Masterarbeit

Weiterentwicklung und Implementierung des Projekts "Instahub" für die Sekundarstufe I mit dem Themenschwerpunkt Datenschutz

April 2019

Eingereicht von:

Jan Savelsberg

Matrikelnummer:

213100964

Betreuer: Prof. Dr. Stefan Müller

Alexander Hug

Universität Koblenz-Landau, Campus Koblenz

Fachbereich 4

Institut für Computervisualistik

<u>Eidesstattliche Erklärung:</u>

Hiermit bestätige ich, dass die vorliegende Arbeit von mir selbständig verfasst wurde und ich keine anderen als die angegebenen Hilfsmittel – insbesondere keine im Quellenverzeichnis nicht benannten Internet-Quellen – benutzt habe und die Arbeit von mir vorher nicht in einem anderen Prüfungsverfahren eingereicht wurde. Die eingereichte schriftliche Fassung entspricht der auf dem elektronischen Speichermedium (CD-ROM). Mit der Einstellung dieser Arbeit in die Bibliothek bin ich einverstanden.

_____

Ort, Datum, Unterschrift

Für die Unterstützung in allen Bereichen,

möchte ich mich bei

Alexander Hug,

als wissenschaftlicher Mitarbeiter der Fachdidaktik Informatik,

der mir bei allen Problemen im Laufe der Arbeit mit Rat und Tat zur Seite stand,

Prof. Dr. Stefan Müller,

als Professor, für die Betreuung meiner Arbeit,

Julian Dorn

als Betreiber von Instahub, der mir durch sein Projekt und Hilfe diese Arbeit erst ermöglicht hat,

Martin Ortseifer und **Maximilian Blaum,**

als Vollzeitlehrer, die mir in ihrem Unterricht die Durchführung meiner Reihe ermöglicht haben,

bei meinen **engen Freunden und Familie**, die durch Ideen und Kritik großen Einfluss genommen haben,

sowie bei meiner **Verlobten**, die während der Entwicklung und Korrektur

immer für mich da gewesen ist,

bedanken

Inhaltsverzeichnis

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

ABKÜRUNGSVERZEICHNIS

AB:	Arbeitsblatt
BDSG:	Bundesdatenschutzgesetz
DSGVO:	Datenschutz-Grundverordnung
EA:	Einzelarbeit
GA:	Gruppenarbeit
LDSG:	Landesdatenschutzgesetz
LV:	Lehrervortrag
PA:	Partnerarbeit
SV:	Schülervortrag
UE:	Unterrichtseinheit(en)

1. Einleitung

1.1 Einführung in den Themenbereich

„Zuckerberg verspricht mehr Privatsphäre bei *Facebook*“, so die Schlagzeile der Frankfurter Allgemeine Zeitung im März 2019 (FAZ 2019). Es wird darüber berichtet, wie Mark Zuckerberg fehlende Datenschutzmaßnahmen einräumt und Besserung verspricht. Seit dem Datenskandal im März 2018 um Cambridge Analytica[1], ist *Facebook* bis heute das umstrittenste Soziale Netzwerk hinsichtlich des Datenschutzes. Gleichzeitig gehört es zu den Umsatzstärksten. Knapp ein Jahr nachdem die neue Datenschutz-Grundverordnung in Kraft getreten ist, räumt der Vorstandsvorsitzende des führenden Netzwerks ein, dass die Daten der Nutzer nicht so sicher sind, wie sie eigentlich sein sollten. Dieser Umstand macht deutlich, wie wichtig und aktuell die Datenschutzthematik ist. Besonders im Bezug auf Soziale Netzwerke, welche vom Großteil der Bevölkerung weltweit genutzt werden (Stevens 2018), ist die Relevanz nicht abzustreiten. Die Tatsache, dass trotz anhaltender Skandale und undurchsichtiger Umstände die Anzahl von Nutzern nicht abnimmt, zeigt, dass der Aufklärungsaspekt künftig eine noch wichtigere Rolle spielen wird, als bisher. Unter diesen Gesichtspunkten muss sich nun die Frage gestellt werden, welche Aufgabe das Bildungssystem in dieser Situation übernimmt.

1.2 Forschungsfrage

Die vorliegende Arbeit soll das hochaktuelle Thema des Datenschutzes verdeutlichen. Insbesondere ist es das Ziel des Autors, die Einführung datenschutzspezifischer Kompetenzen in der Klassenstufe 5 bis 7 zu erarbeiten. In der Studie nach Hug (Hug 2018) zeigt sich, dass besonders im Alter der Sekundarstufe I Defizite in gerade diesen Kompetenzen zu finden sind. Für diese Arbeit wird der Fokus speziell auf die Nutzung von Sozialen Netzwerken gelegt. Durch die Interpretation der Statistiken 2018 (Stevens 2018) konnte gezeigt werden, dass knapp 78% der Internetnutzer auf Sozialen Medien verkehren. Je jünger die Befragten, desto höher die prozentuale Anzahl der Nutzer. Diese Zahlen lassen sich nur bedingt auf die gewählte Altersgruppe anwenden, da eine Nutzung der Sozialen Netzwerken erst ab 16 Jahren

[1] Britisches Datenanalysunternehmen. Bekannt dadurch, dass es 2018 unerlaubt Daten von über 80 Millionen Facebookkunden verarbeitet hat und dadurch Einfluss auf den US-Wahlkampf nahm.

gestattet ist (Europäische Union 04.05.2016 Art. 8 Abs. 1). Nach einer eigenen Umfrage in Lerngruppen der Orientierungsstufe (123 Schüler[2]) an einem Gymnasium in Rheinland-Pfalz ergaben sich trotz des niedrigen Alters ähnliche Ergebnisse (siehe Anhang 1). Das lässt die Vermutung zu, dass sich die Ergebnisse der aktuellen Statistiken über die Nutzung Sozialer Netzwerke auch auf eine Altersgruppe unter 16 Jahren beziehen lassen.

Von den oben angeführten Argumenten ausgehend (Aktualität, Nutzung, mangelnde Kompetenz), ist ein sicherer Umgang mit personenbezogenen Daten im Kontext Sozialer Netzwerke in einer Lerngruppe der Orientierungsstufe ein wünschenswerter Zustand. Hieraus wurde die Forschungsfrage dieser Arbeit herausgearbeitet:

Wie gestaltet sich eine Unterrichtsreihe zum Thema Datenschutz im Kontext Sozialer Netzwerke in der Orientierungsstufe eines Gymnasiums?

Hierzu wird eine bereits etablierte Plattform (*Instahub*[3]) als Grundlage genutzt, die eigens für den Unterrichtseinsatz entwickelt wurde. Der Kontext bietet genügend Motivation für Schülerinnen und Schüler, sodass sich die Entwicklung der Unterrichtsreihe hauptsächlich nach dem Erreichen möglicher Kompetenzen richten kann. Neben der theoretischen Entwicklung der Unterrichtsreihe wird diese in die vorhandene Implementierung eingepflegt und in ihrem Ansatz in zwei geeigneten Lerngruppen eines rheinland-pfälzischen Gymnasiums getestet. Aus Letzterem lassen sich eventuelle Schlüsse auf die Fortführung der Reihe oder etwaige Verbesserungen der entwickelten Unterrichtsmaterialien ziehen.

1.3 Inhaltliche Gliederung der Arbeit

Im ersten Teil der Arbeit wird zunächst die theoretische Grundlage für die Unterrichtsreihe ausgearbeitet. Es werden Begriffe wie *Datenschutz* und *Privatsphäre* mit Hilfe von geeigneter Fachliteratur erläutert und definiert. Daraufhin werden die wichtigsten Punkte der geltenden DSGVO genannt und umschrieben, welche die Anwender von Sozialen Netzwerken betreffen. Außerdem werden mögliche Gefahren im Umgang mit genannten Netzwerken sowie passende Schutzmaßnahmen diesbezüglich erläutert. Im letzten Teil der Grundlagenanalyse

[2] Im Folgenden ist mit „Schüler“ sowohl die männliche als auch die weibliche Form gemeint.
[3] https://instahub.org/

wird der Datenschutzaspekt über das Datenschutzkompetenzmodell in den schulischen Bezug gebracht.

Im nächsten Kapitel (Kapitel 3) wird die Lehr-Lernplattform *Instahub* vorgestellt. Sie wird im Hinblick auf Datenschutz im Unterricht betrachtet. Dem folgt ein Einschub über die Grundlagen von Datenbanken in der Sekundarstufe I, da dies der Hauptinhalt der schon existierenden *Instahub*-Unterrichtsreihe ist und auch in der zu entwickelnden Reihe eine Rolle spielen soll.

In Kapitel 4 wird dann die entwickelte Unterrichtsreihe unter didaktischen und methodischen Gesichtspunkten beschrieben. Es beinhaltet die Konzeption und Unterrichtsideen sowie eine Einordnung in den Lehrplan. Anschließend wird die Unterrichtsreihe als Ganzes betrachtet und Weiterentwicklungs- und Variationsmöglichkeiten werden hier herausgearbeitet.

In den letzten beiden Kapiteln wird zunächst ein Teil der Unterrichtsreihe durch die Erprobung in zwei geeigneten Lerngruppen evaluiert. Etwaige Verbesserungen und Änderungen werden hier behandelt. Anschließend werden die Gesamtergebnisse zusammengefasst und zukunftsorientiert betrachtet. Letzteres soll einen Ausblick auf die mögliche Weiterentwicklung und Nutzung der Unterrichtsreihe zu schulischen Zwecken geben.

2. Grundlagen: Datenschutz

Schwerpunkt dieser Arbeit ist die Entwicklung einer Unterrichtsreihe zum Thema Datenschutz im Kontext der Verwendung Sozialer Netzwerke, geeignet für die Altersklassen einer Orientierungsstufe. Im folgenden Kapitel stehen die Definition und Erläuterung ausgewählter Fachbegriffe und die Einordnung dieser im schulischen Kontext im Vordergrund.

2.1 Definitionen

Wichtigster Grundbegriff der Arbeit ist der des **Datenschutzes**. Diese Komposition aus *Daten* und *Schutz* impliziert bei unvoreingenommener Betrachtung erst einmal einen Zustand, in dem ein gewisser Satz an Daten zu schützen ist. Zuerst erwähnt wurde der Begriff genau unter diesen Umständen im Hessischen Datenschutzgesetz 1970 (Landesrecht Hessen 1970). Letzteres war die erste verabschiedete Verordnung, welche den Datenschutz als das sichere Aufbewahren von digitalen Daten beschrieb. Datensicherheit bedeutete hier das Vermeiden von Verlust, Veränderung und Diebstahl. Durch Ulrich Seidel (Seidel 1970, S. 62-65) wurde der Begriff Datenschutz in seiner Bedeutung in den Schutz von *personenbezogener Daten* umgewandelt. Eine entsprechende Definition deckt demnach den *Schutz vor missbräuchlicher Datenverarbeitung*, den *Schutz des Rechts auf informationelle Selbstbestimmung*[4] und des *Persönlichkeitsrechts* sowie den *Schutz der Privatsphäre* ab.

Von **Daten** spricht man bei Angaben, Werten oder (formulierbaren) Befunden, die u.a. durch Messungen oder Beobachtung gefunden werden können (Bibliographisches Institut GmbH 2015). Erst durch eine Interpretation dieser Daten mit einem dem Kontext entsprechenden Sinn werden diese zu Informationen (Bodendorf 2003, S. 1). Ein Beispiel hierfür wären Angaben zu einer Person, wie Name, Geburtstag, Geschlecht, usw. Diese Angaben sind ein reiner Datensatz, der erst mit dem Bezug zu einer realen Person eine Sinnhaftigkeit erhält. Im weiteren Sinne wird in dieser Arbeit meistens der Begriff Daten mit digital gespeicherten Datensätzen[5] gleichgesetzt. Von digital gespeicherten Daten spricht man, sobald ein Datensatz in einer maschinell auslesbaren, diskreten Form gespeichert wird.

[4] Begriff geht aus der Volksabstimmung 1983 (S. 7 Abs. 3) hervor
[5] Zusammengehörige Daten (z.B. über eine Person, zu einem Fall gehörige etc.)

Im Zuge des Datenschutzes sind vor allem **personenbezogene Daten** von größter Wichtigkeit. Personenbezogene Daten sind nach der DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen (Europäische Union 04.05.2016, Art. 4). Genauer definiert wird dies durch die Erkennbarkeit einer Identität durch eine Anhäufung von Daten (z.B. Name, Geburtsort, Merkmale etc.) zu einem realen Individuum. Bei einer Identität wird (gem. DSGVO Art. 4) wiederum unterschieden zwischen einer physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen und sozialen Identität.

Um zu klären, in welchen Fällen es sich um **missbräuchliche Datenverarbeitung** handelt, muss zunächst geklärt werden, welche Aktionen sich überhaupt hinter einer **Verarbeitung** von Daten verbergen. Die DSGVO beschreibt dies als jeglichen Vorgang bzw. Vorgangsreihe mit personenbezogenen Daten. Beispielhaft genannt werden „das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“ (Art. 4, Abs. 2 DSGVO). Diese Definition umfasst sowohl manuelle als auch vollständig automatisierte Vorgänge sowie deren Mischformen. Die Bezeichnung „missbräuchlicher Umgang“ beinhaltet demnach alle Vorgänge der Verarbeitung, die gegen geltendes Datenschutzrecht (u.a. DSGVO) verstoßen. Umfang, Bedingungen und Verstöße der DSGVO werden im Abschnitt 2.2 näher erörtert.

Das Persönlichkeitsrecht ist (gem. GG Art. 2 Abs. 1) ein Grundrecht in der Bundesrepublik Deutschland (Bundesamt für Justiz und für Verbraucherschutz 2017). Dieses Recht bestimmt in Verbindung mit Art. 1 Abs 1 GG das Recht zur **informationellen Selbstbestimmung**. Dieses formuliert die Volkszählung 1983 (Bundesverfassungsgericht 1983, IV.) als Grundrecht. Zusammenfassend betrachtet, bestimmt dieser Grundsatzentscheid, dass jede Person alleinig über die Verwendung und Preisgabe der eigenen, personenbezogenen Daten entscheiden dar, sofern durch die Verweigerung dessen nicht richterliche und polizeiliche Arbeit (öffentliche Gewalt) beeinträchtigt wird (Art. 6 Abs. 1 DSGVO). Weitere Ausnahmen können unter bestimmten Bedingungen auch statistische Zwecke, im öffentlichen Interesse liegende

Archivzwecke oder Forschungszwecke[6] sein. Dieses Recht unterscheidet per Gesetz nicht zwischen sensiblen und unsensiblen Daten. **Sensible Daten** sind Daten, die Rückschlüsse auf rassische und ethnische Herkunft, religiöse Ansichten, politische Meinungen und Sexualleben zulassen. Ebenso biometrische und genetische Daten und Daten mit Bezug auf die Gesundheit, die einer realen Person zugeordnet werden können (Art. 9 Abs. 1 DSGVO). Der Begriff der **unsensiblen Daten** ist nicht näher definiert, bezeichnet allgemein jedoch die Daten, auf welche die genannten Kriterien nicht zutreffen. Weiterhin wird in ähnlichen Zusammenhängen der **Selbstdatenschutz** erwähnt. Dieser beschreibt die technischen, organisatorischen und rechtlichen Maßnahmen, die ein Individuum ergreift, um seine informationelle Selbstbestimmung zu gewährleisten. Das Wissen um Gegenmaßnahmen und ihre Anwendung werden ebenfalls unter diesem Begriff zusammengefasst (Bundesministerium für Bildung und Forschung 13.10.2014).

Oft im Zusammenhang zum Schutz personenbezogener Daten wird der Begriff der **Privatsphäre** erwähnt (vgl. Das Europäische Parlament und der Rat der europäischen Union 2002 Abs. 1) und bleibt noch zu definieren. Abweichend von den klaren Definitionen zuvor ist die Privatsphäre nicht klar ausgelegt. Betrachtet man zunächst die Privatsphäre als einen vom Datenschutz unabhängigen Begriff, so lässt sich vermuten, dass es sich um Informationen über eine Person handelt, die nicht für die Öffentlichkeit bestimmt sind. Im Bezug auf das dieser Arbeit zugrundeliegende Thema könnte man die Privatsphäre mit den zu schützenden, personenbezogenen Daten gleichsetzen. Egger und Schillinger (1997) beschreiben die Privatsphäre durch drei Hypothesen.

(1) Das Sphärenmodell[7] geht davon aus, dass sich „Datenschatten“ in unterschiedliche Sensibilitätsgruppen einordnen lassen. Genannt werden hier im Bereich der sensiblen Daten Individual-, Privat- und Geheimsphäre sowie Öffentlichkeits-, Sozial-, Vertrauens- und Intimsphäre. Letzteres beschreibt den Bereich der Persönlichkeit, auf den nur das Individuum selbst zugreifen kann. Die Idee dahinter ist, dass man durch Aufteilung der Daten in genannte Sphären einen beschränkten Zugriff auf spezifische Informationen bewerkstelligen könnte. Ein

[6] Sowohl historische als auch wissenschaftliche Forschung

[7] Hier kann von einem Modell ausgegangen werden, da die Mosaik- und Rollenhypothese auf diesem Modell aufbauen. In der Literatur wird jedoch ebenfalls von einer Hypothese gesprochen.

Datentransfer wäre nach der Hypothese nur in den Überschneidungssektoren nötig und würde so die anderen Sphären nicht bedrohen oder beeinflussen. Der Nachteil der Sphärenhypothese ist deutlich: Die Grenzen zwischen den Sektoren sind nicht immer klar aufzuweisen und nur schwer definierbar. Außerdem müsste festgelegt werden, wer berechtigt dazu ist, die sensiblen Daten den Privatsphären zuzuordnen.

(2) Die zweite Hypothese, Mosaikhypothese genannt, erweitert die Sphärenhypothese. Neben den zuerst geforderten Teilsphären soll die Mosaikhypothese zudem noch die Daten mit einbeziehen, welche durch Verknüpfung mehrerer Datensätze aus unterschiedlichen Sphären eventuelle Rückschlüsse auf Daten aus der Intimsphäre ermöglichen. Einfach ausgedrückt sollen auch Datenverarbeitungsvorgänge, die in verschiedenen Ebenen arbeiten, betrachtet werden. Neben den schon genannten, nicht unerheblichen Nachteilen kommt hier noch einmal eine unfassbare Breite an Möglichkeiten hinzu, Daten auszuwerten.

(3) Die Rollenhypothese ist die Dritte. Sie geht davon aus, dass eine Person immer Träger mehrerer Rollen in der Gesellschaft ist und sich die Persönlichkeit aus allen Rollen zusammensetzt. Das würde wiederum bedeuten, dass die Sensibilität der Daten auch von der Rolle des Interaktionspartners abhängt. Damit wäre subjektiv betrachtet jedes Datum ein schützenswertes Gut.

2.2 Die Datenschutz-Grundverordnung

Im nachfolgenden Abschnitt werden die noch nicht genannten Grundaspekte der DSGVO erörtert. Da eine Abhandlung der vollständigen DSGVO den Rahmen dieser Arbeit sprengen würde, werden nur für dieses Thema relevante Bereiche ausgearbeitet. Letzteres entspricht denen für den Informatikunterricht umsetzbaren Gesetzesteilen, die den Schutz personenbezogener Daten aus Sicht der Betroffenen (hier: Schüler) definieren.

Die aktuelle Fassung der DSGVO wurde am 27. April 2016 verabschiedet und trat am 25. Mai 2018 in Kraft[8]. Damit löste die DSGVO die bis dahin geltenden Datenschutzverordnung von

[8] Zusätzlich wurde eine Schonfrist für Unternehmen bis Jahresbeginn 2019 bekanntgegeben, die (vor allem kleinen Unternehmen bzw. Unternehmern) die Möglichkeit einräumt, den Zeitraum für eine korrekte Umsetzung zu nutzen.

1995 (Europäische Gemeinschaft 1995) ab. Die aktuellen Bestimmungen teilen sich in elf Unterkapitel mit ihren jeweiligen Artikeln auf. Ausgehend von den Themen besagter Artikel, erfordert es eine genauere Betrachtung der Artikel 5 bis 23 (*Grundsätze* und *Rechte der betroffenen Person*). Wichtige Elemente der allgemeinen Bestimmungen (Art. 1-4) wurden bereits im Abschnitt 2.1 näher erörtert.

2.2.1 Einwilligung betroffener Personen

Art. 5 Abs. 1 bestimmt, dass personenbezogene Daten nur dann verarbeitet werden dürfen, wenn entweder eine direkte **Einwilligung** der betroffenen Person vorliegt, die einen oder mehrere Zwecke der Verarbeitung beschreiben oder die Einhaltung von Verträgen, in denen die genannte Person involviert ist, nur dann erfolgen können, wenn gewisse Daten verarbeitet werden dürfen. Weitere Ausnahmen sind Situationen, in denen die öffentliche Sicherheit oder die Sicherheit einer unbeteiligten Person in Gefahr ist. Der Begriff des Zwecks verweist hier auf selbigen Artikel, der zusätzlich festlegt, dass die Einwilligung fest an einen Grund geknüpft ist, in welchem Rahmen die Verarbeitung stattfindet. Ist dieser Zweck nicht mehr gegeben, so entfällt die ursprüngliche Einwilligung dahingehend. Diese Zweckbindung wird durch Ausnahmen hiervon erweitert. Sollten persönliche Rechte des Betroffenen (Grundrechte oder vergleichbare) oder das öffentliche Interesse bei der Ausübung eines Öffentlichkeitsdienstes durch die Person gefährdet sein, so wird keine zusätzliche Einwilligung benötigt (vgl. Art. 6 DSGVO).

Die im letzten Abschnitt genannte Einwilligung wird durch Artikel 7 und 8 genauer definiert. Die Einwilligung muss (Art. 7 Abs. 1 ff. DSGVO) in einer abrufbaren, verständlichen, klar definierten Form vorhanden sein. Zudem ist ein Widerrufen dieser zu jeder Zeit möglich. Das bedeutet, dass ein Widerruf (in schriftlicher Form) die vollständige Löschung der in diesem Zusammenhang verwendeten Daten nach sich zieht. Daraus folgt, dass dem Verarbeitenden[9] die Pflicht obliegt, passende Daten in einem geordneten, auffindbaren Zustand zu speichern[10]. Dieser Zustand wird durch die DSGVO als *Datenminimierung* bezeichnet. Der Begriff der

[9] Hier: Unternehmen bzw. Unternehmer

[10] „Speichern“ kann in diesem Zusammenhang auch z.B. ein „abgeheftetes Dokument“ bedeuten.

Datenminimierung beschreibt allgemein das Erzielen der geringsten Anzahl von Datensätzen und dem Vermeiden von Redundanz bei der Speicherung (vgl. Erwägungsgrund 156 DSGVO).

Für diese Arbeit besonders interessant ist der anschließende Artikel 8. Dieser legt die Bedingungen an die Einwilligung fest, falls es sich bei der betroffenen Person um eine minderjährige Person handelt. Eine Einwilligung ist in diesem Falle nur rechtmäßig, wenn eine Person das sechzehnte Lebensjahr erreicht hat. Sollte dies nicht zutreffen, so muss eine entsprechende Bewilligung eines Erziehungsberechtigten vorliegen. Zudem muss der Verantwortliche „unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen“ (Art. 8 Abs. 2 DSGVO) vorweisen können, die nachweisen können, ob eine elterliche Zustimmung wirklich gegeben ist. Dies könnte z.B. mit Hilfe einer Kopie des Ausweises o.ä. erfolgen. Einzelnen Staaten der Europäischen Union ist es erlaubt, diese Regel herunterzusetzen. Ein verpflichtendes Mindestalter ist jedoch das dreizehnte Lebensjahr. Alle anderen Rechte für betroffene Personen bleiben hiervon unberührt.

2.2.2 Rechte der betroffenen Personen

Die einzelnen Rechte der Betroffenen werden durch die Artikel 12-23 definiert.

Artikel 12 bestimmt, dass Verantwortliche die gespeicherten Daten von Personen so ablegen, dass genannte Personen jederzeit einen strukturierten und klar verständlichen Überblick über die verwendeten Daten erlangen können (vgl. 2.2.1). Dies soll völlige Transparenz gewährleisten. Um diese verständliche, strukturierte, transparente Form der Datenbereitstellung zu gewährleisten, darf der Verantwortliche mit Hilfe von Bildsymbolen arbeiten. Das bedeutet, dass hier auch nutzerfreundliche Werkzeuge genutzt werden. Häufig wird dies durch ein sogenanntes *„privacy dashboard“* bewerkstelligt. Dabei handelt es sich um eine abrufbare Oberfläche, meist eine Webseite oder Bestandteil der Anbietersoftware, die alle derzeit verarbeitenden Informationen einer Person in direkter Anbindung an deren Zweck darstellt (Zimmermann und Accorsi 2013). Grundsätzlich ist davon auszugehen, dass auch alle Nutzeranfragen (z.B. Datenlöschungsanträge) von hier aus zu tätigen sind (UC Berkeley School of Information), wenn ein solches Dashboard vorhanden ist. Beispielhaft dafür wäre das

W*indows Privacy Dashboard (WPD)*[11] für Windows 10, die alle aktuellen Privatsphäre-Einstellungen auf einen Blick für den Nutzer verfügbar macht. Abb. 1 zeigt die Übersichtsfunktion der Applikation.

Artikel 13-15 beschreiben weiter, welche Informationen und in welchem Umfang der Verantwortliche diese bereitzustellen hat, um damit so wenige „graue" Zonen in der Datenverarbeitung wie möglich zu bieten. Rechtsanwalt Christian Solmecke bezeichnet in einer Zusammenfassung der DSGVO die Artikel 12-15 passend als ein „umfassendes Auskunftsrecht" (Christian Solmecke 2019).

Artikel 16 und 17 decken die Veränderung sämtlicher personenbezogener Daten ab. Sowohl eine legitime Berichtigung der Daten (Art. 16 Abs. 1) als auch die sofortige Löschung aller vorhandenen Datensätze (Art. 17 Abs. 1) können somit von Betroffenen angefordert werden.

