Masterarbeit

Entwicklung einer Unterrichtsreihe
mit dem Thema *Datenschutz*
zur Verbesserung der Datenschutzkompetenz
von Schülerinnen und Schülern der Klassenstufe 6
an einem Gymnasium

Eingereicht von:
Johannes Georg Thielen
Matrikelnummer:
214 100 726

Betreuer: Prof. Dr. Rüdiger Grimm
Alexander Hug

Universität Koblenz-Landau, Campus Koblenz

Fachbereich 4,
Institut für Computervisualistik,
Fachdidaktik Informatik

Eidesstattliche Erklärung

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).

Bezüglich der genutzten Arbeitsmaterialien von klicksafe, wurde eine Nutzungsgenehmigung ausgesprochen:

Lieber Herr Thielen!
Es freut mich, dass Sie unsere Materialien verwenden wollen. Hiermit gestatten wir die Verwendung in der von Ihnen vorgeschlagenen Art und Weise. In Zukunft werden wir unsere Lizenzen dahingehend ändern, dass eine Veränderung möglich ist,

Viele Grüße,

Stefanie Rack

Referentin EU-Projekt klicksafe

Landeszentrale für Medien und Kommunikation (LMK)
Turmstraße 10
67059 Ludwigshafen

Tel.: 0621 - 5202 113

_____

Koblenz, 9. Oktober 2018 – Johannes Georg Thielen

Für die Unterstützung in allen Bereichen,
möchte ich mich bei

Alexander Hug,
als wissenschaftlicher Mitarbeiter im Bereich Datenschutz,
bei dem ich tiefe Einblicke in die wissenschaftliche Forschung und das Themengebiet Datenschutz durch meine Mitarbeit als wissenschaftliche Hilfskraft erhalten habe,

Professor Dr. Rüdiger Grimm,
als emeritierter Professor, für die Betreuung meiner Arbeit bedanken,

Fabian Bildhauer,
als Lehrkraft am Hildagymnasium in Koblenz,
welcher den praktischen Teil ermöglichte,

bei meinen Eltern und Geschwistern,
die in der Endphase noch Korrektur gelesen haben,

sowie bei meiner engen Familie
Svenja und Till

bedanken.

Inhaltsverzeichnis

Abkürzungsverzeichnis

LV: Lehrervortrag

EA: Einzelarbeit

PA: Partnerarbeit

GA: Gruppenarbeit

DSGVO: Datenschutzgrundverordnung

BDSG: Bundesdatenschutzgesetz

LDSG: Landesdatenschutzgesetz

Tabellenverzeichnis

Abbildungsverzeichnis

1. Einleitung

1.1. Einführung

"Datenschutz ist unerlässliche Voraussetzung für
eine demokratisch verantwortbare Informationsgesellschaft."
- Hartmut Lubomierski[1]

Wenn Datenschutz die notwendige Bedingung von einer demokratisch verantwortbaren Informationsgesellschaft ist, so muss Datenschutz auch ein festes Ziel innerhalb der Bildung aller Kinder und Jugendlichen sein. Datenschutz dient nicht nur dem Schutz des Individuums, es ist auch Machtkontrolle sowie Schutz der informationellen Selbstbestimmung und somit auch Schutz der demokratischen Freiheit. Die Grundpfeiler der Demokratie beruhen auf der Legislative, der Exekutive und der Judikative. Die drei theoretischen Grundpfeiler werden immer durch Personen repräsentiert, die frei Entscheidungen treffen sollen. Stellt man sich nun vor, dass diese Personen aufgrund eines schlechten Datenschutzes erpressbar werden (siehe NDR-Bericht „Nackt im Netz: Intime Details von Politikern im Handel“[2]), so fällt ein Grundpfeiler und die Demokratie kommt ins Wanken.

Daraus folgt, dass die heutige Gesellschaft zum Erhalt der demokratischen Freiheit in Bezug auf persönliche Daten, den dazugehörigen Gefahren und dem Schutz der Daten sensibilisiert werden muss. So schreiben Eggert et al. 2016: „Eine Sensibilisierung für die Situationen und Umstände, in denen wir Datenspuren hinterlassen und in denen Daten gesammelt werden, ist eine notwendige Voraussetzung, um die daraus resultierende Gefahr für die eigene Privatsphäre einschätzen zu können.“ (Eggert et al. 2016, S. 18) Somit muss die Grundlage allgemeiner Bildung in Bezug auf Datenschutz sein, ein Bewusstsein für die (ungewollte) Datenverarbeitung zu schaffen, auf der dann aufbauend die *Datenschutzkompetenz* gestärkt werden kann. Dabei sollte an die Handlungskompetenz der Lernenden angeknüpft werden, da diese häufig weitreichender als die der Lehrenden ist. Zu berücksichtigen ist auch, dass im Leben der Lernenden die digitalen Möglichkeiten nicht mehr weg zu denken sind. Daher sollte es bei der Vermittlung von Datenschutzkompetenz nicht um eine Verteuflung der neuen digitalen Möglichkeiten und dem Oktroyieren einer Ablehnungshaltung gegenüber aller digitalen Neuheiten gehen, sondern um eine Sensibilisierung für entstehende Gefahrenquellen mit dem Ziel einer kompetenten, verantwortungsbewussten Nutzung der digitalen Möglichkeiten.

[1] Presseerklärung zum 1. Europäischen Datenschutztag am 28. Januar 2007, fhh.hamburg.de
[2] https://www.youtube.com/watch?v=yGXb-ChrSFA (abgerufen am 12.09.2018)

Für die Umsetzung an allgemeinbildenden Schulen schreibt die Kultusministerkonferenz (KMK) in ihrem Strategiepapier „Bildung in der digitalen Welt“, dass Lehrende „durch ihre Kenntnisse über … Datenschutz und Datensicherheit … die Schülerinnen und Schüler … befähigen [sollen], bewusst und überlegt mit Medien und eigenen Daten in digitalen Räumen umzugehen und sich der Folgen des eigenen Handelns bewusst zu sein.“ (Kultusministerkonferenz 2016, S. 27) Durch die Kultushoheit der Länder werden die Vorschläge der KMK unterschiedlich umgesetzt. In Rheinland-Pfalz findet sich das Thema einerseits stellenweise in den fächerspezifischen Lehrplänen und andererseits in der fächerübergreifenden Medien- und Verbraucherbildung wieder (siehe dazu (Groß et al. 2014) sowie (Ministerium für Bildung, Wissenschaft, Jugend und Kultur Rheinland-Pfalz 2010b)). Dabei bilden die letzten beiden nur Empfehlungen und Richtlinien, welche in schulinternen Medienkonzepten und Arbeitsplänen verankert werden sollten. Daher bleibt es bei individuellen Umsetzungen der Schulen, das Thema *Datenschutz* als Lerninhalt aufzugreifen.

1.2. Forschungsziel

Diese Arbeit soll erneut das wichtige Thema *Datenschutz* als Unterrichtsthema in den Blickpunkt allgemeiner Bildung rücken. Seit den ersten Unterrichtsversuchen das Thema aufzugreifen, wie zum Beispiel das Planspiel – Jugend im Datennetz von Brandt et al. aus dem Jahre 1991, sind noch einige weitere Unterrichtsansätze entstanden. Wie sich jedoch in der Studie von Hug herausstellte, sind gerade Kinder im Alter von zehn bis dreizehn Jahren in ihrer Datenschutzkompetenz noch eingeschränkt (vgl. Hug 2018b). Da gerade in dieser Altersklasse jedoch das Smartphone als Zugang zum Internet eine immer größere Bedeutung erhält (vgl. Feierabend et al. 2016, 29 f.), sollte die Datenschutzkompetenz auch früher gefördert beziehungsweise verstärkt ausgebildet werden.

Die Frage der hier vorliegenden Arbeit lautet daher:

Wie kann eine Unterrichtsreihe zum Thema *Datenschutz* aussehen, sodass Schülerinnen und Schüler erstens dafür ein Interesse entwickeln und zweitens sich dann, aus der intrinsischen Motivation heraus, in das Thema vertiefen?

Hierzu soll ein Ansatz aufgezeigt werden, der einen motivierenden Aspekt mit sich bringt und verschiedene, auch fachübergreifende, Vertiefungsansätze bietet. Neben einer theoretischen Erarbeitung wird diese auch praktisch getestet, wodurch Verbesserungsansätze gefunden werden können.

1.3. Inhaltliche Gliederung

In den folgenden Kapiteln soll ausgehend von den Grundlagen zu der Thematik *Datenschutz* zuerst die Datenschutzkompetenz erläutert werden. Anschließend folgt eine Übersicht über Unterrichtsmaterialien zum Kompetenzstärkung von Schülerinnen und Schülern. Darauf aufbauend wird eine Unterrichtsreihe in Ergänzung mit eigenen Materialien erstellt, welche praktisch getestet und damit evaluiert wird.

Kapitel 2 beginnt mit der Definition von personenbezogenen Daten. Hierbei werden die Begriffe Datenschutz und Privatsphäre erläutert. Das Schutzbedürfnis setzt die Existenz von Gefahren voraus, welche in Bezug auf persönliche Daten in Folge kategorisiert werden. Im Abschnitt 2.3 werden dann Situationen gezeigt, in denen die schützenswerten Daten teils unbewusst und ungewollt öffentlich werden können. Um dennoch geschützt zu sein, werden Anwendungen von Datenschutz aufgezeigt: Beginnend mit dem rechtlichen Rahmen, über Techniken und Tools zum Selbstdatenschutz bis hin zu Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik. Zum Abschluss wird Datenschutzkompetenz nach Hug und Grimm definiert, welche bei Schülern und Schülerinnen durch diese Arbeit gestärkt werden soll. Neben den themenbezogenen Begriffen werden auch die spezifischen Themen für die spätere Unterrichtsreihe erarbeitet und im Kontext bestimmt.

In Kapitel 3 sollen existierende Unterrichtsansätze, die in die weitere Arbeit einfließen, aufgezeigt werden. Im Fokus steht dabei die EU-Initiative für mehr Sicherheit im Netz unter dem Namen *klicksafe*[3]. Hier wird ein breites Themenspektrum bezüglich *Datenschutz* abgebildet. Exemplarisch vorgestellt werden die Unterrichtseinheiten zu den Themen personenbezogene Daten, Schadsoftware und Tracking. Weitere Unterrichtsideen entstammen aus der Zusammenarbeit von *klicksafe* und *Handysektor*[4], ein gemeinschaftliches Projekt der Landesanstalt für Medien NRW und des Medienpädagogischen Forschungsverbundes Südwest (mpfs). Diese stellen Themen rund um das Smartphone, wie App-Berechtigungen oder Bewegungsprofile, als Unterrichtsthema bereit. Die letzten beiden berücksichtigten Unterrichtsansätze behandeln Rechte und Gesetze zum Thema *Datenschutz* sowie Passwörter als Grundlage von Selbstdatenschutz.

Auf Basis der in Kapitel 2 beschriebenen Themen sowie der Materialien aus Kapitel 3 wird in Kapitel 4 eine mögliche Unterrichtsreihe zum Thema *Datenschutz* erarbeitet. Um auf die Lerngruppe eingehen zu können, wurde dafür eine Vorbereitungsumfrage durchgeführt. Die Unterrichtsreihe wird anhand der Struktur einer Unterrichtsplanung aus der Fachdidaktik Informatik skizziert. Abweichend davon wird hier zuerst die Didaktik für die gesamte Unterrichtsreihe in Abschnitt 4.2 erarbeitet und im

[3] https://www.klicksafe.de/
[4] https://www.handysektor.de/

Anschluss daran die Methodik für die einzelnen Stunden im Abschnitt 4.3 beschrieben, inklusive der Beschreibung des Stundenverlaufs der praktischen Erprobung in einer 6. Klasse des Hilda-Gymnasiums Koblenz. Dazu wurden fünf Schulstunden genutzt, welche im Rahmen von Klassenleiterstunden und Mathematikstunden[5] lagen. Somit können in die methodische Planung jeder Einzelstunde in Abschnitt 4.3 die Resultate der vorangegangenen Stunde miteinfließen.

In Kapitel 5 wird der gesamte Unterrichtsversuch zusammengefasst sowie durch eine Untersuchung mit dem Fragebogen der Studie von Hug zur Datenschutzkompetenz von Schülerinnen und Schüler in der Orientierungsstufe evaluiert (siehe Hug 2018a). Die Versuchsklasse hatte schon an der Studie teilgenommen und so soll gezeigt werden, wie sich die Datenschutzkompetenz verändert hat.

Abschließend wird daraus in Kapitel 6 ein allgemeines Resümee gezogen, um anschließend weitergehende Forschungsfragen und -ansätze aufzuzeigen.

[5] In Rheinland-Pfalz gibt es keinen Informatikunterricht in der Orientierungsstufe, daher wird das Thema *Datenschutz* im Bereich der Medien- und Verbraucherbildung aufgegriffen, welche fächerübergreifend vermittelt werden soll.

2. Datenschutz

Um *Datenschutz* als Unterrichtsthema aufzuarbeiten, wird zuerst der Begriff selbst definiert. Darauf aufbauend werden Gefahren erörtert, gegen die der Datenschutz wirken soll. Abschließend werden verschiedene Schutzmechanismen beschrieben und erläutert sowie der Begriff der Datenschutzkompetenz erarbeitet.

2.1. Definitionen

Der Begriff *Datenschutz* setzt sich zusammen aus den Begriffen Daten und Schutz. Dabei geht es um den Schutz von Daten. Aber nicht Schutz von Daten im Sinne der Datensicherung (engl. protection), z.B. vor Verlust, Veränderung oder Ähnlichem, sondern Schutz von persönlichen Daten (engl. privacy) wie Name, Alter, Wohnort, aber auch Interessen und Vorlieben, gegenüber unerlaubter Verwendung durch unbefugte Dritte (vgl. Seidel 1970, S. 1583).

Daten werden in diesem Fall gleichgesetzt mit Informationen über etwas oder über Personen. Die Fachliteratur unterscheidet hier nochmals in Datum (Einzahl von Daten) als eine Aneinanderreihung von Zeichen ohne ersichtliche Bedeutung und in Information als Datum im Kontext. Das heißt, Daten werden zu einer Information, indem ihnen eine Bedeutung zugeordnet wird und mit der die Daten interpretiert werden können. Auf der anderen Seite können Informationen in verschiedenen Datenobjekten dargestellt werden. So liegt die Artikelnummer in einer Datenbank im Binärcode vor, wohingegen ein User die Artikelnummer als Tastatureingabe im Dezimalzahlsystem dem Eingabepuffer übergibt (vgl. Czernik).

In der Thematik von Datenschutz stehen vor allem **personenbezogene Daten** im Mittelpunkt. Personenbezogene Daten[6] sind nach der Datenschutzgrundverordnung (Europäische Union 04.05.2016) Angaben, die bei Zuordnung zu einer natürlichen Person Einblicke in deren physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität ermöglichen. So sind auch personenbezogene Daten im Bundesdatenschutzgesetz definiert als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen“ (§46 in Bundesministeriums der Justiz und für Verbraucherschutz 30.06.2017). Dabei bedeutet identifizierbar, dass es eine eindeutige Zuordnung zwischen den Daten und der Person, zum Beispiel durch einen Benutzernamen oder Name in Verbindung zum Geburtsdatum, geben muss. Das heißt, alle Daten mit Bedeutung zu einer Person, wie zum Beispiel Alter, Größe, Besitz und Vermögen bis hin zu Interessen, Hobbies und Religion, sind personenbezogene Daten, die schützenswert sind.

[6] Im Folgenden auch oft persönliche Daten genannt.

Im Zusammenhang mit dem Begriff *Datenschutz* fällt auch häufig der Begriff der **Privatsphäre**. In diesem soll definiert werden, welche personenbezogenen Daten schützenswert sind und welche eher belanglos öffentlich sein können. Der Begriff der Privatsphäre ist nach Egger und Schillinger 1997 nicht trennscharf zu definieren. So beschreiben Egger et al. verschiedene Versuche, Hypothesen bezüglich Privatsphären aufzustellen.

Einerseits gibt es die Sphärenhypothese, welche die Lebensbereiche und deren zugehörige Daten in verschieden Sphären aufgliedert, von Intimsphäre über Vertrauenssphäre bis hin zur Öffentlichkeitssphäre. Dabei soll auf die absolut geschützte Intimsphäre keinerlei Zugriff anderer erlaubt sein. Währenddessen auf die Informationen der Privatsphäre, wie zum Beispiel den Bereich der Gesundheit, durch befugte Institutionen (Arzt, Krankenhaus) zugegriffen werden muss. Dabei sollen bestimmte Institutionen im Sinne des Datenschutzes aber auch nur auf Sektoren von solchen Sphären zugreifen dürfen, die für sie relevant sind. Zum Beispiel soll das Finanzamt personenbezogene Daten über die Einkünfte erheben können, nicht aber Zugriff auf den Bereich der Gesundheit haben. Die Schwachpunkte an dieser Hypothese sind die undefinierbaren Grenzen der Sektoren für die Zugriffsmöglichkeiten sowie das subjektive Empfinden des Bereiches der Privatsphäre. So empfindet man heute das Bekanntwerden seiner Religionszugehörigkeit oftmals als unsensibel, wohingegen vor 80 Jahren genau diese Information das Todesurteil bedeuten konnte.

Die Mosaikhypothese erweitert die voran genannte Hypothese um den Aspekt, dass auch jene Daten geschützt werden sollten, welche für sich alleine stehend keine intimen, privaten Informationen vermitteln, aber in Verbindung zu anderen Daten brisante Informationen darstellen können. Als Beispiel dazu dient das KFZ-Zeichen, welches ohne weiteres Zusatzwissen keiner Person zugeordnet werden kann. Die Person wird aber bestimmbar, sobald man auf die Datenbank der KFZ-Zulassungsbehörde zugreifen kann oder über Fotos beziehungsweise häufige übereinstimmende Standortdaten die Verknüpfung schaffen kann. Über solche Verknüpfungen kann der Person dann auch ein finanzieller Status (die Person kann sich ein Auto einer bestimmten Marke oder Typs leisten) zugeordnet und weitere personenbezogene Daten generiert werden. Genau diese Hypothese zeigt die heutige Schwierigkeit des Datenschutzes. Durch das Nutzen vernetzter IT-System können Informationen (fast) grenzenlos und unbewusst für die betroffene Person kombiniert werden.

Eine weitere Hypothese, die Rollenhypothese, nimmt die verschiedenen Rollen eines Individuums in den Fokus. So ist ein Jugendlicher vermutlich Schüler und zugleich Mitbürger und an anderer Stelle Patient. In dieser Hypothese sollen den Institutionen nur rollenspezifische Daten preisgeben werden, wobei die Sensibilität von dem jeweiligen Interaktionspartner abhängt. Die Schule darf alle schulrelevanten Daten von der Person erhalten, aber keinen Zugriff auf die Krankenakte des Schülers haben. Auch hier gibt es Grenzfälle, zum Beispiel indem Krankmeldungen des Schülers der Schule

vorgelegt werden. In diesem Fall der Rollenhypothese hat Datenschutz genau den Zweck, die Zusammenführung der Rollenbilder zu verhindern.

Kern der Ausführung ist, dass Privatsphäre schwierig zu definieren und somit auch die Wertigkeit des Schutzes gewisser Informationen nicht einfach zu bestimmen ist. So lässt sich zusammenfassen, dass als Privatsphäre (und die dazugehörigen Informationen) der Bereich der persönlichen Lebensführung bezeichnet werden kann, zu dem nur das engste persönliche Umfeld des Einzelnen Zugang hat. Das bedeutet, zur Privatsphäre gehört allem voran die eigene Wohnung, aber auch das Familienleben. Des Weiteren gehört zur Privatsphäre die private Kommunikation mit Freunden und alle dazugehörigen spezifischen personenbezogenen Daten von Name, Alter, Adresse über Sexualität bis hin zu Kommunikationsdaten, wann wer wem eine Nachricht geschickt hat usw. (vgl. Artikel 12 Vereinte Nationen - Generalversammlung 10.12.1948). Trotz aller Bemühungen lassen sich personenbezogene Informationen nicht in überschneidungsfreie Sphären oder Rollen einteilen, sodass eine eindeutige Begründung, welche Daten schützenswert sind, nicht aus den Hypothesen zur Privatsphäre erwachsen kann.

Der Begriff **Datenschutz** im engeren Sinne (engl. privacy) beschreibt nach dem deutschen Bundesdatenschutzgesetz (Bundesministeriums der Justiz und für Verbraucherschutz 30.06.2017) allgemein die Fähigkeit einer natürlichen Person, die Weitergabe von persönlichen Informationen zu kontrollieren. In diesen Bereich fallen insbesondere Sicherheitsanforderungen, die der deutsche Gesetzgeber durch das informationelle Selbstbestimmungsrecht geregelt hat (siehe Abschnitt 2.4).

Datenschutz lässt sich in zwei Bereiche aufteilen, den **Systemdatenschutz** und den **Selbstdatenschutz**. Der Selbstdatenschutz fängt bei der eigenen bewussten Preisgabe von personenbezogenen Daten an, kann durch Techniken wie Pseudonymisierung oder Anonymisierung unterstützt werden und endet bei der informationellen Selbstbestimmung. Der Systemdatenschutz dagegen garantiert den Betroffen, deren Daten verarbeitet werden, dass die datenverarbeitenden Systeme einerseits so wenig wie möglich personenbezogene Daten verarbeiten und andererseits nur berechtigten Personen Zugriff auf die Daten ermöglichen beziehungsweise ansonsten die Inhalte vor unbefugten Dritten verbergen. Hierbei spielt auch die Datensicherheit mit ihren Zugangs- und Verarbeitungskontrollen eine Rolle. Ein weiterer Schritt im Systemdatenschutz wäre eine einfache Kontrollmöglichkeit für den Betroffenen, welche Daten dem System vorliegen und wie diese verarbeitet werden, ohne jedes Mal auf das Recht der Auskunft gegenüber Unternehmen und Behörden willentlich zugreifen zu müssen, sowie die Verpflichtung, dass die Hersteller ihre Geräte und Systeme in einer datenschutzfreundlichen Ausgangskonfiguration vertreiben (privacy by default) und Dienstleister auf datenschützende Grundeinstellungen achten (vgl. Andersen und Woyke 2013, 106 f.). Dies wird aber von den zuständigen Institutionen noch nicht umgesetzt und ist auch (noch) nicht rechtlich geregelt.

2.2. Gefahren

Nachdem der Begriff Datenschutz definiert ist, soll in diesem Abschnitt auf vier mögliche Gefahrentypen eingegangen werden (vgl. Bengesser 2017). Diese sollen den Schülerinnen und Schülern, die an der Unterrichtsreihe *Datenschutz* teilnehmen werden (vgl. Kapitel 4), bewusst gemacht werden.

2.2.1. Kriminalität

Die offensichtlichste Gefahr ist, dass mit personenbezogenen Daten kriminelle Aktivitäten ermöglicht werden. So können zum Beispiel Fremde mit gestohlenen Passwörtern, Kreditkartennummern sowie Kundennummern in Onlineshops Dinge auf fremde Kosten bestellen, sodass es zu einer persönlichen finanziellen Schädigung kommen kann. Ein weiterer finanzieller Schaden kann durch Industriespionage oder den Diebstahl von geistigem Eigentum entstehen, wobei dies für den einzelnen Bürger (oder Schüler und Schülerin) keine direkte Gefahr bedeutet, sondern eher für Unternehmen. Eine weitere Gefahr im Bereich Kriminalität stellt der Identitätsdiebstahl dar, bei dem im schlimmsten Fall Verbrechen im Namen anderer geschehen können und die Behörden unschuldige Personen belangen wollen. Auf niedrigerem Niveau kann dies aber auch zu Problemen führen, wie zum Beispiel bei Cybermobbing in der Schule. Hier schreiben Jugendliche im Namen des Betroffenen peinliche oder negativ auslegbare Nachrichten, sodass ein falsches Bild über die Person entsteht. Als Betroffener muss man in diesen Fällen nachweisen, nicht der Ausführende gewesen zu sein, weder bei der Bestellung noch bei den Nachrichten oder im schlimmsten Fall bei dem Verbrechen. Dies ist aber immer mit weiteren Mühen verbunden, und in Zeiten des Internets, in dem durch die Verbreitung alles auch gespeichert wird, ist es schwer, das negative Bild der eigenen Person wieder zu korrigieren.

2.2.2. Überwachung

Das Bundesverfassungsgericht beschreibt im Volkszählungsurteil die Folgen von (unnötiger) Überwachung folgendermaßen: Die Ungewissheit darüber, ob von der Norm abweichende Verhaltensweisen registriert, notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, beeinflusst einen Menschen insofern, dass er versuchen wird, nicht durch solche Verhaltensweisen aufzufallen. Dies beeinträchtigt die individuellen Entfaltungschancen des Einzelnen. Außerdem stellt das nicht nur eine Gefahr für den Einzelnen dar, sondern auch für die Gesellschaft, da Selbstbestimmung ein elementarer Baustein der freiheitlichen Demokratie ist, welche auf freie Handlungs- und Mitwirkungsfähigkeit seiner Bürger angewiesen ist (vgl. Bundesverfassungsgericht, Urteil vom 15.12.1983). Dies zeigt, wie die Gefahr der Überwachung das Leben und Verhalten von Personen verändern kann. Hier sollen Gesetze (siehe Abschnitt 2.4) diese Gefahr einschränken. Es gibt trotzdem Stellen, an denen Überwachung beginnen und erfolgen kann.

So hat beispielsweise jeder Bürger bei der Beantragung des Personalausweises oder Reisepasses ein biometrisches Bild abgegeben. Mit diesen Daten wäre es möglich, auf Bildern von Überwachungskameras an öffentlichen Plätzen Menschen zu identifizieren und zu verfolgen (vgl. Eckert 2013, S. 508). Ein weiterer gerichtlich und medial aufgearbeiteter Fall ist die Vorratsdatenspeicherung von Verbindungsdaten von Mobilfunk- und Internetkommunikation (siehe auch Verwaltungsgericht Köln, Urteil vom 20.04.2018). Über sie könnten Bewegungs- und Kommunikationsprofile einzelner Personen erstellt werden. Am Beispiel des Bundestagabgeordneten Malte Spitz[7] wird ersichtlich, wie weitreichend die Speicherung von eigentlich zunächst ungenauen Verbindungsdaten sind. Der Bundestagsabgeordnete forderte seine Verbindungsdaten von der Telekom an und hat diese von *Zeit Online* in einer Karte visualisieren lassen. Neben den Aufenthaltsorten seines Handys wird auch die Dauer und Anzahl von Gesprächen und Nachrichten sichtbar. Verknüpft man diese Daten noch mit anderen personenbezogenen Daten aus anderen Quellen, so lässt sich ein relativ genauer Tagesablauf rekonstruieren. Die Gefahr - neben dem oben beschriebenen Andersverhalten bei Überwachung - liegt auch in der Fehlinterpretation solcher Daten, sodass es zu falschen Beschuldigungen kommen kann. (vgl. Kapitel 2.2.3)

Eine andere Art der Überwachung erfolgt durch die Privatwirtschaft: Während des Surfens im Internet sammelt man beispielsweise Cookies, durch die ein User-Tracking erfolgen kann. Die Cookies dienen dem Wiedererkennen von Besuchern auf Seiten und / oder protokollieren sogar das Userverhalten im Netz, wie beispielsweise die Cookies von Google Analytics (siehe Vollmert und Lück 2015). Ähnlich funktionieren auch in der realen Welt Bonuskarten, wie zum Beispiel *Payback*[8] oder *DeutschlandCard*. Vordergründig wird diese Technik angeboten, um dem Benutzer ein optimales Surf- / Einkaufserlebnis zu ermöglichen, indem die Webseite /das Einkaufsgeschäft dem Nutzerverhalten angepasst wird und wiederkehrende Eingabe durch den Benutzer unterbleiben können. Im Hintergrund können dabei aber Benutzerprofile mit Verhaltens- und Konsumgewohnheiten erstellt werden, sodass beispielsweise benutzerspezifische Werbung eingeblendet werden kann oder Konsumenten anlockende Rabattaktionen erhalten können.

Genauso verfahren auch „kostenlose“ soziale Netzwerke wie *Facebook* oder *YouTube*, die das Ziel verfolgen, digitale Personenprofile anzulegen. Mit der Vermarktung von userspezifischer Werbefläche lässt sich dann deutlich mehr Geld verdienen. Manch einer wird dies zunächst positiv und kundenfreundlich beurteilen, vergisst dabei aber die weitreichenden Folgen. Zur Erstellung von den Profilen werden sogar teilweise die Inhalte der gesendeten Nachrichten ausgewertet, sodass an dieser

[7] https://www.zeit.de/datenschutz/malte-spitz-vorratsdaten (zuletzt abgerufen am 13.09.2018)

[8] Hier locken sogenannte Coupons als Vergünstigungen beim nächsten Einkauf.

Stelle schon sehr deutlich in die Privatsphäre der Person eingegriffen wird. Falls diese Daten dann auch noch nicht entsprechend gesichert und aufgrund von Datenpannen von andere Unternehmen oder Personen ausgewertet bzw. mit weiteren Daten verknüpft werden können, entstehen von den Nutzern genauere digitale Abbilder, als ihnen lieb sein kann (siehe Dachwitz et al. 2018).

2.2.3. Bewertung der eigenen Person

Auf Grundlage der oben beschriebenen digitalen Abbilder, entstanden aus Überwachung der Person, können nun Bewertungen der eigenen Person erstellt werden, ohne dass es einen persönlichen Kontakt gegeben haben muss. So suchen zum Beispiel Personalchefs von Unternehmen im Voraus Informationen über die Bewerber zusammen, um daraus eine mögliche (Nicht-)Einstellung abzuleiten. Fällt der Bewerber durch unvorteilhafte Fotos oder Äußerungen auf, welche eine Interpretation seiner Arbeitseinstellung ableiten lassen, kann daraus eine Ablehnung im Einstellungsverfahren erfolgen (vgl. Jaax 2016).

Weitere Bewertungen erfolgen beispielsweise im Kontext der Kreditwürdigkeit einer Person, das sogenannte Scoring, wie es etwa die *SCHUFA*[9] als privatwirtschaftliche deutsche Wirtschaftsauskunftei betreibt. Werden dort negative Informationen verknüpft, können für die betroffene Person höhere Kreditzinsen anfallen oder Verträge gänzlich verweigert werden. Des Weiteren sind auch im Gesundheitsbereich Datendeals denkbar, so können Gesundheits-Apps die Vitalwerte der Nutzer überwachen und darauf aufbauend mit den Krankenkassen gesonderte Tarife verhandelt werden, welche aber auch negativ für ungesund lebende Menschen ausfallen könnten. Dies lässt sich in Amerika beobachten, in Deutschland gibt es solch eine Überwachung bisher nur bei KFZ-Versicherungen im Bereich des Fahrverhaltens.

