FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Der Einfluss von Bildungsmaßnahmen auf die Relevanz von Internet Privacy für Endnutzer

MAGISTERARBEIT

zur Erlangung des akademischen Grades

Magister der Sozial- und Wirtschaftswissenschaften

im Rahmen des Studiums

Informatikmanagement

eingereicht von

Christian Schmidt
Matrikelnummer 0325576

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung
Betreuer/in: PD Dr. Edgar Weippl

Wien, 24.07.2014

(Unterschrift Verfasser/in)

(Unterschrift Betreuer/in)

Schmidt Christian
Loitzbach 10
3240 Mank

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 24.07.2014

(Unterschrift Verfasser/in)

Zusammenfassung

Internet Privacy bzw. der Datenschutz im Internet beschäftigt sich mit der Anwendung identitätsbezogener Informationen und deren Kontrolle. Jede reale Person bildet mit den im Internet gesetzten Aktivitäten und der Menge an preisgegebenen persönlichen Details eine virtuelle Identität und ist über diese definierbar. Die Privatsphäre eines Internet Nutzers ist somit bei jeder Nutzung eines Webdienstes oder beim Internetzugang selbst (Vorratsdatenspeicherung) potentiell gefährdet, wobei fremde Kommunikationsteilnehmer in der Lage sind, Nutzerinformationen zu sammeln und Verhaltens-, Bewegungs- oder Kommunikationsprofile zu erstellen. Dieser schwerwiegende Eingriff in die Privatsphäre der Internet Nutzer wird vielfach unterschätzt, da mögliche langfristige Konsequenzen der sensiblen Informationsoffenlegung für den Einzelnen oft nicht greifbar sind.

In dieser Arbeit wird eine empirische Untersuchung vorgestellt, bei der in erster Linie das Bewusstsein für Privatsphäre im Internet von Endnutzern erhoben wird, um anschließend die Relevanz von Bildungsmaßnahmen zu analysieren. Zu diesem Zweck wurde ein didaktisches Model ausgearbeitet, welches als Schulungsmaßnahme (Treatment) für die Untersuchung verwendet wird. Den Probanden wird dabei wesentliches Wissen über die Thematik vermittelt und mögliche Lösungsansätze zum Schutz der virtuellen Privatsphäre präsentiert. Zudem wurde die Lehrmethode verschiedenen Lerntypen angepasst, sodass die Inhalte nach auditiven, visuellen, kommunikativen oder motorischen Gesichtspunkten vorgetragen werden. Abschließend wurde nach der Lerneinheit der Lernerfolg unter den Untersuchungsteilnehmern evaluiert und die kurz- und langfristigen Veränderungen im Umgang mit personenbezogenen Daten beim Internetsurfen festgehalten. Diese gesammelten Erfahrungen stellen wertvolle Erkenntnisse dar, um Ausbildungsmaßnahmen in diesem Bereich möglichst effizient zu gestalten. Die Erhöhung des Bewusstseins über die Privatsphäre im Internet und die Vermittlung von Lösungssätzen diese zu schützen stellen das Gesamtziel der Masterarbeit dar.

Abstract

Internet privacy and data protection on the Internet deal with the application of identity-related information and their control. A person can be defined by a virtual identity composed of disclosed snippets of personal details and activities on the Internet (data exhaust). Consequently a user‘s privacy is potentially endangered through each use of Web services or the Internet access itself. Third parties are able to intercept and collect user information in order to create profiles of a user's behavior and their movement or communication patterns. This serious encroachment on the privacy of Internet users is often underestimated as possible long-term consequences concerning sensitive information disclosure are generally not tangible for individuals.

In this work, an empirical study is presented, in which the awareness for privacy on the Internet by end-users is investigated in order to subsequently analyze the relevance of education measures. To this end, a didactic model has been developed, which is used as a training measure (treatment) for the current study. The participants obtain essential knowledge about the topic and potential solutions for the protection of virtual privacy. In addition, the method of teaching has been adjusted to different types of learners taking into account various auditory, visual, communicative or motoric aspects. Finally, the learning outcome among the study participants was evaluated and the short- and long-term changes in the handling of personal data while surfing were examined and retained. The lessons learned provide valuable insights for making training and education in this area as efficient as possible. The increasing awareness about privacy on the Internet and methods to protect and guard it form the overall objective of this thesis.

Inhaltsverzeichnis

Zusammenfassung **iii**

Abstract **iv**

Inhaltsverzeichnis **v**

Abbildungsverzeichnis **vi**

Tabellenverzeichnis **vii**

1 Einführung **1**
1.1 Fragestellung und Zielsetzung der Arbeit 1
1.2 Einbettung in Wissenschaft und Forschung 3
1.3 Aufbau der Arbeit 10

2 Vorstellung und Durchführung der Untersuchungsmethode **11**
2.1 Vorstellung des Untersuchungsdesigns 11
2.2 Probanden der Untersuchung 12
2.3 Grundzüge der Untersuchungsmethode 13
2.4 Durchführung der Studie 18
2.5 Auswertungsstrategie 19

3 Inhalt und Aufbau des lerntypenabhängigen, didaktischen Modell **21**
3.1 Inhalte der Lerneinheit 21
3.2 Anpassung des didaktischen Modells an verschiedene Lerntypen 29
3.3 Didaktische Modell für den auditiven Lerntypen 30
3.4 Didaktische Modell für den kommunikativen Lerntypen 33
3.5 Didaktische Modell für den visuellen Lerntypen 37
3.6 Didaktische Modell für den motorischen Lerntypen 41

4 Ergebnisse der empirischen Analyse **47**
4.1 Ergebnisse der Pretest-Analyse 47
4.2 Ergebnisse der Posttest-Analyse 57
4.3 Qualitative Erkenntnisse der Lerneinheiten 59

4.4 Langzeitevaluierung der Bildungsmaßnahmen 61

5 Schlussfolgerung und Ausblicke **65**
5.1 Diskussion über zentrale Ergebnisse 65
5.2 Kritische Aspekte der Studie 72
5.3 Ausblick auf weitere Forschungsfragen 73

A Folien der Lerneinheit **75**

B Fragenbögen Pretest, Posttest und Langzeitevaluierung **79**
B.1 Fragebogen für Pretest 79
B.2 Fragebogen für Posttest 90
B.3 Fragebogen für Langzeitevaluierung 93

C Diagramme der empirischen Analyse **97**
C.1 Diagramme der Pretest-Analyse 97
C.2 Diagramme der Posttest-Analyse 106
C.3 Diagramme der qualitativen Analyse 108
C.4 Diagramme der Langzeitevaluierung 109

Literaturverzeichnis **111**

Abbildungsverzeichnis

2.1 Ergebnis eines Lerntypentests nach Sütterlin 15

4.1 Testpersonen nach Alter, Geschlecht und Ausbildung 48
4.2 Verantwortliche für Datenschutz 50
4.3 Nutzung des Internets 51
4.4 Regelmässig besuchte Internetplattformen 52
4.5 Persönliche Profilangaben in sozialen Netzwerken 53
4.6 Vertrauen an IT-Firmen im Umgang mit privaten Daten 56
4.7 Änderung des Telekommunikationsverhalten 57
4.8 Einschätzung des Lernzuwachs 58
4.9 Lösung der praktischen Teile beim Posttest 60
4.10 Dauer der einzelnen Untersuchungen 60
4.11 Erklärung von Begriffen 62
4.12 Vertrauen in IT-Firmen im Umgang mit privaten Daten 64

A.1 Folien für die Einführung 76
A.2 Folien für die Begriffe Privacy, Identität, Anonymität 76
A.3 Folien für User Tracking 77
A.4 Folien für weitere Gefahren und Risiken 77
A.5 Folien für prakt. Lösungsansätze und Conclusio 77

C.1 Erklärungsversuche durch den Probanden 97
C.2 Wichtigkeit von Privatsphäre (nach Ausbildung) 98
C.3 Fragen zur Nutzung von Anonymisierungstechniken und Preisgabe von persönlichen Daten 98
C.4 Bestandteile eines Benutzernamens 98
C.5 Verschiedene Fragen zu Privatsphäre im Internet 99
C.6 Verwendungszweck der im Internet veröffentlichten Inhalte 100
C.7 Besitz eines Smartphones 100
C.8 Genutze Internetplattformen (nach Altersgruppe) 101
C.9 Anzahl an Registrierungen über alle Plattformen 101
C.10 Anzahl an betreuten Benutzerkonten 102
C.11 Beliebte Suchmaschinen und Weitergabe von Suchtermen 102
C.12 Handhabung von Suchmaschinen 103
C.13 Aktive und passive Nutzung von Internetdiensten 104
C.14 Übermittlung persönlicher Daten 104
C.15 Umgang mit der Vorratsdatenspeicherung (VDS) 105
C.16 Dauer der Speicherung von Verkehrsdaten 105
C.17 Wissen über Anonymisierungsdienste 105
C.18 Vorschläge für Verbesserungsansätze 106
C.19 Begriffsdefinitionen 106
C.20 Fragen zum theoretischen Verständnis 107
C.21 Rückfragen durch Probanden 108
C.22 Software auf eigenen Gerät ausprobiert 108
C.23 Daten der Vorratsdatenspeicherung 109
C.24 Berührungspunkte mit Privatsphäre im Internet 109
C.25 Veränderungen durch Bildungsmaßnahmen 109

Tabellenverzeichnis

3.1 Didaktisches Modell, Lernziel und geplante Zeitaufteilung 22
3.2 Angewandtes didaktisches Modell für den auditiven Lerntypen 34

3.3 Angewandtes didaktisches Modell für den kommunikativen Lerntypen 38
3.4 Angewandtes didaktisches Modell für den visuellen Lerntypen 42
3.5 Angewandtes didaktisches Modell für den motorischen Lerntypen 46

KAPITEL 1

Einführung

1.1 Fragestellung und Zielsetzung der Arbeit

Internet Privacy oder der Datenschutz im Internet beschäftigt sich mit der Anwendung identitätsbezogener Informationen und deren Kontrolle. Jeder Internet User ist mit einer virtuellen Identität definierbar, die sich aus mehreren persönlichen Details zusammensetzt. Bei jeder Nutzung von freien Webdiensten (Suchmaschinen, Sprachübersetzungs-Tools, Email-Dienste oder soziale Netzwerke) werden potentiell sensible Daten in Form von Inhalten, Aktivitätsaufzeichnungen oder Nutzerinteressen preisgegeben. Auch beim Internetzugang selbst können personenbezogene Daten gespeichert werden, wie das beispielsweise bei der gesetzlichen Regelung der Vorratsdatenspeicherung der Fall ist. Zudem werden auch beim normalen Internetsurfen Informationen (Browserparameter, Verkehrsdaten) an den Zielserver gesandt, womit unter Umständen ein User einer realen Person eindeutig zugeordnet werden kann.

Obwohl dabei teilweise tief in die Privatsphäre eingegriffen wird, kann diese Informationssammlung für den User durchaus nützlich sein. Kennt ein Webdienst die Interessen eines Internet Users oder beliebte Produkte eines Kunden, ist diese Instanz in der Lage, relevante Produkte und Dienstleistungen vorzuschlagen oder Gutschriften und Rabatte zu vergeben. Auch die Anwendung von Webdiensten, wie zum Beispiel die Google-Suchmaschine, ist gratis und kann in voller Funktionalität genutzt werden. Trotz dieser eher positiven Eigenschaften ergeben sich für den Nutzer auch Schattenseiten. Beim Internetsurfen oder Nutzung von Webdiensten besteht das Risiko, dass vom User sensible Informationen offengelegt werden und diese von anderen über die Zeit gesammelt werden. So kann im geeigneten Kontext oft vom virtuellen Nutzer auf eine reale Person rückgeschlossen werden und aufgrund von Verhaltensweisen und Interessen ein Personenprofil erstellt werden. Diese Profile sind vor allem für die Werbewirtschaft interessant, die ihre virtuellen Werbebanner entsprechend anpassen kann und damit auf Facebook oder auf anderen Webseiten zielgerechte Werbung schalten kann. Letztendlich könnte sich der Internet User in einer Umgebung befinden, wo ihm keine neuen Sachen mehr angeboten werden und sich nur mehr im eigenen Interessensgebiet aufhält. Dabei übernehmen möglicherweise andere Instanzen das „Denken“ und entscheiden, was für einen User interessant ist.

Beim Internetsurfen oder bei der Nutzung von verschiedenen Webdiensten werden oft kleine Datenfragmente der User preisgegeben und erscheinen als solche harmlos. Der in einem ACM-Paper von Sobiesk et.al. [1] postulierte Satz „A man has nothing to fear“ trifft diesen Gedankengang sehr treffend. Oft findet sich der Internet User mit dieser Informationsoffenlegung ab und rechnet sogar damit, dass diese Daten für weitere Zwecke verwendet werden. Er stellt dabei die kurzfristige Nutzung des Dienstes über die langfristigen Konsequenzen. Die Aggregation und Zusammensetzung dieser über die Zeit gesammelten Nutzerinformationen ergeben jedoch ein viel umfassenderes Bild über einen User oder einer realen Person. Verhaltensweisen, Interessen oder Kommunikationswege können abgeleitet und langfristig festgehalten werden. Diese Tatsache stellt potentiell einen tiefen Eingriff in die Privatsphäre dar.

Technische Gegenmaßnahmen, die die Privatsphäre schützen, sind häufig dem User nicht bekannt oder werden aus Gründen der Performance (TOR) nicht verwendet. Doch oft hilft schon die einfache Installierung und Nutzung eines fremden VPN-Netzwerks oder eines Firefox Plug-Ins, um die Sammlung der Userdaten zu stoppen, ohne Einbußen in der Surfgeschwindigkeit zu erleiden. Auch bei der Nutzung diverser Webdienste lauern oft Risiken und Gefahren, wogegen sich der User mithilfe von Software-Tools oder durch Know-how schützen kann.

Aus dieser Problemstellung beschäftigt sich die vorliegende Magisterarbeit mit der Frage, welchen Einfluss Bildungsmaßnahmen auf die Relevanz von Privatsphäre im Internet für Endnutzer haben. Zur Beantwortung dieser Frage wurde eine empirische Untersuchung aufgesetzt, die dem „Ein-Gruppen-Pretest-Posttest-Design“ [2] angehalten ist. In Form einer „Pretest“-Messung wird analysiert, welche Rolle Internet-Privacy bei den Testpersonen spielt. Als „Treatment“ wird je nach Lerntyp eine angepasste Lehreinheit durchgeführt, wobei der Proband entsprechende Lernziele erreichen soll. Mit der Unterstützung eines Lerntypentests wird festgestellt, nach welchen Gesichtspunkten (auditiv, visuell, kommunikativ oder motorisch) die Lerneinheit angepasst wird. Nach ausgewählter Lernmethode wird eine entsprechend didaktisch aufbereitete Einführung in die Problematik durchgeführt, wodurch mögliche Gefahren, Risiken und die praktische Lösungsansätze vorgestellt werden. Nach den Bildungsmaßnahmen wird im Rahmen eines „Posttests“ untersucht, ob die Lernziele erreicht wurden und ob sich das Interesse für den virtuellen Datenschutz verändert hat. Nach einer Zeit von etwa 2-3 Monaten wird die Testperson in Rahmen einer Langzeitevaluierung nochmals gefragt, ob sich langfristige Änderungen beim Internetsurfen ergeben haben. Zusammenfassend verfolgt die Untersuchung grundsätzlich folgende Ziele:

- Eine Bestandsaufnahme der Relevanz des Themas „Privatsphäre im Internet“. Wie ernst nehmen es die Teilnehmer der Studie mit dem virtuellen Datenschutz?

- Entwicklung eines didaktischen Modells zur Schaffung eines Bewusstseins für Internet Privacy, welches den jeweiligen Lerntypen optimal unterstützen sollte.

- Ermittlung des Lernerfolgs der Bildungsmaßnahmen. Wie wurde die Lerneinheit wahrgenommen?

- Feststellung von kurz- und langfristigen Veränderungen beim Internetsurfen.

1.2 Einbettung in Wissenschaft und Forschung

Forschungsmethoden und Evaluation: Für Human- und Sozialwissenschaftler

Das Buch von Bortz et. al. [2] gibt einen guten Überblick über die Planung und Durchführung einer empirischen Untersuchung und beschäftigt sich mit quantitativen und qualitativen Auswertungskriterien. Unter anderem gibt es zwei Kapitel, die einen wesentlichen Beitrag zu der vorliegenden Magisterarbeit geleistet haben. Kapitel 2 „Von einer interessanten Fragestellung zur empirischen Untersuchung“ gibt einen umfassenden Überblick in die Planung einer empirischen Untersuchung. Dabei wurde das Untersuchungsdesign „Ein-Gruppen-Pretest-Posttest-Design“ abgeleitet und angewendet. Darüber hinaus gab das Kapitel gute Ratschläge, wie ein Untersuchungsbericht aufgebaut und strukturiert werden sollte.

Nachdem bei der gewählten Untersuchungsmethode eine Reihe an Messungen in Form von Befragungen durchzuführen ist, war auch das Kapitelt 4 „Quantitative Methoden der Datenerhebung“ von hohem Interesse. Dieses Kapitel gibt einen umfassenden Einblick in Aufbau und Erstellung eines Fragebogens (schriftliche Befragung für Pre- und Posttests) als auch zur Durchführung der Interviews mit den Untersuchungsteilnehmern (mündliche Befragung bei der Langzeitevaluierung).

Didaktik der Informatik: Grundlagen, Konzepte, Beispiele

Dieses Werk von Hubwieser [3] gibt eine grundsätzliche Idee, wie Lerninhalte unterrichtet und Übungen aufgebaut werden. Im Teil C „Unterrichtsbeispiele“ werden verschiedene Vorschläge präsentiert, wie Lernübungen geplant und dabei diverse Lernziele ausgegeben werden.

Dieses Buch bildet die Grundlage für die Formulierung des didaktischen Models, welches als Schulungsmaßnahme in die Untersuchung eingebettet wird.

Vier Lerntypen und wie sie am effektivsten lernen

Diese Ausarbeitung nach Sütterlin [4] beschreibt die Theorie der verschiedenen Lerntypen, wonach jedes Individuum seine Stärken und Schwächen beim Lernen aufweist. Diese Tatsache erklärt sich damit, da jede Person unterschiedlich stark ihre verschiedenen Sinnesorgane (Augen, Ohren, Geruch-, Geschmacks- und Muskelsinn) in Anspruch nimmt, um Inhalte zu erfassen und zu verstehen.

Sütterlin unterscheidet in diesem Beitrag zwischen vier Arten von Lerntypen: auditiv, visuell, kommunikativ und motorisch. Für jeden dieser Typen wird beschrieben und mit Beispielen belegt, mit welchen Hilfsmittel und Methoden eine Person am besten beim Lernen unterstützt werden kann. Zudem wird darauf aufmerksam gemacht, dass prinzipiell je mehr Sinne beim Lernen benutzt werden, desto besser können im Gehirn Verknüpfungen erstellt und der Lernstoff besser eingeprägt werden. Eine komplette Beschränkung auf einen Lerntyp wäre somit nicht zielführend oder sogar fatal. Es ist daher ratsam, beim Lernen möglichst alle Sinne anzusprechen und zu nutzen.

Im Rahmen dieser Ausarbeitung wird weiterführend ein Test angeboten, bei dem in 31 Fragen der Lerntyp prozentuell festgestellt wird, der am ehesten zum Antwortgeber passt.

Aufgrund dieser Typenunterscheidung beim Lernen wird in der vorliegenden Arbeit ein didaktisches Modell ausgearbeitet, womit jeder Proband jeweils am besten unterstützt wird, sich den Lernstoff am effektivsten einzuprägen.

Network Security: Private Communications in a Public World

Das Buch von Speciner et.al. [5] beschäftigt sich mit der Absicherung von IT-Netzwerken und stellt prinzipielle Konzepte der virtuellen Kommunikation vor. Für die vorliegende Arbeit sind im Besonderen zwei Kapitel von Interesse. Im Abschnitt „Web Issues“ werden unter anderem das Konzept der Cookies vorgestellt. In diesem Zusammenhang wird eindrucksvoll dargestellt, wie User Tracking funktioniert und wie dagegen vorgegangen werden kann. Zudem wird das Konzept des „Spoofings“ vorgestellt, wobei bösartige Webseiten dem Internet User vorgetäuscht werden, um so persönliche und private Informationen zu entlocken. So erklärt dieser Abschnitt wesentliche Bedrohungsszenarien, die beim Internetsurfen auftreten können.

Ein weiteres Kapitel „Firewalls“ erklärt, wie zwei verschiedene Netzwerke voneinander abgesichert werden und diese über das Konzept einer Firewall miteinander kommunizieren. Zudem werden auch virtuelle Netzwerke, sogenannte VPNs (Virtual Private Network), ausgiebig erklärt, die einen verschlüsselten Datenverkehr ermöglichen. Da dieses Konzept eine gute und schnelle Möglichkeit ist, den eigenen Internetverkehr gegenüber anderen Instanzen (Internet Service Provider, Arbeitgeber, offene WLANs) abzusichern und zu verschlüsseln, werden VPNs unter anderem als Lösungsansatz bei der Lerneinheit vorgestellt.

Introduction to computer security

Das Buch von Bishop [6] gibt eine umfassende Einführung in die Computersicherheit, wobei aus zwei Kapiteln umfangreiches Basiswissen für die vorliegende Magisterarbeit gewonnen werden konnte. Im Kapitel 13 („Representing Identity“) wird im Wesentlichen der Begriff der Identität erklärt und dargestellt, wie dieser in der Informationstechnologie angewendet wird. Meist wird eine Identität aus einer Menge von Eigenschaften oder Privilegien definiert, die ein User inne hat. Eine besondere Rolle bekommt dieser Begriff im Kontext des Internets. Dabei wird häufig eine virtuelle Identität über IP-Adressen oder über Cookies-Informationen wahrgenommen. Ferner wird der Begriff der Anonymität behandelt und erklärt, welche Bedeutung dieser im Web hat. Somit bietet dieses Kapitel grundlegende Basisinformation über diese beiden Begriffe, welche im Rahmen der Lerneinheit den Probanden vermittelt werden.

Darüber hinaus behandelt Kapitel 23 („Network Security“) verschiedene Netzwerkarchitekturen, die zur Absicherungen diverser Netzwerke nützlich sind. Um Anonymität im Bereich des Internets anzuwenden, sind grundlegende Kenntnisse in diesem Bereich unabdingbar. Dieses Kapitel gibt eine Einführung in unterschiedliche Konzepte, wie DMZ-Organisationen („Demilitarized Zone“) oder Firewall- und Proxykonfigurationen. Dieses Wissen ist notwendig, um den Probanden adäquate Lösungen in Form von Software Tools oder organisatorische Ansätze anzubieten, um so ihre Privatsphäre im Internet bestmöglich zu schützen.

Big Data: Die Revolution, die unser Leben verändern wird

Das Buch von Mayer-Schönberger et.al. [7] gibt eine Einführung in „Big Data“. Dabei werden Möglichkeiten und Potentiale beschrieben, die sich aus der Gewinnung und Analyse von großen Datenmengen ergeben. Weiters werden Möglichkeiten erläutert, die über die primäre Nutzung der Daten hinausgehen. Durch die spätere Zweit- oder Drittnutzung von erhobenen Daten können zusätzliche Analysen gestartet werden. All diese Ansätze werden durch mehrere kleine Beispiele unterlegt.

Dieses Buch gibt einen guten Überblick, welches Potential in großen Datenansammlungen steckt und welche langfristigen Konsequenzen sich für die Internet User daraus ergeben. Diese Erkenntnisse bilden eine Grundlage für Bildungsmaßnahmen, in welcher dem Probanden viele Beispiele und mögliche Folgen der sensiblen Informationsoffenlegung vermittelt werden.

An Honest Man Has Nothing to Fear: User Perceptions on Web-based Information Disclosure

In diesem Paper von Sobiesk et.al. [1] wird eine Studie vorgestellt, bei der die Messung der Wahrnehmung von Datenschutz durch den Internet User ermittelt wird. Durch eine Vielzahl an frei-nutzbaren Webdiensten und deren Geschäftsmodellen, welche vorrangig mit gesammelten Vorratsdaten und zielgerechten Werbeschaltungen ihr Geld verdienen, schwankt der User immer zwischen der Nutzung des Dienstes und etwaigen Datenschutzbedenken. Um diesen Zwiespalt wirklich verstehen zu können, müssen erstmal Standpunkte, Vorstellungen und Erwartungshaltungen der User gegenüber diesen Diensten festgehalten werden. Nur so kann eine Umgebung geschaffen werden, wo der Internet User die Möglichkeit bekommt, den Umgang mit seinen Daten besser abschätzen zu können. Im Rahmen dieser Studie steht vorwiegend die Beantwortung folgender Schlüsselfragen im Raum:

- Wie und wie oft nutzt ein typischer Internet User solche Online-Dienste?
- Welche Erwartungshaltung ist in Bezug auf Datenschutz vorhanden?
- Wie wird der Umgang, die Nutzung und die Wiederverwertung persönlicher Daten eingeschätzt?

Bei der vorgestellten Umfrage nahmen 352 College-Studenten und 25 Erwachsene teil, welche mit 25 Fragen zu folgenden Bereichen konfrontiert wurden:

- Suchaktivitäten und präferierte Suchmaschinen
- Suche von sensible Informationen
- Verantwortung für persönlichen Datenschutz
- Vertrautheit mit Vorratsdatenspeicherung und Wahrnehmen der AOL Suchbegriffsveröffentlichung von August 2006
- Vertrauen in IT-Firmen

- Verständnis für Online-Anonymität
- Erwünschte Balance zwischen Privatheit und Nutzen solcher Webdienste

Nach einer Reihe von Auswertungen der einzelnen Fragen werden Hauptergebnisse vorgestellt, die im Rahmen der Analyse wahrgenommen werden konnten. Dabei wurde festgestellt, dass einer überwiegenden Mehrheit aller Befragten der Vorfall über die Veröffentlichung der Suchbegriffe der eingestellten Suchmaschine der Firma AOL nicht bekannt war. Erst durch diesen Zwischenfall wurden Suchbegriffe als sensible Informationen wahrgenommen, weil aus diesen Daten persönliche Interessen oder private Details abgeleitet werden konnten.

Als ein weiteres zentrales Analyseergebnis wurde die These „An Honest Man Has Nothing to Fear“ aufgestellt, wobei die Umfrage folgende Trends aufzeigte:

- User zeigen sich zufrieden bezüglich ihres virtuellen Datenschutzes
- Nutzer zeigen sich zufrieden bezüglich Datenschutz für Suchanfragen sensibler Informationen
- User sehen keine Notwendigkeit für die Anonymisierung ihrer Online-Aktivitäten
- Trotz häufiger Nutzung der Webdienste vertrauen User nicht blind der Firma, die diese bereitstellt
- Obwohl Vorratsdatenspeicherung nicht komplett verstanden wurde, würden die User nur minimale Veränderungen an ihren Online-Verhalten hinnehmen, wenn dabei wirklich alle Aktivitäten mitgespeichert werden würden
- Datenschutz liegt laut User in der persönlichen Verantwortung

Als drittes Hauptergebnis wurden signifikante Unterschiede zwischen den jüngeren und älteren Befragten vorgestellt, die bei der Analyse der einzelnen Fragen ersichtlich wurden. Letztendlich wird in diesem Paper postuliert, dass der kurzfristige Nutzen über langfristige Risiken gestellt wird.

Dieses Paper gibt einen umfassenden Überblick über die Planung, Aufbau und Durchführung einer Umfrage, welche eine gute Basis jeglicher Messungen in dieser Arbeit darstellt.

The Privacy in the Time of the Internet: Secrecy vs Transparency

Das Paper von Pontual et.al. [8] beschäftigt sich mit potentiellen Gefahren und Risiken, die ein Individuum eingeht, wenn von diesem persönliche Informationen öffentlich gemacht werden. Mit der wachsenden Popularität von sozialen Netzwerken (Facebook, MySpace, Orkut, etc.) geben ihre User immer mehr von ihren privaten Details (Namenangaben, Wohnort, Bilder, Adressen, Telefonnummern, Email-Adressen, persönliche Webseiten, etc.) bekannt, ohne die möglichen Konsequenzen zu verstehen. Aber auch Organisationen wie Firmen, Universitäten oder sogar Staatsinstitutionen veröffentlichen aus Gründen der Transparenz sensible Informationen über ihre Kunden, Angestellten oder Einwohner. So werden beispielsweise in Schweden

Einkommenssteuererklärungen im Internet veröffentlicht oder in Texas durch den „Texas Public Information Act“ sensible Daten von allen öffentlichen Angestellten publiziert.

Die vorwiegende Zielsetzung dieser vorliegenden Arbeit ist es, ein Bewusstsein dafür zu schaffen, dass es durchaus möglich ist, persönliche Informationen aus öffentlichen oder nicht-öffentlichen Quellen zu sammeln. In diesem Sinne wurden im Rahmen dieses Papers folgende Arbeiten durchgeführt:

- Design und Entwicklung eines Open Source Frameworks, welches Crawler für verschiedene Webseiten bereitstellt.
- Durchführung einer Informationssammlung von über 6000 Angestellten der Universität von Texas in San Antonio. Zusätzlich wurden Wahrscheinlichkeitsberechnungen angestellt, die messen, wie wahrscheinlich einzelne private Daten (Adresse, Telefonnummer, etc.) in dieser Suche gefunden werden.
- Eine Webseite mit einer kostenpflichtigen Registrierung (Net Detective[1]) und freie Webseiten wurden ebenfalls nach den gleichen Daten abgesucht. Dabei konnten sogar aus den freien Sourcen mehr Daten lukriert werden als von der bezahlten Quelle.

Obwohl einzelne Personen die Offenlegung von kleinen Stücken an privaten Informationen oft als harmlos einstufen würden, zeigt dieses Paper, wie diese Daten zu Teilprofilen aggregiert werden können. Diese zusammengesetzten Profile könnten später durch einen Angreifer gegen Individuen eingesetzt werden. Natürlich ist dieser potentielle Schaden von verschiedenen Faktoren des Opfers, wie Job, wirtschaftlicher Situation oder Wohnort, abhängig. In einem Entwicklungsland mit einer hoher Kriminalitätsrate ist es beispielsweise nicht ratsam, wenn Gehälter und Wohnadressen öffentlich gemacht werden. Mit solchen und weiteren Beispielen zeigt diese Arbeit eine Reihe von möglichen Gefahren für eine Person auf, deren privaten Details an die Öffentlichkeit gelangen:

- Angepasste Werbung: Dabei werden persönliche Informationen über Individuen gesammelt, um so Werbung zielgerecht zu erstellen. Dieses ist zwar keine direkte Bedrohung für den Einzelnen, kann aber aggressiv und lästig sein.
- Stalking, Entführung und Diebstahl: Bei diesen Bedrohungen werden persönliche Daten genutzt, um im realen Leben einer Person Schaden zuzuführen.
- Identitätsdiebstahl: Dabei handelt es sich um den Diebstahl einer Identität aus der realen oder virtuellen Welt (Social Engineering).
- Phishing, Spam und Betrug: Mit dem Einsatz von „Social Engineering“ Techniken werden scheinbar vertrauenswürdige Identitäten vorgespielt, um so zu Kreditkartennummern oder Passwörtern zu gelangen.

[1] `http://www.netdetective.com/`, Juni 2014

- Rufschädigung: Die Schädigung einer Reputation ist von der veröffentlichten Information abhängig. Beispielsweise überprüfen Firmen immer öfters ihre Jobanwärter auf Facebook, um so deren Reputation wahrzunehmen.

Diese Arbeit beschreibt die Möglichkeit, wie private Details aus freien oder bezahlten Quellen gesammelt werden und zeichnet ein umfassendes Bedrohungsszenario für den einzelnen Internet User. Dieses Wissen wird in das didaktische Modell (Kapitel 3) eingearbeitet, um so die möglichen Gefahren für den Internet User während der Lerneinheit zu vermitteln.

Self-monitoring of Web-based Information Disclosure

Mit diesem Paper von Abdullah et.al. [9] wird ein Ansatz vorgestellt, bei dem mit verschieden Visualisierungen ein Bewusstsein dafür geschaffen wird, welche sensiblen Daten bei der Nutzung von freien Online-Tools potenziell an die Öffentlichkeit gelangen. Um die dafür notwendigen Anforderungen zu erarbeiten, wurde eine Gruppe von 18 College-Studenten mit dem Enthüllungsvorfall rund um die AOL-Suchmaschine im Jahr 2006 konfrontiert. Danach wurde diese Gruppe nach ihren Vorschlägen gefragt, was ein System bieten müsste, um solche Vorfälle zu verhindern:

- Zeitbasierte Auflistung von allen potentiellen Veröffentlichungen
- Gruppierung und Kategorisierung von veröffentlichten Informationen nach Inhalt und Webdienst
- Überwachung der am häufig genutzten Suchbegriffe
- Auflistung von meistbesuchten Webseiten
- Überwachung von Cookies
- Ermittlung der Aufenthaltsdauer auf den verschieden Webseiten
- Überwachung aller Aktivitäten auf den Webseiten

Nach dieser Befragung konzentrierte sich das Paper auf die Überwachung von Suchtermen und konstruierte ein Mock-up System, welches benutzte Suchbegriffe über die Zeit mit verschiedenen Diagrammen visualisiert. Für eine weitere Evaluierung sollten weitere 52 Studenten anfangs mit diesem Visualisierungssystem arbeiten, um später nach Nützlichkeit, Effektivität und Sinnhaftigkeit befragt zu werden. Fazit dieser Evaluierung war es, dass die Mehrheit der Befragten es für sehr nützlich empfunden hat, die eigenen Suchaktivitäten zu überwachen und zu sehen, welche Informationen preisgegeben werden.

Dieses Paper zeigt, wie erfolgreich ein derartiges Selbst-Überwachungswerkzeug arbeitet und wie das Bewusstsein von Individuen oder Organisationen gestärkt werden kann, um so die Menge an sensibler Informationsoffenlegungen zu minimieren.

Googling Considered Harmful

Im Internet wird eine Reihe von frei nutzbaren Diensten (Suchmaschinen, Email-Dienste, Sprachübersetzung etc.) angeboten, die häufig von Privatpersonen oder Organisationen für private oder berufliche Zwecke eingesetzt werden. Bei der Nutzung dieser Plattformen wird in der Regel eine Fülle an sensiblen Informationen preisgegeben. Conti et.al. [10] analysiert in dieser Arbeit mögliche Gefahren, die bei der Offenlegung persönlicher Daten drohen. Am Fallbeispiel „Google“ werden zwei Schlüsselaspekte näher betrachtet:

- Bedrohung durch Informationsoffenlegung: Mit jeder Interaktion mit einem Servicebetreiber werden Informationen bekanntgegeben. In diesem Abschnitt wird eine Fülle von Google-Diensten analysiert und aufgezeigt, welche Information jeweils preisgegeben wird. Ergänzend wird eine theoretische Analyse durchgeführt, wie sich die Veröffentlichung sensibler Daten bei mehreren Diensten vom gleichen Anbieter über die Zeit verhält.
- Gefährdung durch Fingerprints: Bei der Nutzung von diesen Diensten werden auch passiv Informationen dem Betreiber übermittelt, wobei der Internet User potentiell eindeutig identifiziert werden kann. In diesem Zusammenhang werden fünf Kernprobleme aufgezählt:
  - Netzwerkadresse: Identifizierung allein durch die IP-Adresse
  - Cookies: Diese Datenschnipsel wurden für das Wiedererkennen von User konzipiert und werden von allen üblichen Browser unterstützt. Dies ist der einfachste Weg einen User eindeutig identifizierbar zu machen und dessen Aktionen zu verfolgen.
  - Browserparameter: Durch das http-Protokoll wird eine Reihe von Browserparameter dem Zielserver übermittelt, wobei Sprache, Bildschirmauflösung, vorhandene Schriftarten, etc. bekannt gegeben werden. Die Kombination dieser Parameter bieten eine gute Möglichkeit einen User eindeutig identifizierbar zu machen.
  - Registrierung: Oft verlangt die Nutzung dieser Dienste eine Registrierung durch Benutzername und Passwort, wodurch ebenfalls der User eindeutig wird.
  - Fingerprints von Inhalten: Bei dieser Bedrohung werden die Inhalte analysiert, um so den Fingerprint festzumachen. Diese Art der Informationsoffenlegung kombiniert mit der Aufzeichnung von Interaktionsverhalten ist es sehr schwer zu verhindern.

Ferner werden mögliche Gegenmaßnahmen diskutiert, die die Wahrscheinlichkeit von Fingerprints erheblich reduzieren:

- Nutzung von verschieden Accounts
- Nutzung von verschiedenen Geräten und Netzwerken
- Verstecken hinter einer Netzwerkarchitektur (NAT-Systeme)
- Nutzung von Proxies

- Schaffung von Bewusstsein
- Direkte Verbindung zum Zielserver
- Erstellung von Richtlinien als Gegenmaßnahmen
- Verwendung von Cookie-Management-Tools
- Abstinenz

Prinzipiell steht immer die Frage im Raum, wie der Nutzen für den User maximiert und der potentielle Schaden in Folge der Informationsoffenlegung möglichst minimiert werden kann. Dieses Paper gibt eine gute Übersicht über alle potentielle Bedrohungsszenarien und erläutert auch mögliche Gegenmaßnahmen. Auch am Fallbeispiel Google lassen sich die einzelnen Arten von Informationen festhalten, die bei jedem Dienst veröffentlicht werden. Vor allem dieses Fallbeispiel wird ausführlich in Kapitel 3.1 vorgestellt und während der Lerneinheit mit dem Probanden diskutiert.

1.3 Aufbau der Arbeit

Die Arbeit setzt in Kapitel 2 mit der Vorstellung der empirischen Untersuchung fort, wobei das Design, alle Messungen und der Plan für die Durchführung und Auswertung ausführlich erläutert werden. Im Kapitel 3 wird das didaktische Modell formuliert, welches als Bildungsmaßnahme in die Untersuchung eingebettet wurde. Zudem werden die Inhalte und die Anpassung an die verschiedenen Lerntypen beschrieben. Kapitel 4 führt die quantitative und qualitative Analyse aller Tests durch, indem alle Fragestellungen ausgewertet werden. Kapitel 5 diskutiert die zentralen Ergebnisse der Untersuchung und führt eine kritische Betrachtung der Untersuchung durch. Abschließend wird ein Ausblick auf weitere Forschungsfragen geboten.