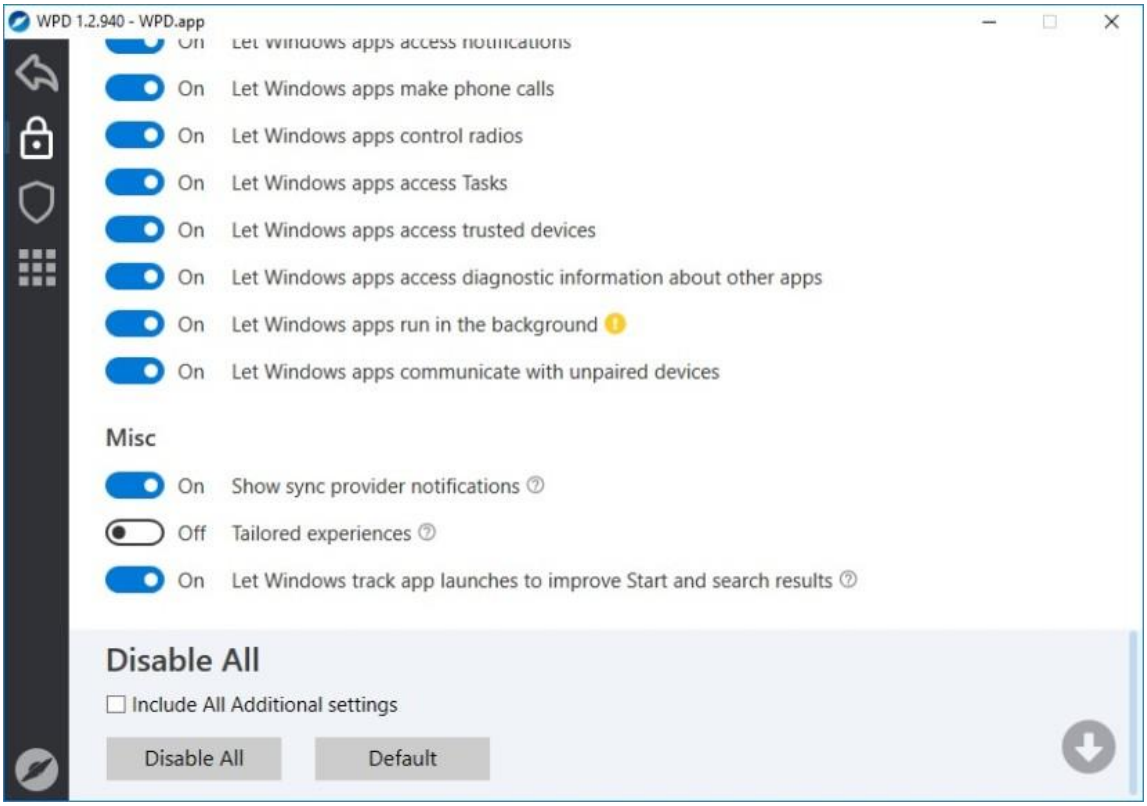


***Abbildung 1**: WPD-Applikation von Windows 10*[12]

[11] www.wpd.app (zuletzt geprüft: 03.04.2019)
[12]Quelle: https://www.computerbild.de/download/Windows-Privacy-Dashboard-WPD-22567087.html (zuletzt geprüft: 03.04.2019)

Diese Gesetze stehen unter den gleichen Ausnahmebedingungen wie in 2.2.1 beschrieben. Besonders der Begriff der Datenminimierung spielt hier eine wichtige Rolle.

Das Recht auf Datenübertragbarkeit wird über Artikel 20 beschrieben. Dieses Recht war in solch einer oder ähnlichen Form zuvor nicht vorhanden. Hiermit ist die betroffene Person in der Lage, sich beim Verantwortlichen die hinterlegten Daten in einem passenden, maschinenlesbaren Format aushändigen zu lassen. Zudem ist es möglich, eine direkte Übertragung zu einem anderen Verantwortlichen, also z.B. einem Konkurrenzunternehmen, anzufordern. Auch hier wird deutlich, wie wichtig es aus Sicht der Verantwortlichen ist, personenbezogene Daten strukturiert und redundanzfrei abzulegen. Aus der Perspektive der betroffenen Person ermöglichen sich dadurch deutlich größere, einfachere Umgangsmöglichkeiten bezüglich der Nutzerfreundlichkeit und der Verwaltung der eigenen Daten. Gerade dieser Gesetzesteil spricht deutlich für die positiven Auswirkungen der DSGVO von 2016.

„Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.“ (Art. 21 Abs. 1 DSGVO) Damit wird gesichert, dass vor allem besonders heikle Entscheidungen über Privatsphäre, oder allgemein den Datenschutz betreffend, nicht automatisiert bearbeitet werden dürfen, wenn personenbezogene Daten behandelt werden. Das **Profiling** bezeichnet hier eine automatisierte Bewertung der Daten. Kritische Themenbereiche der Daten sind z.B. Gesundheit, Wohnort, wirtschaftliche Lage, Arbeitsleistung usw. Es wird sowohl die automatische Analyse als auch die automatische Vorhersage (also die Interpretation der Analyse) untersagt (vgl. Art. 4 Abs. 4).

2.3 Gefahren im Umgang mit Daten

Nachdem die Definition und der Umfang des Begriffes Datenschutz erläutert wurden, werden nun die Situationen beschrieben, die zu dessen Verletzung führen. Dabei werden allgemein Fälle genannt und erläutert, welche sich auf den Themenschwerpunkt Soziale Netzwerke beziehen lassen oder diese direkt betreffen. In der anschließenden Unterrichtsreihe werden diese Fälle bearbeitet und den Schülern bewusst gemacht.

2.3.1 Preisgabe der eigenen Daten

Aus der Sicht eines Schülers ist der Umgang mit den eigenen Daten, die schützenswert sind, der natürlichste Ansatzpunkt, um eine schützenswerte Privatsphäre zu thematisieren. Besonders im Kontext von sozialen Netzwerken ist dies der erste Konfrontationspunkt bei der Anmeldung zu einem solchen Dienst.

Unter **Sozialen Netzwerken** (engl.: Social Network) versteht man eine Gemeinschaft (auch Community genannt) von Nutzern, die eigens für diesen Zweck ein Profil angelegt haben, in dem eine unbestimmte Anzahl von Informationen über diese Person vorhanden ist (vgl. Obar und Wildman 2015). Der Umfang und die Bedeutung der Informationen variieren von Community zu Community. Wie der Begriff Gemeinschaft bereits impliziert, ist die Hauptfunktion des Sozialen Netzwerks die Verbindung zwischen den Nutzern bzw. Profilen (Boyd und Ellison 2007). Vernetzungen sollen so den Austausch von Wissen, Meinungen und vergleichbaren Informationen sowie kollaboratives Arbeiten ermöglichen (Brennan 2010, S. 8-9). Zudem lassen sich Social Network Plattformen in zwei Kategorien einteilen (Alby 2007 S. 89 ff.):

1. Plattformen zur Kommunikation
2. Plattformen, deren zusätzliche Funktion im Kreieren von Nutzerinhalten (engl.: user-generated content) liegt (Videos, Podcasts, Textbeiträge etc.)

Beispiele für die erste Kategorie sind *Facebook*, *LinkedIn*, *Snapchat*, *Twitter* und *Instagram*. Die Plattformen *YouTube*, *Twitch* und *Reddit* lassen sich besser durch die zweite Kategorie einordnen. Die nachfolgende Tabelle gibt eine Übersicht über die inhaltlichen Schwerpunkte der genannten Plattformen. Es gibt noch deutlich mehr nennenswerte Beispiele. Diese wurden aufgrund der Präferenz des Autors ausgewählt.

Plattform	Inhaltsschwerpunkt	zu finden unter
Facebook	- Kommunikation, Bilden von Gemeinschaften (Gruppen) - Verbreiten von Inhalten (Werbung, mediale Inhalte)	www.facebook.com
LinkedIn	- Kommunikation - In Verbindung stehen/bleiben - Hauptsächlich geschäftlicher Hintergrund	www.linkedin.com
Snapchat	- Austausch von Bildern und Kurzvideos - Inhalte nur temporär verfügbar	www.snapchat.com (Applikation für mobiles Endgerät)
Twitter	- Kommunikation - Wird oft zum Ausdruck der eigenen Meinung, Bewertungen oder Neuigkeiten verwendet - Nachrichten- und Informationsquelle	www.twitter.com
Instagram	- Austausch von Bildern und Kurzvideos - Inhalte permanent verfügbar - Selbstdarstellung / Werbung	www.instagram.com (Applikation für mobiles Endgerät)
YouTube	- Videostreaming-Portal - Kreieren von Videoinhalten - Entwicklung einer Fangemeinde zu (sog.) Kanälen	www.youtube.com
Twitch	- Livestream, direkter Kontakt zum Streamer - Entwicklung einer Fangemeinde	www.twitch.com
Reddit	- Anonyme Kommunikation (Verwendung von Pseudonymen) - Kreieren von Inhalten wie Videos, Textbeiträgen u.v.m., sowie gegenseitige Bewertung - Häufig kritische Themen (aktuell, politisch, …) mit hoher Medienpräsenz	www.reddit.com

***Tabelle 1**: Inhaltliche Schwerpunkte diverser Sozialer Netzwerke*

Eine weitere Eigenschaft, die fast alle Sozialen Netzwerke aufweisen, ist die Befreiung von jeglichen Gebühren zum Nutzen der Dienste. Es gibt nur wenige Ausnahmen davon und meistens handelt es sich dabei um ein gebührenpflichtiges Zusatzkonzept zum eigentlichen

Medium (z.B. YouTube-Premium). Doch das äußerliche Bild trügt. Ganz nach dem populären Zitat „If you are not paying for it, you're not the customer; you're the product being sold." [13] (blue_beetle 2010) finanzieren sich Soziale Medien weltweit über die Nutzung personenbezogener Daten. Die Haupteinnahmequelle ist das Schalten von Werbung. Der Anreiz für Unternehmen Werbung auf den Plattformen zu schalten ist die gigantische Menge an Nutzern und damit potentiellen Kunden. Werden nun die Daten der Nutzer umfangreich analysiert, kann durch den Verantwortlichen ein aussagekräftiges Profil des Konsumenten erstellt werden. Dieses wiederum wird dazu verwendet, Usern auf sie abgeschnittene Werbung zu bieten. Es ist daher leicht vorstellbar, dass Gewinne mit Werbeeinnahmen dadurch maximiert werden können. Nutzungsverhalten, Verweildauer auf bestimmten Seiten, Interessen, selbst-veröffentlichte Informationen und Filtern nach Stichwörtern in öffentlichen Beiträgen sind nur einige der Datenquellen, die sozialen Plattformen zur Verfügung stehen. Auch nach neuem, geltendem Recht der DSGVO fällt das Verarbeiten personenbezogener Daten zu Werbezwecken unter „einem berechtigten Interesse dienend" (ErwGr. 47 DSGVO).

Die direkte Gefahr, die in diesen Tatsachen liegt, ist dass der Nutzer, also auch der Schüler aus unserer Sicht, sich nicht im Klaren sind, welche Daten überhaupt erfasst und verarbeitet werden. Schlussendlich liegt es im Aufgabenbereich des Nutzers zu entscheiden, welche Daten für ihn als schützenswert einzuordnen sind. Mangelndes Wissen über genannte Punkte ist vor allem der unübersichtlichen Präsentation dieser Informationen geschuldet. Allein die Datenrichtlinien von *Facebook*, die nur beschreiben, welche Daten verarbeitet werden, haben einen Umfang von ca. 4700 Wörtern auf acht Seiten. Diese Richtlinien werden zusammen mit den Nutzungsbedingungen und Richtlinien zur Verwendung von Cookies mit wenigen Klicks bei der Anmeldung bestätigt. Eine Befragung von Facebooknutzern zeigt, dass gerade einmal 21% der Befragten sich als „von *Facebook* ausreichend über die Richtlinien informiert" fühlten (Rothmann 2017, S10). Schätzungsweise ist die tatsächliche Anzahl wesentlich geringer, da die Umfrage auf einer persönlichen Einschätzung als Antwort basiert. Dies zeigt, dass nicht nur das Nutzen der Plattformen selbst betrachtet werden muss, sondern ebenfalls der Prozess der

[13] dt.: Wenn du dafür nicht bezahlst, bist du nicht der Nutzer, sondern das Produkt.

Datenpreisgabe. Hier kommt es durch Fehleinschätzung und unreflektiertem Verhalten zur Preisgabe von Daten in einem Ausmaß, dem der Nutzer sich nicht gänzlich bewusst ist.

Als zusätzliche Gefahrenquelle sieht Eckert (Eckert 2013, S. 901 ff.) das Verwenden von Applikationen auf mobilen Endgeräten. Meistens werden beispielhaft genannte Soziale Plattformen auch als mobile Version angeboten. Dadurch wird die Menge an auszuwertenden Daten durch neue Elemente stark vergrößert. Zum Beispiel können GPS und Bild-Metadaten genutzt werden, um ein deutlich besseres Bewegungsprofil der Nutzer zu erstellen. Stimmerkennung sowie Kalender- und Kontaktdaten sind nur einige der zusätzlichen Datenquellen.

Eine weitere Möglichkeit, an persönliche Daten zu gelangen, ist Schadsoftware. Da dies nicht Hauptbestandteil der Unterrichtsreihe ist, wird dieser Themenbereich nicht weiter ausdifferenziert, soll aber der Vollständigkeit halber nicht ungenannt bleiben.

2.3.2 Überwachung

Die Umstände von Überwachung sind die wahrscheinlich widersprüchlichsten im Zusammenhang mit Datenschutz. Allgemein bedeutet Überwachung, dass zu einem bestimmten Grund (zum Beispiel Gefahr im Verzug) Informationen (hier: über eine Person) erhoben werden, um das Allgemeinwohl und das Wohl einzelner Personen zu schützen. Dabei dürfen weder nach DSGVO noch nach anderem geltenden Recht die Grundrechte einer Person beeinträchtigt werden. Die Legitimation von Überwachung liegt also im Schutz der Personen, indem der Schutz von personenbezogenen Daten beeinträchtigt wird, was zunächst einen Widerspruch vermuten lässt. Es ist also von größter Wichtigkeit, abgesteckte Grenzen zu wahren und vor allem diese zu kennen.

Theoretisch gesehen ist es möglich, jede Person anhand der biometrischen Daten aufzuspüren. Diese werden grundsätzlich immer bei dem Erstellen von Personalausweis oder Reisepass eingefordert. Das bedeutet, es wäre nur ein Zugriff auf besagte Daten, ein (nicht ganz unbeträchtlicher) Zugang zu öffentlichen Videokameras (z.B. Überwachungs- oder Verkehrskameras) und ein funktionierender Algorithmus für diese Zwecke nötig, um einen vollständigen Bewegungsablauf einer Person zu erstellen. Informationen dieser Art können

mit Telefon- und Internetnutzungsdaten ergänzt werden (vgl. Bundespolizeipräsidiums und Deutsche Bahn AG 2017-2018, S. 23-35).

Ein weiterer Aspekt der Überwachung ist die Überwachung im wirtschaftlichen Sinne. Im Kapitel 2.2.2 wurde bereits angedeutet, dass die Möglichkeit besteht, personenbezogene Daten zu nutzen, um Werbung zu personalisieren. Dazu verwendet werden unter anderem *Cookies*[14]. Grundsätzlich handelt es sich um einen kurzen Abschnitt von Code, der zwischen Webbrowser (Nutzer) und Webserver (Anbieter) ausgetauscht wird. Dieser Code dient dazu, einen Nutzer als ein und dieselbe Person wiederzuerkennen. Dadurch können benutzerspezifische Daten über einen längeren Zeitraum erhalten bleiben, ohne dass ein Austausch von persönlichen Daten erforderlich ist (vgl. Schwartz 2001). Beispielsweise kann so der Warenkorb in einem Onlineshop beim wiederholten Einwählen in den Shop einem bestimmten Nutzer zugeordnet werden und so ein personalisiertes Ergebnis der Seite präsentieren. Die Schattenseite dieser Maßnahme ist, dass Informationen, welche diese Cookies bereitstellen, zum Erstellen von Nutzerprofilen genutzt werden können. Wenn dies über mehrere Webseitenanbieter hinaus erfolgt, wird dies in der Webanalytik als *User-Tracking* bezeichnet (Oberle et al. 2003, S. 155-164). Zudem verwenden große Unternehmen, beispielsweise *Amazon*[15]*,* besagte Daten, um ihren Profit im eigenen Verkauf zu steigern. Wählt man ein Produkt immer wieder an, so wird dies registriert und führt dazu, dass bei der Wiederanwahl desselben Produkts ein höherer Preis angegeben wird. So werden Produkte, über die sich der Kunde eventuell mehrfach informiert, was wiederum durch Cookies erkannt wird, zu einem höheren Endpreis für eben diese Kunden angeboten. Ebenfalls wird bei der Nutzung von mobilen Endgeräten unterschieden, welches Gerät genutzt wird. Theoretisch gesehen kann ein Kunde mit einem teureren Smartphone auch mehr Geld für andere Produkte ausgeben. In Fachkreisen wird diese Marketingstrategie als *„Dynamic Pricing“* bezeichnet und deckt durchaus noch mehr Möglichkeiten zur Preisoptimierung ab (International World Wide Web Conference Committee 2016).

[14] ursprünglich von dem Begriff „magic cookies“ abgeleitet. Ein kurzes Programm, das ähnliche Aufgaben wie heutige Cookies erledigte

[15] www.amazon.com (zuletzt geprüft: 03.04.2019)

Die genannten Aspekte sind nur ein kleiner Teil des Ausmaßes, das die Auswertung von personenbezogenen Daten im Bezug auf Überwachung annehmen kann. Es steht außer Frage, ob eine Aufklärung von Nutzern (in Falle der Arbeit: Schülern) nötig ist.

2.3.3 Schutzmaßnahmen

Nachdem die grundlegenden Gefahren des Datenschutzes aufgezeigt wurden, werden nun mögliche Schutzmaßnahmen gegen diese genannt. Da folgende Maßnahmen nicht alle Möglichkeiten abdecken, werden zudem noch die Grenzen und Nachteile angeführt.

Um seine Identität in einer Umgebung wie einem Sozialen Netzwerk zu schützen, gibt es die Möglichkeit der **Pseudonymisierung** bzw. **Anonymisierung**. Wie schon vorher erwähnt, bestimmt nicht nur das verwendete Netzwerk darüber, wie viele Informationen preisgegeben werden, sondern auch der Nutzer selbst (vgl. 2.3.1). Die Anonymisierung beschreibt den Vorgang, nach dem das Zuordnen von Profil und realer Person nicht mehr möglich ist. Dies geschieht durch Verändern oder vollständiges Weglassen der nötigen Informationen. Bei der Pseudonymisierung wird der Name durch ein Pseudonym, also einen ausgedachten Namen, ersetzt. Dies gilt als abgeschwächte Form der Anonymisierung, da der Bezug zwischen realer Person und Profil nur schwieriger herzustellen ist (Pfitzmann und Hansen 2008, S. 20-24). In der Realität findet dieser Ansatz nur bedingt Anwendung. Die Fülle an Informationen, die über betroffene Personen gesammelt werden, ist so umfangreich, dass auch bei einem „anonymen“ Auftreten ein Bezug zur realen Person hergestellt werden kann. Letzteres nur unter weitaus größerem Aufwand als bei nicht anonymisierten Profilen. Außerdem sind führende Unternehmen, beispielsweise *Facebook*, dazu übergegangen, die Pseudonymisierung gänzlich zu untersagen und zuwiderhandelnden Personen den Dienst zu verweigern. Legitimiert wird dies durch eine dadurch sicherere Gemeinschaft, die „stärker zur Rechenschaft gezogen werden“ kann (Facebook 2019, Abs. 3). Somit ist zumindest in der Theorie die Pseudonymisierung nicht immer möglich. Andere Dienste, wie z.B. *Reddit,* fördern diese sogar. Der große Erfolg dieser Anbieter beruht sicherlich zu einem beträchtlichen Teil auf der Anonymität der Nutzer.

Ein weiterer Aspekt ist das User-Tracking. Das „Verfolgtwerden“ im Internet ist nahezu unmöglich zu umgehen. Dennoch gibt es einige Maßnahmen, welche diesem entgegenwirken.

Die üblichen Internetbrowser bieten zu ihrer eigenen Software fast immer optionale Erweiterungen an. Diese Add-Ons sind zumeist kostenfrei und von externen Anbietern. AdBlock[16] und HideMyAss[17] sind nur zwei der zahlreichen Angebote. Dadurch lassen sich Werbeflächen ausblenden, Proxy-Server verwenden oder Cookies umgehen. Durch die individuellen Einstellungsmöglichkeiten der Browser lassen sich also viele Teile des User-Trackings umgehen. Auf der anderen Seite jedoch, bringen diese Erweiterungen auch einige Nachteile mit sich, die in direktem Gegensatz zu ihrem Nutzen stehen. Durch die Applikation AdBlock beispielsweise, können Werbeflächen auf Webseiten ausgeblendet bzw. blockiert werden. Dadurch kann personalisierte Werbung gänzlich verhindert werden. Einige Webseitenanbieter wollen jedoch nicht auf die Werbeeinnahmen verzichten und nutzen selbst Software, welche z.B. AdBlock erkennt. Sollte ein Besucher der Seite eine solche Software verwenden, so wird bis zum Zeitpunkt der Deaktivierung der Zugang zur Seite versperrt. Außerdem wäre es denkbar, dass Unternehmen hinter AdBlockern Geld von Webseitenanbietern nehmen, um deren Werbung als akzeptable Werbung zu deklarieren. Diese wird dann wiederum dem Nutzer der kostenfreien Version von AdBlock angezeigt. Ein weiterer nennenswerter Aspekt ist die Individualisierung des Browsers selbst. Bei jedem Webseitenbesuch werden dem Webserver Daten über den Nutzer übermittelt. Unter anderem auch, welcher Browser verwendet wird und in welcher Version sich dieser befindet. Ebenfalls werden genutzte Add-Ons und andere Daten registriert. Damit lässt sich dann durch das Browserprofil des Nutzers wieder eine individuelle Person und damit ein potenzielles Profiling erstellen.

Ein bisher ungenannter Punkt zum Datenschutz ist die Passwortsicherheit. Ein sicheres Passwort gewährleistet, dass private Informationen geschützt bleiben und ein Identitätsdiebstahl verhindert werden kann. Das *Bundesamt für Sicherheit in der Informationstechnik* empfiehlt einige Punkte, die zur Sicherheit des Passworts beitragen (Bundesamt für Sicherheit in der Informationstechnik). Das Passwort sollte …

- sich leicht merken lassen. Es werden Hilfssätze und Leetspeak[18] empfohlen.

[16] www.adblockplus.org (zuletzt geprüft: 03.04.2019)
[17] Kurz: HMA, www.hidemyass.com (zuletzt geprüft: 03.04.2019)
[18] Das Ersetzen von Buchstaben durch Zahlen, besser bekannt unter „1337“ *(„Leet“ in Leetspeak)*

- so lang wie möglich sein (mind. 8 Zeichen, mind. 20 für WPA-Verschlüsselung)
- sich aus Klein- und Großbuchstaben, Sonderzeichen, Leerzeichen und Ziffern zusammensetzen. Es sollte eine Mischung aus allen erlaubten Möglichkeiten sein.
- nicht in einem Wörterbuch vorkommen oder Familiennamen, Geschwisternamen oder Adressen enthalten. Genauso unsicher sind Geburtstage oder Hochzeitsdaten.
- nicht am Ende oder Anfang mit einem Sonderzeichen oder Ziffernfolge ergänzt werden, da diese häufig genutzt und auch geknackt werden.
- regelmäßig geändert werden.

Außerdem wird empfohlen, für den Umgang mit den Passwörtern einen Passwortmanager zu betreiben. Dieser enthält unter anderem die Funktionen: Testen des Passworts auf Sicherheit, Hinweis auf Änderung in regelmäßigen Abständen und Hinweise, wo welches Passwort verwendet wurde.

Abschließend ist zu sagen, dass alle genannten Punkte darauf aufbauen, dass die betroffene Person um die Ausmaße des Datenflusses der eigenen Daten Bescheid weiß und die erforderlichen Maßnahmen kennt. Außerdem wird ein gewisses Maß an Selbstreflexion zum Thema Datenschutz vorausgesetzt. Diese Eigenschaften werden im Datenschutzmodell nach Hug und Grimm aufgegriffen (vgl. 2.4).

2.4 Datenschutzkompetenzmodell nach Hug und Grimm

Wichtiger Inhalt der Unterrichtsreihe ist, dass Schüler im Laufe der Reihe Kompetenz im Bereich des Datenschutzes erlangen und ausschärfen. Hug und Grimm machen in ihrer Arbeit deutlich, dass die beiden Begriffe *Medienkompetenz* und *Datenschutzkompetenz* zu trennen sind. Grundlage für die Kompetenzbestimmung ist das *Medienkompetenzmodell* nach Six und Gimmler (Six et al. 2007). Erweitert wird dies durch Hug und Grimm mit dem Aspekt der Risikobewertung aus dem *Referenzmodell* nach Grimm et al., welches das Vorgehen bei der IT-Sicherheitsanalyse beschreibt (Grimm et al. 2016, S. 2-20). Dies bildet letztendlich das **Datenschutzkompetenzmodell** (Hug und Grimm 2017, S. 15-18).

Zusätzlich zur Medienkompetenz ist die Datenschutzkompetenz zu sehen. Diese bildet den Grundsatz im Umgang mit Sozialen Netzwerken und ähnlichen Diensten. Die

Datenschutzkompetenz spielt ebenso bei Versicherungsverträgen, Kaufverträgen, Patientenakten etc. eine Rolle, jedoch wird nur der Bezug zu Sozialen Netzwerken für diese Arbeit benötigt. Nach Six et. al. ist Medienkompetenz „die Fähigkeit für einen kritischen, selbstbestimmten, kreativen und verantwortlichen Medienumgang […] Kompetenter Medienumgang zeichnet sich dadurch aus, dass er selbstbestimmt, reflektiert und selbstreguliert sowie an eigenen Anliegen orientiert, zielgerichtet und funktional gleichzeitig aber auch persönlich sowie sozial verträglich und angemessen ist“ (Six et al. 2007, S. 281). Die Medienkompetenz wird dafür in acht Dimensionen beschrieben. Hug und Grimm verwenden für ihr Modell die Dimensionen, welche eine Datenschutzrelevanz aufweisen.