Alle Personen, mit denen man zukünftig in Kontakt tritt wie zum Beispiel Vermieter, Kollegen, Vorgesetzte etc., können bzw. könnten sich aus online zur Verfügung stehenden Informationen eine Meinung bilden, ohne dass man selbst die Möglichkeit hat, einen womöglich negativen Eindruck zu berichtigen. Dabei fällt vor allem die dauerhafte Speicherung von Daten im Internet sowie ein Objektivitätsverlust schwer ins Gewicht. Wenn noch vor 50 Jahren Begebenheit über die Zeit in Vergessenheit geraten sind, wird heute durch das Internet alles digital Veröffentlichte gespeichert, und durch die optimierten Suchmaschinen kann es leichter aufgefunden werden. Dadurch können negativ interpretierbare Bilder, welche bei Aktionen in der Kindheit und Jugend entstanden sind, das spätere (Berufs-)Leben beeinflussen, wie zum Beispiel bei Bewerbungen. Des Weiteren wird trotz der Datenfülle ein Mensch im Internet immer auf ein Abbild reduziert. Hier lässt sich Stachowiak

[9] https://www.schufa.de/de/

aufgreifen, der in seiner Abhandlung zum allgemeinen Modellbegriff Modelle als Abbildungen, Repräsentationen von Originalen beschreibt, vergleiche Definition von Abbildungsmerkmal in (Stachowiak 1973). So kann nach Stachowiak auch konstatiert werden, dass Modelle „im allgemeinen nicht alle Attribute des durch sie repräsentierten Originals, sondern nur solche, die den jeweiligen Modellerschaffern und / oder Modellbenutzern relevant scheinen, [erfassen].“ (Stachowiak 1973, S. 132) Dies beschreibt das Verkürzungsmerkmal von Modellen. Dadurch sind Bewertungen der eigenen Person auf Grundlage digital gefundener Daten immer unvollständig und aufgrund der Interpretation durch Algorithmen oder Personen auch subjektiv.

2.2.4. Gefahr vor den eigenen Daten

Schon 1997 beschreiben Egger und Schillinger die Gefahr vor eigenen Daten, denn „von Geburt an wird von allen möglichen Institutionen ein sogenannter Datenschatten über jede/n Einzelne/n angefertigt. In den Datenbanken entstehen daher Abbilder von Personen, die sich aus Informationen verschiedenster Bereiche zusammensetzen. Diese Beschreibungen besitzen im Vergleich zu früheren Methoden der Sammlung und Verarbeitung von Daten folgende, [im vorhergehenden Kapitel erörterten], Eigenschaften: Die Unvergesslichkeit, der Objektivitätsverlust, sowie die Präventivbeschuldigung.“ (Eckert 2013, S. 55) Das heißt, man muss sich auch vor den entstehenden Abbildern der eigenen Person schützen. Sind diese Abbilder fehlerhaft, unvollständig, irreführend oder sogar manipuliert, so entstehen auch falsche subjektive Interpretationen davon, und diese schränken uns in unserer Freiheit und der Lebensgestaltung ein bis hin, dass sie sogar zu Diskriminierung führen können.

Eine beispielhafte Einschränkung erfährt man, wenn es um Suchergebnisse geht, die auf den Suchenden zurechtgeschnitten sind. So entscheiden Computeralgorithmen darüber, welche Informationen uns noch zur Verfügung stehen, und es kann zur sogenannten **Filterblase** kommen. Die Filterblase besagt, dass man durch die Personalisierung nur noch Inhalte angezeigt bekommt, die (zumindest aufgrund der verwendeten Algorithmen) zu einem passen, und widersprechende Standpunkte nicht mehr erscheinen. So sieht man in Facebook beispielhaft nur noch News von gleichgesinnten Freunden oder Seiten, die man gelikt hat, die gleiche Standpunkte haben und repräsentieren (siehe Pariser 2011).

Um sich in den Abbildern, welche im ersten Abschnitt angesprochenen wurden, zumindest selbst wiederfinden zu können, bedarf es bei jeder persönlichen Preisgabe von Daten der Überlegung, inwieweit die Veröffentlichung zu einem Verschieben des digitalen Abbildes führen kann. So sollte man immer darauf achten, dass Daten außer Kontrolle geraten können. Wenn diese einmal veröffentlicht wurden, können sie von anderen kopiert und gespeichert werden und dadurch auch später wieder zum Vorschein kommen. Dabei müssen sie noch nicht einmal die Intention und Bedeutung behalten,

sondern können von anderen aus dem ursprünglichen Kontext gelöst und weiterverbreitet worden sein. Damit kann eine Veröffentlichung von Daten immer zu einem „Eigenleben“ dieser Daten führen, welches in der persönlichen Vorgehensweise berücksichtigt werden sollte (vgl. Müsgens 2015, S. 9). Eine mögliche Folgerung, deswegen möglichst gar keine Informationen preiszugeben, ist nicht unbedingt angeraten, sondern es sollte einem bewusst sein, dass die veröffentlichten Daten interpretiert und daraus falsche Schlüsse über die eigene Person gezogen werden können.

Allgemein kann zusammengefasst werden: Datenschutz hat einerseits die Funktion, die veröffentlichten Daten (sofern möglich) zu kontrollieren, sodass sie nicht in anderen als dem beabsichtigten Kontext verwendet werden, und andererseits eine ungewollte Veröffentlichung persönlicher Daten zu vermeiden. Dies hilft dabei, negativen Bewertungen aufgrund schlechter digitaler Abbildungen zu vermeiden und eine Überwachung der Person einzuschränken. Durch eine minimalistische Veröffentlichung persönlicher Daten werden auch Angriffspunkte für (kriminelle) Machenschaften reduziert.

2.3. Datenpreisgabe

In diesem Abschnitt soll herausgearbeitet werden, wie schützenswerte personenbezogene Daten in Umlauf geraten können. Hier kann in drei spezifische Kategorien unterteilt werden.

2.3.1. Kriminelle Energien

Seit Beginn der digitalen Datenverarbeitung gibt es Kriminelle, die versuchen Daten und Ressourcen von anderen abzugreifen oder zu beschädigen. Wo anfangs noch über portable Speichermedien, wie Disketten, Schadsoftware (engl. Maleware) verteilt wurde, folgte mit dem Internet eine leichtere Verbreitung über Webseiten oder per E-Mail. Maleware lässt sich in verschiedene Kategorien einteilen; hier soll nur auf vier typische eingegangen werden:

Ein **Virus**[10] ist eine „bösartige Software, welche Dateien infiziert, um sich zu verbreiten.“ (übersetzt aus Dunham und Abu-Nimeh 2009, S. 14) Das bedeutet, ein Virus ist eine Befehlsfolge innerhalb einer Datei, welche immer ein Wirtsprogramm zur Ausführung benötigt. Wird die Datei durch das Wirtsprogramm aufgerufen, so wird meistens eine Kopie (originalgetreu oder modifiziert) erstellt, sodass der Virus bei Weitergabe der Dateien sich verbreiten kann. Somit ist der Virus reproduktionsfähig. Neben dem Teil der Reproduktion enthält der Virus auch einen Schadensteil, der

[10] Synonym aus der Biologie

direkt, aber auch später durch eine Bedingung (wie zum Beispiel das Erreichen eines Jahrestages), ausgelöst werden kann (vgl. Fischer und Hofer 2011, S. 971).

Im Gegensatz zum Virus ist ein **Wurm** eine eigenständige Schadsoftware, das heißt, es wird kein Wirtsprogramm zur Ausführung benötigt. Der Begriff Wurm kommt durch die Verbindung von Programmteilen (auch Wurmsegmente genannt) zustande. Der Wurm reproduziert sich bei Ausführung wie ein Virus, hier bei findet meist eine Kommunikation zwischen den Wurmsegmenten statt. So verbreiten sich Würmer beispielswiese über Emailanhänge. Öffnete man diese Dateien, so replizierte sich der Wurm und versendet sich selbst an alle in der Adressdatei von des Emailprogramms gespeicherten Adressen. Der Schadensteil kann daraufhin gezielt Dateien auf der Festplatte zerstören oder durchsucht den PC nach gespeicherten Passwörtern. (vgl. Fischer und Hofer 2011, S. 1015)

Eine dritte Schadsoftware stellen **Trojaner**[11] dar. Ein Trojaner ist eine versteckte Schadsoftware, denn sie maskiert sich vordergründig als eine nützliche Software, um im Hintergrund Daten abzugreifen oder anderen Schaden zu verursachen. Ein Trojaner repliziert sich nicht selbstständig, sondern verteilt sich durch das manuelle Downloaden der User, welche die vordergründigen Angebote nutzen wollen. (Dunham und Abu-Nimeh 2009, S. 14; Heuer et al. 2009)

Trojaner, welche Daten abgreifen und an die Server der Kriminellen schicken, werden auch als **Spyware** bezeichnet. Spyware sind unerwünschte Programme, die meist eine Endbenutzer-Lizenzvereinbarung enthalten, welche sie dazu berechtigt, verschiedene unerwünschte Aktionen auszuführen. Die Installation solcher Programme erfolgt meist manuell, aber in der Regel unreflektiert durch den Benutzer, zum Beispiel als Anhang in einem Softwarepaket. Der Schadensteil beinhalten häufig Popup-Werbungen und zeichnet das Benutzerverhalten auf, um es an einen entfernten Server zu senden. (vgl. Dunham und Abu-Nimeh 2009, S. 13)

Neben expliziter Schadsoftware versuchen Kriminelle auch durch aktive Angriffe auf Webserver Daten zu erlangen. Die stupideste Variante dabei ist die **Bruteforce-Methode**, bei der in Login-Bereichen durch strukturiertes Ausprobieren ein Zugang gefunden werden soll. Strukturiert bedeutet, dass zuerst Standardpasswörter und häufig genutzte Passwörter, wie Wörter aus verschiedenen Lexika, durchprobiert werden, bis hin zum Ausprobieren aller Möglichkeiten von Zeichenkombinationen.

Durch solch kriminellen Machenschaften können Dritte in Besitz von personenbezogenen Daten gelangen. Jedoch ist dies nicht die einzige Quelle, durch die man seine Daten preisgibt. Die schnelle Entwicklung von Informationstechnik und den Gebrauch davon im Privaten macht es Datensammlern

[11] Der Begriff Trojaner leitet sich von der Sage um den Kampf Troja ab, welchen die Griechen durch die List mit dem Trojanischen Pferd, in dem Soldaten versteckt waren, gewannen.

einfach. Denn durch Soziale Netzwerke sowie das Bedienen von Smartphones mit einer Vielzahl an Apps, lässt man sich teils leichtfertig aushorchen und gibt sogar leichtfertig Daten preis.

2.3.2. Daten als Bezahlungsmittel

Im Internet gibt es viele Gratisdienste wie E-Mailanbieter, Suchmaschinen oder Soziale Netzwerke. Die Anbieter, welche die Dienste zur Verfügung stellen, verdienen auf andere Weise ihr Geld. So finanzieren sich die Dienste oft durch Werbeflächen. Ein noch höherer Gewinn lässt sich dann erzielen, wenn die Werbefläche nicht nur einer möglichst großen Anzahl an Personen präsentiert wird, sondern wenn sie die gewünschte Zielgruppe erreicht. Gerade Soziale Netzwerke können durch ihre Struktur, Menschen zu verbinden und ihnen dadurch Daten, wie Interessen und Vorlieben, zu entlocken, auf einen großen Datensatz zurückgreifen. Dabei werden die Daten häufig ganz bewusst, oft aber unreflektiert veröffentlicht. Denn möchte man andere Menschen mit ähnlichen Interessen finden, muss man zuerst seine Interessen preisgeben. Beispielsweise sammelt Facebook durch den Like-Button viele interessensbezogene Daten über ihre Nutzer, die alleingestellt keine große Aussage haben, aber in Verbindung mit anderen Daten große Wirkung entfalten können. Soziale Netzwerke und Webseiten sammeln neben den bewussten Eingaben auch andere Daten wie Verweildauer, Surfverhalten oder ähnliches und berechnen durch Algorithmen relativ gute Nutzerprofile (siehe Unterabschnitt 2.2.2 Überwachung). Somit steigern Unternehmen wie Facebook und Google durch personalisierte Werbung ihre Einnahmen. Eine andere Möglichkeit für die Unternehmen bietet der Datenhandel, denn Daten sind in der Wirtschaft viel Geld wert. Neben der personalisierten und zielgruppenorientierten Werbung können durch personenbezogene Daten auch personenbezogene Produkte entwickelt oder passende Bewerber ausgewählt werden. Dies kann bis zur Beeinflussung von Politik und Gesellschaft gehen (Rieger 2013; Saint-Mont 2013, 106 ff.; Wolf 2011).

In ähnlicher Weise finanzieren sich kostenlose Applikationen (Apps) für Smartphones. Die Apps benötigen gewisse Berechtigungen, um auf dem Smartphone zu funktionieren. Teilweise bedienen sich die Apps aber auch gewisser Berechtigungen, die sie für den eigentlichen Zweck nicht benötigen. Dies hat zum Zweck, Daten zu sammeln, welche sie (legaler Weise, da der User den allgemeinen Geschäftsbedingungen (AGB) zugestimmt hat) an den Programmentwickler weiterleiten. Das Problem daran ist, dass die AGB häufig nicht gelesen werden. Gründe hierfür sind in der Regel die Länge der AGB, deren Sprache (häufig in juristischen Phrasen geschrieben) sowie das Desinteresse der App-Nutzer. Apps wie Snapchat oder Musical.ly nutzen dies zu ihrem Vorteil. Snapchat beispielsweise ist eine App zum Versenden von Schnappschüssen (engl. Snapshot), welche mit Filtern, Effekten, Emojis und Texten aufgebessert werden können. Gerade bei Jugendlichen ist diese App sehr beliebt, da es eine kreative Messenger App ist, mit der man untereinander gut in Kontakt bleiben kann. Das anfängliche Versprechen, dass die Snaps (Fotos in Snapchat) nur für eine gewisse Zeit sichtbar sind und

danach „verschwinden“, verleitete zum Versenden persönlicher und teilweise sogar intimer Bilder. Schaut man sich jedoch die AGBs von Snapchat genauer an, sollte man bewusst entscheiden, welche Fotos man über die App senden möchte:

„…gewährst du der Snap Group Limited, Snap Inc. und ihren verbundenen Unternehmen, solange du die Services nutzt, eine weltweite, gebührenfreie, unterlizenzierbare und übertragbare Lizenz zum Hosten, Speichern, Verwenden, Anzeigen, Reproduzieren, Verändern, Anpassen, Bearbeiten, Veröffentlichen, und Verteilen aller Inhalte, die du an die Services übermittelst. Diese Lizenz wird ausschließlich zu dem Zweck erteilt, die Services zu betreiben, weiterzuentwickeln, zur Verfügung zu stellen, zu bewerben und zu verbessern sowie neue Services zu erforschen und zu entwickeln.“ (Snap Group Limited 2018)

Dies zeigt, dass Snapchat alle Daten, die übermittelt werden, auch zu seinen Zwecken verwenden darf. Hierbei ist gerade der Abschnitt „zum Zwecke erteilt, die Services zu betreiben“ sehr undifferenziert beschrieben, denn um den Service bereitstellen zu können, benötigt das Unternehmen Geld und kann dann, in weitem Sinne, dafür die Daten auch verkaufen.

Aber auch andere Apps wie Musical.ly[12], in dem Jugendliche zu Musikausschnitten Videos erstellen und versenden können, oder Instagram, eine ähnliche App wie Snapchat (nur ohne Zeiteinschränkung), verfahren genauso.

Gerade mobile Apps werden von Eckert als Gefahrenquelle gesehen, denn Smartphones sind heutzutage eine Art persönliche Informationszentrale und durch den always-on Status (vgl. Rack und Sauer 2018b) auch immer mit dem Netz verbunden (vgl. Eckert 2013, S. 88). Nebenbei können diese Miniatur-IT-Systeme durch die vielen Sensoren eine Menge an Daten produzieren, sodass Bewegungsprofile erstellt werden können. Dies vereinfacht es digital versierten Personen, auf persönlichen Daten zugreifen und in die Privatsphäre eindringen zu können.

Generell lässt sich konstatieren, dass gerade kostenlose, teilweise aber auch kostenpflichtige digitale Angebote wie Apps oder Soziale Netzwerke immer durch eine Datenpreisgabe bezahlt werden.

2.3.3. Freiwillige (unreflektierte) Datenpreisgabe

Andere bewusste Herausgaben von Daten finden in Kaufprozessen, in Anmeldungen bei Online-Diensten, bei denen gewisse Daten erforderlich sind, sowie häufig auch bei Gewinnspielen statt. Hierbei werden die Daten teils unreflektiert herausgegeben, denn häufig fordern die Formulare Daten,

[12] Im Verlauf wurde die App Musical.ly an die Firma Medienfirma Beijing Bytedance Technology verkauft und nun unter dem Titel Tik Tok vertrieben.

die nicht explizit für den spezifischen Prozess gebraucht werden. Trotzdem füllen viele Menschen die gegebenen Datenfelder aus. Auch so können Datensammler legal an weitere persönliche Daten gelangen (vgl. Ruff o.J.; Löbering 2014).

Weitere Datenpannen passieren Jugendlichen auch dadurch, dass sie einem bestimmten Freundeskreis Daten zukommen lassen wollen, aber aufgrund einer teils undurchsichtigen Veröffentlichungsreichweite einem zu großen Kreis an Personen die Daten bekannt geben. Aus den Medien wird dies immer wieder ersichtlich, siehe (Miklis 2011) und aktueller Bericht in den Fernsehnachrichten (hessenschau.de 2018).

2.4. Anwendung von Datenschutz

Wie in Kapitel 2.1 beschrieben steht das Recht auf **informationelle Selbstbestimmung** im Mittelpunkt des Datenschutzes. Es entstand als Erweiterung des allgemeinen Persönlichkeitsrechts, auch aufgrund von erheblichen Verfassungsbeschwerden gegen das Volkzählungsgesetz von 1983 (siehe Bundesverfassungsgericht, Urteil vom 15.12.1983).

Das Recht auf informationelle Selbstbestimmung besagt, dass niemand persönliche Daten ohne Zustimmung der betroffenen Person speichern, veröffentlichen oder weitergeben darf. Daraus resultiert auch, dass Betroffene, deren Daten verarbeitet werden, jederzeit das Recht haben eine Auskunft einzufordern, welche Daten in der Institution oder dem Unternehmen verarbeitet und gespeichert werden.

Nach Egger und Schillinger ist informationelle Selbstbestimmung auch die Freiheit auf Selbstdarstellung. Jeder mündige Bürger soll das Recht auf Individualität haben und eigenständig Einfluss auf seine soziale Umwelt in dem Maße nehmen können, dass er das Verhalten seiner Mitmenschen zu seinem Personenbild steuern kann. Dies ist aber nur möglich, wenn man selbst entscheiden kann, welche Informationen über einen existieren. „Durch das Recht auf informationelle Selbstbestimmung soll gewährleistet werden, dass der einzelne Bürger tatsächlich ein respektiertes Individuum im Gesellschaftsgefüge bleibt und nicht aus verschiedenen Daten zusammensetzbare Teile der Masse.“ (Egger und Schillinger 1997, S. 53)

Das Recht auf Selbstbestimmung ist aber nicht der einzige Passus in der deutschen Gesetzgebung. Die Datenverarbeitung wird auch explizit im Bundesdatenschutzgesetz (BDSG) geregelt. Das BDSG, herausgegeben vom Bundesministerium der Justiz und Verbraucherbildung, ist die nationale Umsetzung der europäischen Datenschutzgrundverordnung (Europäische Union 04.05.2016) (DSGVO), in der europaweite Regelungen bezüglich des Datenschutzes getroffen wurden. Diese europaweite Regelung ist in Zeiten der standortunabhängigen digitalen Dienstleistungen insofern wichtig, als dass

sich die Unternehmen durch ein Hosten ihrer Services in Ländern mit schwächeren Datenschutzgesetzen nicht aus der Verantwortung ziehen können. Die DSGVO beinhaltet neben allgemeinen Bestimmungen und Grundsätzen zum Thema *Datenschutz* auch Rechte von Betroffenen sowie Pflichten von datenverarbeitenden Institutionen.

Des Weiteren hat auch jedes Bundesland ein spezifisches Landesdatenschutzgesetz, so dass man sich als Betroffener auch an den Landesdatenschutzbeauftragten[13] wenden kann. In juristischen Datenschutzfällen sind auch andere Gesetze zurate zu ziehen, wie zum Beispiel das Teledienstgesetz, das Teledienstedatenschutzgesetz, das Telekommunikationsgesetz, die Telekommunikationsüberwachungsverordnung, das Telemediengesetz oder auch das Arbeitsrecht. All diese Rechtsvorschriften dienen dem Schutz personenbezogener Daten vor Missbrauch.

Zusätzlich dazu, dass Gesetze den (Daten-)Schutz der Bürger regeln, kann auch jeder selbst im Bereich des Schutzes seiner Daten aktiv werden. Jeder ist selbst verantwortlich, welche Daten er anderen zur Verfügung stellt und wie weit man sich online im positiven wie negativen Sinne präsentiert haben möchte. Um Datenschutz zu betreiben, kann man hierbei auch auf die Techniken der **Anonymisierung** und der **Pseudonymisierung** zurückgreifen. So bezeichnet Eckert Anonymisierung als „Verändern personenbezogener Daten der Art, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit großem Aufwand an Zeit, Kosten … einer bestimmten Person zugeordnet werden können." (Eckert 2013, S. 13). Pseudonymisierung ist eine schwächere Form der Anonymisierung. Hier nutzt man Pseudonyme, um ein Zuordnen der Daten zu einer natürlichen Person zu erschweren. Dabei liegt der Vorteil darin, dass die wissenden Akteure die Zuordnung zwischen Pseudonym und natürliche Person herstellen können, während unbeteiligte Dritte diese Verbindung nur schwer bis gar nicht nachvollziehen können. Während Pseudonyme durch Erstellung von Fake-E-Mailadressen und Nutzung von Spitznamen umsetzbar sind, muss man zur Anonymisierung auf Dienste, wie zum Beispiel VPN zur IP-Verschleierung, zurückgreifen. Anonymisierungsdienste kombinieren Vermeidungs- und Verschleierungstechniken, sodass keine Bewegungs-, Kommunikations- oder Zugriffsprofile einzelner Nutzer durch unautorisierte Dritte erstellt werden können (vgl. Eckert 2013, S. 13).

Zur weiteren Unterstützung kann man auf **Browsererweiterungen** wie AdBlocker, Ghostery, Lightbeam und andere zurückgreifen (vgl.Schallaböck, S. 6). Diese Erweiterungen lassen sich in verschiedene Kategorien einteilen. So blenden AdBlocker, wie Adblock plus, Werbeflächen auf Webseiten aus, sodass keine personalisierte Werbung angezeigt werden kann. Ghostery, Self-Destroying

[13] https://www.datenschutz.rlp.de/de/startseite/ (zuletzt abgerufen am 18.08.2018)

Cookies und Privacy Badger versuchen, eine Personalisierung dadurch zu vermeiden, dass Tracking-tools der Webseiten in ihrer Arbeit behindert und Cookies spätestens beim Schließen des Browsers gelöscht werden. Zusätzlich existieren Browsererweiterungen wie Lightbeam und FlagFox, welche zwar nicht aktiv zum Datenschutz beitragen, aber den Benutzer in seiner Entscheidung, Daten zu veröffentlichen oder die Veröffentlichung doch zu unterlassen, unterstützen. Dies erfolgt, indem sie anzeigen, wie viele Third Party Cookies die Webseite im Hintergrund lädt oder wo der Server, auf dem die Webseite gehostet ist, steht, sodass nachvollzogen werden kann, welches nationale Datenschutz-recht zugrunde liegt.

Ein weiterer Schritt, gerade gegenüber krimineller Datenerhebung, ist die Verwendung starker **Passwörter**. So empfiehlt das Bundesamt für Sicherheit und Informationstechnik mindestens folgende Kriterien einzuhalten: (vgl. Bundesamt für Sicherheit in der Informationstechnik 2011)

1. Das Passwort sollte gut merkbar sein, sodass es nicht notiert werden muss.
2. Das Passwort sollte aus mindestens acht Zeichen bestehen. Je länger, desto besser!
3. Das Passwort sollte aus Groß- und Kleinbuchstaben, Ziffern sowie Sonderzeichen bestehen.
4. Vermieden werden sollten Wörter, die in Lexika stehen, sowie gängige Varianten aus Tastaturmustern wie 123456
5. Änderung des Passwortes in regelmäßigen Abständen, mindestens einmal im Jahr.
6. Keine Mehrfachverwendung von Passwörtern bei verschiedenen Diensten.

Des Weiteren können auch sogenannte Passwort-Checker, wie der des Datenschutzbeauftragten im Kanton Zürich[14], genutzt werden um, die Stärke eines Passwortes zu ermitteln. Hier wird jedoch auch geraten, nur vergleichbare Passwörter einzugeben, denn man weiß nicht immer, wer hinter diesen Passwort-Check-Diensten steht.

Gerade der letzte Abschnitt lässt erkennen. wie wichtig die eigene Kompetenz der Person im Datenschutz ist. Daher wird im nächsten Abschnitt auf den Begriff der Datenschutzkompetenz – hier nach Hug und Grimm – vertiefend eingegangen.

2.5. Das Datenschutzkompetenzmodell nach Hug und Grimm

Der folgende Absatz bezieht sich auf den Artikel von Hug und Grimm im Tagungsband der INFOS[15] 2017. Darin beschreiben die Autoren ein **Datenschutzkompetenzmodell**. Sie nehmen dabei Bezug auf das *Medienkompetenzmodell* von Six und Gimmler (Six et al. 2007a) und ergänzen dieses um die

[14] https://www.passwortcheck.ch/passwortcheck/passwortchecko

[15] INFOS ist die zweijährig stattfindende Tagung des Fachausschusses Informatik und Schule der Gesellschaft für Informatik (GI e.V.).

Aspekte der Risikobewertung aus dem *Referenzmodell* von Grimm et al. aus dem Jahr 2016 für ein Vorgehen bei der IT-Sicherheitsanalyse (siehe Grimm et al. 2016).

Medienkompetenz stellt eine Grundlage von Datenschutzkompetenz dar, denn Datenschutz muss vor allem bei der Mediennutzung gewahrt werden. Dabei ist Medienkompetenz ein schwer zu definierender Begriff. Zumindest nach Six und Gimmler 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. 2007b, S. 281) Um diese genauer zu beschreiben unterteilen sie die Medienkompetenz in acht Dimensionen. Davon nehmen sich Hug und Grimm die datenschutzrelevanten Elemente heraus. So benötigt man, um Datenschutz anwenden zu können, grundlegend Hintergrundwissen. Neben den Gründen, warum Datenschutz wichtig ist, muss die Person in Situationen mit personenbezogenen Daten über die Vorgänge von Datenverarbeitung Bescheid wissen, sowie Gefahren kennen und diesbezüglich auch seine Rechte und Möglichkeiten kennen. Das Hintergrundwissen wird erweitert mit Orientierungswissen[16] in der spezifischen Situation, um datenschutzkonform handeln zu können. So muss der Person bekannt sein, dass es beispielsweise bei Onlinediensten, welche sie nutzen möchte, häufig Funktionen gibt, um personenbezogene Daten zu schützen. Aber auch das Wissen über die verschiedenen Tools zum Anonymisieren stellt ein Orientierungswissen dar. Neben den Wissensdimensionen benötigt die Person eine Auswahl- und Nutzungskompetenz, um reflektiert eine Auswahl zwischen Optionen, im Bereich von Tools oder Diensten sowie im Bereich von Einstellungsmöglichkeiten und so fort treffen zu können. Die Nutzungskompetenz beschreibt das Können der praktischen Umsetzung der getroffenen Auswahl. Auf Grundlage des Wissens und der Auswahl- und Nutzungskompetenz sollte die Person zu einem Urteil kommen, ob und in welchem Rahmen die Onlinedienste genutzt oder bestimmte Browser und Tools eingesetzt werden. Dies spiegelt sich in der Urteilskompetenz im Medienkompetenzmodell wieder.

Ergänzt man die beschriebenen Dimensionen um eine Dimension der Risikobewertung, so erhält man nach Hug und Grimm ein Datenschutzkompetenzmodell (vgl. Hug und Grimm 2017). Die Nutzung datenverarbeitender Dienste und damit des Internets basiert auf einer Wechselwirkung zwischen Selbstkontrolle, was macht der Nutzer und vor allem wie, und dem Vertrauen in die Dienste mit ihren Systemen und Akteuren. Vertiefende Erläuterungen zu Vertrauen finden sich in dem zugrundeliegenden Vertrauensmodell von Mayer et al. 1995, welches die Zusammenhänge beim Abschätzen, inwieweit man dem Gegenüber vertrauen kann, beschreibt. Die Einschätzung der

[16] Im Rahmen der weiteren Forschung zum Datenschutzkompetenzmodell wurden die beiden Wissensdimensionen vereint, da eine Differenzierung der beiden sich als schwierig erwies.

Vertrauenswürdigkeit von Diensten und Anbietern ist eine Grundlage der Risikobewertung. Zur Entwicklung des Begriffs der Risikobewertungskompetenz greifen Hug und Grimm auf Teile des Referenzmodells von Grimm et al. (2016) zurück, welches eigentlich für Entwickler von Sicherheitssystemen gedacht ist, jedoch auch auf die Einschätzung eines Nutzungsrisikos angewendet werden kann. Dabei werden nur die folgenden datenschutzrelevanten Aspekte genutzt.

Das Referenzmodell beruht auf einer Ist-Analyse, einer Potenzial-Analyse sowie der Entwicklung und Installation eines Sicherheitskonzeptes. Anhand eines Beispiels zum Thema „Senden eines Fotos in SnapChat“ soll der Ablauf der Risikobewertung zu einer Nutzung dieser App beschrieben werden. In der Ist-Analyse wird die aktuelle Situation bewertet. Grundlage dabei sind erstens die Güter, in diesem Fall das Foto mit all seinen personenbezogenen Daten. Zweitens fließen in die Risikobewertung das Vertrauen in die IT-Systeme, die Smartphones des Senders und Empfängers sowie die Server des Dienstanbieters ein. Auch die beteiligten Menschen, wie die schon erwähnten Sender und Empfänger sowie der Dienstleister, werden in der Situationsbewertung berücksichtigt. Als weitere Personen werden im Referenzmodell externen Dritten aufgenommen, die durch explizite Angriffe oder Lücken im System an die Daten gelangen könnten. Zwischen den Menschen kann es zu Interessenkonflikten kommen: So möchte der Sender das Foto eigentlich nur dem Empfänger zur Verfügung stellen, während der Empfänger das Foto weiterzeigen oder der Dienstanbieter das Foto eventuell auch als Werbung nutzen möchte. In der Ist-Analyse werden neben diesen Interessenkonflikten auch Schwachstellen der IT-Systeme beschrieben. So soll zwar bei SnapChat das Foto nach kurzer Zeit gelöscht werden, aber mit den Smartphones kann beispielsweise ein Screenshot gemacht werden, während das Foto angezeigt wird. Neben diesen bewussten Angriffen kann es aber auch beispielsweise zu Datenpannen im Bereich der Server kommen und das Foto ungewollt veröffentlicht werden. Diese Interessenskonflikte und Schwachstellen werden in der Potential-Analyse bewertet und in Relation zum gewünschten „Geschäftsziel“, hier besser Grund der Veröffentlichung, gesetzt. Daraus resultierend wird ein Sicherheitskonzept entwickelt, wie zum Beispiel nur weniger intime Fotos zu senden, die Einstellungsoptionen des Empfängerkreises zu berücksichtigen oder das Foto gar auf anderem Wege (siehe Auswahl- und Nutzungskompetenz) zu senden. Der letzte Schritt im Referenzmodell ist die Installation des Sicherheitskonzeptes. Im Sinne der Datenschutzkompetenz stellt dies die Umsetzung des Sicherheitskonzeptes sowie die Anwendung von Handlungsmustern dar.