KAPITEL 2

Vorstellung und Durchführung der Untersuchungsmethode

Dieses Kapitel stellt das Design und deren formale Beschreibung der Untersuchung vor, wie sie in der Literatur bekannt ist. Darauf aufbauend wird die praktische Anwendung auf diese Studie dargestellt. Weiters wird die Auswahl der Probanden für die Untersuchung beschrieben und erläutert, welches Procedere die Testpersonen durchlaufen müssen. Am Schluss dieses Kapitels wird die praktische Umsetzung der Untersuchung sowie die Auswertung der einzelnen Tests erläutert.

2.1 Vorstellung des Untersuchungsdesigns

Für diese Untersuchung wurde eine Methode gewählt, welche in der Literatur als „Ein-Gruppen-Pretest-Posttest-Design“ bekannt ist. [2] Dabei wird die Veränderung einer Schulungsmaßnahme durch vorherige und spätere Messungen festgestellt. Formal wird diese Methode durch folgende Charakteristik beschrieben:

$$M_1 \rightarrow \mathrm{T} \rightarrow M_2$$

„M“ steht für eine Messung und symbolisiert eine Befragung einer Testperson. Der Buchstabe „T“ ist Platzhalter für „Treatment“, wobei experimentelle Eingriffe, Manipulationen oder Bildungsmaßnahmen durchgeführt werden. Der Vergleich der Resultate von M_1 und M_2 soll die Veränderung des Treatment (T) messen. Um dieses formale Modell anzuwenden, wird bei dieser Untersuchung der derzeitige Wissenstand (M_1) einer Testperson in Form eines „Pretests“ festgestellt. Nach einer Lerneinheit (T) wird der Lernerfolg mit einem „Posttest“ (M_2) gemessen.

Wie oben beschrieben, wird mit dem Pretest der Ist-Zustand gemessen. Dabei wird beim Probanden erhoben, welche Rolle Privatsphäre im Allgemeinen für ihn spielt. Ferner wird gefragt, ob er sich zu themenbezogenen Begriffen etwas vorstellen kann. Beispielsweise wird dabei

ermittelt, wie wichtig ihm Anonymität im Internet sei. Auch auf die Internetnutzung wird eingegangen und dabei eruiert, wo und mit welchem Gerät er sich mit dem Internet verbindet oder welche Webdienste (soziale Medien, Suchmaschinen,...) dabei in erster Linie genutzt werden. Abschließend wird der Proband mit der aktuellen Diskussion rund um die Vorratsdatenspeicherung (VDS) konfrontiert und dabei festgestellt, ob ein Bewusstsein für dieses Thema vorhanden ist. Eine detaillierte Beschreibung des Pretests folgt in Kapitel 2.3. Im Rahmen der Voruntersuchung wird auch ein Lerntypentest durchgeführt, welcher sich mit den Stärken und Schwächen beim Lernen der Testperson auseinandersetzen soll. Dieser Test wird in Kapitel 2.3 näher erklärt.

Als Treatment wird eine Lerneinheit durchgeführt, wobei der Proband in die Thematik (mit Theorie und Praxiswissen) eingeführt wird. Dabei werden primär die Inhalte vorgetragen, die im Kapitel 3.1 eingehend beschrieben werden. Der Vortrag selbst wird nach den Ergebnissen des Lerntypentests angepasst, um so den größtmöglichen Lernerfolg zu erzielen. Dabei wird zwischen 4 Lerntypen (visuell, auditiv, kommunikativ und motorisch) unterschieden, für welche jeweils ein didaktisches Modell in Kapitel 3.2 vorgestellt wird. Für alle Modelle gelten die gleichen Lernzielvorgaben:

- Vermittlung von Begriffen und Definitionen (z. B.: Privatsphäre, Identität und Anonymität)
- Bewusstseinsschaffung über aktuelle Themen wie Vorratsdatenspeicherung (VDS) und Profilerstellung via User Tracking
- Erörterung möglicher Gefahren und Risiken (z. B.: Search Term Analyse, Tracking Web Interactions, Social Engineering)
- Vorstellung von praktischen Lösungsansätzen zur Erreichung virtueller Anonymität

Direkt nach dem Treatment wird die Messung des Posttests durchgeführt. Ziel des in Kapitel 2.3 vorgestellten Fragebogens ist die Feststellung des Lernerfolgs. Im Vergleich zum Pretest wird gemessen, ob ein Bewusstsein zur Privatsphäre im Internet geschaffen wurde oder sogar das Interesse für diese Thematik gesteigert wurde. Zusätzlich zum Posttest wird eine weitere Langzeitevaluierung durchgeführt, welche in Kapitel 2.3 vorgestellt wird. Dabei wird der Proband nach etwa 2-3 Monaten erneut befragt, was er sich von der Lerneinheit gemerkt hat bzw. welche Erfahrungen er bezüglich Privatsphäre im Internet bis dahin gemacht hat.

Nach der Durchführung der Untersuchung mit allen Testpersonen, werden alle Messungspunkte (Pretest, Posttest, Langzeitevaluierung) zusammengetragen und ausgewertet. Es werden sowohl quantitative als auch qualitative Kriterien bei der Analyse berücksichtigt, welche im Kapitel 4 eingehend diskutiert werden. Die Auswahl der Testpersonen wird im folgenden Unterkapitel 2.2 erläutert.

2.2 Probanden der Untersuchung

Bei der Auswahl der Probanden wird insofern planmäßig vorgegangen, sodass jede Testperson über Mindestkriterien verfügen muss. So wird im Umgang mit dem Internet ein Level ange-

nommen, indem Kenntnisse von Online-Grundlagen einer ECDL Base Zertifizierung[1] vorhanden sein müssen. Dabei werden wesentliche Kenntnisse und Fertigkeiten vorausgesetzt, die für Web-Browsing, effiziente Informationssuche, Online-Kommunikation und E-Mail-Nutzung nötig sind.

Eine Person, die die Mindestkriterien erfüllt, wird bei der Erstanfrage über die grundsätzlichen Ziele der Studie aufgeklärt. Dabei wird der persönliche Nutzen der Lerneinheit erklärt, um auf diese Weise das Interesse zu wecken. Ist ein starkes Interesse und Motivation für dieses Thema bei der gefragten Zielperson feststellbar, wird sofort ein Termin und Ort zur Durchführung der Untersuchung ausgemacht. Lehnt eine Person kategorisch ab, wird nach dem Grund nachgegangen und dokumentiert. Möglicherweise kann die Person durch eine kurze Diskussion und vorgebrachten Argumenten doch noch überredet werden.

Es sollten für diese Studie mindestens 30 Testpersonen gefunden werden. Um diese Anzahl an Untersuchungsteilnehmern zu lukrieren, werden zuerst 50 Namen in eine engere Auswahl genommen, bei denen ausgegangen wird, dass sie die Mindestkriterien erfüllen würden. Zudem wird ein guter Mix an Personen gewählt, die über einen möglichst verschiedenen Ausbildungsgrad verfügen und einer unterschiedlichen Beschäftigung nachgehen, um so einen guten Durchschnitt der Gesellschaft zu erhalten. Weiters wird versucht, eine quantitativ bewertbare Anzahl an Testpersonen für alle 5 Altersklassen (<20, 20-29, 30-39, 40-49, >50) zu finden, die für die Auswertung eine wesentliche Rolle spielen. Dabei werden Verhaltensunterschiede zwischen den Altersklassen festgestellt und diverse Vergleiche angestellt.

Erklärt sich eine Person bereit, an der Untersuchung teilzunehmen, werden Details wie Termin und Ort geklärt. Nachdem eine Lerneinheit nur zwischen Vortragenden und dem Probanden durchgeführt wird, bekommt jede Testperson einen eigenen Termin. Dabei sollte ein Zeitpunkt gefunden werden, bei dem sich die Person in möglichst ungestresster und aufnahmefähiger Situation befindet. Zum Beispiel sollte vermieden werden, dass die Untersuchung nach einem harten Arbeitstag stattfindet, da eine optimale Wissensvermittlung unter diesen Umständen nur schwer möglich wäre. Somit werden Termine am Wochenende oder an freien Tagen bevorzugt. Bezüglich der Örtlichkeit wird darauf geachtet, eine möglichst ruhige Umgebung zu finden, so dass sich der Proband gut auf die Thematik konzentrieren kann und ein ungestörter Vortrag möglich ist.

2.3 Grundzüge der Untersuchungsmethode

Ist eine adäquate Anzahl an Testpersonen mit den beschriebenen Mindestkriterien gefunden worden, durchläuft jeder Proband das gleiche Procedere:

1. Lerntypentest
2. Pretest
3. Lerneinheit
4. Posttest

[1] ECDL Base Zertifikat, http://www.ecdl.at/de/ecdl-base, Jänner 2014

5. Langzeitevaluierung

Da die Lerneinheit didaktisch angepasst wird, wird jede Testperson als Erstes einen Lerntypentest durchführen. Danach wird ein Pretest ausgefüllt, welcher die erste Messung der Untersuchung darstellt und den aktuellen Wissensstand festhält. Im Anschluss wird die Lerneinheit mit dem Probanden durchgeführt, wobei ihm die Thematik näher gebracht wird. Danach wird die 2. Messung in Form des Posttests durchgeführt, welcher im Wesentlichen die Veränderungen des Wissenstandes feststellen soll. Nach 2-3 Monaten wird die Langzeitevaluierung durchgeführt, welche die gesammelten Erfahrungen der Probanden rund um die Privatsphäre im Internet dokumentieren sollte. Um die Untersuchung abzuschließen, werden alle durchgeführten Messungen ausgewertet und einer Analyse unterzogen.

Feststellung des Lerntypen

Die Sinnesorgane einer Person sind für das Lernen maßgebend, wobei neben Augen und Ohren auch Geruchswahrnehmung, Geschmacks- und Muskelsinn beansprucht werden. Durch deren unterschiedliche Ausprägungen hat jede Person bestimmte Stärken und Schwächen beim Lernen. So wird in der Literatur zwischen auditiven, visuellen, kommunikativen und motorischen Lerntypen unterschieden, welche jeweils verschiedene Zugänge beim Lernen aufweisen. Wie der jeweilige Lerntyp didaktisch optimal für die Lerneinheit unterstützt wird, wird in Kapitel 3.2 ausführlich beschrieben. [4]

Zur Feststellung eines Lerntypen wird für diese Untersuchung ein Online-Test[2] herangezogen, der in 32 Fragen versucht, die Stärken und Schwächen einer Testperson beim Lernen herauszufinden. Der Test gibt als Ergebnis eine Prozentzahl für jeden Lerntyp an. Beträgt die Prozentanzahl für einen Typen über 50%, so besitzt der Proband gewisse Stärken für diese Art zu lernen. Es sollten somit Lernmethoden angewendet werden, die im Besonderen diesen Lerntypen unterstützen. Ein Resultat eines Lerntypentests, wie in Abbildung 2.1 dargestellt, würde bedeuten, dass der Proband besonderes durch Gespräche gut lernt. So würde in diesem Fall die Lerneinheit nach auditiven Lernmethoden angepasst werden.

Fragebogen für den Pretest

Wie schon im Untersuchungsdesign in Kapitel 2.1 erwähnt, misst der Pretest den aktuellen Wissensstand und das generelle Bewusstsein für die Thematik der Privatsphäre. Der vollständige Fragebogen für den Pretest ist im Anhang B.1 zu finden. Die einzelnen Fragestellungen wurden zum Teil von einer bestehenden Studie „Portable Privacy“ [11] abgeleitet, aber auch in Eigenkreation verfasst. Dabei wurden Fragen zu folgenden Sektionen gestellt:

- Demographie
- Bildung und Beschäftigung
- Privatsphäre

[2] http://www.philognosie.net/index.php/tests/testsview/150/, Petra Sütterlin, 2004

- Internetnutzung
- Soziale Medien
- Suchdienste
- Webdienste und -plattformen
- Vertrauen gegenüber IT-Unternehmen
- Vorratsdatenspeicherung

In den ersten beiden Sektionen des Pretests „Demographie“ und „Bildung und Beschäftigung“ werden jeweils Daten abgefragt, nach welchen später in der Analyse kategorisiert wird. Konkret werden Alter, Geschlecht, berufliche Tätigkeit und Bildung erhoben, um so etwaige Trends herauszufinden.

In der Sektion „Privatsphäre“ wird der Proband gefragt, wie wichtig ihm die Privatsphäre im Internet sei. Dabei wird die Testperson mit einigen Begriffen konfrontiert und gefragt, ob sie sich darunter etwas vorstellen kann. Mit Fragen, aus welchen Bestandteilen sich in der Regel der Benutzername zusammensetzt oder in wessen Verantwortungsbereich dieses Thema gesehen wird, wird der Umgang mit persönlichen Daten dokumentiert. Ferner wird gefragt, ob sich der Proband vorstellen kann, dass die im Internet preisgegebenen Informationen für Verbrechensbekämpfung oder Versicherungsprofile verwendet werden könnten. Hintergrund dieser Fragestellung ist, herauszufinden, ob sich der Betroffene schon einmal Gedanken gemacht hat, welche potentiellen Konsequenzen daraus folgen, wenn persönliche Daten ins Internet gestellt werden.

Abbildung 2.1: Ergebnis eines Lerntypentests nach Sütterlin

In der nächsten Sektion „Internetnutzung“ wird das Surfverhalten unter die Lupe genommen. Mit den Fragen, wo die Testperson ihre Internetverbindungen aufbaut und ob sie im Besitz eines Smartphones oder Tablets sei, werden Rückschlüsse auf potenzielle Gefahren beim Internetsurfen gezogen. Um später auf die Profilerstellung eines Internet Users hinzuweisen, wird auch nach regelmäßig genutzten Internetplattformen gefragt, welche auch quantitativ eingeschätzt werden sollten. So sollte die Testperson zählen, bei wie vielen Internetdiensten bereits vorhandene Benutzerkonten bestehen, aus denen potentiell ein Profil erstellt werden kann. Dabei wird eine Liste aus diversen Kategorien an Internetplattformen zur Verfügung gestellt, um so der Testperson eine Hilfestellung zu bieten.

In „Soziale Medien“ wird nach der Anzahl aktiv genutzter Dienste und nach dabei preisgegebenen Informationen gefragt. Diese beiden Fragestellungen erlauben einen kleinen Einblick, auf wie vielen Plattformen persönliche Informationen öffentlich gemacht werden. Auch nach regelmäßig genutzten „Suchdiensten“ wird nachgefragt, welche ebenfalls persönliche Informationen in Form von Suchbegriffen verarbeiten und analysieren könnten. Mit der Frage, ob es der Testperson etwas ausmachen würde, gestellte Suchbegriffe ihrem Umfeld (Arbeitgebern, Eltern,...) weiterzugeben, wird festgestellt, wie sensibel der Proband mit Suchanfragen umgeht.

Im Unterkapitel „Dienste und Plattformen“ wird erforscht, wie häufig die Testperson aktiv oder passiv verschiedene Internetdiensten nutzt. Auch diese Frage hat zum Ziel, festzustellen, wie viele persönliche Informationen veröffentlicht werden, aus denen Profile erstellt werden könnten.

In der Sektion „Vertrauen gegenüber Unternehmen“ wird versucht, das generelle Vertrauen gegenüber Internet und deren Akteuren zu messen. Mit der gezielten Frage, wie die Testperson einzelne Firmen im Umgang mit persönlichen Daten einschätzen würde, wird das in sie gesetzte Vertrauen analysiert. Der Vergleich von Smartphone-Hersteller (Apple), Online-Shops (Amazon, Zalando), Suchmaschinen (Google) und Telekommunikationsanbieter (A1, T-Mobile) bildet in dieser Fragestellung ein interessantes Detail. Ferner wird die Übermittlung von persönlichen Daten wie Kreditkartennummer oder persönliche Adresse infrage gestellt und ermittelt, ob die Testperson diese im Internet bedenkenlos versenden würde.

Als letzter Punkt wird der Informationstand nach der in Österreich eingeführten Vorratsdatenspeicherung (VDS) erhoben. Dabei wird die Testperson gefragt, ob diese Regelung relevante Auswirkung auf das Surfverhalten hat und ob sie wisse, wie sie umgangen werden könnte – Stichwort anonym surfen oder telefonieren.

Fragebogen für den Posttest

Wie schon in Kapitel 2.1) erklärt, ist die Hauptintension des Posttests einerseits die Messung des Lernerfolgs der Lerneinheit und andererseits die Feststellung, ob sich das Bewusstsein und Interesse für das Thema Datenschutz verändert hat. Alle Fragen des Posttests sind im Anhang B.2 aufgelistet.

In der ersten Sektion des Posttests „Fragen zur Lerneinheit selbst“ wird evaluiert, wie der Proband die Lerneinheit wahrgenommen hat. Damit soll geklärt werden, ob sich die Testperson mit der Methodik des Vortrags wohl gefühlt hat, oder ob etwas gefehlt hat. Weiters wird gefragt, wie der persönliche Lernzuwachs einzuschätzen ist. Hintergrund dieser Frage ist, ob der richtige Level im Sinne von Über- oder Unterforderung des Lernenden getroffen wurde.

Ob sich der Proband von der Theorie der Lerneinheit etwas gemerkt hat, wird in der folgenden Sektion „Wissen über theoretischen Background“ abgefragt. Dabei wird nach potentiellen Informationssammlern und Begriffsdefinitionen nachgefragt. Kann der Proband diese Fragen beantworten, ist sichergestellt, dass er von der Theorie wichtige Punkte nachhaltig verstanden hat.

Beim Unterkapitel „Bewusstsein für möglich Gefahren, Risiken und Themen wie Vorratsdatenspeicherung“ werden kleine Details abgefragt, die während der Lerneinheit erwähnt wurden. Stichprobenartig wird ermittelt, ob sich der Proband wichtige Dinge durch logisches Verständnis gemerkt hat.

Bei der letzten Sektion „Verständnis für Lösungsansätze“ wird das Verständnis der praktischen Teile abgeprüft. Ob der Proband in der Lage ist, die eigene virtuelle Identität festzustellen oder eine Anonymisierungssoftware zu bedienen, ist wesentlicher Bestandteil dieser Abfragesektion. Dabei wird der Proband angeleitet, bestimmte Schritte zu tätigen und dabei Zwischenergebnisse zu dokumentieren.

Langzeitevaluierung

Etwa 2-3 Monaten nach der Durchführung der Lerneinheit werden die Probanden noch einmal für eine Langzeitevaluierung befragt. Damit wird festgestellt, ob sich die Probanden vom Vortrag etwas gemerkt haben und ob sich das Bewusstsein für Privatsphäre im Internet langfristig geändert hat. Der Fragebogen, welcher im Anhang B.3 aufgelistet ist, umfasst Fragestellung, wobei einerseits gezielt nach konkreten Veränderungen des Surfverhaltens nachgefragt wird, andererseits wird geprüft, ob sich der Proband Tatsachen und vorgestellte Begriffe gemerkt hat. Nachdem es sich bei dieser Befragung nur um eine überschaubare Anzahl an Fragestellungen handelt, werden die Antworten in einem kurzen Telefonat ermittelt.

Zu Beginn wird der Proband befragt, ob er sich an die Lerneinheit grundsätzlich erinnern kann und ob er in Situationen gekommen sei, in der er an die vorgetragenen Lerninhalte gedacht hat. Ferner wird erhoben, ob sich der Teilnehmer mit anderen Personen über die Problematik der Privatsphären unterhalten hat und worum es sich dabei konkret gehandelt hat. Dabei wird der Proband unter anderem auch nach Begriffen befragt, die ihm bei der Lerneinheit vorgetragen wurden. Vorrangig gilt es zu ermitteln, ob er das erhaltene Wissen langfristig anwenden konnte und eventuell weitergeben konnte.

In weiterer Folge wird gefragt, ob der Proband nach dem Vortrag jemals in Situationen gekommen sei, in der er sich anonym im Internet bewegen wollte. Wurden jemals die Privatsphäre-Einstellungen von Facebook verändert oder wurde jemals bewusst nachgedacht, welche persönlichen Informationen im Internet preisgegeben werden? Welches Vertrauen gewährt der Proband Firmen wie Microsoft, Apple oder Google im Umgang mit persönlichen Daten speziell nach den Bildungsmaßnahmen? Wurden beim Surfverhalten Veränderungen wahrgenommen? Wesentliches Ziel dieses Fragenblocks ist es zu eruieren, ob sich der Proband Gedanken über Anonymität und Privatsphäre im Internet gemacht hat und welche konkreten Auswirkungen durch die Lerneinheit erreicht wurden.

Abschließend werden Fragen zur Vorratsdatenspeicherung gestellt und ermittelt, ob der Proband jemals wieder etwas von dieser Regelung gehört hat. Speziell bei diesem Thema wird bei der Langzeitevaluierung analysiert, ob sich die Probanden jemals wieder Gedanken darüber ge-

macht haben, oder ob dieses Thema bei ihm einfach durch mangelnde Medienpräsenz stark in den Hintergrund geraten sei.

2.4 Durchführung der Studie

Wie in Kapitel 2.2 beschrieben, wurde ein Liste von ca. 50 Personen angefertigt, die potentiell die ECDL-Mindestkriterien erfüllen. Die meisten haben bei der ersten Anfrage, ob sie an der Untersuchung teilnehmen würden, positiv reagiert und Interesse für die Thematik gezeigt. Man kann daraus den Schluss ziehen, dass sich das Interesse an Privatsphäre im Internet durch die Medienpräsenz der NSA-Skandale verstärkt wurde. Auch Personen, die sich weniger mit dem Internet beschäftigen, zeigten grundsätzlich Interesse, wenn auch der Vortrag letztendlich oft eine Überforderung war.

Mit den Personen, die ihre Teilnahme an der Untersuchung grundsätzlich zugesagt haben, wurde versucht, einen Termin zu finden. Auch eine entsprechende Örtlichkeit wurde arrangiert, um eine möglichst ruhige Umgebung zu gewährleisten. Praktisch ergab es sich jedoch häufig so, dass sich in Kaffehäusern oder Bibliotheken getroffen wurde. Mit manchen Probanden wurde die Untersuchung in einer privaten Wohnung durchgeführt, was für angenehme und ruhige Atmosphäre sorgte.

Die Erfahrung zeigte bald, dass sich entgegen der Planung oft nur Termine nach der Arbeit und eben nicht am Wochenende finden ließen. Wenn es sich zeitmäßig nicht ausging, wurde die komplette Untersuchung so aufgeteilt, dass der Pretest und der Lerntypentest schon an einem früheren Zeitpunkt ausgefüllt wurde. Somit konnte die Zeit ausschließlich für die Vermittlung der Inhalte verwendet werden, wobei eine höhere Konzentrationsfähigkeit bei der Testperson erreicht werden konnte.

War der Vortrag einmal gestartet, zeigten sich alle Probanden sehr interessiert und es kam oft zu viele Rückfragen, welche die Untersuchung länger machten. Somit konnten die angestrebten Zeiten, die bei der Planung des didaktischen Modells (Kapitel 3.1) anberaumt wurden, nur selten erreicht werden. Trotzdem wurde versucht, den kompletten Lernstoff durchzubringen. Die daraus entstehende Dauer der durchgeführten Einheiten wird im Rahmen der Analyse präsentiert.

Nach Beendigung des offiziellen Teils der Untersuchung mit dem Posttest ergab sich oft eine weiterführende Diskussion, wo sich die Testpersonen über eigene Anwendungsfälle informierten. Oft ging es dabei, wie viel Informationen preisgegeben werden sollten und welche potentiellen Auswirkungen sich ergeben, wenn mehr Daten als oft nötig angegeben wird. Aus diesen Diskussionen lässt sich durchwegs die Erkenntnis gewinnen, dass dieses Thema oft nicht greifbar für den Einzelnen ist. Es ist für den Einzelnen schwierig, mögliche Konsequenzen der eigenen Internetaktivitäten abzuschätzen.

Ferner kam auch oft das Thema, wie Kindern ein „guter Umgang"‘ mit Facebook beigebracht wird. Dabei wurde jeweils auf die möglichen Gefahren einer im Facebook dokumentierten Lebensgeschichte hingewiesen. In der ersten Linie wurde dabei Sensibilität erweckt, dass etwa zukünftige Arbeitgeber, Versicherungen und Behörden wie Polizei höchstwahrscheinlich auf solche Informationen zurückgreifen werden, falls sie Erhebungen über eine Person vornehmen müssen. Spätestens bei diesem Beispiel wurden die Untersuchungsteilnehmer hellhörig und es entstand das erste Bewusstsein für Privatsphäre im Internet.

2.5 Auswertungsstrategie

Wie schon in Kapitel 2.1 beschrieben, werden während einer Untersuchungseinheit mit einem Probanden mehrere Tests durchgeführt. Die Zielsetzung dieser Tests sind oft verschieden und werden daher auch unterschiedlich bewertet. Der Lerntypentest ist ein Online-Test, welcher in Kapitel 2.3 ausführlich beschrieben wurde. Nachdem alle Fragen vom Probanden beantwortet worden sind, werden diese durch das Drücken eines Buttons ausgewertet und das Resultat direkt auf einer weiterführenden Webseite angezeigt. Wie diese Ergebnis zu deuten ist, wird in Kapitel 2.3 diskutiert.

Der Pretest wird dem Probanden als Fragebogen in Papierform vorgelegt. Dessen Ergebnisse werden in ein Excel-Sheet übertragen und ausgewertet. Dabei wird jede Frage zeilenweise angeführt, in jeder Spalte werden die Ergebnisse pro Testperson eingetragen. Für JA-NEIN Antworten wird 0 oder 1 eingetragen, um so die Frage über alle Ergebnisse aufzusummieren und auszuwerten. Bei Fragen, wo es Antworten in 4 Kategorien gibt (zum Beispiel: „Stimme zu“, „Stimme eher zu“, „Stimme eher nicht zu“, „Stimme nicht zu“, „Keine Ahnung“), wird ein Zahl zwischen 1 und 4 zugeteilt, für „Keine Ahnung“ wird 0 vergeben. Auch Antworten von offenen Fragestellungen werden zusammengefasst ins Excel-Sheet eingetragen. Diese werden eine Hilfestellung für mögliche Antworten sein, die bei der Analyse der Ergebnisse miteinbezogen werden. Die meisten Fragen werden quantitativ ausgewertet. Zusätzlich wird bei einer Stichprobe von ca. 30 Personen im Rahmen dieser Untersuchung auch ein Schwerpunkt auf qualitative Kriterien gelegt. Speziell die offenen Frage geben hier die Möglichkeit, wie genau und mit welchen begleiteten Gedanken der Proband die Frage beantwortet hat. Die Messungen des Posttests und der Langzeitevaluierung werden im gleichen Modus ausgewertet. Die Antworten werden in ein Excel-Sheet übertragen und dort evaluiert.

KAPITEL 3

Inhalt und Aufbau des lerntypenabhängigen, didaktischen Modell

In diesem Kapitel wird ein didaktisches Modell vorgestellt, welches als Bildungsmaßnahme im Rahmen der „Ein-Gruppen-Pretest-Posttest“-Untersuchung (Kapitel 2) verwendet wird. Ziel dieser Lerneinheit ist es, dem Probanden einen tieferen Einblick in unterschiedliche Fragestellungen des Datenschutzes im Internet zu gewähren. Prinzipiell sollte auf bisherigen Erfahrungen der Testperson aufgebaut werden, um so ein stärkeres Bewusstsein für diese Thematik zu fördern. Wichtige themenspezifische Begriffe werden erläutert, um so eine Basis für potentielle Diskussionen und bewussteres Internetsurfen zu legen. Ferner sollte die Testperson danach in der Lage sein, technische bzw. organisatorische Lösungsansätze anzuwenden.

Zusätzlich zur Lerneinheit wird bei deren Durchführung auf den jeweiligen Lerntyp geachtet. Je nach Auswertung des Lerntypentests wird für den Probanden eine optimale Methodik des Vortrags angewandt. Zudem werden in diesem Kapitel verschiedene didaktische Modelle formuliert, welche nach auditiven, kommunikativen, visuellen oder motorischen Kriterien entsprechend angepasst wurden.

Die folgenden Kapitel beschreiben zuerst den inhaltlichen und zeitlichen Ablauf der Lernsession, um im Anschluss die vier angepassten Lerneinheiten im Detail vorzustellen.

3.1 Inhalte der Lerneinheit

Dieses Unterkapitel präsentiert das didaktische Modell, welches als Grundlage für die Bildungsmaßnahmen der Untersuchung dient. Wie in Tabelle 3.1 aufgelistet, werden dabei für jeden Abschnitt der Inhalt, das vorgesehene Lernziel und die geplante Durchführungszeit beschrieben.

Tabelle 3.1: Didaktisches Modell, Lernziel und geplante Zeitaufteilung

Inhalt	Didaktik	Lernziel	Zeit
Einführung	Vorstellung der Lerneinheit • Vorstellung der empirischen Untersuchung • Hinweis auf persönlichen Nutzen des Problanden • Ziel: Angst nehmen - Bewusstsein schaffen	Der Proband besitzt einen guten Überblick der gesamten Untesuchung und weiß um seinen persönlichen Nutzen und Lernziele Bescheid	5min
Identität, Privacy, Anonymität	Definition und theoretische Erläuterung: • Zitat von Kardinal Richelieu • Hauptakteure beim Internetsurfen • Begriff: Privatsphäre im Internet • Begriff: virtuelle vs. reale Identität • Begriff: „Anonymität“	Verständnis für die vorgestellten Begriffe und Gegebenheiten beim Internetsurfen	10min
User Tracking Methoden	Vorstellung der Themenkomplexe: • Vorratsdatenspeicherung (VDS), inkl. öster. Rechtslage • „Browser Tracking“	Verständnis für die Themenbereiche und deren mögliche Auswirkungen beim täglichen Surfen	10min
weitere Gefahren & Risiken	Vermittlung weiterer Problemfelder: • Methoden zur Analyse von Konsum - und Surfverhalten; Netzwerkanalyse • Search Term Analyse • Tracking Web Interaktionen; Firefox-Plugin „Lightbeam“ • Social Engineering	Proband versteht die Themenkomplexe; Bewusstseinsschaffung für eigenes Verhalten beim Surfen	10min
tech. und org. Lösungsansätze	Vorstellung von Lösungsansätzen • Feststellung der eigenen Identität im Netz • Gründe zur Verschleierung der eigenen Identität • Techn. Tools zur Verschleierung • Firefox-Plugins für „Anti-Tracking-Mode“ • „sichere Google-Abfragen“	Kennenlernen von Anonymisierungstechniken und deren praktischen Umgang	20min
Abschluss	Abschluß der Lerneinheit • Rückfragen klären • Besprechnung von Fallbeispielen des Probanden	alle Unklarheiten beseitigt; Bewusstsein für Privatsphäre geschaffen	5min
Gesamtdauer			60min

Einführung

Die Lerneinheit wird mit einem kurzen Einführungsteil gestartet, der nicht länger als 5 Minuten in Anspruch nehmen soll. Dabei wird in groben Zügen eine Übersicht über die Lerneinheit gegeben und der konkrete Ablauf der empirischen Untersuchung vorgestellt. Zudem werden erste Begriffe erläutert und auf den persönlichen Nutzen hingewiesen, den der Proband aus der Lerneinheit zieht. Ziel diese Abschnitts ist es, dass die Testperson nach diesem Einführungsabschnitt einen guten Überblick über die Untersuchung gewinnt und weiß, welche Erkenntnisse gewonnen werden. Ungeachtet der angewandten Methodik ist die Motivation und Begeisterung für diese Lerneinheit ein zentraler Aspekt. Abschließend werden grundlegende Ziele der Session ausgegeben. Generell sollten etwaige Bedenken und Unsicherheiten bezüglich Privatsphäre im Internet durch gezielte Aufklärung ausgeräumt werden. Zudem sollte ein starkes Bewusstsein für die gesamte Thematik entwickelt werden, um so die Teilnehmer der Studie vor potentiellen Gefahren und Risiken der Internetnutzung zu schützen.

Begriffe Internet Privacy, Identität, Anonymität

Im nächsten Schritt der Lerneinheit wird die theoretische Basis für die Thematik gelegt, wofür rund 10 Minuten eingeplant sind. Dem Probanden sollten grundsätzlichen Begriffe wie Internet Privacy, reale oder virtuelle Identitäten und Anonymität im Internet so vermittelt werden, dass er diese selbst erklären könnte. Mit einem Zitat von Armand-Jean I. du Plessis de Richelieu [12] (auch genannt als Kardinal Richelieu 1585-1642: *„Man gebe mir sechs Zeilen, geschrieben vom redlichsten Menschen, und ich werde darin etwas finden, um ihn aufhängen zu lassen.“*) sollte anfänglich die Informationsgesellschaft von früher im Gegensatz zu heute verglichen werden. Früher reichten vermutlich ein paar Gerüchte, um einen Menschen zu kompromittieren oder ihm etwas anzulasten. Die Gegenwart bietet in der virtuellen Welt viel weitreichendere Möglichkeiten. Mit kurzen Anfragen bei Google oder Facebook können beispielsweise viele Informationen über eine Person herausgefunden werden. Gerade deswegen sollte mit der Offenlegung persönlicher Daten auf diversen Medien (eigene Homepage, soziale Medien) Vorsicht geboten sein.

Um technisch einen schnellen Überblick zu geben, werden die Hauptakteure beim üblichen Internetsurfen vorgestellt. Wie auf Folie „Akteure beim Surfen“ A.2 abgebildet, werden dabei alle betroffenen Knotenpunkte (wie PC/Smartphone, Internet Service Provider (ISP) und Ziel-Webserver) vereinfacht dargestellt. In diesem Zusammenhang werden die beiden DOS-Befehle „ipconfig“[1] und „tracert“[2] erwähnt, die dabei helfen, Informationen wie die aktuelle IP-Adresse oder die unzähligen Knotenpunkte selbst aus dem Netzwerk zu ermitteln. Es wird darauf hingewiesen, dass grundsätzlich bei jeder Instanz die Möglichkeit besteht, jemanden beim Surfen zu beobachten und die angesteuerten Webseiten auf Vorrat mitzuspeichern. Daraus könnte ein Profil erstellt werden, welches eindeutig zu einem User zuordenbar ist.

Um die generelle Problemstellung und deren Zusammenhänge weitreichender und besser zu verstehen, werden an dieser Stelle mehrere Begriffe erläutert:

[1] http://de.wikipedia.org/wiki/Ipconfig, Jänner 2014
[2] http://de.wikipedia.org/wiki/Traceroute, Jänner 2014

Privatsphäre im Internet Um diesen Begriff zu beschreiben, wurde eine Definition herangezogen, welche aus dem PRIME-Tutorium [13] zitiert wurde: *„Allgemein ist Privatheit das Recht einer Person in jedem Kontext für sich selbst entscheiden zu können, wann und unter welchen Bedingungen personenbezogene Daten herausgegeben und von anderen Personen verwendet werden können. In diesem Zusammenhang ist die Privatheit eng mit der Freiheit einer Person verbunden, sich private Freiräume zu schaffen - frei von Einflüssen und Störungen anderer.“* Auch die Firma Bitkom versucht mit ihrem Online-Tutorium[3] diesen Begriff des Online-Datenschutzes mit Videos aufzuarbeiten. In einem Einleitungsvideo[4] wird die Wichtigkeit des Datenschutzes hervorgehoben. Unter anderem wird darauf hingewiesen, wo Datenspuren anfallen, welche dann durch deren gezielte Sammlung gegen Internet User verwendet werden könnten. Als weitere Grundlage wird ein Video[5] gezeigt, welches den Begriff der „Informationellen Selbstbestimmung“ behandelt, wobei jede Person ein Bestimmungsrecht besitzt, was mit ihren Daten passiert. Dabei bilden zum Beispiel Behörden eine Ausnahme, die zur Erfüllung ihrer gesetzlichen Aufgaben persönliche Daten von Internet Usern verwenden dürfen. Deshalb sollte ein verantwortungsvoller Umgang mit persönlichen Daten sichergestellt werden, um so möglichen Konsequenzen nicht nur in unmittelbarer Zukunft, sondern auch in Ausblick auf spätere Jahre entgegenzustehen.

Virtuelle vs. reale Identität Jeder Mensch hat in der realen Welt eine Identität, die im Wesentlichen aus einer Menge von Attributen besteht. Die Zusammenfassung aller Eigenschaften wie das Erscheinungsbild, Größe, charakteristische Merkmale, Sprechweise, usw. zeichnet einen Menschen als Individuum aus und macht ihn zugleich unterscheidbar von anderen Menschen. Ist von einem Menschen nur eine kleine Menge von Attributen bekannt, wie in Abbildung der Folie „Begriffe“ A.2 hellblau angedeutet, wird auch von einer Teilidentität gesprochen. Demnach kennen Dritte, wie Behörden, diverse Organisation (Arzt, Firmen,...) oder andere Personen, immer nur eine Teilidentität eines Individuums, aber niemals die vollständige Identität (ganzer dunkelblauer Kreis auf Folie „Begriffe“ A.2). Dieses Konzept der (Teil)-Identitäten kann auch auf die virtuelle Welt transformiert werden. Dabei wird eine Identität viel mehr über digitale Daten definiert, wie zum Beispiel IP-Adresse oder Profil-Daten bei diversen Webdiensten. Vor allem bei den sozialen Netzwerken wie Facebook, Twitter oder LinkedIn kann jeder User selbst bestimmen, wie viele persönliche Details ins Web gestellt werden. Je mehr private Informationen ins Netz gelangen, desto besser ist seine Identität im Web beschrieben. Aussagekräftiges Beispiel in diesem Bereich ist die kundenangepasste Werbung, wo jeder User Werbung für Artikel eingeblendet bekommt, für die er sich auf diversen Webseiten einmal interessiert zeigte. In diesem Zusammenhang ist der Begriff der „Verkettbarkeit“ zu erwähnen, wo versucht wird, virtuelle Teilidentitäten zu verbinden, um noch mehr Eigenschaften eines Einzelnen (Userprofile) zu generieren. Wenn beispielsweise ein Nutzer alle Google Services verwendet, könnte dieser Betreiber diese Accounts in Zusammenhang stellen, um so eine umfassendere Identität zu bekommen. Theoretisch könnte Google eine Wissensbasis über

[3] http://www.bitkom-datenschutz.de, Dezember 2013
[4] http://www.bitkom-datenschutz.de/44004.htm, Dezember 2013
[5] http://www.bitkom-datenschutz.de/44006.htm, Dezember 2013

einen User aufbauen, welche gespeichert hat, wofür sich ein User interessiert (Google Search), wo er wohnt bzw. welche Destinationen er anzielt (Google Maps) und welche sozialen Kontakte er pflegt (Google+, Gmail). Deshalb ist ein Nutzer immer gut beraten, diese Internetdienste von möglichst mehr als einem Anbieter zu beziehen[13].

