig unabhängig vom tatsächlichen Wahrheitsgehalt) das Risiko, das Vertrauen des Benutzers zu verlieren“ [Richter09]. Es ist nämlich so, dass jede Aussage Misstrauen hervorruft und eine Reihe von Prüfungsmechanismen beim Leser aktiviert werden. Die Aussage „Wir sind kompetent“ ruft beim Benutzer beispielsweise die Misstrauensfrage „Sind die wirklich kompetent?“ hervor. Daraus folgt, je einfacher der Benutzer sein Misstrauen formulieren kann, umso schneller wird die Anwendung ihre Glaubwürdigkeit verlieren (vgl. [Richter09]) und damit auch das bereits gewonnene Vertrauen.

Ein weiterer Hinweis für die Formulierung des Einleitungstextes ist, dass man umfassende Grundaussagen in mehrere unbedeutende Einzelaussagen teilt (vgl. [Richter09]). Folgendes Beispiel liefert Richter in seinem Dokument „Wie Vertrauen funktioniert“:

Umfassende Grundaussage: *„Wir haben alles, was Sie fürs Internet brauchen.“*
Unterteilung in unbedeutende Einzelaussagen: *„Wir haben einen Webcounter, wir haben schnelle Leitungen, wir haben kompetente Mitarbeiter, …“*

Diese Aussagen könnte man nun wie folgt für einen Online-Fragebogen verwenden:

Umfassende Grundaussage: *„Wir tun alles in unserer Macht stehende für die Sicherheit Ihrer Daten.“*

Unterteilung in unbedeutende Einzelaussagen: *„Wir verschlüsseln Ihre Daten mit dem SSL-Verfahren, wir geben Ihre Daten nicht an Dritte weiter, …“*

Wie schon im Kapitel 3.1 erwähnt wurde, baut sich Vertrauen durch zwischenmenschliche Kommunikation und Erfahrungsaustausch auf. Bei einem Online-Fragebogen ist der Befragte meist auf sich selbst gestellt und hat daher nicht die Möglichkeit mit dem Untersuchungsleiter[25] in persönlichen Kontakt zu treten. Um eine gewisse „soziale Präsenz“ ([Döring03], S. 233) entstehen zu lassen, hilft es, ein Foto vom Untersuchungsleiter im Begleittext zu veröffentlichen. Durch das Foto wird Vertrauen zwischen dem Benutzer und dem Untersuchungsleiter bzw. dem Online-Fragebogen erzeugt und es steigert zudem noch die Antwortbereitschaft (vgl. [Döring03], S. 233).

Eggs und Müller beschreiben, welche Hinweise man dem Benutzer geben sollte, damit sich Vertrauen bei Transaktionen bilden kann. In diesem Fall ist mit dem Begriff „Transaktion“ allerdings nicht „eine Folge von Operationen, die nur komplett oder gar nicht durchgeführt wird“ [Wiki09t2] gemeint, welche die IT-Bedeutung ist, sondern „eine gegenseitige Übertragung von Gütern und Informationen zwischen zwei Wirtschaftssubjekten“ [Wiki09t2].

Daraus folgt, dass bei einem Online-Fragebogen die Transaktion die gegenseitige Übertragung von Informationen zwischen den Wirtschaftssubjekten Befragter und Fragender ist. Somit formulieren Eggs und Müller folgende Aussagen, die als Informationen im Begleittext enthalten sein sollten, damit der Benutzer das Vertrauen in die Transaktion bekommt (vgl. [EggMüller01], S. 37). Zitiert werden im Folgenden nur die Punkte, die wichtig für einen Online-Fragebogen sind:

[25] Der Untersuchungsleiter ist die verantwortliche Person für den Online-Fragebogen (vgl. Glossar – Untersuchungsleiter).

- *[...]*
- *klare Informationen über die Identität von Online-Unternehmen, [...] sowie die Modalitäten und Bedingungen einer jeden Transaktion,*
- *[...]*
- *Schutz der Privatsphäre.*

[EggMüller01], S. 37

Neben dem Begleittext sollte es auch einen Instruktionstext geben. Welche Hinweise in diesem enthalten sein sollten, wird im folgenden Kapitel erläutert.

4.3.2 Instruktionstext

Der Instruktionstext soll „Kenntnisse für das richtige Ausfüllen des Erhebungsinstruments vermitteln“ [Stangl09]. Wie bereits mehrfach beschrieben, ist das in dieser Arbeit beobachtete Erhebungsinstrument der Online-Fragebogen. Folgende Instruktionen für die Beantwortung von Online-Fragebögen sollten im Text formuliert werden. Die Aufzählung liefert Stangl in seinen Arbeitsblättern:

- *Vollständigkeit der Antworten beachten.*
- *Aufrichtig zu antworten - Anonymität wird garantiert.*
- *Möglichst zügig zu antworten,*

  da Versuchspersonen in der Regel Fragebögen mit "Intelligenz- oder Leistungstest" verknüpfen, kann man im Instruktionstest [sic!] diesem Eindruck entgegenwirken, indem man ausdrücklich darauf hinweist,
- *dass es bei dieser Art von Untersuchung keine richtigen oder falschen Antworten gibt, dass also jede persönliche Antwort richtig sei, da es sich nicht um einen Leistungstest handelt. In bestimmten Fällen, in denen es notwendig erscheint, kann es auch günstig sein darauf hinzuweisen,*

- *dass die Untersuchung lediglich zu Forschungszwecken ausgeführt wird und nicht der Bestimmung individueller Diagnosen mit Konsequenzen für die Versuchsperson dient, sondern dass man sich nur für eine gruppenstatistische Auswertung interessiert sowie,*
- *dass ausreichender Datenschutz gewährleistet ist.*

[Stangl09]

Außerdem sollte man im Instruktionstext dem Benutzer die ungefähre Dauer zum Ausfüllen des Bogens nennen bzw. ihm während der einzelnen Fragen anzeigen, wie viel Prozent o. ä. er bereits ausgefüllt hat. Damit verhindert man z. B. den Abbruch des Online-Fragebogens. Ohne eine Fortschrittsanzeige könnte es passieren, dass bei einer der letzten Frage abgebrochen wird, weil das Interesse nicht mehr vorhanden ist. Mithilfe einer Fortschrittsanzeige kann der Benutzer besser entscheiden, ob er die noch fehlenden Fragen beantworten möchte.

Die Einleitung eines Online-Fragebogens sollte jedoch nicht zu lang sein. Es besteht die Möglichkeit, den Instruktionstext mit dem Begleittext zu verbinden, da ein zu langer Text die eben gewonnene Motivation direkt wieder verringern könnte.

Auf die beiden Teile, Begleit- und Instruktionstext, sollte man bei der Gestaltung des Online-Fragebogens ein besonderes Augenmerk haben, da „dieser Einstieg oft den Erfolg der Untersuchung“ [Stangl09] ausmacht. Durch die Hinweise auf „ausreichenden Datenschutz“ und „garantierte Anonymität“ kann auch schon ein gewisses Vertrauen aufgebaut werden.

4.3.3 Gestaltung

Ein Online-Fragebogen sollte einige der vielfältigen Möglichkeiten zur Gestaltung eines Webauftritts enthalten, damit der Fragebogen vertraut auf den Benutzer wirkt und dieser motiviert wird, den Bogen auszufüllen.

Die richtige Gestaltung des Webauftritts kann dem Benutzer auf einfache Weise die Sicherheit vermitteln, den richtigen Webauftritt erreicht zu haben. Diese Sicherheit

fördert den Aufbau des Vertrauens, welcher zusätzlich dadurch gestärkt werden kann, dass das Unternehmensdesign im Layout wiedererkennbar wird (vgl. [Richter09]).

Es ist außerdem wichtig, dass eine gewisse Einheitlichkeit des Layouts vorhanden ist, da ein übermäßiger Wechsel von vielen Schriftarten, Farben oder Zeichenattributen (z. B. kursiv, fett, unterstrichen) störend wirkt (vgl. [Mekelburg03]).

In der Ausarbeitung von Pratzner wird folgende Aussage zur Gestaltung eines Webauftritts gegeben:

> *Aus der Usability[26]-Forschung zur Benutzbarkeit von Internet-Auftritten ist bekannt, dass Nutzer wenig Verständnis für schlechtes Design aufbringen.*
>
> *[Pratzner01c]*

Diese Aussage trifft nicht nur auf allgemeine Webauftritte zu, sondern kann auch für die spezielle Anwendung Online-Fragebogen verwendet werden. Dieses Zitat sagt also aus, dass auch die Gestaltung gut durchdacht werden sollte, wenn man zum Benutzer Vertrauen aufbauen möchte.

4.3.4 Benutzerfreundlichkeit

Bei der Gestaltung des Online-Fragebogens spielt nicht nur das Layout eine wichtige Rolle, sondern auch die Benutzerfreundlichkeit, auch *Usability* genannt. Der Begriff Benutzerfreundlichkeit wird in der freien Enzyklopädie Wikipedia wie folgt definiert:

> *Benutzerfreundlichkeit [...] bezeichnet die vom Nutzer erlebte Nutzungsqualität bei der Interaktion mit einem System. Eine besonders einfache, zum Nutzer und seinen Aufgaben passende Bedienung wird dabei als benutzerfreundlich angesehen.*
>
> *[Wiki09b1]*

[26] Mit Usability ist die Benutzerfreundlichkeit gemeint, auf die im nächsten Abschnitt eingegangen wird oder vgl. Glossar – Usability.