Damit definieren Hug und Grimm „Datenschutzkompetenz als den 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)

3. Datenschutz als Unterrichtsthema

In Kapitel 1 wurde auf vorhandene Unterrichtsideen zum Thema *Datenschutz* verwiesen. An dieser Stelle werden nun einige Ideen exemplarisch vorgestellt, da auf diese in Kapitel 4 zurückgegriffen wird. Viele der hier aufgeführten Unterrichtsideen zum Thema Datenschutz sowie auch andere zu Themen rund um Digitalisierung sind unter klicksafe[17], einer EU-Initiative für mehr Sicherheit im Netz, gesammelt. Weitere Materialien zum Thema *Datenschutz* werden in der parallel laufenden Masterarbeit von (Makosch 2018) untersucht, kategorisiert und zusammengefasst.

3.1. Personenbezogene Daten

Die Reihe von klicksafe „Ich bin öffentlich ganz privat. Datenschutz und Persönlichkeitsrechte im Web." (Rack und Fileccia 2015) beginnt mit dem Thema personenbezogener Daten als Unterrichtseinheit. Die Schülerinnen und Schüler[18] sollen hierbei einerseits lernen, was personenbezogene Daten sind und andererseits erkennen, warum Datenschutz wichtig ist. Hierfür stellen die Autoren von klicksafe (Rack und Fileccia 2015, 43 f.) zwei Arbeitsblätter zur Verfügung. Die erste Aufgabe im Rahmen der Arbeitsblätter ist aus einer Auswahl an Daten solche zu identifiziert, welche einen Personenbezug haben. Nachdem dies jeder Schüler für sich getan hat, werden die Ergebnisse in Gruppen verglichen und ergänzt. Im Anschluss daran wird Antwort auf die Frage „Warum Datenschutz wichtig ist" innerhalb der Gruppe mit der Placemat Methode (siehe Brüning und Saum 2008, S. 25) erarbeitet. Die Placemat Methode fördert und strukturiert hierbei das Gruppengespräch, indem auf einem Plakat, welches auf dem Tisch liegt, jedem Gruppenmitglied ein Feld zugeteilt wird, welches zur eigenen Erarbeitung der Antwort genutzt wird. Anschließend hält die Gruppe das Gruppenergebnis in einem weiteren Feld in der Mitte fest. Auf dem zweiten Arbeitsblatt geht es um die persönliche Einschätzung, welche Daten privat bleiben sollten und welche Daten veröffentlicht werden können. Dazu sollen die Schüler die Typen von personenbezogenen Daten in die Kategorien „Auf jeden Fall privat" über „Nicht eindeutig" bis „Kann ich eventuell weitergeben" einsortieren. Am Schluss werden die Ergebnisse in der Klasse diskutiert und es wird gemeinsam erarbeitet, warum es teilweise keine genauen Grenzen zwischen „persönlich" und „zum Veröffentlichen geeignet" gibt.

Diese Unterrichtseinheit eignet sich zum Einstieg, da relativ langsam und einfach in das Thema eingeführt wird. Die Gruppenarbeit zum Thema Gefahren fußt auf keine Grundlage, sodass dies nur in

[17] https://www.klicksafe.de/themen/datenschutz (zuletzt abgerufen am 26.08.2018)

[18] Im Folgenden wird zur besseren Lesbarkeit das generische Maskulin verwendet, welches gleichermaßen die weibliche Form impliziert.

Lerngruppen mit Vorwissen gewinnbringend umsetzbar ist. Dagegen ist die letzte Aufgabe wieder für alle geeignet, da hier die Risikobewertungskompetenz und eigene Einschätzung abgefragt wird.

3.2. Schadsoftware

Im klicksafe Lehrerhandbuch findet sich ein Kapitel zum Thema Spam und Schadsoftware. (Fileccia et al. 2016, 205 ff.) Im Rahmen dieses Kapitels wird eine Unterrichtseinheit für die Klassenstufe 8 unter dem Titel „Ein ganzer Zoo im Computer und auf dem Handy“ skizziert. In der Einheit sollen die Schüler verschiedene Arten von Schadsoftware kennenlernen und fertigen dazu eine Übersicht an. Neben dem Erarbeiten von neuem Wissen soll auch die Basiskompetenz informatischer Bildung (Freis 2012) gestärkt werden. In diesem Fall lernen „Schülerinnen und Schüler […]neue Kommunikationstechniken zur Informationsbeschaffung sicher an[zu]wenden“ (Freis 2012, S. 10). Dazu sollen die Schüler zu dem gegebenen didaktisch reduzierten Überblick (siehe auch Anhang A. 11.1.) auf den Internetseiten von klicksafe.de[19] und dem Bundesamt für Sicherheit in der Informationstechnik[20] weitere Informationen zu Schadsoftware sowie Schutzmaßnahmen dagegen suchen. Die Autoren verweisen hierbei auf eine Vorarbeit sowie Hilfestellungen der Lehrkraft, da die Internetseiten regelmäßig aktualisiert werden und die Seiten auch sehr umfangreich sind. Im Anschluss an die Informationsrecherche sollen die Schüler dem Nachbarn oder der Nachbarin erklären, welche Schutzmaßnahmen sie gefunden haben. Die Autoren schlagen dazu die Methode „Partnerinterviews“ vor. In der letzten Aufgabe erfolgt die Sicherung durch die Erstellung eines Merkblattes mit den wichtigsten Informationen. In dieser Aufgabe wird erneut die Basiskompetenzen informatischer Bildung im Bereich Textverarbeitung gestärkt (Freis 2012).

Ausgehend von der guten Zusammenfassung verschiedener Schadsoftware kann den Schülern durch die dazugehörige Recherche entsprechende themenspezifische Internetseiten gezeigt werden. Eine Altersfestlegung auf die 8 Klasse liegt vermutlich an der Komplexität der Internetrecherche. Durch eine Reduzierung auf altersgerechte Seiten und Texte, kann diese Unterrichtseinheit aber auch schon früher stattfinden. An dieser Einheit lässt sich erkennen, wie neben der Vermittlung datenschutzrelevanten Inhalts auch durch die Methoden Medienkompetenz im Sinne informatischer (Grund-)Bildung erfolgen kann.

[19] www.klicksafe.de/themen/technische-schutzmassnahmen/den-pc-schuetzen/ (zuletzt abgerufen am 24.08.2018)
[20] https://www.bsi-fuer-buerger.de/ (zuletzt abgerufen am 24.08.2018)

3.3. Tracking

Zum Thema Tracking findet man eine Unterrichtseinheit in klicksafe to go – Datensatz Datenschatz (Haschler 2017, S. 13) für die Klassenstufen 6/7. Zum Einstieg in das Thema soll ein Filmausschnitt aus „Minority Report“ als stiller Impuls genutzt werden. In diesem wird der Protagonist in einer Einkaufsmall durch einen Iris-Scan identifiziert und erhält aufgrund dessen personalisierte Werbung. Im Anschluss an den Film wird die Lebenswelt der Schüler eingebunden, indem sie von eigenen Erfahrungen mit personalisierter Werbung berichten sollen. Um das Thema Tracking anschließend aufzuarbeiten, wird in der Unterrichtsstunde in einer „Live-Show“ durch die Lehrkraft das Firefox-Plug-In „Lightbeam“ (siehe Abschnitt 2.4) gezeigt. Anhand dessen wird ersichtlich, dass neben den Anbietern der besuchten Webseiten, auch Dritte im Hintergrund den durchgeführten Seitenaufruf erfahren. Um den Schülern den technischen Ablauf beim Surfen zu erklären, wird hier auf ein Rollenspiel (Haschler 2017, S. 18) zurückgegriffen, in dem vier Schüler die Akteure innerhalb eines Surfvorganges darstellen und nachspielen. Als optionale Zusatzaufgabe können die Schüler auf ihren eigenen Geräten nachschauen, welche Cookies gespeichert sind. Hierbei ist zu berücksichtigen, dass teilweise auch durch die Cookies relativ detailliert auf das Surfverhalten zurückgeschlossen werden kann. Daher empfehlen die Autoren, diese Aufgabe nicht in Gruppen zu machen. Nach dem Erkenntnisgewinn, was Tracking ist, sollen die Lernenden Schutzmaßnahmen erarbeiten. Dies soll zuerst in Einzelarbeit geschehen, um eine größere Menge an Maßnahmen abzuleiten. Haschler gibt dazu sechs beispielhafte Schutzmaßnahmen vor. Die Sicherung erfolgt dann durch das Zusammentragen der Ergebnisse und die sechste Schutzmaßnahme (Haschler 2017, S. 17), das Nutzen einer Proxy-Suchmaschine, kann anhand eines Vergleiches zwischen den Suchergebnisse der Suchmaschine Google und denen der Proxy-Suchmaschine Startpage vorgeführt werden. Zum Schluss oder als Hausaufgabe können Vor- und Nachteile von personalisierter Werbung erörtert werden. Dazu dienen zwei gegensätzliche Aussagen als Diskussionsgrundlage.

Der Filmausschnitt ist zwar von der Thematik sehr passend gewählt, jedoch ist er sehr kurz, sodass eine Erkenntnis der Schüler nicht unbedingt zu erwarten ist. Die Visualisierung von Traking beim Surfen durch Lightbeam ist eine gelungene Idee, hier die Schüler aber selbst aktiv werden zu lassen könnte noch gewinnbringender sein. Das Rollenspiel ist ein sehr einfaches und dadurch auch schülerverständnisvolles Modell von den Abläufen bei einem Seitenaufruf. Auf Grundlage dessen können die Schüler auch weiterdenken und Gefahren, die daraus resultieren können, erarbeiten.

3.4. Berechtigungen von Apps

Neben klicksafe bereitet auch der Webauftritt handysektor.de, ein gemeinschaftliches Projekt der Landesanstalt für Medien NRW und des Medienpädagogischen Forschungsverbundes Südwest (mpfs),

Datenschutzthemen insbesondere rund um das Smartphone jugendgerecht auf. So entstand aus der Kooperation von klicksafe und Handysektor ein Heft „Safer Smartphone“ (Rack und Sauer 2018a) in der Unterrichtreihe „Mobile Medien – Neue Herausforderungen“. In diesem Heft beschreiben die Autoren auf den Seiten 20 bis 24 ein Projekt zum Thema App-Berechtigungen. Auch hier ist der Einstieg ein stiller Impuls mit einem Erklärvideo[21] von Handysektor. Daran soll im Anschluss die Frage „Wozu sind bei Apps Berechtigungen nötig?“ aufgearbeitet werden. Des Weiteren soll den Schülern aufgezeigt werden, dass Apps, welche zu viele (nicht nötige) Berechtigungen einfordern, darauf abzielen, Daten sammeln zu können. Das Problem für Kinder und Jugendliche ist dabei, dass Berechtigungen nicht immer selbsterklärende Namen tragen. Um den Lernenden ein erstes Grundverständnis zu bieten, beginnt die Erarbeitung mit der Memory-Methode (vgl. Brenner und Brenner 2010, 250 f.). Im Memory-Spiel sollen den Berechtigungen die Erklärungen von Handysektor zu sortiert werden. Im Anschluss daran entscheiden die Schüler bei vier fiktiven, auf einem Arbeitsblatt beschriebenen Apps, ob sie diese herunterladen würden oder nicht. Auch hier findet als Sicherung ein Sammeln von Tipps statt, wie Kinder und Jugendliche die Kontrolle bei App-Berechtigungen behalten können. Die Autoren Rack und Sauer beschreiben vier Maßnahmen, die beispielhaft ergriffen werden können. Als Zusatzaufgabe überprüfen die Schüler ihre drei Lieblings-Apps auf deren Zugriffsberechtigung.

Am eigenen Gerät das Thema zu betrachten, kann eine große Motivation darstellen. Daher stellt sich die Frage, wieso dies nur als Zusatzaufgabe genutzt wird. Dagegen stellt das Memorie-Spiel nur eine verspielte Methode von Wissensaneignung dar, welche aber an dieser Stelle keine Verbindung zwischen Motivation und Lernstoff herstellen kann. Anhand der fiktiven Apps kann die Risikobewertungskompetenz gut evaluiert werden und ist somit eine geeignete Methode um die eigene Risikobewertungskompetenz einzuschätzen und zu verbessern.

3.5. Bewegungsprofil

Eine weitere Unterrichtseinheit, welche hier beschrieben werden soll, dreht sich um die Thematik von Bewegungsprofilen. Gerade in der heutigen Zeit trägt man mit dem Smartphone dauerhaft eine mit vielen Sensoren ausgestattete Wanze mit sich. So beschreiben Rack und Sauer in SaferSmartphone die Gefahren von Bewegungsprofilen und wie man sich dagegen wehren kann (Rack und Sauer 2018a, S. 13). Im Lehrerhandbuch von klicksafe findet sich dazu ein Unterrichtsentwurf zum Thema „Du und dein Smartphone: Ständige Kontrolle garantiert!“. In dem skizzierten Unterricht wird ein Arbeitsblatt bearbeitet, anhand dessen problematische Aspekte von Smartphones den Schülern aufgezeigt werden

[21] https://www.handysektor.de/artikel/handysektor-erklaert-was-sind-eigentlich-app-berechtigungen/ (zuletzt abgerufen am 09.09.2018)

sollen (Fileccia et al. 2016, S. 60). Den Einstieg bildet wieder ein Video von Handysektor, diesmal zu dem Thema Bewegungsprofil. Dazu werden dann in der ersten Aufgabe die Begriffe Smartphone, Funkzelle mit Funkmast, Netzanbieter, Wlan und GPS arbeitsteilig recherchiert und anschließend den Mitschülern erklärt. Vordergründig scheint an den Begriffen noch kein Datenschutzproblem ersichtlich. In der folgenden Aufgabe werden dann mit der Methode des Gruppenpuzzles die Begriffe in Fragen zusammengefasst. Hierunter fallen Fragen wie zum Beispiel: „Wieso ist jeder mit Smartphone unter „ständiger Beobachtung"?" oder „Was ist an einem Bewegungsprofil so problematisch". Spätestens an dieser Stelle sollte das Problem erkennbar werden. Als Vertiefung kann die Anfangsgeschichte aus dem Video weitererzählt werden und durch die Schüler in einer Fotostory oder einem kurzen Erklär-Video aufgearbeitet werden. Als Zusatzaufgabe nennen die Autoren noch das Erstellen eines Zeitstrahles zum Thema „Die Geschichte der Mobiltelefonie".

Das Video zum Einstieg ist ansprechend sowie fachlich sehr passend für die Unterrichtseinheit. Die Recherche der Begriffe ist nicht Datenschutz spezifisch und wird im Folgenden nicht weiter genutzt, aber die Aufgabe zu den Fragen kann später noch genutzt werden.

3.6. Rechtliches

In dem Zusatzmodul „Ich bin öffentlich ganz privat" von Rack und Fileccia findet sich eine weitere Unterrichtseinheit mit dem Titel: „Recht und Gesetz und meine Daten" (Rack und Fileccia 2015, S. 47). In dieser Einheit werden drei datenschutzrelevante Ausschnitte aus den, im Abschnitt 2.4 beschriebenen, Gesetzestexten aufgearbeitet. An fiktiven Beispielsituation mit dem Lehrer „Dr. Tafel" sollen die Schüler bestimmen, ob der Lehrer in den beschriebenen Situationen gesetzeskonform handelt. Im Klassengespräch können und sollten die Gesetze nochmals aufgearbeitet werden, denn gerade durch die juristische Schreibweise können Verständnisprobleme auftreten. Die beiden weiteren Aufgaben führen das Thema wieder auf die Lebenswelt der Schüler zurück. Hier sollen zuerst die wichtigsten Rechte herausgeschrieben und mit Beispielen aus facebook, YouTube oder Ähnlichem ergänzt werden. Danach sollen die Rechte mit den Beispielen von den Schülern auf einem Plakat mit dem Titel „Ich und das Gesetz" festgehalten werden. Für einen Ausblick ist das Arbeitsblatt noch mit einem Hinweis versehen, dass die Lernenden zum tieferen Verständnis von Datenverarbeitung in die allgemeinen Geschäftsbedingungen und die Datenschutzerklärung von beispielsweise facebook schauen sollen.

Die Aufarbeitung der Gesetzestexte ist sehr schülergerecht und sollte auch in einer sechsten Klasse genutzt werden können. Die Behandlung derer anhand Beispielen mit einem Lehrer tangiert auch die den Lernort Schule und ist somit motivierend. Inwieweit Schüler der sechsten Klasse die letzte

Aufgaben umsetzen können, hängt an der Frage, ob sie die Rechte auf ihre sozialen Netzwerke übertragen können. Hier muss man immer den Lern- und Leistungsstand der Gruppe beachten.

3.7. Passwörter

Fileccia et al. beschreiben in ihrem Lehrerhandbuch im Kapitel „8.1 Kritisches Surfverhalten und Passwörter“ (Fileccia et al. 2016, 229 ff.) unter anderem, wie wichtig starke Passwörter gerade im Bereich Datenschutz sind und was starke Passwörter ausmacht. Hierzu skizzieren die Autoren auch zwei Unterrichtsstunden für eine 8. Klasse zum Thema „Sichere Passwörter – wie geht das?“ Mit der Entzifferung einer Geheimbotschaft wird der Einstieg spielerisch gestaltet. Der nächste Arbeitsauftrag ist, selbst kreativ zu werden, eine Geheimsprache zu entwickeln und Partnerweise diese wieder zu entschlüsseln. Den Zusammenhang von Geheimsprache und sicherem Passwort präsentiert ein Infokasten auf dem Arbeitsblatt. So wird im nächsten Schritt ein System für Passwörter erarbeitet, welches starke Passwörter generiert, jedoch auch relativ einfach zu merken ist. Aufbauend auf diesem System sollen die Schüler ein eigenes System für die Erstellung von Passwörtern entwickeln, welches sie nutzen können und daher nicht mit den anderen austauschen sollten. Den Abschluss bildet eine Überprüfung der Passwortstärke. Hierbei wird der Internetdienst[22] von mecodia genutzt, die auch die Seite von Handysektor betreuen.

Diese Unterrichtseinheit steigt per Geheimbotschaft sehr spielerisch ein, führt aber bald auch zum Lerninhalt. Eine Altersbegrenzung ab der 8. Klasse ist nicht nachvollziehbar, da auch jüngere Schüler daran schon Spaß und Interesse haben. Eine Methode zur Passworterstellung sollte auch jüngeren Kindern an die Hand gegeben werden, und so kann auch der Abschluss mit der Passwortstärke in früheren Klassenstufen aufgegriffen werden.

3.8. Exkurs zur didaktischen und methodischen Unterrichtsplanung

Eine Unterrichtsplanung besteht aus zwei Teilen: Erarbeitung der Didaktik sowie methodische Überlegungen.
Didaktik ist die Wissenschaft und Lehre vom Lehren und Lernen, wobei in diesem Kontext die Spezifizierung auf Didaktik als Theorie der Lehr- bzw. Bildungsinhalte, ihrer Struktur, Auswahl und Zusammensetzung umgesetzt wird (vgl. Schubert und Schwill 2011, 12 f.). Dies beschreibt den „Versuch – über subjektive Theoriebildung hinaus – auf verschiedenen Ebenen mit unterschiedlicher Praxisnähe die Komplexität [von Unterricht und seinen Bildungsinhalte] gestaltend zu reduzieren und damit unterrichtliches Handeln rational planbar und kontrollierbar zu machen“ (Humbert 2006, S. 4).

[22] https://checkdeinpasswort.de/ (zuletzt abgerufen am 15.09.2018)

Der Planung liegt hierbei die Frage nach der Sache, die gelernt werden soll, zugrunde. Fachübergreifende Elemente des Themas können hier auch aufgezeigt werden.
In der Methodik hingegen wird die Frage „Wie gelernt wird“ beantwortet, indem sie die konkrete Planung und Durchführung des Unterrichts skizziert. „Sie beschreibt die Inszenierung des Unterrichts durch die zielgerichtete Organisation der Arbeit, durch soziale Interaktion und sinnstiftende Verständigung mit den Schülern. Handlungskompetenzen der Lehrer im Feld der Unterrichtsmethoden bezeichnen die Fähigkeit, in Unterrichtssituationen Lernprozesse für die Schüler auf dem Hintergrund der Rahmenbedingungen zu organisieren.“ (Humbert 2006, S. 4) Hierbei sollen auch Hürden und Schwierigkeiten aufgegriffen werden, welche durch die Auswahl einer passenden Methode oder Sozialform abzumildern gilt.

4. Didaktische und methodische Ausarbeitung

In diesem Kapitel soll eine Unterrichtsreihe mit dem Thema *Datenschutz* zur Verbesserung der Datenschutzkompetenz von Schülerinnen und Schülern der Klassenstufe 6 an einem Gymnasium entwickelt werden. Dies wird in Form einer Unterrichtsplanung dargestellt, welche auch erprobt und somit evaluiert wird.

Zur besseren Planung wurde eine Vorbereitungsumfrage durchgeführt, welche inklusive ihrer Ergebnisse im ersten Abschnitt vorgestellt wird. Daran orientiert sich dann auch die didaktische Planung des darauffolgenden Abschnitts. Da die Methodik, anders als die Didaktik, für die einzelnen Stunden differenziert betrachtet werden muss, wird sie Abschnitt 4.3. beschrieben. Dabei wird auch auf die Umsetzung der Stunden eingegangen, um Entscheidungen für die Folgestunde begründen zu können.

4.1. Vorbereitungsumfrage

Um den Unterricht an der Zielgruppe auszurichten, vergleiche Kapitel 7 in (Hartmann et al. 2007, S. 29), wurde eine Umfrage bei den Schülern der Lerngruppe durchgeführt, um ihre Interessen zu erfahren (siehe Anhang A. 1). Darin wurde nach der Benutzung von Computer und Smartphone sowie nach den meistgenutzten Internetseiten, Sozialen Netzwerken und Apps gefragt. Das Resultat der 26 Rückmeldungen sah folgendermaßen aus: Alle Schüler der Klasse besitzen ein eigenes Smartphone. Bei der Frage nach Computer gaben jedoch nur 58% an, einen eigenen Computer zu besitzen. Hier liegt jedoch die Vermutung nahe, dass Lernenden auch dann einen Computer angaben, wenn sie auf den elterlichen Rechner zurückgreifen können, denn laut der KIM-Studie (Feierabend et al. 2016, S. 28) besitzt nur jedes fünfte Kind einen eigenen Computer. Die Apps YouTube, WhatsApp, SnapChat und Instagram werden am meisten genutzt, wobei zu berücksichtigen ist, dass YouTube von zwei Dritteln der Klasse genutzt wird, während nur noch acht Personen Instagram als App verwenden. Ähnlich sieht es bei der Frage nach genutzten Internetseiten und Sozialen Netzwerken aus. Mit mehr als 75% ist YouTube Spitzenreiter, gefolgt von Instagram als Webseite mit 46%. Laut Umfrage war WhatsApp mit 38,5 % das dritthäufigste genutzte Soziale Netzwerk, wobei aus der Fragestellung „Welche drei Internetseiten / Soziale Netzwerke nutzt du am häufigsten?“ nicht ersichtlich wird, ob die Schüler WhatsApp nur als Soziales Netzwerk ansehen oder sogar die Anwendung im Browser nutzen. Zweiteres würde sich in einer gesteigerten Auswahl- und Nutzungskompetenz widerspiegeln. Gleiches gilt auch für Snapchat mit einer Nutzung von 30%, wobei es hier nur als Soziales Netzwerk genannt werden kann, da die Webseite nur eine Werbe und Dokumentationsfläche (für Datenschutzerklärung etc.) darstellt und keine weiteren Angebote bietet. Interessant ist auch, dass nur ein Drittel aller Umfrageteilnehmer Spiele als meistgenutzte App für das Smartphone angaben. Dies steht im

Widerspruch zur KIM-Studie (Feierabend et al. 2016, S. 54), wonach 44 Prozent der Kinder und Jugendlichen in diesem Alter Spiele auf dem Handy nutzen. Diese unterschiedlichen Daten können dadurch entstanden sein, da in der Umfrage nur nach den drei meist genutzten Apps gefragt wurde und somit YouTube, WhatsApp und andere Fotomessenger erstmal Priorität bei den Schülern haben. Zu der Frage „Was interessiert dich zum Thema *Datenschutz*?“ antworteten acht Schüler mit „Nichts“ bis hin zu „Mich interessiert das Thema allgemein nicht.“. Dies zeigt erstmal ein Desinteresse an dem Unterrichtsthema, sodass eine Motivierung der Schüler zum Thema am Anfang eine große Bedeutung hat.

Alle weiteren Ergebnisse der Vorbereitungsumfrage befinden sich im Anhang A2.

Auf Grundlage der Interessen der Schüler könnte eine mögliche Unterrichtsreihe, wie in den nächsten Abschnitten beschrieben, aussehen. Dabei müsste zur Adaption in andere Klassen der Unterabschnitt zur 4.2.2 Bemerkungen zu Lerngruppe sowie der Abschnitt 4.3. Methodische Planung auf die jeweilige Lerngruppe und die Umgebung angepasst werden.

4.2. Didaktische Unterrichtsplanung

In diesem Abschnitt wird der erste Teil der Unterrichtsplanung beschrieben. Dieser besteht aus den Hauptlernzielen, den Bemerkungen zur Lerngruppe, in der an dieser Stelle die Versuchsklasse beschrieben wird, der fachwissenschaftlichen Bemerkung sowie der didaktischen Analyse.

4.2.1. Bestimmung der Lernziele und Kompetenzen

Hauptlernziele

- Die Schülerinnen und Schüler können Grundbegriffe des Datenschutzes erklären.
- Die Schülerinnen und Schüler sind in der Lage, das Risiko in datenschutzkritischen Situationen objektiv einzuschätzen.
- Die Schülerinnen und Schüler beherrschen einen sensiblen Umgang mit ihren persönlichen Daten und können Handlungsmuster anwenden, um diese zu schützen.

4.2.2. Bemerkungen zur Lerngruppe

Der Unterricht erfolgt in einer sechsten Klasse des Hilda-Gymnasiums Koblenz im Fach Mathematik. Die Klasse besteht aus zwölf Schülern und zehn Schülerinnen im Alter von elf bis zwölf Jahren. Wie die in Abschnitt 4.1 vorgestellte Vorbereitungsumfrage ergeben hat, besitzen alle Schüler ein Smartphone und nutzen darauf vor allem die Apps YouTube, WhatsApp und SnapChat. Dem Thema *Datenschutz* scheint die Klasse eher abgeneigt zu sein (vgl. Abschnitt 4.1.). Trotz Desinteresse am Thema *Datenschutz* könnte jedoch die Erlaubnis der Handynutzung im Unterricht, trotz schulweitem Handyverbot, eine Motivation der Schüler darstellen.

Da der Autor die Klasse nicht vor der Erprobung kennen lernen konnte, bezieht er sich auf die Auskunft des Klassenlehrers: Die allgemeine Leistungsfähigkeit der Klasse liegt eher im Mittelmaß. Explizit wurde auf das etwas langsamere Lesetempo von einem Großteil der Klasse verwiesen. An sich folgen die Schüler dem Unterricht solange sie angeleitet und Rituale angewendet werden. Es muss darauf geachtet werden, dass Arbeitsaufträge bezüglich Arbeitsform, Inhalt und Methode klar formuliert sind, bevor die Schüler mit der Bearbeitung starten. Folgt der Unterricht nicht einer Linie, so müssen die Schüler des Öfteren ermahnt und zum Weiterarbeiten aufgefordert werden.

Andererseits ist der Autor auch der Klasse als Lehrperson unbekannt, sodass ein Interesse an der neuen Person vorliegt. Er bringt durch sein Lehramtsstudium der Fächer Informatik und Mathematik sowie durch seinen Nebenjob als wissenschaftliche Hilfskraft von Herrn Hug Kompetenzen im Bereich Unterricht und Datenschutz mit.

Den Schülern soll die Methode der Stationenarbeit, laut Klassenlehrer, bekannt sein, sie wurde zumindest schon zweimal von ihm eingesetzt. Da später auf diese Methode zurückgegriffen werden soll, stellt dies eine wichtige Information dar.

Dadurch, dass die Klasse dem Autor im Vorhinein unbekannt war, lässt sich auf die Lerngruppe an dieser Stelle nicht weiter eingehen. Im Nachgang kann erwähnt werden, dass die Klasse die Lehrperson respektierte. Es gab auch eine Gruppe von fünf Jungen, die durch ihr Verhalten den Unterricht stellenweise störten. Dies wurde einerseits durch die Methodik, vgl. Abschnitt 4.5, und andererseits durch eine veränderte Sitzordnung unterbunden.

4.2.3. Fachwissenschaftliche Bemerkungen

Die fachwissenschaftliche Bemerkung wurde in Kapitel 2 intensiv erarbeitet. An dieser Stelle sollen nur noch einmal folgende unterrichtsrelevanten Begriffen und Zusammenhänge erwähnt werden:

Als persönliche Daten (oder auch personenbezogene Daten) werden jegliche Informationen bezeichnet, die natürlichen Personen zuordenbar sind. Die Gefahr für die Person bei der Veröffentlichung ihrer personenbezogenen Daten besteht darin, dass sie überwachbar und dadurch manipulierbar wird, sowie durch kriminellen Missbrauch der Daten finanziell oder auch immateriell geschädigt werden kann. Kriminelle Zugriffe auf Daten können durch Viren, Trojaner und andere Maleware entstehen. Heutzutage werden viele persönliche Daten aber auch legal gesammelt. So gibt ein Smartphone-Nutzer bei Verwendung einer App dieser, gegebenenfalls, die Berechtigung auf gewisse Bereiche des Smartphones und damit auf gewisse Daten, wie Kalender oder Kontaktdaten, oder Sensoren, wie die Kamera, zuzugreifen. Nicht immer sind diese Berechtigungen für den Gebrauch der App jedoch notwendig.