Anonymität im Internet Bei unverschlüsseltem Internetverkehr und ohne Verschleierung der virtuellen Nutzerinformationen (IP-Adresse, Browserinformationen,...) wäre es theoretisch leicht möglich, dass der Internetverkehr eines Users beobachtet und analysiert wird. Mit diesen Daten könnte ein komplettes Kommunikations- und Personenprofil erstellt werden, welches dann unter Umständen gegen den User verwendet werden kann [14]. Um zu einer Anonymität im Internet zu gelangen, muss im Wesentlichem die eigene Identität verschleiert werden, indem sich eine andere Identität angeeignet wird. Somit sollte es möglich sein, gegenüber einem Webdienst oder Server anonym in Form einer anderen Identität aufzutreten [15]. Die technische Möglichkeiten werden in Unterkapitel 3.1 vorgestellt, wobei diverse Software-Werkzeuge und Lösungsansätze vorgestellt werden.

User Tracking Methoden

In dieser Sektion werden zwei gängige Methoden der Userverfolgung vorgestellt, wofür in der Lerneinheit 10 Minuten eingeplant werden. Lernziel für diesen Teil der Lerneinheit ist, dem Probanden diese beiden Themenbereiche verständlich zu erklären und mit ihm über die konkreten Auswirkungen im realen Leben zu sprechen:

Vorratsdatenspeicherung (VDS) Österreich führte die VDS mit 1.April 2012 gesetzlich ein und setzte damit die EU-Richtlinie 2006/24/EG [16] um. Im Detail wird darunter die Aufzeichnung oder Speicherung von personenbezogenen Telekommunikationsdaten durch und für öffentlichen Stellen verstanden. Diese werden auf Vorrat mindestens 6 Monate gespeichert und können nur dann abgerufen werden, sollten sie von einer Behörde durch richterlichen Beschluss oder bei Gefahr im Verzug benötigt werden. Diese Regelung zwingt die Anbieter von Internet-Zugangsdiensten, öffentlichen Telefondiensten und E-Maildiensten jegliche Verkehrsdaten (jedoch keine Inhalte) von allen Kommunikationsteilnehmer mitzuspeichern [17]. Ein YouTube-Video der Lernplattform Sempervideo[6] versucht das Grundprinzip der Vorratsspeicherung zu erklären. Dabei wird die Thematik visuell aufbereitet und gezeigt, welche Server zu welchem Zeitpunkt welche Daten zu speichern haben. Darüber hinaus wird gezeigt, wie dieser Mechanismus leicht umgangen werden kann. Für die beispielhafte Visualisierung solcher Daten hat der Grünenpolitiker Malte Spitz seine persönlichen Vorratsdaten von der Telekom eingeklagt und der ZEIT ONLINE[7] zur Verfügung gestellt. Dessen gespeicherten Geo-Daten werden mit allen öffentlich verfügbaren Daten (zum Beispiel Tweets) verknüpft und auf einer Karte dargestellt. Mit einem Geschwindigkeitsregler kann zu jedem Zeitpunkt jegliche Telekommunikation (Telefongespräche, SMS,...) oder örtliche Standpunkte von Spitz visuell beobachtet werden.

[6] http://www.youtube.com/watch?v=1maZNx_ElKQ, Dezember 2013
[7] http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten, Dezember 2013

Browser Tracking Ein Browser fügt bei jeder Serveranfrage mehrere Informationen (HTTP-Parameter, Metainformationen über Browser-Plug-Ins, usw.) bei, um eine Webserver zu fragen, wie dessen Webseite optimal darzustellen ist. Im Internet kursieren viele Tools[8], die diese Informationen anzeigen. Genau diese Metadaten können aber auch dazu benutzt werden, um einen bestimmten Browser wiederzuerkennen - und das ohne den Einsatz von Cookies. Ferner können über diesen Fingerabdruck der Metadaten bestimmte Internet User wiedererkannt werden, um so zum Beispiel herauszufinden, welche Interessen ein User primär verfolgt oder wie sein Surfverhalten ist. Verschiedene wissenschaftliche Arbeiten [18] und Projekte weisen auf dieses Problem hin. Allen voran zeigt das Forschungsprojekt „Panopticlick“[9,10] auf, welche Informationen bei derzeitiger Browserkonfiguration preisgegeben werden. Zusätzlich wird errechnet, unter wie vielen unterschiedlichen Browsern ein Nutzer theoretisch wiedererkennbar ist.

Weitere Gefahren und Risiken

In diesem Teil der Lerneinheit wird auf weitere Gefahren und Risiken aufmerksam gemacht, unter denen ein Internet User beim üblichen Surfen potentiell ausgesetzt ist. Wie schon in den vorigen Kapiteln geht es meist darum, noch mehr Informationen über den Kunden oder Internet User herauszufinden. Es werden dabei weitere 10 Minuten des Vortrags eingeplant, um Verständnis für diese Problemstellungen bei der Testperson zu generieren:

Kundenverhalten, Surfverhalten, Netzwerkanalyse In diesem Block werden gängige Praktiken vorgestellt, die im virtuellen Netz, aber auch in der realen Welt gängige Praxis sind. In beiden Welten gilt es als entscheidender Erfolgsfaktor, über das Kaufverhalten der eigenen Kundschaft Bescheid zu wissen. Im Handel (Lebensmittelgeschäfte, Baumärkte,...) werden oft Kundenkarten angeboten, über die bestimmte Rabatte und Gutschriften vergeben werden. Was für den Kunden als Vorteil erscheint, könnte auch als Abkaufen des Kundenverhaltens gewertet werden. Ist das Konsumverhalten eines Kunden bekannt, werden ihm ähnliche oder komplementäre Produkte angeboten, um so eine wesentliche Umsatzsteigerung zu erreichen. Auch das Surfverhalten der User einer Webseite könnte von Interesse des Betreibers sein. Interessiert sich ein Kunde für eine Reihe gewisser Artikel, können genau diese auf der Startseite oder auf anderen Internetportalen beworben werden (siehe Amazon-Werbung). Ferner könnte für einen Provider das soziale Netzwerk eines Kunden von Interesse sein. Denn auch virtuelle „Freunde“ könnten sich für diese Artikel interessieren.

Search Term Analyse Bei dieser Art von Analyse wird versucht, von einer Menge von Suchtermen auf einen bestimmten Internet User zu schließen. Diese besondere Assoziation ist eher zufällig sichtbar geworden, als von einer bereits abgesetzten Suchmaschine alle Suchterme für wissenschaftliche Zwecke zur Verfügung[11] gestellt wurden. Wissenschaftler forschten aus diesen Daten Personen aus, welche genau diese Suchanfragen an diese

[8] http://browserspy.dk, Jänner 2014
[9] https://panopticlick.eff.org, Jänner 2014
[10] http://www.sempervideo.de/?p=9692, Jänner 2014
[11] http://www.aolstalker.com/, Jänner 2014

Suchmaschine gestellt hatten. [19] Derzeit bietet Google History[12] die Möglichkeit, sich zu registrieren, um die an Google gestellten Suchanfragen zu visualisieren.

Tracking Web Interaktionen Im Laufe der Zeit haben sich auf vielen Webseiten diverse Werbebanner als fester Bestandteil etabliert. Diese werden meist von professionellen Firmen geschalten, die sich als Ziel gesetzt haben, für jeden User die „richtige“ Werbung einzublenden, deren Inhalte relevante oder potentiell interessante Produkte oder Dienstleistungen sind. Wird eine Webseite durch einen Browser angefordert, werden somit diese Werbeinhalte indirekt von andere Quellen aufgerufen. Eine Firefox-Plug-In namens „Lightbeam“[13] (früher „Collusion“)[14] visualisiert diese Zusammenhänge und zeigt die indirekt aufgerufen Instanzen. Bei einem mehrwöchigen Betrieb dieses Plug-Ins wird eindrucksvoll gezeigt, welche Knotenpunkte am meisten aufgerufen werden. Wie sich bei einem Testbetrieb herausstellte, waren Knotenpunkte von derzeitigen Internetgrößen wie Google, Facebook oder Twitter die am meisten aufgerufenen Instanzen.

Social Engineering Bei „Social Engineering“ handelt es sich um die Manipulation von Personen, um das Ziel eines Angreifers zu erreichen[15]. Ein Fallbeispiel wäre, wenn ein Hacker eine Facebook-Profilseite vortäuscht, um mit dieser einen Kontakt mit einer Zielperson herzustellen. Für den Angreifer ist es nun eine leichte Aufgabe, dem irre geführten Facebook-User auf diesem Weg Informationen zu entlocken, die er sonst nicht bekommen könnte. Daher sollte es immer oberstes Gebot sein, genau zu prüfen, mit wem virtuelle Freundschaften eingegangen werden. In diesem Zusammenhang ist auch darauf hinzuweisen, dass gerade Facebook in regelmäßigen Abständen ihre Privatsphäreneinstellungen[16] ändert. Es ist dringend ratsam, diese regelmäßig zu kontrollieren.

Technische und organisatorische Lösungsansätze

Nach den theoretischen Einführungen werden in der Lerneinheit praktische Werkzeuge vorgestellt, die eine Hilfestellung für die Wahrung der Privatsphäre im Internet geben sollten. Für diesen Teil sind in etwa 20 Minuten anberaumt, um dem Probanden die praktische Fertigkeit zu vermitteln sowie auch die Hintergründe der einzelnen Tools zu erklären. Anfangs wird das Feststellen und die Verschleierung der eigenen virtuellen Identität im Internet beleuchtet. Dabei wird im Wesentlichen auf die IP Adresse und die Browserparameter eingegangen. Im Internet befindet sich eine Vielzahl an Webdiensten[17,18], welche die IP-Adresse eines Internet Users anzeigen. Sogenannte ProxyChecker[19] oder ProxyJudges[20,21,22] zeigen nicht nur die IP-Adresse, son-

[12] https://history.google.com/history/, Jänner 2014
[13] http://www.mozilla.org/en-US/lightbeam/
[14] Ted Video: http://www.ted.com/talks/gary_kovacs_tracking_the_trackers.html, Jänner 2014
[15] http://www.social-engineer.org, Jänner 2014
[16] http://mattmckeon.com/facebook-privacy/, Jänner 2014
[17] http://www.myip.is/
[18] http://whatismyipaddress.com/
[19] http://www.proxy-listen.de/Proxy/Proxychecker.html
[20] http://ocl.opoint.com/proxyjudge/prxjdg.cgi
[21] http://www.xav.com/env.pl
[22] http://www.proxy-listen.de/azenv.php

dern auch weitere HTTP-Variablen, die mit den Serveranfragen mitgesendet werden. Gründe für das Verschleiern der virtuellen Identität sind vielfältig. Zum einen ermöglicht es die Benutzung von ausländischen Webdiensten, die nur für Nutzer des jeweiligen Landes gedacht sind. Dabei könnte sich ein User hinter einer virtuellen Identität dieses Landes verstecken, um das Service trotzdem zu nutzen. Andererseits ist ein virtueller Identitätenwechsel ratsam, wenn Internet-Recherchen über eine Thema eingeholt werden, wo nicht einmal der Anschein des Interesses gegenüber enge Bekannte, Arbeitgeber, Behörden, Provider oder der Vorratsdatenspeicherung geweckt werden sollte. Recherchiert ein User mit der eigenen Identität über Krankheiten, Jobwechsel oder politische Ansichten, könnte dies gegen ihn verwendet werden.

Bekannte Werkzeuge für das Verschleiern der eigenen IP Adresse sind Tor[23], VPN-Netzwerke und offene Proxies. Beim Tor-Projekt handelt es sich um ein Netzwerk, welches den HTTP-Verkehr mit dem sogenannten „Onion-Routing“ verschlüsselt. Erfahrungsgemäß müssen jedoch bei dieser Methode Einbußen der Bandbreite hingenommen werden. Dies macht das Surfen im Internet etwas träge. Bei offenen Proxies handelt es sich um Proxy-Server, die bewusst oder unbewusst offen konfiguriert wurden. Ein Nutzer kann sich mit diesen Servern ohne Anmeldung verbinden, um so die Identität des Servers anzunehmen. Das Auffinden eines schnellen, anonymisierten, offenen Proxies und die Schwierigkeit der Konfiguration im Browser macht diese Art der Anonymisierung für den Laien etwas kompliziert. Die dritte Methode stellen VPN-Netzwerke dar, welche grundsätzlich einfach zu installieren sind und schnell beim einfachen Internetsurfen sind. Dabei wird das jeweilige Gerät (PC, Notebook, Smartphone,...) in ein virtuelles Netz angemeldet, um später mit dessen Internetzugang zu Surfen[24]. Es gibt eine Reihe von Providern, die ein VPN kommerziell oder als freies Service anbieten. Beispielweise drosselt der VPN Provider CyberGhost[25] beim Gratis-Betrieb die Bandbreite, welche aber für das einfache Surfen reichen sollte (Stand Jänner 2014).

Das Verschleiern der mitgelieferten Browserinformationen ist ein weiterer Faktor, wenn die Anonymität im Netz gewahrt werden sollte. Dabei hilft das Firefox Plug-In namens „Fireglove“, welches die bei einer Serveranfrage beigefügt Browserparameter (siehe Browser Tracking Kapitel 3.1) verändert oder komplett weglässt. Ein Video des Lernportals SemperVideo[26] erklärt die sehr einfache Handhabung dieses Plug-Ins. Wie so oft geht die erreichte Anonymität auf Kosten von Bequemlichkeit. Denn beim Testen mehrerer Webseiten fällt sofort auf, dass manche Seiten schlecht bzw. gar nicht dargestellt werden können. Um das Problem des „Tracking Web Interaction“ entgegenzuwirken, werden auf der Webseite „fixtracking.com“[27] weitere Tools vorgestellt, welche beim Datenschutz im Internet helfen. Allen voran wird das Firefox Plugin "DoNotTrackMe"vorgestellt, welches alle Instanzen blockt, die als Dritte bei einer Webseiten-Anfrage aufgerufen werden. Dabei wird verhindert, dass Firmen, die über Werbung beim Surfen passiv aufgerufen werden, den Internet User in dieser Weise ausspionieren.

Auch gegen die Search Term Analyse kann sich ein Internet User wehren. Gegen diese Gefahr bietet DuckDuckgo.com[28] eine anonymisierte Alternative zu bekannten Suchmaschinen

[23] https://www.torproject.org/

[24] http://www.sempervideo.de/?p=7384

[25] http://cyberghostvpn.com, Jänner 2014

[26] http://www.sempervideo.de/?p=9692, Jänner 2014

[27] http://fixtracking.com, Jänner 2014

[28] https://duckduckgo.com/

wie Google oder Bing an. Dabei wird versprochen, dass Suchbegriffe nicht analysiert werden und keine Profilerstellung von Internet Usern durchgeführt wird. Sollte doch Google benutzt werden, ist es empfehlenswert, sich das Firefox Plugin „GoogleSharing“[29] zu installieren. Alle Google-Anfragen werden anstatt direkt an Google über einen Proxy gesendet, wodurch es für diese Suchmaschine nicht mehr möglich ist, gewisse Suchbegriffe einem User zuzuordnen.

Abschluss

Zum Abschluss der Lerneinheit werden alle Rückfragen beantwortet und Lösungen für mögliche Fallbespiele diskutiert. Beim Probanden sollte nach dieser Lerneinheit ein Bewusstsein für die Thematik geschaffen sein, um dieses für das weitere Internetsurfen anwenden zu können. Mögliche Folgen und Konsequenzen für jede Interaktion im Web sollten nun dem Untersuchungsteilnehmer klar sein.

3.2 Anpassung des didaktischen Modells an verschiedene Lerntypen

Werden die in Tabelle 3.1 vorgesehenen Durchführungszeiten aller Abschnitte zusammengezählt, dauert die gesamte Lerneinheit rund 60 Minuten. Zusammen mit dem Ausfüllen von Pretest, Lerntypentest und Posttest wird der Proband zirka 120 Minuten mit dem Thema Privatsphäre im Internet beschäftigt sein. Jede Rückfrage durch die Testperson und deren tiefer gehende Erklärung verlängert diese planmäßige Dauer des Vortrags. Um die Konzentration des Probanden möglichst hoch zu halten, wird didaktisch auf die Stärken beim Lernen des Probanden acht genommen. Beim Lernen gibt es verschieden Arten, die je nach Lerntyp leichter fallen.[4] Manche Leute können sich einen Lernstoff gut merken, wenn sie ihn lesen, andere merken sich ihn schon bei der Vorlesung. Der visuelle Typ muss mitschreiben und den Lernstoff skizzieren, und wieder andere müssen mit jemanden darüber sprechen. Deshalb gilt die Prämisse für die Lerneinheit, dass der Untersuchungsteilnehmer in relativ kurzer Zeit möglichst viel und effizient lernen soll.

Zur Feststellung des Lerntypen wird im Rahmen dieser Untersuchung (Kapitel 2.3) ein einfacher online Test herangezogen, der zwischen auditiven, visuellen, kommunikativen und motorischen Lerntypen unterscheidet. Dieser Test führt eine prozentuelle Bewertung durch, inwieweit die jeweiligen Stärken eines Lerntypen vorhanden sind. Je höher ein Prozentsatz für einen Typ ist, desto eher wird der Proband beim Lernen durch die typenspezifischen Lernhilfen unterstützt. Es gilt jedoch als bewiesen, dass den Lernerfolg entsprechend gesteigert werden kann, indem Lernhilfen von verschiedenen Lerntypen angewendet werden.[20] Deshalb werden bei der Auswertung und Bestimmung des Lerntypen die beide besten Ergebnisse kombiniert und Lernhilfen von diesen Lerntypen für die Lerneinheit herangezogen.

Die folgenden Unterkapitel erläutern, wie die Inhalte der Lerneinheit von Kapitel 3.1 didaktisch aufbereitet werden. Dabei wird für jeden Lerntyp die angewendete Methodik und der jeweilige Medieneinsatz erläutert.

[29] https://addons.mozilla.org/de/firefox/addon/googlesharing/, Jänner 2014

3.3 Didaktische Modell für den auditiven Lerntypen

Beim auditiven Modell werden die Lehrinhalte vorwiegend als Vortrag unterrichtet. Nachdem der auditive Typ sehr sensibel auf Lärm und diverse Nebengeräusche reagiert, wird besonders für diesen Lerntypus eine eher ruhige Lernumgebung gesucht, um so eine hohe Konzentrationsfähigkeit sicherzustellen. Bei Rückfragen wird gezielt versucht, in einem Gespräch den Sachverhalt zu klären. Weiters soll der Proband immer wieder dazu bewogen werden, die Erklärungen mit seinen eigenen Worten zu wiederholen. Auch so kann er unterstützt werden, um sich den Lernstoff besser zu merken. [4]

Wie in Tabelle 3.2 skizziert, beschreiben die folgenden Sektionen ein didaktische Modell, welches besonders den auditiven Lerntypen unterstützt. Dabei werden jeweils die dafür notwendigen Lernhilfen und deren Medieneinsatz vorgestellt.

Einführung

Zur Einführung werden beim auditiven Lerntyp alle Punkte der Einführungsfolien A.1 mündlich erklärt. Sollte sich bei möglichen Rückfragen ein kurzes Gespräch ergeben, wird dieses bewusst forciert, um das Verständnis und Motivation für diese Thematik zu fördern. Es sollte auch nach persönlichen Berührungspunkten mit dem Thema Datenschutz im Internet nachgefragt werden, um die Betroffenheit der Testperson zu erzeugen.

Begriffe Internet Privacy, Identität, Anonymität

Zu Beginn dieses Teils der Lerneinheit wird Richelieu's Zitat von der Präsentationsfolie „Zitat zum Datenschutz" A.2 vorgelesen und kurz diskutiert, welche Bedeutung dieses Zitat in der Gegenwart haben könnte. Dabei sollte auf die persönlichen Daten hingewiesen werden, die in den sozialen Medien preisgegeben werden oder die über Google über eine Person zu finden sind. Es sollte eine persönliche Betroffenheit des Probanden erreicht werden, indem kurz über die eigene Situation gesprochen wird.

Anhand der Folienabbildung „Akteure beim Surfen" A.2 werden die Akteuren beim Internetsurfen vorgestellt. Zusätzlich wird darauf hingewiesen, dass bei jeder Instanz potenziell eine Profilerstellung des Internet Users möglich ist. Als Fallbeispiel wird skizziert, welche Instanzen bei einem Besuch auf der Amazon-Webseite involviert sind.

Als Nächstes werden mithilfe der Folie „Begriffe" A.2 folgende Begriffe erklärt:

Privatsphäre im Internet Für diese Definition werden die beiden Videos[30,31] des Datenschutz-Portals der Firma Bitkom gezeigt und Rückfragen des Probanden beantwortet.

Virtuelle vs. reale Identität Zuerst wird der Begriff der Identität mündlich erläutert. Danach wird mit der Folienabbildung A.2 gezeigt, wie dieser Begriff sowohl im realen Leben als auch im Internet anwendbar ist. Am Beispiel der Anwendung der gesamten Servicepalette von Google wird die Verknüpfbarkeit der einzelnen Identitäten gezeigt und auf deren Folgen und Konsequenzen hingewiesen.

[30] http://www.bitkom-datenschutz.de/44004.htm, Dezember 2013
[31] http://www.bitkom-datenschutz.de/44006.htm, Dezember 2013

Anonymität im Internet In diesem Zusammenhang wird mündlich erklärt, welche Folgen ein unverschlüsselter Internetverkehr haben kann und wie Anonymität im Internet verstanden werden sollte.

User Tracking Methoden

Dieser Teil wird mit einer kurzen mündlichen Erklärung von User Tracking Methoden eingeleitet. Es werden die Bedeutung sowie die positiven und negativen Effekte von diesen Methoden erläutert, um später 2 Beispiele genauer zu beleuchten:

Vorratsdatenspeicherung (VDS) Für die Erklärung der VDS wird ein SemperVideo[32] vorgespielt, welches die Grundlagen und einiges an Hintergrundwissen vermittelt. Die österreichische Umsetzung wird anhand einer Webseite [17] erklärt, die in einem Browser geöffnet wird und Punkt für Punkt mündlich durchbesprochen wird. Zur praktischen Darstellung der VDS wird zusätzlich noch der ZEIT ONLINE Artikel „Verräterisches Handy“[33] gezeigt, welcher die Visualisierung von Vorratsdaten (Telekommunikationsdaten) zeigt.

Browser Tracking Anhand der Webseite Panopticlick[34] und einem SemperVideo[35] wird die Funktionsweise von Browser Tracking im Detail erklärt. Die bei jeder HTTP-Anfrage automatisch mitgelieferten Browser-Parameter werden anhand der BrowserSpy-Webseite[36] vorgeführt.

Weitere Gefahren und Risiken

In diesem Abschnitt wird gezielt gefragt, warum es besonders im Handel sogenannte Bonuskarten gibt, mit denen ein Kunde Rabatte beim Kauf bestimmter Artikel bekommt. Oder weiters, warum Google diverse Web Services wie Gmail oder eine Suchmaschine gratis anbietet? Dabei soll dem Probanden mündlich vermittelt werden, dass es sich dabei jeweils beim User um einen Verlust der Privatsphäre handelt.

Die Search Term Analyse wird zuerst mündlich grob erklärt. Mit der Geschichte rund um die eingestellten AOL-Suchmaschine[37], deren Folgen [19] und dem Vorstellen von Google History[38] wird der Untersuchungsteilnehmer auch mit praktischen Beispielen konfrontiert. Auch beim Thema „Tracking Web Interaction“ wird zuerst dessen Bedeutung mündlich erörtert. Mit dem Firefox Plug-In „Lightbeam“[39] wird diese Thematik auch praktisch dargestellt.

Beim Thema „Social Engineering“ werden grundsätzliche Punkte verbal erläutert, um später darauf hinzuweisen, dass Vorsicht geboten sei, mit wem in den sozialen Medien kommuniziert

[32] http://www.youtube.com/watch?v=1maZNx_ElKQ, Dezember 2013
[33] http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten, Dezember 2013
[34] https://panopticlick.eff.org/, Jänner 2014
[35] http://www.sempervideo.de/?p=9692, Jänner 2014
[36] http://browserspy.dk, Jänner 2014
[37] http://www.aolstalker.com/
[38] https://history.google.com/history/
[39] http://www.mozilla.org/en-US/lightbeam/

wird. Auch auf die Privatsphäre-Einstellungen der einzelnen Medien (Facebook, LinkedIn, Twitter,...) wird mit einer Webseite[40] aufmerksam gemacht, da sich diese im Laufe der Zeit ändern können.

Technische und organisatorische Lösungsansätze

In diesem Teil der Lerneinheit steht die Vermittlung praktischer Lösungsansätze im Vordergrund. Anfangs gibt es eine verbale Erklärung über die virtuelle Identität eines Internet Users. Dabei werden diverse Tools[41,42] vorgestellt, die bei der Ermittlung der IP-Adresse hilfreich sind. Weiters werden ProxyChecker[43] und ProxyJudges[44,45,46] gezeigt und erklärt, die zusätzlich zur IP-Adresse auch noch andere Parameter anzeigen. Anschließend werden noch Gründe für die Verschleierung der Identität aufgezählt und kurz diskutiert.

Als Nächstes werden praktische Lösungsansätze zur Verschleierung der Identität vorgestellt. TOR[47] und das Prinzip der offenen Proxies werden nur schematisch mündlich erläutert. Auf Nachfrage werden genauere Information über diese Techniken gegeben, wie zum Beispiel die Installation von TOR oder das Finden und Konfigurieren offener Proxies (Proxylisten). Detaillierter werden die Grundlagen von VPN-Netzwerken durch das Vorspielen eines SemperVideos[48] dargestellt. Als Beispiel wird die Software und deren Hintergrund von CyberGhost[49] vorgestellt. Mit dem Probanden wird die Software gestartet und eine Verbindung zu einem ausländischen Server aufgebaut. Durch einen kurzen IP-Check (wie anfangs erklärt) wird gezeigt, ob sich nun der Teilnehmer mit einer fremden Identität im Internet bewegt.

Zur Verschleierung der HTTP-Parameter wird das Firefox-Plug-In „Fireglove“ durch Ausschnitte eines YouTube-Video [50] vorgestellt und praktisch am Browser gezeigt. Im Anschluss wird die Webseite fixtracking.com[51] mit deren Firefox-Plug-In "DoNotTrackMe"mündlich erläutert.

Um sich gegen die Search Term Analyse zu wehren, werden Alternativen zur Suchmaschine Google gezeigt. Als Beispiel wird dabei die Suchmaschine DuckDuckgo.com[52] vorgestellt und deren Vertrauenswürdigkeit erörtert. Für den Fall, das sich die betroffene Person doch von Google nicht trennen will, wird das Firefox-Plug-Ins „GoogleSharing“[53] vorgestellt und deren Funktionalität erklärt.

---

[40] http://mattmckeon.com/facebook-privacy/
[41] http://www.myip.is/
[42] http://whatismyipaddress.com/
[43] http://www.proxy-listen.de/Proxy/Proxychecker.html
[44] http://ocl.opoint.com/proxyjudge/prxjdg.cgi
[45] http://www.xav.com/env.pl
[46] http://www.proxy-listen.de/azenv.php
[47] https://www.torproject.org/
[48] http://www.sempervideo.de/?p=7384
[49] http://cyberghostvpn.com, Jänner 2014
[50] http://www.sempervideo.de/?p=9692, Jänner 2014
[51] http://fixtracking.com, Jänner 2014
[52] https://duckduckgo.com/
[53] https://addons.mozilla.org/de/firefox/addon/googlesharing/

Abschluss

Um einen Abschluss für die Lerneinheit zu finden, wird der Proband gefragt, welche Rückschlüsse er von dieser Thematik zieht und wie es ihm bei der Lerneinheit gegangen sei. Etwaige Rückfragen werden verständlich erklärt. Vielleicht ergeben sich im Laufe der Diskussion auch Fallbeispiele, welche Fragen zum Datenschutz aufwerfen. Diese werden aktiv aufgegriffen und mögliche Lösungsansätze (eventuell mit Hilfe der vorgestellten Tools) besprochen.

3.4 Didaktische Modell für den kommunikativen Lerntypen

Da dem kommunikativen Lerntypen die sprachliche Auseinandersetzung wichtig ist, wird das didaktische Modell eher nach kommunikativen Lernhilfen ausgerichtet. Demnach werden die einzelnen Lehrinhalte zuerst mündlich erklärt, um sie danach in einer kleinen Diskussion zu vertiefen. Somit werden etwaige Unklarheiten sofort geklärt, um das Verständnis beim Probanden bestmöglich zu fördern. Fallweise wird auch ein Frage-Antwort-Spiel angewendet, indem der Lernende noch vor der Erklärung gefragt wird, was er unter dem jeweiligen Begriff verstehen würde. Somit wird das bisherige Wissen abgefragt und später richtig gestellt. [4]

Das didaktische Modell für den kommunikativen Lerntypen von Tabelle 3.3 wird in den folgenden Sektionen im Detail diskutiert.

Einführung

Der Proband wird im Einführungsteil befragt, ob ihm der Begriff „Privatsphäre im Internet“ etwas sagt und ob er damit schon persönlich Erfahrungen gemacht hat. Es wird gezielt der Dialog gesucht und dabei die Punkte auf den Folien A.1 erläutert. Es sollte in dieser Phase der aktuelle Wissenstand des Probanden über diese Thematik festgehalten werden und der potentielle persönliche Nutzen der Lerneinheit in Aussicht gestellt werden.

Begriffe Internet Privacy, Identität, Anonymität

Bei diesem Teil der Lerneinheit wird das Zitat von Kardinal Richelieu auf der Präsentationsfolie „Zitat zum Datenschutz“ A.2 vorgelesen und ein kurzes Gespräch initiiert. Es wird die Frage in den Raum gestellt, wie dieses Zitat in der Gegenwart zu verstehen ist. Dabei wird mündlich auf die persönlichen Daten hingewiesen, die bereits durch die Testperson im Internet bzw. in den sozialen Medien absichtlich oder unabsichtlich offengelegt wurden.

Welche Akteure beim Internetsurfen beteiligt sind, wird kurz mit der Folienabbildung auf der Folie „Akteure beim Surfen“ A.2 diskutiert. Zusätzlich wird mündlich darauf hingewiesen, dass bei jeder Instanz potenziell eine Profilerstellung des Internet Users möglich ist. Beispielsweise wird gezeigt, welche Instanzen bei einem Besuch der Amazon-Webseite beteiligt sind.

Als Nächstes werden alle Begriffe der Folie „Begriffe“ A.2 kurz erläutert:

Privatsphäre im Internet Um diesen Begriff zu erklären, wird die Definition des Datenschutzes nach PRIME (Kapitel 3.1) vorgelesen. Wenn notwendig, wird der Begriff im Dialog vertiefend besprochen.

Tabelle 3.2: Angewandtes didaktisches Modell für den auditiven Lerntypen

Inhalt	Medien	Methodik
Einführung	PPT-Folie „Inhalt“ (A.1)	• Mündliche Erklärung der empirischen Untersuchung (Ablauf, Inhalt, Ziel) • Vortragsmäßige Aufklärung über Inhalt (eventuell anhand der Komik auf der PPT-Folie) • Mündliche Erläuterung über den persönlichen Nutzen des Probanden • nach möglichen früheren Berührungspunkten mit Datenschutz nachfragen; mögliche Diskussion anregen
Identität, Privacy, Anonymität	PPT-Folien „Zitat zum Datenschutz“, „Akteure beim Surfen“, „Begriffe“ (A.2); YouTube-Videos	• Richelieu’s Zitat mündlich erklären und Vergleiche ziehen • Akteure beim Surfen mit Folienabbildung erklären • Privacy(YouTube-Videos), Teil-Identitäten (Folienabbildung), anonym Surfen (mündl. Definition)
User Tracking Methoden	PPT-Folien „User Tracking“ (A.3), YouTube-Videos, Web-Links	• Begriff „User Tracking“ mündlich erklären • VDS: YouTube-Video vorspielen; Web-Links herzeigen und Rückfragen klären; • Browser Tracking mit „Panopticlick“ vorstellen; auf HTTP-Parameter hinweisen
weitere Gefahren & Risiken	PPT-Folie „Weitere Gefahren & Risiken“ (A.4), Firefox-Browser	• Infrage stellen und Diskussion: Warum gibt es Bonuskarten? Surfverhalten? • Mündl. erklären (Beispiel): Search Term Analyse (Google History), Web Interaction (Lightbeam) • Social Engineering mündlich erläutern
tech. und org. Lösungsansätze	PPT-Folie „Lösungsansätze“ (A.5), Firefox Plugins, CyberGhost, YouTube-Videos	• verbale Erklärung: virtuelle Identität (WhatIsMyIP), Gründe für Anonymität • TOR, Open Proxies kurz erklären; CyberGhost (YouTube, Software zeigen) • Vorstellen der Firefox-Plugins „DNTM“„Fireglove“ (YouTube) • DuckDuckGo und Firefox-Plugins „GoogleSharing“ zeigen und mündlich erläutern
Abschluss	PPT-Folie „Conclusio“ (A.5)	• Abschließende Diskussion anregen, Rückfragen beantworten • bei Bedarf Use Case des Probanden diskutieren

Virtuelle vs. reale Identität Mit Folie A.2 wird der Begriff der Identität mündlich erläutert, und zugleich die offline und online Identität der Testperson als Beispiel herangezogen. Im Dialog wird festgestellt, ob der Proband Google Web Services nutzt und welche Möglichkeiten Google im Sinne der Verknüpfbarkeit von Nutzerkonten hat.

Anonymität im Internet Es wird eine kurze Diskussion initiiert, wobei mögliche Folgen von unverschlüsseltem Internetverkehr sowie der Anonymität im Internet besprochen werden.

User Tracking Methoden

Zu Beginn dieses Abschnitts wird die Frage gestellt, ob sich der Proband etwas unter User Tracking vorstellen kann. Im Dialog wird versucht, die Bedeutung dieser Methoden verständlich zu machen. Dabei werden vertiefend 2 Beispiele erwähnt:

Vorratsdatenspeicherung (VDS) Im Gespräch und mit Skizzen auf Zetteln werden die Grundzüge der Vorratsdatenspeicherung samt deren Hintergründen erläutert. Die österreichische Umsetzung wird anhand einer Webseite [17] erklärt, die in einem Browser geöffnet und Punkt für Punkt durchbesprochen wird. Abschließend wird eine Visualisierung von Vorratsdaten anhand des ZEIT ONLINE Artikel „Verräterisches Handy“[54] gezeigt.

Browser Tracking Die Webseite Panopticlick[55] wird vorgeführt und im Dialog besprochen. Zusätzlich werden die bei jeder HTTP-Anfrage mitgelieferten Browser-Parameter mit der BrowserSpy-Webseite[56] gezeigt.

Weitere Gefahren und Risiken

Um den nächsten Teil der Lerneinheit einzuleiten, werden die Fragen aufgeworfen, warum es im Handel sogenannte Bonuskarten gibt oder warum ein Nutzer Google Web Services gratis benutzen darf? Worin liegt der Sinn dessen, dass Firmen solche Dienste anbieten? In einem kurzen Dialog werden Antworten auf diese Fragen erörtert.

Beim Thema Search Term Analyse wird der Proband zuerst nach deren Bedeutung gefragt. Dabei wird im Gespräch die Theorie erklärt und die Geschichte rund um die eingestellte AOL-Suchmaschine[57] und deren Folgen [19] erzählt. Zusätzlich wird noch ein kleiner Blick auf Google History[58] gewährt, wo die einzelnen Visualisierungen hergezeigt werden. Zuerst wird die Bedeutung der Thematik „Tracking Web Interaction“ diskutiert. Mit dem Firefox-Plug-In „Lightbeam“[59] wird sie auch praktisch dargestellt.

Auch der Begriff „Social Engineering“ wird angesprochen und nach deren Bedeutung gefragt. Nach der Aufklärung wird darauf hingewiesen, dass Vorsicht geboten sei, mit wem in den

[54] http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten, Dezember 2013
[55] https://panopticlick.eff.org/, Jänner 2014
[56] http://browserspy.dk, Jänner 2014
[57] http://www.aolstalker.com/
[58] https://history.google.com/history/
[59] http://www.mozilla.org/en-US/lightbeam/

sozialen Medien kommuniziert wird. Zusätzlich wird auf die Privatsphäre-Einstellungen der einzelnen Medien (Facebook, LinkedIn, Twitter,...) aufmerksam gemacht, welche im Laufe der Zeit durch den Betreiber fallweise geändert werden. Anhand der Webseite von Mattmckeon[60], welche diese Veränderungen visuell aufbereitet, wird über diesen Aspekt diskutiert.

Technische und organisatorische Lösungsansätze

In diesem Teil der Lerneinheit steht die Vermittlung praktischer Lösungsansätze im Vordergrund. Es wird eine Diskussion über die virtuelle Identität eines Internet Users angeregt. Dabei werden diverse Tools[61,62] vorgestellt, die bei der Ermittlung der IP-Adresse hilfreich sind. Des Weiteren werden ProxyChecker[63] und ProxyJudges[64,65,66] gezeigt, die zusätzliche HTTP-Parameter anzeigen. Anschließend wird mit dem Probanden diskutiert, welche Gründe es zur Verschleierung der Identität geben könnte.