Zum einen benötigt man für eine Datenschutzkompetenz einen ausreichenden Fundus an Hintergrundwissen. Darunter fallen die Gründe, warum Datenschutz im medialen Umgang Relevanz aufweist. Außerdem wird ein Wissen um die Vorgänge bei der Datenverarbeitung von personenbezogenen Daten genannt. Dazu kommen noch die Rechte und Pflichten der betroffenen Person (bzgl. der DSGVO) sowie das Wissen um einhergehende Gefahren und geeignete Schutzmaßnahmen diesbezüglich. Erweitert wird das Hintergrundwissen durch das Orientierungswissen in spezifischen Situationen. Dies beschreibt die Fähigkeit, in genannten Situationen die passenden Maßnahmen zu kennen und anzuwenden. Beispiele hierfür sind benutzerspezifische Einstellungsmaßnahmen zum Schutz der eigenen personenbezogenen Daten, wie sie z.B. von *Facebook* und anderen Onlinediensten angeboten werden sowie das Wissen um die Existenz und Anwendbarkeit von Sicherheits- bzw. Anonymisierungstools beim Nutzen der Dienste (siehe 2.3.3). Letztendlich verschmelzen diese beiden unter dem Begriff „Wissen“. Letzteres geht fließend in die Dimension der Nutzungs- und Auswahlkompetenz über. Die Nutzungskompetenz beschreibt die Fähigkeit diverse Funktionen, die durch die Auswahlkompetenz bestimmt wurden, praktisch durchzuführen. Das Zusammenführen von Wissensdimension, Nutzungs- und Auswahlkompetenz ergibt einen reflektierten Umgang mit den eigenen personenbezogenen Daten. Im Medienkompetenzmodell wird zusätzlich die Validierung von angebotenen Tools und Funktionen als Urteilskompetenz benannt.

Diese ausgewählten Aspekte werden durch Hug und Grimm um den Aspekt der *Risikobewertung* ergänzt. Die Nutzung von Onlinediensten, speziell von Sozialen Netzwerken, beruht auf einer Wechselwirkung zwischen dem Selbstdatenschutz der Betroffenen und dem

aufgebrachten Vertrauen gegenüber den Verantwortlichen bzgl. der zu verarbeitenden Daten. Grundlage für diese Wechselwirkung ist das Vertrauensmodell nach Mayer et al. (Mayer et al. 1995, S. 709-734). Abbildung 2 zeigt eine grafische Darstellung des genannten Modells.

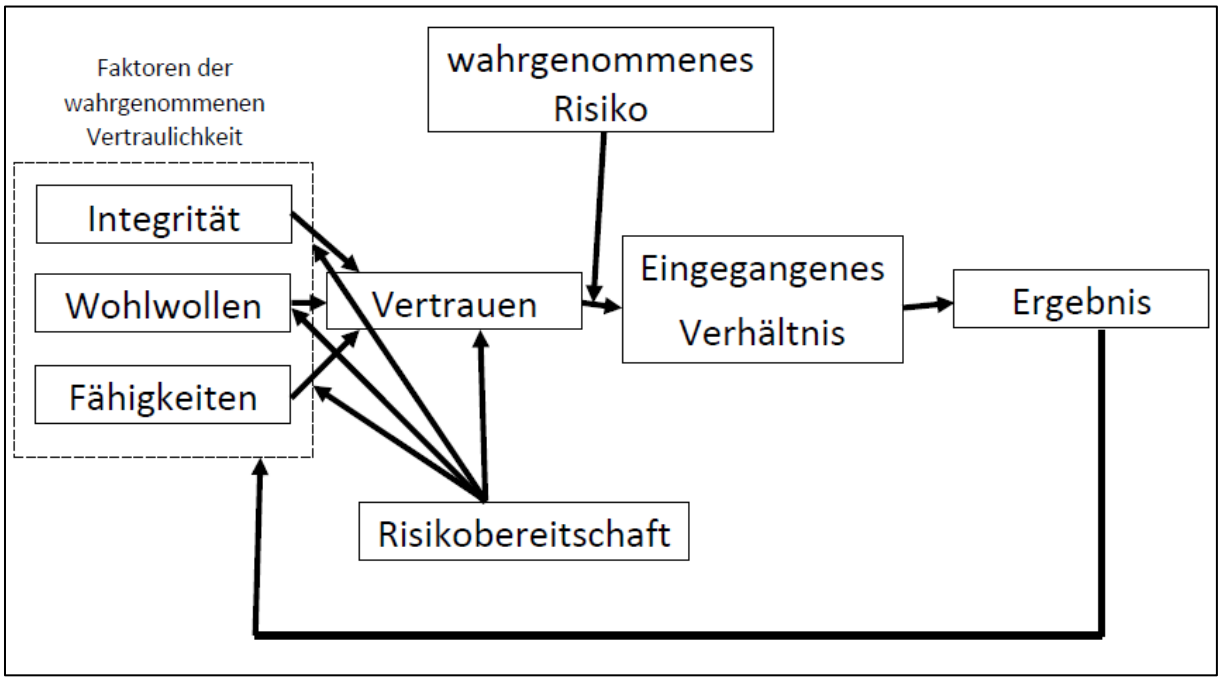


***Abbildung 2**: Vertrauensmodell (nach Mayer et al., S. 715)*

Demnach wird dem eingegangenen Verhältnis (Risk Taking in Relationship[19]) zwischen Verantwortlichem und Betroffenem das entgegengebrachte Vertrauen (Trust) und das wahrgenommene Risiko (Perceived Risk) vorangestellt. Das Vertrauen des Betroffenen setzt sich zusammen aus dessen Risikobereitschaft (Trustor's Propensity) und den Faktoren der wahrgenommenen Vertraulichkeit dem Verantwortlichen gegenüber (Factors of Perceived Trustworthiness), welche unterteilt werden in Integrität (Integrity), Wohlwollen (Benevolence) und den zu erwartenden Fähigkeiten (Ability) des Verantwortlichen. Das Ergebnis aus dem Verhältnis (Outcomes), also z.B. die Rahmenbedingungen und der Ablauf eines Geschäfts, beeinflusst wiederum die drei genannten Faktoren beim nächsten oder einem vergleichbaren Verhältnis.

[19] Die englischen Begriffe stammen aus dem verwendeten Modell nach Mayer et al.

Um nun aus diesem Vertrauensmodell eine Risikobewertungskompetenz abzuleiten, nutzen Hug und Grimm das Referenzmodell der IT-Sicherheitsanalyse, welches eigentlich für die Analyse von IT-Systemen ausgelegt ist. Jedoch lässt es sich auch auf die Einschätzung des Nutzungsrisikos anwenden, indem nur die datenschutzrelevanten Aspekte betrachtet werden. Das Referenzmodell als solches besteht aus einer Ist-Analyse, einer Potenzial-Analyse und der Installation eines daraus resultierenden Sicherheitskonzeptes. Der Ablauf des Modells wird am Beispiel „Veröffentlichen einer Story[20] auf *Instagram*“ erläutert. In der Ist-Analyse werden zunächst alle Güter bestimmt. Dabei handelt es sich um alle Objekte, die personenbezogene Daten beinhalten. Darunter fallen in diesem Fall das hochgeladene Foto und all dessen Informationen (zu erkennende Personen, Ort und soziale Interaktionen), beigefügte Texte und angemerkte Tags[21]. Weiterhin umfasst die Ist-Analyse das angebrachte Vertrauen in die involvierten IT-Systeme. Eingebundene Systeme sind u.a. das mobile Endgerät des Nutzers, von dem der Upload stattfindet, verwendete Übertragungssysteme des Internetanbieters sowie die Server des Dienstanbieters (*Instagram*). Beteiligte Personen auf beiden Seiten werden mit einbezogen. Zusätzlich benennt die Ist-Analyse mögliche Angreifer, die innerhalb des Übertragungsweges die Integrität, Authentizität und Vertraulichkeit (vgl. Eckert 2013, S. 390 ff.) des Uploads gefährden. Diese Personen werden im Modell als externe Dritte bezeichnet. In der Potenzial-Analyse werden nun mögliche, vom Publikmachenden unbeabsichtigte Folgen beschrieben. In diesem Fall wäre das beispielsweise eine Speicherung der Story durch Dritte. Damit wäre die Veröffentlichung des Fotos bzw. Textbeitrages nicht mehr als temporär zu bezeichnen, da dieses bzw. dieser auf anderem Weg weiter genutzt werden könnte. Ebenfalls wäre ein Bezug auf den Inhalt ohne den konkreten Kontext denkbar. So könnte eine andere Person den Textbeitrag z.B. zitieren und in einen anderen, womöglich falschen Zusammenhang stellen. Aus den beiden Analyseteilen wird im Modell nun ein Sicherheitskonzept abgeleitet. In diesem Fall wäre das z.B. das Anonymisieren des Beitrages, um es externen Personen zu erschweren, die Inhalte in einen falschen Zusammenhang zustellen. Ein weiterer Punkt wäre das reflektierte Betrachten des Inhalts vor der Veröffentlichung. Allgemeingesehen wäre das Vermeiden von Beiträgen, welche die eigene

[20] Temporär verfügbare Bilder, die ein Nutzer mit Textbeiträgen in *Instagram* veröffentlichen kann. Diese werden zum Folgetag automatisch wieder für alle Beteiligten unzugänglich.

[21] Stichwörter, die vom Publikmachenden hinzugefügt werden, um die Story mit Hilfe einer Suchfunktion zu finden.

Intimsphäre betreffen, ein wichtiger Punkt im konstruierten Beispiel. Im Sinne der Datenschutzkompetenz stellt die Umsetzung des Sicherheitskonzepts den Aspekt *Anwendung* dar.

Zu den genannten Aspekten und Kompetenzen lassen sich noch die *Sensibilität* und die *Selbstreflexion* des Anwenders einordnen. Im Bereich der IT-Sicherheit wird der Zusammenschluss dieser beiden Fähigkeiten als (*Security) Awareness* bezeichnet (Helisch et al. 2009, S. 9).

Dadurch wird die Datenschutzkompetenz von Hug und Grimm als der „Zusammenschluss von Hintergrundwissen, Orientierungswissen, Urteilskompetenz, Handlungs- und Nutzungskompetenz, Risikobewertungskompetenz und die Anwendung von Handlungsmustern mit Bezug auf das schützenswerte Gut der persönlichen Daten“ (Hug und Grimm 2017, S. 18) bezeichnet. Datenschutzkompetenz besitzt derjenige, der in den genannten Aspekten ein „ausreichendes Maß“ an Kompetenz erlangt hat.

2.5 Datenschutz im Schulunterricht

Bevor in Kapitel 4 die Unterrichtsreihe zum Thema Datenschutz im Kontext Sozialer Netzwerke mit Hilfe von *Instahub* beschrieben wird, soll zunächst der Umfang und die abzudeckenden Teilbereiche bestimmt werden. Da diese Arbeit als Erweiterung der Lehrplattform *Instahub* zu verstehen ist, wird versucht, sämtlichen Inhalt über diese Plattform aufzubauen. Dadurch, dass in Rheinland-Pfalz das Pflichtfach Informatik für die Sekundarstufe I nicht eingerichtet ist (Stand: März 2019), wird der inhaltliche Bereich abgeleitet aus dem Lehrplan Informatik Wahlfach und Wahlpflichtfach an Gymnasien und Integrierten Gesamtschulen (Sekundarstufe I) (Ministerium für Bildung, Wissenschaft, Jugend und Kultur Rheinland-Pfalz 2010) sowie den Richtlinien für Verbraucherbildung an allgemeinbildenden Schulen in Rheinland-Pfalz (Krieger und Schmatzinski-Damp 2010, S.30). Diese Richtlinien stellen ein Curriculum für die Sekundarstufe I – II zur Verfügung, um Schüler mit ihrem Inhalt auf die Alltagsbewältigung vorzubereiten. Ihr Inhalt ist in drei Kernbereiche aufgeteilt, wobei der *Kernbereich III: Datenschutz* und darunter genannte Kompetenzen für diese Arbeit relevant sind. Eine weitere Grundlage zur Thematisierung bildet die DSGVO (vgl. 2.3) und die Bildungsstandards der GI für den Informatikunterricht der Sekundarstufe I (Gesellschaft für Informatik e.V. (GI) 2008a).

2.5.1 Datenschutz als Recht

Der Lehrplan Informatik (Wahlpflichtfach/Wahlfach Sek. I) ordnet das Thema Datenschutz direkt in die Thematik der *Nutzung und Modellierung von Datenbanken* (Ministerium für Bildung, Wissenschaft, Jugend und Kultur Rheinland-Pfalz 2010, S. 23 ff.) ein. Der Datenschutz wird unter dem Aspekt der Datenerhebung und Sicherheit von IT-Systemen betrachtet. Datenbanken sollen mit Hilfe von Datenschutzaspekten bewertet werden. Weiterhin ist hierzu die Definition von informationeller Selbstbestimmung und den Rechten von Betroffenen aus der DSGVO zu betrachten.

Die Richtlinie für Verbraucherbildung[22] setzt diesem jedoch noch einen Punkt voraus. So heißt es im Curriculum „Schülerinnen und Schüler sind bereit und in der Lage, Datenschutz als Bürger- und Menschenrecht anzuerkennen“ (Krieger und Schmatzinski-Damp 2010, S. 30). Daraus ableiten lässt sich für den Informatikunterricht, dass zuerst ein Bewusstsein für Datenschutz geschaffen werden muss, dem eine für Schüler ausreichende Legitimation vorausgeht. Deshalb soll sich der Beginn der zu entwickelnden Unterrichtsreihe vor allem hiermit beschäftigen (vgl. 3.1).

2.5.2 Gefahren und Schutzmaßnahmen

Die Richtlinie für Verbraucherbildung fasst diesen Inhaltsbereich unter *Selbstdatenschutz* sowie *Selbstdarstellung im Netz* zusammen. Vor allem sollen dem Schüler hier aber Werkzeuge an die Hand gegeben werden, die sie im Kontext eines realen Sozialen Netzwerks nutzen können, und die Fähigkeit ihr Handeln kritisch zu hinterfragen gefördert werden. Darüber hinaus soll das Verständnis für die Notwendigkeit dieser Werkzeuge weiter ausgeschärft werden. Zu finden sind diese Kompetenzen im Modell nach Hug und Grimm in der Urteils-, Auswahl-, Nutzungs- und Handlungskompetenz. Darüber hinaus werden Maßnahmen zur Sicherung der eigenen Daten behandelt. Darunter zu verstehen ist das Entwickeln eines sicheren Passwortes, das Anonymisieren und das Zurückhalten von eigenen

[22] Curriculum um Kinder und Jugendliche über den Bildungsweg auf alltägliche Probleme vorzubereiten.

Daten, welche die Privatsphäre betreffen. Hierzu werden Ansätze aus dem online verfügbaren Schulbuch *inf-schule*[23] genutzt sowie Ideen aus Teilmodulen von *moodle@rlp*[24].

2.5.3 Sensibilität und Selbstreflexion

Anknüpfend an das Datenschutzkompetenzmodell nach Hug und Grimm (Hug und Grimm 2017) wird das Hauptaugenmerk der Unterrichtsreihe darauf liegen, einen selbstreflektierten Umgang mit personenbezogenen Daten zu fördern. Diskussionen und Bewertungen innerhalb der Reihe sollen an diesem Punkt ansetzen. Durch rege Diskussion untereinander, aber auch durch das Bewerten der eigenen Internetauftritte wird auf eine Sensibilisierung hinsichtlich des Datenschutzes hingearbeitet. Unter anderem kann hierbei das Erstellen eines Kriterienkatalogs (z.B. „Kriterien für ein sicheres Profil“) genutzt werden. Es wird versucht, dass Ideen, Kriterien und Methoden hauptsächlich schülerseitig erarbeiten werden.

2.5.4 Exkurs zur didaktischen und methodischen Unterrichtsplanung

Der nachfolgende Abschnitt erläutert kurz die Teilbereiche der Unterrichtsplanung, um dem Leser die folgenden Kapitel ersichtlicher zu machen.

Unterrichtsplanung wird in zwei nicht voneinander unabhängige Teilbereiche aufgebrochen: Die *Didaktik* und die *Methodik*. Schubert und Schwill bezeichnen die Didaktik als die Wissenschaft (und Lehre) über das Lehr-Lern-Verhältnis. Sie entscheidet über die Auswahl, Zusammensetzung und Struktur von Lehr- bzw. Bildungsinhalten sowie die Steuerung von Lernprozessen (Schubert und Schwill 2011, S. 12 f.). Sie ist allgemein gesehen die notwendige, theoretische Grundlage und Vorbereitungsweise eines differenzierten, didaktisch reduzierten[25] Unterrichts. Humbert fasst es zusammen als den „Versuch – über subjektive Theoriebildung hinaus – auf verschiedenen Ebenen mit unterschiedlicher Praxisnähe die Komplexität gestaltend zu reduzieren und damit unterrichtliches Handeln rational planbar und

[23] www.inf-schule.de, frei verfügbares Informatikschulbuch
[24] https://lms.bildung-rp.de/austausch, Austauschplattform über Unterrichtskonzeptionen und -materialien für den Informatikunterricht. Betreiber ist das Pädagogische Landesinstitut Rheinland-Pfalz.
[25] Inhalte in ihrer Komplexität so reduziert, dass sie für die Schule relevant und nutzbar sind.

kontrollierbar zu machen“ (Humbert 2006, S. 4). Der didaktische Teil beschäftigt sich demnach mit dem sachlichen Bereich der Unterrichtsplanung.

Die Methodik geht der Frage nach der Art und Weise der Wissensvermittlung auf den Grund, sprich, wie gelernt wird. Sie umfasst alle verwendeten Unterrichts- bzw. Sozialformen und ermöglicht so „die Inszenierung des Unterrichts durch die zielgerichtete Organisation der Arbeit, durch soziale Interaktion und sinnstiftende Verständigung mit den Schülern“ (Humbert 2006, S. 4). Weiterhin beschreibt Humbert die „Handlungskompetenzen der Lehrer im Feld der Unterrichtsmethoden … in Unterrichtssituationen Lernprozesse für die Schüler auf dem Hintergrund der Rahmenbedingungen zu organisieren.“ Auch die Methodik kann Mittel zur Differenzierung des Lehr-Lern-Raumes sein. Beispiele für Unterrichtsmethoden sind z. B. Lernaufgaben, Leitprogramme, Gruppenarbeiten, Fallstudien, Projektarbeit oder entdeckendes Lernen.

Die *Differenzierung* ist Teil einer guten Unterrichtsplanung (vgl. Meyer 2003, S. 39). Dabei handelt es sich um „die Auflösung des heterogenen Klassenverbands zugunsten homogener Gruppen in Bezug auf die Leistungsfähigkeit oder die Interessenrichtung der Schüler“ (Hubwieser 2007, S. 22). Differenzierung lässt sich in verschiedene Organisationsformen aufteilen. Bezogen auf den Informatikunterricht wird nur die Binnendifferenzierung betrachtet. Schüler sollen durch innere Differenzierung ihren eigenen Schwerpunkt bezüglich des Unterrichtsgegenstandes erkennen und weiterentwickeln. Für diese Unterrichtsreihe interessant ist die Differenzierung nach Arbeitstempo und Auffassungsgabe sowie Interesse und Motivation des Schülers. Im Sinne des Kontextes und dem Umfang der Reihe ist es sinnvoll, dass nur zielgleich differenziert wird[26]. Die Unterrichtsreihe in Kapitel 4 gibt deshalb Hinweise und Umsetzungsmöglichkeiten zur inneren Differenzierung.

Ein weiterer Punkt für eine erfolgreiche Unterrichtsplanung wäre die Charakterisierung der Lerngruppe. Dies ist für die Planung dieser Reihe nicht notwendig, da sie allgemein verfasst wird. Die Nennung dient lediglich der Vollständigkeit des Unterrichtsplanungsprozesses.

[26] Das gleiche Lernziel, aber mit anderen Methoden oder Materialien (Ministerium für Bildung, Wissenschaft, Weiterbildung und Kultur Rheinland-Pfalz 2015, S11)

3. Das Projekt: Instahub

Instahub ist ein von Julian Dorn[27] ins Leben gerufenes Projekt. Es handelt sich um ein für schulische Zwecke einsetzbares Soziales Netzwerk zur Erarbeitung des Unterrichtsthemas Datenbanken. Das folgende Kapitel befasst sich mit der Entstehung, dem inhaltlichen Aufbau und Konzeption sowie den wissenschaftlichen Grundlagen für die Thematik. Anschließend wird die Bedeutung für diese Arbeit herausgestellt.

3.1 Entwicklung und inhaltliche sowie didaktische Konzeption von Instahub

Das Ursprungsprojekt *friendzone*[28] wurde 2016 von Dorn veröffentlicht. *Friendzone* stellt ein fiktives Start-Up-Unternehmen dar, bestehend aus einer Chefin, einem Programmierer und einem Datenbankadministrator. Letztere Rolle übernimmt der Schüler im Unterricht. Der Zugang zum Quelltext, den Datenbanken und den Lehrmaterialien ist kostenfrei verfügbar (siehe Dorn 2016). Die Unterrichtsreihe ist darauf ausgelegt, dass Schüler mit Hilfe von *phpMyAdmin*[29] in einem Planspiel das Thema Datenbanksysteme erarbeiten. So soll ein Einblick in ein reales Arbeitsumfeld der IT-Branche gegeben werden.

Aus diesem Projekt heraus entstand *Instahub*[30]*. Instahub* verzichtet auf das Planspiel aus *friendzone* und behandelt ausschließlich die Rolle des Datenbankadministrators. Während *friendzone* sich eher an der Oberfläche von *Facebook* orientierte, orientiert sich *Instahub* in Design und Funktionsumfang an *Instagram*. Abb. 3 zeigt beispielhaft ein Profil aus einem Hub[31].

[27] Lehrkraft im Bundesland Sachsen. Im Jahre 2017 verlieh die Gesellschaft für Informatik e.V. Herrn Dorn im Rahmen der INFORMATIK 2017 den *Unterrichtspreis 2017* für das Projekt (Gesellschaft für Informatik e.V. (GI) 28.09.2017).
[28] https://blog.wi-wissen.de/post/friendzone (zuletzt geprüft: 03.04.2019)
[29] https://www.phpmyadmin.net/ (zuletzt geprüft: 03.04.2019)
[30] Das Projekt belegte am 22.03.2019 den ersten Platz des Preises „innovative MINT-Unterrichtsideen“ des MNU e.V.
[31] Dies ist ein eigenständiges, voll funktionierendes Netzwerk eines Schülers.

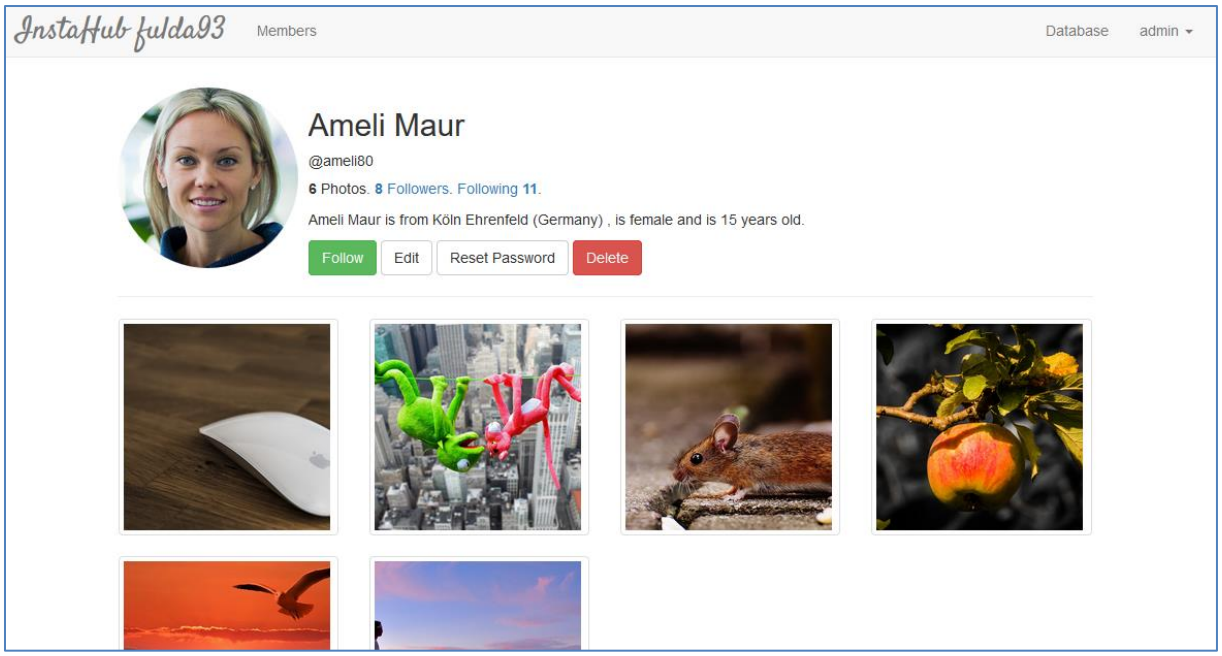


***Abbildung 3**: Beispielhaftes Profil auf Instahub*[32]

Ein weiterer Unterschied zu *friendzone* ist, dass *Instahub* ein voll funktionierendes Soziales Netzwerk für jeden Schüler bietet. Auch eine Interaktion zwischen den Schülern ist im Gegensatz zu seinem Vorgängerprojekt möglich. Um den Schwerpunkt der Unterrichtseinheiten auf SQL-Befehle und Datenbankmodellierung zu legen, wurde auf die Verwendung von phpMyAdmin verzichtet. Stattdessen verwendet *Instahub* nur eine einfache Eingabezeile, die alle nötigen SQL-Befehle (und mehr) verarbeiten kann (siehe Abb. 4). Für das Nutzen von *Instahub* ist lediglich ein Lehrer-Account nötig. Dieser muss von Dorn händisch bestätigt werden. Anschließend können Schüler unter Benennung der *Teacher-ID* ihren eigenen Hub erstellen und nach einer Bestätigung durch die Lehrperson vollständig darauf zugreifen. *Instahub* lässt sich ebenfalls in das Intranet eines Schulnetzwerkes einpflegen, sodass ein Betrieb ohne Internetzugang möglich ist. Der Quelltext und die bereitgestellten Materialien sind, wie in *friendzone*, frei zugänglich und können von jedem erweitert oder verbessert werden.