In Zeiten des Internets werden auch viele Daten beim Surfen preisgegeben. Webseiten- und Dienstanbieter tracken die Zugriffe der Webseitenbesucher, in dem sie die Besucher zum Beispiel durch Cookies, welche auf dem Rechner abgelegt werden, wiedererkennen und dies teilweise nicht nur in Bezug auf der konkreten Webseite, sondern auch über Webseiten hinweg. Um sich gegen die Gefahren zu schützen, gibt es Ansätze zum Selbstdatenschutz, zum Beispiel bewusste Entscheidungen zur Veröffentlichung treffen, Berechtigungen bei Apps beachten, Privatsphäre-Einstellungen in Sozialen Netzwerken anpassen und das Nutzen von Tools wie Adblocker, Ghostery, Self Destroying Cookies, FlagFox und ähnliche. Bei Login-Vorgängen ist die Verwendung von starken, individuellen Passwörtern zu beachten. Neben dem Bereich des Selbstdatenschutzes, können die Daten der Benutzer von Systemen auch durch Systemdatenschutz geschützt werden, worauf die einzelne Person jedoch keinen Einfluss hat. Des Weiteren werden die Rechte der Bürger zum Datenschutz durch Gesetze wie die Datenschutzgrundverordnung (DSGVO), das Bundesdatenschutzgesetzt (BDSG), sowie das Landesdatenschutzgesetz (LDSG) festgelegt und gestärkt.

Einen weiteren fachwissenschaftlichen Inhalt stellt die Kombinatorik dar. So lassen sich zum Beispiel aus der Stellenanzahl eines Passwortes sowie den möglichen Zeichen die Anzahl an Möglichkeiten für das Passwort berechnen.

4.2.4. Didaktische Analyse

a. Legitimation

Datenschutz ist ein fachungebundenes Thema und im Kontext von fächerübergreifender Medien- und Verbraucherbildung zu finden. Aufbauend auf dem Strategiepapier „Bildung in der digitalen Welt“ der Kultusministerkonferenz (KMK), entwickelte diese dazu auch einen Kompetenzrahmen, in dem der Datenschutz unter „4. Schützen und sicher Agieren“ (Kultusministerkonferenz 2016, S. 17) aufgegriffen wird. Dabei soll jedes einzelne Fach, mit seinen spezifischen Zugängen zur digitalen Welt, zur Entwicklung von Kompetenzen für die digitale Welt beitragen. Auf Länderebene wird dies unterschiedlich umgesetzt.

Das Land Rheinland-Pfalz greift diese Kompetenzentwicklung einerseits in den Lehrplänen vieler Fächer auf, andererseits sind die Schulen in Rheinland-Pfalz verpflichtet ein eigenes Konzept zum Kompetenzerwerb in der Medienbildung zu erarbeiten (vgl. Groß et al. 2014, S. 8). Festgeschrieben ist dies auch im Orientierungsrahmen Schulqualität im Bereich *Unterricht* und der Dimension *Fachlichkeit und Kompetenzerwerb*: „Lehrerinnen und Lehrer führen über die gesamte Schulzeit hinweg Schülerinnen und Schüler an den reflektierten Umgang mit digitalen Medien heran, [und] fördern in allen Fächern den systematischen Erwerb digitaler Kompetenzen (und dokumentieren diesen im Medienkomp@ss, der für die allgemeinbildenden Schulen zur Verfügung steht)“ (Ministerium für Bildung 2017, S. 8). Dies ist zwar allgemein formuliert, Datenschutz ist aber Teil eines reflektierten Umgangs und stellt eine digitale Kompetenz dar.

Der genannte Medienkomp@ss beinhaltet grundlegende Kompetenzen der Medienbildung, so werden im Bereich *Analysieren und Reflektieren* auch folgende datenschutzrelevanten Kompetenzen erwartet: Die Schülerinnen und Schüler sollen „den Einfluss von Medien auf Wertvorstellungen, Handlungsweisen, Konsumverhalten [bewerten] und … sozial verantwortlich mit Medien um[gehen] … . [Die Schülerinnen und Schüler] sind umfassend über Manipulations- und Missbrauchsmöglichkeiten [… informiert] und kennen Anlaufstellen und Beratungsangebote [sowie] reflektieren ihre Medienerfahrungen und beurteilen den eigenen Umgang mit Medien. [Dabei] beschäftigen [sie] sich mit den Phänomenen der Mediengesellschaft, der Rolle der Medien als Wirtschaftsfaktor und Sozialisationsinstanz“ (Groß et al. 2014, S. 13)

Neben der Handreichung zur Medienkonzeptentwicklung gab das Land Rheinland-Pfalz schon 2010 Richtlinien zur Verbraucherbildung heraus (Ministerium für Bildung, Wissenschaft, Jugend und Kultur Rheinland-Pfalz 2010b), in dem Datenschutz als Kernbereich der Verbraucherbildung aufgegriffen wird. Verbraucherbildung soll dabei in allen Schulstufen und allen Bildungsgängen sowie allen Fächern verankert werden. Explizit verweisen die Richtlinien darauf, dass für „eine wirksame Integration von Fragen der Verbraucherbildung in ein schlüssiges Konzept schulischer Bildung […] eine verstärkte

Kooperation der Fächer [notwendig ist].“(Ministerium für Bildung, Wissenschaft, Jugend und Kultur Rheinland-Pfalz 2010b, S. 16). Eine Zuordnung zu gewissen Fächern findet daher nicht statt. Für die Sekundarstufe I werden aber die gesellschaftswissenschaftlichen Fächer als Hauptträger herausgestellt sowie Anknüpfungspunkte zu den Fächern Religion / Ethik genannt. Weiterhin werden auch, gerade beim Kernbereich Datenschutz relevant, das Fach Informatik beziehungsweise der Bereich der Informatischen Bildung angesprochen.

Im Bereich der informatischen Bildung werden von rheinland-pfälzischen Schülern folgende Kompetenzen erwartet: „Die Schülerinnen und Schüler können den Begriff *Informationssicherheit* erläutern sowie auch die Bedrohung durch Computer-Viren richtig einschätzen und sich davor schützen. […] Sie geben Auskunft über das Urheberecht und das Datenschutzgesetz ihres Landes“ (Freis 2012, S. 9)[23] Hier werden diese Kompetenzen jedoch erst ab der Klassenstufe 9 erwartet. Wie aber in Kapitel 1 beschrieben, scheint dies mit der heutigen Entwicklung im Bereich der Smartphone-Nutzung von Kindern und Jugendlichen zu spät. Daher sollten diese Kompetenzen schon früher gestärkt und vorausgesetzt werden.

Mit den Fachlerninhalten beschäftig sich grundlegen die Fachdidaktik. So hob Hubwieser, als Fachdidaktiker der Informatik, Datenschutz als einen informatischen Lerninhalt hervor (vgl. Hubwieser 2007, S. 81). Diesen sah er im Bereich *Interpretation von Repräsentationen* verankert, sodass auch innerhalb dieser Fachdidaktik das Thema *Datenschutz* legitimiert wird. Die Forschung der Fachdidaktiker fließt in die Bildungsstandards ein.

Somit findet sich Datenschutz auch in den Bildungsstandards der Informatik wieder. Im Bereich *Informatik, Mensch und Gesellschaft* steht folgender Abschnitt zum Thema *Datenschutz*: 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. 2008, 49 f.)Aber auch im Lehrplan der Informatik für die Sekundarstufe 1 sind folgende Kompetenzerwartungen aufgenommen: „Rechtliche Aspekte beim Umgang mit Information beachten“ (Ministerium für Bildung, Wissenschaft, Jugend und Kultur Rheinland-Pfalz o. J., S. 13) sowie „Datenerhebungen unter dem Aspekt Datenschutz bewerten“ (Ministerium für Bildung, Wissenschaft, Jugend und Kultur Rheinland-Pfalz o. J., S. 25). Da Informatik in Rheinland-Pfalz kein Pflichtfach ist, werden dieselben Kompetenzbeschreibungen auch im Lehrplan der Sekundarstufe II aufgegriffen. So findet sich die

[23] „Auskunft geben“ ist nach der Fachdidaktik kein Operator; Die Messung, ob der Erwartungshorizont erreicht wurde gestaltet sich schwierig und was hinter dem Begriff „Auskunft geben“ als Handlung genau erwartet wird, ist nicht eindeutig.

gleiche Wortwahl wieder im Teil des Grundfaches unter dem Inhaltsbereich „Information und ihre Darstellung“ (vgl. Ministerium für Bildung, Wissenschaft, Jugend und Kultur Rheinland-Pfalz 2010a). Im Leistungsfachteil, der die Inhaltsbereiche des Lehrplans der Sekundarstufe I voraussetzt, findet sich die Vertiefung des Themas *Datenschutz* im Inhaltsbereich „Wechselwirkungen zwischen Informatiksystemen, Individuum und Gesellschaft“. Betrachtet man Informatik als Fach, indem das Thema *Datenschutz* fachlich vermittelt werden soll, so zeigt sich daran die Problematik, dass Informatik frühestens und auch nur freiwillig in der neunten Klasse belegt werden kann. Da, wie in Kapitel 1 beschrieben, die Datenschutzkompetenz schon früher im Schüleralltag benötigt wird und auch allgemeine Bildung sein soll, muss diese Kompetenz in anderen (Pflicht-)Fächern schon aufgegriffen werden.

In anderen Fächern hat das Thema *Datenschutz* zumindest über die Verbraucher- und Medienbildung Einzug erhalten. Der Lehrplan der Sekundarstufe I Deutsch verweist zwar noch[24] darauf, dass „Medienerziehung … nicht allein Aufgabe des Deutschunterrichts sein [kann], doch hat gerade er [der Deutschunterricht] sich im Sinne des erweiterten Lern- und Textbegriffs mit den neuen Qualitäten des Sehens und Handelns auseinanderzusetzen. Ein medienkundliches Wissen gehört selbstverständlich dazu, doch liegt der Schwerpunkt fachlicher und pädagogischer Bemühungen darin, junge Menschen so zu stärken, dass sie im Umgang mit Massenmedien denk- und handlungsfähig werden“ (Ministerium für Bildung, Wissenschaft und Weiterbildung 1998, S. 30).

Dahingehend liefert der Lehrplan der Sekundarstufe I für Ethik einen vertieften Einblick in Datenschutz. Im Rahmen der Lebenssituation „Umgang mit PC-Welten“ beschreibt er die „Bereitschaft [der Schüler und Schülerinnen], den Umgang mit Daten verantwortlich zu gestalten … [sowie die] Bereitschaft, sich mit den Chancen und Risiken der neuen Informationstechnologien für ein selbstbestimmtes und gelingendes Leben auseinander zu setzen“ (Ministerium für Bildung, Wissenschaft und Weiterbildung RLP 2000, S. 71). Vergleicht man dazu die Lehrpläne der Sekundarstufe I für evangelische und katholische Religion, so zeigt sich, dass hier der ethische Aspekt vom Thema *Datenschutz* nicht aufgegriffen wird. Daran wird die Problematik erkennbar, dass Datenschutz zwar in der Bildung vermittelt wird, aber nicht jeder Schüler in gleichem Maße Erfahrungen dazu sammeln kann. Auch der Lehrplan Sekundarstufe I der Sozialkunde greift Datenschutz als Grundbegriff im Themenfeld „Leben in der Mediengesellschaft“ auf (vgl. Ministerium für Bildung, Wissenschaft, Weiterbildung und Kultur 2016, S. 154), wobei an dieser Stelle die zeitliche Einführung des Faches Sozialkunde erst zur siebten Klasse zu erwähnen ist.

[24] Der Lehrplan ist von 1998, sodass gerade mit Blick auf den technischen Fortschritt eine Überarbeitung des medienbezogenen Teils anstehen sollte.

b. Interdependenz der Unterrichtsreihe

Die Unterrichtsreihe wird innerhalb des Faches Mathematik direkt nach den Sommerferien praktisch umgesetzt. Daher muss und kann auch nicht auf ein vorheriges Thema eingegangen werden.

Die nun einsetzende Unterrichtsreihe *Datenschutz* hat folgende Schwerpunkte:

- Das Erkennen von persönlichen Daten sowie das Schaffen eines Bewusstseins für die Gefahren durch deren Verarbeitung,
- Das Herausbilden eines Verständnisses für die Funktionsweise von Schadsoftware und die Vermittlung von empfohlenen Schutzmaßnahmen,
- Das Durchschauen der Problematik von zu vielen Berechtigungen bei Apps und dem damit verbundenen, nicht offensichtlich zugestimmten Sammeln von Daten,
- Das Wissen über die Erstellung von Bewegungsprofilen und der davon ausgehenden Gefahr der Überwachung,
- Die Erkenntnis der Funktion von Cookies und dem Browserverlauf zur Erstellung von Profilen,
- Das Kennenlernen von Tools zum Selbstdatenschutz,
- Das Vermitteln von Rechten und Gesetzen im Datenschutz für die Verbraucher,
- Sowie die Erarbeitung von Regeln zu Passwörtern, um die Sicherheit von Daten in Onlinediensten zu erhöhen.

Das letzte Thema Passwörter bietet eine gute Verknüpfung zum Fach Mathematik. So möchte die Fachlehrkraft im Anschluss das Thema Kombinatorik erarbeiten, weshalb die Reihe mit diesem Unterrichtsthema, welches auf Kombinatorik aufbaut, enden kann.

c. Relevanz des Unterrichtsgegenstands

Durch die fortschreitende Entwicklung von digitalen Geräten und die immer frühere Nutzung dieser im Kindesalter muss die Datenschutzkompetenz frühzeitig gelernt und gestärkt werden. Wie beispielsweise in der Vorbereitungsumfrage bereits ermittelt, besitzen alle Schülerinnen und Schüler dieser Lerngruppe ein Smartphone. Auch zeigt die KIM-Studie von 2016, dass mehr als 50% der Kinder in diesem Alter täglich Nachrichten mit ihren Smartphones verschicken (vgl. Feierabend et al. 2016, S. 16) sowie mehr als 80 % nutzen das Internet mindestens einmal wöchentlich (vgl. Feierabend et al. 2016, S. 34). Dadurch kommen diese auch in ihrem Alltag regelmäßig in Kontakt mit datenverarbeitenden Diensten und sollten daher einerseits die Schutzrelevanz von personenbezogenen Daten aufgrund verschiedener Gefahren erkennen, aber vor allem auch die Kompetenz zur Gefahrenminimierung und zur Anwendung von Schutzmaßnahmen haben. Diese Kompetenzen zu entwickeln, ist im Rahmen der Medien- und Verbraucherbildung in Rheinland-Pfalz Aufgabe aller Fächer und sollte durch einen Medienplan der Schule fest vorgeschrieben sein.

d. Didaktische Konzeption

In dieser Unterrichtsreihe sollen die Schülerinnen und Schüler in ihrer Datenschutzkompetenz gestärkt werden. Dazu muss zuerst ein Verständnis für Datenschutz hervorgerufen und eine Definition der Thematik geliefert werden. Daher steigt die erste Stunde mit der Erarbeitung der Begriffe von persönlichen Daten und Datenschutz ein. Zudem muss auf die Gefahren bei missbräuchlicher Verwendung von persönlichen Daten eingegangen werden. Ein Zugang wäre über Zeitungsberichte von Datenschutzpannen und deren Folgen möglich. Da die Klasse jedoch in der Texterarbeitung noch recht langsam ist, wird dieser Zugang verworfen. Stattdessen wird das Interesse der Klasse an der unbekannten Lehrperson ausgenutzt und so sollen personenbezogene Daten über die Lehrkraft herausgearbeitet werden (vergleiche dazu Anhang A3 erste Folie). Erstes Ziel stellt somit das Erkennen personenbezogener Daten dar, welche kategorisiert gesammelt werden. Anhand der erarbeiteten Liste von personenbezogenen Daten, sollen die Schülerinnen und Schüler begründet entscheiden, ob sie diese veröffentlichen würden oder nicht.

In einem folgenden Schritt kann dann die persönliche Einschätzung mit dem Grundtenor der Klassengemeinschaft verglichen werden, anhand dessen herausgearbeitet wird, dass es unterschiedliche Ansichten über Privatsphäre und Schutzrelevanz gibt und dass eine generelle Zurückhaltung bei Datenveröffentlichung zu empfehlen ist.

Diese theoretische Erarbeitung bringt jedoch, neben der Motivation etwas über die Lehrkraft zu erfahren, noch nicht die nötige Motivation für das Thema *Datenschutz* hervor. Daher wird im Anschluss daran anhand eines Alltagsbeispiels aus der Lebenswelt der Schüler das Interesse geweckt. Hier lohnt sich als motivationaler Faktor der Einsatz des Smartphones im Unterricht. Der Bezug zur Lebenswelt entsteht, indem an einer von den Schülerinnen und Schüler genutzten App gezeigt wird, wie die Nutzer die Datenverarbeitung der App einschätzen und wie die App laut allgemeinen Geschäftsbedingungen Daten verarbeiten darf. In dieser Stunde wird dazu die App SnapChat verwendet, da diese in der Klassenstufe immer häufiger verwendet wird und aus den Allgemeinen Geschäftsbedingungen von SnapChat ein hohes Risiko bezüglich unsachgemäßer Datenverarbeitung hervorgeht. Wie vormals schon genannt, sollte auf Grund des langsamen Leseverständnisses nur auf die themenrelevanten Absätze in den Allgemeinen Geschäftsbedingung eingegangen werden (siehe

Anhang A. 3. zweite Folie). Snapchat verwendet persönliche Fotos und Stories, um daraus Werbeclips für den eigenen Dienst zu kreieren. Vom spezifischen Fall kann dann auf generelle Onlinedienste und deren Art und Weise von Datenverarbeitung wieder verallgemeinert werden.

Durch den Alltagsbezug und dadurch vorhandenen Vorkenntnissen zu den Apps werden bei den Schülerinnen und Schüler vermutlich viele Fragen aufkommen, die für die Folgestunden gesammelt werden können, um das motivationale Interesse zu erhalten. Neben der nun exemplarisch kennengelernten Gefahr, dass persönliche Daten auch anders verwendet werden können, als dies im Sinne der betroffenen Person ist, erarbeiten die Schülerinnen und Schüler auch andere Gefahren, die im Rahmen von veröffentlichten persönlichen Daten zu befürchten sind. Dies kann je nach Länge der vorhergehenden Diskussion aus Zeitgründen auch in die Hausaufgaben verschoben werden.

Für die nächste Stunde wird eine Doppelstunde geplant. In dieser soll Grundlagenwissen von verschiedenen datenschutzrelevanten Themen aufgearbeitet werden. Hierbei können aber nicht alle Themen von Adresshandel bis Zusatztools, die den Bereich Datenschutz tangieren, in ihrer komplexen Tiefe erarbeitet werden. Daher wird auf Stationenarbeit zurückgegriffen, welche im Abschnitt der Methodik genauer beschrieben wird, um den Schülerinnen und Schülern ein breites Angebot aus verschiedenen Themenbereichen bieten zu können und sie somit einen ersten Überblick über die Thematik Datenschutz erhalten. Durch die Stationenarbeit wird auch eine Binnendifferenzierung nach Interessen ermöglicht. Das Grundlagenwissen zum Thema *Datenschutz* wird aus Zeitgründen von 90 Minuten auf folgende sechs Einheiten didaktisch reduziert, sodass für jede Einheit zehn bis fünfzehn Minuten geplant werden können. Die Themen ergeben sich aus der Auswertung der noch unveröffentlichten Studie von Hug bezüglich seines Datenschutzkompetenzmodells. (Hug 2018b) Bei diesen Themen scheinen die Schülerinnen und Schüler dieser Altersklasse noch Wissenslücken aufzuweisen.

Im Folgenden werden die sechs Einheiten und ihre Zusammenhänge kurz dargestellt:

Bei der Einheit *Viren und Trojaner* lernen die Schülerinnen und Schüler eine Grundauswahl an Schadsoftware kennen, mit der sie im Alltag in Kontakt kommen könnten, und erarbeiten sich dazu Handlungsmaßnahmen, wie man sich gegen diese Gefahren schützen kann. Explizit stehen dabei Viren und Trojaner im Vordergrund, da Viren die größte Verbreitung haben und Trojaner eine Ähnlichkeit zu Apps aufweisen, welche vordergründig einen Nutzen haben, im Hintergrund aber durch zu viele Zugriffsrechte Daten sammeln können.

Dabei kann dann von den Schülerinnen und Schülern eine Verbindung zur Einheit zum Thema *Berechtigungen von Apps* gezogen werden. In dieser Einheit sollen die Schülerinnen und Schüler den

Sinn der Berechtigungsvergabe verstehen und auf ihren Smartphones nachschauen, welche Berechtigungen ihre Lieblings-Apps beanspruchen.
Dabei das eigene Handy nutzen zu dürfen, ist ein großer Motivationsfaktor. Im Anschluss daran soll dann die Urteilskompetenz bezüglich Apps gestärkt werden. Da zu dieser Aufgabe eine Musterbeschreibung vorliegt und die Lernenden am Ende nicht einfach nur die Lösung in ihren Alltag kopieren sollen, sondern selbstkritisch mit den eigenen Apps arbeiten sollen, werden in dieser Aufgabe nur fiktive Apps bewertet.

Ein weiterer Zusammenhang besteht dann zur Einheit, welche explizit die Berechtigung des Zugriffs auf den Standort/Ortungsdienst in den Mittelpunkt stellt. Hierbei sollen die Schülerinnen und Schüler nachvollziehen, wie viel ihr Handy über sie verraten kann, wenn sie es nur mit sich führen. Die Lernenden definieren den Begriff *Bewegungsprofil* und lernen welchen Gefahren sie sich dadurch aussetzen. Sollte mehr Zeit zur Verfügung stehen, könnte diese Einheit von dem Grundbegriff Bewegungsprofil ausgedehnt werden. So finden sich weitere Unterrichtsvorschläge dazu in SaferSmartphone von klicksafe, siehe Abschnitt 3.5 Bewegungsprofil oder (Rack und Sauer 2018a). Generell geht es an dieser Station um das Konzeptwissen, das bedeutet, die Schüler verstehen den Zusammenhang hinter dem Begriff von Bewegungsprofilen. (vgl. Hartmann et al. 2007, S. 23) Aus Zeitgründen durch die Beschränkung auf zehn bis fünfzehn Minuten bleibt es jedoch erstmal nur bei der Definition des Begriffs und der Erarbeitung der Gefahrengrundlage.

Neben Bewegungsprofilen gibt es auch andere Profile im Zusammenhang von Internet. Es entstehen auch beim Surfen Profile über die Nutzer. In der Einheit zu *Cookies und Browserverlauf* lernen die Schülerinnen und Schüler ein didaktisch reduziertes Schema eines Webseitenaufrufes kennen. Daran soll das Verständnis geweckt werden, wie auf neuen Seiten durch Cookies entsprechende Werbung zu vorherbesuchten Seiten eingeblendet werden können. Anhand des Schemas beschreiben die Schülerinnen und Schüler in eigenen Worten was Cookies und ihre Vorteile sind. Im Anschluss daran wird der Nachteil von solchen Cookies und deren Verknüpfung von Webseiten über gemeinsam genutzte Cookies, welche durch das Add-On Lightbeam sichtbar gemacht werden, erarbeitet.

Daraus folgt auch die weitere Einheit zur Anwendung von Selbstdatenschutz. In dieser lernen die Schülerinnen und Schüler verschieden *Software* und explizit auch Firefox-Addons kennen, die die Nutzer im Datenschutz unterstützen. Hier steht das Produktwissen im Vordergrund, jedoch sollen und können die Schüler von den vorgegebenen Tools abstrahieren (vgl. Hartmann et al. 2007, S. 23). Hierfür wurde ein Konsortium aus verschiedenen Tools ausgewählt, welche die Fachcommunity empfiehlt. Den Schülerinnen und Schülern wird dazu die Liste der Tools vorgelegt und sie sollen zu jedem Addon herausfinden, welche Funktion dieses Tool hat. Aus didaktischen Gründen wurden die größeren und komplizierten Tools exemplarisch schon beschrieben (siehe Anhang A. 11.6). Dann sollen die Schüler

und Schülerinnen die Tools auch praktisch ausprobieren und eigene Erfahrungen damit sammeln, um ihre Auswahl und Nutzungskompetenz zu stärken. Dies geschieht in einer kurzen Anwendungszeit im Browser, in der das Verhalten der Tools beobachtet und dokumentiert werden soll.

Die letzte Einheit beschäftigt sich mit *Rechten und Gesetzen* zum Thema *Datenschutz*. In diesem Abschnitt wird erarbeitet, wie in Deutschland Datenschutz durch Gesetze gewährleistet werden soll. Dazu bearbeiten die Schülerinnen und Schüler eine Aufgabe, in der zuerst Auszüge der wichtigsten Gesetze für den Datenschutz zusammengefasst sind.
Hierbei wird wieder die Lesekompetenz der Schüler berücksichtigt und die Gesetzestexte nur auszugsweise dargestellt (siehe Anhang A. 11.2). Eine weitere Differenzierungsmöglichkeit wäre eine Darstellung in leichter Sprache, welche im Rahmen dieser Arbeit aber auf Grund der Ausgangsschilderung des Klassenleiters zur Kompetenz der Lerngruppe erstmal nicht in Betracht gezogen wurde.
Danach sollen die Schüler auf dieser Grundlage entscheiden, ob ein fiktiver Lehrer in verschiedenen Situationen gesetzeskonform agiert. Durch den Lehrer und die Schulsituationen wird wieder ein Bezug zur Alltagsnähe der Schülerinnen und Schüler geschaffen. Ein abschließender Hinweis zur Datenverarbeitung von sozialen Netzwerken wie YouTube oder Snapchat, schließt den Kreis zur Einstiegsstunde.

Trotz der Querverbindungen zwischen den einzelnen Stationen ist eine freie Wahl der Reihenfolge möglich. Soweit bei einer Station auf eine andere verwiesen wird, dient dies nur zur Interessensteigerung, warum es sich auch lohnt die andere Station zu bearbeiten.

Die Differenzierung erfolgt durch die Stationenarbeit, da die Schülerinnen und Schüler eigenständig die Reihenfolge und Tiefe der Bearbeitung der Einheiten wählen können. Dabei treffen die Lernenden ihre Entscheidung einerseits durch die Themen der Einheiten und andererseits auch durch die methodische Aufarbeitung der Station. Dies fördert die Lernbereitschaft durch Mitbestimmungsrecht der Lernenden und motiviert durch vielfältige Mediennutzung (von Texten über Einstiegsvideos bis hin zu einem Rollenspiel). Gerade die Einheit zu den Berechtigungen von Apps kann durch ein Ausprobieren am eigenen Smartphone motivierend wirken. Geplant ist zwar, dass jede und jeder alle Stationen bearbeitet, jedoch kann jeder Lernende in seinem Tempo arbeiten. Als Hausaufgabe wird gefordert, dass die Schülerinnen und Schüler die Einheit mit der Software am eigenen PC zuhause umsetzen oder zumindest mit den Eltern darüber sprechen, wie es mit einer Installation der Tools am gemeinsamen Rechner aussieht, um das Gelernte weiter zu vertiefen. Sollte bei einer der Einheiten die Schülerinnen und Schüler vertiefende Fragen stellen und eine längere (aufgrund des regen Interesses) Verweildauer aufzeigen, so kann diese Einheit in einer Folgestunde nochmals vertieft werden.

Die abschließende Doppelstunde der Unterrichtsreihe beschäftigt sich mit dem Thema Passwörter. Passwörter schützen den Zugang zu privaten digitalen Bereichen, in denen häufig personenbezogene Daten wie Adresse bis hin zu Bankdaten, zu finden sind. Andererseits dienen Passwörter zur Authentifikation. Daher sind gute Passwörter gerade im Bereich Datenschutz wichtig. Wenn unberechtigte Dritte Besitz über Passwörter erlangen wollen, so versuchen sie es häufig über Phishing-Mails oder Spyware wie Trojaner. Hier kann der Querverweis zur vorherigen Stunde erfolgen. Sind die Angreifer auf diesem Weg erfolglos oder gelangen in den Besitz der Zugangsdatenbank des Betreibers eines Dienstes, so können sie über die Bruteforce-Methode (siehe Unterabschnitt 2.3.1) alle Passwortmöglichkeiten durchprobieren. Daran erkennen die Schülerinnen und Schüler wie wichtig es ist, eine gewisse Länge und verschiedene Zeichen zu verwenden. Die Motivation kann dadurch geweckt werden, dass die Schüler als Einstieg selbst die Bruteforce-Methode nachvollziehen, indem sie versuchen einen ein- beziehungsweise zweistelligen PIN zu knacken. Anhand des Versuches wird die Berechnung der Anzahl an Möglichkeiten vorgestellt. Im Anschluss wiederholen die Lernenden den praktischen Versuch mit einem dreistelligen Schloss. Um aber nicht alle 1000 Möglichkeiten durchprobieren zu müssen, werden verschiedene Hinweise zur möglichen Zahlenkombination gegeben. Damit lässt sich die Aufgabe differenzieren, langsamere Schüler bekommen stärkere (oder mehr) Hinweise, während schnelle Schülerinnen und Schüler sich der Aufgabe stellen dürfen, alle 1000 Möglichkeiten durchzuprobieren. Die Berechnung der reduzierten Möglichkeiten bei der Verwendung von Hinweisen gibt weitere Einblicke in das nachfolgende Thema der Kombinatorik. Genauso wird auch die Aufgabenstellung erweitert auf die Berechnung der Anzahl an Möglichkeiten bei mehr Stellen sowie bei mehr Ziffern. Dadurch gelangt man wieder zum Passwort mit Ziffern und Buchstaben sowie Sonderzeichen. Die Schüler erkennen die Schwierigkeit, solche Passwörter noch mit Bruteforce zu knacken. Im Folgenden wird dann auf die Problematik der Nutzung von starken Passwörtern, welche aber einfach zu merken sind, eingegangen. Hier erarbeiten die Schüler sich Regeln zu Passwörtern und Merktechniken. Damit wird die Unterrichtseinheit, ausgehenden von dem Erkennen von personenbezogenen Daten sowie der Gefahren bei vernachlässigtem Datenschutz über verschiedene Bereiche in der Thematik hin zu dem Bewusstsein der Schutzfunktionen von Passwörtern, abgerundet.

In der Planung einer Unterrichtsstunde folgt nun normalerweise die Methodik der Umsetzung sowie ein Verlaufsplan. Da in die Methodik jedoch die Ergebnisse aus der Stunde vorher mit einfließt, werden die Stunden im folgenden Kapitel einzeln beschrieben. Dabei werden ausgehend von den Feinlernzielen der einzelnen Stunden, diese methodisch aufgearbeitet sowie der Verlaufsplan der Stunde skizziert. Im Anschluss wird der Verlauf der Stunde beschrieben und zusammengefasst, sodass auf Grundlage dessen die nächste Stunde methodisch geplant werden kann.