Als Nächstes werden praktische Lösungsansätze zur Verschleierung der Identität vorgestellt. TOR[67] und das Prinzip der offenen Proxies werden nur schematisch mündlich erläutert. Auf Nachfrage werden genauere Information über diese Themen gegeben. Detaillierter werden die Grundlagen der VPN-Netzwerke durch das Vorspielen einer SemperVideos[68] vorgestellt. Als Beispiel wird die Software CyberGhost[69] und deren Hintergründe vorgestellt. Mit dem Probanden wird die Software gestartet und eine Verbindung zu einem ausländischen Server aufgebaut. Durch einen kurzen IP-Check (wie anfangs erklärt) wird gezeigt, dass sich der User nun mit einer fremden Identität im Internet bewegt.

Zur Verschleierung der HTTP-Parameter wird das Firefox-Plug-In „Fireglove“ erklärt und praktisch am Browser gezeigt. Im Anschluss wird die Webseite fixtracking.com[70] mit deren Firefox-Plug-In "DoNotTrackMe"vorgestellt.

Damit sich der Proband gegen die Search-Term Analyse wehren kann, werden Alternativen zur Suchmaschine Google gezeigt. Als Beispiel wird dabei die Suchmaschine DuckDuckgo.com[71] vorgestellt und deren Vertrauenswürdigkeit diskutiert. Sollte sich der Teilnehmer von Google nicht trennen wollen, wird das Firefox-Plug-Ins „GoogleSharing“[72] und dessen Funktionalität erklärt.

---

[60] http://mattmckeon.com/facebook-privacy/
[61] http://www.myip.is/
[62] http://whatismyipaddress.com/
[63] http://www.proxy-listen.de/Proxy/Proxychecker.html
[64] http://ocl.opoint.com/proxyjudge/prxjdg.cgi
[65] http://www.xav.com/env.pl
[66] http://www.proxy-listen.de/azenv.php
[67] https://www.torproject.org/
[68] http://www.sempervideo.de/?p=7384
[69] http://cyberghostvpn.com, Jänner 2014
[70] http://fixtracking.com, Jänner 2014
[71] https://duckduckgo.com/
[72] https://addons.mozilla.org/de/firefox/addon/googlesharing/

Abschluss

Um einen Abschluss für die Lerneinheit zu finden, wird der Proband gefragt, welche Rückschlüsse er von dieser Thematik gezogen hat und wie es ihm während dem Vortrag gegangen sei. Etwaige Rückfragen werden verständlich erklärt. Vielleicht ergeben sich im Laufe der Diskussion auch Fallbeispiele, welche Datenschutz-relevante Fragen aufwerfen. Dabei werden mögliche Lösungsansätze (eventuell mit Hilfe der vorgestellten Tools) besprochen.

3.5 Didaktische Modell für den visuellen Lerntypen

Beim visuellen Lerntypen bedient sich das didaktische Modell vorwiegend bildhaften Lernhilfen wie Skizzen, Grafiken und Videos. Dieser Art des Lernens geht davon aus, dass der Lernende durch das Beobachten von Handlungsabläufen den Lernstoff am besten verinnerlicht.[4] So werden gewisse Begriffe und Abläufe einfach auf einem Zettel skizziert, mit Bildern erklärt oder anhand von Videos demonstriert. Gerade in diesem Bereich bietet das Online-Lernportal SemperVideo[73] viele Videos an, die viele technische Abläufe zeigen. Zusätzlich werden auch themenspezifische Webseiten herangezogen, wo diverse Sachverhalte Punkt für Punkt erklärt werden.

Die folgenden Sektionen erklären das visuelle Modell (Tabelle 3.4) mit dem jeweiligen Medieneinsatz im Detail.

Einführung

Nach kurzer Erläuterung der Komik auf den Einführungsfolien A.1, wird der Proband nach persönlichen Erfahrungen mit Datenschutz im Internet befragt. Danach wird der Ablauf der empirischen Untersuchung auf einem Zettel skizziert und das Ziel der Lerneinheit mündlich erläutert. Durch konkrete Beispiele wird versucht, das Interesse entsprechend zu wecken.

Begriffe Internet Privacy, Identität, Anonymität

Zu Beginn wird Richelieu's Zitat von der Präsentationsfolie „Zitat zum Datenschutz“ A.2 vorgelesen und kurz deren Bedeutung in der Gegenwart verbal erläutert. Dabei sollte auf die persönlichen Daten hingewiesen werden, die die Testperson möglicherweise schon in den sozialen Medien preisgegeben hat oder die über Google sie zu finden sind. Es sollte eine persönliche Betroffenheit des Probanden erreicht werden.

Danach wird die Abbildung auf Folie „Akteure beim Surfen“ A.2 gezeigt und die einzelnen Knotenpunkte erklärt. In diesem Zusammenhang werden die beiden DOS-Kommandos „ipconfig“ und „tracert“ und deren Anwendung gezeigt. Zusätzlich wird darauf hingewiesen, dass bei jeder Instanz potenziell eine Profilerstellung des Internet Users möglich ist.

Ferner werden alle Begriffe, die auf Folie „Begriffe“ A.2 gelistet sind, wie folgt erörtert:

Privatsphäre im Internet Für diesen Begriff werden die beiden Videos[74,75] des Datenschutz-

[73] http://www.sempervideo.de/, Jänner 2014

[74] http://www.bitkom-datenschutz.de/44004.htm, Dezember 2013

[75] http://www.bitkom-datenschutz.de/44006.htm, Dezember 2013

Tabelle 3.3: Angewandtes didaktisches Modell für den kommunikativen Lerntypen

Inhalt	Medien	Methodik
Einführung	PPT-Folie „Inhalt“ (A.1)	• Erklärung der empirischen Untersuchung (Ablauf, Inhalt, Ziel) • Anhand der Komik auf der PPT-Folie Gespräch über den Inhalt initiieren • Dialog über den persönlichen Nutzen des Probanden • Bewusstsein für die Datenschutz-Materie durch Diskussion feststellen
Identität, Privacy, Anonymität	PPT-Folien „Zitat zum Datenschutz“, „Akteure beim Surfen“, „Begriffe“ (A.2)	• kurzes Gespräch über Richelieu’s Zitat initiieren • Akteure beim Surfen mit Folienabb. diskutieren • Privacy (Definition diskutieren), Teil-Identitäten (Diskussion über Abbildung), Anonym surfen (mündlich)
User Tracking Methoden	PPT-Folien „User Tracking“ (A.3), Web-Links	• Infrage stellen von „User Tracking“ und Diskussion über den Begriff • VDS: Theorie im Dialog vorstellen (Frage-Antwort-Spiel, auf Zettel skizzieren); zeigen der Web-Links und Rückfragen klären; • Browser Tracking mit „Panopticlick“ vorstellen; auf HTTP-Parameter hinweisen
weitere Gefahren & Risiken	PPT-Folie „Weitere Gefahren & Risiken“ (A.4), Firefox-Browser	• Diskussionspunkte: Warum gibt es Bonuskarten? Warum darf man Google Services gratis nutzen? • Frage-Antwort-Spiel: Search Term Analyse (Google History), Web Interaction (Lightbeam) • im Gespräch Social Engineering erläutern
tech. und org. Lösungsansätze	PPT-Folie „Lösungsansätze“ (A.5), Firefox Plugins, CyberGhost, YouTube-Videos	• Dialog über virtuelle Identität (WhatIsMyIP) und Gründe für Anonymität • TOR, Open Proxies kurz erklären; CyberGhost (Youtube, Software zeigen) • Firefox-Plugins „DNTM“„Fireglove“ am Browser zeigen • Diskussion über DuckDuckGo und Firefox-Plugins „GoogleSharing“
Abschluss	PPT-Folie „Conclusio“ (A.5)	• Abschließende Diskussion anregen, Rückfragen beantworten • bei Bedarf Use Case des Probanden diskutieren

Portals der Firma Bitkom gezeigt und Rückfragen des Probanden geklärt.

Virtuelle vs. reale Identität Der Begriff der realen Identität wird mithilfe der Abbildung auf Folie „Begriffe“ A.2 erklärt. Danach werden auf einen Zettel Benutzerkonten skizziert, um so die verschiedenen virtuellen Identitäten anzudeuten. Am Beispiel der Anwendung der gesamten Servicepalette von Google wird die Verknüpfbarkeit der einzelnen Identitäten gezeigt und auf deren Folgen und Konsequenzen hingewiesen.

Anonymität im Internet In diesem Zusammenhang wird mündlich erklärt, welche Folgen ein unverschlüsselter Internetverkehr haben kann und wie Anonymität im Internet verstanden werden sollte.

User Tracking Methoden

Für diesen Abschnitt wird die Definition und Bedeutung von User Tracking nur kurz erläutert, um später mit visuellen Lehrmethoden die folgenden Beispiele vorzustellen:

Vorratsdatenspeicherung (VDS) Die VDS wird durch das SemperVideo[76] erklärt, welches ihre Grundzüge anhand visueller Darstellungen im Detail erklärt. Wie dieses Gesetz in Österreich umgesetzt wurde, wird dem Probanden durch eine Webseite[17] am Browser erklärt. Zur praktischen Darstellung der VDS wird zusätzlich noch der ZEIT ONLINE Artikel „Verräterisches Handy“[77] gezeigt, welcher die Telekommunikationsdaten visuell aufbereitet.

Browser Tracking Anhand der Webseite Panopticlick[78] und einem SemperVideo[79] wird Browser Tracking im Detail erklärt. Mit der BrowserSpy-Webseite[80] werden die mitgelieferten HTTP-Parameter des Browsers vorgestellt.

Weitere Gefahren und Risiken

Bei diesem Teil wird anfangs das Prinzip der Bonuskarte auf einen Zettel skizziert. Auch das Feststellen des Surfverhaltens durch die Gratis-Nutzung von Webservices (Google) wird ähnlich erklärt. Dem Probanden sollte vermittelt werden, dass es sich dabei jeweils um einen Verlust der Privatsphäre handelt.

Die Search Term Analyse wird anhand der Geschichte rund um die eingestellten AOL-Suchmaschine[81] mit deren Folgen [19] gezeigt und erklärt. Danach wird dem Probanden Google History[82] vorgestellt, wobei verschiedene Visualisierungen gezeigt werden. Auch das Thema

[76] http://www.youtube.com/watch?v=1maZNx_ElKQ, Dezember 2013
[77] http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten, Dezember 2013
[78] https://panopticlick.eff.org/, Jänner 2014
[79] http://www.sempervideo.de/?p=9692, Jänner 2014
[80] http://browserspy.dk, Jänner 2014
[81] http://www.aolstalker.com/
[82] https://history.google.com/history/

„Tracking Web Interaction“ wird anhand des Firefox Plug-Ins „Lightbeam“[83] praktisch erklärt und deren Grafiken präsentiert.

Das Thema „Social Engineering“ wird nur kurz erklärend angerissen, um darauf hinzuweisen, dass Vorsicht geboten sei, mit wem in sozialen Medien kommuniziert wird. Auch auf die Privatsphäre-Einstellungen der einzelnen Medien (Facebook, LinkedIn, Twitter,...) wird mit einer Webseite[84] aufmerksam gemacht, da sich diese im Laufe der Zeit ändern können.

Technische und organisatorische Lösungsansätze

In diesem Teil der Lerneinheit steht die Vermittlung praktischer Lösungsansätze im Vordergrund. Anfangs wird die virtuelle Identität eines Internet Users mithilfe von Skizzen auf einen Zettel erklärt und es werden dabei diverse Tools[85,86] vorgestellt. Weiters werden ProxyChecker[87] und ProxyJudges[88,89,90] gezeigt und erklärt, die zusätzlich zur IP-Adresse auch noch weitere Parameter anzeigen. Anschließend werden noch Argumente für die Verschleierung der Identität aufgezählt und kurz diskutiert.

Als Nächstes werden praktische Lösungsansätze zur Verschleierung der Identität vorgestellt. TOR[91] und das Prinzip der offenen Proxies werden nur schematisch auf einem Zettel skizziert. Auf Nachfrage werden genauere Information über diese Themen gegeben. Detaillierter werden die Grundlagen der VPN-Netzwerke durch das Vorspielen eines SemperVideos[92] gezeigt. Als Beispiel wird die Software CyberGhost[93] vorgestellt und deren Hintergründe erklärt. Mit dem Probanden wird die Software gestartet und eine Verbindung zu einem ausländischen Server aufgebaut. Durch einen kurzen IP-Check wird gezeigt, dass sich der Nutzer nun mit einer fremden Identität im Internet bewegt.

Zur Verschleierung der HTTP-Parameter wird das Firefox-Plug-In „Fireglove“ durch Ausschnitte eines YouTube-Video[94] skizziert und praktisch am Browser gezeigt. Im Anschluss wird die Webseite fixtracking.com[95] mit dem Firefox Plug-In „DoNotTrackMe“ mündlich erläutert.

Damit sich der Teilnehmer gegen die Search-Term Analyse wehren kann, werden alternativen zur Suchmaschine Google gezeigt. Als Beispiel wird dabei die Suchmaschine DuckDuckgo.com[96] vorgestellt und deren Vertrauenswürdigkeit erörtert. Falls sich der Proband doch nicht von Google trennen will, wird das Firefox-Plug-in „GoogleSharing“[97] und deren Funktionalität mithilfe einer Skizze erklärt.

---

[83] http://www.mozilla.org/en-US/lightbeam/
[84] http://mattmckeon.com/facebook-privacy/
[85] http://www.myip.is/
[86] http://whatismyipaddress.com/
[87] http://www.proxy-listen.de/Proxy/Proxychecker.html
[88] http://ocl.opoint.com/proxyjudge/prxjdg.cgi
[89] http://www.xav.com/env.pl
[90] http://www.proxy-listen.de/azenv.php
[91] https://www.torproject.org/
[92] http://www.sempervideo.de/?p=7384
[93] http://cyberghostvpn.com, Jänner 2014
[94] http://www.sempervideo.de/?p=9692, Jänner 2014
[95] http://fixtracking.com, Jänner 2014
[96] https://duckduckgo.com/
[97] https://addons.mozilla.org/de/firefox/addon/googlesharing/

Abschluss

Um einen Abschluss für die Lerneinheit zu finden, wird der Proband gefragt, welche Rückschlüsse er von dieser Thematik gezogen hat und wie es ihm bei der Lerneinheit gegangen sei. Etwaige Rückfragen werden verständlich erklärt. Eventuell ergeben sich im Laufe der Diskussion Fallbeispiele, welche Datenschutz-relevante Fragen aufwerfen. Dabei werden mögliche Lösungsansätze (etwa mit Hilfe der vorgestellten Tools) erörtert.

3.6 Didaktische Modell für den motorischen Lerntypen

Beim motorischen Lerntyp wird ein didaktisches Modell angewandt, welches sich an die „learning by doing“ - Methode anlehnt. Es wird davon ausgegangen, dass ein Proband am besten lernt, indem er gewisse Handlungsabläufe selber durchführt und selbst seine Erfahrungen sammelt. Somit wird der Lernende während der Lerneinheit nebst der mündlichen Erklärung immer wieder angehalten, gewisse Handlungen selbst durchzuführen. Dabei wird er vom Vortragenden angeleitet, Programme zu starten, diese anzuwenden und selbst Videos oder Webseiten zu öffnen. Bei weiteren Fragestellungen werden auch einfache Rollenspiele angewendet, indem der Proband in Situationen versetzt wird und selbst bestimmte Lösungsansätze ausarbeiten soll.[4]

In den folgenden Sektionen wird dieses didaktische Modell erläutert, welches auch in der Tabelle 3.5 zusammengefasst wurde.

Einführung

Nach einer mündlichen Einführung über die empirische Untersuchung und der Thematik mit den Präsentationsfolien A.1 wird ein kurzes Rollenspiel durchgeführt. Die Testperson müsse sich vorstellen, er habe eine E-Mail von einem dubiosen Absender „andreas12linz82@hotmail.com“ bekommen. Er solle alle potentiellen Informationen über den Absender nennen. Nach kurzem Dialog wird darauf hingewiesen, welche Informationen schon aus einer einfachen E-Mail-Adresse offengelegt werden. Danach wird der persönliche Nutzen und die Bewusstseinsschaffung in den Raum gestellt, um so das Interesse für den weiteren Vortrag entsprechend zu erwecken.

Begriffe Internet Privacy, Identität, Anonymität

Anfangs wird das Zitat von Kardinal Richelieu von der Präsentationsfolie „Zitat zum Datenschutz“ A.2 vorgelesen. Die Testperson wird danach mit der Frage konfrontiert, welche Bedeutung das Zitat in der heutigen Zeit haben könnte. Um auf die persönlichen Daten hinzuweisen, die bereits im Internet zu finden sind, wird der Proband aufgefordert, eine Google-Anfrage mit seinem Namen als Suchbegriff durchzuführen. Weiters wird ihm aufgetragen, seine persönliche Daten seines Facebook-Kontos zu prüfen.

Danach werden die Akteure beim Internetsurfen mit der Abbildung auf der Folie „Akteure beim Surfen“ A.2 erklärt. Daraufhin wird der Proband aufgefordert, die beiden DOS-Kommandos „ipconfig“ und „tracert“ in Anwendung zu bringen. Er wird dazu angeleitet und

Tabelle 3.4: Angewandtes didaktisches Modell für den visuellen Lerntypen

Inhalt	Medien	Methodik
Einführung	PPT-Folie „Inhalt“ (A.1)	• Erklärung der empirischen Untersuchung (Ablauf, Inhalt, Ziel) durch schematisches Skizzieren auf einem Zettel • Einführung zur Thematik anhand der Komik auf der PPT-Folie • Erläuterung des persönlichen Nutzen des Probanden (durch konkrete Beispiele)
Identität, Privacy, Anonymität	PPT-Folien „Zitat zum Datenschutz“, „Akteure beim Surfen“, „Begriffe“ (A.2); YouTube-Videos	• Anhand Richelieu’s Zitat Vergleiche ziehen • Akteure beim Surfen durch Folienabbildung zeigen; zeigen der Befehle „ipconfig“, „tracert“ • Privacy (YouTube-Videos), Teil-Identitäten (Folienabbildung), Anonym surfen (mündlich)
User Tracking Methoden	PPT-Folien „User Tracking“ (A.3), YouTube-Vidoes, Web-Links	• „User Tracking“ kurz erklären • VDS: Youtube-Video vorspielen, Web-Links herzeigen und erklären • Browser Tracking mit „Panopticlick“ zeigen; HTTP-Parameter mit Web-Link „BrowserSpy“ vermitteln
weitere Gefahren & Risiken	PPT-Folie „Weitere Gefahren & Risiken“ (A.4), Firefox-Browser	• Bonuskartenprinzip auf Zettel skizzieren, Surfverhalten - gratis Google Services? • am Browser zeigen: Search Term Analyse (Google History), Web Interaction (Lightbeam) • Social Engineering (Beispiel auf Zettel skizzieren)
tech. und org. Lösungsansätze	PPT-Folie „Lösungsansätze“ (A.5), Firefox Plugins, CyberGhost, YouTube-Video	• Erklärung und Skizzen: virtuelle Identität (WhatIsMyIP), Gründe für Anonymität • TOR, Open Proxies kurz erklären; CyberGhost zeigen (YouTube-Video) • Firefox-Plugins „DNTM“, „Fireglove“ zeigen • DuckDuckGo und Firefox-Plugins „GoogleSharing“ zeigen und am Zettel skizzieren
Abschluss	PPT-Folie „Conclusio“ (A.5)	• Abschließende Diskussion anregen, Rückfragen beantworten • bei Bedarf Use Case des Probanden diskutieren

die Ausgabe der Kommandos wird im Detail erklärt. Außerdem wird er darauf hingewiesen, dass bei jeder Instanz potenziell eine Profilerstellung eines Internet Users möglich ist.

Als Nächstes werden alle Begriffe auf der Folie „Begriffe“ A.2 kurz diskutiert:

Privatsphäre im Internet Bei diesem Begriff wird gefragt, welche Bedeutung dieser haben könnte. Langsam werden die Unterschiede zwischen seinem Verständnis und der Definition des Datenschutzes nach PRIME (Kapitel 3.1) herausgearbeitet

Virtuelle vs. reale Identität Mit der Abbildung auf Folie A.2 wird der Begriff der Identität und deren virtuelle und reale Ausprägung mündlich erläutert. Danach wird der Proband aufgefordert, er solle Beispiele für virtuelle und reale Teilidentitäten nennen. Im Dialog wird festgestellt, ob die Testperson Google Web Services nutzt und welche Möglichkeiten Google im Sinne der Verknüpfbarkeit von Nutzerkonten in diesem Zusammenhang hat.

Anonymität im Internet Es wird eine kurze Diskussion initiiert, wobei die Frage der möglichen Folgen von unverschlüsseltem Internetverkehr besprochen und wie Anonymität im Internet verstanden werden sollte.

User Tracking Methoden

In diesem Teil wird gefragt, ob er mit dem Begriff „User Tracking“ etwas anfangen könne. Es wird versucht das vorhandene Verständnis im Gespräch durch die Theorie zu berichtigen. Danach werden 2 Beispiele vorgestellt:

Vorratsdatenspeicherung (VDS) Es wird eine verkürzte Fassung von einem SemperVideo[98] gezeigt, und anhand dessen die wichtigsten Aspekte der VDS erklärt. Die österreichische Umsetzung wird zusammen mit einer Webseite [17] und einer vom Probanden gezeichneten Mindmap beschrieben und gezeichnet. Danach wird die Testperson aufgefordert, den ZEIT ONLINE Artikel „Verräterisches Handy“[99] in einem Browser zu öffnen. Nach kurzer Erklärung soll sie unter Anleitung mit der Visualisierung experimentieren und selbst Erkenntnisse daraus schließen.

Browser Tracking Der Proband soll die Webseite Panopticlick[100] in einem Browser öffnen und auf den Test-Button drücken. Danach wird das Ergebnis erklärt und vertiefend das SemperVideo[101] gezeigt. Anschließend wird dem Probanden die BrowserSpy-Webseite[102] vorgestellt. Dabei wird dem Probanden die Möglichkeit gegeben, die Webseite selbst auszutesten.

[98] http://www.youtube.com/watch?v=1maZNx_ElKQ, Dezember 2013
[99] http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten, Dezember 2013
[100] https://panopticlick.eff.org/, Jänner 2014
[101] http://www.sempervideo.de/?p=9692, Jänner 2014
[102] http://browserspy.dk, Jänner 2014

Weitere Gefahren und Risiken

Im nächsten Abschnitt wird die Testperson aufgefordert, er solle sich in die Rolle eines Verkäufers versetzen und herausfinden, wie er das Kaufverhalten seiner Kunden feststellten könnte. Die gleiche Problematik soll im Zusammenhang mit den verschiedenen Google-Diensten und dem Feststellen des Surfverhaltens vermittelt werden. Es soll dabei selbst die Erfahrung gemacht werden, wie jeweils die Firmen agieren müssten, um zu diesen Informationen zu gelangen.

Die Bedeutung der Search Term Analyse wird zuerst mündlich erklärt. Unter Anleitung wird der Proband aufgefordert, er solle sich in Google History[103] einloggen und sich die einzelnen Visualisierungen ansehen. Nebenbei wird von der Geschichte rund um die eingestellten AOL-Suchmaschine[104] und deren Folgen [19] erzählt.

Beim Thema „Tracking Web Interaction“ soll mit dem Firefox-Plug-In „Lightbeam“[105] experimentiert werden, nebenbei wird deren Bedeutung verbal vermittelt.

Auch das Thema „Social Engineering“ wird mit einem Rollenspiel erklärt. Dabei wird die Frage gestellt, wie der Proband persönliche Informationen von einem seiner Freunde erhalten würde, ohne ihn hacken zu müssen. Dabei wird diese Fragestellung besprochen und etwaige Erkenntnisse daraus gezogen. Auch die Webseite von Mattmckeon[106] soll in einem Browser geöffnet werden, wo er mit der Visualisierung selbst die Erfahrung machen kann, wie sich die Privacy-Einstellungen von Facebook im Laufe der Jahre geändert haben.

Technische und organisatorische Lösungsansätze

In diesem Teil der Lerneinheit steht die Vermittlung praktischer Lösungsansätze im Vordergrund. Anfangs wird die virtuelle Identität eines Internet Users diskutiert und es werden dabei diverse Tools[107,108] vorgestellt. Der Proband wird angeleitet, ProxyChecker[109] und ProxyJudges[110,111,112] anzuwenden, die zusätzlich zur IP-Adresse auch noch die durch die HTTP-Anfrage mitgelieferten Parameter anzeigen. Anschließend werden noch Argumente für die Verschleierung der Identität aufgezählt und kurz diskutiert.

Als Nächstes werden praktische Lösungsansätze zur Verschleierung der Identität vorgestellt. TOR[113] und das Prinzip der offenen Proxies werden nur schematisch mündlich erläutert. Auf Nachfrage werden genauere Information über diese Themen gegeben. Detaillierter werden die Grundlagen der VPN-Netzwerke durch das Vorspielen einer SemperVideos[114] vorgestellt. Als Beispiel wird die Software CyberGhost[115] und deren Hintergründe vorgestellt. Mit dem Proban-

[103] https://history.google.com/history/
[104] http://www.aolstalker.com/
[105] http://www.mozilla.org/en-US/lightbeam/
[106] http://mattmckeon.com/facebook-privacy/
[107] http://www.myip.is/
[108] http://whatismyipaddress.com/
[109] http://www.proxy-listen.de/Proxy/Proxychecker.html
[110] http://ocl.opoint.com/proxyjudge/prxjdg.cgi
[111] http://www.xav.com/env.pl
[112] http://www.proxy-listen.de/azenv.php
[113] https://www.torproject.org/
[114] http://www.sempervideo.de/?p=7384
[115] http://cyberghostvpn.com, Jänner 2014

den wird die Software gestartet und eine Verbindung zu einem ausländischen Server aufgebaut. Durch einen kurzen IP-Check (wie anfangs erklärt) wird gezeigt, dass sich der Nutzer nun mit einer fremden Identität im Internet bewegt.

Als eine Möglichkeit zur Verschleierung der HTTP-Parametern wird das Firefox-Plug-In „Fireglove“ mithilfe von Ausschnitten eines YouTube-Video [116] erklärt. Danach bekommt der Proband die Aufgabe, es selber auszuprobieren. Im Anschluss wird die Webseite fixtracking.com[117] mit deren Firefox-Plug-In „DoNotTrackMe“ mündlich erläutert und ausprobiert.

Damit sich der Teilnehmer gegen die Search-Term Analyse wehren kann, werden Alternativen zur Suchmaschine Google gezeigt. Als Beispiel wird dabei die Suchmaschine DuckDuckgo.com[118] vorgestellt und deren Vertrauenswürdigkeit erörtert. Falls der Proband jedoch weiter mit Google arbeiten will, wird das Firefox-Plug-Ins „GoogleSharing“[119] und deren Funktionalität erklärt.

Abschluss

Um einen Abschluss für die Lerneinheit zu finden, wird die Testperson gefragt, welche Rückschlüsse sie von dieser Thematik gezogen hat und wie es ihr während der Session gegangen sei. Etwaige Rückfragen werden verständlich erklärt. Vielleicht ergibt sich im Laufe der Diskussion auch ein Fallbeispiel, vor dem sie schon mal gestanden ist. Dieser wird aufgegriffen und mögliche Lösungsansätze (eventuell mit Hilfe der vorgestellten Tools) durchdiskutiert.

[116] http://www.sempervideo.de/?p=9692, Jänner 2014
[117] http://fixtracking.com, Jänner 2014
[118] https://duckduckgo.com/
[119] https://addons.mozilla.org/de/firefox/addon/googlesharing/

Tabelle 3.5: Angewandtes didaktisches Modell für den motorischen Lerntypen

Inhalt	Medien	Methodik
Einführung	PPT-Folie „Inhalt“ (A.1)	• Erklärung der empirischen Untersuchung (Ablauf, Inhalt, Ziel) anhand der Komik auf der PPT-Folie • Inhalt erklären mittels Fragestellung: Wie viel Information kann aus der Mail-Adresse „andreas12linz82@hotmail.com“ herausgelesen werden? • Anleitung zur bevorstehenden Lerneinheit geben und Diskussion über persönlichen Nutzen des Probanden initiieren
Identität, Privacy, Anonymität	PPT-Folien „Zitat zum Datenschutz“, „Akteure beim Surfen“, „Begriffe“ (A.2)	• Infrage stellen von Richelieu’s Zitat • Erklärung der Akteure beim Surfen (Folienabb.); Befehle „ipconfig“, „tracert“ (Proband anleiten) • Privacy (infrage stellen, Vergleich zur Theorie), Teil-Identitäten (Folienabbildung diskutieren), Anonym surfen (mündlich)
User Tracking Methoden	PPT-Folien „User Tracking“ (A.3), YouTube-Vidoes, Web-Links	• „User Tracking“ infrage stellen und Begriffsklärung • VDS mit Youtube-Video; VDS in Ö erklären; mit „Verräterisches Handy“ experimentieren lassen • Webseiten „Panopticlick“ und „BrowserSpy“ kurz erläuteren; Proband unter Anleitung selbst probieren lassen
weitere Gefahren & Risiken	PPT-Folie „Weitere Gefahren & Risiken“ (A.4), Firefox-Browser	• kurzes Rollenspiel: Wie könnte man das Kauf- oder Surfverhalten der Kunden feststellen? - Bonuskarten; gratis Google Services • Proband anleiten: Search Term Analyse (Google History), Web Interaction (Lightbeam) • Rollenspiel: Wie finde ich ohne „Hacken“ persönliche Informationen heraus? - Social Engineering!
tech. und org. Lösungsansätze	PPT-Folie „Lösungsansätze“ (A.5), Firefox Plugins, CyberGhost, YouTube-Videos	• Diskussion und Proband ausprobieren lassen: virtuelle Identität (WhatIsMyIP), Gründe für Anonymität • TOR, Open Proxies erklären; CyberGhost (YouTube-Video, Software zeigen, Anleitung) • Proband anleiten: Plugins „DNTM“, „Fireglove“ • DuckDuckGo, Plugin „GoogleSharing“ (Anleitung)
Abschluss	PPT-Folie „Conclusio“ (A.5)	• Abschl. Diskussion anregen, Rückfragen behandeln • bei Bedarf Use Case des Probanden diskutieren

KAPITEL 4

Ergebnisse der empirischen Analyse

Dieses Kapitel widmet sich der quantitativen Analyse der Pretest- und Posttestmessung sowie der Langzeitevaluierung. Dabei wurde nach der Auswertungsstrategie vorgegangen, die im Kapitel 2.5 im Detail vorgestellt wurde. Zusätzlich wurde eine qualitative Bewertung aller Lerneinheiten vorgenommen, wodurch Eindrücke und Beobachtungen des Vortragenden festgehalten wurden.

4.1 Ergebnisse der Pretest-Analyse

In diesem Abschnitt werden die Antworten und statistische Auswertungen des Pretests diskutiert. Diese Messung wurde im Rahmen der Untersuchung noch vor der Bildungsmaßnahme durchgeführt (Kapitel 2.3) und diente als Bestandsaufnahme des Wissensstandes beim Probanden über das Thema Privatsphäre im Internet.

Teilnehmer der Untersuchung

Insgesamt stellten sich 34 Personen zur Verfügung, um als Proband der Untersuchung teilzunehmen. Im Rahmen des Pretests wurden neben den fachlichen Fragen auch Alter, Geschlecht und Ausbildung der Testperson erhoben. So konnte bei der Analyse der einzelnen Antworten auch auf diese Aspekte Rücksicht genommen werden und Vergleiche gezogen werden.

Wie Abbildung 4.1 zeigt, gliedert sich die Untersuchungsstichprobe in 59% männliche und 41% weibliche Probanden auf. In Bezug auf das Alter wurden in der Analyse alle Testpersonen in 5 Altersklassen (<20, 20-29, 30-39, 40-49, >50) eingeteilt. Dabei konnten für die Gruppe 20 - 29 Jahren mit 32% die meisten Personen für die Untersuchung akquiriert werden. Am schwierigsten war es, Personen für die Gruppe „über 50“ zu finden, die den Mindestkriterien (Kapitel 2.2) entsprechen. Über alle Altersklassen betrachtet, waren mehr als die Hälfte (52%) aller Testpersonen unter 30 Jahre. Trotzdem konnten für jede Altersklasse und für jedes Geschlecht ausreichend viele Personen gefunden werden, so dass für jede Gruppe eine Aussage getroffen werden konnte.

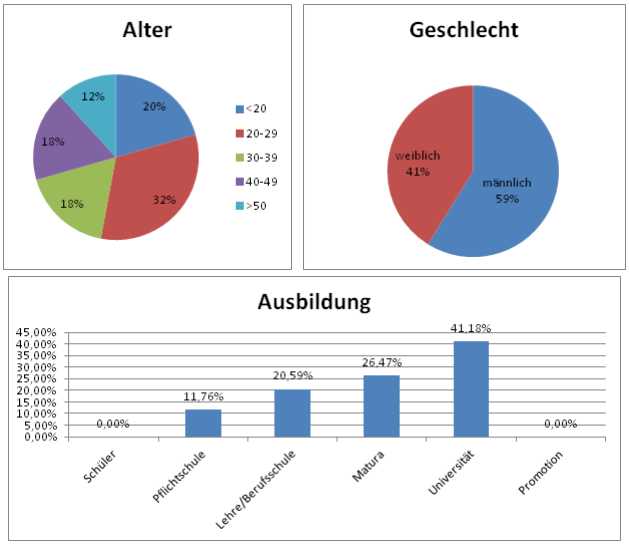


Abbildung 4.1: Testpersonen nach Alter, Geschlecht und Ausbildung

Auch bezüglich Ausbildung war es das Ziel, genügend Personen für jede Gruppe zu finden. Wie jedoch das Diagramm „Ausbildung“ in Abbildung 4.1 zeigt, ergab sich bei der Untersuchung eine sehr unausgewogenes Bild an Teilnehmern bezüglich ihres Bildungsstandes. Eindeutig die größte Gruppe (41%) war jene, die in Besitz eines Universitätsabschlusses ist. Weiters ist anzumerken, dass ein überwiegender Anteil (67%) aller teilgenommenen Probanden eine Matura besitzt. Speziell dieser Gruppe könnte aufgrund des hohen Bildungsstandes eine breite Affinität mit dem Internet unterstellt werden, so dass die Mindestkriterien besonders gut erfüllt werden. Der Rest befindet sich derzeit in der Pflichtschule, in berufsbildenden Schulen oder in der Lehre.

Die Rolle von Privatsphäre

Der erste thematische Block des Pretests beschäftigt sich mit der Wertigkeit von Datenschutz im Internet. Dabei wird der Proband mit themenbezogenen Begriffen konfrontiert und gefragt, was er sich unter bestimmten Stichworten vorstellen kann. Zudem wird der Verantwortungsbereich von Privatsphäre infrage gestellt und eine Einschätzung verlangt, wie Institutionen wie der Staat, IT-Firmen oder Versicherungen mit privaten Daten umgehen.

Wie Abbildung C.1 veranschaulicht, wurde der Proband nach einer Erklärung zu folgenden Begriffen gefragt, die stichwortartig zu beschreiben waren:

- Privatsphäre im Internet
- virtuelle Identität
- Vorratsdatenspeicherung (VDS)

Für den Begriff „Privatsphäre im Internet“ gaben 76% aller Befragten eine Definition ab. Dabei wurden vielfach die Privatsphäre-Einstellungen von Facebook und die Veröffentlichungen persönlicher Daten auf sozialen Medien genannt. Andere gaben eine Erklärung ab, dass es sowieso keine Privatsphäre im Internet gäbe und das Internet total überwacht werde. Ein Internet User müsse dabei mitspielen, ansonsten könne er diese Webdienste nicht nützen. Auch richtige Erklärungsansätze wurden gefunden, wobei private Daten im Internet auch privat bleiben sollten und jeder für sich selbst das alleinige Bestimmungsrecht für seine Daten beanspruchen sollte. Unter dem Begriff der „virtuellen Identität“ konnten sich nur mehr 53% aller Befragten etwas vorstellen. Häufig wird dieser Begriff mit einem Profil oder mit dem Auftritt auf sozialen Medien (meist Facebook) in Verbindung gebracht. Manche vergleichen diesen Begriff mit einem „virtuellen Fußabdruck im Web“, wobei alle Informationen gemeint sind, die im Internet (Google) über die eigene Person zu finden sind. Andere finden auch einen generellen Erklärungsansatz, indem diesen Begriff als eine künstliche Identität im Web sehen, die durch eine reale Person kreiert wurde und damit auch Teil der realen Identität ist. Auch Begriff der Vorratsdatenspeicherung (VDS) ist 53% aller Befragten nach eigenen Angaben bekannt. Unter den Antworten befinden sich oft richtige Beschreibungen, indem die VDS als Speicherung aller Verkehrsdaten jeglicher Telekommunikation verstanden wird. Andere hingegen verstehen diesen Begriff als Suchverlauf von Amazon oder Google. Diese Firmen würden mitspeichern, für welche Artikel sich eine Person interessiert oder auf welche Webseiten sie surft. Auch die Datensammlung von Facebook wird in diesem Zusammenhang erwähnt.

Nach den offenen Fragen wurde die Wichtigkeit von Privatsphäre im Allgemeinen erhoben. In der Analyse der Antworten (Abbildung C.2), fällt sofort auf, dass dies für die meisten Befragten ein wichtiges Thema sei. Je höher die Ausbildung, desto höher wird der Prozentanteil an „sehr wichtig“ - Antworten. Diese Tatsache könnte dadurch erklärbar sein, dass mit dem höheren Bildungsgrad auch eine stärkere Internetnutzung einhergeht und dadurch das Bedürfnis an Privatsphäre besonders hoch ist. Weniger Gedanken über dieses Thema machen sich offensichtlich die jüngeren Menschen, die sich noch in Ausbildung (Pflicht- oder Berufsschule, Lehre) befinden. Denn nur Personen in dieser Ausbildungskategorie beantworteten die Frage mit „weniger wichtig“ order „keine Ahnung“. Obwohl die Mehrheit der Befragten angibt, dass Privatsphäre zumindest „wichtig“ sei, geben nur 15% (Abbildung C.3) an, dass sie Techniken zur Anonymisierung der Internet-Aktivitäten verwenden. Somit unternimmt nur ein kleiner Teil aller Probanden aktiv etwas für den eigenen Datenschutz beim Internetsurfen, wobei in diesem Zusammenhang oft die Nutzung des bekannten Tor-Netzwerks genannt wird.