Bei einem Online-Fragebogen sind daher zwei Benutzeraspekte von großer Bedeutung. Zum einen sollte das oben beschriebene Layout der Seite so aufgebaut werden, dass der Benutzer nicht scrollen muss. Zum anderen sollte das Wechseln „von Tastatur und Maus so selten wie möglich stattfinden“ [Pratzner01c] müssen.

Das Wort Scrollen „bedeutet Rollen auf dem Bildschirm innerhalb eines Dokuments“ [Druckbesser09]. „Um andere Inhalte des Bereichs zu sehen“ [Kirk99], muss man daher scrollen. Dies tut man, indem man die Bildlaufleiste am linken/rechten bzw. oberen/unteren Rand des Bildschirms betätigt (vgl. [Druckbesser09]).

Die Aussage bzgl. des Scrollens, bedeutet, dass eine Seite des Fragebogens nicht zu lang sein sollte und man stattdessen versuchen sollte, den Online-Fragebogen in mehrere Seiten aufzuteilen (vgl. [Pratzner01b]). Hierbei ist jedoch zu beachten, dass der Online-Fragebogen in seinem Gesamtumfang nicht zu groß wird, da beim Benutzer ein Ermüdungseffekt eintritt (vgl. [Stangl09]) und die Chance sinkt, dass er den Online-Fragebogen komplett zu Ende ausfüllt.

Der zweite Aspekt – das Wechseln von Tastatur und Maus – wurde von Gräf in „Optimierung von WWW-Umfragen[27] – Das Online Pretest-Studio“ dokumentiert. Gräf schrieb, dass Befragte es lästig finden, wenn sie „die Maus von links nach rechts bewegen“ ([Gräf99], S. 162) müssen, um ihre Meinung auszudrücken. In seinen Fragebogentests „gaben die Ausfüller häufig an, dass sie entlang einer Spalte geantwortet haben“ ([Gräf99], S. 162). Aus dieser Aussage kann man den Schluss ziehen, dass auf diese Weise ggf. nicht ganz ehrliche Meinungen abgegeben werden, und somit das Ergebnis des Fragebogens verfälscht wird. Für das Erstellen des Fragebogens bedeutet dies, dass man Matrixfragen[28] vermeiden sollte, da sie den Benutzer dazu verleiten, Antworten nach einem „Muster“ zu wählen. Und somit nicht ihre ehrliche Antwort geben, da dies bedeutet, dass der Benutzer die Maus zusätzlich weiter bewegen muss.

[27] WWW-Umfragen sind Befragungen, die im World Wide Web durchgeführt werden (vgl. Glossar – WWW-Umfragen).
[28] Erläuterung und weitere Hinweise zu Matrixfragen werden in Kap. 4.4.2 geliefert.

Neben den bereits genannten Merkmalen für die Benutzerfreundlichkeit nennt Mekelburg auf seiner Webseite noch weitere Kriterien, die „zur Beurteilung der Benutzbarkeit von Softwareprodukten“ [Mekelburg03] beachtet werden sollten. Wie bereits erwähnt, können einige Hinweise zu Softwareprodukten auch auf einen Online-Fragebogen angewendet werden. Die hierfür sinnvollen Hilfestellungen werden nachfolgend dargestellt:

- *Das Dialogverhalten innerhalb der Anwendung muss einheitlich und konsistent sein.*
- *Der Benutzer muss jederzeit auswählen können, ob er einen Dialogschritt durchführen, abbrechen oder zurücknehmen will.*
- *Ungültige Eingaben sind so früh wie möglich, also beireits [sic!] von der Oberfläche, zu verhindern.*

[Mekelburg03]

Der dritte Punkt dieser Aufzählung lässt sich jedoch nur mit JavaScript realisieren. An diesem Punkt muss der Fragebogenersteller entscheiden, was wichtiger ist. Ist gewollt, dass jeder Benutzer ohne Einschränkungen den Online-Fragebogen nutzen kann, dann muss der dritte Punkt ignoriert werden. Soll der dritte Punkt jedoch unbedingt implementiert werden, dann muss JavaScript genutzt werden.

Zu Bedenken bei dieser Entscheidung ist allerdings, dass im Kapitel 2.2.2 „Technologien zur sicheren Datenübertragung“ die Empfehlung ausgesprochen wurde, JavaScript wegen der Einschränkungsmöglichkeiten im Webbrowser nicht zu nutzen.

Die in diesem Abschnitt erläuterten Hinweise sollten bei der Gestaltung des Online-Fragebogens in Bezug auf die Benutzerfreundlichkeit bedacht werden, damit der Benutzer nicht durch eine schlechte Navigation die Lust und Motivation am Online-Fragebogen verliert. Denn durch den Verlust von Motivation verliert der Benutzer auch ein gewisses Vertrauen in das System.

4.3.5 Sicherheitsmerkmale

Wie bereits im Kapitel 4.2 „Empfehlungen für die IT“ beschrieben, sollte eine SSL-Verbindung für die Übermittlung der Daten genutzt werden. Die bekanntesten Firmen, die digitale Schlüssel zertifizieren, sind VeriSign und thawte (vgl. [Friedemann01], S. 16).

Es ist auf einfachem Wege möglich, wenn man digitale Schlüssel von einem dieser beiden Unternehmen nutzt, die Sicherheit auf der Benutzeroberfläche darzustellen.

Abbildung 13: Sicherheitsgrafik von thawte[29]

Man kann auf dem Webauftritt, also auch beim Online-Fragebogen, eine Grafik einbinden, über die man weitere Informationen zum Zertifikat erhält (siehe Abbildung 13 und Abbildung 14). So eine Grafik wird Secured Logo genannt und sagt dem Benutzer, dass der Webseitenersteller sich mit dem Thema Sicherheit beschäftigt haben muss, da eine Grafik in den Webauftritt eingepflegt wurde.

Abbildung 14: Sicherheitsgrafik von VeriSign[30]

Ein zusätzlicher Vorteil der Grafik ist, dass sie auf jeder beliebigen Webseite des Webauftritts eingebunden werden kann. D. h. es muss nicht das SSL-Protokoll gestartet werden, damit die Grafik sichtbar wird. Alle anderen bereits vorgestellten Merkmale des SSL-Protokolls (siehe Kapitel 4.2 „Empfehlungen für die IT") sind erst erkennbar, wenn das SSL-Protokoll aktiv ist.

[29] Quelle: http://www.thawte.com/.
[30] Quelle: http://www.verisign.com/ssl/secured-seal/index.html?sl=a_box.

Abbildung 15: RosyTec.de – Secured Logo von VeriSign auf der Startseite

In der Abbildung 15 sieht man in der Navigationsleiste (Pfeil 1) kein *https* bzw. es ist auch nirgends auf der Seite ein Schloss zu finden, dass auf eine bestehende SSL-Verbindung hinweist. Sodass man auf den ersten Blick keine Informationen über die Sicherheit finden würde, wenn nicht der gesonderte Hinweis (Pfeil 2) abgebildet wäre.

Die über dem Secured Logo liegende Grafik ist eine Art Gütesiegel für Online-Shops und sagt aus, dass der Online-Shop sehr hohe Sicherheitsstandards besitzt und zertifiziert wurde (vgl. [Hafenbradl07]). Dieses Siegel ist allerdings für einen Online-Fragebogen irrelevant und wird nur vollständigkeitshalber erklärt.

Wenn man auf das Secured Logo in Abbildung 15 (Pfeil 2) klickt, öffnet sich ein zusätzliches Fenster. In diesem werden weitere Informationen zum Zertifikat geliefert. Diese Daten werden verschlüsselt übermittelt, was durch die Sicherheitsmerkmale gekennzeichnet wird.