[32] Quelle: https://blog.wi-wissen.de/post/instahub

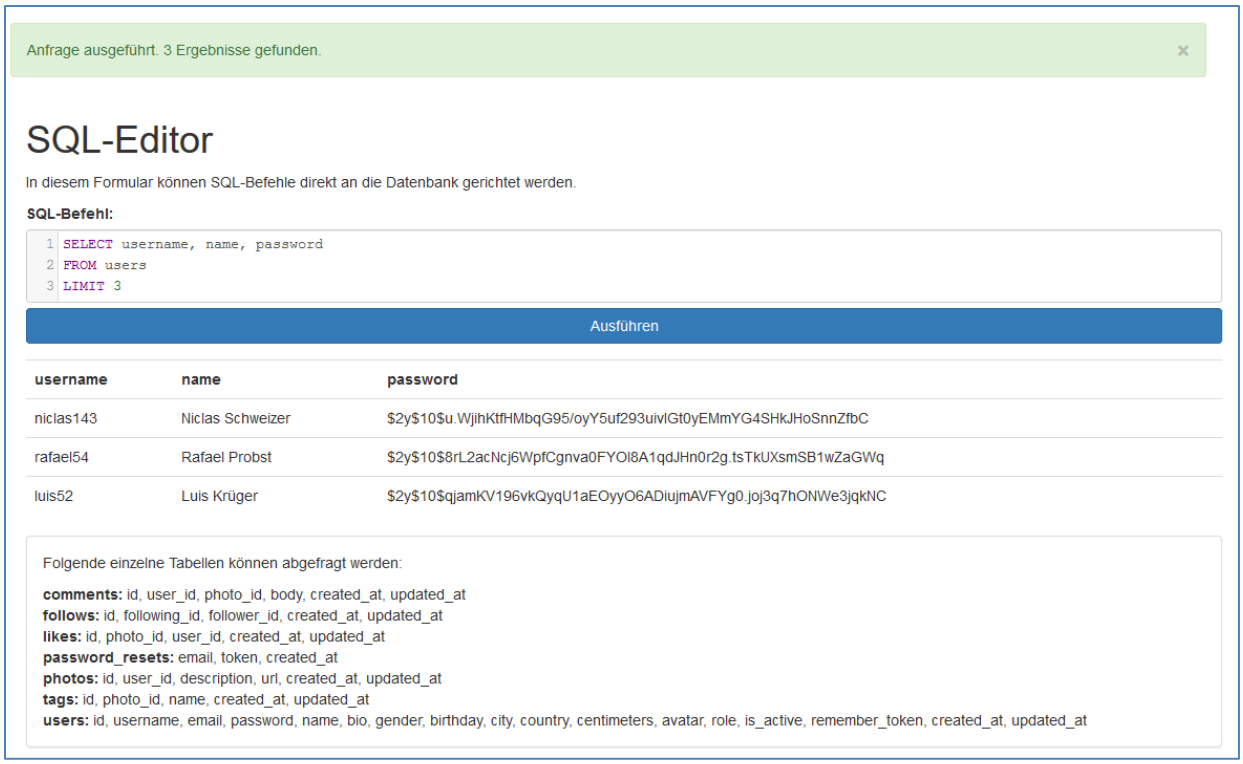


***Abbildung 4**: SQL-Editor von Instahub*[33]

Die fachlichen Inhalte umfassen fünf Bereiche:

- Relationale Datenbanken
- Datenmodellierung
- Client-Server-Architektur
- Einblick und Motivation Datensicherheit
- Einblick und Motivation Datenschutz

Relationale Datenbanken lassen sich dazu noch in die Bereiche *Datenbankmanagementsysteme, SQL als Abfragesprache* und *Relationen* aufteilen. Die Datenmodellierung besteht aus Dokumentation mit Hilfe von *ERM*[34] und *Normalisierung*. Die notwendigen fachlichen Hintergründe für die Sekundarstufe I werden in Abschnitt 3.3 weiter ausgeführt.

[33] Quelle: https://blog.wi-wissen.de/post/instahub
[34] Entity-Relationship-Modell

Die didaktische Konzeption baut in der Reihenfolge auf den inhaltlichen Bereichen auf. Als mögliche didaktische Ansätze definiert Dorn (Dorn 2019):

(1) Auswerten und Modellieren von Datenbanken

(2) Datenschutz und -sicherheit

(3) Perspektivenwechsel: Rolle des Administrators und Werbekunden eines sozialen Netzwerks

(1) Unter *Auswerten und Modellieren von Datenbanken* versteht sich das Hauptkonzept von *Instahub*. Es orientiert sich am Lehrplan für Informatik der Sekundarstufe II (Grundkurs) in Sachsen (Staatsministerium für Kultus des Freistaates Sachsen 2004, S. 15-20) und deckt den vollständigen Inhaltsbereich *Datenbanken* ab. Die nachfolgende Tabelle gibt eine kurze Übersicht über die Unterrichtseinheiten und ihren Inhalt. Dieser Ansatz wurde bereits mit über 150 Schülern erfolgreich durchgeführt und evaluiert.

Nr.	Titel	Thema	Dauer
1	Client-Server-Architektur	Wdh. Netzwerke	1 UE
2	Erster Arbeitstag	Motivation und Account einrichten	
3	Datenbanken allgemein	Grundlagen	1-4 UE
4	Auswerten von Daten I	SQL innerhalb einer Tabelle	4 UE
5	Verändern von Daten	CRUD-Befehle innerhalb einer Tabelle	2 UE
6	Datenschutz und -sicherheit	Gesellschaftliche Aspekte von DBs	2 UE
7	Photos und Tags im InstaHub	1:n-Kardinalitäten	2 UE
8	Followers, Likes und Kommentare im Instahub	n:m-Kardinalitäten	1 UE
9	Modellieren von Daten	Modelle mit klaren Anforderungen	2-4 UE
10	Auswerten von Daten II	tabellenübergreifende SQL-Befehle	2 UE
11	Die Macht verknüpfter Daten	tabellenübergreifende CRUD-Befehle	2 UE
12	Komplexaufgaben	Modelle mit offenen Anforderungen	2-4 UE
Insgesamt: 21-28 UE			

***Tabelle 2**: Übersicht zur Unterrichtsreihe "Auswerten und Modellieren von Datenbanken"*[35]

(2) *Datenschutz und -sicherheit* beschreibt den datenschutzrelevanten Ansatz. Er zielt darauf ab, dass Schüler durch das Nutzen ihres Hubs und durch eigenes Interesse erkennen, dass der Umgang mit Datenbanken schnell unter dem Datenschutzaspekt betrachtet werden muss. Derzeit besteht jedoch nur die theoretische Idee für diesen didaktischen Ansatz sowie zwei Unterrichtseinheiten im ersten Ansatz (siehe Tabelle 2). Hier wird die vorliegende Arbeit ansetzen und diesen Aspekt weiterentwickeln.

(3) Der dritte Ansatz nutzt die neue Funktionalität der benutzerorientierten Werbung auf *Instahub*. Seit November 2018 kann innerhalb des Hubs (fiktive) personalisierte Werbung

[35] Quelle: https://wi-wissen.github.io/instahub-doc-de/#/didactic-modellierung-sql (zuletzt geprüft: 03.04.2019)

angezeigt werden. Mithilfe dessen können Schüler den Prozess hinter Werbung und User-Tracking begreifen und erarbeiten. In der Reihe wird dieser Ansatz *Perspektivenwechsel* genannt.

3.2 Erweiterbarkeit und Bedeutung für diese Arbeit

Dorn macht in seinem Projekt mehrfach deutlich, dass *Instahub* noch zu mehr fähig ist, als es bereits umgesetzt wurde. Die beiden didaktischen Ansätze *Perspektivenwechsel* und *Datenschutz und -sicherheit* geben einen Ausblick dahingehend. Die Tatsache, dass *Instahub* auf freien Lizenzen basiert und der Quelltext für jeden zugänglich ist, ermöglicht dies das Erweitern der Plattform in jeglicher Hinsicht.

Bezüglich der Intention dieser Arbeit, eine Datenschutz-Unterrichtsreihe für die Orientierungsstufe im Kontext Sozialer Netzwerke zu entwerfen, bietet sich *Instahub* als Ansatzpunkt an. Nichtsdestotrotz ist es nötig für die ausgewählte Lerngruppe (Klassenstufe 5-6) einen völlig neuen Ansatz zu finden, da sich der aktuelle, datenschutzrelevante Teil der Materialien auf eine Lerngruppe in der Sekundarstufe II bezieht. Zum einen müssen die Lerninhalte dem Niveau der jüngeren Schüler angepasst und didaktisch reduziert werden. Zum anderen soll die neue Unterrichtsreihe den Schwerpunkt im Bereich *Schutz personenbezogener Daten* und *Internetsicherheit* aufweisen. Damit die geplante Reihe sich inhaltlich nicht zu weit von der Ursprungsidee von *Instahub* entfernt, wird das *Nutzen und Modellieren* von Datenbanken als Exkurs in den Materialien eingereiht. Anschließend wird die vollständige Unterrichtsreihe in das System von *Instahub* integriert.

3.3 Grundlage: Datenbanken in der Sekundarstufe I

Für den Exkurs Datenbanken in der Unterrichtsreihe dieser Arbeit ist es nötig, die entsprechenden Fachinhalte für die Sekundarstufe I auszuarbeiten.

Datenbanken und dem Nutzen von Datenbanken wird in der heutigen Zeit eine wichtige Rolle zugesprochen. Sie sind Basis der meisten Informationssysteme, wobei im Arbeitsumfeld besonders die Bereiche *Modellieren* und *Abstrahieren* von Datenbanken herausstechen. Das Abstrahieren soll aufgrund des jungen Alters der Zielgruppe nur eine nebensächliche Rolle spielen. Weiterhin, so beschreiben Burkert et al., sind Datenbanken „ein guter Repräsentant

vieler Problemstellungen in der Informatik. Datenstrukturen, Wertebereiche, Modellbildung, Parametrisierung, Datenkapselung, Datenorganisiation, Programmierung, Mensch-Maschine-Kommunikation u.v.m. finden sich hier wieder“ (Burkert et al. 2005, S. 3).

Unter zu Hilfenahme des Lehrplans für Informatik des Wahlpflichtfach/Wahlfach der Sekundarstufe I (Ministerium für Bildung, Wissenschaft, Jugend und Kultur Rheinland-Pfalz 2010, S. 23) lassen sich die inhaltlichen Themen für den Informatik-Unterricht einschränken auf:

- Die Bedeutung und Eigenschaften von Datenbanksystemen erläutern
- Miniwelten mit Hilfe von Tabellen modellieren (optional: ERM-Modellierung)
- Abfragen an eine Datenbank entwerfen
- Datenerhebungen unter dem Aspekt Datenschutz bewerten

Der letzte Punkt kann im datenbankspezifischen Teil dieser Arbeit vernachlässigt werden, da es Bestandteil der restlichen Reihe ist. Weiterhin bedarf es noch der Klärung der Fachbegriffe in diesem Zusammenhang.

Zuerst wird die Art der genutzten Datenbank auf eine **relationale Datenbank** festgelegt, da ausschließlich mit solchen in *Instahub* gearbeitet wird. Eine relationale Datenbank, oder genauer, eine tabellenbasierte relationale Datenbank, dient der elektronischen Datenverwaltung in Computersystemen. Sie beruht auf einem zu Grunde gelegten Modell, welches wiederum aus Tabellen besteht. Diese Tabellen beschreiben *Relationen* zwischen den Daten, auf denen wiederum gewisse, definierte *Operationen* möglich sind. Zum Abfragen der Daten sowie Ausführen der Operationen (Einfügen, Verändern, Löschen, Auslesen) wird eine geeignete Datenbanksprache benötigt. In diesem Fall wird dies durch die Sprache **SQL**[36] ermöglicht. Sie orientiert sich in ihrer Semantik an der englischen Sprache und wird durch die ISO[37] und IEC[38] standardisiert. Durch die Nutzung von SQL erfüllt die genutzte Datenbank sämtliche Anforderungen für eine relationale Datenbank (Keltz 1998, Kap. 6).

[36] SQL ist die Kurzform von *structured query language.* Die Sprache basiert auf einer relationalen Algebra.
[37] International Organisation for Standardisation, www.iso.org (zuletzt geprüft: 03.04.2019)
[38] International Electrotechnical Commission, www.iec.ch (zuletzt geprüft: 03.04.2019)

Das **Datenbankmodell** besteht in unserem Fall aus Tabellen (die generische Datenstruktur). Die Tabelle selbst besteht aus Spalten (genannt *Attribute)* und Zeilen (genannt *Tupel*). Beschrieben wird die Tabelle durch das *Relationsschema*, welches die Art der Attribute festlegt. Genau ein Attribut kann als *Primärschlüssel* festgelegt werden. Dieser ist der Referenzwert für den kompletten Datensatz. Die Tabelle kann ebenfalls sogenannte *Fremdschlüssel* enthalten, die auf Primärschlüssel (oder Attribute) aus anderen Tabellen verweisen. Sogenannte *flache Tabellen* enthalten keine Fremdschlüssel (vgl. Codd 1991, S. 1 ff.). Tabelle 3 zeigt beispielhaft eine Tabelle aus einer möglichen Datenbankstruktur.

Buchnummer *(Primärschl.)*	**Autor** *(Attribut 1)*	**Verlag** *(Attribut 2)*	**Jahr** *(Attribut 3 + Fremdschl.)*	**Titel** *(Attribut 4)*	**Datum** *(Attribut 5)*
123456	Hans Vielschreiber	Musterverlag	2007	Wir lernen SQL	13.01.2007
123457	J. Gutenberg	Gutenberg und Co.	1452	Drucken leicht gemacht	01.01.1452
123458	Galileo Galilei	Inquisition International	1640	Eppur si muove	1641
123459	Charles Darwin	Vatikan Verlag	1860	Adam und Eva	1862

***Tabelle 3**: Beispieltabelle aus einer Datenbank*[39]

[39] Quelle: https://goo.gl/SSB4L8 (zuletzt geprüft: 03.04.2019)

Das **ER-Modell** dient zur Beschreibung der Datenbanksemantik in einem realen Bezug. Häufig wird diese Art der Modellierung in der Entwicklungsphase eines Projekts genutzt, um eine gemeinsame Basis zwischen Anwendern und Entwicklern zu schaffen, welches von beiden Seiten interpretiert und diskutiert werden kann. Es besteht aus einer endlichen Menge an *Objekten* (**Entitäten**) und ihren *Attributen* (Eigenschaften) sowie deren Verknüpfungen (engl.: **relations**) untereinander (vgl. Chen 1976, S. 10 ff.). Der Aufbau des Modells befolgt bestimmte Regeln bezüglich der Kardinalitäten von Beziehungen und hinsichtlich der Notation. Diese sind für eine Verwendung in der Orientierungsstufe jedoch nicht von Nöten. Abb. 5 zeigt ein simples ERM für *Instahub*.

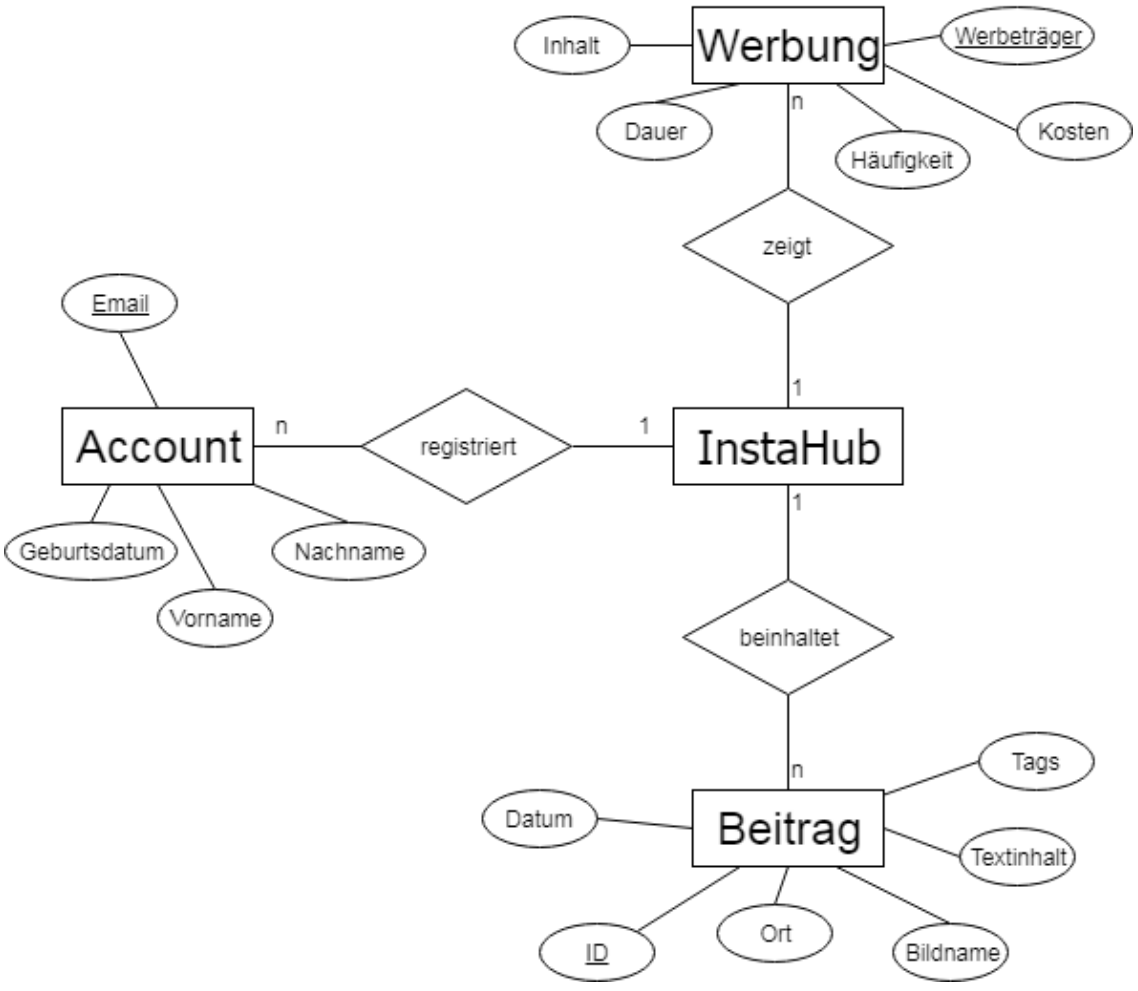


***Abbildung 5**: Simples ERM zu Instahub*[40]

[40] Die Objekte werden durch Rechtecke dargestellt, Attribute durch Ellipsen und Verknüpfungen durch Linien und Rauten. Primärschlüssel werden durch Unterstreichen gekennzeichnet.

SQL-Befehle, welche die Unterrichtsreihe betreffen, lassen sich mit dem **DML**[41]-Teil der SQL-Sprache abdecken. Für eine übersichtliche Beschreibung wurde die „Ultrakurzeinführung für SQL“ von Unterstein und Matthiessen anschaulich zusammengefasst (siehe Unterstein und Matthiessen 2012, S. 1-5).

Befehl	Bedeutung	Beispielcode
SELECT … FROM	Auslesen von Tabellenspalten.	SELECT spalte1, spalte2 … FROM tabellenname;
SELECT DISTINCT	Auslesen von Tabellenspalten. Jede Zeile mit gleichem Inhalt wird zusammengefasst.	SELECT DISTINCT * FROM tabellenname;
MIN / MAX / LIMIT	Klauseln, um die Auswahl (bzgl. der Anzahl) einzuschränken.	SELECT MIN(*spalte1*), … FROM *tabellenname;*
WHERE	Klausel, die weitere Bedingungen angibt, um SELECT zu präzisieren.	SELECT *spalte1, spalte2, …* FROM *tabellenname* WHERE *bedingung;*
AND / OR / NOT	Logische Operatoren, um WHERE-Klausel zu beschreiben.	SELECT *spalte1, spalte2, …* FROM *tabellenname* WHERE *bedingung1* AND *bedingung2* OR …;
ORDER BY	Sortiert die Ausgabe. Weiterhin durch ASC und DESC definierbar. (aufsteigend/absteigend)	SELECT *spalte1, spalte2, …* FROM *tabellenname* ORDER BY *spalte1, spalte2, …* ASC;
DELETE FROM	Löschen eines Eintrags.	DELETE FROM *tabellenname* WHERE *bedingung*;

[41] DML steht für *Data Manipulation Language* und umfasst alle Befehle, die sich in ihrer Funktion durch *Lesen, Einfügen, Ändern* oder *Löschen* beschreiben lassen.

INSERT INTO … VALUES	Einfügen eines Eintrags. VALUES gibt Werte des Eintrags an.	INSERT INTO *tabellenname* VALUES *(wert1, wert2, wert3, …);*
UPDATE … SET	Verändern eines Eintrags. SET gibt neue Werte des Eintrags an.	UPDATE *tabellenname* SET *spalte1 = wert1, spalte2 = wert2, …* WHERE *bedingung;*

***Tabelle 4**: Übersicht grundlegender SQL-Befehle*

Das Projekt Instahub soll nun im Rahmen dieser Arbeit durch eine weitere Unterrichtsreihe erweitert werden. Dabei wird das Thema Datenschutz in den Mittelpunkt gerückt. Zielgruppe der folgenden Reihe sind die Klassenstufen 5-6 eines Gymnasiums.

4. Didaktische und methodische Ausarbeitung

Dieses Kapitel beinhaltet den Hauptteil der Arbeit. In den folgenden Unterkapiteln wird zunächst die Konzeption der entwickelten Unterrichtsreihe vorgestellt. Danach werden die einzelnen Unterrichtseinheiten erläutert sowie hinsichtlich der Didaktik und Methodik ausgearbeitet. Aus inhaltlichen Gründen werden manche Einheiten zusammengefasst. Zum Abschluss wird ein Teil der Reihe an einer geeigneten Lerngruppe getestet und damit evaluiert (siehe dazu 5.1).

4.1 Konzeption der Reihe

Die geplante Unterrichtsreihe baut zu großen Teilen auf der Plattform *Instahub* und ihren Funktionen auf. Deshalb geht die Planung ebenfalls von dem bereits beschriebenen Aspekt *Datenschutz und -sicherheit* (vgl. 3.1) aus. Zielgruppe dieser Lerneinheiten ist die Klassenstufe 5-6 einer weiterführenden Schule, also die Orientierungsstufe. Weiterhin ist es das Ziel der Reihe, Datenschutz als Themenschwerpunkt zu erhalten, jedoch den eigentlichen Hintergrund von *Instahub*, nämlich die Nutzung von Datenbanken im Kontext Sozialer Netzwerke, nicht außer Acht zu lassen. Außerdem gibt der Inhalt der UE einen Ausblick auf den Unterricht in der Sekundarstufe II bzw. das Wahlpflichtfach in höheren Klassenstufen.

Als Unterrichtsmaterialien wurden Arbeitsblätter gewählt. Dadurch soll ermöglicht werden, dass Arbeitsblätter auch in Eigenregie, ohne das beschriebene didaktische Unterrichtskonzept, bearbeitet werden können. Weiterhin sind Inhalt und Aufgabenstellungen so allgemein wie möglich formuliert. Somit wird der Lehrperson die Möglichkeit geboten, die Arbeitsblätter auch unabhängig von dieser Ausarbeitung zu nutzen, die Reihenfolge zu ändern oder Themenbereiche einzufügen und wegzulassen.

In Anlehnung an die Konzeption der Unterrichtsreihe von *Instahub* (vgl. Tab. 2) wurde eine Konzeptionsübersicht für die neue Reihe erstellt. Sie beinhaltet die Themenbereiche, eine Übersicht über die jeweiligen Inhalte und eine vermutete Anzahl an Unterrichtseinheiten, die im schulischen Sinne dafür benötigt werden (45 Minuten pro Einheit). Diese Übersicht ist in Tab. 5 festgehalten:

Teilbereich der Reihe		Inhalt	vermutete Anzahl d. UE
Datenschutz in Sozialen Netzwerken	Als Anwender	Welche Informationen sind schützenswert? Was ist ein sicheres Profil? Bewertung von gegebenen Profilen.	2 – 4 UE
	Aus der Sicht von Sozialen Netzwerken	Was sind Nutzungsbedingungen? Wo finde ich diese? Welche Schutzmaßnahmen bieten mir Soziale Netzwerke? Warum sammeln diese meine Daten?	1 – 2 UE
Browsersicherheit / Sicherheit im Netz		Wie werden Daten gesammelt (u.a. User Tracking)? Welche Möglichkeiten habe ich, um mich im Internet generell abzusichern (Plug-Ins, Proxyserver, Browserindividualisierung …). Wissen um Tools. Nutzen von Tools.	2 – 3 UE
Exkurs: Datenbanken	Nutzen und Modellieren von DB	Wie werden Daten gespeichert? Modellbildung. Nutzen von Instahub mit SQL Befehlen per Dropdown-Menü.	4 UE

***Tabelle 5**: Konzeption der Unterrichtsreihe*

Da die Reihe sich spezifisch im Kontext der Sozialen Netzwerke ansiedelt, wird zunächst darauf verzichtet, die Schüler mit dem Aufbau und der Funktionsweise von Datenbanken zu

konfrontieren. Zudem ist sie im Sinne der IniK[42] kontextorientiert, sodass die Schülermotivation dadurch gesichert wird. Dazu wird der Teil Datenschutz in Sozialen Netzwerken in zwei Bereiche aufgeteilt: Aus der *Sicht des Anwenders* (hier: Schüler) und aus der *Sicht des Betreibers* des Sozialen Netzwerks.

Der Fokus des Einstiegs liegt auf der Begründung des Datenschutzes. Geltende Gesetze und Verordnungen, wie die DSGVO, das BDSG und LDSG stützen diesen Bereich durch ihren Inhalt. Die Lernenden sollen selbst das Gefühl entwickeln, dass ihre Daten, die sie eventuell bereits preisgeben, schützenswert sind. Dazu sollen in *Instahub* unterschiedliche Profile betrachtet werden. Nach dem Festlegen von Kriterien, die ein öffentliches Profil (bzgl. des Datenschutzes) sicher machen, sollen diese Profile zusätzlich noch bewertet werden. Die Schüler sollen nach diesem Teil in der Lage sein, ihr eigenes, in einem realen Sozialen Netzwerk existierendes Profil einzuschätzen und gegebenenfalls abzuändern.

Im zweiten Bereich geht es um den Datenschutzaspekt aus der Sicht des Sozialen Netzwerks. Das Auseinandersetzen mit den Nutzungsbedingungen, die Schutzmaßnahmen, die dem Anwender geboten werden sowie das Sammeln von Anwenderdaten durch Netzwerke sind hierbei prägnante Kernpunkte. Dabei sollen Schüler vor allem in eigener Recherche in Erfahrung bringen, wo besagte Informationen zu finden sind und welche Verträge der Anwender eingeht, wenn er sich in einem Netzwerk wie *Instahub* anmeldet.

Der zweite Teil der Reihe behandelt die generelle Sicherheit im Internet und welche Rolle dabei die Browserindividualisierung spielt. Es wird die Frage geklärt, warum Daten gesammelt werden. Anschließend werden Tools bzw. Plug-Ins behandelt, um den Schülern eine Übersicht ihrer Auswahlmöglichkeiten zu geben. Zusätzlich werden die Schüler die Tools in dieser Phase auch ausprobieren, um Vor- und Nachteile herauszuarbeiten und anschließend eine Bewertung abzugeben.