Die nächsten Fragen beschäftigen sich mit der Problemstellung, wie viel persönliche Daten im Internet in der Wahrnehmung der Probanden preisgegeben werden. Dass im Internet oft mehr privaten Informationen verraten werden als dies in der realen Welt der Fall wäre, verneint eine überwiegende Mehrheit von 82% aller Befragten (Abbildung C.3). Nur ein kleiner Anteil aller Testpersonen ist der Meinung, dass oft leichtfertig persönlich Daten im Internet angegeben werden. Auch die Antworten der nächsten Frage beweist weiters, dass sich die User offensichtlich der Informationspreisgabe von privaten Details oft nicht bewusst sind. Denn häufig werden persönliche Informationen bei der Wahl von Benutzernamen oder Passwörtern beigefügt, welche sich oft aus Daten wie Name, Alter, Heimatstadt oder Geburtsjahr zusammensetzt. Somit ist es oft ein leichtes Spiel, vom Benutzernamen auf eine reale Person zu schließen. Wie

Abbildung C.4 zeigt, geben nur 56% der Testpersonen an, Pseudonyme für diese Zwecke zu verwenden.

In der Frage des Verantwortungsbereichs für Datenschutz im Internet zeichnet sich kein eindeutiger Trend ab. Wie Abbildung 4.2 zeigt, sehen nur 54% aller Probanden die Verantwortung beim Internet User selbst. Demnach sind fast die Hälfte aller Befragten anderer Meinung und sehen den Verantwortungsbereich für Privatsphäre bei anderen Instanzen, wie beim Internet Service Provider (ISP), beim Arbeitgeber oder beim verwendeten Webdienst selbst. Daraus ergibt sich die Schlussfolgerung, dass viele Internet User dieses Problem (noch) nicht als das Eigene sehen und sich lieber andere darum kümmern sollten. Aufklärung scheint in diesem Fall unumgänglich zu sein, um diese Thematik mehr in das Bewusstsein der Internet User zu rücken.

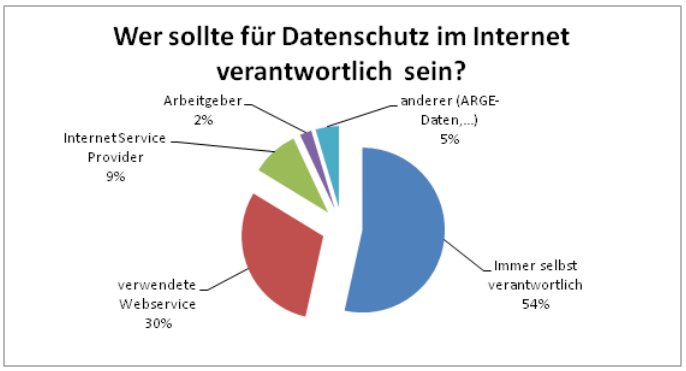


Abbildung 4.2: Verantwortliche für Datenschutz

Wie sehr trotzdem das Thema Privatsphäre im Internet im Bewusstsein der Befragten verankert ist, kann aus den Auswertungen von Abbildung C.5 abgelesen werden. Eine überwiegende Mehrheit von 94% ist der Meinung, dass Privatsphäre im Zeitalter des Internets immer mehr an Bedeutung gewinnt. Diese Tatsache lässt den Schluss zu, dass sich die Untersuchungsteilnehmer im Klaren sind, sich mit diesem Thema früher oder später auseinandersetzen zu müssen. Auch angesichts des wachsenden Sicherheitsgedanken und der zunehmenden Bedrohung durch Terrorismus ist dem Großteil (79%) klar, dass immer mehr Informationen des Bürgers durch Behörden eingefordert und offengelegt werden. 76% der Probanden sagen, dass das Internet die Offenlegung persönlicher Daten seiner Nutzer grundsätzlich beschleunige. Zudem sind 81% der Meinung, dass diese vielfach leichtfertig im Internet sogar veröffentlicht werden. Aber nicht nur der Staat sammelt persönliche Daten, sondern auch private Unternehmen. In diesem Zusammenhang herrscht überwiegend der Eindruck (82%), dass dabei oft mehr Informationen sammeln als notwendig. Daher sind sich alle Befragten einig, dass in diesem Bereich aktiv im Vorfeld auf Privatsphäre geachtet werden sollte. Dieser Eindruck wird dadurch bestärkt, dass 70% aller Befragten der Meinung sind, dass die Privatsphäre im Internet derzeit nicht gewahrt sei und die Veröffentlichung privater Daten oft nicht mehr in der eigenen Hand liege. Speziell diese Reihe von Antworten lässt den Schluss zu, dass die künftige Wichtigkeit von Datenschutz im Internet doch durch die User wahrgenommen wird. Umso wichtiger erscheint es, Aufklärung und die Bildung von Kompetenzen in diesem Bereich zu forcieren.

Abschließend zur Rolle von Datenschutz wird der Proband nach einer Einschätzung gefragt, für welchen Zweck Institutionen wie Staat, IT-Firmen oder Versicherungen öffentliche Internetpostings auswerten (Abbildung C.6). Dabei geben fast 80% an, dass die im Internet veröffentlichten Inhalte für gezielte personalisierte Werbung verwendet wird. Diese große Zustimmung könnte daher stammen, dass die Probanden selbst schon die Erfahrung mit dieser Art von Werbung gemacht haben. Ob diese Daten auch für Terror- und Verbrechensbekämpfung verwendet werden würden, gibt die Umfrage keine klare Antwort. Diese Aussagen unterstützen annähernd genauso viele Leute, wie die, die diese ablehnen bzw. keine Ahnung davon haben. Offensichtlich ist nicht allen ganz bewusst, dass veröffentlichte Inhalte auch von Behörden (z. B.: der Polizei) analysiert werden. Weiters können sich über 82% vorstellen, dass Firmen Informationen über ihre Job-Werber im Internet (Google) oder in den sozialen Medien (wie Facebook und Twitter) suchen, bevor sie diese zu einem Gespräch einladen. Ähnliches ergibt die Analyse für Nachstellen oder Belästigen durch Privatpersonen. Beide Szenarien wurden in den Medien schon öfters diskutiert, das Problem ist somit im Allgemeinen bekannt. Ob auch Versicherungen Personenprofile aus den Internet-Postings erstellen, ergibt die Umfrage keine klaren Ergebnisse. Über 70% würden dieser Annahme Glauben schenken, mehr als ein Viertel aller Befragten ist sich in dieser Frage jedoch uneinig. Zusammenfassend kann impliziert werden, dass sich eine überwiegende Mehrheit klar ist, dass ihre Inhalte von Dritten verwendet und analysiert werden.

Fragen zur Internetnutzung

Dieser Abschnitt widmet sich der generellen Internetnutzung der Probanden und versucht dabei deren Gewohnheiten zu analysieren. Dabei stehen die folgende Fragen im Raum: Wo wird das Internet vorwiegend genutzt? Welche Dienste oder Plattformen werden dabei in Anspruch genommen?

Wie Abbildung 4.3 zeigt, wird das Internet hauptsächlich am Arbeitsplatz (über 32%) oder von zuhause (über 24%) aus genutzt. Alternativ wird auch ein mobiler Zugang via Smartphone oder WLAN an Schulen und Universtäten verwendet. 12% aller Befragten geben nach eigenen Angaben an, sie verbinden sich mit dem Internet über öffentlich angebotene WLANs an Orten wie Hotels oder Internet-Cafés. Dabei verbindet sich der User oftmals völlig unverschlüsselt mit dem jeweiligen Hotspot und ist damit schutzlos gegenüber potentiellen Angreifern ausgeliefert.

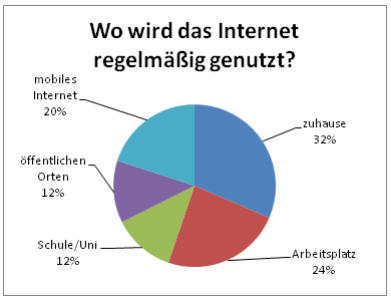


Abbildung 4.3: Nutzung des Internets

Ferner gibt eine überwiegende Mehrheit von 79% (Abbildung C.7) aller Testpersonen an,

dass sie in Besitz eines Smartphones sind. Dabei ergibt sich die Möglichkeit, zu jeder Tageszeit unabhängig vom aktuellen Standort sofort mobil ins Internet zu steigen. Dieser Anwendungsfall stellt ein Paradebeispiel für die Vorratsdatenspeicherung dar, wo jede Internetverbindung und letztlich auch andere Telekommunikation mitgespeichert wird. Alle Smartphone-Besitzer wurden zusätzlich gefragt, von welcher Marke ihr Gerät stammen würde. Wie Abbildung C.7 zeigt, gibt mehr als die Hälfte aller Befragten dabei an, sie besitzen ein Android-Handy (41% Samsung, 11% Sony und 4% LG). Annähernd ein Drittel (29%) verwendet ein iPhone von Apple. Diese Verteilung stimmt auch annähernd mit aktuellen Berichten des Marktforschers „comScore“ [21] überein.

Neben der Art des Internetzuganges wurde der Proband weiters gefragt, welche Dienste er dabei vorwiegend nutzt. Dabei sollte die Testperson die Top 5 Webseiten aufzählen. Eine Analyse von Abbildung 4.4 ergibt, dass diese Zeit hauptsächlich für das Lesen von Nachrichten (32%), für die Interaktion in sozialen Medien (22%) und für Webmail (18%) genutz wird. Werden nur die auf Platz 1 und 2 gereihten Dienste ausgewertet, werden zu 86% (Abbildung C.8) nur Dienste aus diesen Kategorien genannt. Besonders Suchmaschinen, Online Shops und Netbanking nehmen in dieser Statistik eher eine Nebenrolle ein.

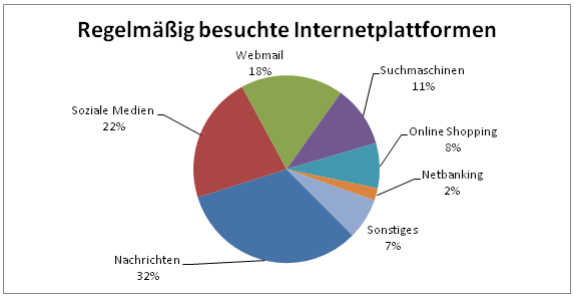


Abbildung 4.4: Regelmässig besuchte Internetplattformen

Im Bereich Nachrichten wurden in dieser Umfrage am häufigsten „orf.at“, „cnn.com“, diverse Sportseiten und verschiedenste Wetterseiten aufgezählt. Diese Art von Webseiten spielt bei den unter 20-Jährigen kaum eine Rolle, ist aber bei Personen zwischen 20 bis 30 Jahre besonders beliebt. Generell kann aber gesagt werden, je älter die Personen sind, desto eher werden Nachrichten konsumiert. Bei sozialen Medien wurde neben dem beliebten Facebook auch YouTube und Twitter erwähnt. Auffallend in diesem Bereich ist, dass besonders bei unter 20-Jährigen die sozialen Medien eine wichtige Rolle spielen, nachdem 78% in dieser Alterskategorie (Abbildung C.8) solche Plattformen an der ersten Stelle sehen. Generell gilt jedoch der Trend, je Älter desto weniger werden soziale Medien erwähnt. Vorwiegend sind aber Leute unter 40 Jahre in sozialen Medien vertreten.

Weiters zeigt Abbildung 4.4, dass nicht einmal ein Fünftel (18%) E-Mail-Dienste als regelmäßig benutzte Webservices erwähnt, wobei besonders die älteren Testpersonen diese Dienste noch am ehesten verwenden. 11% aller Befragten geben eine Suchmaschine an den ersten Plätzen an, wobei Google hier eine Hauptrolle einnimmt. Bei Online Shopping (8%) werden hauptsächlich Amazon, eBay und willhaben.at genannt, welche besonders oft von Leuten über

30 erwähnt werden (Abbildung C.8). Überraschend selten werden Netbanking-Dienste (2%) erwähnt. Den Rest bilden sonstige Dienste wie Reiseportale, Schulportale oder Onlinespiele. Abschließend zu Abbildung C.8 sollte noch erwähnt werden, dass vor allem Personen zwischen 30 und 40 Jahre alle genannten Kategorien an Webseiten ausgeglichen oft nutzen. Möglicherweise verfügt gerade diese Altersklasse über die meiste Erfahrung mit dem Internet und versteht es somit am besten, annähernd alle Kategorien an Internetplattformen zu nutzen.

Abschließend zur Analyse der Internetnutzung sollte der Proband eine Schätzung abgeben, bei wie vielen Internetportalen (nicht nur soziale Medien) er registriert sei. Wie Abbildung C.9 zeigt, würden in dieser Frage fast ein Drittel (32%) aller Befragten mehr als 20 Registrierungen schätzen. 70% würden sogar mehr als 5 Konten zählen, die sie mehr oder weniger aktiv verwenden. Somit besitzt die überwiegende Mehrheit der Probanden mehrere Profilkonten, wo sich bei der Benützung des jeweiligen Services persönliche Daten anhäufen.

Nutzung von sozialen Medien

Da in sozialen Medien oft private Details mittels Profilinformationen oder veröffentlichte Postings verraten werden, könnte deren Ausmaß der Nutzung ein weiterer Indikator für den persönlichen Datenschutz sein.

Um dieser Fragestellung näher auf den Grund zu gehen, wird der Proband zunächst nach der Anzahl an Profilen in sozialen Netzwerken gefragt. Die Auswertung von Abbildung C.10 zeigt eindeutig, dass je jünger die Person ist desto eher ist sie in Besitz von mindestens einem Profil in einem sozialen Medium. Speziell Leute unter 30 Jahre geben an, dass sie nur ein Konto betreuen, wobei es sich meist um Facebook handelt. Fast 30% an unter 20-Jähringen geben sogar an, das sie mehr als 3 soziale Benutzerkonten führen, wobei neben Facebook auch diverse Spielplattformen oder YouTube eine Rolle spielen. Auch zwischen 30 und 50 wird oft über mehrere Konten verfügt. Dabei steht aber eher die Pflege beruflicher Beziehungen (Xing, LinkedIn) im Vordergrund.

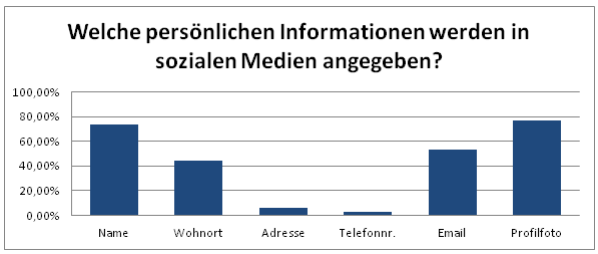


Abbildung 4.5: Persönliche Profilangaben in sozialen Netzwerken

Welche privaten Details in solchen Profilen preisgegeben werden, wird in Abbildung 4.5 dargestellt. Dabei wird gezeigt, dass neben dem Namen und einem Profilfoto auch oftmals der Wohnort und die E-Mail-Adresse angeführt werden. Nur die Angabe von genauer Adresse und Telefonnummer wird in diesem Zusammenhang eher vermieden.

Gebrauch von Suchmaschinen

In diesem Abschnitt wurde die Frage gestellt, wie Suchmaschinen durch den Internet User genutzt werden. Dabei wurde in erster Linie geklärt, welche die beliebteste Suchmaschine ist. Zudem wurde später auf die Suchanfragen selbst eingegangen.

Eine überwiegende Mehrheit von 89% der Befragten (Abbildung C.11) nutzt hauptsächlich Google, wenn sie für ein Thema recherchieren. Am Rande befinden sich auch die Konkurrenten Bing und Yahoo unter den Antworten, diese Plattformen werden aber bei weitem nicht so oft genutzt wie der Platzhirsch Google.

Neben der präferierten Suchmaschine wurden auch Fragen bezüglich der Suchanfragen selbst gestellt. Generell würden die meisten Befragten (94%, Abbildung C.11) ihre Suchbegriffe eher nicht an engere Bekannte, Eltern oder an den Arbeitgeber weitergeben. Offensichtlich besitzen solche Suchterme viel Persönliches, was die Untersuchungsteilnehmer nicht bereit sind zu teilen. Dieser Trend wird durch die Analysen unterstrichen, die in Abbildung C.12 dargestellt sind. Dabei geben fast 60% der Befragten an, sie hätten schon einmal nach einem Thema recherchiert, welche sie explizit nicht Eltern oder Lebenspartner sagen würden. Noch weniger dürfen Arbeitsgeber wissen, da fast 80% der Meinung sind, dass diese Suchanfragen geheim bleiben sollten. Das Stöbern nach Informationen von Freunden und Arbeitskollegen ist hingegen eine gängige Vorgangsweise, behaupten zumindest 80% aller Befragten, die das schon einmal gemacht haben. 50% der Testpersonen bedienen sich sogar regelmäßig dieser Möglichkeit. Demnach ist es sehr empfehlenswert, des Öfteren nach dem eigenen Namen zu suchen, um den hinterlassenen Fußabdruck im Web zu überprüfen. Der Umfrage nach machen dies auch fast 50% regelmäßig. Nur eine Minderheit von 6% gibt an, noch nie Informationen über sich selbst in einer Suchmaschine abgefragt zu haben.

Aktive und passive Nutzung von Webdiensten

In diesem Teilabschnitt der Pretest-Untersuchung wurde der Proband gefragt, ob und in welcher Art und Weise er die verschiedenen Webdienste verwendet. Konkret wird dabei zwischen einer aktiven und passiven Nutzung unterschieden. Eine aktive Nutzung eines Dienstes bedeutet, dass der Internet User aktiv Inhalte veröffentlicht. Am Beispiel Facebook sind solche Inhalte Statusmeldungen oder Profileigenschaften. Bei der passiven Nutzung werden diese Inhalte lediglich gelesen. Dahingehend wurde der Proband zu folgenden Internetdiensten und -plattformen befragt:

- Soziale Medien (z.B. Facebook,...)
- Instant Messaging (z.B. ICQ, Skype,...)
- Fotos (z.B. Flickr,...)
- Videos (z.B. YouTube,...)
- Nachrichten (z.B. orf.at, laola1.at,...)
- Foren (z.B. Gästebücher,...)

- Microblogging (z.B. Tumblr, Twitter,...)
- Musik (z.B. Spotify, Last.fm, ...)
- Dating (z.B. WebSingles,...)
- Reiseportale (z.B. Expedia, eBookers,...)
- Blogs (z.B. Blogger, WordPress,...)
- Shopping (z.B. Amazon,...)
- Enzyklopädien (z.B. Wikipedia,...)

Zwei Drittel aller Befragten (67%, blaue Balken, Abbildung C.13) geben an, dass sie auf Plattformen von sozialen Medien (Facebook, Twitter, ...) nur selten bis gar nie Inhalte posten und damit das Service fast nie aktiv nutzen. Nur knapp ein Drittel gibt an, sich regelmäßig aktiv zu beteiligen. Werden die Antworten über alle Kategorien an Plattformen (rechtes Diagramm, Abbildung C.13) aufkumuliert, so setzt sich dieser Trend fort. In der Summe werden die Dienste kaum aktiv genutzt, es wird eher lesend teilgenommen.

Vertrauen gegenüber IT-Unternehmen

Welche Relevanz Vertrauen im IT-Bereich spielt, versucht der Pretest im Rahmen dieser Sektion festzustellen. Dabei soll der Proband bewerten, wie er den Umgang von personenbezogenen Daten durch bekannte IT-Firmen einschätzen würde. Überdies sollte er die Übermittlung privater Informationen im Internet beurteilen.

Am sichersten fühlen sich die Probanden bei Telekommunikationsanbieter aufgehoben, welche der Umfrage nach zu 80% (Abbildung 4.6) zumindest ein gesundes Maß an Vertrauen erhalten. Microsoft, Apple und Online-Shopping-Firmen (eBay, willhaben.at, Zalando, Amazon) werden dabei mit 60% mindestens ein bedingtes Vertrauen ausgesprochen. Besonders diese Firmen sind unter den Testpersonen gut bekannt und deren Produkte befinden sich fast täglich in ihrer Anwendung (Betriebssystem Windows, iPhone,...). Viele Probanden meinten auf Nachfrage, sie würden es durch die Medien schon erfahren, sollten sich mit deren Produkten Datenschutzprobleme ergeben. Bis dahin wird ihnen ein gewisses Maß an Vertrauen in diesen Bereich gewährt. Am schlechtesten steigt in dieser Statistik Google aus, wo fast zwei Drittel (60%, Abbildung 4.6) aller Befragten dieser Firma ein sehr geringes Vertrauen in Sachen Privatsphäre aussprechen. Womöglich ist diese Einschätzung damit erklärbar, dass viele Internet User besonders viele Google-Dienste (Gmail, Suchmaschine, Android,...) verwenden und somit besonders viele private Daten gespeichert haben.

Weiters wurde in diesem Abschnitt die Frage gestellt, ob die bloße Übermittlung von persönlichen Daten über das Internet (via E-Mail oder persönlicher Nachricht über soziale Netzwerke) problematisch seien. Mit jeweils mehr als 50% (Abbildung C.14) werden Kreditkarten, Bankverbindung, private Adresse und vor allem Reisepassdaten als besonders kritische Daten bewertet. Gegensätzlich ist das Verhalten bei Daten wie E-Mail-Adresse, Name, und Geburtsdaten wie Ort und Datum, die nur von 20% der Befragten als problematisch eingestuft werden.

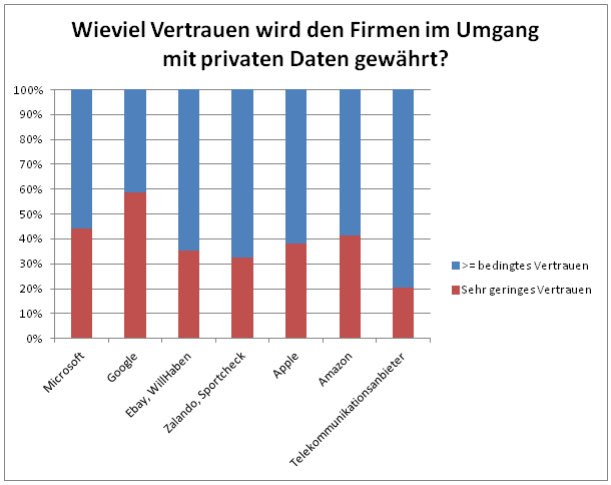


Abbildung 4.6: Vertrauen an IT-Firmen im Umgang mit privaten Daten

Besonders die berufliche Adresse sticht in dieser Umfrage heraus, wobei viele die Übermittlung dieser Information als unproblematisch betrachten würden. Unsicherheiten gibt es vor allem bei Kreditkarten, Bankverbindung und E-Mail-Adresse, wo sich jeweils. 20% nicht sicher sind, wie kritisch die Übermittlung zu bewerten ist.

Fragen zur Vorratsdatenspeicherung

Als Schlusspunkt für den Pretest wurde die Testperson nach der Vorratsdatenspeicherung (VDS) befragt. Dabei sollten die Rahmenbedingungen für diese Regelung eingeschätzt werden und ob sich am Surfverhalten etwas ändern würde.

Der Proband wurde zuerst mit Aussagen konfrontiert, welche auf die Art der betroffenen Daten Bezug nehmen. Wie die Abbildung C.15 zeigt, ist sich knapp die Mehrheit bewusst (jeweils mehr als 50%), dass Metadaten über bestehende Internetverbindungen, einzelne Aufrufe von Internetseiten, Telefongespräche und geografische Standorte immer gespeichert werden. Nur vereinzelt gab es Antworten, wo nur manchmal oder nie diese Daten auf Vorrat angelegt werden. Die Frage nach der Dauer der Speicherung dieser Verkehrsdaten beantworten 58% aller Befragten (Abbildung C.16) so, dass diese für ein Jahr oder gar für immer gespeichert bleiben würden. Nur 30% schätzen die Speicherdauer von einem halben Jahr richtig ein.

Weiters würde zirka ein Drittel aller Befragten (Abbildung 4.7) nichts an ihren Telekommunikationsverhalten ändern, sollte die VDS wirklich alle Verbindungen speichern. Es erklärte sich aber auch niemand bereit, das Verhalten komplett zu ändern. Nur annähernd zwei Drittel (65%) aller Befragten würden minimale Änderungen in Kauf nehmen oder auf mögliche Gefahren und Risiken mehr aufpassen.

Sollte man sich beim Telefonieren gegen die Vorratsdatenspeicherung (VDS) schützen wollen, geben nur 12% (Abbildung C.17) aller Testpersonen an zu wissen, wie dies umzusetzen sei. Dabei gaben viele die Benützung eines Handys einer anderen Person oder ein Wertkarten-Telefon als Antwort. Andere sehen das bloße Unterdrücken der Telefonnummer schon als Schritt

Abbildung 4.7: Änderung des Telekommunikationsverhalten

der Anonymisierung. Immerhin doppelt so viele (24%, Abbildung C.17) glauben nach eigenen Angaben zu wissen, wie der Umgang mit einem Anonymisierungsdienst beim Internetsurfen funktioniert. Dabei würden sie es mithilfe von offenen Proxies, diversen VPN-Diensten oder dem Tor-Netzwerk lösen. Andere würden sich mit der Privat-Einstellung eines Internet Browsers begnügen oder finden sich im Glauben, dass eine HTTPS-Verbindung genug Absicherung sei.

4.2 Ergebnisse der Posttest-Analyse

Dieser Abschnitt widmet sich der Analyse des Posttest, welcher im Rahmen der Untersuchung (Kapitel 2.3) direkt nach der Lerneinheit durchgeführt wurde. Dabei stand die Messung des Lernerfolgs im Mittelpunkt.

Wahrnehmung des Treatments

Im ersten Unterkapitel wird analysiert, wie die Probanden den Vortrag nach eigenen Angaben wahrgenommen haben und welche zusätzlichen Eindrücke gewonnen wurden. Zudem soll der eigene Lernzuwachs eingeschätzt werden und eine Bewertung abgegeben werden, ob die Methodik der nach Lerntypen didaktisch angepassten Lerneinheit geeignet war.

Bei der Einschätzung der Lerneinheit durch die Testpersonen wird vielfach angegeben, dass alles verständlich erklärt wurde und der Lehrstoff sinnvoll aufbereitet war. Ferner hatten alle das Gefühl, dass sie jeden Schritt der Lerneinheit optimal verfolgen konnten und damit ein roter Faden durch den Vortrag gegeben war. Diese Zustimmung gibt ein gutes Zeugnis für die generelle Struktur und Aufbau der Lerneinheit ab.

Weiters wurden die Probanden gefragt, inwieweit sie sich durch die Lerntypen-angepasste Didaktik unterstützt fühlten und ob für sie die richtige Lernmethodik gewählt wurde. Dabei gaben wiederum alle Beteiligten ihre Zustimmung, obwohl es auch Verbesserungsvorschläge gab. Wie die Abbildung C.18 zeigt, wurde fallweise der Wunsch geäußert, noch mehr Videos über das Thema zu sehen, was den zeitlichen Rahmen noch mehr gesprengt hätte. Andere kritisierten die gezeigten Videos selbst oder forderten noch mehr Beispiele und Lösungsansätze für die einzelnen Problemstellungen. Manche gaben auch Einwände an, wobei den Probanden zum Beispiel der Input für die dafür geplante Zeit zu viel war.

Bei der Einschätzung, wie die Testpersonen den Lernzuwachs einschätzen würde, gab eine überwiegende Mehrheit von 71% (Abbildung 4.8) an, dass sie schon einmal von der Problematik gehört hätte, zugleich jedoch viel Neues erfahren hätten. Für 26% aller Befragten war das Thema ein Neuland und sie hörten zum ersten Mal etwas von der Privatsphäre im Internet. Nur ein kleiner Teil von 3% aller Testpersonen fühlte sich schon vor der Lerneinheit aufgeklärt und gab an nur wenig dazugelernt zu haben.

Abbildung 4.8: Einschätzung des Lernzuwachs

Verständnis für den theoretischen Background

Eine besonders wichtige Frage ist, ob sich die Testpersonen die vorgetragen Lehrinhalte auch merken konnten. Um den Posttest nicht allzu lang werden zu lassen, wurden nur stichprobenartig und von jedem Abschnitt der Lerneinheit Fragen gestellt.

Zunächst wurde eine Verständnisfrage bezüglich der beteiligten Akteure beim Internet Surfen gestellt. Dabei sollte der Proband alle richtigen Akteure erkennen, die potentiell beim Surfen mitwirken und die Möglichkeit haben, Informationen über die User zu sammeln. Wie Abbildung C.20 zeigt, erkannten fast alle der Befragten das verwendete Webservice und den Internet Service Provider (ISP) als potentiellen Informationssammler. Auch eindeutig falsche Antworten wie „der Nachbar“, „diverse Freunde“ oder „Familienangehörige“ wurden als richtig erkannt. Wenn es Uneinigkeiten unter den Befragten gab, dann war es beim eigenen Computer und bei diversen Behörden. Fast ein Drittel (29%) sehen den eigenen Computer nicht als potentiellen Informationssammler. Dabei ist gerade diese Instanz mit vielen Risiken behaftet. Durch Viren oder schadhafte Programme kann der User potentiell ausspioniert werden. Die größte Unsicherheit herrschte bei der Frage, ob Behörden über einen Internet User sammeln würden. Obwohl sie nicht direkt über einen User Informationen akquirieren können, sind sie beispielsweise über den Weg der Vorratsdatenspeicherung in der Lage, sensible Daten abzufragen.

Des Weiteren wurde die Definition von Privatsphäre im Internet abgefragt. Dabei sollten die Befragten eine richtige Erklärung (aus 4 möglichen) für diesen Begriff finden. Nur gut zwei Drittel (68%, Abbildung C.20) aller Befragten kreuzten bei dieser Single-Choice Fragestellung die richtige Antwort an. Als nächste Aufgabe musste die Testperson verschiedene Identitätsprofile der realen oder der virtuellen Welt zuordnen. Dabei wurden die virtuellen Profile (blaue Markierung, Abbildung C.20), wie Facebook-Profile oder Suchterme, richtig erkannt. Auch Identitäten, die eher der realen Welt (rote Markierung) zugeordnet werden, sind mit Ausnahmen der Kreditkarte richtig zugeordnet worden. Rund ein Viertel würde die Kreditkarte als virtuelle Identität

sehen. Im Rahmen des Posttests wurden auch Fragen zur Vorratsdatenspeicherung (VDS) gestellt. Dabei wurden hauptsächlich die 2 wichtigsten Fakten abgefragt: Welche Daten davon betroffen sind und wie lange diese vom Telekommunikationsanbieter gespeichert werden. Dass nur Verkehrsdaten (blaue Markierung) und keine Inhalte (rote Markierung) für die VDS relevant seien, wurde weitestgehend richtig erkannt. Auch die Frage nach der Mindestdauer der Speicherung von 6 Monaten wurde von allen richtig beantwortet (Abbildung C.20).

Um den Lehrstoff etwas tiefgehender abzuprüfen, sollten Problemstellungen, die beim Vortrag präsentiert wurden, erklärt werden können. Dazu wurden Schlagwörter genannt und der Proband sollte eine Erklärung in seinen Worten angeben. Damit sollte festgestellt werden, ob und wie die Begriffe verstanden wurden (Abbildung C.19). Den erste Begriff „Browser Tracking“ konnten dabei nur knapp die Hälfte (45%) aller Befragten einigermaßen richtig erklären. Unter der „Search Term Analyse“ konnten sich schon wesentlich mehr Probanden etwas vorstellen. Fast zwei Drittel (64%) gaben eine annähernd richtige Erklärung dafür ab. Zudem ist aus den Antworten zu erkennen, dass durchauch ein Bewusstsein für die Sensibilität von Suchbegriffen vorhanden ist. Überraschend viele Probanden konnten sich den Begriff des „Social Engineering“ verinnerlichen, wobei 73% eine gute Begriffsdefinition gefunden haben. Dabei spielt sicher die Tatsache eine Hauptrolle, dass fast jeder Befragte über ein Facebook-Profil verfügt und somit die Problematik sehr präsent ist. Bei den falschen Antworten war häufig das Problem, das Begriffsdefinitionen nur sehr oberflächlich ausfielen, wobei die Problemstellung merklich nicht verstanden wurde. Mehrfach wurden auch verschiedene Begriffe miteinander verwechselt oder eben gar keine Antwort geliefert.

Anwendung der praktischen Lösungansätze

Bei der Frage, inwieweit die diversen Lösungsansätze verstanden wurden, kann den Probanden ein positives Zeugnis ausgestellt werden. Natürlich brauchten manche Testpersonen etwas mehr Hilfe in der Handhabung der Software-Tools. Jedoch konnten dabei die Handlungsanweisungen teilweise zu 100% erfüllt werden und jeder Schritt wurde zufriedenstellend ausgeführt. Jeder war in der Lage, seine eigene virtuelle Identität in Form von einer IP-Adresse festzustellen und diese mittels CyberGhost hinter einer anderen zu verstecken. Auch die Google-Alternative „DuckDuckgo.com“ wurde von den meisten erfolgreich angewendet.

4.3 Qualitative Erkenntnisse der Lerneinheiten

Direkt nach der Posttest-Messung wurde eine Bewertung der Lerneinheit durch den Vortragenden vorgenommen. Neben quantitativen Kriterien wurden auch eine qualitative Aspekte dokumentiert. Es wurden Aussagen getroffen, inwieweit die Testperson die Konzentration während des Vortrages aufrecht halten konnte und ob sie viele Rückfragen stellte. Bei den praktischen Teilen konnte beobachtet werden, ob die ihnen gestellten Aufgaben leicht gelöst werden konnten oder Hilfe benötigt wurde. Auch sonstige Eindrücke und Beobachtungen wurden durch den Vortragenden festgehalten und dokumentiert.

Über alle Untersuchungen kann der Schluss gezogen werden, dass ausnahmslos alle Probanden grundsätzlich ein hohes Maß an Interesse gezeigt hatten. Es konnte fast immer die Konzen-

tration der Testperson während der Lerneinheit relativ hoch gehalten werden und der Vortrag konnte immer bis zum Ende durchgeführt werden. Naturgemäß war das Interesse und die Neugier zu Beginn der Lerneinheit höher und nahm dann mit der Dauer des Vortrags ab. Wie Abbildung C.21 zeigt, stellten fast 80% aller Probanden dabei überdurchschnittlich viele Rückfragen zu den einzelnen Problemstellungen. Der Rest hörte vielmehr passiv zu und stellte nur selten Fragen.

Ursprünglich war es geplant, dass im Zuge der Lerneinheit alle Software-Tools auf dem PC oder Notebook der Testperson zu installieren. Aus organisatorischen Gründen war dies jedoch nur fallweise möglich und konnte nur bei fast 10% (Abbildung C.22) aller Sessions durchgeführt werden. Die Übungen wurden dann auf dem Notebook des Vortragenden ausgeführt. Trotzdem konnten die praktischen Teilaufgaben beim Posttest oft in Eigenregie gelöst werden. Bei knapp zwei Drittel (Abbildung 4.9) der Fälle brauchte die Testperson keinerlei Unterstützung. Beim Rest musste mehr oder weniger helfend zur Seite gestanden werden und die einzelnen Schritte fallweise mehrmals erklärt werden.

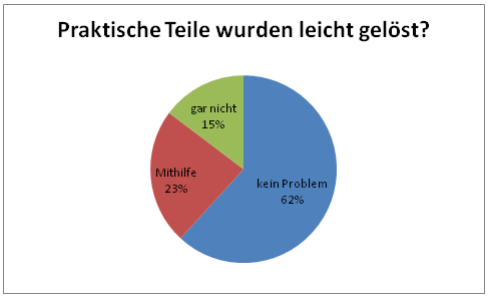


Abbildung 4.9: Lösung der praktischen Teile beim Posttest

Je nach Menge der Rückfragen und Diskussionspunkte variierte die Dauer der einzelnen Untersuchungen stark. Wie die Abbildung 4.10 zeigt, konnten nur 3% aller Lernsessions planmäßig in 60 Minuten abgehalten werden, der Rest dauerte mehr als 90 Minuten. Bei fast einem Viertel aller Lerneinheiten wurden sogar mehr als 2 Stunden benötigt.

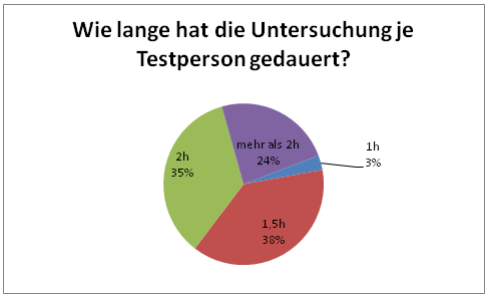


Abbildung 4.10: Dauer der einzelnen Untersuchungen

Wie schon erwähnt, wurde bei der qualitativen Bewertung auch das Verhalten des Probanden aufmerksam beobachtet. Dabei konnten unterschiedliche Verhaltensweise festgestellt und

ungleiche Eindrücke wahrgenommen werden. In den seltenen Fällen (3%, Abbildung 4.10), bei denen die Lerneinheit relativ zügig durchgeführt werden konnte, gab es dafür gute Gründe. Oft nahmen sich die Testpersonen offensichtlich nicht genug Zeit und wollten den Vortrag so schnell wie möglich hinter sich bringen. Dabei wurden wenige Rückfragen während des Vortrags gestellt und die praktischen Anweisungen wurden sehr schnell und ohne etwas zu hinterfragen durchgeführt. Andere Gründe für einen schnellen Verlauf der Untersuchung waren gut informierte Probanden, die sich in diesem Themengebiet rund um das Internet schon gut auskannten. Diese Personen haben nicht viel Neues erfahren, somit auch kaum Rückfragen gestellt.