4.3. Methodische Planung und Durchführung der Einzelstunden

4.3.1. Erste Stunde

a. Feinlernziele

- Die Schülerinnen und Schüler können Daten mit Personenbezug identifizieren.
- Die Schülerinnen und Schüler werden sich potenzieller Gefahren in Bezug auf personenbezogene Daten bewusst und hinterfragen ihr Verhalten dementsprechend.[25]
- Die Schülerinnen und Schüler sind motiviert sich mit der Thematik *Datenschutz* auseinanderzusetzen.[26]

b. Methodik

Aus der Vorbereitungsumfrage wurde ersichtlich, dass einige Schüler keinerlei Interesse an dem Thema haben. Daher wird die Einstiegsstunde genutzt, um die Schüler für die gesamte Unterrichtsreihe zu motivieren. Zum Einstieg stellt die Lehrkraft sich vor, dafür verwendet der Autor eine Präsentation zur Person anhand derer die Schüler personenbezogene Datenarten identifizieren können (vergleich

[25] Dies stellt ein affektives Lernziel dar, der Autor ist sich der Schwierigkeit des Bemessens bewusst. Trotzdem ist es Ziel der ersten Stunde, gerade das Desinteresse der Klasse zu überwinden und für die Folgestunden zu motivieren.

[26] Siehe Fußnote 21.

Anhang A. 3 Folie 1). Dies wirkt in dem Sinne motivierend, da die Schüler ein Interesse an der neuen Lehrkraft haben. Die Schüler sammeln in einer Tabelle an der Tafel persönliche Datenarten, wie Name und Adresse (vergleiche dazu Anhang A. 4, die erste Spalte), wobei hier durch eine Variation der Redekette die Lehrkraft sich erstmal zurücknimmt (siehe Mattes 2011, S. 22). Ein Schüler beginnt und gibt dann die Kreide in der Klasse weiter. So kann gemeinsam die Aufgabe der Identifikation von Datenarten gelöst werden. Die Lehrkraft tritt dabei in den Hintergrund und dient nur als Moderator. Die dadurch gewonnene Zeit kann von dem Lehrer genutzt werden, um einen ersten Überblick über die soziale Struktur der Klasse und die Sitzordnung zu erhalten. Dabei liegt der Fokus einerseits auf dem Lernen der Schülernamen sowie der frühzeitigen Identifikation von Unruheherden.

Im Anschluss wird ein Arbeitsblatt (siehe Anhang A. 13) ausgeteilt, welches einerseits zur Sicherung verwendet wird und andererseits weitere Aufgabenstellungen beinhaltet. So sollen die Schüler fünf Datenarten von der Tafel auf das Arbeitsblatt übertragen und dabei einschätzen, ob sie diese für veröffentlichungswürdig in Sozialen Netzwerken halten oder nicht. Dazu dient auf dem Blatt auch die dritte Spalte in der Tabelle, in der eine Begründung zur Entscheidung festgehalten werden soll.

Zur Motivation der nächsten Schritte folgt eine Live-Demonstration, in der ein Extremum von Datenverarbeitung, wie es aber SnapChat laut AGBs möglich ist, gezeigt wird. Dazu wird ein Schüler oder eine Schülerin mit einem Markenartikel fotografiert. Um den Datenschutz der Lernenden zu wahren, werden hierbei nur eine Kamera und ein Computer, auf den das Foto übertragen wird, genutzt. Es ist zu beachten, dass die Person um Erlaubnis gefragt und das Foto danach auch wieder gelöscht wird. Automatische Synchronisationsprogramme sollten aus Datenschutzgründen im Schulalltag ausgeschaltet sein. Anhand des Fotos kann live per Beamer gezeigt werden, welche weiteren Informationen in den Fotoeigenschaften mit übertragen werden, (zum Beispiel Zeit und Name der Kamera sowie eventuell auch Koordinaten der Aufnahme und Namen des Fotografen, siehe Anhang A. 6). In der folgenden Diskussion wird die Gefahr erarbeitet, dass allein aus diesen Daten durch Kombination mehrerer Fotos ein Profil erstellt werden kann.

An Auszügen aus den AGBs von SnapChat zeigt und erklärt die Lehrkraft, dass man durch das Akzeptieren dieser, dem Dienst, neben den Rechten an der Datenverarbeitung, auch volle Rechte an den Fotos überträgt. Um das auditive visuell zu unterstreichen, wird ein Bild einer Stadt mit vielen Werbeflächen gezeigt, auf denen nach der Erklärung, dass SnapChat die Fotos auch als Werbung nutzen darf, überall das Foto des freiwilligen Schülers mit Markenartikel erscheint. (siehe Anhang). Dieser „Schock“-Moment wird bei den Schülerinnen und Schülern vermutlich viele Frage aufwerfen, die konstruktiv genutzt werden sollen (zum Beispiel „Warum sollte SnapChat so etwas tun?“). Daher werden die Fragen an der Tafel gesammelt und in einem Unterrichtsgespräch zwischen den Schülern geklärt. Fragen, die auf die Themen der nächsten Stunde abzielen, wie zum Beispiel „Gibt es keine

Gesetze, die sowas verbieten?“, können dorthin verwiesen werden, wohingegen alle anderen Fragen entweder diskutiert oder in einer späteren Stunde nochmals aufgegriffen werden sollten. Nachdem die Lernenden die Gefahr der ungewollten Verwendung von persönlichen Fotos kennen gelernt haben, sollen sie in Gruppenarbeit mit Hilfe der Texte auf dem Arbeitsblatt weitere Gefahren für die anfangs gesammelten Datenarten herausarbeiten.

In einer letzten Sicherungsphase werden die Ergebnisse zusammengetragen, indem eine Gruppe mit einer Dokumentenkamera ihre Erkenntnisse präsentieren darf und die anderen Gruppen ergänzende Meinungen beitragen können. Sollte für die Gruppenarbeit keine Zeit mehr sein, wird die letzte Aufgabe in die Hausaufgaben verlegt. Des Weiteren wird den Schülern erlaubt, für die Folgestunden ihre Smartphones mitzubringen, damit sie Probleme und Fragestellungen direkt an ihrem Gerät bearbeiten können.

c. Geplanter Unterrichtsverlauf

Phase	Inhalt, Besonderes	Methode, Sozialform	Medium
Organisation	Begrüßung / Vorstellung	LV	Präsentation
Einstieg	Persönliche Daten	Brainstorming, UG	Tafel / Steckbrief
Erarbeitung	Risikoeinschätzung bei Veröffentlichung in Sozialen Netzwerken	EA	Arbeitsblatt
Motivation	Smartphones / Apps als Datenschnüffler	LV / UG	Handy / Werbeartikel / Laptop
Erarbeitung	Gefahren der Datenpreisgabe	PA / GA	Arbeitsblatt
Sicherung	Präsentation der Ergebnisse	SV	Dokumentenkamera

Tabelle 1: Verlaufsplan der 1. Stunde

d. Beschreibung des Verlaufs

Die Schüler kamen überpünktlich zum Unterricht, sodass in der Zeit bis zum Beginn schon ein Foto eines Schülers mit dessen Einverständnis gemacht werden konnte, da er gerade am Trinken eines Markensaftes war. Dies dient der Vorbereitung der später folgenden Live-Demo und entzerrt die Problematik mit der Überspielzeit auf den Rechner.

Der Klassenlehrer begrüßte am Anfang die Klasse und übergab nach ein paar einleitenden Worten die Stundenleitung für die Folgestunden an den Autor. Nachdem dieser sich vorgestellt und die Folie mit seinen personenbezogenen Daten präsentiert hat, fanden die Schülerinnen und Schüler auf die Frage „Was habt ihr über mich erfahren?“ schnell verschiedene Arten von personenbezogenen Daten heraus. Dabei differenzierten sie sogar zwischen „aktueller Ort“ und „Ort zu einer gewissen Zeit“, welches für das später folgende Thema *Bewegungsprofil* wichtig ist.

Im zweiten Teil der Einstiegsphase wurden schon die unterschiedlichen Meinungen zur Privatsphäre sowie die Problematik offensichtlich, dass die Schülerinnen und Schüler teilweise keine Gefahren sehen, wenn sie persönliche Daten offenbaren. So kam die Rückfrage, wieso es gefährlich sein soll, seinen aktuellen Ort zu verraten oder warum das Geburtsdatum ein schützenwertes Datum ist.

Die Motivation in der dritten Phase gelang relativ gut, auch wenn die Live-Demonstration noch nicht ausreichend genug, im Vorhinein erläutert wurde. Trotzdem ergab die Diskussion danach jede Menge an Fragen, die jedoch nicht wie geplant an der Tafel gesammelt, sondern auf Grund des bevorstehenden Unterrichtsende durch die Lehrkraft auf nächste Stunden verschoben oder direkt beantwortet wurden. Fragen, die später wieder aufgegriffen werden können und sollten sind folgende:

- Was macht Snapchat mit den Daten und was ist an personalisierter Werbung gefährlich? Diese Frage wird in den nächsten zwei Stunden erarbeitet.
- Welche Apps kann man denn dann noch verwenden?
  Eine mögliche Antwort folgender Art soll in der nächsten Stunde gegeben werden: „Man kann alle Apps verwenden, aber man sollte diese bewusst auswählen und nach Alternativen schauen. Als Beispiel kann man sich bei WhatsApp überlegen, ob man dem Anbieter Facebook noch vertraut oder welche Alternativen es dazu gibt. Da gibt es zum Beispiel Telegram, Threema, welches Geld kostet, oder Signal. Generell muss man allen Anbietern vertrauen und kritische Themen sollte man lieber persönlich als über Instantmassaging erzählen.“ Hier wäre eine Aufgabe, in der die Schüler die Apps kritisch vergleichen möglich.
- Wie kann ich mich vor solcher Datenverarbeitung schützen?
  Auch diese Frage wird in den nächsten zwei Stunden durch die Schüler erarbeitet.

Der Lehrer beendete mit diesen offenen Fragen den Unterricht und gestattete den Schülern, zum Zwecke der thematischen Erarbeitung, in den Folgestunden ihre Smartphones, wenn vorhanden, mitzubringen.

4.3.2. Zweite und dritte Stunde

a. Feinlernziele

- Die Schülerinnen und Schüler können die Begriffe Virus und Trojaner definieren und deren Gefahrenpotenzial in Bezug auf Datenschutz richtig einschätzen.
- Die Schülerinnen und Schüler sind in der Lage ihre Rechte und Pflichten in Bezug auf Datenschutz anzugeben, Datenschutzgesetze zu benennen und in datenschutzkritischen Situationen damit Stellung zu nehmen.
- Die Schülerinnen und Schüler können den Vorgang eines Internetseitenaufrufes inklusive des Nutzens von Cookies erklären und durchschauen die Problematik der Profilerstellung.
- Die Schülerinnen und Schüler nutzen die Berechtigungseinstellungen von Apps, um ihre Daten zu schützen, und können bei neuen Apps deren Berechtigungen hinterfragen.
- Den Schülerinnen und Schülern ist die Gefahr, welche von Bewegungsprofilen ausgeht, bewusst und sie können dagegen Sicherheitsmaßnahmen anwenden.
- Die Schülerinnen und Schüler können Softwaretools, welche die Benutzer im Selbstdatenschutz unterstützen, angeben und wählen davon jene aus, die sie für ihr Handeln als nützlich einschätzen.

b. Methodik

Die nächsten beiden Stunden erlangen die Schülerinnen und Schüler einen allgemeinen Überblick über Datenschutzthemen. In der Didaktik wurde hier eine Doppelstunde eingeplant. Auf Grund der schulischen Rahmenbedingung stehen in der Praxis jedoch nur zwei Einzelstunden zur Verfügung, sodass die Doppelstunde mit Unterbrechung geplant wird. Um die große Themenauswahl abzubilden wird eine Stationenarbeit über die zwei Stunden implementiert. Diese hat die Vorteile, dass ein Überblick über verschieden Themenbereiche von Datenschutz gegeben werden kann sowie in den Stationen verschieden Methoden zum Tragen kommen. Dabei kann auch eine Binnendifferenzierung stattfinden, da die Lernenden selbst entscheiden, in welcher Reihenfolge, Zeit und Tiefe, sie die Stationen bearbeiten (vgl.Wiechmann und Wildhirt 2016, S. 73). Die Tiefe beschreibt an dieser Stelle, ob sie die schwierigeren Zusatzaufgaben lösen. Des Weiteren kann durch Stationenarbeit die Leistungsfähigkeit eines Schülers der Sekundarstufe I zu konzentrierter Arbeit berücksichtigt werden. Die Grenze liegt dabei zwischen fünfzehn bis zwanzig Minuten und daher wird bei der Planung der Station auf den entsprechenden Umfang geachtet, sodass nach dieser Zeit ein Stationenwechsel mit körperlicher Bewegung ansteht. (vgl.Bauer 2008, S. 34)

Die Stationenarbeit wird folgendermaßen eingeführt: Zuerst werden die Regeln von Stationenarbeit durch die Lehrkraft erläutert (siehe Anhang A. 8), dem sich in einem Rundgang eine kurze Vorstellung aller Stationen anschließt, in der diese, inklusive ihrer Aufgaben, vorgestellt werden (siehe Anhang A. 9) (vgl. Wiechmann und Wildhirt 2016, S. 76). Um die Arbeitsaufträge klar zu gestalten, liegt an jeder Station für jeden Schüler ein Arbeitsblatt vor, welches er zum Abschließen der Station bis auf die eventuell vorhandene Zusatzaufgabe vollständig bearbeitet.

Nach der Vorstellung beginnt der offene Unterricht, in dem die Schülerinnen und Schüler anhand von Laufzetteln ihren Lernstand kontrollieren und wissen, welche Stationen noch zu bearbeiten sind (siehe Anhang A. 10). Um ein Überlaufen einzelner Stationen zu vermeiden, werden die Anfangsstationen eines jeden Schülers zu Beginn ausgelost. Im Anschluss entscheiden die Schülerinnen und Schüler selbst nach Interesse, aktuelles Befinden, Methode und Medien, sowie Platz an den Stationen, welche Station sie als nächstes ansteuern. Eine Problematik resultiert jedoch aus der geringen Bereitstellung von Rechnern und dem Fehlen eines für alle freien Internetzugangs. Es können zwar zwei Rechner bereitgestellt werden, von denen einer den Internetzugang über einen von der Lehrkraft aufgebauten Hotspot erhält. Dieser PC wird für eine Station, in der die Schüler Add-Ons beim Surfen ausprobieren sollen, reserviert. Die Möglichkeit des Rechnereinsatzes im Klassenraum an verschiedenen Stationen ist daher eingeschränkt und so muss auf einen stetigen Wechsel geachtet werden, damit alle Schülerinnen und Schüler die Möglichkeit haben in der vorgesehenen Zeit die Stationen zu bearbeiten. Der Einsatz der Smartphones ist auch auf den Offlinemodus eingeschränkt, womit die Recherchen der

Lernenden an Computer und Smartphone entfallen und weitestgehend auf kopierte Texte zurückgegriffen werden muss. Die einzelnen Stationen unterscheiden sich wie beschrieben neben der Thematik auch in der Methode und den genutzten Medien. So werden alle Stationen im Folgenden einzeln vorgestellt und daran die Methodik erörtert:

Die erste Station beschäftigt sich mit dem Thema *Viren und Trojaner*. Diese Station wird in Partnerarbeit bearbeitet, dies hat die Vorteile, dass bei Verständnisproblemen gegebenenfalls der Partner unterstützend wirken kann und andererseits eine Arbeitsteilung und eine Vergleichsinstanz verfügbar ist (Meyer 2018, S. 41). Zuerst soll eine Definition von Viren und Trojanern recherchiert werden. Als Grundlage dient dazu die in Abschnitt 3.2 beschriebene Zusammenfassung[27] von klicksafe. Im Anschluss daran werden in einer arbeitsteiligen Textarbeit Gefahren durch Viren und Trojaner und Handlungsmaßnahmen dagegen erarbeitet. Als Textgrundlage dazu dienen thematische Auszüge aus dem Portal des Bundesamtes für Sicherheit in der Informationstechnik. (siehe Anhang A. 11.1, Seite 2 und 4) Dadurch erhalten die Lernenden gleichzeitig eine offizielle Informationsquelle, falls sie weitere Fragen in diesem Bereich haben. Während der eine Lernende sich mit der Thematik Viren beschäftigt, konzentriert sich der Partner auf das Thema der Trojaner. So erfolgt die Sicherung dieser Station durch eine Zusammenfassung für den Lernpartner.

Mit dem Thema *Rechte und Gesetze zum Datenschutz* beschäftigt sich die zweite Station. Hierbei wird auf das Arbeitsblatt von klicksafe (siehe Abschnitt 3.6) zurückgegriffen, welches für die Stationenarbeit leicht verändert wurde (vergleiche Anhang A. 11.2.). Auch hier werden die Aufgaben in Partnerarbeit, im Spezifischen sogar Tandemarbeit mit gegenseitiger Aufgabenkorrektur, bearbeitet, sodass der Lernerfolg direkt eigenständig kontrolliert werden kann. In der ersten Aufgabe wird die Lesekompetenz anhand von Gesetzesausschnitten trainiert und in Aufgabe 2 sollen die Gesetzestexte nochmals vereinfacht dem Tandempartner erläutert werden. In der dritten Aufgabe wird in einem Multiple-Choice-Test überprüft, inwiefern die Gesetze verstanden worden sind. Neben einer gemeinschaftlichen Korrektur des Tests mit dem Tandempartner, soll auch die Musterlösung zu Hilfe genommen werde. Fallen hierbei Probleme auf, ist die Musterlösung um Erklärungen ergänzt, sodass das Lerntandem sich eigenständig korrigieren kann. Als offene vertiefende Aufgabe wird auf die Datenschutzerklärung und die AGBs von YouTube und SnapChat verwiesen, sodass ein selbstständiges weiterrecherchieren gefördert wird.

An der dritten Station beginnen die Schülerinnen und Schüler in einer Vierergruppe. Hier soll in einem von klicksafe adaptierten Rollenspiel das Thema *Webseitenaufruf und Kommunikation zwischen Server*

[27] Die Unterrichtsreihe „Ein ganzer Zoo im Computer und auf dem Handy“ ist zwar für die Klassenstufe 8 ausgelegt, die didaktisch reduzierte Übersicht sollte jedoch auch für die Klassenstufe 6 geeignet sein.

und Client, vereinfacht nachgestellt werden (siehe Abschnitt 3.3). Im Fokus liegt hierbei die Verwendung von Cookies. Das Rollenspiel motiviert die Lernenden den Zusammenhang nachzuvollziehen (vgl. Wiechmann und Wildhirt 2016, S. 92). Durch Zettel von Webseitenrepräsentationen und Cookies wird das Ganze noch enaktiv angeregt, sodass auch jüngere Schüler ein Verständnis für den Vorgang entwickeln sollten. Die Person, welche die Browserrolle spielt, erhält von den Personen, welche die Server repräsentieren, neben den Webseiteninhalten auch Cookies. Die Webseiteninhalte zeigt sie der Person, welche den Benutzer darstellt. Die Cookies werden im Verlauf von den Serverrollen angefragt, worauf diese Webseiten mit entsprechender Werbung gestalten und an die Browserrolle leiten (vergleiche dazu Anhang A. 12). Die Lernenden fassen das Rollenspiel zusammen, indem sie die Funktion von Cookies beschreiben. Anhand eines Screenshots von dem Add-On Lightbeam auf dem Arbeitsblatt (siehe Anhang A. 11.3.) sollen die Schülerinnen und Schüler die Problematik von Tracking per Cookies erkennen. Daraus ableitend sollen Risiken, welche aus der Erstellung von Nutzerprofilen entstehen, beschrieben werden. Die Erarbeitung des Add-Ons findet in der Station 6 statt, auf die an dieser Stelle verwiesen wird.

Mit einem Video von Handysektor[28] als Impuls steigt die vierte Station ein. Im Video bekommen die Lernenden erklärt, was App-Berechtigungen sind, worin die Gefahr dabei liegt und worauf man achten kann. Da den Schülern kein Internet zur Verfügung steht, ist der Stationsbeginn nur an einem Rechner möglich, auf den das Video überspielt wurde. Im Anschluss sollen die Schülerinnen und Schüler an ihren eigenen Smartphones kontrollieren, welche Berechtigungen ihre Lieblings-Apps beanspruchen. Das Nutzen der eigenen Smartphones kann einen hohen motivationalen Faktor haben. Auf dem Arbeitsblatt (siehe Anhang A. 11.4) befindet sich eine Kurzanleitung für Android und iOS, wie die Einstellungen zu finden sind. Nach der Betriebssystemverteilung von Smartphones ist zu erwarten, dass diese beiden von den Schülern genutzt werden (Statista GmbH 2018). Die Problematik an dieser Aufgabe ist, dass auf den Smartphones der Schüler verschiedene Software und verschiedene Versionen vorhanden sind. Daher kann die Anleitung nur als Ansatz genommen werden und jeder Schüler muss diese an seinem Smartphone nachvollziehen. Sollte ein Schüler kein Handy dabeihaben, liegen an der Station die Zusatzbeschreibungen von medienscout (siehe Landesanstalt für Medien Nordrhein-Westfalen 2014, 27 f.), aus denen er zumindest für Facebook, WhatsApp und Instagram die Berechtigungen erarbeiten kann. Im zweiten Teil dieser Station soll an fiktiven Apps die Urteilskompetenz der Schüler trainiert werden, indem die Lernenden begründet entscheiden, welche der Apps sie (nicht) installieren würden. Die fiktiven Apps mit ihren Berechtigungsansprüchen sind auf

[28] https://www.handysektor.de/artikel/handysektor-erklaert-was-sind-eigentlich-app-berechtigungen/ (zuletzt abgerufen am 14.09.2018)

dem Arbeitsblatt von klicksafe (siehe Anhang A. 11.4. Seite 2) dargestellt und dieses wird an dieser Stelle genutzt. Die Sicherung erfolgt wieder durch den Vergleich mit dem Partner.

Die fünfte Station ist eine sehr offene Aufgabengestaltung. An dieser Station sollen die Schüler wesentliche Merkmale von Bewegungsprofilen herausarbeiten. Als Grundlage dazu dienen ein Text aus SaferSmartphone (Rack und Sauer 2018a, S. 13) und ein zweites Video[29] von Handysektor. Die Aufgabe auf dem Arbeitsblatt (siehe Anhang A. 11.5) umfasst das Erstellen von drei Fragen, welche dem Lernpartner an dieser Station vorgelegt werden, sodass dieser die Fragen des Anderen beantworten soll. Dadurch wählen die Lernenden selbst ihre wichtigsten Punkte zum Thema. Hierbei wird eine Binnendifferenzierung[30] durch die selbstbestimmte Bearbeitungstiefe umgesetzt, indem die Schüler nur Fragen für ihren Partner entwickeln, die sich durch Überfliegen der Quellen lösen lassen, oder sie wählen Fragen, die tief im Detail liegen, sodass Text und Video mehrmals gelesen und geschaut werden müssen. Wegen der Problematik mit dem Nichtvorhandensein von Internet, ist auch diese Station auf einen Rechner mit dem heruntergeladenen Video beschränkt.

Die letzte Station beschäftigt sich mit der praktischen Anwendung von Selbstdatenschutz. Dabei wird stellenweise auf die Unterrichtsreihe von klicksafe zum Thema *Tracking* zurückgegriffen (siehe Abschnitt 3.3). Die dortige Altersbestimmung bezieht sich auf die Handlungskompetenz der Schüler im Umgang mit dem Browser, welche in dieser Lerngruppe durch die Entwicklung der immer früheren Nutzung solcher gegeben sein sollte. In dieser Station sollen die Schüler sich mit Add-Ons und Programmen auseinandersetzen, welche sie im Selbstdatenschutz unterstützen. Zuerst erarbeiten die Lernenden sich die Funktionen der Tools anhand eines Textes in Einzel- oder Partnerarbeit. Dazu liegt eine Tabelle mit den Tools vor, die mit den Funktionen ergänzt werden soll (siehe Anhang A. 11.6.). Besser für die Recherche wäre es, das Internet zu nutzen, dies steht, wie oben beschrieben, jedoch leider nur in eingeschränktem Rahmen zur Verfügung.
Im Anschluss daran kommt das Sammeln der praktischen Erfahrung. Dazu wird ein Rechner mit vorinstallierten Add-Ons im Firefox bereitgestellt. Die Schüler dürfen eine Weile im Internet surfen, welches an diesem expliziten Rechner per Hotspot zur Verfügung gestellt wird. Dabei sollen sie die Funktionsweise der Add-Ons beobachten, wozu einerseits auf dem Arbeitsblatt explizite Webseiten genannt werden, um eine Ablenkung[31] der Schüler durch themenferne Seiten zu vermeiden, und

[29] https://www.handysektor.de/artikel/handysektor-erklaert-was-ist-eigentlich-ein-bewegungsprofil/ (zuletzt abgerufen am 14.09.2018)

[30] Der Lehrkraft ist die offene Gestaltung bewusst und die Motivation der Schüler bezüglich der Bearbeitungstiefe ist abzuwarten. Darauf aufbauend können in Zukunft weiterhin solch offene Aufgaben gestellt werden oder es muss zu einer strenger geführten Form der Aufgabenstellung zurückgegangen werden.

[31] Hier wird im Hintergrund auch eine Blacklist genutzt, sodass bei Schülern beliebte sowie auch schülergefährdende Webseiten, im Vorhinein schon gesperrt sind.

andererseits eine detaillierte Anleitung auf dem Arbeitsblatt (siehe Anhang A. 11.6.) zur Unterstützung bei der praktischen Untersuchung der Add-Ons gegeben wird. Gerade die Erstellung von Benutzerprofilen über Cookies soll mit dem Add-On Lightbeam veranschaulicht werden. Hier wird eine Verbindung zu der Station 3 gegeben. Unterstützend dabei wirkt auch der Vergleich zwischen dem Surfen mit aktiven Tools und dem Surfen ohne, mit deaktivierten, Tools. Durch das Bereitstellen an nur einem Rechner, kann diese Station leider nicht so effektiv durch die Schüler genutzt werden, daher ist eine Vertiefung als Hausaufgabe empfehlenswert. Im Sinne der praktischen Umsetzung wird aufgrund der unbekannten Lerngruppe und deren häuslicher Rahmenbedingungen, wie die Einstellung der Eltern zur Verwendung von Computern, diese Hausaufgabe nicht gegeben.

Am Ende der dritten Stunden sollen alle Schüler und Schülerinnen alle Stationen bearbeitet haben, wobei die Tiefe sowie die Verweildauer selbstbestimmt erfolgen kann. Der Schnitt beim Stundenwechsel zwischen den Einzelstunden wird zur Sicherung der bisher bearbeiteten Stationen genutzt. So soll zu jeder Station ein Schüler in drei Sätzen erklären, was er an dieser Station gelernt hat. Die Reduzierung auf drei Sätze fördert einerseits das Herausarbeiten der wichtigsten Punkt und ermöglicht andererseits einen Überblick über die sechs Stationen in kurzer Zeit. Geplant für diese Sicherung sind fünf Minuten. Zur Unterstützung erhalten die vorstellenden Schüler im Voraus einen kleinen Zettel (siehe Anhang A. 13), den sie bei der Bearbeitung ihrer Station schon ausfüllen können. Genauso steigt auch die dritte Stunde ein, in dem in einem kurzen „Werbeblock“ sechs Schüler erklären, warum für sie die Station, die sie letzte Stunde bearbeitet haben empfehlenswert ist. Dazu können sie die oben beschriebenen Zettel aus der vorherigen Stunde nutzen. Die weitere Zeit verbringen die Schüler an den Stationen bis dann in den letzten fünfzehn Minuten alle Ergebnisse als Sicherung gesammelt werden. Dabei sollen einzelnen Schüler ihre Ergebnisse unter einer Dokumentenkamera vorstellen. Zu einer guten Stationenarbeit gehört am Ende auch eine Reflexion der Methode und der Aufgabenstellung an den einzelnen Stationen (vgl. Hegele 2016). Dafür wird die Feedbackmethode der Evaluationszielscheibe verwendet (siehe Anhang A. 15), auf der die Meinung zu den einzelnen Stationen sowie zur gesamten Stationenarbeit abgefragt werden soll. Darauf können die Schüler mit Punkten markieren, wie gut ihnen die Themen jeweils gefallen haben. (vgl. Bastian et al. 2016, S. 148)

c. Unterrichtsverlauf

Erste Einzelstunde

Phase	Inhalt, Besonderes	Methode, Sozialform	Medium
Organisation	Stationsarbeit erklären	LV	-
Erarbeitung	Stationen nach Interessenswahl	EA/PA	Stationen
Sicherung	Was habe ich an der letzten Station gelernt	UG	Stichpunktzettel

Zweite Einzelstunde

Phase	Inhalt, Besonderes	Methode, Sozialform	Medium
Reorganisation	Werbeblog, warum Station empfehlenswert	UG	Stichpunktzettel
Vertiefung	Weitere Stationen nutzen	EA/PA	Stationen
Sicherung	Ich habe gelernt	UG	Dokumentenkamera
Reflexion	Stationenarbeit	UG	Zielscheibe

Tabelle 2: Verlaufsplan der 2. und 3. Stunde

d. Beschreibung des Verlaufs

Die Stationenarbeit ist eine Form des offenen Unterrichts und kann daher nicht bis in das kleinste Detail geplant werden. Trotzdem gelang es, eine arbeitsame Atmosphäre zu schaffen und die Schüler zu motivieren. Dem Einstieg mit Erklärung zu den Regeln von Stationenarbeit und den thematischen Inhalten der einzelnen Stationen folgten die Schüler sehr aufmerksam. Auch die Zuteilung zu den Anfangsstationen stellte keine Probleme dar. Jedoch ergaben sich im Verlauf der ersten Stunde der Stationenarbeit folgende Probleme, sodass die Folgestunde etwas umgeplant werden muss (siehe nächster Unterabschnitt 4.3.3).

Problematisch war die Klassenraumgröße und die reduzierte Bereitstellung von Recherchemöglichkeiten. So kam es zu einem Rückstau an den Stationen, welche aufgrund eines Videos oder der zu erprobenden Tools einen Rechner voraussetzten. Durch die kleine Raumgröße konnten die Stationen nicht gut verteilt werden, sodass Arbeitsblätter von verschiedenen Stationen auf einem Tisch lagen und somit nicht auseinandergehalten werden konnten. Hier wäre es ratsam gewesen, die Tischaufstellung zu verändern und Stationen-Tischgruppen zu bilden, anstatt die Schüler an ihren Plätzen die Stationen bearbeiten zu lassen und dann von den drei Tischen mit Arbeitsblättern die nächste Station zu holen (vgl.Wiechmann und Wildhirt 2016, S. 73).