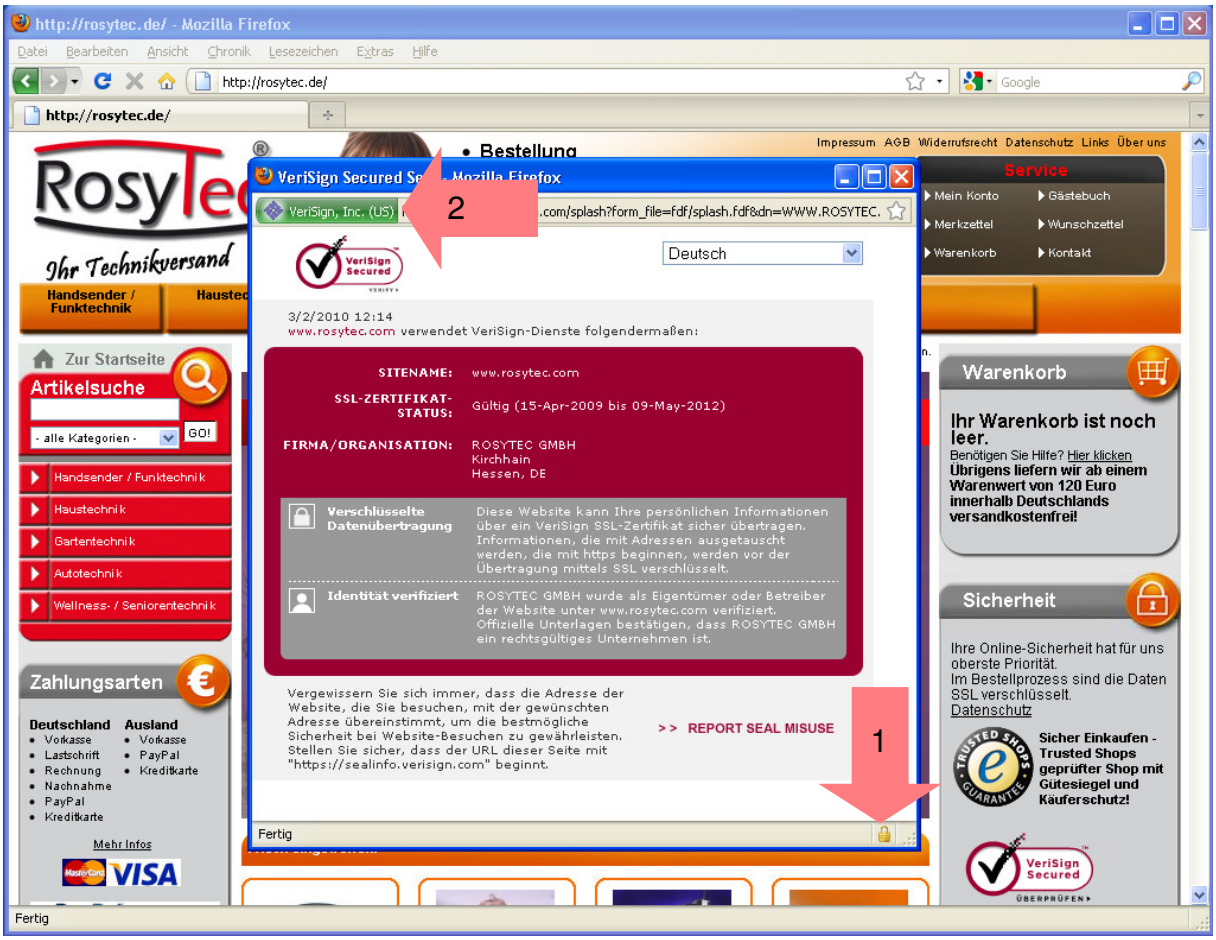

Abbildung 16: RosyTec.de – Darstellung der Zertifikatsinformationen

Die Abbildung 16 stellt die Zertifikatsinformation in einem Fenster mit den Sicherheitsmerkmalen dar. Am unteren Rand des kleinen Fensters ist das Schloss zu finden (Pfeil 1) und auch die Navigationsleiste ist grün eingefärbt (Pfeil 2), was auf die SSL-Verschlüsselung hinweist.

Durch so ein Secured Logo kann der Benutzer direkt über die Startseite des Online-Fragebogens bzw. der Webseite das von ihm geforderte Sicherheitsmerkmal finden, damit er Vertrauen aufbauen kann. Wie im Kapitel 3.3 beschrieben, benötigt der Benutzer Sicherheitsmerkmale, die er erkennen kann, um Vertrauen aufzubauen. Mithilfe der oben dargestellten Symbole gibt der Online-Fragebogenersteller dem Benutzer

schon auf nicht verschlüsselten Seiten einen Hinweis auf seine Bemühungen zur Sicherheit und baut damit Vertrauen auf.

Neben dem Secured Logo, das auf freiwilliger Basis vom Webseitenbetreiber eingebunden werden kann, hat ein Webseitenbetreiber die Pflicht, eine Datenschutzerklärung abzugeben.

Abbildung 17: RosyTec.de – Link zur Datenschutzerklärung

Die Webseite des Online-Shops RosyTec ist ein ideales Beispiel in Bezug auf die Sicherheitsmerkmale. Es besitzt nicht nur das Secured Logo von VeriSign auf der Startseite, sondern es beinhaltet auch einen direkten Link zur Datenschutzerklärung. Dieser befindet sich im „Sicherheits“-Bereich der Startseite ebenso wie das Secured Logo. Bei Klick auf „Datenschutz“ (Pfeil 1 in Abbildung 17) gelangt der Benutzer zur Datenschutzerklärung des Webseitenbetreibers.

Die Datenschutzerklärung des Online-Shops ist an das Design der Webseite angepasst (siehe Abbildung 18) und bestärkt die Aussage, dass der Webseitenbetreiber sich bemüht, seine Seriosität und die Bemühungen zum Schutz der sensiblen Daten dem Benutzer zu zeigen.

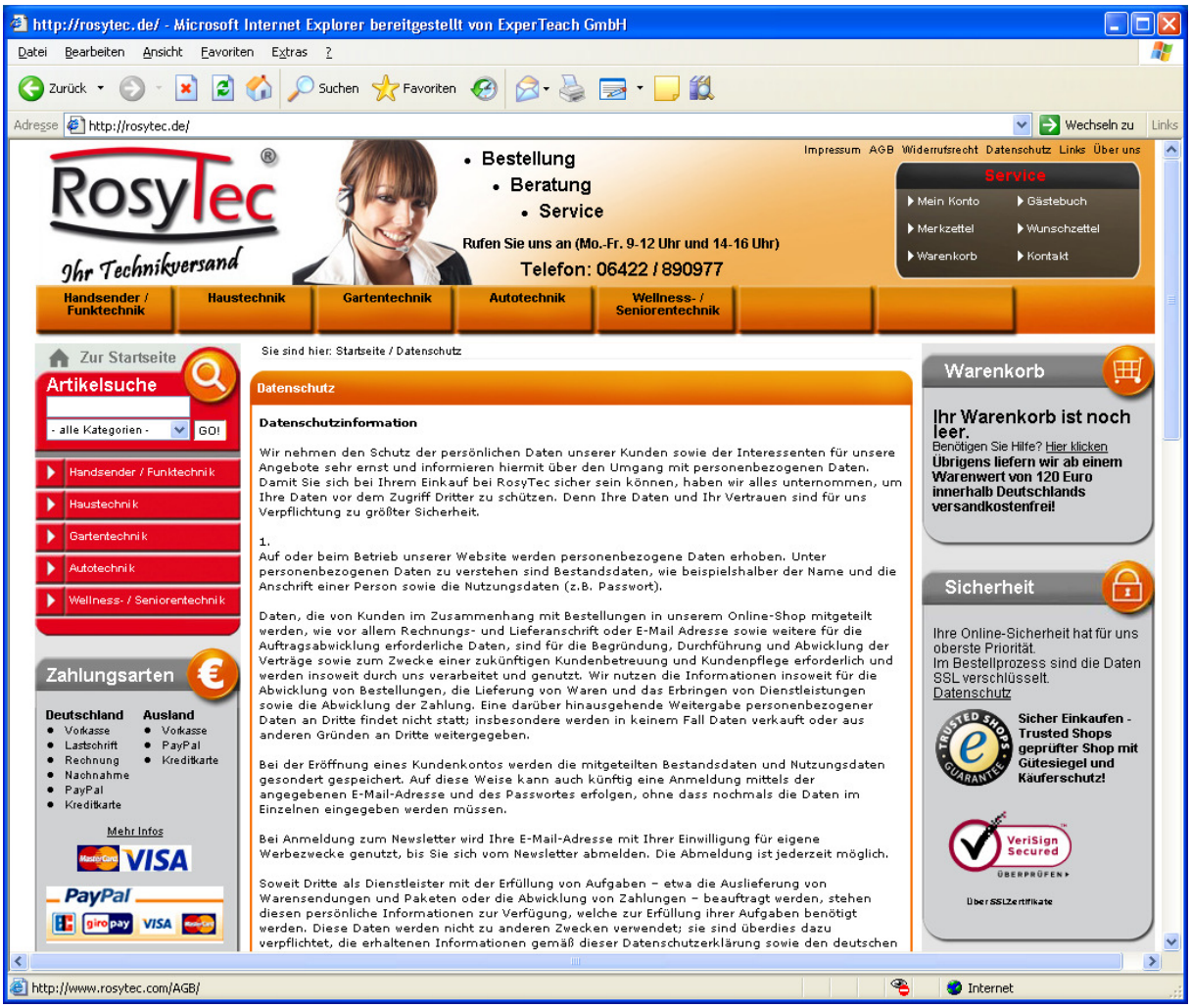

Abbildung 18: RosyTec.de – Datenschutzerklärung

Wie bereits im Kapitel 2.2.4 genauer erläutert, liefert diese Erklärung dem Benutzer Informationen darüber, wie Datenschutz betrieben wird. Außerdem sichert diese Erklärung den Benutzer rechtlich ab, sodass es wichtig ist, sie dem Benutzer nicht vorzuenthalten. Durch den konkreten Hinweis auf die Datenschutzerklärung sieht der Benutzer, dass es dem Webseitenbetreiber wichtig ist, ihm alle wichtigen Informationen zu liefern. Der Benutzer baut Vertrauen auf, da ihm durch diese Methode ein weiteres Mal gezeigt wird, dass dem Webseitenbetreiber die Sicherheit der Daten wichtig ist.

4.4 Hinweise zur Fragenkonstruktion

Der folgende Abschnitt beinhaltet einige wichtige Hinweise, was man bei der Formulierung der Fragen für den Online-Fragebogen beachten sollte, um schlussendlich sicher sein zu können, dass die Qualität der Antworten zufriedenstellend ist. Denn nur gute und ehrliche Antworten erfüllen den Zweck eines Fragebogens.

Im ersten Unterkapitel wird erläutert, was bei Einleitungsfragen beachtet werden sollte (Kap. 4.4.1), während im zweiten Kapitel erklärt wird, was Matrixfragen sind und inwieweit man sie in einem Online-Fragebogen nutzen bzw. nicht nutzen sollte (Kap. 4.4.2). Am Ende dieses Kapitels folgen allgemeine Hinweise zur Konstruktion von Fragebögen (Kap. 4.4.3).

Die in diesem Kapitel diskutierten Aspekte zielen auf die Qualität des Online-Fragebogens ab. Doch es ist bekannt, dass Qualität auch das Vertrauen steigen lässt. Mithilfe von Empfehlungsdiensten[31], in denen die gute Qualität des Online-Fragebogens gelobt werden könnte, kann dem Online-Fragebogen bereits zu Beginn Vertrauen entgegengebracht werden.