Der letzte Abschnitt der Reihe behandelt den Unterrichtsschwerpunkt Datenbanken. Im Mittelpunkt stehen Nutzen und Modellieren von Datenbanken. Dazu wird zunächst, angelehnt

[42] Kurz für Informatik im Kontext. Dies ist ein Unterrichtskonzept, das darauf zielt, Schüler stärker in ihrer Lebenswelt abzuholen und so für die Gestaltung von Informatiksystemen zu sensibilisieren.

an das ER-Modell, dargestellt, wie Datenbanken arbeiten. Darauf aufbauend, sollen die Schüler mit Hilfe einer vereinfachten Oberfläche simple Operatoren auf die Datenbanktabellen anwenden. Angedacht war zunächst noch ein kurzer Abschnitt über die Sicherheit von Datenbanksystemen. Hinsichtlich des jungen Alters der Lerngruppe, wurde diese Idee jedoch im Konzept verworfen. Um herauszustellen, welche Bedeutung Datenbanken als solches in der IT-Sicherheit spielen, benötigt es Informationen, die deutlich komplexer sind als die zuvor behandelten Themen. Dies würde das Unterrichtsniveau der Orientierungsstufe deutlich überschreiten.

Da sich das Unterrichtskonzept von Dorn hauptsächlich auf Datenbanken konzentriert und das Thema Datenschutz nur als Teilaspekt zu sehen ist, jedoch Schwerpunkt dieser Arbeit sein soll, wird die erarbeitete Unterrichtsreihe losgelöst von Dorns Ansatz sein. Während Schüler im ursprünglichen Ansatz als Administratoren des Sozialen Netzwerks agieren, verwenden diese *Instahub* in der neuen Reihe ausschließlich als Anwender. Lediglich der letzte Teil der Reihe bildet hierzu eine Ausnahme.

4.2 Vorbemerkungen zur Unterrichtsplanung

Die Struktur der Planung orientiert sich an den Gesichtspunkten für Unterrichtsplanung nach Esslinger-Hinz et al. (Esslinger-Hinz et al. 2013, S. 27-118). Zuerst werden die Hauptlernziele der Reihe genannt, gefolgt von Bemerkungen zur theoretischen Lerngruppe und den fachwissenschaftlichen Bemerkungen.

4.2.1 Hauptlernziele

Das Hauptlernziel der Reihe ist die Förderung von Datenschutzkompetenz. Hinsichtlich dem zeitlichen wie auch inhaltlichen Umfang der Reihe sowie dem jungen Alter der erwarteten Lerngruppen, lässt sich das Ziel weiter einschränken. Die Reihe soll demnach grundlegende Teilkompetenzen der Datenschutzkompetenz fördern. Die Datenschutzkompetenz wurde bereits in 2.4 näher definiert und erläutert. Es ist davon auszugehen, dass die gegebenen Lerngruppen sehr wenig bis keine Kompetenzen in den Bereichen besitzen.

4.2.2 Bemerkungen zur Lerngruppe

Da die Unterrichtsreihe nicht für eine bestimmte Lerngruppe entwickelt wurde, sind die Bemerkungen als theoretische Hinweise zu sehen. Durch den Umstand, dass es bisher keinen Informatikunterricht in der Orientierungsstufe an weiterführenden Schulen gibt, wird diese Reihe wahrscheinlich im Rahmen eines anderen Faches durchgeführt. Weiterhin ist davon auszugehen, dass es sich dabei um den Anfangsunterricht für die Schüler im Bereich der Informatik handelt. Daraus ist zu schließen, dass es sich bei der Lerngruppe um eine mehr oder weniger inhomogene Gruppe handelt, mit deutlichen Unterschieden in ihren individuellen Vorkenntnissen. Es ist möglicherweise ein Mangel an Kooperationsbereitschaft und ein gewisses Maß an Selbstüberschätzung bei den Schülern zu erwarten. Besonders im Hinblick auf den Kontext der Sozialen Medien kann es vorkommen, dass Schüler sich im spielerischen Aspekt der Unterrichtsstunden verlieren. Bezogen auf den letzten Punkt wurde versucht, die Reihe nicht zu spielerisch zu gestalten, ohne dabei die Eigenaktivierung seitens der Schüler zu unterbinden.

Im Hinblick auf die Unterrichtsinhalte sollte ein gewisser Umgang mit dem Computer vorausgesetzt sein:

- Das Ein- und Ausschalten der Rechner
- An- und Abmeldung im Schulnetzwerk
- Nutzen eines Internetbrowsers (Eingabe der URL, Nutzen einer Suchmaschine)
- Eventuell Abspeichern von Ergebnissen und Abrufen gespeicherter Aufgaben

4.2.3 Fachwissenschaftliche Bemerkungen

Die fachwissenschaftlichen Inhalte wurden bereits in Kapitel 2 und 3.3 ausgiebig erörtert. Folgend sollen nur kurz die für die Unterrichtseinheiten wichtigen Aspekte genannt werden.

Mit der Anmeldung in Sozialen Netzwerken gibt der Nutzer dem Anbieter die Einwilligung zur Verarbeitung seiner personenbezogenen Daten. Personenbezogene Daten sind Daten, mit Hilfe derer eine reale Person direkt oder über die Verarbeitung und Verbindung dieser indirekt identifiziert werden kann. Die Einwilligung ist auf Grund der informationellen Selbstbestimmung von Nöten und kann jederzeit vom Nutzer wiederrufen werden. Weiterhin

muss der Betreiber der betroffenen Person zu jeder Zeit mitteilen können, welche Daten momentan verarbeitet werden, gespeichert sind, angelegt wurden und gelöscht werden können. Die DSGVO steht trotz ihres Umfangs der missbräuchlichen Datenverarbeitung gegenüber. Überwachung, unreflektierte Datenpreisgabe und Schadsoftware sind Gefahren, die in der Unterrichtsreihe behandelt oder erwähnt werden. Der Schwerpunkt bezieht sich jedoch auf die Schutzmaßnahmen, wie das Erstellen eines sicheren Passworts und das Verwenden von Anonymisierungstools im Browser.

Weiterhin wird der Bereich der Datenbanken thematisiert. Grundlegende Befehle in SQL und die Modellierung mit Hilfe des Entity-Relationship-Modells bilden die Basis dieser Einheit. Aufgrund ihrer Komplexität werden diese sehr reduziert behandelt.

4.2.4 Legitimation der Unterrichtsreihe

Über die Aktualität der Datenschutzproblematik und der Präsenz von Gefahren bzgl. personenbezogener Daten wurde die Umsetzung der Unterrichtsreihe mehrfach legitimiert. Weiterhin wurde sie mit Hilfe des Lehrplans wie auch den Richtlinien des Verbraucherschutzes begründet (vgl. 2.1).

Datenschutz ist nicht nur in der informatischen Bildung zu finden. Die Kultusministerkonferenz (KMK) entwickelt in ihrem Papier *Bildung in der digitalen Welt* Kompetenzrahmen für fächerübergreifende Inhalte. Die entwickelte Reihe ist gut im Bereich *Schützen und sicher Agieren* einzuordnen (Kultusministerkonferenz 2016, S. 16).

Der Orientierungsrahmen für Schulqualität greift diese Kompetenzbildung im Bereich Medien mit der Formulierung auf, dass „Lehrerinnen und Lehrer […] über die gesamte Schulzeit hinweg Schülerinnen und Schüler an den reflektierten Umgang mit digitalen Medien heran [führen und diese] […] in allen Fächern den systematischen Erwerb digitaler Kompetenzen [fördern]“ (Ministerium für Bildung, Wissenschaft, Jugend und Kultur Rheinland-Pfalz 2017, S. 8).

Weiterhin ist der Datenschutz auch in den Bildungsstandards der GI wiederzufinden: „[Die Schülerinnen und Schüler] benennen Wechselwirkungen zwischen Informatiksystemen und ihrer gesellschaftlichen Einbettung, nehmen Entscheidungsfreiheiten im Umgang mit

Informatiksystemen wahr und handeln in Übereinstimmung mit gesellschaftlichen Normen, reagieren angemessen auf Risiken bei der Nutzung von Informatiksystemen“ (Gesellschaft für Informatik e.V. (GI) 2008b).

Zusammenfassend ist zu sagen, dass das Thema Datenschutz und die damit einhergehenden Kompetenzen mehr als ausreichend an verschiedenen Stellen als Unterrichtsinhalt legitimiert werden.

4.3 Unterrichtseinheit 1: Einstieg

Didaktische Analyse:

Die zu erreichenden Teillernziele der Unterrichtsreihe für diese Stunde:

- Schüler nutzen *Instahub* sachgerecht.
- Schüler entnehmen vorgegebenen Profilen alle Informationen und sortieren diese entsprechend.

Passend zur Unterrichtseinheit ist das Arbeitsblatt 1 (siehe Anhang 2) hinzuzuziehen.

Zum Einstieg der Unterrichtsreihe steht das Heranführen der Schüler in den Themenbereich sowie der Umgang mit *Instahub* als Lernplattform im Mittelpunkt. Es wird vorausgesetzt, dass sich die meisten Schüler (auch in der Klassenstufe 5-6) in ihrer Freizeit zu einem großen Anteil mit Sozialen Netzwerken beschäftigen (vgl. Medienpädagogischer Forschungsverbund Südwest 2015, S. 31-39). Daran geknüpft sind gewisse Kenntnisse im Umgang mit diesen Diensten: Erstellen von Beiträgen, Bewerten von Beiträgen, Kommentieren, Orientierung auf der Webseite des Anbieters und das Prinzip von *Follow/Unfollow*[43]. Hier ist bereits die erste Schwierigkeit zu erkennen. Es ist nicht mit Sicherheit jeder Schüler mit dem Umgang vertraut, ebenso wenig ist das Kompetenzniveau dahingehend ausgeglichen. Da *Instahub* als solches ein neues Netzwerk für die Schüler darstellt, kann verhindert werden, dass erfahrenere Schüler die Anderen inhaltlich abhängen. Jedoch sind die Strukturen der Plattform an

[43] Jemandem in einem Sozialen Netzwerk zu folgen, bedeutet über ihre Beiträge, Profileinträge etc. benachrichtigt zu werden.

bekannte Netzwerke angelehnt, sodass Vorkenntnisse leicht auf *Instahub* übertragen werden können. Der Einstieg in *Instahub* ist die Grundlage für die gesamte Unterrichtsreihe und sollte deshalb soweit ausgebaut sein, dass jeder Schüler sich ohne größere Schwierigkeiten im Hub orientieren und die wichtigsten Funktionen nutzen kann.

Aufbauend auf den Umgang mit *Instahub* sollen die Schüler im zweiten Teil der Stunde Informationen aus Profilen der Plattform heraussuchen. Damit sollen die zuvor erarbeiteten Umgangsfähigkeiten aus dem ersten Teil erprobt werden. Die Schüler sollen durch das Nutzen aller Funktionen von *Instahub* sämtliche Informationen über die Personen in Erfahrung bringen. Je mehr Funktionen sie dazu nutzen, desto mehr Informationen erhalten sie. Unterschiedlicher Umfang dieser Informationen kann bei einer Besprechung zur Diskussion genutzt werden.

Methodische Konzeption:

Der Stundeneinstieg kann leicht durch den Themenbereich Soziale Netzwerke geführt werden. Für diese Reihe wurde ein stummer Impuls über die Logos diverser Netzwerke gewählt (siehe Anhang 3). Diese werden als Projektion, z.B. als Folie auf einem Overheadprojektor, an die Wand des Klassenzimmers/Computerraums geworfen. Die meisten Netzwerke sollten den Schülern bekannt sein, wodurch jeder Schüler etwas dazu sagen kann. Bedenkzeit räumt hierbei auch weniger aktiven Schülern die Möglichkeit ein, Sprachbeiträge zu äußern. Anschließend werden Ideen im Unterrichtsgespräch gesammelt. Im Gespräch werden Schülerinteressen bzgl. Sozialer Netzwerke thematisiert. Weiterhin bietet es sich hier an, die Schüler nach dem Mindestalter für die Nutzung von den gezeigten Diensten zu fragen. Durch gezieltes Nachfragen kann hier bei den Schülern ein gewisses Interesse an den Richtlinien und dem Überdenken des eigenen Vorgehens geweckt werden.

Folgend soll die Plattform *Instahub* kurz als Lehrervortrag vorgestellt werden. Hierbei sollen die Vorgaben aus dem Einführungsprotokoll genutzt werden (siehe Anhang 4). Das Einführungsprotokoll ist Voraussetzung für die kommenden Unterrichtseinheiten. Die Schüler melden sich auf einem Hub an und beginnen danach mit der Bearbeitung des ersten Arbeitsblattes.

Die Bearbeitung des Arbeitsblattes findet grundsätzlich immer in Partnerarbeit am Computer statt. Es wird davon ausgegangen, dass die Schule nicht über mehr PCs pro Raum als Schüler pro Klasse verfügt. Deshalb ist die Arbeit am Rechner immer als Partnerarbeit konzipiert und die Arbeitsblätter immer in der zweiten Person Plural formuliert. Außerdem wurden Zahlen innerhalb der Aufgabenstellungen immer als Ziffer formuliert, um Unklarheiten vorzubeugen (z.B.: „Fügt 3 weitere Faktoren hinzu“).

Im ersten Teil der Aufgabenstellungen arbeiten die Schüler mit den Funktionen von *Instahub*. Sie erkunden die Seite und werden durch die Aufgabenstellung mit allen für diesen Teil relevanten Funktionen vertraut gemacht. Anschließend nutzen sie im zweiten Abschnitt ihre Kenntnisse von den vorangegangenen Aufgaben, um Informationen über drei Personen herauszusuchen. Die Daten sind absichtlich so angelegt, dass hier Schüler durchaus zu anderen Ergebnissen kommen können. Beispielsweise ist der richtige Vorname von *So Dingenskirchen* im Benutzernamen versteckt. Die Lehrperson steht in dieser Phase als Unterstützer zur Verfügung. Sollten Handlungsabläufe im Hub unklar sein, kann hier durch vereinzelte Hilfe Klarheit verschafft werden.

Im letzten Teil der Unterrichtseinheit werden die Ergebnisse der Partnerarbeit im Unterrichtsgespräch zusammengetragen. Dazu bietet sich erneut der Overheadprojektor oder eine Tafel als Medium an. Das Medium wird zur Aktivierung der Schüler genutzt, damit diese die Tabelle aus Aufgabe 3 im Plenum vervollständigen und an Tafel oder Overheadprojektor ausfüllen. Alternativ kann statt einem Unterrichtsgespräch auch ein von Schülern geführtes Gespräch genutzt werden, wobei sich die Schüler gegenseitig aufrufen. In beiden Formen fungiert die Lehrperson als Moderator. Diese Phase soll zur Diskussion unter den Schülern anregen, welche Informationen wo gefunden werden konnten. Dadurch soll die Vorstellung der Schüler, wie viele Daten bei der Nutzung der Netzwerke preisgegeben werden, erweitert werden. Es ist für die nächste Unterrichtseinheit wichtig, dass die Schüler die gleichen Informationen in ihrer Tabelle in Aufgabe 3 eingetragen haben.

Die nachfolgende Tabelle zeigt einen Kurzentwurf über den Verlauf der Einstiegseinheit. Der Kurzentwurf wird am Ende jeder Unterrichtseinheit durch eine vergleichbare Tabelle zusammengefasst:

Nummerierung	Unterrichtsteil	Inhalt	Dauer [min]	Sozialform / Medium
1	Im Lernkontext ankommen	- Erkennen von Logos Sozialer Netzwerke - Erläuterung von Funktionen der Netzwerke -Eigenschaften benennen -Eigene Nutzung beschreiben	5	UG / stummer Impuls, Projektor
2	Vorwissen aktivieren	- Aufgaben 1-2 - Nutzung von Instahub	5-10	PA / Computer, AB
3	Lernprodukt erstellen	- Aufgabe 3 (Tabelle)	15	PA / AB
4	Lernprodukt diskutieren	- Gemeinsame Lösung der Tabelle erstellen - Diskutieren der Ergebnisse / Vorgehensweisen	15	UG / Tafel, Folie

***Tabelle 6**: Kurzentwurf UE 1*

Im Hinblick auf die Dauer des Anmeldeprozesses in *Instahub*, kann diese Unterrichtseinheit mit der Einführung auch auf zwei Einheiten oder eine Doppelstunde ausgeweitet werden.

4.4 Unterrichtseinheit 2: Das sichere Profil

Didaktische Analyse:

Die zu erreichenden Teillernziele der Unterrichtsreihe für diese Stunde:

- Schüler unterscheiden zwischen positiven und negativen Kriterien für ein Onlineprofil.
- Schüler bewerten ein vorgegebenes Profil anhand einer Kriterienliste und begründen ihre Entscheidung.

Im Datenschutzkompetenzmodell finden sich diese Teillernziele im Wissensaspekt und der Auswahl- und Nutzungskompetenz sowie Urteilskompetenz wieder. Passend zur Unterrichtseinheit ist das Arbeitsblatt 2 (siehe Anhang 5) hinzuzuziehen.

In diesem Abschnitt der Reihe werden die Schüler mit Kriterien für ein datenschutzkonformes Profil in Sozialen Netzwerken konfrontiert. Inhaltlich gibt es Begriffe wie Selbstdatenschutz, Datenschutzkonformität und informationelle Selbstbestimmung. Diese werden jedoch aufgrund der Klassenstufe (5-6) nicht als solche genannt[44]. Ein Profil, das der Datenschutzkonformität entspricht, wird im Unterricht als *sicheres Profil* bezeichnet (vgl. 2.3.1). Im Gesamtbild ist dieser Teil der Reihe als besonders wichtig einzustufen. Die Fähigkeit, ein Profil auf ihre Datenschutzkonformität zu überprüfen, ist diese, welche sie auch im Alltag anwenden müssen. Da sich viele von den Schülern bereits mit Sozialen Netzwerken auseinandersetzen, hat das Erlangen von Teilkompetenzen in diesem Bereich eine bedeutsame Auswirkung auf ihr eigenes Tun und Handeln. Es ist auch hier davon auszugehen, dass die Schüler bereits durch Einfluss ihrer Eltern, Geschwister oder Mitschüler eine gewisse Sensibilität hinsichtlich des sicheren Profils ausgebildet haben. Nichts desto Trotz sind diese Vorerfahrungen nicht mit einer konkreten Kriterienliste versehen worden. Der inhaltliche Schwerpunkt der Stunde wird daher das Erstellen eines Kriterienkatalogs sein, der für den weiteren Unterricht wie auch den Alltag verwendet werden kann.

Im weiteren Verlauf der Stunde werden die Schüler den gefundenen Katalog dazu nutzen, die Profile aus der ersten Unterrichtseinheit zu bewerten. Deshalb sollten bei der vorherigen Erstellung des Katalogs sämtliche Zweifel und Unklarheiten seitens der Schüler ausgeräumt sein. Dabei ist zu beachten, dass manchen Schülern gewisse Kriterien als unwichtig erscheinen, oder unpassende Kriterien als wichtig. Aufgrund dessen sollte jedes Kriterium ausgiebig mit Beispielen belegt werden.

[44] In höheren Klassenstufen der Sekundarstufe I können die Begriffe durchaus im Verlauf der Unterrichtsreihe erläutert und definiert werden.

Methodische Konzeption:

Die zweite Unterrichtseinheit schließt thematisch direkt an die erste an. Eine gute Variante in der Umsetzung wäre daher eine Doppelstunde für beide Unterrichtseinheiten. Sollte zwischen den Einheiten ein etwas längerer Zeitraum liegen, könnte der Unterricht durch eine Wiederholung der Kernpunkte aus der letzten Stunde zusammengefasst werden. Bevorzugt wird die Variante, in der zwei Schüler ausgewählt werden. Der eine fasst die wichtigsten Punkte der letzten Stunde zusammen. Der andere Schüler unterstützt durch Korrektur und Ergänzungen.

Im Hauptteil der Unterrichtseinheit wird ein Kriterienkatalog für ein sicheres Profil erstellt. Dazu bearbeiten die Schüler, je nach Lerngruppe in Partner- oder Einzelarbeit, die Aufgabe 1 des Arbeitsblattes Nr. 2. Die Schüler müssen die Kriterien hier nur als positiv oder negativ für ein sicheres Profil einordnen. Dadurch wird sichergestellt, dass jedem Schüler ein ausreichend umfangreicher Katalog zur Verfügung steht. Die Zusatzaufgabe „*Fügt weitere Kriterien hinzu*“ für besonders schnelle Schüler ist hier ratsam. Anschließend wird der Katalog im Unterrichtsgespräch besprochen und diskutiert. Einige der Kriterien sind absichtlich ungenau definiert, sodass hier Diskussionsbedarf besteht. Ein Beispiel dafür wäre das Kriterium *Partybilder hochladen*. Hiermit könnten sowohl Bilder von Alkoholexzessen als auch Bilder von Schulveranstaltungen gemeint sein. Das Unterrichtsgespräch wird dazu genutzt, verschiedene Aspekte und Ansichten für jedes Kriterium zu sammeln und diese dann für alle mit der Tabelle zu definieren.

Im zweiten Teil der Stunde sollen mit Hilfe des Kriterienkatalogs die Profile aus der vorangegangenen Einheit bewertet werden (Aufgabe 2). Der Schwerpunkt liegt hier auf der Begründung für ihre Entscheidung. Die Bearbeitung findet wieder in Partnerarbeit statt. Die anschließende Besprechung sollte eine Mischung aus Unterrichtsgespräch und Schülervortrag sein. Die Ergebnisse werden schriftlich auf einer Tafel/Folie festgehalten, um für alle Schüler das gleiche Endergebnis darzustellen.

Alternativ lässt sich die Stunde auch mit einer Mindmap-Konzeption beginnen. Dafür wäre der Einsatz des Arbeitsblattes obsolet. Die Erstellung der Kriterienliste würde in Gruppenarbeit oder im Unterrichtsgespräch stattfinden. Die Bewertung der Profile wäre als mündlicher

Auftrag zu geben. Für die durchgeführten Stunden wurde sich jedoch für die zuerst beschriebene Variante entschieden, um die Gesamtstruktur der Unterrichtsreihe einzuhalten (vgl. 4.1).

Nummerierung	Unterrichtsteil	Inhalt	Dauer [min]	Sozialform / Medium
1	Im Lernkontext ankommen	- Zusammenfassen der letzten Stunde und ihrer Kernpunkte/Lernziele	5	SV, UG oder LV
2	Lernprodukt erstellen	- Aufgabe 1 (Tabelle)	15	PA oder EA / AB
3	Lernprodukt diskutieren	- Kriterien gemeinsam zuordnen (Besprechung) - Diskussion der Aussage von Kriterien	15	UG / Tafel, Folie
4	Sichern und vernetzen	- Bewerten von Profilen - Begründung vorstellen	10	PA, UG / Tafel, Folie

Tabelle 7: Kurzentwurf UE 2

4.5 Unterrichtseinheiten 3 – 4: Passwortsicherheit

Didaktische Analyse:

Die zu erreichenden Teillernziele der Unterrichtsreihe für diese Stunden:

- Schüler benennen schützenswerte Informationen eines Profils.
- Schüler nutzen Werkzeuge, um die Passwortsicherheit zu überprüfen.
- Schüler erstellen sichere Passwörter.
- Schüler nennen Schadsoftwarearten und ihre Eigenschaften.
- Schüler nennen Zusammenhänge zwischen Schadsoftware und Passwortsicherheit.

Im Datenschutzkompetenzmodell finden sich diese Teillernziele in der Auswahl- und Nutzungskompetenz sowie dem Wissen wieder. Passend zur Unterrichtseinheit ist das Arbeitsblatt 3 (siehe Anhang 6) hinzuzuziehen.

Im ersten Abschnitt des Unterrichts liegt der Schwerpunkt darauf, dass die Schüler erkennen, welche Informationen ihres Profils schützenswert sind, um dann daraus zu folgern, dass ihr Passwort einen Großteil davon schützt und deshalb von ebenso großer Relevanz ist. Es ist davon auszugehen, dass jeder der Schüler schon einmal ein Passwort erstellt oder verwendet hat. Deshalb ist weiterhin zu schlussfolgern, dass jeder Schüler grob zwischen einem guten und einem schlechten Passwort unterscheiden kann. Um den zuvor vorgestellten Faktoren für ein ausreichendes Passwort (siehe 2.3.3) gerecht zu werden, benötigt es ein Wissen um Faktoren für diese und ein Wissen um Überprüfungsmöglichkeiten. Diese Unterrichtseinheit soll damit den Abschluss zum Bereich *Datenschutz in Sozialen Netzwerken als Anwender* bilden.

Der Themenbereich Schadsoftware gehört nur indirekt in diesen Bereich der Datenschutzreihe. Er hängt nicht mit der Profilsicherheit in Sozialen Netzwerken zusammen und nimmt doch einen großen Einfluss darauf. Dadurch, dass Schadsoftware die Passwortsicherheit (z.B. durch Malware) beeinflusst, soll dieser Bereich zwar erwähnt werden, jedoch nicht den Schwerpunkt der Unterrichtseinheit bilden.

Methodische Konzeption:

Ein möglicher Einstieg in die Unterrichtseinheit ist ein Brainstorming. Die Schüler nennen ohne Zusammenhänge alle schützenswerten Informationen aus einem Onlineprofil. Anschließend wird in einem Unterrichtsgespräch ermittelt, wie sich diese Notizen gruppieren lassen. Beispiele hierfür sind z.B. Informationen über meine Person, Informationen über meine Aufenthalte, Informationen über meine Vorlieben usw. Das Ziel ist es, zu zeigen, dass das Passwort einen wesentlichen Teil beim Schützen dieser Daten spielt. Dazu müssen die Ideen aus dem Brainstorming zunächst an der Tafel/auf einer Folie gesammelt werden. Durch farbliche Markierungen können diese dann in Gruppen einsortiert werden. Das Passwort, sofern es genannt wird, sollte übrigbleiben und damit den Übergang zum zweiten Teil der Stunde bilden.

Der Hauptteil der Stunde findet in Einzel- oder Partnerarbeit statt. Das Arbeitsblatt Nr. 3 bietet mit den Aufgaben 1-3 genug Möglichkeiten, sich mit der Sicherheit von Passwörtern auseinanderzusetzen. Die Schüler entwickeln zuerst eine eigene Vorstellung von Kriterien, überprüfen diese und entwickeln danach mit Hilfe von zusätzlichen Informationsquellen einen ausgereiften Kriterienkatalog für ein sicheres Passwort. Um die erarbeiteten Kataloge zu sichern, wird im anschließenden Unterrichtsgespräch ein Schülerkatalog vorgestellt, gemeinsam korrigiert und ergänzt sowie auf einige Schülerbeispiele angewandt.