Positiv durch die Stationenarbeit war der Grad an aktiven Lernenden. Dadurch, dass alle Lernenden an ihren Arbeitsaufträgen saßen, konnte die Lehrkraft bei einigen Gruppen helfen, da es Verständnisprobleme mit der Aufgabenstellung gab. Zum Beispiel verstanden die Schüler an der

Station zum Thema *Cookies und Browserverlauf* nicht, wie sie das Rollenspiel durchzuführen haben. Selbst nachdem die Lehrkraft auf den Stationenzettel (siehe Anhang A. 9. Erläuterung der Stationen) hingewiesen hatte, konnte die Gruppe die Aufgabe nicht umsetzten, sodass eine nochmalige mündliche Erklärung notwendig war. Hierbei ist zu beachten, dass die Schüler das Rollenspiel als Methode noch nicht kannten und durch die vielen einzelnen Zettel, welche das enaktive Handeln fördern sollten, eher mehr Verwirrung gestiftet wurde. Dies hätte in der Planung berücksichtigt werden sollen. Aber auch an der Station *Viren und Trojaner* gab es Probleme, so hatte zumindest ein Schüler große Schwierigkeiten beim Textlesen, sodass diese Station zu textlastig für ihn war. Hier wäre eine Differenzierung bezüglich *Leichte Sprache* mit ihrer Lern- und Brückenfunktion eine sinnvolle Erweiterung gewesen (vgl. Bredel und Maaß 2016, S. 56). Daraus resultierte nämlich auch eine hohe Frustration bei seinem Partner, der die Station dann auch nicht gewinnbringend bearbeiten konnte.

Andere Station wurden aber auch sehr überraschend positiv bearbeitet. Die offene Station zum Thema Bewegungsprofil, bei der die Bearbeitungstiefe durch die Schüler ungewiss war, wurde von zwei Schülerinnen so differenziert bearbeitet, sodass der Rechner über 15 Minuten von ihnen beansprucht wurde. Daher konnten auch nicht wie geplant mindestens drei Gruppen diese Station bearbeiten. Die Station der Tools wurde zwar nur von zwei Lernpaaren bearbeitet, dabei hielten sich die Schüler an die vorgeschlagenen Seiten, sodass ein Eingreifen der Lehrkraft nicht erforderlich war.

Es kann festgestellt werden, dass die Beschreibung der Stationen nicht optimal gewesen ist, was aus vielen Schülerrückfragen hervorgeht, und sollten für einen erneuten Versuch überarbeitet und präsenter an den Stationen ausgelegt oder ausgehangen werden. Auch sollte diesbezüglich eine Überarbeitung der Texte auf den Arbeitsblättern stattfinden, sodass diese noch genauer an den Leistungsstand der Klasse angepasst werden.

Die Sicherung erfolgte aus Zeitgründen nicht unter Zuhilfenahme der Zettel, sondern nur mündlich, da die Schüler die Stationen ordentlich zu Ende führen sollten. Durch die von Seiten der Schüler spontan zu gebenden Antworten ergab sich dann kein so effektives Resultat und ermöglichte dem Lehrer dadurch auch keine genaue Lernstandskontrolle. Zumindest ein kurzes Meinungsbild zeigte, dass durch die genannten Probleme viele Schüler nur ein bis zwei Stationen geschafft haben, anstatt der für die erste Stunde geplanten drei. Positiv zu bemerken ist jedoch, dass alle gearbeitet haben und sich keiner aus dem Lernprozess zurückgezogen hat. Eventuell war die Unterrichtsform für die, dem Autor anfangs unbekannte, Klasse zu offen und die Schüler waren zu unsicher in der eigenständigen Arbeit.

Im Ausblick auf nächste Stunde wird die Stationenarbeit nicht mehr in dieser freien Form weitergeführt, sondern - um gerade bei Verständnisprobleme besser agieren zu können - auf das gleichzeitige Bearbeiten einer Station reduziert. Hierbei wurde von den Schülerinnen und Schüler das Interesse noch abgefragt und beschlossen das Thema App-Berechtigungen zu vertiefen. Trotzdem

werden die Schülerinnen und Schüler alle Stationsblätter sowie weitere Informationsmöglichkeiten dazu erhalten (siehe Anhang A. 14. Deckblatt Stationenarbeit). Darauf sind Links zu *Handysektor*, *klicksafe.de* sowie interessanten Videos und Spielen, die sich mit dem Thema *Datenschutz* beschäftigen. Dadurch soll die in der ersten Stunde aktivierte Motivation weiter erhalten bleiben.

4.3.3. Anpassung der dritten Stunde

Da diese Stunde als zweiter Teil der Stationenarbeit geplant war, erfolgt in diesem Abschnitt auch nur die Anpassung der Methodik durch die oben beschriebene Problematik. In dieser Stunde bearbeiten alle Schüler die Station 4 zum Thema *App-Berechtigungen*, außer die Schüler, die diese Station schon letzte Stunde bearbeitet haben. Diese Schüler bearbeiten die Station 1 *Viren und Trojaner* und Station 2 *Rechte und Gesetze*, da für diese keine weiteren Medien benötigt werden und sie in relativer Stillarbeit erfolgen können. Somit stehen folgende Lernziele im Fokus:

a. Feinlernziele

- Die Schülerinnen und Schüler sollen die Gefahr erfassen, wenn Apps unnötige Berechtigung fordern.
- Die Schülerinnen und Schüler können erkennen, welche Berechtigungen ihre Apps fordern.
- Die Schülerinnen und Schüler können die Berechtigungseinstellungen von Apps nutzen, um ihre Daten zu schützen, sowie hinterfrage bei neuen Apps deren Berechtigungen.

b. Methodik

Die Methodik der Station 4 wurde schon in der vorherigen Unterrichtsplanung beschrieben, sie wird infolge der gemeinsamen Bearbeitung nur wie folgt abgeändert.

Das Einstiegsvideo wird als stiller Impuls genutzt (vgl. Lehrfilm inMeyer 2017, S. 139) und im Plenum per Beamer gezeigt. Danach folgt in Partnerarbeit die zweite Aufgabe, in der die Schüler die Berechtigungen der Apps auf dem eigenen Smartphone nachschauen sollen. Sollten Schüler dabei Schwierigkeiten haben, kann die Lehrkraft explizit helfen. Zur Sicherung trägt die Lehrkraft, anhand von Schülerbeiträgen, die Berechtigungen der zwei meist genutzten Apps in das, an die Wand projizierte, Arbeitsblatt ein. Ein selbstständiges Eintragen durch die Schülerinnen und Schüler wäre möglich, jedoch ist dies sehr zeitaufwendig und wird daher vermieden. Im Anschluss daran bearbeiten die Schüler die dritte Aufgabe, in der sie ihre Einschätzungen zu den auf dem Arbeitsblatt (siehe Anhang A. 11.4 Seite 2) stehenden fiktiven Apps geben sollen. In einem Unterrichtsgespräch werden dann die Meinungen der Schülerinnen und Schüler zu den einzelnen Apps gehört. Sollte ein Schüler ein Urteil zugunsten einer datenschutzkritischen App fällen, kann über ein Meinungsbild in der Klasse gezeigt werden, wie die App im Allgemeinen eingeschätzt wird.

Zum Abschluss soll noch einmal die ganze Stationenarbeit gesichert werden, indem die Blätter (siehe Anhang A. 13) zur Zusammenfassung der Stationen ausgeteilt und in fünf Minuten bearbeitet werden, sodass sie dann vorgestellt werden können. Das Ende bildet die geplante Feedbackmethode, welche kurz erläutert werden muss, sodass die Schüler beim Verlassen des Raumes ihre Punkte auf die Zielscheibe setzen können.

c. Unterrichtsverlauf

Alternative Unterrichtsstunde

Phase	**Inhalt, Besonderes**	**Methode, Sozialform**	**Medium**
Reorganisation	Wie sieht die heutige Stunde aus	LV	Arbeitsblatt Hefte
Motivation	Was sind App-Berechtigungen	Lehrfilm	Video / Beamer / Ton?
Erarbeitung	*Berechtigungen von Apps*	PA	Arbeitsblatt (+ Infotext)
(Alternativ)	*Viren und Trojaner* oder *Rechte und Gesetze*	EA/PA	
Sicherung	Welche Berechtigungen sind ok?	UG	Beamer / digitales Arbeitsblatt
Erarbeitung	Kurzvortrag zu Station	PA	Stationen
Sicherung	An der Station hat man gelernt, dass…	UG	

Tabelle 3: Korrigierter Verlaufsplan der 3. Stunde

d. Beschreibung des Verlaufs

Diese Unterrichtsstunde verlief von der Erarbeitung her relativ gut. Dabei waren die Schüler sehr motiviert das eigene Handy zu nutzen und die Berechtigungen ihrer Apps nachzuschauen. So war auch relativ schnell die zweite Aufgabe besprochen. Bei der dritten Aufgabe waren dann jedoch fünf Jungs unachtsam und störten die Lernatmosphäre durch lautes Reden. Das Resultat davon war, dass einer der Schüler bei der Sicherung der Aufgabe sogar absichtlich falsch antwortete. Dahingehend wurde er durch das Meinungsbild der Klasse korrigiert, jedoch beanspruchte dieses Ausschweifen einiges an Zeit. Bei einer professionalisierten Lehrperson wäre diese Störung nicht so ausufernd ausgefallen und dadurch nicht zulasten des Lernstoffes und der Sicherung gefallen. In der nächsten Stunde werden diese fünf Schüler durch eine veränderte Sitzordnung getrennt, sodass es zukünftig zu keiner Wiederholung dieser Störung kommen sollte. Nach der Besprechung der Aufgabe drei, verblieb leider keine Zeit mehr für die große Sicherung aller Stationen. Auch konnte die in der Planung angesprochene Feedbackmethode nicht mehr erklärt werden und wurde daher nicht umgesetzt.

4.3.4. Vierte und fünfte Unterrichtsstunde

a. Feinlernziele

- Die Schülerinnen und Schüler erkennen die Wichtigkeit starker Passwörter.
- Die Schüler können Regeln zur Verwendung starker Passwörter anwenden.
- Die Schüler können Grundlagen der Kombinatorik anwenden um Möglichkeiten zu berechnen.
- Die Schüler können anhand der Kombinationsmöglichkeiten begründen wann ein Passwort sicher ist.

b. Methodik

Die letzte Stunde wird als Doppelstunde zum Thema Passwörter geplant.

Als motivationaler Einstieg wird ein kleiner Wettkampf ausgeführt, zudem die Klasse in zwei Gruppen geteilt wird. Im Rahmen dessen kann die Gruppe der fünf störenden Schüler durch eine neue Sitzordnung getrennt werden, um die Form des Störfaktors der Vorstunde auszuschließen. Jede Gruppe bestimmt aus ihrer Reihe zwei Kandidaten, welche per Bruteforce zwei Zahlenschlösser öffnen sollen. Dabei hat das erste Zahlenschloss eine Ziffer und das zweite Zahlenschloss zwei Ziffern, somit sind die Möglichkeiten noch auf 10 beziehungsweise 100 reduziert. Da es ein Wettkampf zwischen den beiden Teams ist, sollen die Gruppen ihre Kandidaten anfeuern. Das Gewinnerpaar darf ihr Vorgehen beschreiben und soll erklären, wie viele Möglichkeiten es durchprobiert hat. Dies wird gleichzeitig in einem Tafelbild (siehe Anhang A. 16) gesichert. Im Rahmen des Einstiegs in die Kombinatorik wird an den Zahlenschlössern mit einer und zwei Stellen die Möglichkeiten des Pins berechnet. Danach dürfen alle Schüler aktiv werden und bekommen immer zu zweit[32] ein Schloss mit drei Stellen und die Aufgabe aus dem Wettkampf. Um jedoch nicht 1000 Stellen durchprobieren zu müssen, erhalten die Schülerinnen und Schüler dazu ein Arbeitsblatt mit jeweils einem Hinweis darauf. Die Hinweise unterscheiden sich, wie in der Didaktik beschrieben, in dem Maße, wie viele restliche Möglichkeiten bestehen bleiben (siehe auch Anhang A. 18). Haben die Schülerinnen und Schüler das Zahlenschloss geöffnet, sollen sie die durch den Hinweis reduzierten Möglichkeiten einschätzen, sowie auch in der nächsten Aufgabe die Möglichkeiten bei Erweiterung auf Buchstaben und auf Buchstaben und Zahlen zusammen berechnen. Die Resultate davon werden an der Tafel gesammelt. Sollten die Lernenden für den praktischen Teil mehr Zeit brauchen, kann hier (da es eine Einstiegsstunde in Kombinatorik darstellt) nur auf exemplarische Beispiele von Möglichkeiten mit Hinweisen eingegangen werden.

[32] besser wäre eine Einzelarbeit, aber dazu gab es nicht genug Schlösser

Der zweite Teil der Stunde findet in einem Computerraum statt, da neben der Erarbeitung von Regeln zu Passwörtern auch die Medienkompetenz der Schülerinnen und Schüler gestärkt werden sowie am Ende die Stärke von Passwörtern in einem Onlinetool überprüft werden soll.

Als Impuls dient dazu ein Einstiegsfilm[33] zu Passphrasen. Daraus sollen die Schülerinnen und Schüler Regeln ableiten, welche sie in einer Gruppenarbeit an einem Rechner digital visualisieren, um es im Anschluss danach zu präsentieren. Im Rahmen der Präsentation stellt eine Gruppe ihre Ergebnisse vor und die Mitschüler dürfen dann noch weitere Aspekte dazu ergänzen.

Den Abschluss der Einheit bildet dann die Kreierung eines starken Passwortes, welches durch einen Passwortchecker (Online) überprüft werden sollen. Um die Stunde ausklingen zu lassen, wie sie begonnen hat, wird dazu ein Wettbewerb bezüglich des stärksten Passwortes ausgerufen.

c. Unterrichtsverlauf

Phase	Inhalt, Besonderes	Methode, Sozialform	Medium
Einstieg / Motivation	Öffnen eines Zahlenschlosses	GA	Zahlenschlösser
Erarbeitung	Kombinatorik anhand von Passwörtern	EA / GA	Freiarbeit / AB mit Aufgaben
Sicherung	Präsentation der Ergebnisse	UG	Tafel
Motivation	Passsätze		Video
Vertiefung	Passwortregeln	EA / GA	Word-Dokument
Sicherung 1	Passwortregeln	SV	Beamer
Sicherung 2	Passwortstärke prüfen	EA	Computer

Tabelle 4: Verlaufsplan der 4. und 5. Stunde

d. Beschreibung des Verlaufs

Der Wettkampf zum Einstieg motivierte die Schülerinnen und Schüler sehr. Darauf aufbauend konnten die Schülerinnen und Schüler auch die Anzahl an Möglichkeiten herleiten. In der folgenden Partnerarbeit waren alle Schüler aktiv, wobei zwei Gruppen die Schlösser nicht öffnen konnten, da sie kaputt waren. Dies führte zu einer Enttäuschung bei den Schülern. Des Weiteren waren die Schüler teilweise durch das praktische Ausprobieren derart abgelenkt, dass sie die theoretischen Aufgaben der Kombinatorik nicht bearbeitet haben. Hierauf muss im Folgenden mehr geachtet werden. Eine weitere Optimierung an der Stelle der Berechnung der Möglichkeiten wäre, direkt den Vergleich zur Bruteforce-Methode zu ziehen. So erkennen die Schüler nicht nur den Zusammenhang zwischen einer Stelle mehr und der wachsenden Anzahl an Möglichkeiten, sondern auch direkt den Zusammenhang zwischen einer Stelle mehr und der wachsenden Zeit, die ein Rechner zum Knacken des Passwortes benötigt. Die zweite Stunde war nicht effektiv geplant, so sollte der Computerraum anders genutzt

[33] https://www.handysektor.de/artikel/sichere-passwoerter-lang-und-schwer-zu-erraten/ (zuletzt abgerufen am 15.09.2018)

werden und berücksichtigt werden, dass in dieser Klassenstufe einerseits Zeit für das Anmelden der Schüler im Netzwerk gebraucht wird und andererseits die fehlende Medienkompetenz in dieser Klassenstufe auch mehr Zeit beansprucht. Auch ergab sich durch die Präsentation kein neuer Lerninhalt, da an dieser Stelle nur die Aussagen des Einstiegfilmes zusammengefasst und wiederholt wurden. Des Weiteren wich die Lehrkraft spontan von der Planung, dass nur eine Gruppe vorträgt und die Mitschüler ergänzen, zugunsten einer Präsentationsübung für alle Schülerinnen und Schüler ab, was an dieser Stelle jedoch durch die daraus resultierende mehrmalige Wiederholung desselben Lerninhaltes ungünstig und nicht zielführend war. Hier wäre eine Gruppenarbeit zu Beginn und eine Sicherung durch das Video, als Bestätigung sowie Ergänzung zu den erarbeiteten Aspekten in dieser Lerngruppe sinnvoller gewesen. Durch die beschriebene Umsetzung konnte die letzte Phase und der eigentliche Grund für den Wechsel in den Computerraum dann nicht mehr behandelt werden.

Trotz allem haben die Schüler zum Thema Passwörter die Regeln vertieft und eine Überleitung zum Thema Kombinatorik wurde aufgebaut. Den Abschluss bildete die Übergabe der Stundenführung wieder zurück an die Fachlehrkraft, welche sich für die themenvielfältige und gute Ausgestaltung der Unterrichtsreihe im Namen aller bedankte.

5. Ergebnis der Durchführung

In diesem Kapitel wird einerseits der Verlauf der Unterrichtseinheit im Gesamten betrachtet, das Erreichen der Ziele überprüft und die Umsetzbarkeit der Unterrichtsreihe in anderen Fächern beschrieben.

5.1. Allgemeine Zusammenfassung des Verlaufs

Die Einstiegsstunde weckte gerade durch die Live-Demo ein hohes Interesse der Schüler an dem Thema *Datenschutz*. Durch den leichten Einstieg über die persönlichen Daten der Lehrkraft konnte jeder etwas beitragen. Die durch den Unterrichtsverlauf entstandenen Schülerfragen hätten, wie eigentlich geplant, besser gesichert werden sollen, sodass auf diese in den Folgestunden hätte eingegangen werden können. So besteht die Möglichkeit, die Fragen auch in expliziten Stationen abzubilden, um die Eingangsmotivation in der späteren Vertiefung zu nutzen. Da die Stunde der Stationenarbeit aber schon am nächsten Tag anstand, war dies zur Umsetzung zu kurzfristig.

Die Stationenarbeit ist eine gute Methode, um verschiedene Themen aufgreifen zu können sowie eine Binnendifferenzierung zu ermöglichen. Diese kann jedoch in der vorgelegten Unterrichtsplanung noch intensiver ausgearbeitet werden. Für diese Lerngruppe wäre es sinnvoll gewesen, mehr Zeit für die einzelnen Stationen einzuplanen. Dabei erwiesen sich die Stationen, trotz vorheriger Rücksprache mit der Fachlehrkraft bei der getroffenen Auswahl der verwendeten Methoden und Materialien, nicht an jeder Stelle für die Lerngruppe als geeignet. Hier wäre eine Überarbeitung, gerade der Stationenbeschreibung zum besseren Verständnis der Aufgabenstellung notwendig. Aus methodischer Sicht stellt sich auch die Frage, inwiefern die nur auditive Vorstellung der einzelnen Stationen zu Beginn der Stationenarbeit sinnvoll war. Denn die Aufmerksamkeitsspanne fiel im Rahmen dessen, obwohl auch den Schülern jeweils nur die Beschreibung ihrer Anfangsstation wichtig war. Des Weiteren entsprachen die Rahmenumstände nicht den in der Planung vorgestellten, sodass hieraus auch Probleme in der Umsetzung der Arbeit entstanden. Das Umplanen der zweiten Stunde der Stationenarbeit war diesen Problemen geschuldet und führte auch nicht zu der gewünschten Verbesserung. Sinnvoller wäre eine direkte Anpassung der Stationen und eine erneute, auch visuelle Vorstellung dieser, am Stundenanfang gewesen.

Im Gesamten aber gefiel der betreuenden Fachlehrkraft gerade diese Einheit, sodass sie eine positive Rückmeldung aus ihrer professionellen Sichtweise geben konnte und bestätigte, dass die Schüler trotz der Hürden, doch aktiv am Arbeiten waren und einiges gelernt haben.

Die Abschlussstunde beschäftigte sich mit Passwörtern. Den Einstieg dazu bildete die Bruteforce-Methode zum Entschlüsseln von Passwörtern, welche an Zahlenschlössern realisiert wurde. Dies kam

bei den Lernenden sehr gut an und brachte auch eine sichtbare Motivation zur Auseinandersetzung mit der dahinter liegenden Theorie. Der zweite Teil sollte methodisch überarbeitet werden, um zu einer höheren effektiven Lernzeit zu gelangen. So sollte eine, spontan entstandene, mehrmalige Wiederholung des gleichen Lerninhaltes vermieden werden, zum Beispiel durch inhaltsdifferente Aufgaben zur Präsentation oder durch die wie auch geplante Präsentation von nur einer Gruppe. Der Abschluss mit dem Entwickeln starker Passwörter auf Grund der erarbeiteten Regeln konnte leider nicht erprobt werden, sodass hier eine hoher Motivationsfaktor und eine gewinnbringende Erfahrung für die Lernenden weiterhin nur vermutet werden kann.

Im Rahmen der Umsetzung stellten sich Parallelen zu *Informatik im Kontext* (IniK)[34] heraus, sodass die vorliegende Unterrichtsreihe auch unter diesem Titel aufgearbeitet werden kann. „Informatik im Kontext basiert auf drei Prinzipien:

1. Orientierung an Kontexten
2. Orientierung an Standards für die Informatik in der Schule
3. Methodenvielfalt“ (Koubek et al. 2009)

Das Thema *Datenschutz* ist der Kontext, welcher viele „historische, rechtliche, politische, ökonomische, soziale, ethische, kulturelle und nicht zuletzt eine informationstechnische Dimension [bietet], die unabhängig voneinander behandelt werden können.“ (Koubek et al. 2009, S. 272). Dabei lässt sich durch die Anwendung und Umsetzung von Datenschutz im Alltag sowie durch die Gefahren, denen die Schüler im Alltag im Zusammenhang mit dieser Thematik ausgesetzt sind, ein Bezug zur Lebenswelt der Schüler schaffen. Exemplarisch wird hier eine technische Seite von Datenschutz in den Add-Ons, eine rechtlich, politische Seite in der Aufarbeitung entsprechender Gesetze, eine ökonomische Seite in persönliche Daten als Bezahlungsmittel und eine ethische Seite in Bezug auf Überwachung mit Bewegungsprofilen aufgegriffen. Dass die Unterrichtsreihe Bezug auf die Bildungsstandards der Informatik nimmt, wird in der Legitimation der Unterrichtsreihe ersichtlich (vergleiche dazu Unterabschnitt 4.2.4 a). Der Aspekt der Methodenvielfalt wurde in allen Stunden gewahrt und gerade durch die Umsetzung in Stationenarbeit mit verschiedenen Methoden und Medien explizit gefördert. Diese Vielfalt bietet dadurch auch eine stärkeren Partizipation der Schüler. An dieser Stelle kann in weiteren Arbeiten angesetzt werden.

Trotz einiger Mängel zeigt sich, dass die Unterrichtseinheit im Gesamten umsetzungswürdig ist, wobei viele der entstandenen Probleme und Umsetzungsschwierigkeiten an den Rahmenbedingungen, der spezifischen Lerngruppe sowie der nicht ausgereiften Professionalität der umsetzenden Lehrkraft, die

[34] http://www.informatik-im-kontext.de/

erst am Ende des ersten Ausbildungsabschnitts befindet, hingen. Im Sinne wissenschaftlicher Arbeit wären hier zudem Vergleichsgruppen nötig, um diese Einflussvariablen ausschließen zu können.

5.2. Überprüfung der Durchführung

Um den Erfolg der Umsetzung der Unterrichtsreihe zu testen, füllte die Klassen drei Wochen später eine Abschlussumfrage aus. Dabei wurde auf den Fragebogen der Studie von Hug zurückgegriffen, anhand derer Datenschutzkompetenz gemessen werden kann (siehe Hug 2018a). Die Versuchsklasse nahm an der damaligen Studie im Dezember 2017 schon teil und so kann nachvollzogen werden, ob es durch die Unterrichtsreihe zu einer Verbesserung der Kompetenzen gekommen ist. Da aus Datenschutzgründen jedoch die Klasse nicht aus der Studie von Hug identifiziert werden kann, werden die jetzigen Ergebnisse zu den allgemeinen Ergebnissen von damals im Vergleich betrachtet (Hug 2018b). Bis auf die erheblich reduzierte Anzahl an Teilnehmern, ist es eine relativ ähnliche Verteilung innerhalb des Geschlechts und des Alters. Dazu muss bemerkt werden, dass Veränderungen in der Datenschutzkompetenz der Schüler aufgrund der vergangenen Zeit genauso mit einfließen, wie die Kompetenzentwicklungen durch die Unterrichtsreihe. Im Anhang A18 finden sich alle Ergebnisse der jetzigen Studie. In diesem Abschnitt werden nur die Items behandelt, welche durch die Unterrichtsreihe beeinflusst worden sein könnten.

Im Item A18.3 wird die Verwendung von sozialen Netzwerken betrachtet. Dabei zeichnet sich zwischen Vorbereitungsumfrage, eigener Überprüfung und Studie von Hug ein ähnliches Ergebnis ab. YouTube ist in dieser Altersklasse das meistgenutzte Soziale Netzwerk. Währenddessen scheint die Unterrichtseinheit den Bekanntheitsgrad von SnapChat und dadurch deren Nutzung gesteigert zu haben, auch wenn dies gerade nicht die Intention war. So verwenden nach der Durchführung 74% der Schüler die App, während es laut der Vorbereitungsumfrage nur 30% und in der Studie von Hug nur 45% aller Schüler waren.

An der Frage A18.4 zur Sensibilität von Daten in Sozialen Netzwerken lässt sich eine gute Richtung der Sensibilisierung erkennen. Jedoch besteht bei den Datenarten wie Vornamen, Geburtsdatum, Lieblingssachen und Religion noch weiterer Bedarf der Überzeugungsarbeit und Verdeutlichung der daraus möglicherweise resultierenden Gefahren. So gaben rund 78% alle Schüler an, dass der Vorname unsensibel ist und nur 42% der Schüler empfinden das Geburtsdatum als hoch sensibel. Auf der anderen Seite schätzen die Schüler die Sensibilität von Adresse und Kontakten mit um die 80% schon sehr hoch ein. In diesem Gesamtitem zur Sensibilisierung erreichten die Schüler einen Wert von 56% in der Risikobewertungskompetenz, welche gut ist, jedoch in weiteren Unterrichtseinheiten gestärkt werden sollte.

Auch die Einschätzung zu „Es ist mir wichtig, selbst bestimmen zu können, wer durch das Internet etwas über mich erfährt und wer nicht“ im Item A18.6 wird von zwölf Schülern als sehr hoch angegeben. Dies ist im Datenschutz sehr wichtig. Im Vergleich zu der Studie von Hug, gab es aber durch die Unterrichtsreihe prozentual keine Veränderung.

Die Unterrichtsreihe hatte als Ziel das Grundlagenwissen zu vertiefen, daher sollte die Erwartung der Kompetenzsteigerung gerade in der Dimension Wissen erfüllt werden. Dies lässt sich durch die Untersuchung auch bestätigen, so erreichten die Schüler in den Items A18.7 32% zur Wissenskompetenz, während der Wert in der Studie von Hug noch 19% betrug. Trotzdem erscheint der Wert der Wissenskompetenz mit 32% nicht hoch, das aber an folgenden Gründen liegen könnte. In der Stationenarbeit haben nicht alle Schüler alle Stationen bearbeitet, so haben beispielsweise nur sechs Schüler die Station 1 zu *Viren und Trojanern* bearbeitet. Unter Berücksichtigung dessen beantworten sieben Schüler die Frage „Was versteht man unter einem Trojaner?“ richtig. Prozentual gesehen haben 20% mehr als in der Studie von Hug diese Frage richtig beantwortet. Gleiches lässt sich auch zur Station 3 *Cookies und Browserverlauf* beschreiben, diese haben vier Schüler inklusive des Rollenspiels bearbeiten. Die Frage „Was ist ein Cookie“ beantworteten fünf Schüler richtig. Die Frage nach „Was ist eine Firewall?“ und „Welche URL garantiert einen datenabhörsicheren Zugriff?“ wurde in der Unterrichtsreihe nicht besprochen und trotzdem gab es gerade bei letzterer eine Steigerung der richtigen Antworten von 21% im Vergleich zur Studie von Hug. Worauf diese zurückzuführen ist, kann aber nicht eindeutig geklärt werden.

In den Items A18.9 spiegelt sich die Station 6 zu *Software zum Datenschutz* wieder. In dieser hätten die Schüler die im Item erfragten Add-Ons kennen lernen können. Aus dem Ergebnis der Umfrage geht hervor, dass selbst die Anforderungsstufe I von den Schülern zum größten Teil nicht erreicht wurde. So geben weiterhin zwölf Schüler an, keine Browsertools zu kennen. Dies spiegelt sich dann auch in dem Ergebnis der Nutzung wieder. So verwenden 78% der Schüler keine Browsertools. Im Vergleich zur Studie von Hug ist dies trotzdem eine Verbesserung, da dort noch 90% der Schüler angaben, keine Tools zu nutzen.

Die Ergebnisse aus dem Item A18.10, wie wichtige den Schülern die Aspekte der Verschlüsselung und der Identifikationsmöglichkeiten bei Messengern sind, sind positiv und zwar derart, dass mehr als 80% der Schüler diese als sehr wichtig erachten. Damit liegen auch sie im Schnitt der Studie von Hug.

Innerhalb der Items in A18.11 lassen sich folgende Punkte herausstellen: Bei der Frage nach der Auswertung von Nutzungsverhalten von Kunden durch Online-Shops antworteten 63% der Schüler korrekt, während dies in der Studie von Hug nur 53% richtig beantworteten. Genauso kam es auch in der Frage zum Selbstdatenschutz, dass durch Löschen von Browserinformationen ein Nachverfolgen erschwert wird, zu einer Steigerung von 15% der korrekten Antworten. Dass die Schüler über ihr Recht

am Bild Bescheid wissen, zeigt die vorletzte Frage. Dies war aber auch schon in der Studie von Hug so. Hier lässt sich die Erarbeitung innerhalb einer anderen Unterrichtseinheit oder außerhalb der Schule annehmen.

Das Item A18.12 bezüglich der Risikobewertungskompetenz zeigt keine positive Verbesserung nach der Unterrichtseinheit. Während in der Studie von Hug hier noch eine durchschnittliche Risikobewertungskompetenz von 65% erreicht wurde, hatte die Testklasse nur noch einen Wert von 47%. Hieran wird die Problematik sichtbar, dass man nicht weiß, wie die Testklasse innerhalb der Studie von Hug in diesem Bereich abgeschnitten hatte.