Andere Testpersonen gaben sich besonders interessiert und stellten während dem Vortrag eine Vielzahl an Fragen. Meist konnten gute und ausführliche Antworten gefunden werden, wobei dadurch die Dauer des Vortrags immer länger wurde. Die Folgen waren Lerneinheiten, die mitunter mehr als 2 Stunden dauerten und der Eindruck des Probanden, dass für die kurze Zeit sehr viel Input gegeben wurde. Um für jede Untersuchung möglichst gleiche Bedingungen zu schaffen, wurde trotzdem versucht, alle geplanten Inhalte der Lerneinheit durchzubringen. Gelegentlich wurden sogar weiterführende Fragen gestellt, welche sich thematisch vom Vortrag etwas entfernten. In diesen Fällen wurde versucht trotzdem Antworten zu finden, um gleich wieder den Anschluss an den Vortrag zu finden.

Ergaben sich fallweise Diskussionen mit der Testperson, konnte oft abgeleitet werden, ob die Lerninhalte wirklich verstanden wurden. Dabei wurde auch ersichtlich, ob das Thema für den Probanden zu komplex wurde und er offensichtlich überforderte wurde. In solchen Fällen fehlte oft grundlegendes Basiswissen rund um das Thema Internet.

Generell konnte aber folgende qualitative Beobachtung gemacht werden. Die jüngeren Testpersonen entgegneten viel Verständnis für den gesamten Themenkomplex rund um die Privatsphäre im Internet. Oft wollten sie sich aber nicht die Zeit nehmen, sich tiefgründig mit der Problemstellung auseinanderzusetzen. Die älteren Probanden brachten das Engagement entgegen, es zu verstehen zu wollen. Sie waren aber oft nicht in der Lage, Gewohnheiten abzulegen und etwaigen Änderungen beim Internetsurfen durchzuführen. Nur Personen, die mit dem Internet aufgewachsen sind und es möglicherweise auch im Beruf häufig nutzen, brachten das Verständnis mit und konnten damit ein entsprechendes Bewusstsein für Datenschutz im Internet entwickeln.

4.4 Langzeitevaluierung der Bildungsmaßnahmen

In diesem Kapitel werden die Ergebnisse der Langzeitevaluierung diskutiert, die im Rahmen der Untersuchung (Kapitel 2.3) durchgeführt wurden. Dabei steht die Evaluierung von langfristigen Veränderungen im Kommunikationsverhalten durch die Bildungsmaßnahmen im Mittelpunkt.

Vermitteltes Wissen langfristig vorhanden?

Um festzustellen, ob die Testperson sich langfristig etwas von den vorgestellten Inhalten merken konnte, werden stichprobenartig Fragen des Posttest herangezogen. Sie werden im Rahmen der Langzeitevaluierung noch einmal gestellt, um so den Vergleich zum Zeitpunkt der Untersuchung zu ziehen.

Zunächst sollten einige Begriffe stichwortartig erläutert werden, die beim Vortrag ausführlich diskutiert wurden. Wie Abbildung 4.11 darstellt, konnten zu mindestens 80% für „Privatsphäre im Internet“, „Virtuelle Identität“ und „Anonym Surfen“ eine nahezu richtige Erklärung liefern. Wogegen Begriffe wie „Browser Tracking“ (40%), „Search Term Analyse“ (60%) und „Social Engineering“ (30%) mehr Schwierigkeiten bereiteten. Sie konnten oft nur sehr oberflächlich erklärt werden oder eben gar nicht. Nur durch kleine Hilfestellungen konnten sich diese Personen an die jeweilige Problemstellung erinnern.

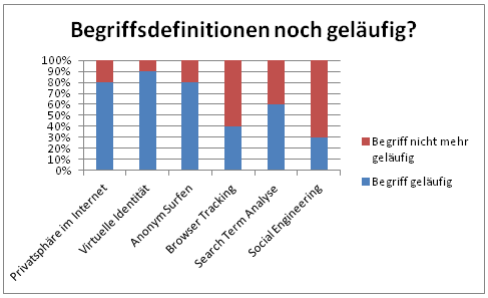


Abbildung 4.11: Erklärung von Begriffen

Nach den eher offenen Fragestellungen wurde der aktuelle Wissensstand für das Fallbeispiel der Vorratsdatenspeicherung (VDS) ermittelt. An die Tatsache, dass die Daten für mindestens 6 Monate gespeichert werden würden, konnten sich auch nach ein paar Monaten alle erinnern. Wie die Abbildung C.23 zeigt, konnte auch die Frage nach der Art der Daten oft richtig beantwortet werden. Die meisten Befragten wussten noch die Grundregel, dass nur Verkehrsdaten und keine Inhalte gespeichert werden.

Im Unterschied zu den Ergebnissen des Posttests (Abbildung C.20) gab es bei der Langzeitevaluierung Unsicherheiten, ob die IMEI-Nummer (Gerätekennungsnummer) eines Handys bei der VDS mitgespeichert werden würde.

Berührungspunkte mit Privatsphäre im Internet

Der nächste Abschnitt der Langzeitevaluierung will etwaige Berührungspunkte des Probanden mit der Thematik festhalten. Dabei wurde gefragt, ob sich irgendwann nach dem Vortrag eine Situation ergeben hätte, in welcher er vorgestellte Inhalte anwenden konnte. Diese Frage beantworten 80% aller Befragten (Abbildung C.24) mit einer Zustimmung. In diesem Zusammenhang wurden unter anderen oft die User-angepassten Werbeeinschaltungen von Amazon und Zalando genannt, bei welchen sich viele Testpersonen manchmal verfolgt fühlten. Bei dieser Problemstellung fragten die Probanden mehrfach nach möglichen Gegenmaßnahmen nach. Weitere Berührungspunkte ergaben sich bei der Erstellung von Benutzerkonten für diverse Internetdienste sowie bei der Veröffentlichungen von verschiedenen Postings in sozialen Netzwerken. In beiden Fällen waren die Probanden mit der Offenlegung von privaten Informationen konfrontiert. Durch die alleinige Erwähnung dieser Situationen kann prinzipiell ein gesteigertes Bewusstsein für die Problematik festgehalten werden. Nachdem viele Probanden die vorgestellten Tools während der Lernsession nicht am eigenen Rechner ausprobiert hatten, holten dies einige an einem

späteren Zeitpunkt nach. Dabei wurden gleichzeitig eigene Erfahrungen mit den Tools in Eigenregie gewonnen und nützliche Software-Tools zum täglichen Gebrauch installiert. In diesem Zusammenhang wurde mehrfach das freie VPN-Tool „CyberGhost“, die alternative Suchmaschine „DuckDuckgo.com“ und das „DNTM-Plug-In“ genannt.

Nach dem eher praktischen Austausch wurde der Proband ferner gefragt, ob er inzwischen in etwaige Diskussionen rund um das Thema Datenschutz im Internet verwickelt worden sei. Wie Abbildung C.24 zeigt, haben dies 60% aller Befragten bejaht. Dabei wurden wiederum auffällig oft die User-angepassten Werbungsbanner erwähnt, die Grund für die daraus resultierenden Diskussionen war. Auf Nachfrage erwähnten viele, dass sie das durch den Vortrag gehörte Wissen auch ins Gespräch einfließen lassen konnten. Mehrmals wurde dabei auf weitere Gefahren und Risiken hingewiesen. Weitere Diskussionspunkte war unter anderem auch, was und wie viel auf Facebook durch Jugendliche sowie auch Erwachsene gepostet wird. Oft wurde dabei die Frage gestellt, wie Kindern und Jugendlichen der Datenschutz bewusst gemacht werden kann.

Auch zum Fallbeispiel Vorratsdatenspeicherung (VDS) wurde nach Berührungspunkte gefragt. Eine überwiegende Mehrheit von 70% (Abbildung C.24) meinte, sie hätten seit dem Vortrag von der VDS nichts mehr gehört. Die Meisten beklagten dabei die fehlende Medienpräsenz dieses Themas. Die restlichen 30% nahmen in sozial Netzwerken etwas wahr oder recherchierten selbst im Internet über das Thema.

Veränderungen und Bewusstseinbildung durch Bildungsmaßnahmen

Im letzten Abschnitt der Langzeitevaluierung wird ermittelt, welche Veränderungen sich im Umgang mit dem Internet durch die Bildungsmaßnahme ergeben haben und ob ein Bewusstsein für Datenschutz langfristig geschaffen wurde.

In diesem Zusammenhang wurde der Proband zunächst gefragt, ob er sich seit dem Vortrag beim Internetsurfen in Situationen befunden hat, in welchen er lieber anonym aufgetreten wäre. Wie Abbildung C.25 darstellt, stimmten dabei 60% aller Befragten dieser Frage zu. Dabei wurden Situationen aufgezählt, wo übers WLAN im Hotel ins Internet gestiegen oder Recherchen über Krankheiten eingeholte wurde. Dabei musste aber von den meisten eingeräumt werden, das es letztendlich zu umständlich und kompliziert gewesen war, sich einen Anonymisier zuzulegen. Bequemlichkeitshalber beließ man es bei Status Quo und nutzte einfach die ungeschützte Internetleitung. Weitere Aufzählungen waren Situationen, wobei ein Internetdienst von einem anderen Land genutzen werden sollte, welcher jedoch für ausländische Nutzer gesperrt war. Auch für Download und Streaming von Filmen würden sich die Untersuchungsteilnehmer mit einem Anonymisierungsdienst wohler fühlen.

Nachdem im Vortrag, wobei unter anderem die Rolle der sozialen Netzwerken in Bezug auf Datenschutz ausführlich diskutiert wurde, wurde die Testperson im Rahmen der Langzeitevaluierung nach der Prüfung der Privatsphäre-Einstellungen gefragt. Dabei gaben 70% der Probanden an (Abbildung C.25), dass sie diese nach der Lerneinheit einem Check unterzogen haben. Die meisten würden dies ohnehin regelmäßig überprüfen.

Die Entwicklung eines Bewusstseins für den Umgang mit privaten Daten im Internet war ein primäres Ziel der Lerneinheit. Nach etwa 2-3 Monaten nach der Lerneinheit gaben 80% aller Probanden (Abbildung C.25) an, dass sie sich gerade nach dem Vortrag mehr Gedanken machen würden, welche privaten Details sie im Internet angeben oder öffentlich publizieren.

Als Beispiel dafür erwähnen die Probanden vielmals den Umgang mit Facebook. Einige würden sich demnach zumindest Gedanken machen, welche möglichen Folgen ein Posting haben könnte und welche privaten Details dabei veröffentlicht werden. Andere gaben wiederum an, sich nicht mehr Gedanken darüber zu machen als vor der Lerneinheit, sodass sich daraus keine Änderung am Verhalten ergeben habe.

Ob die Probanden ihr Surfverhalten verändert hätten, wird zu 90% mit „nein“ beantwortet, wie die Abbildung C.25 entsprechend darlegt. Es kam mehrfach die Begründung, dass es zu umständlich sei, Anonymität zu erreichen. Man sei zu bequem, um sich langfristig eine Lösung wie „CyberGhost“ dauerhaft einzurichten.

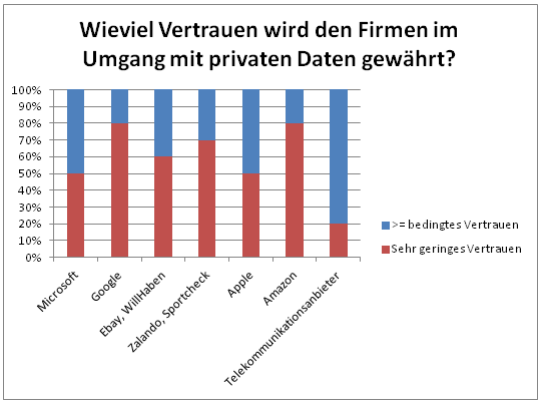


Abbildung 4.12: Vertrauen in IT-Firmen im Umgang mit privaten Daten

Welches Vertrauen in IT-Firmen im Umgang mit privaten Daten (Name, Adressen, Kontaktinformationen,...) gesetzt wird, wurde schon im Rahmen des Pretest ermittelt (Kapitel 4.1). Diese Frage wurde nun ein paar Monate nach der Lerneinheit noch einmal gestellt, um festzustellen, welche Auswirkung die Aufklärung in Form der Lerneinheit zur Folge hatte. Im Vergleich wird schnell die Erkenntnis gewonnen, dass das Misstrauen verstärkt wurde. Vielen Firmen wurden nach den Bildungsmaßnahmen mit teilweise über 70% (Abbildung 4.12) nur mehr die niedrigste Kategorie an Vertrauen ausgesprochen. Auffällig ist, dass gerade Online Shops wie Amazon, Zalando oder Sportcheck prozentuell am meisten Vertrauen einbüßen, wobei das Problem möglicherweise direkt mit den User-angepassten Werbeeinschaltungen zusammen hängt. Firmen wie Apple und Microsoft, deren Produkte sehr intensiv im Alltag benutzt werden, verlieren dahingehend nur leicht. Einzig den Telekommunikationsanbietern wird weiter konstant mit 80% (Abbildung 4.12) ein Mindestmaß an Vertrauen geschenkt.

KAPITEL 5

Schlussfolgerung und Ausblicke

5.1 Diskussion über zentrale Ergebnisse

Bestandsaufnahme: Bewusstsein für Privatsphäre im Internet vorhanden?

Nachdem es eine Zielsetzung der Untersuchung war, eine Bestandsaufnahme rund um das Thema Privatsphäre im Internet zu ermitteln, versucht dieses Kapitel die Ergebnisse des Pretest aus Kapitel 4.1 zu diskutieren. Weiters werden Aussagen getroffen, die aus der Analyse der Voruntersuchung geschlossen werden konnten, um anschließend mögliche Erkenntnis und Verbesserungsvorschläge für die Bildungsmaßnahmen abzuleiten.

„Datenschutz wichtig – Daten werden trotzdem preisgegeben“

Aus der Analyse der Pretest-Antworten kann der Schluss gezogen werden, dass das Thema Privatsphäre im Internet nur bedingt im Bewusstsein der Probanden vorhanden ist. Oft wird das Thema des virtuellen Datenschutzes auf die Privatsphäre-Einstellungen von Facebook reduziert, sodass nur in diesem Bereich die sensible Informationsoffenlegung von privaten und persönlichen Daten wahrgenommen wird. Eine weitere Meinung der Probanden, die in diesem Zusammenhang geäußert wurde, ist, dass es im Internet keine Privatsphäre gäbe und diese in der virtuellen Welt sowieso aufgegeben werden müsse. So zeigt die Untersuchung weiters, dass Webdienste wie Google-Suchmaschine, Facebook und Co. trotzdem sehr beliebt sind und häufig genutzt werden. Die Erkenntnis liegt nahe, dass diese Webdienste genutzt werden, obwohl die User potentielle Gefahren bereits vermuten. Dabei sind ihnen die langfristigen Konsequenzen offenbar nicht bewusst. Auch ein weiteres Indiz stellt das Bewusstsein der Untersuchungsteilnehmer für Datenschutz im Internet sehr infrage. Nur zirka die Hälfte der Testpersonen kann mit den Begriffen wie „virtueller Identität“ oder „Vorratsdatenspeicherung“ etwas anfangen. Zumindest in diesem Bereich fehlt das Wissen, dass alle Internetaktivitäten möglicherweise beobachtet werden und daraus Userprofile erstellt werden.

Direkt nachgefragt, kristallisiert sich entgegen der vorigen Aussagen jedoch eine überwiegende Mehrheit heraus, bei der prinzipiell Datenschutz im Internet an Bedeutung gewinnt. Aus

der Pretest-Analyse konnte der Eindruck gewonnen werden, dass den Probanden einfach das Wissen fehlt, wo genau Informationen preisgeben werden und in welchen Bereichen sie aufpassen müssen. Diese Erkenntnis wird besonders in Abbildung C.3 unterstrichen, wobei die Mehrheit nicht der Meinung ist, selbst mehr private Informationen im Internet preiszugeben als in der realen Welt. Dass dem nicht so ist, zeigt unter anderem eine aktuelle Erhebung des Cybercrime-Competence-Center des Bundeskriminalamtes, welche ebenfalls besagt, dass die Risiken im Internet unterschätzt werden. Keiner würde im Alltag einem Unbekannten private Fotos, Telefonnummer oder die Wohnadresse verraten. Im Internet würde das aber oft passieren [22]. Daher ist es nicht verwunderlich, dass nur ein kleiner Teil aller Befragten (15%) angibt, ihre Internetaktivitäten mit geeigneten Software-Tools zu verschleiern.

Das fehlende Bewusstsein für die unabsichtliche Informationsoffenlegung wird weiters durch die Fragestellung nach der Zusammensetzung von Benutzernamen unterstrichen. Dabei werden oft persönliche Details (Vornamen, Nachname, Geburtsdatum,...) genutzt, anstatt dafür Pseudonyme zu verwenden. Wie schon in der Analyse erwähnt, könnte aus diesen zusammengesetzten Datenschnipseln durchaus auf eine reale Person geschlossen werden. Dass diese und andere sensiblen Informationen für die weitere Verarbeitung und Auswertungen durch Dritte verwendet werden, geben die Teilnehmer der Untersuchung grundsätzlich ihre Zustimmung. Somit erscheint es klar, dass diese Daten für angepasste Werbung, Verbrechensbekämpfung, Versicherungsprofile oder Nachstellen (Stalking) potentiell verwendet werden können.

Auch die Verantwortung für den eigenen Datenschutz sehen viele Probanden nicht unbedingt bei sich selbst. Nach den Antworten des Pretests gäbe es viele andere Instanzen, die auf den Datenschutz und Privatsphäre im Internet achten müssten, was auch durchaus wünschenswert für den unkundigen Internet User wäre. In diesem Zusammenhang ist zu erwähnen, dass der Umgang mit personenbezogenen Daten oft durch nationale Gesetzgebung wie beispielsweise dem österreichische Datenschutzgesetz [23] geregelt wird. Die Betreiber von Webdiensten sind jedoch in den unterschiedlichsten Ländern stationiert, wodurch die nationalen Regelungen oft unterlaufen und ausgehebelt werden. Somit ist und bleibt letztendlich der Internet User selbst dafür verantwortlich, die eigene Privatsphäre im Internet zu schützen.

Zusammenfassend kann gesagt werden, dass in dieser Diskussion sehr oft aufgezeigt wird, wie unsicher und kontrovers sich die Teilnehmer rund um diesem Thema verhalten. Einerseits will der durchschnittliche Internet User nicht auf die Nutzung bestimmter Webservices verzichten, andererseits ist ihm der Schutz der Privatsphäre im Internet prinzipiell wichtig. Ferner ist festzuhalten, dass dem User einfach oft das Wissen fehlt, in welchen Situationen und unter welchen Umständen sensible Informationen offengelegt werden. Daher wird es im Rahmen von Bildungsmaßnahmen wichtig sein, zum Einen Aufklärung darüber zu betreiben, in welchen Bereichen private und persönliche Informationen unabsichtlich offengelegt werden, und zum anderen Möglichkeiten aufzuzeigen, wie die eigene Privatsphäre in der virtuellen Welt geschützt werden kann.

„Internetsurfen – egal ob mich wer beobachtet – Hauptsache Internetsurfen“

Auch der Internetzugang selbst ist relevant für die Privatsphäre. Die Untersuchungsteilnehmer geben beim Pretest an, dass sie das Internet hauptsächlich für das Konsumieren von Nachrichten, für die Interaktion in sozialen Netzwerken und das Lesen von E-Mails nutzen. Dabei in-

teressieren sich jedoch immer mehr Mittelsmänner dafür, wofür das Internet genutzt wird und welche Aktivitäten in diesem Zusammenhang durchgeführt werden. Ferner wurde in der Pretest-Analyse ermittelt, dass oft der Internetzugang zuhause oder am Mobilgerät genutzt wird. Bei dieser Art der Internetverbindung wird davon ausgegangen, dass eine direkte Verbindung zum Internet Service Provider (ISP) besteht. Obwohl diese Betreiber durch die gesetzliche Regelung der Vorratsdatenspeicherung angehalten sind, Verkehrsdaten mitzuspeichern, gibt es in dieser Verbindung keine anderen Instanzen, die unkontrolliert Daten über Internetsurfer sammeln können. Die Probanden geben jedoch auch häufig an, dass sie den Internetzugang in der Arbeit, bei diversen WLANs (Hotels, Cafés,...) oder in Bildungseinrichtungen (Schule oder Universität) suchen würden. In diesem Fall gibt es jeweils eine Instanz, die die Möglichkeit hat, jede Aktivität zu beobachten und aufzuzeichnen. Diese gesammelten „Logs“ könnten später unter Umständen gegen den Internet User verwendet werden. Gerade in diesen Fällen würde eine verschlüsselte Verbindung, beispielsweise via VPN-Service, helfen, den eigenen Internetverkehr gegen solche Mittelsmänner abzusichern. Ob dieses gefährliche Potential durch den Internet User wahrgenommen wird, darf bezweifelt werden. Denn oft überwiegt das Bedürfnis, das Internet zu nutzen, wenn es gebraucht wird und die Funktionalität gegeben ist.

Auch im Zuge der Nutzung des Internets gaben drei Viertel der Befragten an, sie würden mehr als 5 Registrierungen bei verschiedenen Diensten im Web besitzen, bei welchen sie eindeutig via Benutzernamen und Passwort identifiziert werden können. Somit besitzt eine überwiegende Mehrheit Benutzerkonten, wodurch ihr Verhalten, Kommunikation oder Aktivitäten potentiell aufgezeichnet wird. Daraus kann ein Profil erstellt werden, welches später eindeutig einem User oder einer realen Person zugeordnet werden könnte. Auch in Anbetracht dessen, dass Zugangsdaten oft Ziel von Cyberkriminalität werden [24], sollte genau geachtet werden, welche Informationen bei solchen Konten offengelegt werden.

Die Möglichkeiten des User Trackings sollten daher besonders durch den Internet User wahrgenommen werden, um so den persönlichen Datenschutz zu bewahren. Speziell bei der Lerneinheit sollten den Probanden mögliche Konsequenzen bewusst gemacht werden, mit welcher Art des Internetzuganges gesurft wird und welche sensiblen Informationen bei registrierten Webdiensten offengelegt werden.

„Soziale Medien sind besonders Privacy-relevant – über alle Altersgruppen“

Die sozialen Netzwerke sind in den letzten Jahren bezüglich Privatsphäre im Internet immer relevanter geworden. Das große Bedürfnis, Statusmeldungen von sich zu geben, Fotos zu teilen oder persönliche Details bekanntzugeben, stellt oft eine große Herausforderung für den eigenen Datenschutz dar. Wie die Pretestanalyse zeigt, setzen die Teilnehmer der Untersuchung diesen Trend fort, indem sie ebenfalls häufig vollständigen Namen, Profilfoto, Email-Adresse und Wohnort bei einem Profil eines sozialen Mediums angeben.

Ferner spielt bei den jungen Leuten nicht nur Facebook eine Hauptrolle, es wird auch in Twitter, Youtube und in verschieden virtuellen Spielen mit anderen Personen interagiert. Dabei sind gerade Personen der jüngeren Altersklassen, denen langfristige Konsequenzen der Internetnutzung oft nicht bewusst sind, gut beraten, nicht allzu viel in diesen Medien preiszugeben. Denn Personalchefs gehen immer mehr dazu über, Facebook-Profile zu studieren. Aber auch Wissenschaftler interessieren sich offensichtlich für diese Daten, und haben Tools für Persönlichkeits-

tests entwickelt. Dabei können sexuelle Ausrichtung und politische Orientierung durch die Auswertung von Bilder, Gefällt-mir-Angaben, Gruppen und Freunde vorhergesagt werden [25]. Je älter allerdings die Untersuchungsteilnehmer sind, desto weniger Registrierungen nehmen sie in soziale Medien vor. Was nicht heißt, dass ältere Personen soziale Netzwerke nicht verwenden würden. Denn neben Facebook tendiert die ältere Generation eher zu aktiven Konten bei LinkedIn und Xing. Allerdings werden dabei eher Berufsbeziehungen gepflegt.

Aus diesen Erkenntnissen ergibt sich der Schluss, dass soziale Netzwerke für jede Altersgruppe Datenschutz-relevant ist und jeder ein Bewusstsein für mögliche kurz- und langfristige Konsequenzen von Postings oder Veröffentlichung von privaten Details entwickeln sollte.

„Google immer und überall“

Mit den ungewollten Enthüllungen im Zusammenhang mit der eingestellten Suchmaschine von AOL nahm die Informationstechnologiebranche erstmals wahr, dass Suchterme durchaus relevant für die Privatsphäre sind. Diese Erkenntnis kann auch aus den Ergebnissen dieser Untersuchung abgelesen werden, wobei die Teilnehmer zum größten Teil Suchbegriffe nur ungern mit Eltern, Arbeitgeber oder Freunden teilen wollen würde. Dieses Analyseergebnis ist somit ein guter Indikator dafür, dass diese Suchanfragen einen hohen Informationsgehalt an persönlichen und privaten Details der User besitzen.

Auch das Stöbern nach Informationen über andere Personen (Freunde, Jobwerber,...) wird mit 80% Zustimmung als gängige Praxis gesehen. Zudem ist es dann doch überraschend, dass viel weniger Personen (50%) angeben, den eigenen Fußabdruck im Web zu prüfen. In Anbetracht dessen, dass Google von der überwiegenden Mehrheit (90%) benützt wird, muss an dieser Stelle festgehalten werden, dass dieses IT-Unternehmen allein von den Suchanfragen über die Zeit Unmengen an sensiblen Informationen ansammelt und damit für die Privatsphäre des Internet User immer relevanter wird.

Daher wird es im Rahmen von Bildungsmaßnahmen wichtig sein, ein Bewusstsein für die Sensibilität von Suchanfragen bei den Probanden zu schaffen. Zudem sollte darauf hingewiesen werden, den eigenen Fußabdruck im Web mit Google Search mehrmals und regelmäßig zu kontrollieren.

„Inhalte konsumieren anstatt publizieren“

Im Rahmen des Pretests wurde auch untersucht, in welcher Art und Weise die Probanden Webdienste der unterschiedlichsten Kategorien verwenden. Dabei kann zusammenfassend gesagt werden, dass die User eher lesend Webdienste verwenden und eher selten aktive Inhalte publizieren. Angesichts der Analysefähigkeit von Klicks und der Verfolgung von Useraktivitäten ergeben sich trotzdem Datenschutz-relevante Bedenken, die dem Probanden in der Lerneinheit zu vermitteln sind [25].

„Viel Misstrauen gegebenüber IT-Unternehmen – trotzdem werden deren Produkte verwendet“

Geht es nach den Analyseergebnissen, wird den IT-Firmen nur bedingt Vertrauen im Umgang mit personenbezogenen Daten geschenkt. Nach den Antworten der Untersuchungsteilnehmer wird in diesem Bereich häufig darauf vertraut, dass Missstände in Bezug auf Privatsphäre von

IT-Produkten in den Medien schon wahrgenommen werden. In diesem Zusammenhang ergeben sich jedoch zwei Auffälligkeiten. Überdurchschnittlich viel Vertrauensvorschuss im Umgang mit sensiblen Daten bekommen Firmen, die einen Internetzugang anbieten, die sogenannten Internet Service Provider (ISP). Dabei passiert durch die Vorratsdatenspeicherung gerade in diesem Bereich ein tiefer Eingriff in die Privatsphäre. Am anderen Ende der Fahnenstange erhält das IT-Unternehmen Google besonders wenig Vertrauen, obwohl beispielsweise Dienste wie Suchmaschine oder Gmail von Google sehr beliebt unter den Untersuchungsteilnehmern sind. Aus diesen Erkenntnissen wird abermals sichtbar, wie kontrovers die Gedankengänge der Untersuchungsteilnehmer zum Thema Privatsphäre im Internet sind.

Auch der eigene Umgang ist durchaus unterschiedlich zu bewerten. Kreditkartennummer, Bankverbindung, private Wohnadresse und Reisepassinformationen werden richtigerweise als kritische Komponenten eingestuft, welche nur ungern über unverschlüsselte Kanäle weitergegeben werden würde. Namensangaben, Email-Adresse, Geburtsdaten und vor allem Firmenadresse werden jedoch durch die Befragten als unproblematisch in Bezug auf die eigene Privatsphäre eingestuft. Werden die Daten jedoch im geeigneten Kontext gesehen, können auch daraus weitere Informationen abgeleitet werden, sodass über eine reale Person weitere sensible Informationen akquiriert werden könnten. In diesem Zusammenhang kann den Untersuchungsteilnehmern durchaus eine falsche Wahrnehmung unterstellt werden, wie sie den Sachverhalt einschätzen würden und letztendlich den eigenen Umgang mit sensiblen Daten pflegen.

In dieser Angelegenheit ist den Probanden zu vermitteln, dass ein sensibler Umgang mit persönlichen Daten unumgänglich für den Schutz der eigenen Privatsphäre ist. Besonders die Übermittlung von problematischen Informationen wie Kreditkartennummer oder Kontonummer sollte nur über gesicherte und damit verschlüsselte Kanäle erfolgen. Andernfalls könnten andere Instanzen (Betreiber des Webservices, Mittelsmänner,...) diese Daten abfangen und gegen den User verwenden.

„Vorratsdatenspeicherung – Was ist das?“

Durch die gesetzliche Regelung der Vorratsdatenspeicherung wird jeder Internet Service Betreiber verpflichtet, jegliche Verkehrsdaten der Telekommunikation seiner Klienten mitzuspeichern und für mindestens 6 Monate aufzubewahren. Bei der Analyse der Pretest-Antworten kann die Erkenntnis gewonnen werden, dass bei weitem nicht jedem Internet User bewusst ist, dass es diese Regelung gibt und schon gar nicht was dabei passiert. Dass dabei jede Internetaktivität beobachtet wird und dadurch ein tiefer Einschnitt in die Privatsphäre passiert, scheint durch die meisten Untersuchungsteilnehmer nicht wahrgenommen zu werden.

Aber auch bei der Vorstellung solch einer Regelung würde sich überraschenderweise ein Drittel aller Befragten dafür aussprechen, nichts am Surfverhalten zu verändern. Der Rest würde zumindest minimale Veränderung hinnehmen, um so pro-aktiv manche Aktivitäten im Internet zu verschleiern. Somit ist festzuhalten, dass zumindest nicht allen Internet Usern bewusst ist, welche Konsequenzen dieser Einschnitt in die Privatsphäre langfristig mit sich bringt.

Somit wäre es wichtig, dass im Rahmen von Bildungsmaßnahmen die Regelung der Vorratsdatenspeicherung genau erklärt und hingewiesen wird, welche Daten davon betroffen sind. Bei den Probanden sollte ein Bewusstsein dafür geschaffen werden, welche Konsequenzen diese Regelung für die Privatsphäre hat.

Lernerfolg des Lerntypen-angepasste, didaktischen Models

Eine weitere Zielsetzung dieser Arbeit war es, den Lernerfolg der getroffenen Bildungsmaßnahme zu ermitteln. Dieses Kapitel versucht die Ergebnisse des Posttests 4.2 aufzugreifen und zu diskutieren. Meist ergeben sich daraus mögliche Verbesserungspotenziale für die Lerneinheit, sodass die Inhalten noch effizienter vorgestellt werden können.

„Vortrag gut, aber bitte erzähl mir was neues“
Durch die Messung des Posttests wurde der Proband gleich nach der Bildungseinheit befragt, wie er diese wahrgenommen hat. Dabei gaben alle Testpersonen an, dass die Inhalte verständlich erklärt wurden und dem didaktischen Aufbau gut gefolgt werden konnte. Auch die Anpassung nach dem Lerntyp wurde durchwegs positiv wahrgenommen. Der Großteil der Probanden gab jedoch an, die Problematik zu kennen. Sie hätten trotzdem viele neue Details kennengelernt und verschiedene Zusammenhänge verstanden. Nur für ein Viertel der Untersuchungsteilnehmer war das Thema ein komplettes Neuland.

Als Verbesserungspotential für die Lerneinheit sollte vorher der Bildungsstand über die Thematik ermittelt werden. Dadurch könnten die vorgetragenen Inhalte so abgestimmt werden, dass der Proband nicht über- oder unterfordert wird.

„Nicht alles kann man sich gleich beim ersten Mal merken“
Obwohl dem Großteil der Untersuchungsteilnehmer das Thema zumindest bekannt war, zeigt die Messung des Lernerfolges ein eher differenzierteres Bild. Die stichprobenartigen Fragen nach Inhalten konnten trotz vernachlässigbarer Unsicherheit mehrheitlich richtig beantwortet werden. Sollten die Teilnehmen jedoch vorgestellte Anwendungsfälle genauer erklären, kamen die ersten Schwierigkeiten zum Vorschein. Erklärungen von Browser Tracking (45%), Search Term Analyse (64%) und Sozial Engineering (73%) konnten wirklich nur zum Teil richtig beantwortet werden.

Daraus lässt sich schließen, dass kompliziertere Themen schwierig zu verstehen waren. Eine mögliche Erkenntnis wäre, dass die bloße Vorstellung der potentiellen Gefahr für die Privatsphäre nicht genügt. Möglicherweise sollte dies mit praktischen Beispielen mehr unterlegt werden, um so das Verständnis zu erhöhen und mögliche Konsequenzen direkt aufzuzeigen.

„Richtige Anwendung der Softwaretools – ein Klax“
Dass praktische Übungen gut ankommen, beweist der letzte Teil des Posttests, wobei die praktischen Lösungsansätze in Eigenregie durchgeführt werden mussten. Dabei wurden diese zu 100% richtig umgesetzt und es konnten die gezeigten Software-Tools richtig angewendet werden. Fazit aus dieser Analyse ist, dass praktische Übungen durch die Probanden sehr gut angenommen wurden. Es wäre anzudenken, im Rahmen von Bildungsmaßnahmen noch mehr praktische Beispiele zu den einzelnen Fallbeispielen anzubieten, um so das Verständnis und auch das Interesse gezielt zu forcieren.

Langfristige Veränderungen durch Bildungsmaßnahmen

Als letzte Zielsetzung nimmt sich die Untersuchung der Frage an, welche langfristigen Veränderungen durch Bildungsmaßnahmen erzielt wurden. Dabei werden die Ergebnisse der Langzeitevaluierung im Kapitel 4.4 aufgegriffen und mögliche Erkenntnisse daraus geschlossen.

„Oberflächliches Wissen langfristig gemerkt - bitte nicht in die Tiefe gehen“
Auch bei der Langzeitevaluierung ist festzustellen, dass sich die Teilnehmer das vorgestellte Wissen nur oberflächlich gemerkt haben. Wird jedoch genauer nachgefragt, so ergaben sich einige Unsicherheiten. Beispielsweise konnten Begriffe wie Privatsphäre, virtuelle Identität und anonymes Surfen stichwortartig meist richtig erklärt werden, auch Grundzüge der Vorratsdatenspeicherung konnten gut wiedergegeben werden. An komplizierte Themenbereiche wie Browser Tracking, Search Term Analysis oder Social Engineering konnten sich die Untersuchungsteilnehmer langfristig jedoch nicht mehr erinnern.

Bezüglich der Lerneinheit ist natürlich zu hinterfragen, warum die eher komplizierteren Fallbeispiele nicht wiedergegeben werden konnten. Als Konsequenz dieser Erkenntnis sollten diese Inhalte womöglich noch gezielter anhand praktischer Übungen erklärt werden, damit die Probanden diese komplexen Inhalte besser verstehen.

„Berührungspunkte beim Internetsurfen und Diskussionen – nie wieder etwas von Vorratsdatenbank gehört“
In der Zeit nach der Lerneinheit nahmen die Teilnehmer verschiedene Berührungspunkte mit dem Thema Privatsphäre im Internet wahr. Dabei wurden oft die User-angepassten Werbebanner, Angaben von sensiblen Daten bei diversen Nutzerkonten und veröffentlichte Postings auf soziale Medien erwähnt. An diesem Punkt kann festgehalten werden, dass sich die Lerneinheit als sinnvoll erwies. Nachdem sich offensichtlich die Teilnehmer vermehrt Gedanken darüber machen, welche sensiblen Datenschnipsel über sie potentiell veröffentlicht werden und welche möglichen Konsequenzen dies nach sich ziehen kann, ist ein Bewusstsein für die Materie festzustellen und als Erfolg der Lerneinheit zu werten.

Ferner gaben die Teilnehmer an, dass sie in Eigenregie die vorgestellten Software-Tools ausprobiert haben. Auch daraus kann geschlossen werden, dass zumindest Interesse durch die Lerneinheit beim Probanden für die Thematik geweckt werden konnte. 60% aller Testpersonen gaben weiters an, in verschieden Diskussionen rund um das Thema Privatsphäre im Internet teilgenommen zu haben. Somit konnte das gelehrte Wissen an diesen Gesprächen zumindest an Dritte weitergegeben werden und ist ebenfalls als Erfolg der Bildungsmaßnahme einzustufen.

Eher überraschend gab bei der Analyse der Langzeitevaluierung die Mehrheit der Untersuchungsteilnehmer an, nichts mehr über die Vorratsdatenspeicherung gehört zu haben. Wenn sich die Probanden nicht selbst dafür interessiert hätten, hätte es keine Berührungspunkte mit diesem tiefen Einschnitt in die Privatsphäre gegeben.

„Anonymität gewünscht – aktive Anwendung der Software-Tools unerwünscht“
In der Zeit nach der Lerneinheit gab es laut Probanden mehrere Situationen, in der sie sich Anonymität beim Internetsurfen gewünscht hätten. Es wurde jedoch eine überraschende und interessante Aussage durch die meisten Probanden getroffen, warum sie letztlich nichts unter-

nommen haben, um Anonymität zu erreichen. Viele gaben schlichtweg an, es wäre ihnen zu kompliziert und zu aufwändig, sich ein geeignetes Software-Tool zu installieren, um so die eigene Privatsphäre zu schützen. Eine Erkenntnis daraus ist, dass eine Anonymisierungssoftware keinen Aufwand beim Internet User verursachen darf, ansonsten wird sie nicht genutzt.