Alternativ kann für die Stunde auch ein Schülerwettbewerb (innerhalb des Klassenverbandes) angesetzt werden, wer das sicherste Passwort erstellt. Dazu können Passwörter mit bestimmten Kriterien (Länge, Inhalt) gesammelt und verglichen werden. Anschließend könnten die Zusatzinformationsquellen ausgegeben werden, um die zuvor erstellten Passwörter zu verbessern. Es wurde sich im Unterrichtsversuch für die erste Variante entschieden, da im zweiten Beispiel der spielerische Aspekt zu groß ist und damit der Lerneffekt geringer ausfallen könnte.

Die Auseinandersetzung mit Schadsoftware findet in einer weiteren oder mehreren Unterrichtseinheiten in Form eines Vortrags statt. Die Schüler setzen sich in Gruppenarbeit mit den Begriffen der Schadsoftware auseinander. Jede Gruppe übernimmt dabei eine Schadsoftwarekategorie und bereitet einen fünf- bis zehnminütigen Vortrag vor. Zur Unterstützung sind inhaltliche Punkte des Vortrags vorgegeben. Weiterhin sind Quellenangaben als Differenzierungsmaßnahme denkbar. Die wichtigsten Informationen werden auf einem gemeinsamen Plakat gesammelt und im Klassenraum / Computerraum ausgehangen. Der Umfang des Vortrages und ob die Vorbereitung im Rahmen des Unterrichts stattfindet oder außerhalb, steht der Lehrperson offen.

Nummerierung	**Unterrichtsteil**	**Inhalt**	**Dauer [min]**	**Sozialform / Medium**
1	Im Lernkontext ankommen	- Brainstorming zu schützenswerten Informationen in einem Profil - Einteilen in Gruppen	15-20	UG / Tafel

		- Erkennen der Relevanz von Passwörtern		
2	Vorwissen aktivieren + Lernprodukt erstellen	- Aufgaben 1-3	10-15	PA / Computer, AB
4	Lernprodukt diskutieren	- Gemeinsames Sammeln der Ergebnisse - Herausstellen der Unterschiede	10	UG / Tafel, Folie
5	Transferieren und festigen	- Vortrag zu Schadsoftware (5-10 min) - Plakat als Sicherung	45-90	GA

Tabelle 8: *Kurzentwurf UE 3-4*

4.6 Unterrichtseinheiten 5-6: Nutzungsbedingungen und Co.

Didaktische Analyse:

Die zu erreichenden Teillernziele der Unterrichtsreihe für diese Stunde:

- Schüler benennen Eigenschaften der Nutzungsbedingungen, Datenschutzrichtlinien und Cookie-Richtlinien eines Sozialen Netzwerks.
- Schüler nutzen und kennen Privatsphäre-Einstellungen innerhalb eines Sozialen Netzwerks.
- Schüler benennen Eigenschaften von User-Tracking und Cookies und erläutern die Zusammenhänge.
- Schüler nutzen eine Mind-Map zur Visualisierung ihrer Informationen.

Im Datenschutzkompetenzmodell finden sich diese Teillernziele im Wissensaspekt und der Auswahl- und Nutzungskompetenz wieder. Passend zur Unterrichtseinheit ist das Arbeitsblatt 4 (siehe Anhang 7) hinzuzuziehen.

In diesem Abschnitt der Unterrichtsreihe steht die Auseinandersetzung mit Nutzungsbedingungen, Datenschutzrichtlinien und Cookie-Richtlinien im Mittelpunkt. Da der Zugang zu Sozialen Netzwerken selbst für junge Schüler recht einfach möglich ist und nur die benannten Richtlinien genau festlegen, welche Daten verarbeitet werden, ist die Konfrontation mit diesen nicht zu umgehen. Die Schwierigkeit besteht, dass Schüler, besonders junge Anwender, mit der formalen Sprache in diesen Dokumenten überfordert sind. Es ist davon auszugehen, dass kein Schüler sich bereits damit auseinandergesetzt hat, sondern nur vage Vermutungen anstellen kann, was darin formuliert wird. Weiterhin sollte sich jeder Schüler bewusst sein, welche Einschränkungen er selbst bestimmen kann, um die Verarbeitung von Daten zu beeinflussen. Damit sind vor allem Privatsphäre-Einstellungen innerhalb eines Sozialen Netzwerks gemeint. Der Begriff der Datenverarbeitung wird nicht weiter definiert, da er für das Ziel der Unterrichtsreihe nicht als solcher von Bedeutung ist. Er wird im Folgenden mit dem *Nutzen* von persönlichen Daten *seitens des Anbieters* gleichgesetzt. Weiterhin werden die Begriffe *Cookie* und *User-Tracking* innerhalb der Unterrichtseinheit geklärt.

Besonders bei der Umsetzung können hier auf Grund der Komplexität einige Schwierigkeiten seitens der Schüler auftreten. Ebenfalls das Nicht-Vorhandensein eines Profils in einem Sozialen Netzwerk pro Schüler-Team ist ein Problem, das gelöst werden muss.

Methodische Konzeption:

Die Arbeitsblätter zum vierten Teil der Reihe bieten durch ihren Einleitungstext einen guten Einstieg in den Themenbereich, sodass der Beginn der Stunde direkt durch die Bearbeitung von den Aufgaben 1-2 geschafft werden kann. In diesen Aufgaben bearbeiten die Schüler in den üblichen Partnerarbeitsgruppen Aufgaben zu realen Nutzungsbedingungen. Leider kann hier nicht auf die Nutzungsbedingungen und Richtlinien von *Instahub* zurückgegriffen werden, da diese nur sehr unübersichtlich und Mittel zum Zweck sind. Deshalb greift das Arbeitsblatt auf die Richtlinien der Sozialen Netzwerke zurück, welche die Schüler wirklich nutzen. Hier muss vorher sichergestellt werden, dass diese Seiten alle zum Zeitpunkt der Durchführung online sind. Hilfestellungen durch die Lehrperson wären in dieser Unterrichtsphase: Links zu den entsprechenden Seiten und Hilfe bei der Begriffsklärung. Ansonsten ist der erste Teil als

Eigenarbeitsphase der Schüler konzipiert und zwingt sie dazu, sich mit den von ihnen eingewilligten Bedingungen und Richtlinien auseinanderzusetzen. Eine ausgiebige Besprechung der gefundenen Informationen ist hier aufgrund der Komplexität des Themas nötig. Ziel ist es, allgemeine Informationen zu sammeln und die Begriffe *Cookies* und *User-Tracking* als offene Frage im Raum stehen zu lassen.

Im zweiten Teil der Einheit geht es um die Klärung der beiden Begriffe. Die Schüler arbeiten in Eigenarbeit an der Informationsfindung genannter Begriffe. Anschließend werden die Ergebnisse in einer Mind-Map visualisiert. Eines der Ergebnisse der Schüler wird dann im Klassenverband vorgestellt und analysiert. So soll im Unterrichtsgespräch eine vollständige Lösung und Klärung der Begriffe stattfinden, sodass gegebenenfalls weitere Schülerbeiträge hinzugezogen werden können.

Alternativ wäre es möglich, die Recherchearbeit als Hausaufgabe zu formulieren. Das Konzipieren und Analysieren der Informationen wäre dann Hauptbestandteil der Unterrichtsstunde. Ebenfalls denkbar wäre dazu noch eine Unterrichtseinheit einzufügen, die sich mit der Visualisierung durch Mind-Maps allgemein beschäftigt, um die Fähigkeiten der Schüler im Ordnen von Informationen zu stärken.

Nummerierung	**Unterrichtsteil**	**Inhalt**	**Dauer [min]**	**Sozialform / Medium**
1	Im Lernkontext ankommen + Lernprodukt erstellen	- Aufgabenbearbeitung (1-2)	30-45	PA, EA / AB, Computer

3	Lernprodukt diskutieren	- Besprechung der gefundenen Informationen	15-20	UG / Tafel, Folie
4	Lernprodukt erstellen	- Recherche Cookie, User-Tracking	25	PA / AB, Computer
5	Lernprodukt diskutieren	- Analyse einer Mind-Map	20	UG / Folie, Visualizer

***Tabelle 9**: Kurzentwurf UE 5-6*

4.7 Unterrichtseinheiten 7-8: Sicher im Netz unterwegs

Didaktische Analyse:

Die zu erreichenden Teillernziele der Unterrichtsreihe für diese Stunde:

- Schüler nennen verschiedene Datenschutz-Plug-Ins.
- Schüler nennen Eigenschaften, Vorteile sowie Nachteile verschiedener Datenschutz-Plug-Ins.
- Schüler installieren ein Plug-In für den eigenen Browser und nutzen dieses.

Im Datenschutzkompetenzmodell finden sich diese Teillernziele im Wissen, der Auswahl- und Nutzungskompetenz sowie Urteilskompetenz wieder. Passend zur Unterrichtseinheit ist das Arbeitsblatt 5 (siehe Anhang 8) hinzuzuziehen.

In diesem Teil der Unterrichtsreihe (*Browsersicherheit / Sicherheit im Internet*) wird besonders auf die von Hug und Grimm geforderten Kompetenzen abgezielt. Da sich die Schüler nicht nur im Bereich der Sozialen Netzwerke online bewegen, ist das Surfen im Internet allgemein unter dem Datenschutzaspekt zu betrachten. Hauptinhalt der Unterrichtseinheit ist das Installieren, Verstehen und Nutzen von Adblockern. Dies soll zunächst als Beispiel der Möglichkeiten dienen, um die erlangten Kompetenzen später mit dem Wissen um andere Plug-Ins zu erweitern. Der Lernprozess lässt sich also in diese vier Schritte aufteilen: Installation eines

Plug-Ins, Verwenden eines Plug-Ins, Verstehen der Funktion und Transferieren des Wissens auf andere Programme.

Problematisch an diesem Ansatz könnten besonders die unterschiedlichen Vorkenntnisse der Schüler sein. Einige Schüler haben sich vielleicht bereits mit dem Installationsprozess oder sogar dem Nutzen von Plug-Ins für ihren Browser beschäftigt. Dennoch sollten alle Schüler jeden Schritt noch einmal durchgehen, da falscher oder leichtsinniger Umgang mit solchen Programmen auch negative Folgen haben könnte (z.B. Installation von Schadsoftware, Installationsfehler, die zu Abstürzen führen, etc.).

Das Beispiel *Adblock Plus* wurde gewählt, weil es effizient und fast ausnahmslos Werbung blockiert. Werbung auf den Seiten, welche die Schüler selbst besuchen, können so mühelos ausgeschaltet werden und bieten für den Schüler selbst einen besonderen Anreiz. Wichtig ist, dass der Schüler nicht nur die Anwendung versteht, sondern auch welche Rolle dies für den Schutz der eigenen Daten spielt.

Methodische Analyse:

Die Stundenanzahl für die Bearbeitung des fünften Arbeitsblattes ist für etwa zwei Unterrichtseinheiten angesetzt. Sie lässt sich jedoch passend zum Lernstand der Lerngruppe auch ausdehnen oder kürzen.

Der Einstieg erfolgt durch das Vorführen von Adblockern im Browser des Lehrer-Computers. Schüler sollen im Unterrichtsgespräch die Unterschiede zwischen einer Situation mit und einer ohne Adblocker beschreiben. Die Aufgabe der Lehrperson ist es, im Unterrichtsgespräch die Vorteile sowie Nachteile von Werbeblockern herauszustellen. Alternativ kann statt den Webseiten auch ein kurzes YouTube-Video gezeigt werden, welches Werbung einspielt. Die Ergebnisse werden zunächst nicht schriftlich festgehalten, sondern sollen als Anreiz für die Bearbeitung des Arbeitsblattes Nr. 5 dienen.

In der üblichen Partnerarbeit bearbeiten die Schüler anschließend die Aufgaben 1-3. Dabei installieren die Schüler den genannten Adblocker im Browser und testen diesen aus. Vorher genannte Unterschiede, Vorteile und Nachteile werden in der Bearbeitung dieser Aufgaben

wieder aufgegriffen und verschriftlicht. Alternativ können die Schüler hier die portable Version des Browsers nutzen. Dadurch wird auf dem Schulrechner installierte Software nicht verändert oder sogar beschädigt. Eine Vorführung des Installationsprozesses oder eine Vorabinstallierung durch die Lehrperson ist hier für schwächere Lerngruppen denkbar.

Im zweiten Teil der Unterrichtseinheit soll das über den Adblocker erlangte Wissen auf andere Plug-Ins erweitert werden. Dazu beschreibt die Zusatzaufgabe das Erstellen eines Steckbriefes über diverse Datenschutz-Plug-Ins. Der Austausch der Informationen soll nach der in Gruppenarbeit bearbeiteten Aufgabe nach dem Jigsaw-Verfahren[45] stattfinden. Die Gruppen werden neu gemischt. Dabei befindet sich in jeder der neuen Gruppen ein Mitglied aus jeder der alten Gruppen. Diese *Expertenrunde* erläutert sich nun untereinander die wichtigsten Fakten über die anderen Programme. Anschließend werden die Fakten im Unterrichtsgespräch gemeinsam festgehalten.

Nummerierung	**Unterrichtsteil**	**Inhalt**	**Dauer [min]**	**Sozialform / Medium**
1	Im Lernkontext ankommen	- Vorführung des Adblockers durch die Lehrperson - anschließende Diskussion über Vor- und Nachteile	15	LV, UG / Lehrer-PC
2	Lernprodukt erstellen	- Bearbeitung der Aufgaben 1-3	20-25	PA / Computer, AB

[45] Dies wird auch Experten-Puzzle genannt.

3	Lernprodukt diskutieren	- Besprechung des AB	5	UG / AB
4	Sichern und vernetzen + Transferieren und festigen	- Anlegen von Steckbriefen weiterer Plug-Ins - Installation und Nutzen von Plug-Ins	45-90	Jigsaw-Methode

***Tabelle 10**: Kurzentwurf UE 7-8*

Um das Jigsaw-Verfahren zu vervollständigen, findet im Anschluss eine Diskussion statt, was im Verfahren gut und was schlecht gelaufen ist. So kann die Jigsaw-Methode beim erneuten Ausüben effizienter durchgeführt werden.

4.8 Exkurs: Datenbanken in Instahub

Didaktische Analyse:

Die zu erreichenden Teillernziele der Unterrichtsreihe für diese Stunde:

- Schüler modellieren Datenbanken in einem ERM-ähnlichen Modell.
- Schüler lesen Daten aus einer Datenbanktabelle aus.
- Schüler nutzen Selektion zum Auslesen der Tabellen.
- Schüler löschen, verändern und fügen Daten in Tabellen ein.

Dieser Abschnitt der Unterrichtsreihe beschäftigt sich mit dem Exkurs zu Datenbankennutzung und -modellierung. Passend zur Unterrichtseinheit sind die Arbeitsblätter 6-9 (siehe Anhang 9-12) hinzuzuziehen.

Der Exkurs ist ein Einschub zum Thema Datenschutz, um die Kernelemente von *Instahub* in der Reihe einzufügen. Es ist aufgeteilt in die Modellierung und Nutzung der Datenbanken. Die Schwierigkeiten in diesem Teil der Unterrichtsreihe sind fehlendes Vorstellungsvermögen für die Struktur der Datenbanken und fehlendes Abstraktionsvermögen für das Modellieren der

Datenbanken. Um Letzteres zu umgehen werden genug einfache Beispiele angeführt und die Modellierung selbst auf seine Grundlagen reduziert.

Methodische Konzeption:

Die Arbeitsblätter 6-9 sind so konzipiert, dass sie auch unabhängig von den restlichen Arbeitsblättern als Unterrichtsreihe durchgeführt werden können.

Im ersten Abschnitt wird das Modellieren von Datenbanken behandelt. Dazu sollen die Schüler auf dem Arbeitsblatt Nr. 6 die entsprechenden Aufgaben bearbeiten. Die ersten zwei Aufgaben sind so konzipiert, dass die Schüler zunächst einen Einblick in das Modell gewinnen und anschließend erweitern. Eine Sicherungsphase nach diesem Unterrichtsteil sorgt dafür, dass die Grundkonzepte des Modells (Objekte, Beziehungen, Eigenschaften) von den Schülern verinnerlicht werden. Alternativ können hier noch weitere Aufgabenstellungen im gleichen Stil folgen, sodass der Ablauf der Modellierung jedem klar wird. Abschließend zur Modellierung wird ein entsprechendes Modell für *Instahub* angefertigt. Im Unterrichtsgespräch wird dann eine Musterlösung angefertigt, die jeder Schüler in seine Unterlagen überträgt.

Diese Lösung dient als Einstieg in die kommenden Unterrichtseinheiten. Alternativ kann auch die Tabelle von Arbeitsblatt 7 als Einstiegsmittel dienen. Anhand von einem der beiden wird den Schülern durch einen Lehrervortrag das Konzept der Datenbanktabellen erläutert. Mit Hilfe der Arbeitsblätter Nr. 7-9 können die Schüler selbstständig in ihrem eigenen Hub arbeiten. Dabei führen sie Übungen zum Löschen, Verändern, Einfügen und Auslesen durch, ohne dabei die SQL-Sprache beherrschen zu müssen. Dies soll einen Einblick auf die Funktionsweise eines Datenbanksystems geben.

Die Aufgaben werden als Lerntagebuch dokumentiert (siehe Anhang 13). Dazu füllen die Schüler selbstständig den Bogen zur Datenbanknutzung und -modellierung aus. Dies soll der Lehrperson einen Überblick über die aktuellen Lernstände der Schüler geben. Zusätzliche Übungsaufgaben und Lerneinheiten können so individuell eingefügt werden.

Nummerierung	**Unterrichtsteil**	**Inhalt**	**Dauer [min]**	**Sozialform / Medium**
1	Im Lernkontext ankommen	- Beispielmodell: Pizzeria - Aufgaben 1-2 (Blatt 6)	20-25	PA / AB
2		- Schaffen einer gemeinsamen Lernbasis - evtl. Zusatzaufgaben	10-45	UG / Tafel, Folie
3	Lernprodukt erstellen	- Bearbeitung der Aufgabe 3 - Modell zu Instahub	20-25	PA / AB
3	Lernprodukt diskutieren	- Besprechung des Instahub-Modells - Anfertigung einer Musterlösung	20	UG / Tafel, Folie
4	/	- Nutzen der Datenbanken - Löschen, Verändern, Einfügen, Auslesen	45-135	Lerntagebuch

***Tabelle 11**: Kurzentwurf Exkurs*

5. Weiterentwicklung der Unterrichtsreihe

Der letzte Teil der Arbeit beschäftigt sich mit der möglichen Fortführung der entwickelten Unterrichtsreihe. Er beinhaltet eine Durchführung eines Teils der Reihe mit anschließender Evaluation. Weiterhin werden Aspekte zur Implementierung genannt und mögliche Weiterentwicklungsmaßnahmen entwickelt.

5.1 Durchführung und Evaluation der Reihe

Ziel der Reihe ist es, Grundlagen von Datenschutzkompetenz im Unterricht der Orientierungsstufe zu thematisieren. Aufgrund des niedrigen Alters der Zielgruppe wird nicht erwartet, dass die Schüler im Laufe der Reihe Datenschutzkompetenz im ausreichenden Maße, wie von Hug und Grimm verlangt, erreichen. Zusätzlich wird davon ausgegangen, dass die Schüler vor der Unterrichtsreihe wenig bis keine Vorkenntnisse im Bereich Datenschutz einbringen. Um die entwickelte Reihe zu evaluieren, wurden zwei Unterrichtseinheiten der Reihe in zwei ähnlichen Gruppen durchgeführt.

Die zwei ausgewählten Lerngruppen stammen aus der Klassenstufe 5 einer rheinland-pfälzischen Orientierungsstufe (Sekundarstufe I) eines allgemeinbildenden Gymnasiums. Diese Durchführung fand am 30.01.2019 statt. Jede Klasse bestand aus mehr als 25 Schülern (26 und 30) und wurde im Fach ITG[46] unterrichtet, in welchem ein Teil der Reihe stattfand. Es wurde je die Unterrichtseinheit 1 und 2 in Form einer Doppelstunde durchgeführt. Aufgrund der nicht vollständigen Durchführung der kompletten Reihe und dem begrenzten Zeitraum konnte keine Feststellung der Kompetenzen nach dem Datenschutzmodell ausgeführt werden. Aus den festgestellten Aspekten sollen am Ende dieses Abschnitts Korrektur- und Weiterentwicklungsmaßnahmen herausgearbeitet werden.

5.2.1 Lerngruppe 1

Die erste Lerngruppe bestand aus 26 Schülern. Die Anzahl der männlichen und weiblichen Schüler war relativ ausgeglichen (11 Jungen, 15 Mädchen). Es wurden die Aufgabenblätter 1

[46] Informationstechnische Grundbildung

und 2 bearbeitet und die Unterrichtseinheit vollständig durchgeführt. Diese Schülergruppe wurde durch die unterrichtenden Lehrkräfte als die stärkere der beiden bezeichnet.

Es ist positiv anzumerken, dass die Schüleraktivierung sehr hoch war. Die Plattform *Instahub* bereitete den Schülern keinerlei Probleme und wurde schnell angenommen. Die Aufgaben wurden in der geplanten Zeit bearbeitet. Die Diskussion im zweiten Teil der Stunde war unerwartet umfangreich und detailliert. Die Begründungen aus der letzten Aufgabe wurden sehr gründlich bearbeitet und vorgetragen.

Die Aufgabenstellung schien anfangs verwirrend zu sein. Durch die teilweise langen Aufgabenstellungen wurden Teile von den Schülern überlesen oder ignoriert. Außerdem war die Tatsache, dass die Schüler etwas verschriftlichen sollten, nicht Teil des gewohnten Unterrichtsverlaufs. Erst nach mehrmaligem Hinweisen durch die Lehrperson wurden Notizen und Antworten handschriftlich aufgeschrieben. Die Ergebnisse aus dem zweiten Teil der ersten Lerngruppe waren umfangreich und zielführend. Es konnte das Unterrichtsziel (Das Bewerten der Profile durch die Schüler) vollständig erreicht und besprochen bzw. diskutiert werden (vgl. Anhang 14).

Zusammenfassend ist zu sagen, dass das Thema sehr gut von den Schülern angenommen wurde und vermeintliche Einstiegsschwierigkeiten, durch fehlende Vorkenntnisse im Bereich des Datenschutzes, ausblieben. Dennoch wurde klar, dass besonders die Aufgabenstellungen aufgrund ihrer Formulierung ein Hindernis darstellten. Da für die Lehrperson zwischen den Stunden genügend Zeit vorhanden war, wurden für die zweite Lerngruppe bereits kleine Änderungen in der Unterrichtsplanung vorgenommen: Die Aufgabenstellungen sollten mit mehr Hilfestellung ausgeteilt werden. Dazu können Beispielabläufe, z.B. wie man den Hub aufruft und welche Seiten man nutzen soll, vor dem Beginn der Arbeitsphase erläutert werden. Weiterhin wurde für die Schüler der zweiten Lerngruppe ein kurzes Informationsblatt in Form einer Word-Datei angefertigt, welches die englischen Begriffe aus *Instahub* ins Deutsche übersetzt.

5.2.1 Lerngruppe 2

Die Lerngruppe 2 bestand zum Zeitpunkt der Durchführung aus 30 Schülern. Davon 18 Jungen und 12 Mädchen. Auch hier kann die Gruppe als relativ ausgeglichen bezeichnet werden. Zusätzlich wurde diese Lerngruppe von den Lehrpersonen, welche diese in ITG unterrichten, als die deutlich schwächere bezeichnet. Es wurden die Aufgabenblätter 1 und 2 bearbeitet. Die Besprechung der Aufgabe 2 auf dem zweiten Blatt (Bewertung der Profile anhand der Tabelle) konnte leider nur mündlich durchgeführt werden, da die Zeit für eine Visualisierung am Overheadprojektor nicht ausreichte (vgl. Anhang 15).

In der zweiten Lerngruppe konnten die Fehler aus der Ersten fast gänzlich vermieden werden. Die Schüler wussten schon nach wenigen Schritten, was zu tun war. Sie arbeiteten zunächst gewissenhaft an den Aufgaben. Es wurden die gleichen positiven wie negativen Aspekte aus der ersten Stunde festgestellt. Weiterhin fiel auf, dass die Schüler schnell durch die spielerische Seite von *Instahub* abgelenkt wurden. Durch Eingreifen der Lehrperson konnte dies nicht gänzlich verhindert, jedoch reduziert werden.

Durch etwaige Ablenkungen und das geringe Arbeitstempo der Gruppe konnte das Ziel, nämlich die Visualisierung der Ergebnisse am Projektor, nicht ganz erreicht werden. Sie wurde nur mündlich besprochen, um zu überprüfen, ob die Aufgaben vollständig und richtig bearbeitet wurden. Dennoch ist zu sagen, dass das Interesse und die Qualität der Beiträge in der vorherigen Diskussion, ähnlich wie in der ersten Lerngruppe, hoch waren.

5.2 Implementierung

Der Hauptteil der Implementierung beläuft sich auf den letzten Teil der Unterrichtsreihe. Die Nutzung der Datenbankentabellen ist derzeit nur über eine Konsolenzeile möglich, die SQL-Code interpretiert. Im Laufe der Arbeit wurde ein Konzept entwickelt, dies für Schüler der Orientierungsstufe anzupassen. Zusätzlich umfasst die Implementierung den Zugang zu den im Anhang angeführten Unterrichtsmaterialien.

Derzeit besteht eine Offlineversion der besagten Implementierung. Es ist bisher noch nicht gelungen, diese über lizenzfreie Software umzusetzen und online zur Verfügung zu stellen. Der Zugriff auf das Datenbanksystem findet durch die entwickelte Oberfläche über ein

Dropdown-Menü statt. Schüler können darüber künftig Operationen ohne Kenntnis über den eigentlichen SQL-Befehl ausführen. Die Umsetzung umfasst das Auslesen, Verändern, Löschen und Einfügen von Tabelleneinträgen in *Instahub*.