4.4.1 Einleitungsfrage

Unter der Einleitungsfrage versteht man die erste Frage, die in einem Fragebogen gestellt wird. Wichtig hierbei ist, dass diese Frage direkt das Problem anspricht, welches den Befragten interessiert (vgl. [Stangl09]), dabei jedoch möglichst neutral formuliert ist. Damit ist gemeint, dass „keine Zustimmung oder Ablehnung eines Sachverhalts“ ([Bekalarczyk09], S. 9) durch den Befragten erfordert wird und es „ausgewogene Antwortalternativen“ [Stangl09] gibt.

Ein weiterer Aspekt ist der Schwierigkeitsgrad der Frage. Sie sollte leicht zu beantworten sein, um den Befragten von der Vorstellung einer Prüfungssituation zu entlasten (vgl. [Stangl09]). Eine Prüfungssituation empfinden die meisten Menschen als etwas Negatives, was zur Folge haben könnte, dass der Befragte das vorher gewonnene Vertrauen schnell verliert und den Online-Fragebogen nicht weiter ausfüllt.

[31] Empfehlungsdienste generieren Empfehlungen über Güter und Dienstleistungen (vgl. Glossar – Empfehlungsdienst).

Wenn die genannten Punkte beachtet werden, kann „möglichst bald ein Vertrauensklima zwischen Befragten und Interviewer entstehen“ [Stangl09]. Es ist bekannt, dass der Erfolg einer Umfrage von der „Tauglichkeit der Einleitungsfrage abhängt“ [Stangl09].

4.4.2 Matrixfragen

In Kapitel 4.3.4 wird darauf hingewiesen, dass der Fragebogenersteller keine Matrixfragen nutzen sollte, da sonst die Möglichkeit besteht, ein falsches Ergebnis zu erhalten[32].

Als Matrixfragen versteht man mehrere Fragen, denen dieselben Antwortkategorien zugeordnet sind. Mithilfe einer Tabelle lassen sich diese Fragen auf einfache Weise darstellen. In der linken Spalte der Tabelle befindet sich im Normalfall die Frage, wobei die restlichen Spalten bis zum rechten Bildschirmrand die Antwortkategorien füllen (vgl. [Gräf99], S. 161). Die unten dargestellte Abbildung zeigt solche Matrixfragen.

Abbildung 19: Beispiel für Matrixfragen[33]

[32] Vgl. Kap. 4.3.4 „Benutzerfreundlichkeit“ ab S.54.
[33] Grafik entnommen von http://www.e-teaching.org/didaktik/qualitaet/online_umfrage/matrixfrage.

Diese Darstellung wird meistens in schriftlichen Fragebögen eingesetzt, ist jedoch, nach einer Studie von Gräf, für das Medium Internet ungeeignet (vgl. [Gräf99], S. 161). Begründet wird dies dadurch, dass sie die Gefahr in sich birgt, dass der Befragte nach einem Muster antwortet.

Ein Lösungsansatz für dieses Problem wird ebenfalls von Gräf geliefert. Jede Frage sollte „für sich mit den Antworten präsentiert“ ([Gräf99], S. 163) werden. Damit jedoch nicht jede einzelne Frage einzeln übertragen werden muss, sollte man die Fragen mit ihren Antworten untereinander darstellen (siehe Abbildung 20).

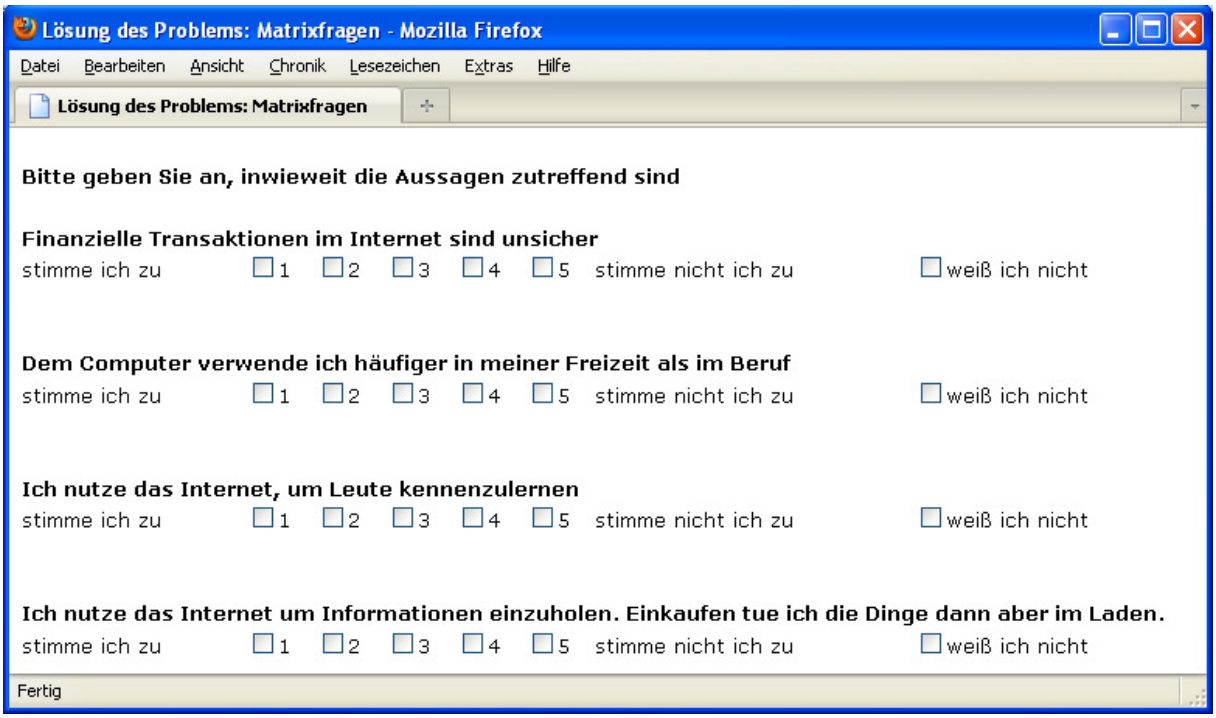

Abbildung 20: Lösung des Problems: Matrixfrage[34]

Stangl verweist auf die Problemstellung einer mittleren Antwortposition. Der Fragebogenersteller sollte sich überlegen, ob er eine solche zur Verfügung stellen will (vgl. [Stangl09]). Wie beide Grafiken in diesem Kapitel zeigen (siehe Abbildung 19 und Abbildung 20), gibt es zu einer Frage immer fünf Antwortmöglichkeiten, d. h. immer eine mittlere Antwortposition (in Abbildung 20 mit „3“ gekennzeichnet). Zusätzlich gibt es in Abbildung 20 noch die Möglichkeit, ein Kreuz bei „weiß ich nicht“ zusetzen.

[34] Nach Abbildung 5 in [Gräf99], S. 164.

Diese beiden Antwortkategorien, gelten als „mittlere Antwortkategorie“ und bergen die Gefahr, dass sich der Befragte nicht konkret entscheiden muss.

Eine mittlere Antwortkategorie kann nach Stangl für „einzelne Versuchspersonen ganz Unterschiedliches aussagen“ [Stangl09]. Welche Bedeutungen beispielsweise bei der Fragestellung „Halten Sie sich für einen geselligen Menschen?“ das sein könnten, soll nun dargestellt werden:

- *eine mittlere Antwortposition (z. B. jemand hält sich für einen in mittlerem Maße geselligen Menschen).*
- *eine "Weiß nicht"-Antwort (z. B. jemand kommt zu keinem endgültigen Urteil darüber, ob er nun gesellig ist oder nicht).*
- *eine "Irrelevanz"-Antwort (z. B. jemand hält die Frage für nicht besonders wichtig usw.).*
- *eine "Protest"-Antwort (z. B. jemand hat etwas gegen die Frage einzuwenden und drückt seine Unmut oder Widerstand gegen die Frage durch das Ankreuzen der mittleren Kategorie aus).*

[Stangl09]

In Abbildung 20 treffen nicht alle vier Aussagen auf die mittlere Position der Skala zu, da es die „weiß ich nicht“-Möglichkeit als Ankreuzfeld gibt. Wäre dies nicht der Fall, würden alle vier Aussagen auf die mittlere Auswahlmöglichkeit zutreffen und eine genaue Auswertung wäre nicht möglich.

4.4.3 Allgemeine Hinweise zur Fragenkonstruktion

Bei der Fragenformulierung muss man sich im Klaren darüber sein, für welches Medium der Fragebogen erstellt werden soll. Es ist bekannt, dass Texte im Internet anders gelesen werden, als gedruckte Materialien (vgl. [Gräf99], S. 160). Texte in Onlinemedien werden „nicht gelesen, sondern eher „gescannt““ ([Gräf99], S. 160). Es werden beim „Überfliegen“ des Textes einige wenige Satzfragmente wahrgenommen, welche dann vom Leser zu einem Sinnzusammenhang ergänzt werden. Der Leser baut diesen Zusammenhang dann anhand seines Vorwissens und seiner

Vorerfahrungen zusammen (vgl. [Gräf99], S. 160). Gräf weist in seinem Text auf Ergebnisse zur Benutzerfreundlichkeit von Nielsen hin, welche besagen, dass „Nutzer über Textbausteine hinwegsehen, die sie nicht für wichtig erachten und statt dessen auf hervorgehobene Textpassagen achten“ ([Gräf99], S. 160f). Nielsen empfiehlt, dass ein guter WWW-Autor 50% weniger schreiben sollte als ein Autor für Papiermedien. Diese Aussage stützt sich darauf, dass „die Lesegeschwindigkeit von Bildschirmtexten im Vergleich zu Papiertexten um 25% geringer“ ([Gräf99], S. 161) sei.