In der letzten Frage wurde das Interesse der Schüler an den Themen „Gefahren beim Surfen“, „technische Möglichkeiten“, „rechtliche Situation“ und „Schutz von Daten“ abgefragt. Hierbei fällt auf, dass bei allen Themen immer noch um die 50% der Schüler weiteres Interesse zeigen. Hier könnte eine weitere Unterrichtseinheit in spezifischen Datenschutzthemen angeschlossen werden. Trotzdem ist das Interesse im Vergleich zur Studie von Hug um durchschnittlich 10 % gesunken. Einerseits kann wiederrum nicht auf die Vergleichbarkeit geschlossen werden, da die Versuchsklasse nicht in dem Datensatz der Studie von Hug identifiziert wurde, andererseits haben die Schüler in allen Themenbereichen neue Informationen erhalten und eventuell somit ihr Interesse befriedigt.

Der Vergleich der erreichten Werte in den Dimensionen sowie deren Mittelwert ist in A18.17 bis A18.19 ersichtlich. Die gerundeten Mittelwerte der Dimension, welche die Schüler erreicht haben, ist relativ identisch zu der Studie von Hug. Hierbei liegt die Verteilung einer Normalverteilung ähnlich um 50%.

In A.18.18 fällt auf, dass die durchschnittliche prozentuale Wissenskompetenz der Versuchsklasse um den Wert 4,9% besser ist als die Wissenskompetenz aller Schüler der Studie von Hug, obwohl der erreichte Maximalwert nur 66,7% beträgt. Dem gegenüber steht die Reduktion der prozentualen Risikobewertungskompetenz um den Wert von 4,7%. Im Schnitt scheint die Unterrichtsreihe nur eine Verbesserung um den Wert von 0,3% im Mittelwert aller Dimensionen gebracht zu haben, wobei ein Vergleich zwischen der Nachuntersuchung und der Studie aufgrund des anderen zugrundeliegenden Teilnehmerkreises wissenschaftlich nicht möglich ist.

5.3. Übertragbarkeit der Unterrichtsreihe in andere Fächer

Wie in Kapitel 1 und auch im Unterabschnitt 4.2.4 der Legitimation der Unterrichtsreihe ersichtlich, kann, darf und muss das Thema *Datenschutz* auch in anderen Fächern aufgegriffen werden. So finden sich auch in denen Anknüpfungspunkte, welche als Einstieg oder anstatt des mathematiklastigen Abschlusses über die Passwörter genutzt werden können.

So kann in im Fach Deutsch beispielsweise das Thema *Datenschutz* im Bereich Medienkonsum aufgegriffen werden und nach einer Einheit zum Thema *Sprache in digitalen Chaträumen* einerseits auf (leichtfertig) veröffentlichte Daten in diesen angespielt sowie andererseits, durch die verkürzte Sprache und der Verwendung von Smilies in den Chaträumen, auf die Problematik von Fehlinterpretationen und Missverständnissen durch unvollständige Informationen eingegangen werden. Alternativ kann auch nach einer Unterrichtsreihe zum Thema *Datenschutz* eine Unterrichtsreihe zum Thema *Tagebücher* folgen, in der rückblickend auf Bewegungsprofile und somit öffentlich einsehbare Tagebücher verwiesen werden kann.

Auch in Ethik, auf Grundlage der Themenbeschreibung im Lehrplan, aber auch in den Fächern evangelische und katholische Religion, kann Datenschutz aufgegriffen werden und im Rahmen ethischer Konflikte durch Datenverarbeitung und der daraus resultierenden Art des gesellschaftlichen Zusammenlebens diskutiert werden. Auch wäre im Bereich Ethik ein Abschluss der Unterrichtsreihe *Datenschutz* mit dem Thema Cybermobbing denkbar. Weitere Unterlagen dazu finden sich im Themenmodul „Was tun bei (Cyber-)Mobbing?“ von klicksafe (Hilt et al. 2018).

Da Datenschutz ein gesellschaftliches Thema sein sollte, werden die gesellschaftswissenschaftlichen Fächer explizit zur Umsetzung der Verbraucherbildung, welche das Thema *Datenschutz* beinhaltet, angesprochen. Dabei kann in der Orientierungsstufe im Fach Erdkunde an das Lernfeld I.6 *Dienstleistungen* mit Rückgriff auf digitale Dienstleistungen und deren Bezahlung durch Daten die Unterrichtsreihe *Datenschutz* angeschlossen werden.

Aber auch im Fach Mathematik gibt es andere Anschlussmöglichkeiten als über die Kombinatorik bei Passwörtern. So kann in diesem Fach die Unterrichtsreihe *Datenschutz* auch innerhalb des passenden Themas *Information und Daten* umgesetzt werden. Gerade im Bereich der Datenerhebung und Statistik finden sich aufgrund der Genese von *Datenschutz* über das Volkszählungsurteil weitere Ansatzpunkte.

6. Resümee

Abschließend soll hier nun die Fragestellung der Ausgangssituation, nämlich „Wie kann eine Unterrichtsreihe zum Thema *Datenschutz* aussehen, sodass Schülerinnen und Schüler erstens dafür ein Interesse entwickeln und zweitens sich dann, aus der intrinsischen Motivation heraus, in das Thema vertiefen?“ beantwortet sowie neue Fragestellungen und Forschungsansätze zu diesem Thema aufgezeigt werden. Den Abschluss der Arbeit bildet das Feedback einer Gruppe von Lehrkräften, denen die Arbeit im Rahmen eines Workshops am Thementag „Digitalisierung im Schulbereich“[35] des Zentrums für Lehrerbildung der Universität Koblenz-Landau, Campus Koblenz, präsentiert wurde.

6.1. Zusammenfassung

Ausgehend von der Erkenntnis, dass eine frühzeitige Erlangung von Datenschutzkompetenz in der Entwicklung von Kindern und Jugendlichen wichtig ist, insbesondere im Hinblick auf die immer jüngeren Nutzer digitaler Angebote, wurde eine Unterrichtseinheit zum Thema *Datenschutz* entwickelt. Dabei wurden vorhandene Materialien gesammelt und mit selbsterstellten Materialien ergänzt. Deren praktische Umsetzung zeigte, dass eine Motivierung der Schüler der 6. Klasse zum Thema *Datenschutz* durch den vorhandenen Alltagsbezug möglich ist und dass die Schüler die Vertiefungsmöglichkeit gerne wahrnehmen. Dies wurde daran beobachtet, dass mit dem gewählten Einstieg in die Unterrichtsreihe über den Begriff personenbezogene Daten und der Gefahren von deren ungewollter Verarbeitung weiteres Interesse geweckt werden konnte. Hierbei ist es wichtig, einen Alltagsbezug herzustellen. Dies gelang durch die kleine Vorbereitungsumfrage, in der nach den meistgenutzten Apps der Schüler gefragt wurde, und der Darstellung der Ergebnisse innerhalb einer kleinen Live-Demo. Die anschließende Vertiefung in verschiedenen Themenbereichen erfolgte durch eine Stationenarbeit. Die Themenwahl lag dabei bei Schadsoftware, Profilbildung durch Browserinformation und Bewegungsdaten sowie der Berechtigungen von Apps bis hin zum Datenschutz in Recht und Gesetz sowie Selbstdatenschutz durch Tools. Hierbei stieß die Lerngruppe auf verschiedene Probleme, welche in einer Überarbeitung und Anpassung an andere Lerngruppen berücksichtigt werden sollten. Den Abschluss und Übergang zu einer mathematischen Folgestunde bildete das Thema Passwörter mit der Gefahr des Knackens per Bruteforce-Methode. Hierbei hat die Anzahl an möglichen Kombinationen einen hohen Stellenwert und leitet in die mathematische Kombinatorik über. Anhand der Nachuntersuchung durch den Fragenbogen aus der Studie von Hug ist erkennbar, dass die Unterrichtsreihe Wirkung gezeigt hat. Eine herausstechende Steigerung der

[35] https://www.uni-koblenz-landau.de/de/koblenz/zfl/Veranstaltungen/ThementagDigi (zuletzt abgerufen am 19.09.2018)

Medienkompetenz durch fünf Stunden Unterrichtsangebot ist jedoch kaum zu erwarten, so dass das Thema im Sinne eines Spiralcurriculums später wieder aufgegriffen und vertieft werden sollte. Bei der Adaption ist zu beachten, dass die Reihe der jeweiligen Lerngruppe und den Rahmenbedingungen angepasst wird. Hier können auch weitergehende Einheiten und Differenzierungsmöglichkeiten, beispielsweise auch Stationen mit leichter Sprache, berücksichtigt werden. Eine solche Anpassung wäre insbesondere in Schwerpunktklassen notwendig.

Somit wurde eine Unterrichtsreihe zum Thema *Datenschutz* skizziert, anhand der die Schülerinnen und Schüler erstens ein Interesse dafür entwickeln und zweitens sich dann in das Thema vertiefen.

6.2. Offene / Neue Fragen

In Folgenden sollen noch offene sowie neue Fragen für eine vertiefte Forschung aufgezeigt werden:

- Die in Abschnitt 5.1. beschriebenen Einflussvariablen auf die Umsetzung der Unterrichtsreihe ergeben den Untersuchungsansatz, ob die Unterrichtsreihe in anderen Rahmenbedingungen kompetenzsteigernd umgesetzt werden könnte und ob die noch aufgezeigten Probleme durch andere Rahmenbedingung weniger gravierende Auswirkungen hätten.
- Aktuell entsteht die Masterarbeit von Frau Makosch unter dem Titel "Entwicklung eines Kriterienkatalogs zur Qualität von Unterrichtsmaterialen und Anwendung dessen durch Analyse von Materialien zum Thema Datenschutz". Anhand deren Ergebnisse sollten auch die Materialien dieser Arbeit überprüft und eventuell überarbeitet oder gar ausgetauscht werden.
- Um eine wissenschaftlichere Überprüfung der theoretischen Arbeit zu gewährleisten, sind in der Längsschnittstudie die Ergebnisse des gleichen Testpersonenkreises notwendig. Dann könnte auch die Bewertung der Unterrichtsreihe begründeter erfolgen.
- Des Weiteren wäre an dieser Stelle auch eine Querschnittsstudie bezüglich der Effektivität der Unterrichtsreihe denkbar. So könnte gezeigt werden, ob die Unterrichtsreihe Vorteile gegenüber anderen Umsetzungsideen hat.
- Durch die Tendenz, dass selbst Kinder in der Grundschule ein eigenes Smartphone haben, stellt sich die Frage, ob die Unterrichtsreihe für die Primarstufe angepasst oder gar eine Unterrichtseinheit speziell für die Grundschüler entwickelt werden sollte. Eine Begründung dazu sowie eine praktische Umsetzung dessen würde in Abwandlung dieser Arbeit möglich sein.
- Die Unterrichtseinheit fand in einem Fach mit begrenzter Stundenanzahl statt. Da Datenschutz ein fächerübergreifendes Thema ist, wäre weiterhin zu untersuchen, ob eine Vermittlung von Datenschutzkompetenz innerhalb eines fächerverbindenden Projektes effektiver ist. So könnt an dieser Stelle auch ein Vergleichsversuch zu dieser Arbeit aufgebaut werden.

6.3. Das Datenschutz-Projekt im Rahmen einer Lehrerfortbildung

Zum Abschluss dieser Arbeit wurde die Unterrichtsreihe im Rahmen des Thementages „Digitalisierung im Schulbereich“ des Zentrum für Lehrerbildung der Universität Koblenz-Landau, Campus Koblenz, aktiven Lehrkräften präsentiert. In einem Workshop wurden zwei Gruppen von insgesamt 20 aktiven Lehrkräften die Unterrichtsreihe vorgestellt und sie konnten die zusammengestellten Unterrichtsmaterialien selbst erproben. Da dafür nur 90 Minuten zur Verfügung standen, wurden die Aufgaben der Einstiegsstunde zum Thema *personenbezogene Daten* sowie der Stunde mit den Passwörtern in die Stationenarbeit integriert. Zur Motivation diente die in Abschnitt 4.3 vorgestellte Live-Demo, wobei zuerst die App SnapChat vorgestellt wurde. Danach durften die Lehrkräfte eigenständig die Stationen bearbeiten.

Durch diese Präsentation kann an dieser Stelle eine die Rückmeldung von Personen mit Professionswissen erfolgen:

Die Lehrkräfte sahen die Schwierigkeiten und Schwachstellen im Material, aus denen die in Abschnitt 4.3 beschriebenen Probleme entstanden. So übten sie konstruktive Kritik bezüglich der Textmenge und des Textniveaus, gerade in der Station 1 zu Viren und Trojanern. Auch empfanden sie die geplante Zeit für die einzelnen Stationen zu kurz und beschrieben, dass die damit verknüpften Informationsfülle in kurzer Zeit Schüler einer 6. Klasse überfordern könnte. Eine weitere Anmerkung gab es zur Station 0, dass diese keine besonders gut geplante Station sei, und besser als einzelnes Unterrichtsthema angesprochen werden solle. Dies ist in der vorliegenden Arbeit aber genauso geplant und nur für den Workshop abgeändert worden.

Auf der anderen Seite gaben die Lehrkräfte auch viele positive Rückmeldungen. So hat ihnen die Material und Medienauswahl sowie die Zusammenstellung verschiedener Themen gut gefallen. Herauszugreifen ist auch die Begeisterung der Lehrkräfte zu dem Nutzen aller drei Darstellungsebenen. So können Schüler in dieser Unterrichtsreihe neben symbolischer Darstellung auch gerade beim Rollenspiel oder den Schlössern enaktiv arbeiten. Des Weiteren bekommen die Schüler durch Lightbeam oder den genutzten Videos die Gefahren im Zusammenhang mit dem Thema *Datenschutz* visualisiert, welches die ikonische Darstellungsebene beschreibt.

Drei abschließende Punkte zeigen die gelungene Entwicklung der Unterrichtsreihe und deren Präsentation im Workshop:

1. Das Feedback der Lehrer war sehr positiv, wie in der Evalutationszielscheibe ersichtlich wird. (siehe Anhang A.20)
2. Es kam die Rückfrage, wann die Arbeit abgedruckt werde und wo die Materialien dann zu beziehen seien.

3. Im Workshop haben viele Lehrkräfte selbst neue Erkenntnisse erlangt und es wird sich diesbezüglich auch eine Lehrerfortbildung gewünscht.

Die abschließende öffentliche Präsentation zeigte, dass das Thema *Datenschutz* im Sinne von IniK und als Kriterium der fundamentalen Ideen der Informatik sowohl lebensweltorientiert als auch langlebig ist, sodass weitere Anstrengungen unternommen werden sollten, das Thema im Unterricht, mit durchaus anderen als hier vorgestellten Methoden sowie auch fächerübergreifend, zu integrieren und zu fördern.

A. Anhang

Fragen zur Vorbereitung des Unterrichts zum Thema Datenschutz

Besitzt du einen eigenen Computer? Ja / Nein

Welche drei Internetseiten / Soziale Netzwerke nutzt du am häufigsten?

_____

_____

_____

Besitzt du ein eigenes Handy? Ja / Nein

Welche drei Apps nutzt du am häufigsten:

_____

_____

_____

Was interessiert dich zum Thema Datenschutz?

_____

_____

_____

	Anzahl	Prozent
Teilnehmer	26	
Computerbesitzer	15	58%
Smartphonebesitzer	26	100%

Tabelle 5: Nutzung von Computer und Smartphones

Internetseiten[36]	**Nutzer**	**Prozent**
YouTube	20	76,9%
Instagram	12	46,2%
WhatsApp	10	38,5%
(Snapchat)	8	30,8%
Google	3	11,5%
Twitch	2	7,7%
Pinterest	1	3,8%
panzoid.com	1	3,8%
discord.com	1	3,8%
epicgames.com	1	3,8%
Twitter	1	3,8%
PlayStationNetwork	1	3,8%

Tabelle 6: Nutzung von Internetseiten

Soziale Netzwerke[31]	**Nutzer**	**Prozent**
YouTube	20	76,9%
Instagram	12	46,2%
WhatsApp	10	38,5%
Snapchat	8	30,8%
musical.ly	5	19,2%
(Google)	3	11,5%
Twitch	2	7,7%
Pinterest	1	3,8%
PlayStationNetwork	1	3,8%
panzoid.com	1	3,8%
discord.com	1	3,8%
Twitter	1	3,8%
epicgames	1	3,8%

Tabelle 7: Nutzung Sozialer Netzwerke

Apps	**Nutzer**	**Prozent**
YouTube	17	65,4%
WhatsApp	14	53,8%
Snapchat	11	42,3%
Instagram	8	30,8%
Spiele[37]	8	30,8%
Playstore	4	15,4%
musical.ly	4	15,4%
Wetter	3	11,5%
Google	2	7,7%
Kalender	1	3,8%
Discord	1	3,8%
Twitter	1	3,8%

Tabelle 8: Nutzung von Apps

[36] Die Tabellen 2 und 3 entstammen aus einer Frage, wobei die Antworten den Kategorien zu sortiert wurden. Hierbei steht SnapChat in Tabelle 2 in Klammern, da die Internetseite nur Werbefläche ist und Dokumente, wie AGBs und Datenschutzerklärung enthält. Genauso auch in Tabelle 3 wurde Google vermutlich nicht als das Soziale Netzwerk Google+ verstanden.

[37] Hier wurden alle genannten Spiele-Apps zusammengefasst

UNIVERSITÄT KOBLENZ · LANDAU

PERSÖNLICHE DATEN

Nicht alle Daten sind aus Datenschutzgründen korrekt!

Name: Johannes Thielen.

Geboren: 21.12.1992 in Landau

Wohnort: Himmelsstraße 13 in Koblenz (56068)

Handynummer: 0111/222333444

Emailadresse: jthielen@uni-koblenz.de

Haus verlassen: um 7:30

Aktueller Aufenthalt: Raum E1 im Hilda-Gymnasium:

GPS-Koordinaten: 50° 21'04.1"N, 7° 35'44.6"E

Mein Lieblingsbäcker ist die Bäckerei Ollig.

Ich mag die TUS Koblenz und interessiere mich für Autos.

Ich bin bei den Pfadfindern FrisKo.

2

UNIVERSITÄT KOBLENZ · LANDAU

AUSZUG: ALLGEMEINE GESCHÄFTSBEDINGUNGEN

… gewährst du Snap Inc. eine weltweite, gebührenfreie, übertragbare Lizenz zum Hosten, Speichern, Verwenden, Anzeigen, Reproduzieren, Verändern, Anpassen, Bearbeiten, **Veröffentlichen** und **Verteilen aller Inhalte**, die du an die Services übermittelst.

… erteilst du uns außerdem eine **zeitlich unbegrenzte Lizenz**, aus den öffentlichen Inhalten abgeleitete Werke zu erstellen sowie sie zu bewerben, auszustellen, auszustrahlen, […], **öffentlich vorzuführen** und öffentlich darzustellen, und zwar in jeder Form und in beliebigen […] Medien und Vertriebskanälen.

… gewährst du Snap Inc. das zeitlich unbegrenzte Recht […] **deinen Namen**, **dein Bild** und **deine Stimme** zu nutzen, und zwar auch in Verbindung mit **gewerblichen** oder gesponserten Inhalten.

6

Thema: Datenschutz

09.08.2018

Lehrkraft: Herr Thielen

Persönliche Daten

Arten von persönliche Daten	Kann man veröffentlichen	Grund der (nicht) Veröffentlichung	Gefahren bei Veröffentlichung
Name	Ja / Nein	Zum Auffinden der Profilseite, besser Spitzname als Pseudonym verwenden	Automatisierte Profilbildung ermöglicht
Geburtsdatum	Nein	Ermöglicht Identitätsdiebstahl, sowie eine genauere Profilbildung.	Identitäsdiebstahl
Wohnort	Nein	Guten Freunden kann man die Adresse persönlich mitteilen	Überwachung und Einbruchsmöglichkeit
Telefonnummer	Nein	Guten Freunden, die einen Anrufen sollen, kann man die Nummer persönlich mitteilen	Missbrauch für Fake-Anrufe
E-Mail-Adresse	Ja / Nein	Zur Identifikation wird diese gebraucht, bei unsicheren Seiten eine Spam-Adresse verwenden	Spam- und Phsing-Mails
Standort /GPS-Koordinaten	Nein	Ermöglicht genaue Überwachung und Nachverfolgung	Überwachung
Interessen	Ja / Nein	Selbstdarstellung	Profilbildung und Missbrauch für Werbezwecke
Hobbies	Ja	Selbstdarstellung	Profilbildung und Missbrauch für Werbezwecke
Bilder	Nein	Unkontrollierbare Weiterverwendung der Bilder	Missbrauch für andere Zwecke

AB: Persönliche Daten **Thema Datenschutz** 09.08.2018

Name: Klasse 6.2 Lehrkraft: J.Thielen

Aufgabe 1. Übertrage von der Tafel 5 Arten von persönlichen Daten.

Aufgabe 2. Kreuze in der zweiten Spalte an, ob du diese Daten veröffentlichen würdest.

Aufgabe 3. Schreibe in die nächste Zeile, weshalb du dich für oder gegen das Veröffentlichen entschieden hast.

Aufgabe 4. Überlege mit deinem Tischnachbarn, welche Gefahren durch die Veröffentlichung der Daten entstehen können und notiert eure Ergebnisse in der letzten Spalte. (Als Hilfestellung könnt ihr den Text auf der Rückseite gemeinsam lesen.)

Persönliche Daten	Kann man veröffentlichen	Grund der (nicht) Veröffentlichung	Gefahren bei Veröffentlichung

Datenschutz-Gefahren: Das Ausspähen von personenbezogenen Daten

Im Internet existieren viele Datenschutz-Gefahren, die dem Nutzer schaden können.

Immer häufiger bist du im Internet unterwegs. Hierbei entsteht eine große Menge an Daten über dich. Manche gibst du selber an, etwa wenn du dich in einer eine App anmeldest oder deine Daten (Nachrichten) in einem sozialen Netzwerk veröffentlichst. Andere Daten entstehen, wenn du zum Beispiel ein Video auf YouTube schaust oder im Playstore nach den neuesten Spielen suchst und Google deine Suchanfragen auswertet.

Grundsätzlich lassen sich die Datenschutz-Gefahren einteilen in zwei Arten, die unterschiedliche Zwecke verfolgen:

1. **Werbezwecke**

Soziale Netzwerke wollen für Werbezwecke zum Beispiel so viele persönliche Daten wie nur möglich haben, um ein genaues Profil des Nutzers zu erstellen. Dazu werden nicht nur Eingaben der Person genutzt, sondern man verfolgt auch die Aktivitäten und Interaktionen zwischen Nutzern und wertet diese aus. Anhand des Profils lässt sich maßgeschneiderte Werbung schalten, mit welcher solche Seiten mehr Geld als mit gewöhnlicher Werbung verdienen.

2. **Kriminelle / missbräuchliche Zwecke**

Bei missbräuchlichen Zwecken werden deine Daten abgegriffen, um dir zu schaden. So kann mit erbeuteten Informationen beispielsweise Identitätsdiebstahl begangen werden. In deinem Namen werden dann Handlungen in krimineller Art verübt, von denen du keine Kenntnis hast.

Im Falle des Stehlens von Bank- oder Kreditkartendaten ist der Schaden finanzieller Natur. Kriminelle können dann Zugriff auf dein Geld erlangen. Dies passiert beispielsweise dann, wenn du (oder deine Eltern) Zahlungsdaten über eine ungesicherte Verbindung übermittelst.

Meistens geht es dabei also um Geld. Allerdings kann es im missbräuchlichen Bereich auch zu **persönlichen Schädigungen** kommen, etwa durch Cybermobbing.

Anhang A. 6. Eigenschaften eines Fotos

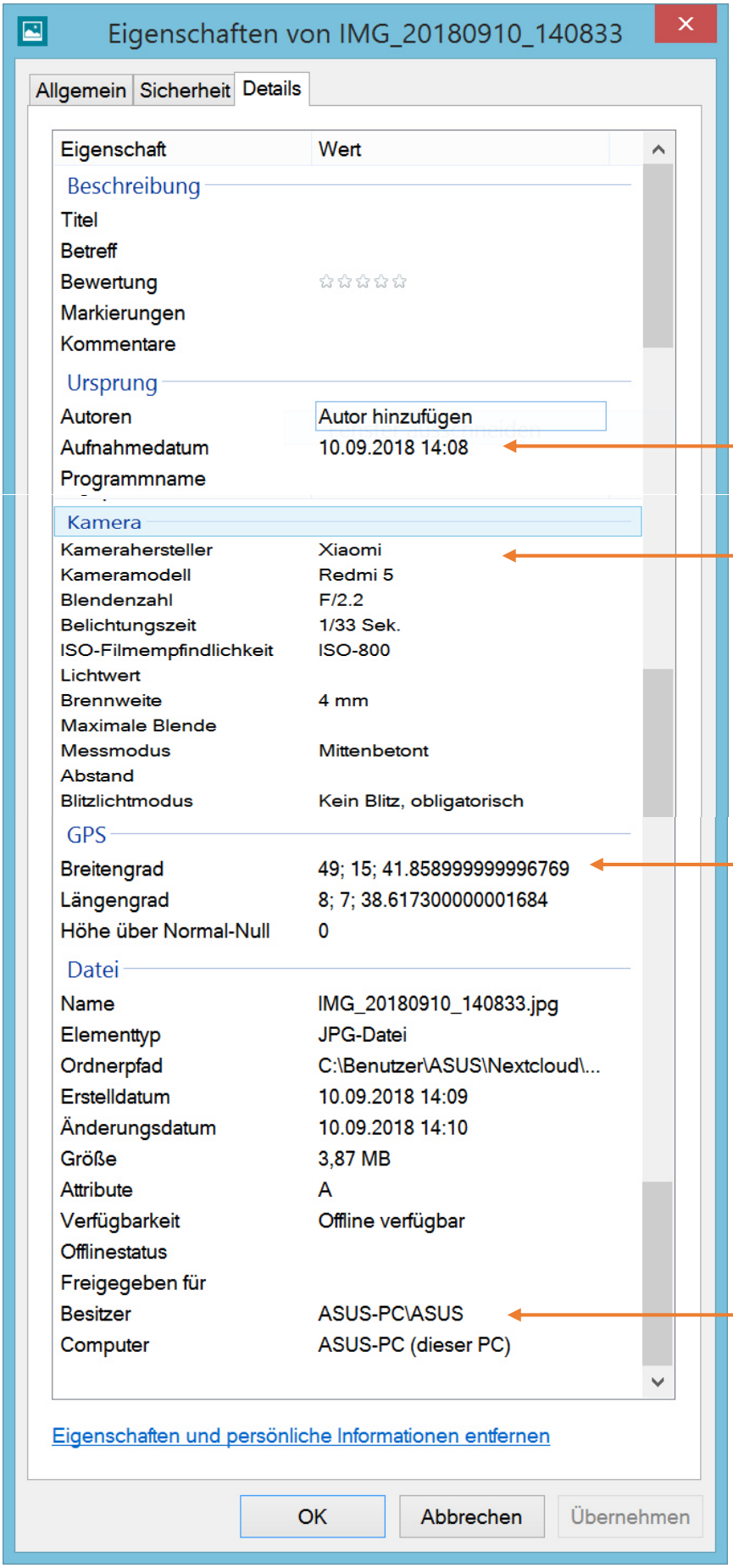


Abbildung 1: Eigenschaften eines Fotos

Anhang A. 7. Bild der Stadt ohne und mit privatem Foto auf den Werbeflächen

Abbildung 2: Stadt mit Werbeflächen

Abbildung 3: Stadt mit persönlichem Foto auf den Werbeflächen

Die Bilder zeigen die Werbeflächen am Piccadilly Circus in London,

Aufgenommen von Diego Delso, weiterbearbeitet unter der Lizenz (CC BY-SA 4.0).

Quelle: https://de.wikipedia.org/wiki/Piccadilly_Circus#/media/File:

Pabell%C3%B3n_de_Londres,_Piccadilly_Circus,_Londres,_Inglaterra,_2014-08-11,_DD_158.JPG

Stationenarbeit

Immer zu zweit!

Station am Platz bearbeiten,

außer

Station 3, diese zu viert in einer Ecke.

Station 6, diese zu zweit am PC.

Station 4 und Station 5, nur die Videos am PC schauen.

danach die Aufgaben am Platz bearbeiten.

Eine Station vollständig bearbeiten:

1. Stationsaufgabe(n) lesen.
   Bei Fragen melden.
2. Stationsaufgabe bearbeiten
3. Dem Partner, der Partnerin die Lösung erklären.
4. Gegenseitig Laufzettel abstempeln.
5. Station so verlassen, wie man diese vorgefunden hat.

Unbekannte Begriffe an die Tafel schreiben.

Die Regeln wurden auf zwei Din A3 Plakate gedruckt und sichtbar an die Tafel gehängt.

Anhang A. 9. Erläuterung der Stationen

Stationenbeschreibung
Viren und Trojaner

An dieser Station gibt es zwei Arbeitsblätter, die ihr an eurem Platz bearbeiten könnt.

Löst diese zu zweit, indem Schüler A das Arbeitsblatt zum Thema Viren und Schüler B das Arbeitsblatt zum Thema Trojaner bearbeitet. Die letzte Aufgabe auf beiden Arbeitsblättern ist das gegenseitige Vorstellen der Ergebnisse.

Stationenbeschreibung
Rechte und Gesetze

An dieser Station gibt es ein Arbeitsblatt von klicksafe, welches ihr an eurem Platz bearbeiten könnt.

Lest die vordere Seite zuerst allein, dann helft euch gegenseitig bei Fragen zu den Gesetzen. Die Aufgabe auf der Rückseite bearbeitet ihr zuerst alleine bevor ihr sie am Ende mit eurem Partner / eurer Partnerin vergleicht.

Stationenbeschreibung
Browserverlauf und Cookies

An dieser Station müsst ihr anfangs zu viert arbeiten, setzt euch dazu mit den Blättern des Rollenspiels in eine Ecke und lest den Text in verteilten Rollen.
An den Stellen mit einem ➔ Pfeil übergebt ihr die genannten Zettel.

Räumt am Ende die Zettel wieder in die richtigen Umschläge zurück, damit die nächsten Gruppen direkt starten können!

Im Anschluss daran bearbeitet ihr das Arbeitsblatt Cookies / Browserverlauf an eurem Arbeitsplatz.
Vergleicht eure Definition von Cookies und tauscht euch über die erdachten Gefahren aus.

Stationenbeschreibung
Berechtigungen von Apps

An dieser Station gibt es zwei Arbeitsblätter, die ihr an eurem Platz bearbeiten könnt.

Bearbeitet zuerst das Blatt App-Berechtigungen.

Das Video (Station 4) zum Einstieg könnt ihr an einem Computer anschauen.
Setzt euch danach an euren Platz zurück.
Helft euch bei der zweiten Aufgabe gegenseitig, die Seite der Berechtigungen auf eurem Handy zu finden.