5.3 Weiterentwicklungsmaßnahmen

Aus den Unterrichtseinheiten der beiden Lerngruppen lassen sich direkt Weiterentwicklungsmaßnahmen für die Unterrichtsreihe ableiten. Zuerst sollten die Aufgabenstellungen vereinfacht und, bei Bedarf, mit Symbolen sowie Screenshots verdeutlicht werden. Dies wurde teilweise auf den Aufgabenblättern bereits umgesetzt (vgl. Anhang 2, Aufgabe 1). Weiterhin mussten die Diskussionen sehr durch die Lehrperson angeregt werden, um die Schüler zu aktivieren und sie in die korrekte „Richtung“ zu leiten. Hierzu wurde das Profil von *David Schmitz* angepasst. Die Profilbeschreibung ist nun etwas provokativer formuliert, sodass Schüler diesen Aspekt leichter erkennen und in die Diskussion einbringen.

Weiterhin sollen ein paar Ideen zur Weiterführung des Projekts genannt werden. Die Erweiterbarkeit ist durch die genutzte Oberfläche (*Instahub*) umsetzbar und gewollt. Dadurch lässt sich die Unterrichtsreihe sowohl inhaltlich als auch visuell ausbauen.

Inhaltlich ist es denkbar, den Themenbereich **Schadsoftware** auszubauen. Das Wissen um Schadsoftwarearten und Schutzmaßnahmen nehmen eine wichtige Rolle im Datenschutz ein. Besonders hinsichtlich des alltäglichen Umgangs mit dem Internet seitens der Schüler ist es von großer Bedeutung für datenschutzangelehnten Unterricht. Der Bereich wird mittels einer Projektarbeit innerhalb der Unterrichtsreihe eingebracht, lässt sich jedoch noch deutlich ausbauen. Ebenso lässt sich der vorhandene Inhalt verbessern. Eine mögliche Idee ist das Einbringen von **Lernvideos**. Diese könnten beispielsweise den Installationsvorgang von Browser-Plug-Ins oder die Nutzung der Datenbank erläutern. So kann der Unterrichtsschwerpunkt mehr auf das Erwerben der Kompetenzen im Datenschutz verlegt werden. Eine Umwandlung der Reihe mit Hilfe der *Flipped-Classroom-Methode* ist ebenfalls denkbar. Das Einbinden der Videos auf der Plattform stellt kein Hindernis dar.

Ein weiterer Punkt zur Weiterentwicklung ist die visuelle Aufwertung der Arbeitsblätter. Da die Zielgruppe der Unterrichtsreihe sehr jung ist, könnte hier durch farbliche Gestaltung und Einbringen von Symbolen und dergleichen die Qualität der Arbeitsblätter selbst deutlich gesteigert werden. Hierdurch wäre eventuell auch die Motivation der Lerngruppen höher oder zielgerichteter. Weiterhin könnten die Hilfestellungen auf den Arbeitsblättern als optionale Karteikarten verwendet werden. Dadurch ließe sich eine übersichtlichere Binnendifferenzierung im Unterrichtsverlauf herstellen.

6. Zusammenfassung

Diese Arbeit dient als Weiterentwicklung des Projekts *Instahub*. Mit Hilfe von aktuellen Datenschutzaspekten und des Datenschutzkompetenzmodells konnte eine Unterrichtsreihe für die Klassenstufe 5-6 erstellt werden, welche sowohl den Datenschutz in einem Sozialen Netzwerk als auch Sicherheitsmaßnahmen im Umgang mit dem Internet sowie Auswirkungen auf den Selbstdatenschutz behandelt. Durch die bereits bestehende Implementierung von *Instahub* gelang es, die Reihe für junge Schüler geeignet und kontextorientiert zu verwirklichen. Die Schüler werden in ihrem Alltag abgeholt und entwickeln im Laufe der Unterrichtseinheiten ein Gefühl für die Bedeutung von Datenschutz. Weiterhin enthält die Reihe einen Einblick in die Nutzung und das Modellieren von Datenbanken, um so einen umfangreicheren Blick in den Bereich der Informatik zu geben. Die Durchführung in zwei ähnlichen Lerngruppen zeigte deutlich, dass die Motivation der Schüler durch den Kontext Sozialer Netzwerke besonders hoch war. Durch die geringe Stundenanzahl der Durchführung konnten nur die Einstiegsthemen behandelt werden. Um zu zeigen, dass die Motivation auch über einen längeren Zeitraum erhalten bleibt und auch der von *Instahub* losgelöste Teil der Internetsicherheit Anklang bei den Schülern findet, benötigt es einer umfassenderen Durchführung und Messung der Lernergebnisse nach der Unterrichtsreihe. Letzteres wäre ein Ansatzpunkt für eine Fortführung der Reihe in höheren Klassenstufen. Es wurde im Laufe der Arbeit klar, dass durch kleine Änderungen des Inhalts, auch diese Reihe für eine ältere Lerngruppe geeignet ist (z.B. durch Einführung von weiteren Fachbegriffen und Weglassen von Hilfestellungen).

Derzeit sind die Unterrichtsmaterialien nicht über *Instahub* erreichbar, sondern nur über diese Arbeit (Stand: April 2019). Im Anschluss an diese Arbeit wird an einer zugänglichen Lösung für den Bereich Datenbanken gearbeitet. Zusätzlich zur Einarbeitung der Reihe in das Projekt, sind Weiterentwicklungsmöglichkeiten der Materialien und Inhalte möglich, da der Betreiber von *Instahub* den verwendeten Quellcode frei zur Verfügung stellt.

7. Anhang

* bekannt das ein Mindestalter existiert aber nicht welches
4/17 sagen Instagram ab 13, laut Appbeschreibung
1 nutzt App seit 1-2 Jahren (vor DSGVO)

Umfrage – Soziale Medien in der Orientierungsstufe

Umfragenstil: Handzeichen zu gegebenen Fragen, anonym

Klassenstufe (Datum)	Anzahl d. SuS d. Soziale Medien [1] nutzen	Anzahl d. SuS die keine Sozialen Medien nutzen	Mindestalter [2] bekannt?
reine Mädchenklasse: 7 (11.02.19)	23	0	17*
6 (13.02.19)	24	2	12
6 (13.02.19)	17	8	10
7 (20.02.19)	21	1	6
5 (20.03.19)	10	17	3
Insgesamt	95 (~ 77%)	28 (~ 23%)	48 (~ 40%)

Durchgeführt von Christoph Noll (i.A. von Jan Savelsberg) an einem rheinland-pfälzischen Gymnasium.

[1] z.B. Facebook, Twitter, Twitch, Youtube, Snapchat, Instagram
[2] 16 (nach DSGVO, Art. 7-8)

ANHANG 2: ARBEITSBLATT NR. 1

Datenschutz mit InstaHub

Der Einstieg

Name: _____

Blatt Nr. 1 Datum: _____

Aufgabe 1

Ruft die Seite aller Mitglieder eures Hubs auf, indem ihr oben in der Leiste auf *Members* klickt.

Aufgabe 2:

Findet nun in der Liste die Profile von *Jen Körtig, So Dingenskirchen* und *David Schmitz.* Folgt den drei genannten Personen, indem ihr auf den grünen Button Follow klickt.

Das könnte hilfreich sein:
Die Namen sind alphabetisch sortiert und ihr könnt in der Leiste oben den Anfangsbuchstaben auswählen.

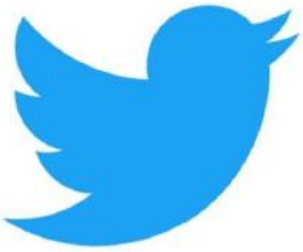
Aufgabe 3:

Schreibt handschriftlich eine Liste mit allen Informationen, die ihr über die drei Personen findet (also z.B. Name, Alter, Hobbies ...).

Jen Körtig	So Dingenskirchen	David Schmitz

Das könnte hilfreich sein:
Auf der Startseite findet ihr einen Überblick der letzten Beiträge. Wenn ihr auf die Namen klickt, gelangt ihr auf das Profil der jeweiligen Person.

ANHANG 3: EINSTIEGSFOLIE UE 1



Datenschutz mit InstaHub

Einführung

Lehrperson

Zunächst muss für den ersten Teil der Unterrichtsreihe ein Hub erstellt werden, auf welches alle Schüler zugreifen können.
Als nächstes muss der veröffentlichte Hub über die nötigen Profiländerungen verfügen. Dazu müssen folgende Änderungen an der Datenbank vorgenommen werden:

- Die Profilbeschreibung von *Jen Körtig* wird geändert in: *„Ich treffe mich gern mit Freunden und verbringe viel Zeit mit Onlinegames. Fragt mich einfach, wenn ihr was wissen wollt.“*

- Die Profilbeschreibung von *David Schmitz* wird geändert in: *„Habt ihr mitbekommen, was für einen Scheiss unser Mathelehrer abzieht?! Ne echte Witzfigur!“*

- Das Alter von *David Schmitz* wird geändert auf: *14*

- Der Name von *Sophia Sänger* wird geändert in *So Dingenskirchen*

- Das Alter von *Sophia Sänger* wird geändert in: *97*

- Der Wohnort von *Sophia Sänger* wird geändert in *Entenhausen*

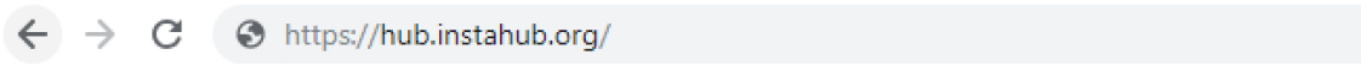
- Die Profilbeschreibung von *Sophia Sänger* wird geändert in: *„In meiner Freizeit lese ich gerne Bücher und gehe mit meinem Hund Rasko spazieren. Dabei mache ich gerne Naturaufnahmen mit meiner Kamera.“*

Weiterhin benötigt jeder Schüler bzw. jedes Schülerteam einen Zugang zu ihrem Hub. Die Anmeldung findet über den Link *hub.instahub.org* statt, wobei *hub* durch den zufällig generierten Namen Ihres Hubs ersetzt werden muss.

Nachdem jeder Schüler / jedes Schülerteam sich angemeldet hat, müssen die Schüleraccounts händisch aktiviert werden.
Gehen Sie dazu auf *...instahub.org/user/username* und aktivieren Sie den jeweiligen Account (*username* durch den gewählten Namen des Schülers / Schülerteams ersetzen).

Schüleraufgabe

1. Gebt den Link, den ihr von eurem Lehrer/eurer Lehrerin erhaltet, in die Adresszeile eures Internetbrowsers ein und bestätigt die Eingabe.



Achtung! „Hub" aus dem Beispielbild muss durch den Hub eurer Klasse ersetzt werden.

2. Benutzt die blaue Schaltfläche Sign Up, um euch im InstaHub zu registrieren. Wählt einen Benutzernamen, der nicht eurem richtigen Namen entspricht. Das Passwort sollte leicht zu merken sein. Schreibt es am besten auf.

3. Gebt eurem Lehrer / eurer Lehrerin den gewählten Benutzernamen, damit der Account aktiviert werden kann.

4. Loggt euch mit dem gewählten Benutzernamen und Passwort über die weiße Schaltfläche Sign In ein.

ANHANG 5: ARBEITSBLATT NR. 2

Datenschutz mit InstaHub

Das „sichere“ Profil

Name: _____

Blatt Nr. 2 Datum: _____

Aufgabe 1:

Die Argumente in den Kästchen beschreiben Kriterien für ein sicheres Profil auf einer Plattform wie Instahub. Findet heraus, welche Argumente für ein sicheres und unsicheres Profil zutreffen und **verbindet sie** passend.

Pseudonym verwenden

Persönliche Daten, wie Geburtsdatum und Schulort angeben

sicheres Passwort verwenden

Aktuellen Standort posten

Kein Profilbild hochladen

Nur meine engsten Freunde können meine Beiträge sehen

Partybilder hochladen

Immer das gleiche Passwort verwenden

Immer ausloggen

Log-In Daten im Browser speichern

sicheres Profil	unsicheres Profil

Aufgabe 2:

Haben Jen, Sophia und David die Punkte eingehalten oder ist ihr Profil noch verbesserungswürdig? Bewertet die Profile mit *„sicher“* oder *„nicht sicher“*. **Notiert** die fehlenden Punkte.

Beispiel:
Das Profil von Sebastian Beuchel ist nicht sicher genug. Er hat für jeden sichtbar ein Foto in Badehose hochgeladen.

Datenschutz mit InstaHub

Ist mein Passwort sicher genug?

Name: _____

Blatt Nr. 3 Datum: _____

*Hinter den Account-Daten eures Profils verstecken sich all eure persönlichen Daten. Sollte jemand Zugriff auf euren Benutzernamen und Passwort haben, hat er damit auch Zugriff auf diese schützenswerten Informationen. Deshalb ist es besonders wichtig, euren Account so gut es geht durch ein starkes Passwort zu schützen. Doch was ist ein **starkes** Passwort?*

Aufgabe 1:

Überlegt euch in Gruppen (max. 3 Personen), was ein starkes Passwort eurer Meinung nach ausmacht.
Notiert mind. 3 Faktoren:

_____

_____

_____

_____

Aufgabe 2:

Erstellt ein neues Passwort mit den Faktoren, die ihr in Aufgabe 1 notiert habt:
_____ (gebt kein Passwort an, das ihr bereits benutzt!).

Unter dem folgenden Link https://checkdeinpasswort.de/ könnt ihr euch angeben lassen, wie sicher euer Passwort ist und wie lange ein herkömmlicher Computer braucht, um es zu berechnen.

Testet den *Passwortchecker* mit mehreren Passwörtern aus. Wie sicher ist euer Passwort? Was kann an eurem geändert werden, damit es sicherer wird?
Notiert weitere Möglichkeiten:

_____

_____

Aufgabe 3:

*Eine weitere Möglichkeit, ein Passwort zu generieren, ist ein Hilfssatz, den ihr euch leicht merken könnt. Ein Beispiel wäre: „**M**ein **L**ieblingslied **i**st **S**mooth **C**riminal **v**on **A**lien **A**nt **F**arm **a**us **d**em **J**ahr 2**001**“. Nimmt man nun die Anfangsbuchstaben aus jedem Wort bzw. Ziffer und kombiniert es mit Sonderzeichen, entsteht das Passwort: **MLiSCvAAFadJ_001***

Testet das Beispielpasswort mit dem *Passwortchecker.*
Überlegt euch einen Satz wie im obigen Beispiel und erstellt damit ein Passwort.

_____

_____

_____

Das könnte hilfreich sein:
Das BSI hat für das Erstellen von Passwörtern eine Liste mit Faktoren veröffentlicht. Vergleicht eure Kriterien mit denen unter folgender Adresse:
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html

Zusatzaufgabe: Vorträge

Schreibt eine Zusammenfassung und haltet einen kurzen Vortrag (5-10 Minuten) über die Begriffe *Malware*, *Trojaner, Computerviren* oder *Hijacking*. Mögliche Fragen, die ihr euch in Gruppen dazu stellen könnt, sind z.B.:

- Was bedeutet der Begriff und wo kommt er vor?
- Wie wirkt sich das auf die Sicherheit meiner Account-Daten aus?
- Wie kann ich mich dagegen schützen?

Erstellt ein gemeinsames Plakat mit den wichtigsten Begriffen und Informationen und hängt es in eurem Klassenraum / Computerraum auf.

ANHANG 7: ARBEITSBLATT NR. 4

Datenschutz mit InstaHub

Nutzungsbedingungen und Co.

Name: _____

Blatt Nr. 4 Datum: _____

Sobald ihr einen Account in Sozialen Netzwerken erstellt, werdet ihr gefragt, ob ihr den Nutzungsbedingungen und Datenschutzrichtlinien zustimmt. Wenn euch eure Eltern die Erlaubnis geben oder ihr bereits 16 Jahre alt seid, dürft ihr eure Einwilligung geben. Mit dieser Einwilligung gebt ihr Facebook, Instagram und Co. viele Freiheiten, die eure persönlichen Daten betreffen.

Aufgabe 1

Ruft die Seite eures Sozialen Netzwerks auf und sucht nach den Nutzungsbedingungen. Falls ihr kein solches Netzwerk benutzen solltet, nutzt hierzu www.facebook.de.
Notiert in Stichworten, welchen Bedingungen (mind. 3) ihr zugestimmt habt und welche Informationen das Netzwerk von euch erhält:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Das könnte hilfreich sein:
Unter den Suchbegriffen Datenschutzrichtlinie, Allgemeine Geschäftsbedingungen und Privatsphäre-Einstellungen findest du noch mehr Informationen.

Aufgabe 2:

Loggt euch auf einem eurer Profile ein und beschreibt kurz die Einstellungsmöglichkeiten für eure Privatsphäre.

_____

_____

_____

_____

Wenn ihr in verschiedenen Netzwerken angemeldet seid, notiert die Unterschiede in den Einstellungsmöglichkeiten:

_____

_____

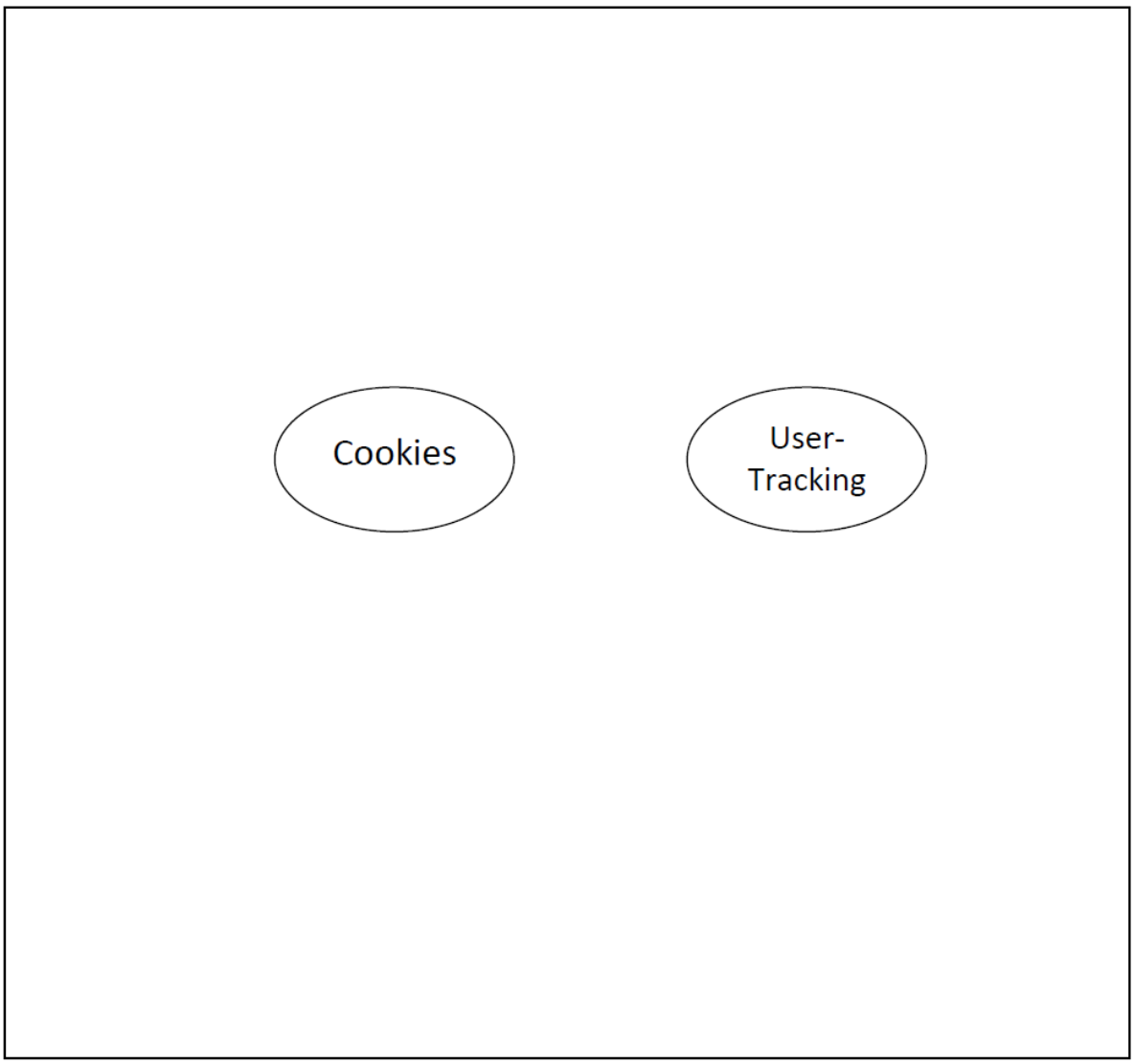
_____

_____

_____

Grundsätzlich sind die angebotenen Dienste von Facebook, Instagram und Co. kostenfrei. Das liegt daran, dass sie mit den von euch bereitgestellten Daten Geld verdienen. Jedes Mal, wenn ihr euch einloggt, sammelt ein Netzwerk wie Facebook Daten über euch: Den aktuellen Standort, eure Vorlieben, was ihr zuletzt unternommen habt, welche Seiten ihr liked oder mit welchen Personen ihr befreundet seid. Diese Informationen, werden dazu genutzt, um auf euch zugeschnittene Werbung zu schalten.
Ihr seht nur das, was Facebook für euch als interessant ansieht. Dafür zahlen Unternehmen, deren Werbung ihr seht, viel Geld. Die Einnahmen von Facebook befinden sich derzeit jährlich im einstelligen Milliardenbereich.

Aufgabe 3:
Um eure Daten auswerten zu können, muss ein Netzwerk diese zuerst einmal sammeln. Diese werden meist durch sogenannte **Cookies** erfasst.
Stellt mit Hilfe einer geeigneten Suchmaschine Nachforschungen über die Begriffe *Cookie* und *User-Tracking* an.
Fasst eure Ergebnisse in einer Mindmap zusammen:



Datenschutz mit InstaHub

Sicher im Netz unterwegs

Name: _____

Blatt Nr. 5 Datum: _____

*Achtung! Auf dem folgenden Arbeitsblatt werden Übungen zu Browsererweiterungen bzw. Plug-Ins behandelt. Dazu verwenden wir den Browser **Chrome** von Google. Es kann natürlich auch jeder andere Browser verwendet werden. Genutzte Plug-Ins sind jedoch eventuell nicht für alle Browser verfügbar. Sollte Chrome nicht auf dem genutzten Computer verfügbar sein, könnt ihr **Google Chrome Portable** auch von einem USB-Stick oder einer CD/DVD starten, ohne diesen vorher installieren zu müssen.*

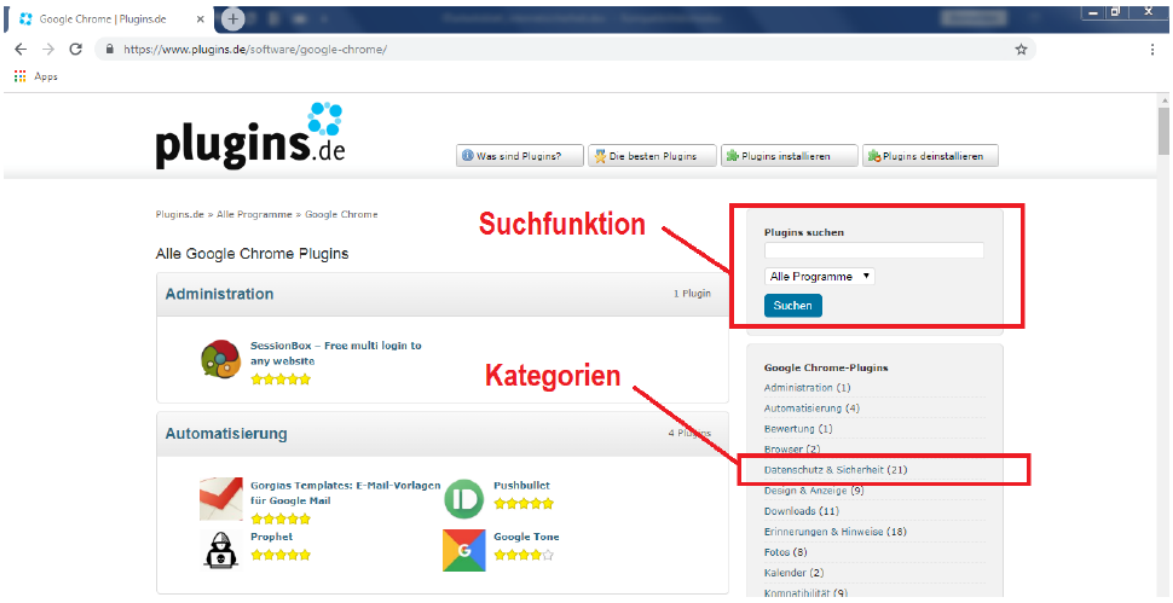
Bei der Nutzung von InstaHub ist euch sicherlich schon aufgefallen, dass auch InstaHub Werbung anzeigt. Geht dazu auf die Startseite eures Hubs. Zwischen den aktuellen Beiträgen eurer Freunde findet ihr immer wieder Werbung. Andere Anbieter sammeln jetzt Daten, um diese Werbung perfekt auf euch zuzuschneiden. Aber ist euch „gute" Werbung mehr Wert, als eure Daten?

Aufgabe 1

PLUG-INS

Plug-Ins sind Programme, die sich in deinem Browser als Zusatzfunktion integrieren lassen.

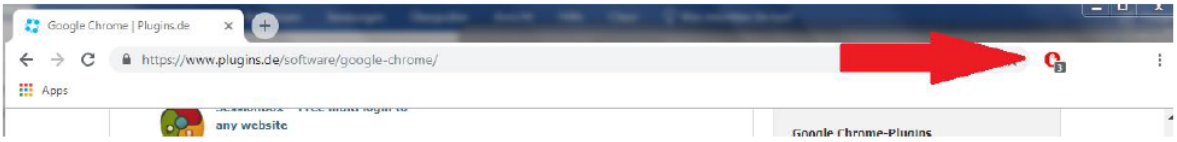
Öffnet den Internetbrowser *Chrome* und ruft die Seite *www.plugins.de/software/google-chrome/* auf. Sucht nach dem Plug-In *AdBlock Plus* für Google Chrome. Dazu könnt ihr entweder die Suchfunktion der Seite oder die Kategorie *Datenschutz & Sicherheit* benutzen.



Aufgabe 2:

Installiert *AdBlock Plus* für euren Browser, indem ihr der Anleitung Schritt für Schritt folgt. Falls ihr unsicher seid, lasst euch von eurem Lehrer / eurer Lehrerin helfen.

Wenn ihr alle Schritte der Installation befolgt habt, sollte ein Symbol oben rechts in eurem Browser zu finden sein:



Aufgabe 3
Ruft nun erneut euren Hub auf.
Notiert die Unterschiede:

_____
_____
_____
_____

Das könnte hilfreich sein:
Ihr könnt die Funktion des Plug-Ins für die aktuelle Seite ausschalten. Rechtsklickt dazu auf das Symbol und wählt die Option: „auf dieser Seite pausieren". Mit „Werbung wieder blockieren" kannst du sie wieder einschalten.