Weiter empfiehlt Gräf, dass man sich, bevor man mit der Formulierung von Fragen beginnt, erst einmal mit den Standards der empirischen Sozialforschung beschäftigen sollte. Zusammenfassend lassen sich folgende Aussagen für alle Fragen im Fragebogen formulieren (vgl. [Gräf99], S. 166):

- Die Fragen sollten von allen Befragten in gleicher Weise verstanden werden.
- Die Fragen sollten kurz und prägnant formuliert werden.
- Die Fragenformulierung darf den Befragten nicht überfordern.
- Konzepte, die dem Befragten nicht bekannt sind, sollten nicht abgefragt werden.
- Bei geschlossenen[35] Fragen müssen die Antwortkategorien vollständig sein und dürfen sich nicht überschneiden.
- Werden Fremdwörter o. ä. verwendet, sollte man zur Beantwortung der Fragen verständliche Hinweise geben.

Weitere Hinweise zur Formulierung der Fragen liefert Stangl. In dieser Auflistung werden jedoch nur noch die Punkte genannt, die nicht bereits in der Zusammenfassung nach Gräf zu finden sind (vgl. [Stangl09]):

- Die Fragen sollten nicht zu allgemein formuliert werden. Sie sollten spezifisch und konkret formuliert werden, jedoch für jeden verständlich.
- Die Fragen sollten umgangssprachlich formuliert werden. Verständlichkeit ist wichtiger als die grammatikalische Richtigkeit.
- Wenn in Fragen nach Häufigkeit, Dauer oder Größe gefragt wird, muss die Einheit angegeben werden, in der die Antwort erfolgen soll.

[35] Geschlossene Fragen sind Fragen, die vorgegebene Antwortmöglichkeiten haben (vgl. Glossar – geschlossene Fragen).

- Die Fragen sollten durchnummeriert werden und es sollte ggf. Sprungmöglichkeiten geben.

5 Abschlussbemerkungen

Der vorliegende Abschnitt teilt sich in drei Kapitel auf und beendet die Abschlussarbeit. Zu Beginn wird das Resümee (Kap. 5.1) formuliert. Darauf folgt das Kapitel „Ausblick und Forschungsdesiderata“ (Kap. 5.2), indem Vorschläge für weitere Forschungsprojekte verfasst werden. Am Ende der Arbeit befindet sich ein persönliches Fazit (Kap. 5.3).

5.1 Resümee

Der Online-Fragebogen ist wohl das schnellste und einfachste Mittel, um Daten im Internet zu sammeln. Auf einfache Weise kann ein Online-Fragebogen erstellt werden. Vor allem dadurch, dass es im Internet sogar Betreiber gibt, die die Online-Fragebogenerstellung und die Auswertung kostenfrei (z. B. http://ofb.msd-media.de/) oder kostenpflichtig (z. B. http://www.onlineumfragen.com) anbieten.

Es sollte jedoch keinesfalls der Zweck eines Fragebogens vergessen werden. Der Sinn eines Fragebogens wird nur erfüllt, wenn die Antworten ehrlich sind und damit die echten Meinungen der Befragten widerspiegeln, d. h. auch sensible Daten werden preisgegeben. Es ist dabei unwichtig, ob es sich um Papier- oder elektronische Fragebögen handelt. Als Grundgedanke lässt sich formulieren, dass man nur echte Antworten erhalten kann, wenn der Befragte dem Fragenden traut. Das bedeutet, dass die befragte Person Vertrauen in den Online-Fragebogen bzw. in die Institution hinter dem Online-Fragebogen haben muss.

Durch die Möglichkeit, einfach und schnell einen Online-Fragebogen zu erstellen, wird oft vergessen, dass verschiedene Hinweise dabei zu beachten sind. Neben der richtigen Formulierung der Fragen, die hier nur marginale Bedeutung hat, stellt sich die Frage, wie ein richtiger Online-Fragebogen aussehen muss. Denn das Erscheinungsbild des Online-Fragebogens kann viel über den Fragenden aussagen und ist daher wichtig für den Vertrauensaufbau.

Aus diesem Grund werden in dieser Ausarbeitung Empfehlungen für die richtige Darstellung eines Online-Fragebogens abgegeben. Neben den Ratschlägen zum Layout

werden weitere zur sicheren Datenübertragung geliefert. All die genannten Hinweise sollen als Vorschlag für einen Online-Fragebogen gesehen werden und wurden im Leitfaden zusammengefasst.

5.2 Ausblick und Forschungsdesiderata

In der Zukunft wird die Online-Befragung wohl noch häufiger genutzt werden, da die Zahl der Internetnutzer jährlich steigt (vgl. [ARDZDF09]). Das könnte in Zukunft den Vorteil bringen, dass die Menschen sich stärker mit der Thematik Internet beschäftigen, was dazu führt, dass die Sicherheitsmerkmale, die für die Vertrauensbildung wichtig sind, besser von jedem Nutzer erkannt werden und die Menschen dem Internet bzw. Online-Fragebogen schneller vertrauen.

Aktuell besteht das Problem, dass vielen Personen die Sicherheitsmerkmale nicht bekannt sind und sie somit aus Unwissen solch einem Online-Fragebogen nicht vertrauen würden. Das bedeutet, dass sie die Sicherheitsmerkmale nicht erkennen und somit auch nicht deuten können. Daraus lässt sich der Schluss ziehen, dass man mithilfe anderer Medien versuchen muss, den Personen die Sicherheitsmerkmale nahe zu bringen. Dafür könnten die Medien Radio und Fernsehen genutzt werden, indem sie z. B. in Reportagen erklären, wie man im Internet sichere Webseiten erkennt. Denn nur wenn die Menschen wissen, woran sie sichere Systeme erkennen, können sie die Sicherheitsmerkmale verstehen.

In einem fortführenden Projekt könnte man den Leitfaden testen, indem man die vorgestellten Hinweise auf einen Online-Fragebogen anwendet und im Online-Fragebogen selber erfragt, inwieweit der Benutzer Vertrauen zum Online-Fragebogen aufbauen konnte bzw. aufgebaut hat. Am Ende könnte man eine Auswertung aus den Ergebnissen entwickeln und den Leitfaden bzw. die Checkliste anpassen.

Im Laufe des Projektes entstand die Frage, inwieweit eine Log-in-Abfrage vor dem Online-Fragebogen den Benutzer daran hindert diesem Vertrauen entgegen zu bringen. Diese Frage konnte nach Sichtung der Fachliteratur nicht zufrieden stellend geklärt werden. Daraus lässt sich für nachfolgende Untersuchungen die Frage formulieren, ob ein Log-in den Benutzer davon abhielte, seine Daten einzugeben und inwieweit es dann überhaupt möglich ist, Vertrauen aufzubauen. Eine Log-in-Abfrage bedeutet nämlich, dass vor Beginn des Fragebogens der Benutzer die Log-in-Daten erhalten muss. Dieser Aspekt ist ein wichtiger Betrachtungspunkt und nimmt eine

zentrale Position in Bezug auf die Anonymität ein, die bei Online-Fragebogen von großer Wichtigkeit ist.

5.3 Fazit

Meines Erachtens haben die beschriebenen Empfehlungen sehr großen Einfluss auf den Vertrauensaufbau und man könnte durch deren Beachtung den Abbruch von Online-Fragebögen verringern bzw. die Befragten-Rate erhöhen. Solch eine Befragung, die diese Aussage belegen würde, konnte im Rahmen der relativ kurzen Bachelorphase nicht durchgeführt werden.

Doch wie bereits in Kapitel 4.3.4 „Benutzerfreundlichkeit“ beschrieben kann es passieren, dass man eine Empfehlung nur berücksichtigen kann, wenn man eine andere nicht beachtet. Aus diesem Grund muss man bei der Betrachtung des Leitfadens darauf achten, dass man nur die Empfehlungen umsetzt, die der Zielgruppe gerecht werden und die dem Online-Fragebogen auch einen Nutzen bringen.

Als wichtigste Aufgabe bei der Erstellung eines Online-Fragebogens sehe ich neben dem Sicherheitsmerkmal durch SSL, die optischen Gestaltungsaspekte an. Wenn der Benutzer bereits begonnen hat, den Fragebogen auszufüllen, wird er diesen mit einer hohen Wahrscheinlichkeit auch zu Ende beantworten. Denn durch eine optimale Gestaltung des Online-Fragebogens kann der Fragende ein hohes Maß an Vertrauen aufbauen.

Durch die richtige Gestaltung eines Online-Fragebogens bekommt der Benutzer auch den Eindruck einer seriösen Umfrage, was grade für die Vertrauensbildung sehr wichtig ist.

Literaturverzeichnis

Bücher und Berichte

[Döring03] Nicola Döring: Sozialpsychologie im Internet (Göttingen, 2003).

[EggMüller01] Holger Eggs, Günter Müller: Sicherheit und Vertrauen: Mehrwert im E-Commerce in: Sicherheitskonzepte für das Internet von Günter Müller, Martin Reichenbach (Hrsg.): (Berlin, 2001).

[Fladnitzer06] Marliese Fladnitzer: Vertrauen als Erfolgsfaktor virtueller Unternehmen (Wiesbaden, 2006).

[Friedemann01] Friedemann Mattern, Marc Langheinrich: Allgegenwärtigkeit des Computers - Datenschutz in einer Welt intelligenter Alltagsdinge in: Sicherheitskonzepte für das Internet von Günter Müller, Martin Reichenbach (Hrsg.): (Berlin, 2001).