Die überwiegende Mehrheit hat auch angegeben, sich generell mehr Gedanken darüber zu machen, welche sensiblen Informationen im Internet preisgegeben werden. Auch dieses Faktum kann als Erfolg der Bildungsmaßnahme gewertet werden. Offensichtlich wurde dadurch ein Bewusstsein aufgebaut, welches die Teilnehmer für dieses Thema sensibler auftreten lässt.

Trotz Bildungsmaßnahmen, bei der viele potentielle Eingriffe in die Privatsphäre vorgestellt wurden, gab der Großteil der Untersuchungsteilnehmer an, keine großartigen Veränderungen beim Internetsurfen wahrgenommen zu haben. Dies lässt den Schluss zu, dass bis dato keine negativen Erfahrungen gemacht wurden und damit auch kein Grund bestehe, etwas zu ändern. Somit wäre ein praktisches Beispiel im Rahmen der Lerneinheit von Vorteil, wo dem Probanden ein Eingriff in seine Privatsphäre veranschaulicht werden würde.

Einen weiteren Erfolg können die Bildungsmaßnahmen beim Vertrauen in IT-Firmen im Umgang mit sensiblen Daten verbuchen. Die Tendenz ist klar ersichtlich. Je mehr die Untersuchungsteilnehmer über das Thema erfahren, desto sensibler wird der Umgang mit privaten Daten gesehen.

5.2 Kritische Aspekte der Studie

Dieses Kapitel versucht die gesamte Untersuchung kritisch zu betrachten und diskutiert die Punkte, die vielleicht nicht optimal bzw. nicht nach Plan gelaufen sind.

Ein großes Problem war mit Sicherheit die Dauer einer Lerneinheit. Wie die Abbildung 4.10 zeigt, konnten nur selten die geplanten 60 Minuten eingehalten werden. Nach den ersten Sessions kristallisierte sich schnell die Erkenntnis heraus, dass die Zeit nur dann einzuhalten war, wenn die Testperson nicht viele Rückfragen stellte und somit die Inhalte zügig vorgetragen werden konnten. Je nach Wissensstand zeigten sich die meisten Probanden jedoch sehr interessiert an der Thematik und stellten viele Fragen zu den einzelnen Bereichen und Fallbeispielen. Meist wurden ungeklärte Situationen angesprochen, die ihnen beim Internetsurfen aufgefallen sind. Wenn die gesamte Lerneinheit innerhalb von 90 Minuten durchgeführt werden konnte, war das meist auch kein Problem. Dauerte die Session jedoch mehr als 2 Stunden, ließ die Konzentration der Testperson oft nach und es entstanden häufiger Verständnisprobleme von komplexen Sachverhalten.

So wäre ein Verbesserungsvorschlag für den gesamten Untersuchungsverlauf, dass die einzelnen Teile der Untersuchung so aufgeteilt werden, dass nicht alle Untersuchungsschritte (alle Messungen, Lerneinheit) am gleichen Termin durchgeführt werden. So sollte beispielsweise der Pretest samt Lerntypentest gleich bei der ersten Kontaktaufnahme ausgefüllt werden. So kann der potentielle Untersuchungsproband gleich abschätzen, ob er sich die Lerneinheit wirklich anhören will und ihn das Thema auch tatsächlich interessiert. Zudem wäre auch anzudenken, die Posttest-Messung erst einem Tag nach der Lerneinheit durchzuführen, um so der Testperson eine Chance zu geben, die vorgetragenen Inhalte zu verinnerlichen und gegebenenfalls auch noch einzelne Rückfragen zu stellen.

Ein weiterer Vorschlag wäre, die Lerneinheit in zumindest zwei Teile aufzuteilen, um so den Probanden mit der Menge des Lernstoffs nicht zu überfordern. Durch diese Maßnahme könnte der Untersuchungsteilnehmer die Inhalte besser verarbeiten und zwischendurch überlegen, welche Auswirkungen dieses Wissen auf das eigene Surfverhalten haben könnte und welche ungeklärten Situationen beim Internetsurfen es in der Vergangenheit noch gegeben hat. Auch die Durchführung des Lerntypentests wäre gleich bei der ersten Kontaktaufnahme sinnvoll, damit der Vortragende sich gezielter auf den jeweiligen Lerntypen vorbereiten kann und den Vortrag entsprechend anpassen kann.

Ein anderes Problem ergab sich mit dem Grad der Komplexität des Vortrages. Da jeder Teilnehmer einen unterschiedlichen Wissenstand über der Thematik mitbrachte, stand der Vortragende oft vor der Herausforderung, dass der Proband bei der Lerneinheit offensichtlich entweder über- oder unterfordert wurde. Eine vorherige Prüfung des aktuellen Wissenstandes des Untersuchungsteilnehmers wäre hilfreich, sodass der Vortragende eine Chance hat, auf gewisse Inhalte tiefergehend einzugehen.

Auch die Auswertung der einzelnen Messung wäre verbesserungswürdig. Alle Fragebögen könnten auf einen Online-Tests umgestellt werden, um so die Antworten anstatt auf einem Blatt Papier gleich in einer Datenbank gespeichert zu haben. Die manuelle Eintragung in ein Excel-Sheet würde erspart bleiben und die Auswertung könnte direkt mit der Datenbank umgesetzt werden. Dafür würde sich die Einbindung von Moodle [1] anbieten, womit sich derartige Datenerhebungen hervorragend umsetzen lassen. Des Weiteren könnte der Untersuchungsteilnehmer alle Messungen von zuhause aus erledigen und ein persönlicher Kontakt wäre nur noch für den eigentlichen Vortrag notwendig. Vielleicht könnten durch diese Maßnahme auch mehr Teilnehmer akquiriert werden, zumindest für die Pretest-Messung.

Abschließend sollte noch Folgendes angemerkt werden: Je mehr Personen bei dieser Untersuchung teilnehmen, desto ausführlicher kann die Analyse durchgeführt werden. Ferner könnten detailliertere Erkenntnisse bezüglich Altersklassen oder Bildungsstand abgeleitet werden.

5.3 Ausblick auf weitere Forschungsfragen

In der vorliegenden Arbeit wurde ein didaktisches Model vorgestellt, welches Aufklärung beim Thema Privatsphäre im Internet bringen sollte. Dieses Model wurde in eine empirische Untersuchung eingebettet, welche die Relevanz von Bildungsmaßnahmen in diesem Bereich messen sollte. Vor jeder Lerneinheit wurde eine Bestandsaufnahme durchgeführt, um so den aktuellen Wissenstand der Probanden rund um das Thema festzuhalten. Nach dem Vortrag wurde eine weitere Messung durchgeführt, die den Lernerfolg messen sollte. Nach etwa 2-3 Monaten wurde eine Langzeitevaluierung durchgeführt, um die langfristige Relevanz von Bildungsmaßnahmen rund um das Thema Privatsphäre im Internet festzustellen.

Die Lerneinheit wurde jeweils in Einzelgesprächen durchgeführt, um speziell auf die individuellen Bedürfnisse der Testpersonen einzugehen. Dabei wurde beispielsweise der jeweilige Lerntyp berücksichtigt und es konnte auf persönliche Erlebnisse oder Fallbeispiele beim Internetsurfen individuell eingegangen werden. Um die Untersuchung mit einer größeren Stichprobe

[1] `https://moodle.org/`, Juni 2014

durchzuführen, könnte das didaktische Model so angepasst werden, dass es auch für eine Gruppe anzuwenden ist (Schulklasse, als Teil einer Vorlesung vor Studenten, Mitarbeiterschulung,...). Für jeden Lerntypen könnten angepasste Übungen angeboten werden, die er später in Eigenregie oder in Kleingruppen ausprobieren könnte.

Das didaktische Model könnte jedoch auch in eine Richtung getrieben werden, in der auf individuelle Bedürfnisse noch spezieller eingegangen werden kann. In den durchgeführten Einzelgesprächen haben Testpersonen, die Elternteile oder Erziehungsberechtigte sind, vermehrt nachgefragt, wie am besten Kinder für das Thema der virtuellen Privatsphäre sensibilisiert werden können. Denn gerade bei jungen Menschen besteht die Gefahr, dass sie einen falschen Umgang mit der eigenen Privatsphäre im Internet lernen und private Details im Internet leichtfertig preisgeben. Wenn das im Vorfeld der Lerneinheit bekannt wäre, könnte sich der Vortragende gezielt vorbereiten und spezielles Wissen vermitteln.

Auch das soziale Verhalten der Probanden könnte von Interesse sein. Dabei könnten die einzelnen Lerneinheiten mit Video aufgezeichnet werden, um so das Verhalten der Testpersonen zu analysieren. Dabei könnten Verhaltensweisen studiert werden, wobei besonders Interesse gezeigt wurde oder Verständnisprobleme entstanden. Diese Erkenntnisse könnten für weitere Vorträge und Lerneinheiten von besonderer Bedeutung sein.

Die gesammelten Erfahrungen sollten auf jeden Fall in die gesamte Untersuchung eingearbeitet werden, sodass jegliche Verbesserungsansätze und Kritikpunkte beachtet werden. Das Ziel sollte sein, die Bildungsmaßnahmen möglichst effizient zu gestalten, so dass es deren Relevanz erhöht und letztendlich eine Hilfe für die Internet User darstellt, die eigene Privatsphäre bestmöglich zu schützen.

ANHANG A

Folien der Lerneinheit

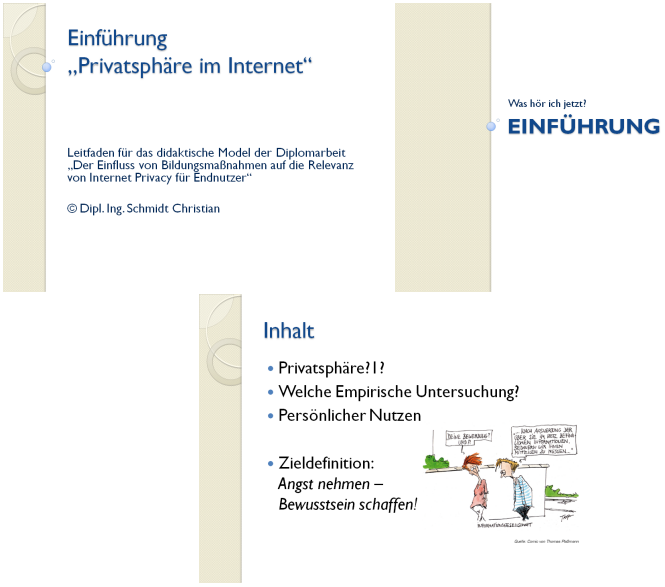


Abbildung A.1: Folien für die Einführung

Abbildung A.2: Folien für die Begriffe Privacy, Identität, Anonymität

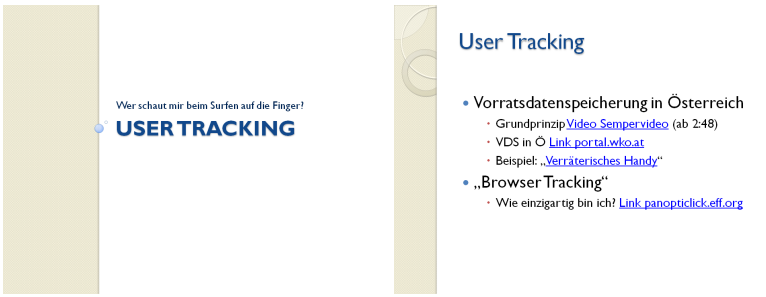


Abbildung A.3: Folien für User Tracking

Abbildung A.4: Folien für weitere Gefahren und Risiken

Abbildung A.5: Folien für prakt. Lösungsansätze und Conclusio

ANHANG B

Fragenbögen Pretest, Posttest und Langzeitevaluierung

B.1 Fragebogen für Pretest

Demographie

1. Wie alt sind Sie?

   Alter: _____

2. Welches Geschlecht haben Sie?

   Männlich ☐ Weiblich ☐

Bildung und Beschäftigung

3. Welches ist Ihr höchster Schulabschluss?

   - ○ SchülerIn
   - ○ Pflichtschule
   - ○ Lehre/Berufsschule
   - ○ Matura (BHS/AHS)
   - ○ Hochschule/Universität
   - ○ Promotion
   - ○ Sonstiges

Fragen zu Privatsphäre

4. Haben Sie eine bestimmte Vorstellung oder Definition von folgenden Begriffen?

   „Privatsphäre im Internet“?

   Ja ☐ Nein ☐
   Wenn Ja, kurze Beschreibung: _____

   „Virtuelle Identität“?

   Ja ☐ Nein ☐
   Wenn Ja, kurze Beschreibung: _____

   „Vorratsdatenspeicherung“?

   Ja ☐ Nein ☐
   Wenn Ja, kurze Beschreibung: _____

5. Wie wichtig ist Ihnen Privatsphäre im Allgemeinen?

   - ○ Sehr wichtig
   - ○ Wichtig
   - ○ Weniger wichtig
   - ○ Gar nicht wichtig
   - ○ Keine Ahnung

6. Verwenden Sie Techniken um anonym zu surfen? (Tor, anonymen VPN, Open Proxy,...)

   Ja ☐ Nein ☐
   Wenn Ja, welche: _____

7. Geben Sie über das Internet mehr Informationen (Name, Telefonnummern, Adresse,...) über sich preis als Sie das in der realen Welt tun würden?

   Ja ☐ Nein ☐

8. Wenn Sie sich bei Internetdiensten registrieren, aus welchen der folgenden Bestandteile setzt sich dann in der Regel Ihr Benutzernamen zusammen? (mehrere Antworten möglich!)

   ☐ Mein vollständiger Name

   ☐ Mein Vorname (oder Abkürzung)

   ☐ Mein Nachname (oder Abkürzung)

   ☐ Pseudonym (oder Spitzname)

   ☐ Name der Stadt, in der ich wohne

   ☐ Mein Geburtsjahr

   ☐ Mein Alter

   ☐ _____

9. Wer sollte letztendlich verantwortlich sein für die persönliche Privatsphäre im Internet? (Bitte nur eine Antwort!)

   ○ Immer selber verantwortlich

   ○ Der Internetdienst, den ich verwende

   ○ Internet Service Provider (Telekom,...)

   ○ Arbeitgeber

   ○ Andere: _____

10. Inwiefern stimmen Sie den folgenden Aussagen zum Thema Privatsphäre zu? (Ankreuzen!)

	Ich stimme zu	Ich stimme eher zu	Ich stimme eher nicht zu	Ich stimme nicht zu	Keine Ahnung
Privatsphäre wird im Zeitalter des Internets immer mehr an Bedeutung gewinnen.	○	○	○	○	○
Durch die Bedrohung des Terrorismus werden immer mehr Informationen des Bürgers offen gelegt.	○	○	○	○	○
Internetdienste erheben in der Regel mehr persönliche Daten als notwendig.	○	○	○	○	○
Das Internet beschleunigt die Offenlegung persönlicher Daten seiner Nutzer	○	○	○	○	○
Im Internet werden persönliche Daten vielfach leichtfertig veröffentlicht.	○	○	○	○	○
Im Internet ist es wichtiger auf Privatsphäre zu achten, weil viele Informationen öffentlich zugänglich sind.	○	○	○	○	○
Die Privatsphäre bleibt auch im Internet gewahrt. Jeder entscheidet selbst darüber welche Informationen preisgegeben werden.	○	○	○	○	○

11. Für wie wahrscheinlich halten Sie es, dass die von Ihnen im Internet veröffentlichten Inhalte oder gesammelten Daten für die folgenden Zwecke verwendet werden könnten? (Ankreuzen!)

	Ich stimme zu	Ich stimme eher zu	Ich stimme eher nicht zu	Ich stimme nicht zu	Keine Ahnung
Bekämpfen von Verbrechen (durch den Staat)	○	○	○	○	○
Bekämpfen von Terror (durch den Staat)	○	○	○	○	○
Erstellen von personalisierter Werbung (durch Unternehmen)	○	○	○	○	○
Bewerten von Bewerbern (durch potentielle Arbeitgeber)	○	○	○	○	○
Erstellen von Krankenversicherten-profilen (durch Krankenkassen)	○	○	○	○	○
Erstellen von Versichertenprofilen (durch andere Versicherungen)	○	○	○	○	○
Nachstellen oder Belästigen (durch Privatpersonen)	○	○	○	○	○

Internetnutzung

12. An welchen Orten nutzen Sie das Internet regelmäßig? (mehrere Antworten möglich!)

    ☐ zuhause
    ☐ am Arbeitsplatz
    ☐ in der Schule/Universität
    ☐ an öffentlichen Orten (öffentliches WLAN, Internet-Café, Hotel-WLAN)
    ☐ über mobilen Internetzugang (Smartphone)
    ☐ sonstige:_____

13. Besitzen Sie ein Smartphone/Tablet?

    Ja ☐ Nein ☐

    Wenn Ja, welches (Apple, Samsung, Nokia,...): _____

14. Gibt es Internetseiten, - dienste, -plattformen, welche Sie regelmäßig besuchen?

    Ja ☐ Nein ☐

    Bitte geben Sie bis zu 5 Adressen von Internetseiten,- diensten, -plattformen, welche Sie regelmäßig besuchen!
    1. _____
    2. _____
    3. _____
    4. _____
    5. _____

15. Bitte schätzen Sie ein, bei wie vielen Internetseiten,- dienste, -plattformen Sie sich für private Zwecke registriert haben oder über ein Benutzerkonto verfügen. Folgende Kategorien werden zur Hilfestellung angeboten:

    - Foren (Gästebuch. . .)
    - Newsportale(laola1.at, ORF inside...)
    - Fachportale (UNI-Portal...)
    - Email (GMX, Hotmail/Outlook, Yahoo, Gmail,...)
    - Social Media (Facebook, Twitter, LinkedIn, Singlebörsen, StudiVZ, Youtube...)
    - Gaming (BWIN, BetAndWin, Tipico...)
    - Tauschbörsen (ebay, Willhaben,...)
    - Shopping (Amazon, Zalando, Frontline,...)
    - Telekommunikation (Apple, Samsung, Windows/Outlook/Hotmail, Nokia, A1,...)
    - Netbanking
    - Cloud-Services (Dropbox...)
    - Reiseportale(miles and more, Expedia...)
    - Andere Web Services (ÖTicket...)

    Kreuzen Sie Zutreffendes an:

    - ○ keins
    - ○ bis zu 5
    - ○ mehr als 5, jedoch weniger als 20
    - ○ 20 oder mehr

Soziale Medien

16. Wie viele Benutzerkonten eines sozialen Mediums (Facebook, Twitter, LinkedIn, Youtube, Singlebörsen. . . .) betreiben Sie, um Text-, Bild-, Ton- oder Videoinhalte im Internet zu veröffentlichen?

    - ○ keins
    - ○ 1
    - ○ 2
    - ○ 3 und mehr

17. Welche der folgenden Angaben sind in Ihren sozialen Medien zu finden? (mehrere Antworten möglich!)

    - ☐ Vollständiger Name
    - ☐ Wohnort
    - ☐ Vollständige Adresse
    - ☐ Telefonnummer (Handy/Festnetz)
    - ☐ E-Mail
    - ☐ Foto von mir
    - ☐ _____
    - ☐ _____

Suchdienste

18. Welche Suchmaschine benutzen, wenn Sie nach etwas recherchieren? (mehrere Antworten möglich!)

    - ☐ Google
    - ☐ Bing
    - ☐ Yahoo
    - ☐ Andere...

19. Würden Sie wollen, dass enge Bekannte/Elternteile/Arbeitgeber wissen, was Sie in einer Suchmaschine suchen (auch sensible Suchbegriffe wie Krankheiten, sexuelle Ausrichtung. . .)?

    Ja ☐ Nein ☐

20. Fragen zu Suchabfragen von sensiblen personenbezogenen Themenbereichen:

	nie	1 oder 2 mal	manchmal	Regelmäßig
Ich habe eine Suchmaschine nach einem Thema befragt, welches ich meinen Eltern/Lebenspartner nicht erzählen würde.	○	○	○	○
Ich habe eine Suchmaschine nach einem Thema befragt, welches ich meinen künftigen Arbeitgeber nicht erzählen würde.	○	○	○	○
Ich habe eine Suchmaschine schon mal nach einem Freund oder Kollegen durchsucht.	○	○	○	○
Ich hab in einer Suchmachine schon mal nach meinem eigenen Namen gesucht.	○	○	○	○

Suchdienste

21. Wie regelmäßig **veröffentlichen Sie Inhalte** bei den nachfolgenden Webseiten bzw. Internetdienste?

	Sehr häufig	regelmäßig	selten	Nutze ich nicht
Soziale Medien (Facebook...)	○	○	○	○
Instant Messaging (Skype...)	○	○	○	○
Fotos (Flickr...)	○	○	○	○
Videos (youtube...)	○	○	○	○
Nachrichten (orf.at, laola1.at...)	○	○	○	○
Foren (Gästebücher...)	○	○	○	○
Microblogging (Twitter...)	○	○	○	○
Musik (Spotify, Last.fm...)	○	○	○	○
Dating (WebSingles...)	○	○	○	○
Reiseportale (eBookers...)	○	○	○	○
Blogs (Blogger, WordPress...)	○	○	○	○
Shopping (Amazon...)	○	○	○	○
Enzyklopädien (Wikipedia...)	○	○	○	○

22. Wie häufig nehmen Sie folgende Webseiten bzw. Internetdienste **nur passiv (nur lesend)** in Anspruch?

	Sehr häufig	regelmäßig	selten	Nutze ich nicht
Soziale Medien (Facebook...)	○	○	○	○
Fotos (Flickr...)	○	○	○	○
Videos (youtube...)	○	○	○	○
Nachrichten (orf.at, laola1.at...)	○	○	○	○
Foren (Gästebücher...)	○	○	○	○
Microblogging (Twitter...)	○	○	○	○
Musik (Spotify, Last.fm...)	○	○	○	○
Dating (WebSingles...)	○	○	○	○
Reiseportale (eBookers...)	○	○	○	○
Blogs (Blogger, WordPress...)	○	○	○	○
Shopping (Amazon...)	○	○	○	○
Enzyklopädien (Wikipedia...)	○	○	○	○

Vertrauen gegenüber Unternehmen

23. Wie viel Vertrauen würden Sie den folgenden Firmen im Umgang mit Ihren privaten Informationen (Name, Adressen, Kontaktinformationen,...) gewähren?

	Sehr geringes Vertrauen	Bedingtes Vertrauen	Vernünftiges Vertrauden	Starkes Vertrauen
Microsoft	○	○	○	○
Google (Search, Android,...)	○	○	○	○
Ebay, willhaben	○	○	○	○
Zalando, Sportcheck...	○	○	○	○
Apple (iphone,...)	○	○	○	○
Amazon	○	○	○	○
Dein Telekommunikationsanbieter (A1, T-Mobile,...)	○	○	○	○

24. Inwiefern halten Sie die Übermittlung folgender Daten über das Internet für unproblematisch bzw. problematisch?

	problematisch	unproblematisch	Ich bin mir nicht sicher
Kreditkartendaten	○	○	○
Bankverbindung	○	○	○
Adresse (privat)	○	○	○
Adresse (beruflich)	○	○	○
Reisepassdaten	○	○	○
E-Mail Adresse	○	○	○
Vor- und Nachname	○	○	○
Geburtsdatum	○	○	○
Geburtsort	○	○	○

Vorratsdatenspeicherung

* Telekommunikationsanbieter sind beispielsweise Mobilfunktanbieter wie A1, T-Mobile, Telering,... aber auch Internet Service Provider wie A1, Tele2 oder UPC

25. Inwiefern würden Sie folgende Aussagen zustimmen?

	nie	manchmal	regelmäßig	immer
Telekommunikationsanbieter* speichern jede Verbindung (Internet, Telefon,...)	◯	◯	◯	◯
Telekommunikationsanbieter* speichern zu welcher Internetseite ich surfe	◯	◯	◯	◯
Telekommunikationsanbieter* speichern mit wem ich telefoniere	◯	◯	◯	◯
Telekommunikationsanbieter* speichert den geografischen Standort mit	◯	◯	◯	◯

26. Wenn Telekommunikationsanbieter* alle meine Verbindungen speichern würden, für wie lange würden diese gespeichert bleiben?

    - ○ Nur für ein paar Stunden
    - ○ einen Tag
    - ○ eine Woche
    - ○ einen Monat
    - ○ halbes Jahr
    - ○ ein Jahr
    - ○ für immer

27. Wenn ich wüsste, dass mein Telekommunikationsanbieter* all meine Verbindungen für immer mitspeichert, würde das mein Surfverhalten bzw. mein Telefonierverhalten ändern?

    - ○ Keine Änderung
    - ○ Minimale Änderung
    - ○ Würde mehr aufpassen

- Verhalten würde sich komplett ändern

28. Ich weiß, wie ich anonym surfen kann?

Ja ☐ Nein ☐
Wenn Ja, wie?: _____

29. Ich weiß, wie ich anonym telefonieren kann?

Ja ☐ Nein ☐
Wenn Ja, wie?: _____

B.2 Fragebogen für Posttest

Fragen zur Lerneinheit selbst (bitte EHRLICH beantworten!!!!)

1. War der Lehrstoff für Sie klar verständlich und sinnvoll aufbereitet?

Ja ☐ Nein ☐
Wenn Nein, warum?: _____

2. Konnten Sie den Schritten folgen?

Ja ☐ Nein ☐
Wenn Nein, warum?: _____

3. Wie schätzen Sie Ihren persönlichen Lernzuwachs ein?

   - Wenig dazugelernt
   - Wusste von der Problematik, konnte aber viel Neues erfahren
   - War komplettes Neuland für mich

4. Wurde der Lernstoff mit der richtigen Methodik vorgetragen?

Ja ☐ Nein ☐
Wenn Nein, warum?: _____

5. Hätte der Vortrag aus Ihrer Sicht verbessert werden können? (mehrere Antworten möglich)

   ☐ Durch mehr Erklärungen
   ☐ Durch mehr Grafiken
   ☐ Durch mehr Videos

- ☐ Durch mehr Handlungsanweisungen
- ☐ Durch mehr „Selbstständiges Lernen“
- ☐ _____

Wissen über theoretischen Background

6. Wer sind potentielle Informationssammler, wenn man eine Webseite aufruft? (mehrere Antworten möglich!)

   - ☐ Nachbar
   - ☐ Verwendetes Webservice (Facebook, Google, einfache Webseite,. . .)
   - ☐ Mein Computer
   - ☐ Freunde
   - ☐ Internet Service Provider (A1, T-Mobile,. . .)
   - ☐ Behörden (Polizei, Finanzamt,. . .)
   - ☐ Familienangehörige

7. Was ist im Allgemeinen mit Privatsphäre im Internet gemeint? Bitte kreuzen Sie das Richtige an, nur ein Satz ist korrekt! (TIPP: genau lesen!)

   - ○ Allgemein ist Privatsphäre das Recht einer Person in jedem Kontext für sich selbst entscheiden zu können, wann und unter welchen Bedingungen seine personenbezogenen Daten zu verkaufen.
   - ○ Allgemein ist Privatsphäre das Recht einer dritten Person entscheiden zu können, wann und unter welchen Bedingungen personenbezogene Daten herausgegeben und von anderen Personen verwendet werden können.
   - ○ Allgemein ist Privatsphäre das Recht einer Person in jedem Kontext für sich selbst entscheiden zu können, wann und unter welchen Bedingungen personenbezogene Daten herausgegeben und von anderen Personen verwendet werden können.
   - ○ Allgemein ist Privatsphäre die Pflicht einer Person in jedem Kontext für sich selbst entscheiden zu können, unter welchen Bedingungen personenbezogene Daten herausgegeben und von anderen Personen verwendet werden können.

8. Ordnen Sie die jeweilige Identität der realen bzw. der virtuellen Welt zu! (Schreiben Sie „V“ für virtuelle Welt, „R“ für reale Welt)

   - _ Facebook-Profil
   - _ Führerschein
   - _ Reisepass
   - _ Personenausweis
   - _ Google-Suchwörter
   - _ Kreditkarte

Bewusstsein für möglich Gefahren, Risiken und Themen wie Vorratsdatenspeicherung

9. Wie lange müssen Kommunikationsdienstbetreiber die Vorratsdaten speichern? (Kreuzen Sie das richtige an, nur eines ist richtig)

   - ○ 1 Woche
   - ○ 3 Monate
   - ○ 6 Monate
   - ○ 1 Jahr
   - ○ Für immer

10. Welche Daten sind von der Vorratsdatenspeicherung betroffen? (Mehrere Antwortmöglichkeiten)

    - ☐ Eigene IP-Adresse
    - ☐ Verbindungsdaten
    - ☐ Inhalte von Emails
    - ☐ Telefongesprächsaufzeichnungen
    - ☐ Chatinhalte
    - ☐ Gerätekennung (IMEI) eines Handys

11. Was verstehen Sie unter folgende Begriffe? (Stichwortartige Beschreibung genügt!)
    „Browser Tracking“: _____
    „Search Term Analysis“: _____
    „Social Engineering“: _____

Verständnis für Lösungsansätze

12. Bitte beantworten Sie folgende Fragen...

    Unter welcher IP-Adresse surfen sie gerade? (Bitte geben sie die aktuelle IP Adresse an!)

    _____

    Unter welchen Provider surfen sie?

    _____

    Starten Sie ein Anonymisierungs-Werkzeug und finden Sie die neue IP heraus; aus welchem Land surfen Sie?

    _____

    Wie führe ich „sichere Google-Abfragen“ durch?

    _____

Qualitätskriterien (Bewertung durch Interviewer)

13. Proband vermittelt interessierten Eindruck?

    Ja ☐ Nein ☐

14. Proband stellte viele Rückfragen?

    Ja ☐ Nein ☐

15. Software auf PC/Notebook des Probanden installiert?

    Ja ☐ Nein ☐

16. Konnten die praktischen Teile leicht gelöst werden?

    Kein Problem ☐ Mithilfe ☐ gar nicht ☐

17. Wie lange hat die komplette Lerneinheit gedauert?

    1h ☐ 1,5 ☐ 2h ☐ mehr als 2h ☐

18. Welcher Lerntyp (laut Lerntypentest)?

    autiv ☐ visuell ☐ kommunikativ ☐ motorisch ☐

B.3 Fragebogen für Langzeitevaluierung

1. Sind sie jemals (z.B. beim Internet-surfen,...) in die Situation gekommen, wo sie an den Privacy-Vortrag gedacht haben, wenn ja welche Situationen waren das? (Stichwort: diverse Internetplattformen, Profilerstellung)
   _____

2. Haben sie seitdem jemals Diskussionen in dieser Thematik geführt? Wenn ja, worum ging es?
   _____

3. Sind ihnen die folgenden Begriffe noch geläufig?
   „Privatsphäre im Internet“: _____
   „Virtuelle Identität“: _____
   „Anonym Surfen“: _____
   „Browser Tracking“: _____
   „Search Term Analysis“: _____
   „Social Engineering“: _____

4. Sind sie seit dem Vortrag, in die Situation gekommen, dass sie sich im Internet anonym bewegen wollen?

   _____

5. Haben sie seit dem die Privacy-Einstellung im Facebook gecheckt?

   _____

6. Haben sie mittlerweile das Gefühl, dass sie ein gewisses Bewusstsein entwickelt haben, wo sie nachdenken, welche privaten Informationen sie im Internet eingeben?

   _____

7. Hat sich ihr Surf-Verhalten irgendwie verändert? Wenn ja, wie?

   _____

8. Wie viel Vertrauen würden Sie den folgenden Firmen im Umgang mit Ihren privaten Informationen (Name, Adressen, Kontaktinformationen,...) gewähren?

	Sehr geringes Vertrauen	Bedingtes Vertrauen	Vernünftiges Vertrauden	Starkes Vertrauen
Microsoft	○	○	○	○
Google (Search, Android,...)	○	○	○	○
Ebay, willhaben	○	○	○	○
Zalando, Sportcheck...	○	○	○	○
Apple (iphone,...)	○	○	○	○
Amazon	○	○	○	○
Dein Telekommunikationsanbieter (A1, T-Mobile,...)	○	○	○	○

9. Haben sie jemals wieder etwas von der Vorratsdatenspeicherung gehört? Berührungspunkte?

   _____

10. Wie lange müssen Kommunikationsdienstbetreiber die Vorratsdaten speichern? (Kreuzen Sie das richtige an, nur eines ist richtig)

    - ○ 1 Woche
    - ○ 3 Monate
    - ○ 6 Monate
    - ○ 1 Jahr
    - ○ Für immer

11. Welche Daten sind von der Vorratsdatenspeicherung betroffen? (Mehrere Antwortmöglichkeiten)

    ☐ Eigene IP-Adresse
    ☐ Verbindungsdaten
    ☐ Inhalte von Emails
    ☐ Telefongesprächsaufzeichnungen
    ☐ Chatinhalte
    ☐ Gerätekennung (IMEI) eines Handys

ANHANG C

Diagramme der empirischen Analyse

C.1 Diagramme der Pretest-Analyse

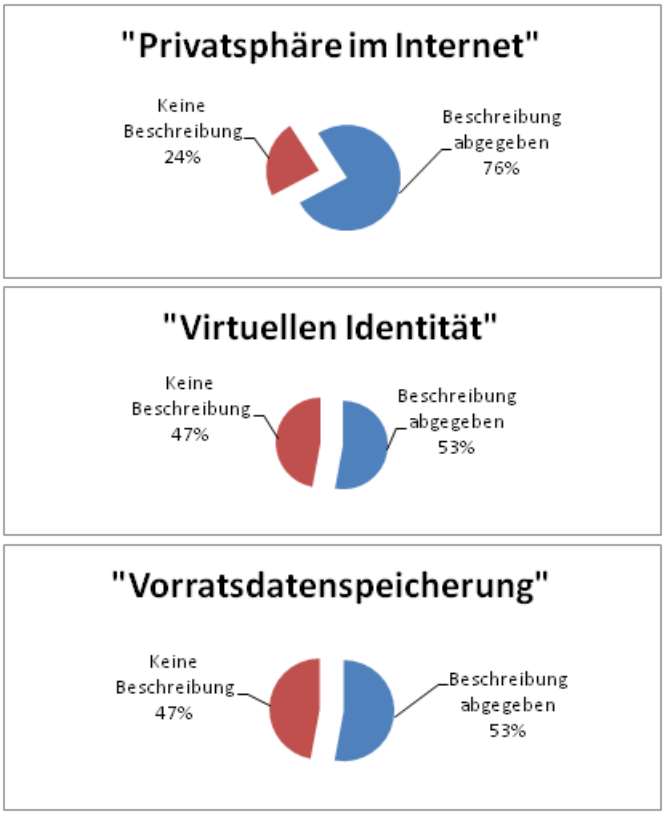
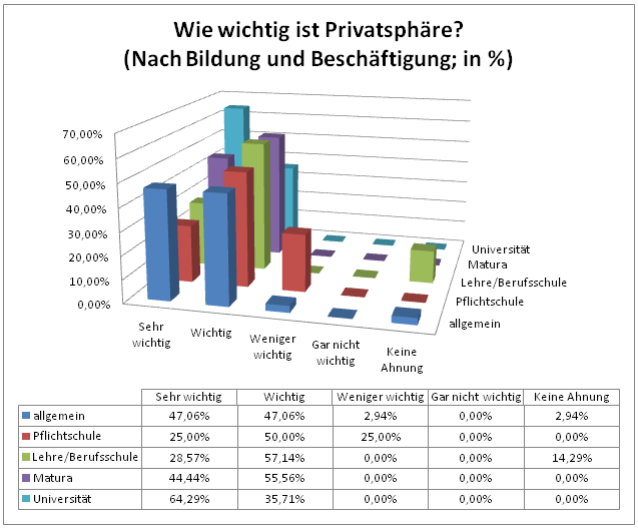


Abbildung C.1: Erklärungsversuche durch den Probanden



	Sehr wichtig	Wichtig	Weniger wichtig	Gar nicht wichtig	Keine Ahnung
allgemein	47,06%	47,06%	2,94%	0,00%	2,94%
Pflichtschule	25,00%	50,00%	25,00%	0,00%	0,00%
Lehre/Berufsschule	28,57%	57,14%	0,00%	0,00%	14,29%
Matura	44,44%	55,56%	0,00%	0,00%	0,00%
Universität	64,29%	35,71%	0,00%	0,00%	0,00%

Abbildung C.2: Wichtigkeit von Privatsphäre (nach Ausbildung)

Abbildung C.3: Fragen zur Nutzung von Anonymisierungstechniken und Preisgabe von persönlichen Daten