Zusatzaufgabe:
Setzt euch in Gruppen (3-5 Personen) zusammen. Informiert euch zusammen über eines der folgenden Plug-Ins:

LastPass, TrafficLight, PanicButton, Vanilla Cookie Manager,
WOT: Web of Trust, Proxy SwitchyOmega

Legt dazu einen Steckbrief mit allen wichtigen Informationen an. Dieser könnte zum Beispiel so aussehen:

Plug-In Name: _____
Funktionen: _____
_____
_____
_____
Vorteile: _____
_____
_____
_____
Nachteile: _____
_____
_____

Mischt die Gruppen und tauscht euch über die verschiedenen Plug-Ins aus.
Notiert, welche Plug-Ins ihr verwenden würdet. Begründet eure Entscheidung.

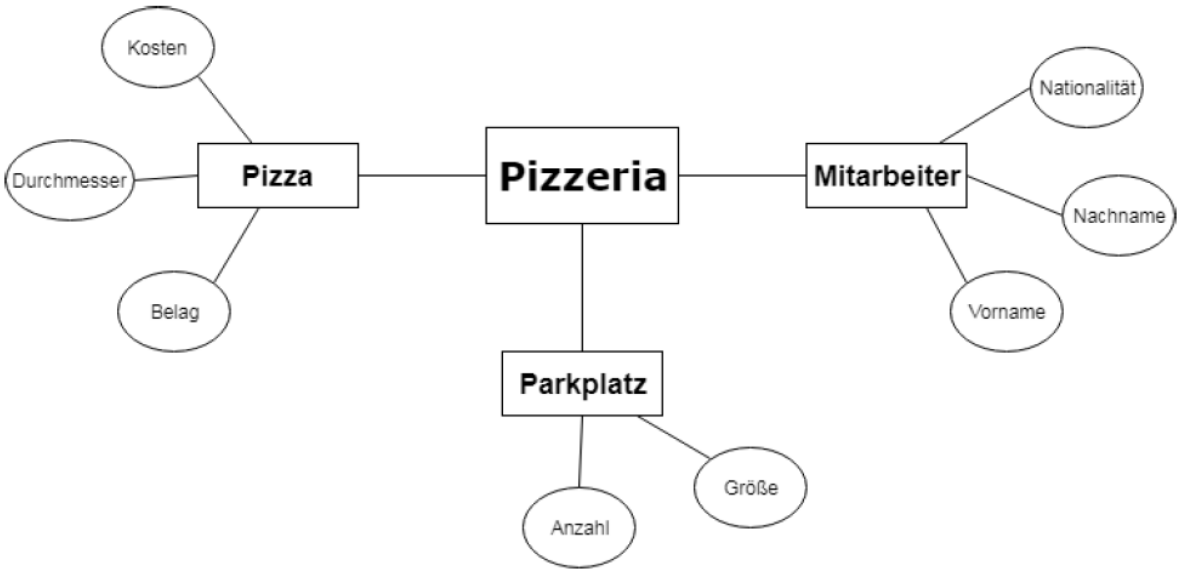
Datenschutz mit InstaHub

Modellieren von Datenbanken

Name: _____

Blatt Nr. 6 Datum: _____

Damit jeder versteht, wie eine Software Daten speichert, werden sogenannte Modelle erstellt. Sie zeigen vereinfacht wo welche Informationen liegen. Ein Beispiel dafür ist dieses Modell einer Pizzeria:



Das könnte hilfreich sein:
RECHTECK: Beschreibt ein Objekt, z.B. einen Gegenstand, eine Person ...
KREIS: Beschreibt eine Eigenschaft eines Objekts, z.B. Farbe, Größe, Alter ...
VERBINDUNG: Beschreibt eine Beziehung zwischen Objekt – Eigenschaft oder Objekt – Objekt.

Aufgabe 1

Übertragt das Modell aus dem Beispiel in euer Heft.
Fügt folgende Dinge hinzu:

Ofen (Objekt),
Temperatur (Eigenschaft von Ofen),
Farbe (Eigenschaft von Ofen),
Anzahl Motorrad-Parkplätze (Eigenschaft von Parkplatz)

Aufgabe 2

Fügt noch **mindestens 3** weitere Objekte oder Eigenschaften hinzu.

Aufgabe 3

Erstellt ein Modell für InstaHub.

Das könnte hilfreich sein:
Mögliche Objekte für Instahub: Account, Beitrag, Werbung ...

Datenschutz mit InstaHub

Nutzung von Datenbanken

Name: _____

Blatt Nr. 7 Datum: _____

Viele Onlinedienste, wie Soziale Netzwerke, müssen viele Daten verwalten. Dazu werden Datenbanken verwendet. Man kann sich das Speichern von Daten in einer Datenbank so vorstellen: Du füllst ein Formular aus und gibst alle Informationen, die benötigt werden, weiter. Diese Daten werden dann im System kategorisch hinterlegt, für jeden Nutzer gleich. Damit die Informationen, die gebraucht werden, gefunden werden können, werden sie mit bestimmten Mustern sortiert.

Ihr könnt euch das Sortieren als eine Tabelle vorstellen:
In jeder Zeile steht ein neuer Kunde und alle Informationen, die über den Kunden bekannt sind.

Kundennummer	*Vorname*	*Nachname*	*Wohnort*	*Kontostand*
1577235	Thomas	Trautmann	Duisburg	174,00 €
4121356	Kevin	Kroll	Koblenz	512,15 €
1560158	Christoph	Noll	Montabaur	0,50 €
9356183	Sebastian	Testmann	Mainz	13,37 €

Hinter Instahub stehen ebenfalls Tabellen, wie im Beispiel oben.

Aufgabe 1

Öffnet euren eigenen Hub und wählt den Reiter *Datenbank* aus. Ihr könnt auch folgenden Link aufrufen, wenn ihr *Hub* durch den Namen eures Hubs ersetzt: *hub.instahub.org/home/testestest*. Mit Hilfe des Menüs könnt ihr ganze Tabellen oder einzelne Zeilen aufrufen.

Lasst euch zunächst alle Mitglieder eures Hubs ausgeben!

Aufgabe 2

a) Nutzt das Menü, um euch die Wohnorte aller Mitglieder ausgeben zu lassen.
b) Lasst euch die Wohnorte ausgeben, ohne dass Orte mehrfach genannt werden.

Aufgabe 3

Lasst euch die Nutzernamen der User ausgeben.
a) Ordnet die Ausgabe mit Hilfe des Menüs in alphabetischer Reihenfolge.
b) Ordnet die Ausgabe in absteigender Reihenfolge.

Zusatzaufgaben

a) Lasst euch insgesamt nur 3 Mitglieder ausgeben.
b) Zeigt wie groß das größte Mitglied ist.
c) Lasst euch die Anzahl der Mitglieder von Instahub ausgeben.

Datenschutz mit InstaHub

Nutzung von Datenbanken (Selektion)

Name: _____

Blatt Nr. 8 Datum: _____

*Zusätzlich zu den bisher genutzten Möglichkeiten, könnt ihr auch spezifisch nach bestimmten Einträgen suchen. Dazu müsst ihr eure Anfrage an die Datenbank genauer beschreiben. Nutzt dazu die **Selektion**-Funktion.*

Aufgabe 1

a) Wählt alle Einträge aus, bei denen das Geschlecht (gender) weiblich (female) ist.
b) Wählt alle Mitglieder aus Deutschland aus.
c) Wählt alle Mitglieder aus, die in Leipzig wohnen.
d) Zeigt nur Emily Faber an.

Ihr könnt die Beispiele aus Aufgabe 1 auch miteinander verbinden:

Aufgabe 2

a) Gebt alle Mitglieder aus, die unter 1,80 Meter groß sind
b) Findet alle Berliner, die Marc heißen.
c) Findet alle Leipziger Frauen.
d) Findet alle Linas und Lorenas.
e) Zeigt Geburtsdatum und Benutzernamen aller Frauen an, die kleiner als 1,60 m sind.

Datenschutz mit InstaHub Name: _____

Nutzung von Datenbanken (Löschen/Verändern/Einfügen) Blatt Nr. 9 Datum: _____

Bisher habt ihr nur Informationen aus der Tabelle ausgelesen. Mit Hilfe der Option ***Verändern von Daten*** *könnt ihr diese zusätzliche verändern, löschen und neue Einträge einfügen:*

Das Löschen von Einträgen aus der Tabelle

Aufgabe 1

a) Löscht ein Mitglied aus der Community

b) Löscht alle Mitglieder, die aus Hamburg stammen.

Das Einfügen von neuen Einträgen in die Tabelle

Aufgabe 2

a) Fügt den User Mila Bach aus Hamburg hinzu. Ihr könnt euch die Einträge in den fehlenden Feldern selbst ausdenken.

b) Fügt 3 weitere Personen ein. Füllt dazu alle Felder aus.

c) Was fällt euch auf, wenn ihr Felder nicht ausfüllt?

_____

_____

_____

Das Verändern von Einträgen aus der Tabelle

Aufgabe 3

a) Setzt die Körpergröße von allen Mitgliedern auf 160.

b) Ändert in dem zuletzt hinzugefügten Eintrag die Stadt auf „Dresden“.

c) Ersetzt den Begriff “Germany” überall durch “Deutschland”

Datenschutz mit InstaHub

Datenbanken

Name: _____

Lerntagebuch

Thema	bearbeitete Aufgaben	Klappt noch nicht so gut	Klappt ganz gut	Klappt sehr gut
Lesen				
Bedingungen				
Abgezeichnet von _____ am _____				
Löschen				
Abgezeichnet von _____ am _____				
Verändern				
Abgezeichnet von _____ am _____				
Einfügen				
Abgezeichnet von _____ am _____				

Jen Körtig	So Dingenskirchen	David Schmitz
Freunde treffen	8 Fotos	14 Jahre
Fortnite zocken	Lesen	Gladbach (D)
München	mit Hund spazieren (Rasko)	hasst seinen Mathelehrer
er ist 16	~~47 Jahre alt~~	6 Fotos
13 Photos	~~aus Erftstadt~~	24 Followers
37 Follower	Naturaufnahmen	9 Follows
21 Follows	28 Followers	männlich
mag Pfannkuchen	4 Follows	@David 470
Männlich	Name: Sophia	unsicher!
Barttträger	weiblich	
@jen84	Sicher!	
Naturaufnahmen		
mag vielleicht Pferde		
Standort		
Unsicher!		

Jen K	So D.	David S.
16 Jahre Freunde treffen Hunden in Deutschland spielt gerne Onlinegames 13 Photos 25 Followers 12 Following Naturphotos männlich	97 Jahre Entenhausen Deutschland Hund spazieren Naturfotos 8 Fotos, 15 F., 4 foll. Hund: Rasko liest Bücher weiblich Sophia	David hasst seinen Math. Lehrer 14 Jahre Bergisch Gladbach Kaule (Dt.) 6 Fotos, 30 F., 9 foll. männlich

Besprechung #2 nur mündlich.

8. Literaturverzeichnis

Alby, Tom (2007): Web 2.0. Konzepte, Anwendungen, Technologien. 2. Aufl.: Hanser-Verlag.

Bibliographisches Institut GmbH (2015): Duden. Deutsches Universalwörterbuch: Dudenverlag.

blue_beetle (2010): User-driven discontent. Kommentar einer Diskussion in einem Onlineforum (MetaFilter). Online verfügbar unter https://www.metafilter.com/95152/Userdriven-discontent#3256046.

Bodendorf, Freimut (2003): Daten- und Wissensmanagement. 2. Aufl. Berlin, Heidelberg: Springer.

Boyd, Danah M.; Ellison, Nicole B. (2007): Social Network Sites: Definition, History, and Scholarship. In: *Journal of Computer-Mediated Communication* (13), S. 210–230. Online verfügbar unter https://academic.oup.com/jcmc/article/13/1/210/4583062, zuletzt geprüft am 17.02.2019.

Brennan, Valerie (2010): Navigating social media in the business world. In: *Licensing Journal* (30), S. 8–9.

Bundesamt für Justiz und für Verbaucherschutz (2017): Grundgesetz für die Bundesrepublik Deutschland. GG. Online verfügbar unter http://www.gesetze-im-internet.de/gg/index.html, zuletzt geprüft am 13.02.2019.

Bundesamt für Sicherheit in der Informationstechnik: Empfehlungen: Passwörter. BSI für Bürger. Ins Internet mit Sicherheit. Online verfügbar unter https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html.

Bundesministerium für Bildung und Forschung (13.10.2014): Bekanntmachung des Bundesministeriums für Bildung und Forschung von Richtlinien zur Förderung von Forschungsinitiativen auf dem Gebiet des Selbstdatenschutzes im Rahmen des Förderprogramms „IKT 2020 – Forschung für Innovationen“. Online verfügbar unter https://www.bmbf.de/foerderungen/bekanntmachung-971.html, zuletzt geprüft am 05.04.2019.

Bundespolizeipräsidiums und Deutsche Bahn AG (2017-2018): Teilprojekt 1: Biometrische Gesichtserkennung. Berlin. Online verfügbar unter https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_down.pdf?_blob=publicationFile, zuletzt geprüft am 28.02.2019.

Bundesverfassungsgericht (1983): Urteil des Ersten Senats vom 15. Dezember 1983, BVerfGE 65, 1 - Volkszählung. Online verfügbar unter http://www.servat.unibe.ch/dfr/bv065001.html#, zuletzt geprüft am 13.02.2019.

Burkert, J.; Lächa, R.; Meyer, D. M. (2005): Datenbanken in der Sekundarstufe II. Theorie und Praxis. Online verfügbar unter http://www.oberstufeninformatik.de/DBinDerSekII_Gesamtwerk.pdf, zuletzt geprüft am 07.03.2019.

Chen, Peter Pin-Shan (1976). The Entity-relationship Model - Toward a Unified View of Data. 1. Aufl. (ACM Trans. Database Syst., 1).

Christian Solmecke, Christian (2019): Die EU-Datenschutzgrundverordnung (DSGVO) – ein Überblick. Online verfügbar unter https://www.wbs-law.de/it-recht/datenschutzrecht/die-eu-datenschutzgrundverordnung/, zuletzt geprüft am 14.02.2019.

Codd, Edgar F. (1991): The relational model for database management. Version 2. Reprinted with corr. Reading, Mass.: Addison-Wesley.

Das Europäische Parlament und der Rat der europäischen Union (2002): Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation). 2002/58/EG. Online verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32002L0058&from=DE, zuletzt geprüft am 28.02.2019.

Dorn, Julian (2016): friendzone. Online verfügbar unter https://blog.wi-wissen.de/post/friendzone, zuletzt geprüft am 06.03.2019.

Dorn, Julian (2019): Didaktik. Ansätze. Online verfügbar unter https://wi-wissen.github.io/instahub-doc-de/#/didactic, zuletzt geprüft am 06.03.2019.

Eckert, Claudia (2013): IT-Sicherheit. Konzepte - Verfahren - Protokolle. 8. Aufl. München: De Gruyter.

Egger, Edeltraud; Schillinger, Bernhard (1997): Datenschutz als Bürgerrecht. In: Peter Fleissner (Hg.): Datensicherheit und Datenschutz. Technische und rechtliche Perspektiven. 2., durchges. Aufl. Innsbruck: Studien-Verl., S. 47–62.

Esslinger-Hinz, Ilona; Wigbers, Melanie; Giovannini, Norbert; Hannig, Jutta; Herbert, Leonore; Jäkel, Lissy et al. (2013): Der ausführliche Unterrichtsentwurf. Weinheim, Basel: Beltz (Pädagogik 2014).

Europäische Gemeinschaft (1995): Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. 95/46/EG. Online verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:31995L0046&from=DE, zuletzt geprüft am 14.02.2019.

Europäische Union (04.05.2016): Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). DSGVO (EU). Online verfügbar unter https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2016/04/CONSIL_ST_5419_2016_INIT_DE_TXT.pdf, zuletzt geprüft am 12.02.2019.

Facebook (2019): Nutzungsbedingungen. Online verfügbar unter https://www.facebook.com/legal/terms/, zuletzt aktualisiert am 18.02.2019.

FAZ (2019): Zuckerberg verspricht mehr Privatsphäre bei Facebook. Konsequenzen aus dem Datenskandal. In: *Frankfurter Allgemeine Zeitung*, 06.03.2019, S. 1–2. Online verfügbar unter https://www.faz.net/aktuell/wirtschaft/diginomics/warum-mark-zuckerberg-bei-facebook-jetzt-auf-datenschutz-setzt-16076072.html, zuletzt geprüft am 14.03.2019.

Gesellschaft für Informatik e.V. (GI) (2008a): Grundsätze und Standards für die Informatik in der Schule. Bildungsstandards Informatik für die Sekundarstufe I. Empfehlungen der Gesellschaft für Informatik e. V. (LOG IN, 28. Jg. (2008), Heft Nr. 150/151). Online verfügbar unter https://www.informatikstandards.de/docs/bildungsstandards_2008.pdf, zuletzt geprüft am 05.04.2019.

Gesellschaft für Informatik e.V. (GI) (Hg.) (2008b): Grundsätze und Standarts für die Informatik in der Schule. Bildungsstandards Informatik für die Sekundarstufe I. *LOG IN 2008 (150/151)*. Berlin: LOG IN-Verlag.

Gesellschaft für Informatik e.V. (GI) (28.09.2017): Julian Dorn erhält Unterrichtspreis 2017 der Gesellschaft für Informatik für „friendzone“. Chemnitz. Online verfügbar unter https://gi.de/meldung/julian-dorn-erhaelt-unterrichtspreis-2017-der-gesellschaft-fuer-informatik-fuer-friendzone/, zuletzt geprüft am 06.03.2019.

Grimm, Rüdiger; Bräunlich, Katharina; Simic-Draws, Daniela; Kasten, Andreas (2016): Referenzmodell für ein Vorgehen bei der IT-Sicherheitsanalyse: Springer (Informatik Spektrum 39, 1). Online verfügbar unter https://link.springer.com/article/10.1007/s00287-014-0807-3, zuletzt geprüft am 04.03.2019.

Helisch, Michael; Pokoyski, Dietmar; Beyer, Marcus (2009): Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung. Wiesbaden: Vieweg + Teubner.

Hubwieser, Peter (2007): Didaktik der Informatik. Grundlagen, Konzepte, Beispiele. 3. Aufl. Berlin, Heidelberg: Springer-Verlag (eXamen.press).

Hug, Alexander (2018): Ergebnisse der Studie zur Datenschutzkompetenz Jugendlicher im Alter von 10 bis 13 Jahren. Koblenz.

Hug, Alexander; Grimm, Rüdiger (2017): Entwicklung eines Datenschutzkompetenzmodells. In: Ira Diethelm (Hg.): Informatische Bildung zum Verstehen und Gestalten der digitalen Welt, Lecture Notes in Informatics (LNI). Bonn. Gesellschaft für Informatik (GI), S. 15–18.

Humbert, Ludger (2006): Didaktik der Informatik. Mit praxiserprobtem Unterrichtsmaterial. 2., überarb. und erw. Aufl. Wiesbaden: B.G. Teubner Verlag | GWV Fachverlage GmbH Wiesbaden (Leitfäden der Informatik).

International World Wide Web Conference Committee (Hg.) (2016): An Empirical Analysis of Algorithmic Pricing on Amazon Marketplace. Unter Mitarbeit von Le Chen, Alan Mislove und Christo Wilson. International World Wide Web Conference 2016. Montréal, Québec (Canada).

Keltz, Andreas (1998): Kriterien für relationale Datenbanken. Hochschule der Medien Stuttgart. Stuttgart. Online verfügbar unter https://www.hdm-stuttgart.de/~riekert/lehre/db-kelz/chap6.htm, zuletzt geprüft am 07.03.2019.

Krieger, C. Patricia; Schmatzinski-Damp, Ute (2010): Richtlinie Verbraucherbildung. an allgemeinbildenden Schulen in Rheinland-Pfalz. Hg. v. Ministerium für Bildung, Wissenschaft, Jugend und Kultur Rheinland-Pfalz. Mainz. Online verfügbar unter https://verbraucherbildung.bildung-rp.de/fileadmin/user_upload/verbraucherbildung.bildung-rp.de/Materialien/Richtlinie_VB.pdf, zuletzt geprüft am 04.03.2019.

Kultusministerkonferenz (2016): Bildung in der digitalen Welt. Strategie der Kultusministerkonferenz. Hg. v. Sekreteriat der Kultusministerkonferenz. Berlin, zuletzt aktualisiert am https://www.kmk.org/fileadmin/Dateien/pdf/PresseUndAktuelles/2018/Digitalstrategie_20, zuletzt geprüft am 15.03.2019.

Landesrecht Hessen (1970): Hessisches Datenschutz- und Informationsfreiheitsgesetz. HDSIG.

Mayer, Roger C.; Davis, James H.; Schoorman, F. David: An Integrative Model of Organizational Trust. In: *The Academy of Management Review* 1995 (20 (3)), S. 709–734. Online verfügbar unter https://www.jstor.org/stable/258792?seq=1#metadata_info_tab_contents, zuletzt geprüft am 04.03.2019.

Medienpädagogischer Forschungsverbund Südwest (Hg.) (2015): KIM-Studie 2014. Kinder + Medien, Computer + Internet. Basisuntersuchung zum Medienumgang 6- bis 13-

Jähriger in Deutschland. Online verfügbar unter https://www.mpfs.de/fileadmin/files/Studien/KIM/2014/KIM_Studie_2014.pdf, zuletzt geprüft am 05.04.2019.

Meyer, Hilbert (2003): Zehn Merkmale guten Unterrichts. Empirische Befunde und didaktische Ratschläge. In: Problemschüler, Bd. 10: Beltz Verlag, S. 36–43. Online verfügbar unter http://www.fdbio-tukl.de/assets/files/fd_documents/evaluation_kriterien/976_9_0_10Merkmaleguten Unterrichts.pdf, zuletzt geprüft am 05.03.2019.

Ministerium für Bildung, Wissenschaft, Jugend und Kultur Rheinland-Pfalz (2010): Lehrplan Informatik. Wahlfach und Wahlpflichtfach an Gymnasien und Integrierten Gesamtschulen (Sekundarstufe I). Mainz. Online verfügbar unter https://static.bildung-rp.de/lehrplaene/gymnasium/Informatik_LP_SekI.pdf, zuletzt geprüft am 04.03.2019.

Ministerium für Bildung, Wissenschaft, Jugend und Kultur Rheinland-Pfalz (2017): Orientierungsrahmen Schulqualität. Online verfügbar unter https://ors.bildung-rp.de/fileadmin/user_upload/ors.bildungrp.de/Broschuere_ORS_2017_WEB.pdf, zuletzt geprüft am 15.03.2019.

Ministerium für Bildung, Wissenschaft, Weiterbildung und Kultur Rheinland-Pfalz (2015): Inklusiver Unterricht in Rheinland-Pfalz. Mainz.

Obar, Jonathan A.; Wildman, Steve (2015): Social Media Definition and the Governance Challenge: An Introduction to the Special issue. University of Ontario Institute of Technology, Michigan State University. Online verfügbar unter https://poseidon01.ssrn.com/delivery.php?ID=819027008027065114093117027030073092037036069049083071005104003093091115119029101093096050033032121023027004081019119002113121023073034069016001096108098104018024010001051116098020121006091094107105106115072117073111116005102088105099031002002064020&EXT=pdf, zuletzt geprüft am 17.02.2019.

Oberle, Daniel; Berendt, Bettina; Hotho, Andreas; Gonzalez, Jorge (2003): Advances in Web Intelligence. First International AtlanticWeb Intelligence Conference, AWIC 2003,

Madrid, Spain, May 5-6, 2003. Proceedings. Berlin, Heidelberg: Springer (Lecture Notes in Computer Science, Lecture Notes in Artificial Intelligence, 2663).

Pfitzmann, Andreas; Hansen, Marit (2008): Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology. Online verfügbar unter http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf, zuletzt aktualisiert am 18.02.2019.

Rothmann, Robert (2017): Die Rechtswirklichkeit der Informierten Zustimmung im Fall von Facebook. Universität Wien. Berlin. Online verfügbar unter http://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/2017-11-02-Jahrestagung-2017/1.1c_Rothmann_Folien_Vortrag_Forum_Privatheit_Berlin_Uni_Wien_2017.pdf, zuletzt geprüft am 17.02.2019.

Schubert, Sigrid; Schwill, Andreas (2011): Didaktik der Informatik. 2. Aufl. Heidelberg: Spektrum Akademischer Verlag.

Schwartz, John (2001): Giving Web a Memory Cost Its Users Privacy. In: *New York Times*, 04.09.2001. Online verfügbar unter https://www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy.html, zuletzt geprüft am 18.02.2019.

Seidel, Ulrich (1970): Persönlichkeitsrechtliche Probleme der elektronischen Speicherung privater Daten. In: *Neue Juristische Wochenschrift*, 1970, S. 1581–1583. Online verfügbar unter https://www.fiff.de/publikationen/fiff-kommunikation/fk-2015/fk-2015-2/fk-2015-2-content/fk-2-15-s62.pdf, zuletzt geprüft am 13.02.2019.

Six, Ulrike; Gleich, Uli; Gimmler, Roland (2007): Kommunikationspsychologie - Medienpsychologie. Lehrbuch. 1. Aufl. Weinheim: Beltz PVU (Anwendung Psychologie).

Staatsministerium für Kultus des Freistaates Sachsen (2004): Lehrplan Gymnasium. Informatik. Hg. v. Sächsisches Staatsministerium für Kultus. Radebeul. Online verfügbar unter

https://www.schule.sachsen.de/lpdb/web/downloads/1430_lp_gy_informatik_2018.pdf?v2, zuletzt aktualisiert am 2018, zuletzt geprüft am 05.04.2019.

Stevens, John (2018): Internet Stats & Facts for 2019. Social Media Statistics 2019. Online verfügbar unter https://hostingfacts.com/internet-facts-stats/, zuletzt geprüft am 12.02.2019.

UC Berkeley School of Information: Privacy Dashboard. Online verfügbar unter https://privacypatterns.org/patterns/Privacy-dashboard, zuletzt geprüft am 14.02.2019.

Unterstein, Michael; Matthiessen, Günter (2012): Relationale Datenbanken und SQL in Theorie und Praxis. 5. Aufl. Berlin: Springer Vieweg (eXamen.press).

Zimmermann, Christian; Accorsi, Rafael (2013): Transparenz durch Privacy Dashboards. Ein Process Mining Ansatz. Universität Freiburg.