[Gräf99] Lorenz Gräf: Optimierung von WWW-Umfragen: Das Online-Pretest-Studio in: Online-Research: Methoden, Anwendungen und Ergebnisse von Bernad Batinic, Lorenz Gräf, et al.: (Göttingen, 1999).

[Greschuchna06] Larissa Greschuchna: Vertrauen in der Unternehmensberatung - Einflussfaktoren und Konsequenzen (Wiesbaden, 2006).

[Grimm01] Rüdiger Grimm: Vertrauen im Internet: Wie sicher soll E-Commerce sein? in: Sicherheitskonzepte für das Internet von Günter Müller, Martin Reichenbach (Hrsg.): (Berlin, 2001).

[Kluck09] Anja Dagmar Kluck: Die Auswirkungen von E-Mail-Kommunikation auf Vertrauen in Unternehmen (Lüneburg, 2009).

[Petermann85] Franz Petermann: Psychologie des Vertrauens (Salzburg, 1985).

[Ulrich08] Dietzer Ulrich, Rainer M. Bösel: Einführung in die Psychologie (Stuttgart, 2008).

[Wenzel01] Harald Wenzel: Kommunikation und Vertrauen in der Ethnomethologie in: Die Abenteuer der Kommunikation von Harald Wenzel: (Weilerswist, 2001).

Onlinequellen

[Albers04] S. Albers, M. Huber, B. Müller, B. Reuschenbach: Fragebogenkonstruktion (2004)
[http://www.pflegeforschung.net/fragebogenkonstruktion.pdf]
(Zugriff am: 12. 01. 2010).

[Apple09] Apple Inc.: Mail 2.0 Help: Signieren und Verschlüsseln von E-Mails (2009)
[http://docs.info.apple.com/article.html?path=Mail/2.0/de/ml1089.html]
(Zugriff am: 12. 01. 2010).

[ARDZDF09] Projektgruppe ARD/ZDF-Multimedia: Home (2009)
[http://www.ard-zdf-onlinestudie.de/]
(Zugriff am: 11. 01. 2010).

[Bekalarczyk09] Dawid Bekalarczyk: Datenerhebungstechniken – Die Befragung (2009)
[http://www.uni-due.de/imperia/md/content/soziologie/6a_erhebung_befragung2.pdf]
(Zugriff am: 06. 01. 2009).

[Bless08] Claudia Bless: Maturaarbeit Claudia Bless (2008)
[http://www.sportwoche.ch/downloads/08MaturaarbeitClaudiaBless.pdf]
(Zugriff am: 25. 01. 2010).

[Druckbesser09] Druckbesser: Bedeutung Scrollen und Begriffserklärung (2009)
[http://www.druckbesser.de/index.php?pg=lexikon-drucksachen&me1=0&me2=16&lid=1133&PHPSESSID=76ad73b237f1a29051ffba389407e37e]
(Zugriff am: 17. 12. 2009).

[educa09] educa.ch - Schweizer Medieninstitut für Bildung und Kultur: educa.ch - Was ist Sicherheit (2009)
[http://www.educa.ch/DYN/109231.asp]
(Zugriff am: 01. 12. 2009).

[Friepoertner09] Ingo Friepoertner: Startseite: Online Fragebogen (2009)
[http://www.online-fragebogen.com/]
(Zugriff am: 27. 11. 2009).

[Groß09] Barbara Groß: Sicherheit im Internet (2009)
[http://www.vetion.de/tipinfo/pdf/webweiser/Sicherheit_2.pdf]
(Zugriff am: 27. 11. 2009).

[Hafenbradl07] Ulrich Hafenbradl: Was ist Trusted Shops? (2007)
[http://www.trustedshops.de/info/trusted-shops/]
(Zugriff am: 03. 02. 2010).

[ITWissen09] IT Wissen: IT Wissen (2009)
[http://www.itwissen.info/definition/lexikon/Benutzeroberflaeche-UI-user-interface.html]
(Zugriff am: 07. 12. 2009).

[Karadeniz09] Besim Karadeniz: netplanet - Sicherheit im Internet - Konzepte für ein sicheres Netzwerk (1998-2009)
[http://www.netplanet.org/sicherheit/sicherheit.shtml]
(Zugriff am: 01. 12. 2009).

[Kassebaum04] Ulf Bernd Kassebaum: Interpersonelles Vertrauen - Entwicklung eines Inventars zur Erfassung spezifischer Aspekte des Konstrukts (2004)
[http://deposit.ddb.de/cgi-bin/dokserv?idn=971588015&dok_var=d1&dok_ext=pdf&filename=971588015.pdf]
(Zugriff am: 04. 01. 2010).

[Kirk99] Alexander Kirk: Scrollen (1999)
[http://www.computerlexikon.com/was-ist-scrollen]
(Zugriff am: 12. 01. 2010).

[Linke10] C. Linke: Surfen Sie noch ohne JavaScript? (2010)
[http://artikel.4.am/archives/20568-Surfen-Sie-noch-ohne-JavaScript.html]
(Zugriff am: 25. 01. 2010).

[Mekelburg03] Hans-G. Mekelburg: Usability: Graphical User Interface (2003)
[http://www.nwn.de/hgm/ergo/kap-gui.htm]
(Zugriff am: 07. 12. 2009).

[Ostwald00] Ingo Ostwald: Ethnomethologie | Die Soziologie des Alltäglichen (2000)
[http://www.ingos-welt.de/go/artikel/text/ethnomethodologie_kurz.pdf]
(Zugriff am: 04. 02. 2010).

[Pratzner01a] Axel Pratzner: 3.3 Aufbau des Fragebogens (2001)
[http://fragebogen.de/aufbau-des-fragebogens.htm]
(Zugriff am: 06. 01. 2010).

[Pratzner01b] Axel Pratzner: 4.6 Die fünf häufigsten Fehler bei webbasierten Umfragen (2001)
[http://www.fragebogen.de/fuenf-haeufigsten-fehler-bei-webbasierten-umfragen.htm]
(Zugriff am: 17. 12. 2009).

[Pratzner01c] Axel Pratzner: 4.7 Empfehlung für webbasierte Umfragen (2001)
[http://fragebogen.de/empfehlungen-fuer-webbasierte-umfragen.htm]
(Zugriff am: 27. 11. 2009).

[Reibold01] Holger Reibold: Hypertext Transfer Protocol - HTTP Grundlagen (2001)
[http://www.tecchannel.de/netzwerk/management/401210/hypertext_transfer_protocol/index6.html]
(Zugriff am: 18. 01. 2010).

[Richter09] Martin Richter: Wie Vertrauen funktioniert (1998)
[http://www.factsoft.de/aktuelles3.phtml]
(Zugriff am: 23. 11. 2009).

[Rohner04] Martin Rohner: Online-Trust (2004)
[http://www.psycho.unibas.ch/mmi/downloads/Rohner2004.pdf]
(Zugriff am: 23. 11. 2009).

[Rojahn07] Matthias Rojahn: Security Server Deutschland (2007)
[http://www.ssl.de/]
(Zugriff am: 04. 12. 2009).

[Stangl09] Werner Stangl: [werner.stangl]s arbeitsblätter (2009)
[http://arbeitsblaetter.stangl-taller.at/FORSCHUNGSMETHODEN/Fragebogen.shtml]
(Zugriff am: 14. 08. 2009).

[Telemediengesetz07] Bundesrepublik Deutschland: Telemediengesetz (2007)
[http://www.gesetze-im-internet.de/bundesrecht/tmg/gesamt.pdf]
(Zugriff am: 04. 12. 2009).

[Thon07] Monika Thon-Soun: Spamabwehr=>Datenschutzerklärung oder Abmahnung bis 50000 Euro (2007)
[http://blog.wordpress-deutschland.org/2007/02/01/spamabwehrdatenschutzerklaerung-oder-abmahnung-bis-50-000euro.html]
(Zugriff am: 26. 01. 2010).

[Trautmann05] Arne Trautmann: Law-Blog (2005)
[http://www.law-blog.de/203/datenschutzerklaerung-webseite/]
(Zugriff am: 04. 12. 2009).

[VeriSign09] VeriSign: FAQ: SSL mit Extended Validation (2009)
[http://www.verisign.de/ssl/ssl-information-center/extended-validation-ssl-certificates/index.html#a3]
(Zugriff am: 17. 12. 2009).

[Wiki09a1] Wikipedia: Asymmetrische Kryptosysteme (2009)
[http://de.wikipedia.org/wiki/Asymmetrische_Verschl%C3%BCsselung]
(Zugriff am: 04. 12. 2009).

[Wiki09b1] Wikipedia: Benutzerfreundlichkeit (2009)
[http://de.wikipedia.org/wiki/Benutzerfreundlichkeit]
(Zugriff am: 17. 12. 2009).

[Wiki09d1] Wikipedia: Digitale Signatur (2009)
[http://de.wikipedia.org/wiki/Digitale_Signatur]
(Zugriff am: 15. 12. 2009).

[Wiki09d2] Wikipedia: Drei-Wege-Handshake (2009)
[http://de.wikipedia.org/wiki/Drei-Wege-Handshake]
(Zugriff am: 15. 12. 2009).

[Wiki09h1] Wikipedia: Hacker (2009)
[http://de.wikipedia.org/wiki/Hacker]
(Zugriff am: 02. 12. 2009).

[Wiki09h2] Wikipedia: HTTP-Authentifizierung (2009)
[http://de.wikipedia.org/wiki/HTTP-Authentifizierung#Basic_Authentication]
(Zugriff am: 02. 12. 2009).