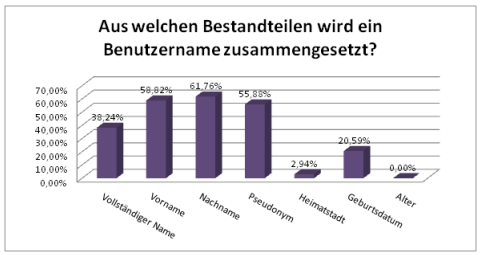


Abbildung C.4: Bestandteile eines Benutzernamens

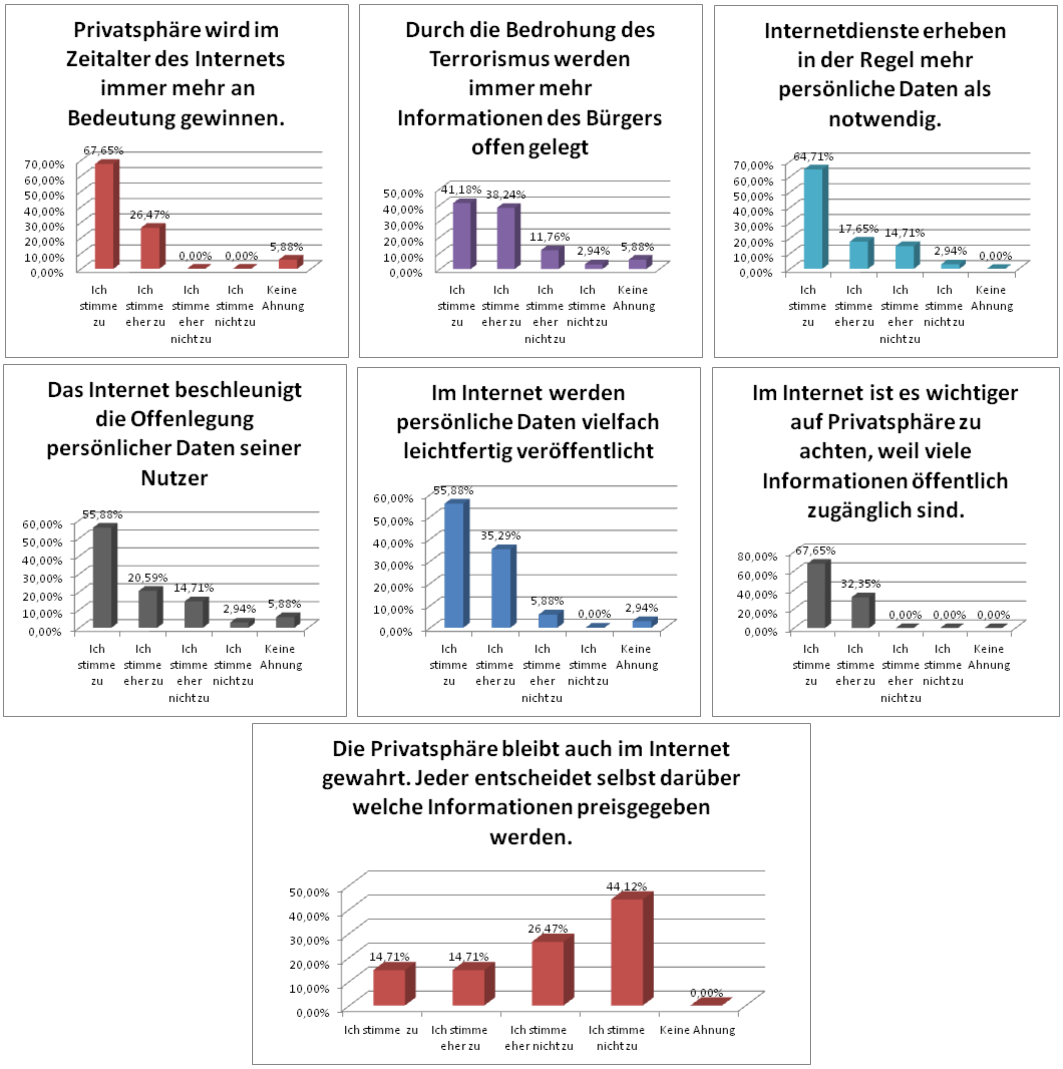


Abbildung C.5: Verschiedene Fragen zu Privatsphäre im Internet

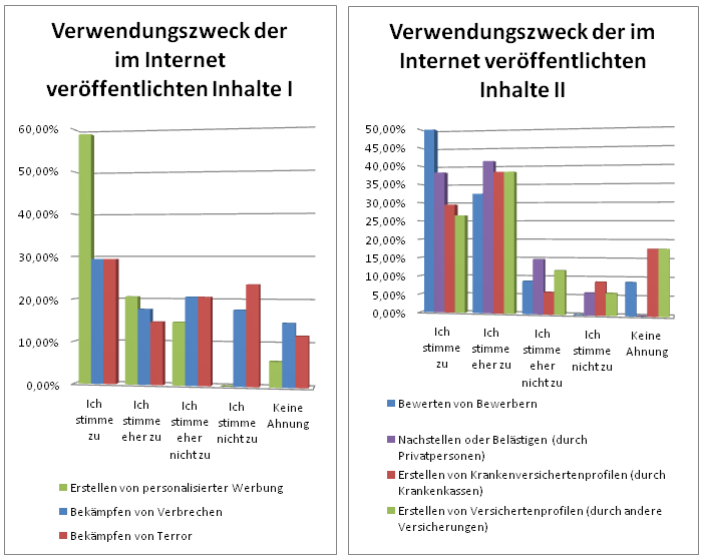


Abbildung C.6: Verwendungszweck der im Internet veröffentlichten Inhalte

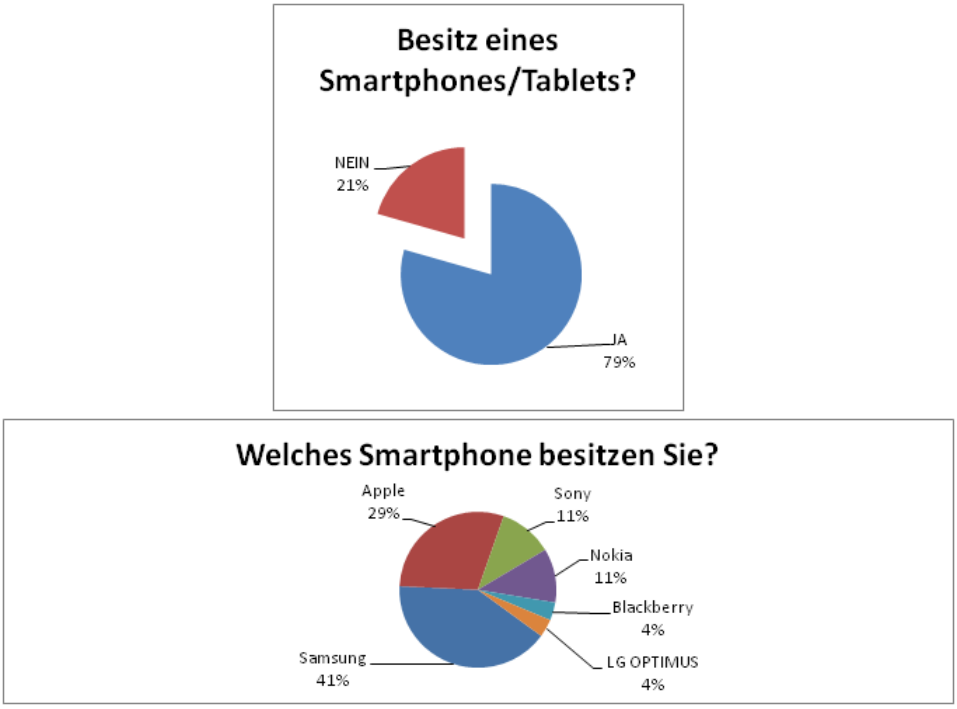


Abbildung C.7: Besitz eines Smartphones

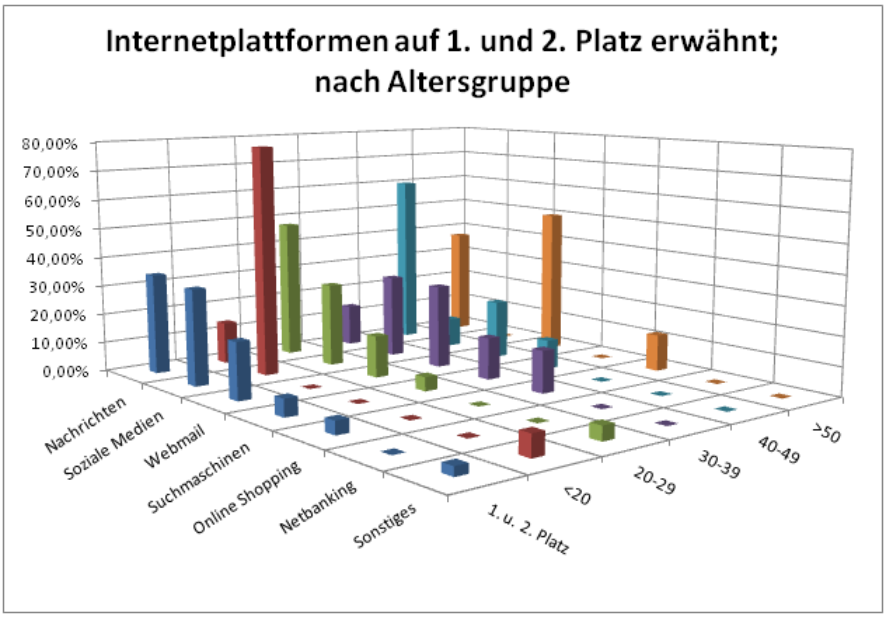


Abbildung C.8: Genutze Internetplattformen (nach Altersgruppe)

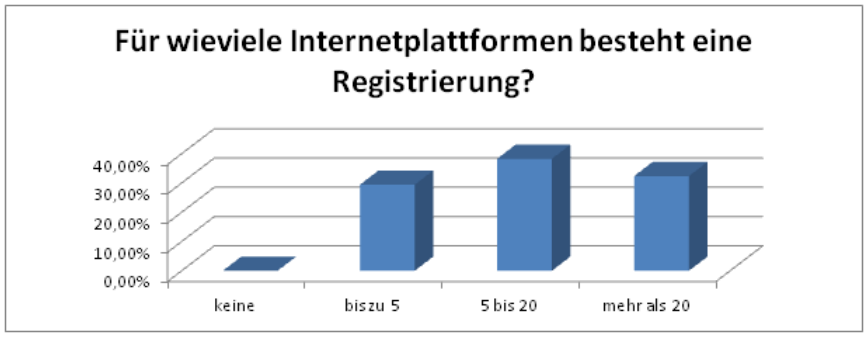


Abbildung C.9: Anzahl an Registrierungen über alle Plattformen

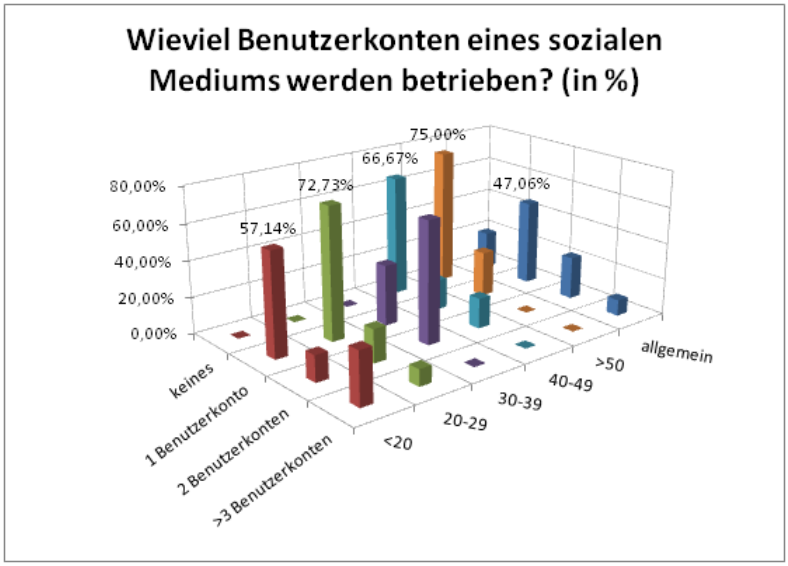


Abbildung C.10: Anzahl an betreuten Benutzerkonten

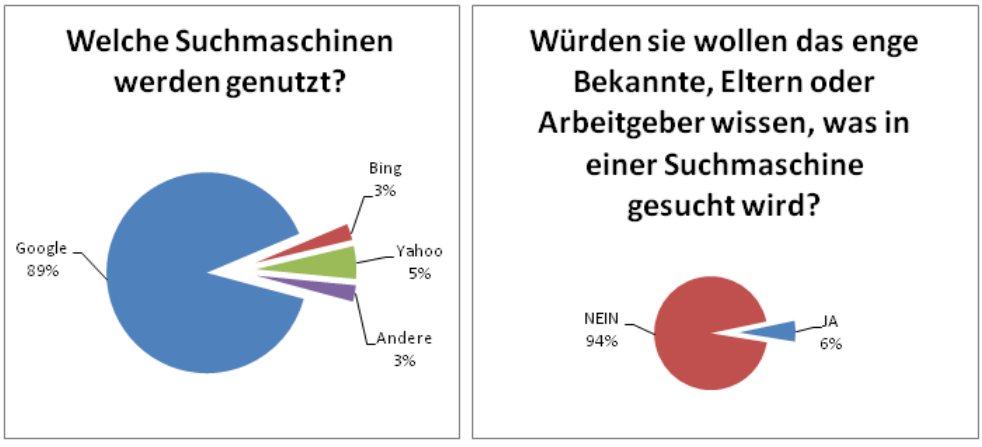


Abbildung C.11: Beliebte Suchmaschinen und Weitergabe von Suchtermen

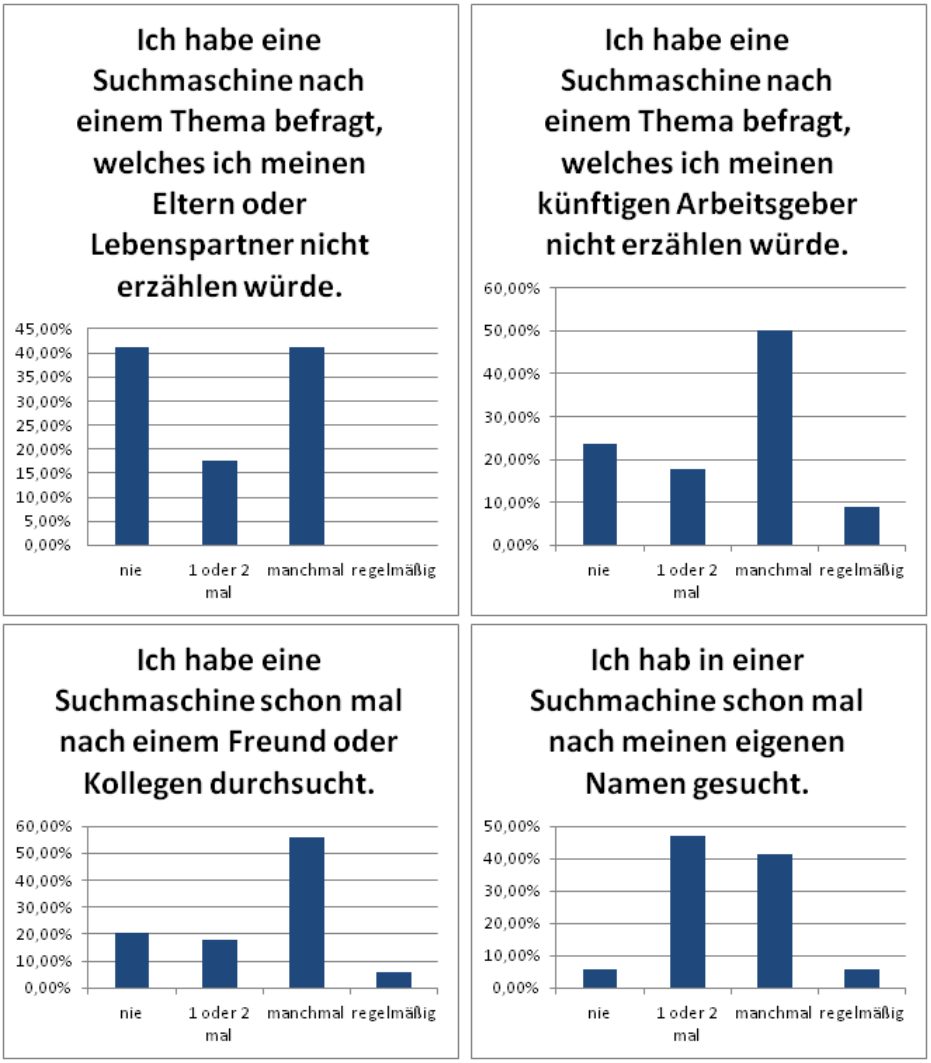


Abbildung C.12: Handhabung von Suchmaschinen

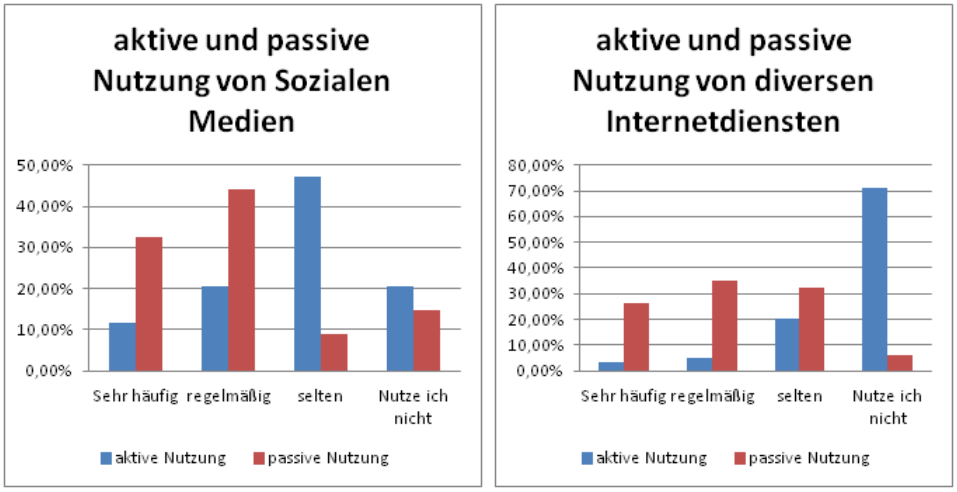


Abbildung C.13: Aktive und passive Nutzung von Internetdiensten

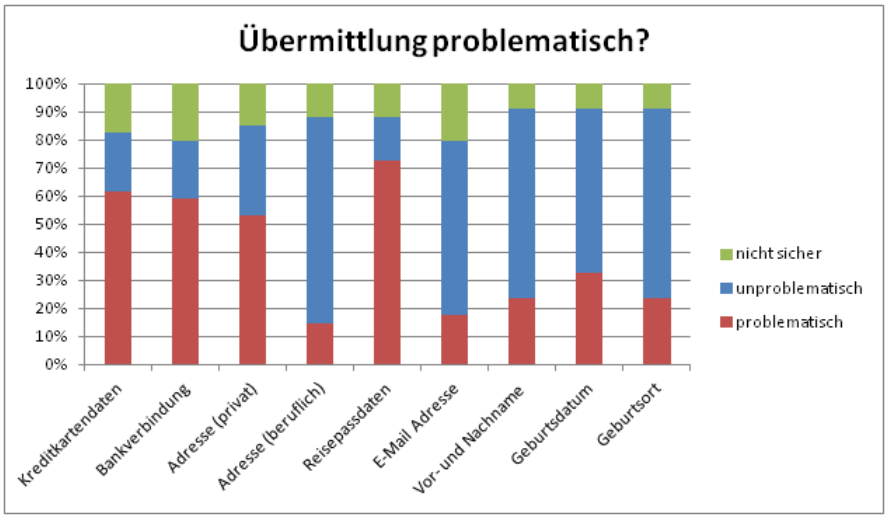


Abbildung C.14: Übermittlung persönlicher Daten

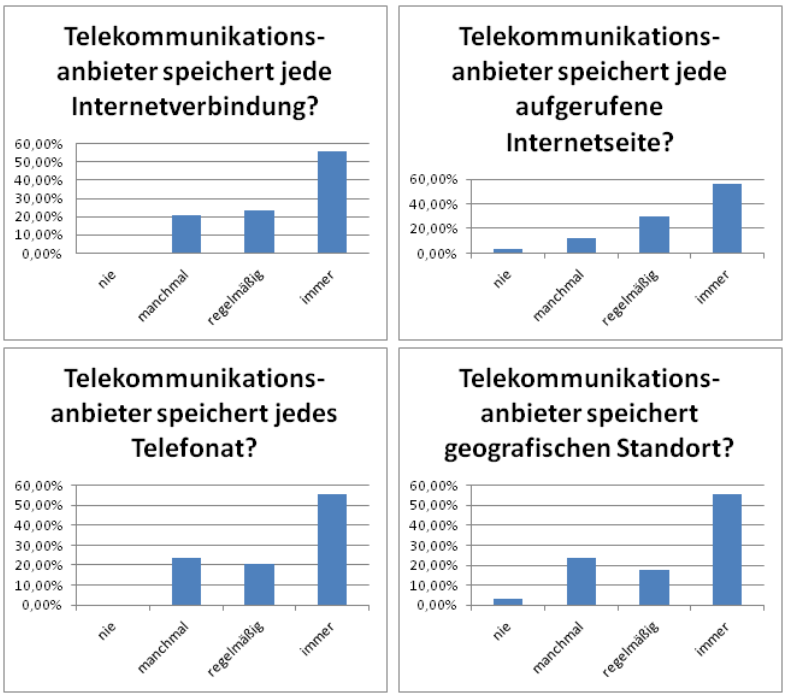


Abbildung C.15: Umgang mit der Vorratsdatenspeicherung (VDS)

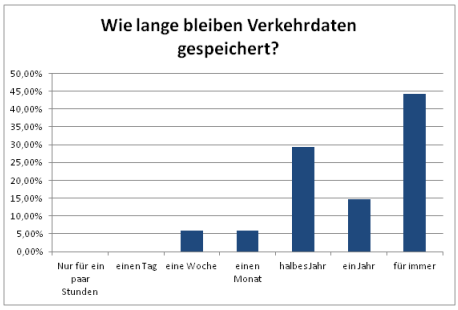


Abbildung C.16: Dauer der Speicherung von Verkehrsdaten

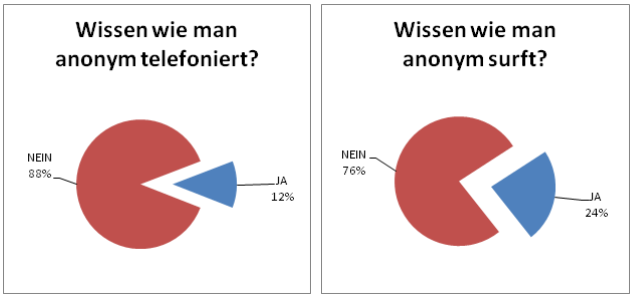


Abbildung C.17: Wissen über Anonymisierungsdienste

C.2 Diagramme der Posttest-Analyse

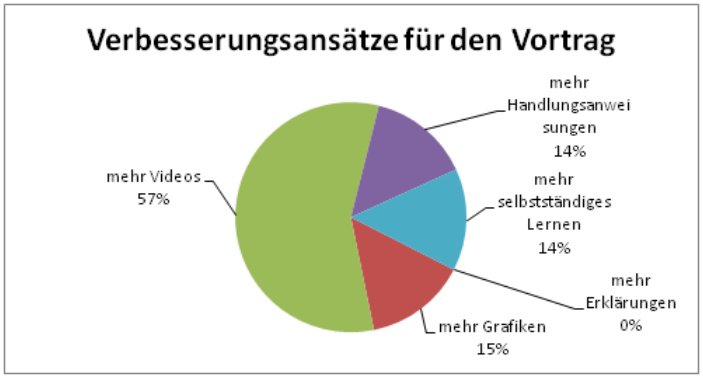


Abbildung C.18: Vorschläge für Verbesserungsansätze

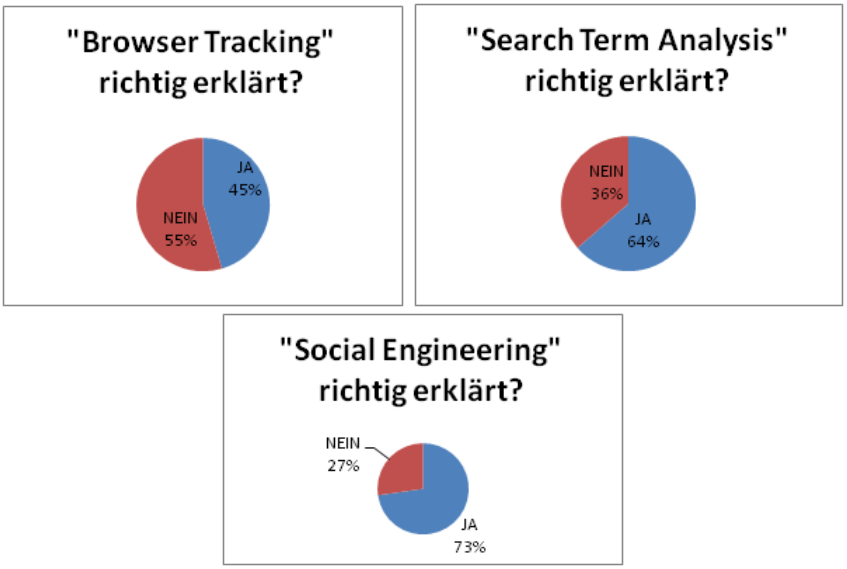
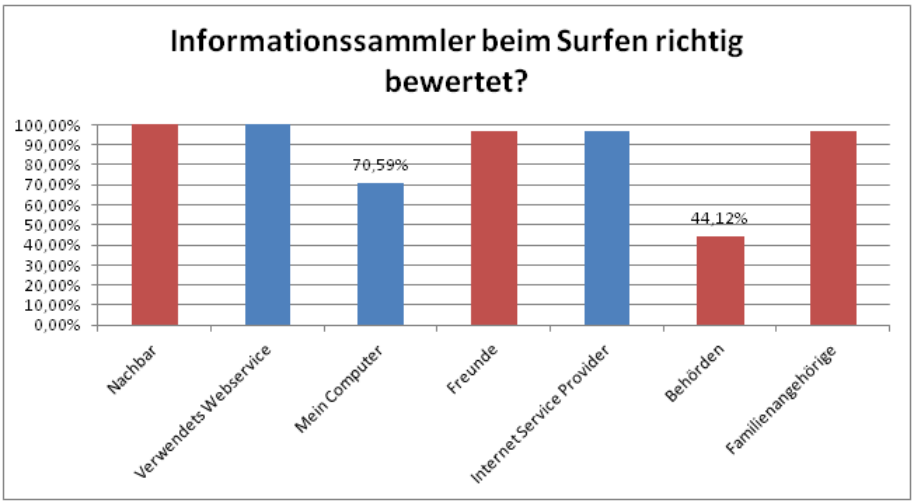
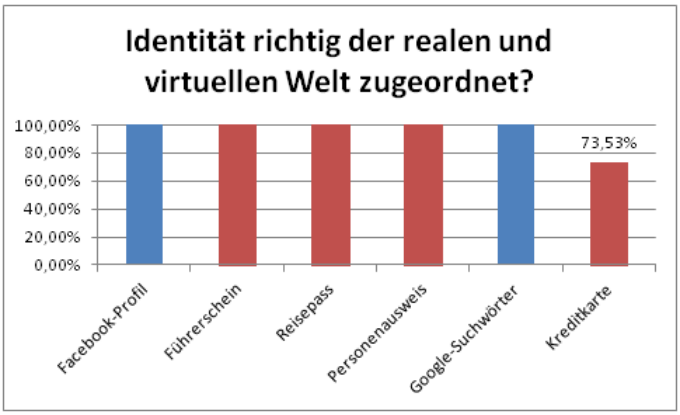


Abbildung C.19: Begriffsdefinitionen





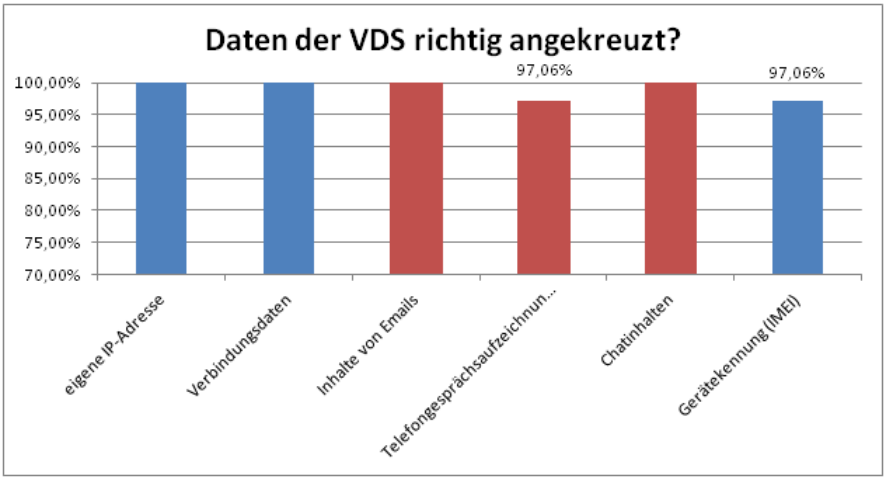


Abbildung C.20: Fragen zum theoretischen Verständnis

C.3 Diagramme der qualitativen Analyse

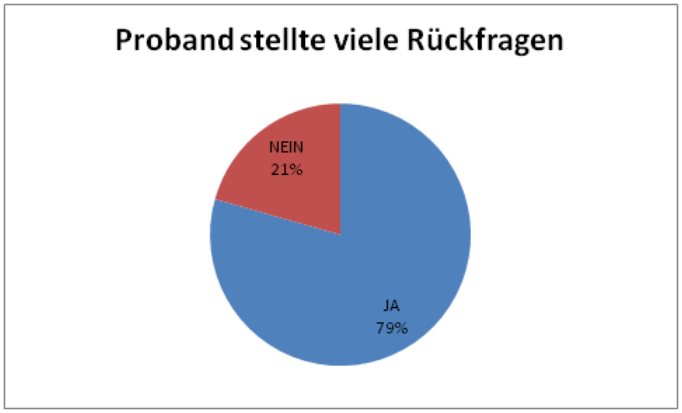


Abbildung C.21: Rückfragen durch Probanden

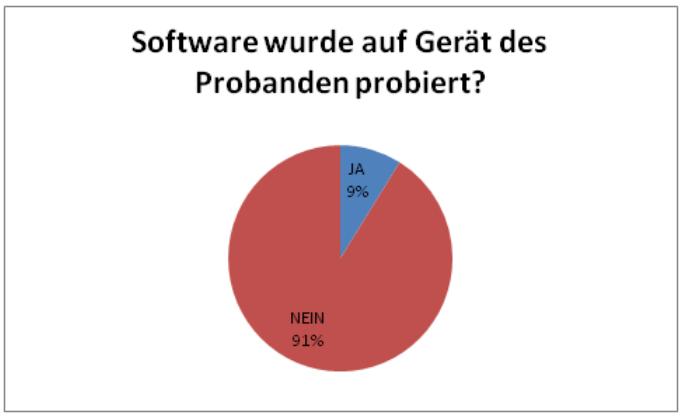


Abbildung C.22: Software auf eigenen Gerät ausprobiert

C.4 Diagramme der Langzeitevaluierung

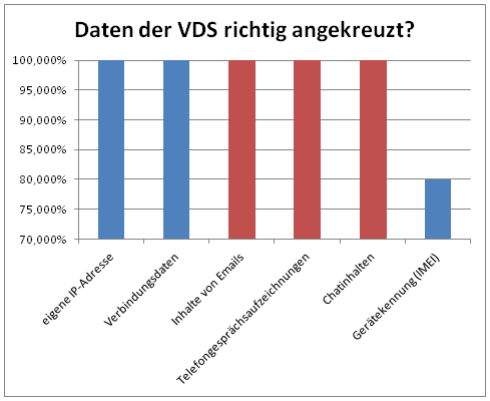


Abbildung C.23: Daten der Vorratsdatenspeicherung

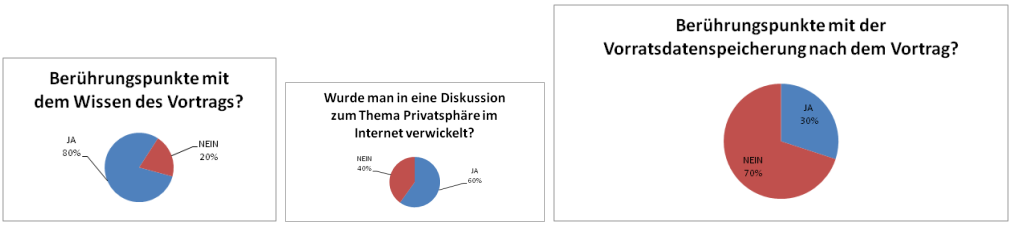


Abbildung C.24: Berührungspunkte mit Privatsphäre im Internet

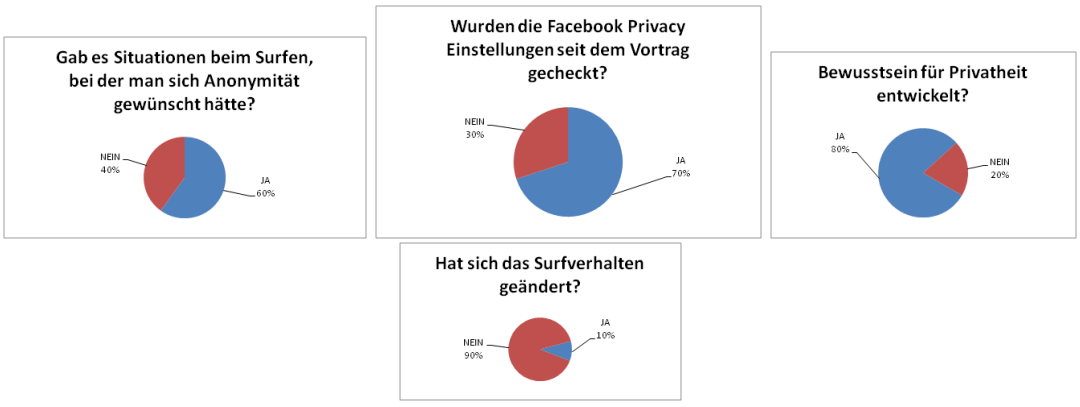


Abbildung C.25: Veränderungen durch Bildungsmaßnahmen

Literaturverzeichnis

[1] Gregory Conti and Edward Sobiesk. An honest man has nothing to fear: User perceptions on web-based information disclosure. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, SOUPS '07, pages 112–121, New York, NY, USA, 2007. ACM.

[2] J. Bortz and N. Döring. *Forschungsmethoden und Evaluation: Für Human- und Sozialwissenschaftler*. Springer-Lehrbuch. Springer London, Limited, 2006.

[3] P. Hubwieser. *Didaktik Der Informatik: Grundlagen, Konzepte, Beispiele*. Springer London, Limited, 2007.

[4] Petra Sütterlin. Vier Lerntypen und wie sie am effektivsten lernen. Internet, Februar 2004. `http://www.philognosie.net/index.php/article/articleview/163/`; Jänner 2014.

[5] M. Speciner, R. Perlman, and C. Kaufman. *Network Security: Private Communications in a Public World*. Pearson Education, 2002.

[6] M.A. Bishop. *Introduction to computer security*. Addison-Wesley, 2005.

[7] Viktor Mayer-Schönberger and Kenneth Cukier. *Big Data: Die Revolution, die unser Leben verändern wird*. Münchner Verlagsgruppe GmbH, 2013.

[8] Murillo Pontual, Andreas Gampe, Omar Chowdhury, Bazoumana Kone, Md. Shamim Ashik, and William H. Winsborough. The privacy in the time of the internet: Secrecy vs transparency. In *Proceedings of the Second ACM Conference on Data and Application Security and Privacy*, CODASPY '12, pages 133–140, New York, NY, USA, 2012. ACM.

[9] Kulsoom Abdullah, Gregory Conti, and Edward Sobiesk. Self-monitoring of web-based information disclosure. In *Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society*, WPES '07, pages 56–59, New York, NY, USA, 2007. ACM.

[10] Gregory Conti. Googling considered harmful. In *Proceedings of the 2006 Workshop on New Security Paradigms*, NSPW '06, pages 67–76, New York, NY, USA, 2007. ACM.

[11] Kai Uhlemeyer. Portable privacy. Internet, August 2009. `http://portableprivacy.org/`; Februar 2014.

[12] André de Guillaume. *Weltherrschaft für Anfänger: Das Handbuch für angehende Diktatoren*, page 54. Bastei Lübbe, 1 edition, 2008.

[13] PRIME Privacy and Identity Management for Europe. Prime general public tutorial and advanced tutorial. 2009. https://www.prime-project.eu/tutorials; August 2009.

[14] Selbstdatenschutz & digitale Selbstverteidigung. Technical report. http://www.selbstdatenschutz.info/; Dezember 2013.

[15] Mikael Berglund Jacob Palme. Anonymity on the Internet. 2002. http://people.dsv.su.se/~jpalme/society/anonymity.html; Dezember 2013.

[16] Amtsblatt der Europäischen Union; Richtlinie 2006/24/EG des europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung. Technical report. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:DE:PDF; Dezember 2013.

[17] Mag. Martina Ertler. Grundzüge der Vorratsdatenspeicherung. Internet, Wirtschaftskammer Österreich, Jänner 2012. https://www.wko.at/Content.Node/branchen/oe/sparte_iuc/Unternehmensberatung-und-Informationstechnologie/IT_Dienstleistung/News/Grundzuege_der_Vorratsdatenspeicherung.html; Dezember 2013.

[18] Patrick Beuth. Der verräterische Fingerabdruck des Browsers. Internet, November 2012. http://www.zeit.de/digital/datenschutz/2012-11/browser-fingerprint-diplomarbeit; Jänner 2014.

[19] Tom Zeller Jr. Michael Barbaro. A face is exposed for aol searcher no. 4417749. Internet, November 2006. http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all&_r=0; Jänner 2014.

[20] Werner Stangl. Lernstrategien - Lerntypen - Lernstile. Internet, April 2002. http://arbeitsblaetter.stangl-taller.at/LERNEN/Lernstrategien.shtml; Jänner 2014.

[21] comScore Reports January 2014 U.S. Smartphone Subscriber Market Share. Technical report. http://www.comscore.com/Insights/Press_Releases/2014/3/comScore_Reports_January_2014_US_Smartphone_Subscriber_Market_Share; März 2014.

[22] Internetkriminalität in Österreich - die unterschätzte Gefahr! April 2014. http://www.vvo.at/internetkriminalitat-in-osterreich-die-unterschatzte-gefahr.html; Mai 2014.

[23] Gesamte Rechtsvorschrift für Datenschutzgesetz 2000. Mai 2014. http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597; Mai 2014.

[24] Datendiebstahlsstatistik für 2013: 552 Millionen Nutzerkonten gestohlen. April 2014. http://www.nzz.ch/aktuell/digital/552-millionen-nutzerkonten-gestohlen-1.18280083; Mai 2014.

[25] Software scannt Facebook-Profile von Bewerbern. März 2014. http://www.welt.de/wirtschaft/karriere/article125314665/Software-scannt-Facebook-Profile-von-Bewerbern.html; Mai 2014.