[Wiki09k1] Wikipedia: Kontingenz (Soziologie) (2009)
[http://de.wikipedia.org/wiki/Kontingenz_%28Soziologie%29]
(Zugriff am: 18. 01. 2010).

[Wiki09s1] Wikipedia: S-HTTP (2009)
[http://de.wikipedia.org/wiki/S-HTTP]
(Zugriff am: 03. 12. 2009).

[Wiki09s2] Wikipedia: Sicherheit (2009)
[http://de.wikipedia.org/wiki/Sicherheit]
(Zugriff am: 02. 12. 2009).

[Wiki09t1] Wikipedia: Transport Layer Security (2009)
[http://de.wikipedia.org/wiki/Transport_Layer_Security]
(Zugriff am: 02. 12. 2009).

[Wiki09t2] Wikipedia: Transaktion (2008)
[http://de.wikipedia.org/wiki/Transaktion]
(Zugriff am: 17. 12. 2009).

[Wiki09u1] Wikipedia: Uniform Resource Locator (2009)
[http://de.wikipedia.org/w/index.php?title=Uniform_Resource_Locator]
(Zugriff am: 18. 01. 2010).

[Wiki09v1] Wikipedia: Verschlüsselung (2009)
[http://de.wikipedia.org/wiki/Verschl%C3%BCsselung]
(Zugriff am: 15. 12. 2009).

[Wiki10a1] Wikipedia: Authentifizierung (2010)
[http://de.wikipedia.org/wiki/Authentifizierung]
(Zugriff am: 12. 01. 2010).

[Wiki10j1] Wikipedia: JavaScript (2010)
[http://de.wikipedia.org/wiki/JavaScript]
(Zugriff am: 07. 01. 2010).

[Zahn98] Annja Zahn: Sichere Datenübertragung im Internet (1998)
[http://www.rz.uni-augsburg.de/connect/1998-02/sicherheit/]
(Zugriff am: 02. 12. 2009).

[Zimmermann09] Mike Zimmermann: Firefox weiter verbreitet als Internet Explorer (2009)
[http://www.browser1.de/news/firefox-weiter-verbreitet-als-internet-explorer-371.html]
(Zugriff am: 03. 02. 2010).

Abbildungsverzeichnis

Abbildung 1: Grenzen zw. Mensch und (tech.) Funktionalität bei "Vertrauen" 30
Abbildung 2: Arten von Vertrauen 33
Abbildung 3: Drei-Phasen-Modell des Vertrauensaufbaus 36
Abbildung 4: Darstellung von SSL beim Internet Explorer 42
Abbildung 5: Darstellung von SSL beim Firefox 42
Abbildung 6: Farbige Navigationsleiste beim Firefox 43
Abbildung 7: Farbige Adressleiste beim Internet Explorer 8 43
Abbildung 8: Fehlerhaftes SSL-Zertifikat beim Firefox 44
Abbildung 9: Hinweisseite beim Internet Explorer 44
Abbildung 10: Fehlerhaftes SSL-Zertifikat beim Internet Explorer 45
Abbildung 11: Zertifikatsinformationen beim Internet Explorer 46
Abbildung 12: Zertifikatsinformationen beim Firefox 47
Abbildung 13: Sicherheitsgrafik von thawte 57
Abbildung 14: Sicherheitsgrafik von VeriSign 57
Abbildung 15: RosyTec.de – Secured Logo von VeriSign auf der Startseite 58
Abbildung 16: RosyTec.de – Darstellung der Zertifikatsinformationen 59
Abbildung 17: RosyTec.de – Link zur Datenschutzerklärung 60
Abbildung 18: RosyTec.de – Datenschutzerklärung 61
Abbildung 19: Beispiel für Matrixfragen 63
Abbildung 20: Lösung des Problems: Matrixfrage 64

Abkürzungsverzeichnis

CUI	Character User Interface
E-Mail	Elektronische Mail
EV-SSL	Extended Validation Secure Socket Layer
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
ID	Identifikator
IT	Informationstechnologie
S-HTTP	Secure Hypertext Transfer Protocol
SSL	Secure Socket Layer
TCP/TP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security
UI	User Interface
URL	Uniform Resource Locator
WWW	World Wide Web

Glossar

Asymmetrische Verschlüsselung	„Jede Partei besitzt den öffentlichen Schlüssel des anderen und seinen eigenen privaten Schlüssel. Der öffentliche Schlüssel ermöglicht es jedem, Daten für den Inhaber des privaten Schlüssels zu verschlüsseln, dessen digitale Signaturen zu prüfen oder ihn zu authentifizieren. Der private Schlüssel ermöglicht es seinem Inhaber, mit dem öffentlichen Schlüssel verschlüsselte Daten zu entschlüsseln, digitale Signaturen zu erzeugen oder sich zu authentisieren. Im Gegensatz zu einer symmetrischen Verschlüsselung müssen die kommunizierenden Parteien keinen gemeinsamen geheimen Schlüssel kennen“ [Wiki09a1].
Authentifizierung	Die Authentifizierung „ist der Nachweis einer behaupteten Eigenschaft einer Partei, die beispielsweise ein Mensch, ein Gerät, ein Dokument oder eine Information sein kann“ [Wiki10a1].
Authentisierung	Die Authentisierung ist eine behauptete Eigenschaft einer Partei o. ä., die bisher keinen Nachweis hat. Bei einer Authentisierung wird eine Authentifizierung gefordert. Der Benutzer authentisiert sich am Server. Der Server authentifiziert den Benutzer.
Benutzerfreundlichkeit	Die Benutzerfreundlichkeit ist die vom Nutzer erlebte Nutzungsqualität bei der Interaktion mit einem System (vgl. Kap. 4.3.4).

Checkliste	Eine Checkliste ist eine Liste, die zur Kontrolle genutzt wird. Der Begriff „Check“ kommt aus dem Englischen und hat in diesem Kontext die Bedeutung „abhaken“.
Chiffrierung	Chiffrierung nennt man den „Vorgang, bei dem ein klar lesbarer Text […] mithilfe eines Verschlüsselungsverfahrens in eine „unleserliche“, das heißt nicht einfach interpretierbare Zeichenfolge umgewandelt wird“ [Wiki09v1].
Digitale Unterschrift	Die digitale Unterschrift „ist ein kryptografisches Verfahren, bei dem zu einer „Nachricht“ […] eine Zahl […] berechnet wird, deren Urheberschaft und Zugehörigkeit zur Nachricht durch jeden geprüft werden können“ [Wiki09d1].
Empfehlungsdienst	„Empfehlungsdienste generieren Empfehlungen über Güter und Dienstleistungen, die sich […] auf deren Qualität […] beziehen“ ([EggMüller01], S. 38).
Ethnomethologie	Die Ethnomethologie ist die Soziologie des Alltäglichen. Sie will die formalen Strukturen der Alltagshandlungen beschreiben (vgl. [Ostwald00]).
Geschlossene Fragen	Unter geschlossenen Fragen versteht man Fragen, die nur vorgegebenen Antwortmöglichkeiten besitzen, z. B. Ja/Nein-Fragen oder Multiple Choice-Fragen (vgl. [Albers04], S. 1).
Handshake	Mit dem Handshake „ist ein Verfahren zum Aufbau verlustfreier Datenübertragungen zwischen zwei Instanzen gemeint“ [Wiki09d2].

Hashcode	Der Hashcode ist eine Zeichenfolge, die aus einer Kombination von unterschiedlichen Werten gebildet wird.
http-Methode	Diese Methode bestimmt die Aktion der Client-Anforderung, d. h. GET, DELETE, CONNECT usw. (vgl. [Reibold01]).
Item	Ein Item stellt eine Antwort-Fragen-Kombination in einem Fragebogen dar.
Kontingenz	In der Philosophie und Soziologie bezeichnet der Begriff, die prinzipielle Offenheit und die Ungewissheit menschlicher Lebenserfahrung (vgl. [Wiki09k1]).
Online-Fragebogen	Elektronischer Fragebogen, d. h. ein Fragebogen der über das Medium Internet Daten erhebt.
Secured Logo	Damit ist eine Grafik des Herstellers von SSL-Zertifikaten gemeint, die darauf hinweist, dass sensible Daten mithilfe des SSL-Protokolls übermittelt werden.
TCP/IP	TCP/IP ist ein Netzwerkprotokoll, das aus den Protokollen TCP und IP besteht. Es regelt im Netzwerk den Datentransport, Datenfluss und die Leitungswege.
Untersuchungsleiter	Der Untersuchungsleiter ist die verantwortliche Person für den Online-Fragebogen.
URL (Uniform Resource Locator)	Die URL wird verwendet, um eine Ressource im Netzwerk zu identifizieren und lokalisieren. Synonym für URL ist der Begriff „Internetadresse“ (vgl. [Wiki09u1]).

Usability	Usability ist der englische Begriff für Benutzerfreundlichkeit.
Verschlüsselung	Vgl. Chiffrierung.
WWW-Umfragen	WWW-Umfragen sind Befragungen die im World Wide Web also dem Internet durchgeführt werden, meist mithilfe von Online-Fragebögen.

Anlage

Im folgenden Abschnitt werden die in der Ausarbeitung genannten Ergebnisse, ein Leitfaden und eine Checkliste, dargestellt.

Der Leitfaden beinhaltet eine Zusammenfassung aller genannten Merkmale, die vor der Erstellung eines Online-Fragebogens beachtet werden sollten.

Die Checkliste ist als Kontrollinstrument gedacht und soll nach der Fertigstellung eines Online-Fragebogens zum Einsatz kommen.

I. Leitfaden zur Erstellung des Online-Fragebogens

Zielgruppenbestimmung

Die Zielgruppe des Online-Fragebogens sollte mithilfe der Beantwortung von folgenden Fragen bestimmt werden:

- Was ist Untersuchungsgegenstand des Online-Fragebogens?
- Welcher Personenkreis soll die Fragen beantworten?
- Können die gewünschten Personen die Fragen beantworten?
- Werden alle Personen über den Online-Fragebogen erreicht?

Empfehlungen für die IT

Zur sicheren Übertragung der Daten des Online-Fragebogens sollte das **SSL-Protokoll** verwendet werden. Diese Form der Datenübertragung kann von jedem Benutzer ohne Aufwand genutzt werden und birgt auch nicht die Gefahr, dass jemand durch diese Technik ausgeschlossen wird.

Wenn möglich sollte man auf **Java Applets** und die Verwendung von **JavaScript verzichten**, da Webbrowser dem Benutzer erlauben, diese zu deaktivieren. Das hätte zur Folge, dass ein fehlerfreier Ablauf verhindert werden könnte.

Gestaltung der Benutzeroberfläche

Es muss ein **Begleittext** erstellt werden, der die Motivation fördert und den Kontext der Untersuchung erklärt. Folgendes sollte bei diesem Text beachtet werden:

- Keine Tatsachenbehauptungen formulieren.
- Umfassende Grundaussagen in mehrere Einzelaussagen teilen.
- Ein Foto des Untersuchungsleiters einbinden, um die soziale Präsenz entstehen zu lassen.
- Klare Informationen über die Identität des Online-Unternehmens mitteilen wie auch über Modalitäten und Bedingungen jeder Transaktion.
- Hinweise zum Schutz der Privatsphäre aufzeigen.

Außerdem sollte ein **Instruktionstext** erstellt werden, welcher die Art des Ausfüllens im Online-Fragebogen erläutert. In diesem Text sollten dem Benutzer folgende benutzerfreundlich formulierten Hinweise mitgegeben werden:

- Vollständige Antworten sind gewünscht.
- Antworten sollen aufrichtig sein.
- Die Anonymität wird garantiert.
- Möglichst zügig zu antworten, da es kein Wissenstest ist.
- Die persönliche Meinung ist entscheidend und es gibt daher keine richtigen oder falschen Antworten.
- Die Daten werden zu Forschungszwecken verwendet und nicht zur Bestimmung individueller Diagnosen mit Konsequenzen für die Versuchsperson.
- Datenschutz wird gewährleistet.
- Die benötigte Dauer zum Ausfüllen des Online-Fragebogens.

Grundsätzlich sollte man bei beiden Texten darauf achten, dass diese **nicht zu lang** werden. Daher besteht auch die Möglichkeit, dass man beide Texte miteinander kombiniert.

Bei der Gestaltung des Layouts ist darauf zu achten, dass ein **einheitliches Layout**, das gegebenenfalls auf das Unternehmensdesign anzupassen ist, gewählt wird. Dies sorgt für einen Wiedererkennungseffekt des Unternehmens. Weiterhin sollt ein starker Wechsel von Schriftarten, Farben usw. unterbunden werden. Hierbei sollte man die **Benutzerfreundlichkeit** des Online-Fragebogens beachten. Folgende Hinweise können helfen, die Benutzerfreundlichkeit zu erhöhen:

- Scrollen vermeiden.
- Häufiges Wechseln von Maus und Tastatur vermeiden, jedoch darauf achten, dass keine Matrixfragen genutzt werden.
- Dialogverhalten sollte einheitlich und konsistent sein.
- Benutzer muss seinen nächsten Schritt jederzeit entscheiden können (Weitermachen, Zurücknehmen oder Abbrechen).
- Ungültige Eingaben sollten bereits von der Oberfläche verhindert werden.

Wenn man ein SSL-Zertifikat von einem der bekannten Hersteller verwendet, gibt es die Möglichkeit, bereits auf nicht verschlüsselten Seiten zu zeigen, dass mittels SSL die Daten verschlüsselt übermittelt werden. Es empfiehlt sich, das **Secured Logo des Zertifikatherstellers** als Sicherheitsmerkmal in das Layout des Online-Fragebogens **einzupflegen**.

Neben der Benutzerfreundlichkeit beim Layout sollte man auch darauf achten, dass die **Datenschutzerklärung des Webseitenbetreibers gut sichtbar** ist bzw. der Link zu dieser Erklärung hervorgehoben wird.

Hinweise zur Fragenkonstruktion

Auf die **Einleitungsfrage** sollte man große Aufmerksamkeit legen, da mit dieser Frage der Online-Fragebogen startet und man bereits Vertrauen aufgebaut hat, welches durch eine ungünstige erste Frage zerstört werden könnte. Folgende Hinweise sollten beachtet werden:

- Diese Frage muss direkt den Untersuchungsinhalt ansprechen.
- Diese Frage muss neutral formuliert sein.
- Die Frage muss leicht zu beantworten sein.

Neben den Hinweisen für die Einleitungsfrage gibt es noch einige Empfehlungen, die allgemein für die **Formulierung von Fragen** wichtig sind. Diese werden in der folgenden Auflistung dargestellt:

- Die Fragen sollten von allen Befragten in gleicher Weise verstanden werden.
- Die Fragen sollten kurz und prägnant formuliert werden.
- Die Fragenformulierung darf den Befragten nicht überfordern.
- Konzepte, die dem Befragten nicht bekannt sein könnten, sollten nicht abgefragt werden.
- Bei geschlossenen Fragen müssen die Antwortkategorien vollständig sein und dürfen sich nicht überschneiden.
- Werden Fremdwörter o. ä. verwendet, sollte man zur Beantwortung der Fragen verständliche Hinweise geben.
- Die Fragen sollten nicht zu allgemein formuliert werden. Sie sollten spezifisch und konkret formuliert werden, jedoch für jeden verständlich.

- Die Fragen sollten umgangssprachlich formuliert werden. Verständlichkeit ist wichtiger als die grammatikalische Richtigkeit.
- Wenn in Fragen nach Häufigkeit, Dauer oder Größe gefragt wird, muss die Einheit angegeben werden, in denen die Antworten erfolgen sollen.
- Die Fragen sollten durchnummeriert werden und es sollte ggf. Sprungmöglichkeiten geben.

II. Checkliste

Zielgruppenbestimmung

- [ ] Untersuchungsgegenstand wurde festgelegt
- [ ] Den zu befragenden Personenkreis definiert
- [ ] Die zu Befragenden können auf den Online-Fragebogen zuzugreifen

Empfehlungen für die IT

- [ ] SSL wird verwendet
- [ ] Java Applets werden vermieden
- [ ] JavaScript wird vermieden

Gestaltung der Benutzeroberfläche

- [ ] Begleittext ist vorhanden
- [ ] → Enthält keine Tatsachenbehauptungen
- [ ] → Umfassende Grundaussagen sind in einzelne Teilaussagen geteilt
- [ ] → Foto des Untersuchungsleiters ist eingebunden
- [ ] → Informationen über das Online-Unternehmen sind enthalten
- [ ] → Modalitäten und Informationen über die Transaktion werden vermittelt
- [ ] → Hinweise zum Schutz der Privatsphäre sind geschildert
- [ ] Instruktionstext ist vorhanden

Der Instruktionstext enthält die Aussage, dass…

- [ ] …vollständige Antworten gewünscht sind
- [ ] … aufrichtig geantwortet werden soll
- [ ] … Anonymität garantiert wird
- [ ] … es kein Wissenstest ist und man daher zügig antworten kann
- [ ] … nur die persönliche Meinung entscheidend ist
- [ ] … Datenschutz gewährleistet wird
- [ ] … die Dauer des Fragebogens x Minuten beträgt
- [ ] … die Daten für Forschungszwecke genutzt werden und der Person kein Nachteil durch die Preisgabe der Daten entsteht

- [ ] Begleit- und Instruktionstext sind nicht zu lang
- [ ] Einheitliches Layout, d. h. kein ständiger Wechsel von Schriftarten und Farben
- [ ] Secured Logo des Zertifikatherstellers wurde eingepflegt
- [ ] Datenschutzerklärung des Webseitenbetreibers ist deutlich zu sehen
- [ ] Hinweise zur Benutzerfreundlichkeit wurden beachtet
- [ ] → Scrollen wird vermieden
- [ ] → Kein starker Wechsel von Maus und Tastatur
- [ ] → Matrixfragen werden vermieden
- [ ] → Verhalten von Dialogen ist konsistent und einheitlich
- [ ] → Benutzer kann seinen nächsten Schritt jederzeit frei entscheiden
- [ ] → Ungültige Eingaben werden bereits von der Oberfläche gemeldet

Hinweise zur Fragenkonstruktion

Die Einleitungsfrage …

- [ ] … spricht den Untersuchungsinhalt an
- [ ] … ist neutral formuliert
- [ ] … ist leicht zu beantworten

Die Fragen …

- [ ] … werden von allen Befragten auf gleiche Weise verstanden
- [ ] … sind kurz und prägnant formuliert
- [ ] … überfordern den Befragten nicht
- [ ] … sind nicht zu allgemein, sondern spezifisch und konkret formuliert
- [ ] … sind umgangssprachlich formuliert
- [ ] … sind durchnummeriert

- [ ] Die genannten Konzepte sind allen Befragten bekannt
- [ ] Bei geschlossenen Fragen sind die Antwortkategorien vollständig
- [ ] Fremd- bzw. Fachwörter werden erläutert
- [ ] Bei Fragen nach Häufigkeit, Dauer oder Größe ist die Einheit angegeben
- [ ] Es gibt Sprungmarken