Bearbeitet das zweite Arbeitsblatt zuerst alleine, bevor ihr mit eurem Partner / eurer Partnerin in einen Dialog startet.

Stationenbeschreibung
Bewegungsdaten

An dieser Station gibt es ein Arbeitsblatt.

Das Video der Station 5 schaut ihr euch zuerst an einem Computer an. Denkt daran beim Videoschauen, euch Fragen für die Partnerin / den Partner aufzuschreiben.

Geht zurück an euren Platz und beantwortet die Fragen des Partners / der Partnerin.

Stationenbeschreibung
Software für Datenschutz

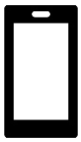
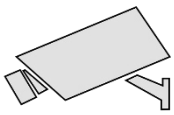
An dieser Station gibt es ein Arbeitsblatt, welches zuerst an eurem Platz und dann an einem PC bearbeiten könnt. Ist kein PC frei, bearbeitet zuerst eine andere Station.

Löst das Arbeitsblatt gemeinsam. Informationen zu Aufgabe 1 könnt ihr auf dem Blatt „InfoB: Software zum Datenschutz“ nachlesen. Für die folgenden Aufgaben startet ihr den Browser Firefox am Computer (die Add-Ons sind aktiviert).

Nach Bearbeiten der Aufgabe, aktiviert ihr die Add-Ons wieder oder meldet euch bei der Lehrkraft, damit dieser den Browser wieder in den Anfangsstatus zurückversetzen kann.

Laufzettel Stationenarbeit Thema Datenschutz 09.08.2018

Name: Klasse 6.2 Lehrkraft: J.Thielen

	Thema:	Erledigt:
 	Viren und Trojaner	
	Rechte und Gesetze	
	Cookies und Browser	
 	App-Berechtigungen	
	Bewegungsdaten	
 	Software für Datenschutz	

Anhang A. 11. Arbeitsblätter der Stationen

Anhang A. 11.1. Station 1: Viren und Trojaner (4.Seiten)

AB: Viren | Thema Datenschutz | 09.08.2018

Name: | Klasse 6.2 | Lehrkraft: J.Thielen

Aufgabe 1. Lese dir folgende Definitionen von Schadsoftware durch. Bei Unklarheiten kannst du im Anschluss deine Partnerin / deinen Partner fragen, wie er die Sache versteht.

Ein ganzer Zoo im Computer und auf dem Handy?

Ein wenig digitale Biologie?
Auf unserem Computer, Smartphone oder Tablet können sich zahllose Schädlinge tummeln.

Computerviren
Darunter sind solche Dinge gefasst wie Bootviren (dann startet der Computer erst gar nicht mehr), Makroviren (weit verbreitet in Office-Programmen), Datei-Viren (sie starten mit einem Programm), Polymorphe Viren (sie heißen so, weil sie sich gut verkleiden können und ständig verwandeln) und die Tarnkappen-Viren (die sich besonders gut verstecken können).

Rogueware
Rogueware ist besonders perfide: Diese Software gaukelt vor, andere Schadsoftware zu entfernen, tut aber das Gegenteil.

SpyApps
SpyApps zeichnen unbemerkt die Kommunikation auf, schalten Mikrofon und Kamera ein oder leiten den Standort des Handys weiter.

Scareware werden gefälschte Warnmeldungen u. ä. bezeichnet, die den Nutzer verunsichern und dazu verleiten sollen, andere Software zu installieren.

„Würmer"
Ein Wurm kann sich selbst vervielfältigen und automatisch Kopien verschicken. Er braucht auch kein anderes Programm (wie ein Virus), sondern arbeitet ganz selbstständig.

„Trojaner" – Trojanische Pferde
(Kennst du die Sage vom Trojanischen Pferd?) Ein Trojaner benutzt einen gemeinen Trick. Das Virus gibt vor, etwas anderes zu sein (z. B. ein Spiel oder nützliches Programm): Kaum hast du es aufgerufen, befällt es deinen Computer. In diesen Trojaner kann auch ein Spionageprogramm versteckt sein, das deinen Computer auskundschaftet (und deine Passwörter munter weiterleitet).

Hoaxes
Ein Hoax (zu Deutsch: „Jux", „Schabernack" oder „Schwindel") ist nichts anderes als eine Falschmeldung, die von Person zu Person verbreitet wird (z. B. via SMS, WhatsApp- oder Facebook-Nachricht). Ein Hoax besteht meist aus drei Elementen; einem Aufhänger, der Echtheit vermitteln soll, gefolgt von einer Aufklärung über die aus dem Internet drohende Gefahr und der abschließenden Bitte, diese Information an so viele Internetnutzer wie möglich weiterzuleiten. Echte Virus-Warnungen werden nie auf diese Weise verschickt.

Und wie kommen diese Viren, Würmer, Trojaner und Hoaxes auf deinen Computer und in dein Handy? Und wie kannst du dich davor schützen?

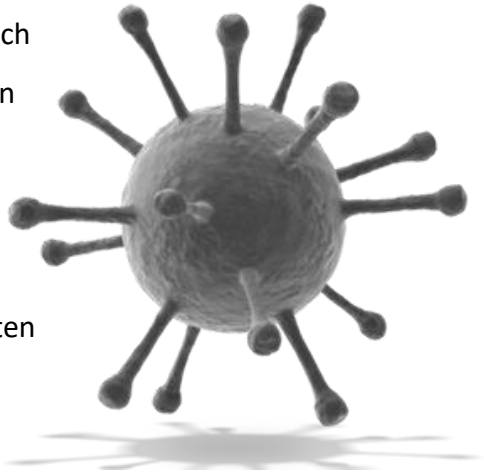
(aus Klicksafe - Datenschutz geht zur Schule)

Aufgabe 2. Informiere dich über das Problem von Viren in dem Text auf der Rückseite.

Aufgabe 3. Erstelle eine Kurzanleitung für einen Handynutzer, wie er sich dagegen schützen kann.

Aufgabe 4. Stelle deinem Partner/ deiner Partnerin das Problem und die Schutzmaßnahmen vor.

Virenschutzprogramme



Ein Virus für deinen PC oder das Smartphone so ähnlich wie für dich eine Grippe. Nur, dass du deinen Computer nicht zum Arzt bringen musst. Wichtiger ist vielmehr, ihn vor der Infektion zu schützen. Das kannst tun, indem du ein Anti-Viren-Programm installierst. Unter Windows ist eine gute Antiviren-Software unerlässlich, da Windows-Rechner aufgrund ihrer weiten Verbreitung am häufigsten angegriffen werden.

Antiviren-Software überprüft neue Dateien (zum Beispiel Anhänge von E-Mails) und den gesamten Computer auf Anzeichen einer Infektion. Dazu vergleicht sie in erster Linie die Daten auf deinem Rechner mit den „Fingerabdrücken“ bekannter Schadprogramme. Diese „Signaturen“ müssen aber immer auf dem aktuellen Stand sein, weil täglich neue Varianten von Schädlingen auftreten. Deshalb musst du die Software regelmäßig aktualisieren (updaten).

Früher mussten die Benutzer das Viren-Schutzprogramm in regelmäßigen Zeitabständen starten und dann wurde die ganze Festplatte, einzelne Laufwerke, Disketten oder CD-ROMs überprüft. Heute ist es viel einfacher. Wenn die Auto-Schutz-Funktion eingeschalten ist, überprüft das Programm deinen Rechner nach jedem Systemstart automatisch im Hintergrund. Du erkennst das am Icon in der Task-Leiste. Wird ein Virus gefunden oder hat der Scanner etwas Verdächtiges bemerkt, erhältst du eine Nachricht in einem Mitteilungsfenster.

Nach: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Schutz-programme/Virenschutzprogramme/virenschutzprogramme_node.html (Abgerufen am 04.08.2018)

AB: Trojaner | Thema Datenschutz | 09.08.2018

Name: | Klasse 6.2 | Lehrkraft: J.Thielen

Aufgabe 1. Lese dir folgende Definitionen von Schadsoftware durch.
Bei Unklarheiten kannst du im Anschluss deine Partnerin / deinen Partner fragen, wie er die Sache versteht.

Ein ganzer Zoo im Computer und auf dem Handy?

Ein wenig digitale Biologie?
Auf unserem Computer, Smartphone oder Tablet können sich zahllose Schädlinge tummeln.

Computerviren
Darunter sind solche Dinge gefasst wie Bootviren (dann startet der Computer erst gar nicht mehr), Makroviren (weit verbreitet in Office-Programmen), Datei-Viren (sie starten mit einem Programm), Polymorphe Viren (sie heißen so, weil sie sich gut verkleiden können und ständig verwandeln) und die Tarnkappen-Viren (die sich besonders gut verstecken können).

Rogueware
Rogueware ist besonders perfide: Diese Software gaukelt vor, andere Schadsoftware zu entfernen, tut aber das Gegenteil.

SpyApps
SpyApps zeichnen unbemerkt die Kommunikation auf, schalten Mikrofon und Kamera ein oder leiten den Standort des Handys weiter.

Scareware werden gefälschte Warnmeldungen u. ä. bezeichnet, die den Nutzer verunsichern und dazu verleiten sollen, andere Software zu installieren.

„Würmer"
Ein Wurm kann sich selbst vervielfältigen und automatisch Kopien verschicken. Er braucht auch kein anderes Programm (wie ein Virus), sondern arbeitet ganz selbstständig.

„Trojaner" – Trojanische Pferde
(Kennst du die Sage vom Trojanischen Pferd?) Ein Trojaner benutzt einen gemeinen Trick. Das Virus gibt vor, etwas anderes zu sein (z. B. ein Spiel oder nützliches Programm): Kaum hast du es aufgerufen, befällt es deinen Computer. In diesen Trojaner kann auch ein Spionageprogramm versteckt sein, das deinen Computer auskundschaftet (und deine Passwörter munter weiterleitet).

Hoaxes
Ein Hoax (zu Deutsch: „Jux", „Schabernack" oder „Schwindel") ist nichts anderes als eine Falschmeldung, die von Person zu Person verbreitet wird (z. B. via SMS, WhatsApp- oder Facebook-Nachricht). Ein Hoax besteht meist aus drei Elementen; einem Aufhänger, der Echtheit vermitteln soll, gefolgt von einer Aufklärung über die aus dem Internet drohende Gefahr und der abschließenden Bitte, diese Information an so viele Internetnutzer wie möglich weiterzuleiten. Echte Virus-Warnungen werden nie auf diese Weise verschickt.

Und wie kommen diese Viren, Würmer, Trojaner und Hoaxes auf deinen Computer und in dein Handy? Und wie kannst du dich davor schützen?

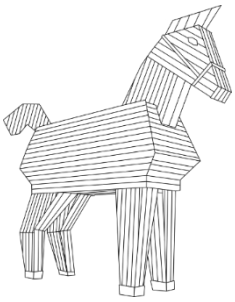
(aus Klicksafe - Datenschutz geht zur Schule)

Aufgabe 2. Informiere dich über das Problem von Trojanern in dem Text auf der Rückseite.

Aufgabe 3. Erstelle eine Kurzanleitung für einen Handynutzer, wie er sich dagegen schützen kann.

Aufgabe 4. Stelle deinem Partner/ deiner Partnerin das Problem und Schutzmaßnahmen vor.

Trojaner



Trojanische Pferde – auch kurz nur Trojaner genannt – verdanken ihren Namen der Sage vom hölzernen Pferd des Odysseus, in dessen Bauch sich griechische Soldaten verbargen. Die arglosen Einwohner Trojas holten mit dem Holz-Pferd eigenhändig den Feind in das Innere der umkämpften Stadt – und besiegelten damit ihren Untergang.

Eine ähnliche List wenden Trojaner-Entwickler an: Sie tarnen ihre Malware als nützliches Programm und hoffen darauf, dass arglose Nutzerinnen und Nutzer sie eigenhändig installieren. Denn anders als Viren und Würmer verfügen Trojaner über keinen Mechanismus zur Selbst-Reproduktion. Stattdessen ist Täuschung ihre Verbreitungsstrategie.

Cyber-Kriminelle versuchen, fremde Systeme über unterschiedlichste Kanäle mit Schadsoftware zu infizieren – zum Beispiel per Dateianhang einer scheinbar vertrauenswürdigen E-Mail, als versteckte "Zugabe" bei einem Freeware-Download oder als bösartiges Makro innerhalb eines Office-Dokuments. Manchmal genügt der bloße Aufruf einer Webseite mit einem präparierten Werbebanner – und schon ist der eigene Computer mit einem Schadprogramm infiziert.

Nach: https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/Schadprogramme/Trojanische Pferde/trojanischepferde_node.html (Abgerufen am 04.08.2018)

Malwareschutz: Android-Trojaner stiehlt Messenger-Daten

Sicherheitsexperten haben eine Android-Malware aufgespürt, die Daten aus Messenger-Apps abgreift. Im Visier des Trojaners sind verschiedene Apps, wie zum Beispiel: Facebook Messenger und Skype. Nutzer können sich davor schützen, indem sie Virenschutz-Programme verwenden. Diese sind auch für mobile Geräte verfügbar, insbesondere solche, die Android-basiert sind. Denn gerade das Betriebssystem Android ist immer wieder anfällig für Malware, auch in Deutschland. Größtes Problem dabei ist die fehlende Aktualität der Betriebssysteme von Android-Smartphones. Um sich zu schützen, sollte man deshalb stets darauf achten, dass das Smartphone auf dem aktuellen Stand ist und man Apps immer nur aus dem offiziellen Google Playstore herunterlädst. Zudem sollte man dafür sorgen, dass ein Basisschutz vorhanden ist, beispielsweise in Form von einer Antiviren-Lösung.

Nach: https://www.bsi-fuer-buerger.de/SharedDocs/Newsletter/DE/BSIFB/BuergerCERT-Newsletter/08_Sicher-Informiert_12-04-2018.html (Abgerufen am 04.08.2018)

Arbeitsblatt vom Name:

Aufgabe 1: Lest die Gesetzestexte alleine. Markiert euch dabei die wichtigsten Punkte.
Aufgabe 2: Erklärt euch gegenseitig in eigenen Worten, worum es in den Gesetzen geht.

Recht und Gesetz und meine Daten

Selbstverständlich gibt es in Deutschland viele Gesetze, die festlegen, wie man mit persönlichen Daten umgehen muss. Hier lernst du einige wichtige kennen.

Bundesdatenschutzgesetz und Landesdatenschutzgesetze

Das Bundesdatenschutzgesetz regelt die Datenverarbeitung der öffentlichen Stellen des Bundes (z. B. Bundesbehörden, bundesunmittelbare Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts usw.) sowie der nicht öffentlichen Stellen (z. B. Händler, Dienstleister, Einzelfirmen, Selbständige, Rechtsanwälte, Ärzte usw.).

Alle Länder haben darüber hinaus für ihre öffentlichen Stellen (z. B. Landesbehörden, Landesanstalten, Landeskörperschaften usw.) eigene Landesdatenschutzgesetze erlassen.

Sowohl das Bundesdatenschutzgesetz als auch die Landesdatenschutzgesetze enthalten wichtige Details zum „Recht auf informationelle Selbstbestimmung". Das informationelle Selbstbestimmungsrecht wurde vom Bundesverfassungsgericht im sog. Volkszählungsurteil vom 15.12.1983 geprägt und leitet sich aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 des Grundgesetzes ab. Grundsätzlich besagt dieses Recht, dass jeder selbst über die Verwendung seiner personenbezogenen Daten bestimmen darf. Die Datenschutzgesetze legen z. B. fest, wie Behörden mit den Daten der Bürger umgehen müssen. Dies gilt etwa für den Umgang mit den Schüler-, Eltern- und Lehrerdaten in der Schule. So dürfen nur die zur Aufgabenerfüllung der Schulen erforderlichen Daten erhoben werden und nur für diesen Zweck verarbeitet und genutzt werden.

Wichtig ist, dass das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen oder Nutzen von Daten nur zulässig ist, wenn dies entweder ausdrücklich durch ein Datenschutzgesetz oder eine andere Rechtsvorschrift erlaubt bzw. angeordnet ist oder der Betroffene zuvor hierin eingewilligt hat.

In den Datenschutzgesetzen sind auch die Rechte der Betroffenen beschrieben. Jeder Bürger hat ein Auskunftsrecht, d. h. er darf nachfragen, was über ihn gespeichert ist. Er hat auch einen Anspruch auf Richtigstellung oder in bestimmten Fällen einen Anspruch auf Sperrung oder sogar Löschung seiner Daten. Ebenfalls kann der Betroffene eine erteilte Einwilligung jederzeit widerrufen. Schließlich kann sich jedermann an den zuständigen Bundes- bzw. Landesdatenschutzbeauftragten wenden, wenn er sich durch den Umgang mit seinen personenbezogenen Daten in seinem informationellen Selbstbestimmungsrecht beeinträchtigt sieht.

Kunsturheberrechtsgesetz

§ 22 „Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden." Dies nennt man auch Recht am eigenen Bild. Es bedeutet, du alleine bestimmst, welche Fotos von dir veröffentlicht werden. Ganz wichtig: Wer ohne dein Einverständnis Bilder von dir ins Netz stellt, macht sich strafbar! Es gibt übrigens Ausnahmen für berühmte Persönlichkeiten wie Sportler, Schauspieler oder Politiker.

Strafgesetzbuch

§ 201a Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen
„(1) Wer von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt Bildaufnahmen herstellt oder überträgt und dadurch deren höchstpersönlichen Lebensbereich verletzt, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft."
Wer also heimlich Fotos in einer Umkleidekabine macht, der macht sich strafbar!

Quelle: klicksafe - Datenschutz geht zur Schule

Arbeitsblatt vom **Name:**

Aufgabe 3:
Und leider gibt es – wahrscheinlich überall – Menschen, die sich nicht an die Gesetze halten. Dr. Tafel ist so einer, der es nicht ganz genau nimmt mit dem „Datenschutz": Kreuze an, ob er das darf (ja) oder nicht (nein)

	Darf er das?	ja	nein
A.	Dr. Tafel fragt die Schulsekretärin nach einer Klassenliste der 7b.		
B.	Dr. Tafel fotografiert alle Schülerinnen und Schüler der 7b – ohne deren Einverständnis.		
C.	Dr. Tafel fragt die Schüler, ob er sie fotografieren dürfe. Er fotografiert nur mit Einverständnis.		
D.	Dr. Tafel veröffentlicht die Fotos auf seiner privaten Homepage.		
E.	Dr. Tafel veröffentlicht die Fotos auf der Schulhomepage.		
F.	Dr. Tafel verkauft die Liste der Schülernamen an einen Schulbuchverlag.		
G.	Dr. Tafel gibt die Liste kostenlos an den Schulkiosk-Besitzer weiter, der Werbung verschickt.		
H.	Dr. Tafel speichert die Schülerfotos auf seinem privaten Laptop.		
I.	Dr. Tafel filmt im Unterricht heimlich zwei Schüler die stören.		
J.	Dr. Tafel stellt das Video der störenden Schüler auf YouTube ein – heimlich.		
K.	Dr. Tafel macht einen Unterrichtsversuch und fragt die Eltern, ob er den Versuch filmen dürfe.		
L.	Dr. Tafel erhält einen Anruf einer besorgten Mutter, die das Foto ihres Kindes auf der Schulhomepage löschen lassen möchte. Muss er?		

Wer wissen möchte, wie und welche Daten in Social Communities wie Youtube oder Snapchat *„verarbeitet" werden, der schaut mal in die „Datenschutzerklärung" und in die „Allgemeinen Geschäftsbedingungen" (AGB)*

Arbeitsaufträge:

Aufgabe 4: Vergleiche deine Antworten mit deinem Partner / deiner Partnerin.

Aufgabe 5: Überprüft eure Antworten mit dem Lösungsblatt. Solltet ihr ein anderes Ergebnis haben, lest das angegeben Gesetz erneut nach.

Quelle: klicksafe - Datenschutz geht zur Schule

	Darf er das?	ja	nein
A.	Dr. Tafel fragt die Schulsekretärin nach einer Klassenliste der 7b. Ja, denn die Schule darf (auf gesetzlicher Grundlage) Daten verarbeiten, ohne eine Klassenliste wäre sein Job als Lehrer nicht möglich.	×	
B.	Dr. Tafel fotografiert alle Schülerinnen und Schüler der 7b – ohne deren Einverständnis. Nein, das „Recht am eigenen Bild" gilt auch und besonders für Minderjährige, gerade wenn das Bild veröffentlicht werden soll. Aber Vorsicht: Es schützt eigentlich nur vor Veröffentlichung, nicht vor der Fotografie an sich! Wenn man aber Befürchtungen hat, das Bild könnte veröffentlich werden, kann man die Löschung vorab verlangen.		×
C.	Dr. Tafel fragt die Schüler, ob er sie fotografieren dürfe. Er fotografiert nur mit Einverständnis. Ja, aber hier gilt auch eine Altersgrenze: Wenn vorausgesetzt werden kann, dass die Minderjährigen den Sinn und Zweck verstehen, müssen sie und die Eltern zustimmen. Oft wird die Grenze bei 12 oder 14 Jahren (14 ist die Regel) gesehen. Bei jüngeren Kindern genügt die Zustimmung der Eltern.	×	
D.	Dr. Tafel veröffentlicht die Fotos auf seiner privaten Homepage. Nein, natürlich nicht. Niemand darf die Fotos ohne Einverständnis veröffentlichen, auch nicht zu privaten (und nicht-kommerziellen) Zwecken.		×
E.	Dr. Tafel veröffentlicht die Fotos auf der Schulhomepage. Nein, auch das nicht. Es sei denn, es liegt das Einverständnis vor – der Schülerinnen und Schüler bzw. bei Minderjährigen: der Eltern!		×
F.	Dr. Tafel verkauft die Liste der Schülernamen an einen Schulbuchverlag. Nein, das kostet ihn wahrscheinlich den Job!		×
G.	Dr. Tafel gibt die Liste kostenlos an den Schulkiosk-Besitzer weiter, der Werbung verschickt. Nein, die Weitergabe von Daten ist strikt verboten, auch an Bekannte, Freunde oder Verwandte. Schulsekretärinnen dürfen bspw. auch am Telefon keine Auskunft über einzelne Schülerinnen / Schüler geben.		×
H.	Dr. Tafel speichert die Schülerfotos auf seinem privaten Laptop. Hierfür braucht er die Genehmigung der Schulleitung; das gilt i.ü. nicht nur für Fotos, sondern auch für sonstige personenbezogenen Schülerdaten; außerdem muss sich Dr. T. damit einverstanden erklären, dass sein Laptop so wie dienstliche Geräte kontrolliert werden können; und den Belangen des Datenschutzes muss ebenfalls Rechnung getragen werden.		×
I.	Dr. Tafel filmt im Unterricht heimlich zwei Schüler die stören. Nein! (Kein Kommentar!) Das Recht am eigenen Bild und dann noch heimlich!		×
J.	Dr. Tafel stellt das Video der störenden Schüler auf YouTube ein – heimlich. Nein, auch hierfür würde er wohl seinen Job verlieren.		×
K.	Dr. Tafel macht einen Unterrichtsversuch und fragt die Eltern, ob er ihn filmen dürfe. Ja, natürlich nur, wenn auch alle Eltern (und Kinder) ihr Einverständnis geben.	×	
L.	Dr. Tafel erhält einen Anruf einer besorgten Mutter, die das Foto ihres Kindes auf der Schulhomepage löschen lassen möchte. Muss er? Es ist umstritten, ob und unter welchen Voraussetzungen eine Einwilligung widerrufen werden kann. Gerichte haben hierzu unterschiedliche Entscheidungen getroffen. Nach einer Ansicht ist die Einwilligung wie ein Vertrag zu behandeln und daher rechtsverbindlich und nur unter den gesetzlich vorgesehenen Voraussetzungen rückgängig zu machen. Nach anderer Ansicht ist eine Einwilligung zwar generell widerruflich, allerdings nur, wenn ein gewichtiger Grund vorliegt. Deshalb sollte Dr. Tafel die Sorgen der Mutter ernst nehmen und versuchen, mit ihr eine gute Lösung zu finden. Für datenschutzrechtliche Einwilligungserklärungen gilt das wiederum nicht, die können tatsächlich frei widerrufen werden.	×	×

Lösungen aus: Klicksafe – Datenschutz geht zur Schule.

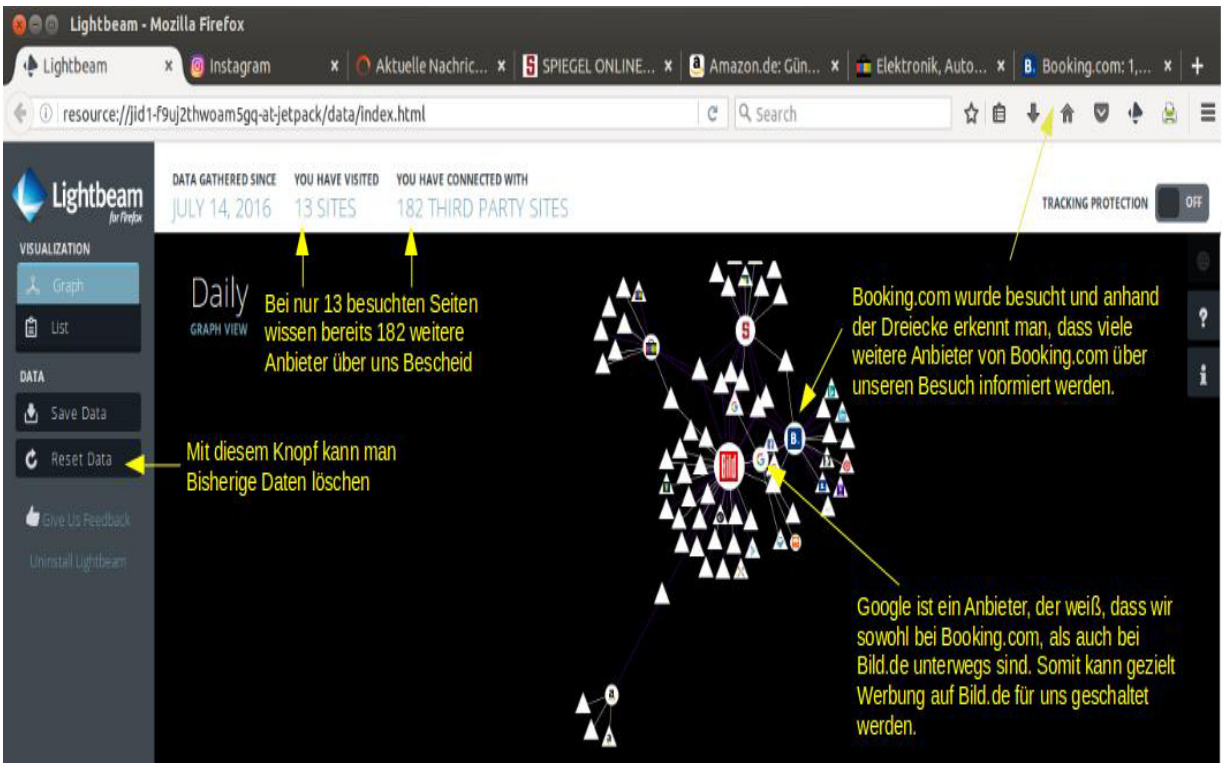
AB: Cookies / Browserverlauf Thema Datenschutz 09.08.2018

Name: Klasse 6.2 Lehrkraft: J.Thielen

Aufgabe 1: Spielt das Rollenspiel mit 4 Personen nach.

Aufgabe 2: Beschreibe was Cookies sind, nenne dabei Vorteile.

An der Station 6 lernst du das Addon Lightbeam kennen. Folgende Grafik zeigt das Addon. Hier kannst du die Anzahl an verknüpften Cookies sehen, nachdem man nur 13 Seiten besucht hat.



Aufgabe 3: Nenne Risiken, welche ein solches Tracking per Cookies birgt.

Anhang A. 11.4. Station 4: App-Berechtigungen (2.Seiten)

AB: App-Berechtigungen Thema Datenschutz 09.08.2018

Name: Klasse 6.2 Lehrkraft: J.Thielen

Aufgabe 1. Schaue dir das folgende Video an: https://bit.ly/2vc6qCr

Aufgabe 2. Überprüfe nun deine zwei Lieblingsapps auf ihre Berechtigungen. Nutze dazu die Anleitungen und helft euch gegenseitig:

Android

1. Öffne auf deinem Gerät die Einstellungen .
2. Tippe je nach verwendetem Gerät auf Apps oder Anwendungsmanager.
3. Tippe die App an, die du kontrollieren möchtest.
4. Tippen Sie auf Berechtigungen.

iOS

1. Öffnet die „Einstellungen“ auf eurem iPhone.
2. Scrollt nach unten bis zum Eintrag „Datenschutz“ und tippt ihn an.
3. Hier findet ihr alle Apps bzw. Funktionen, auf die eure Apps Zugriff haben können:
4. Tippt auf eine der Funktionen, um zu erfahren, welche App eine Zugriffsberechtigung hat

Aufgabe 3. Sammelt in der Tabelle, ob deine Lieblings-App diese Berechtigung fordert und wozu sie diese benötigen könnte. Wenn die App noch weitere Berechtigungen fordert, nehme diese in den letzten Zeilen noch auf.

Berechtigung	Name App1:	Name App2:
Eigene Daten/ Kontakte/ Adressbuch		
Bilder/Videos		
Kalender		
Standort/ Ortungsdienst		
Kamera/ Mikrofon		

Aufgabe 3:

Wann ist eine Berechtigung „OK“ oder wann sagst du eher „Nein“? Würdest du dir die vier unten stehenden Apps Swarmy, Soundo, Wconnect und Style Checkas auf dein Handy laden? Entscheide und begründe!

SWARMY

Beschreibung:
Leite den Fischschwarm durch ein Unterwasserlabyrinth.

Berechtigungen:

- In-App Käufe
- Internetzugriff

App-Logo:

Meine Entscheidung:

Soundo

Beschreibung:
Mit Soundo kannst du nicht nur Musik hören, sondern auch Musik erkennen.

Berechtigungen:

- Mikrofon
- Internetzugriff
- Kontakte

App-Logo:

Meine Entscheidung:

WCONNECT

Beschreibung:
Die neue Messenger-App verbindet alle deine Wünsche: Chatten, Video- und Sprachnachrichten.

Berechtigung:

- Internetzugriff
- Mikrofon
- Kontakte
- Kamera
- Standortdaten

App-Logo:

Meine Entscheidung:

Style Checkas

Beschreibung:
Bist du Beauty oder Loser? Die App sagt es dir.

Berechtigung:

- Internetzugriff
- Mikrofon
- Kontakte
- Kamera
- Standortdaten
- SMS
- Speicher
- In-App Käufe

App-Logo:

Meine Entscheidung:

Aufgabe 4:

Vergleiche deine Entscheidung mit deiner Partnerin / deinem Partner.

Freiwillige Hausaufgabe: Du kannst für jede App ein Logo entwerfen.

AB: Bewegungsdaten | Thema Datenschutz | 09.08.2018

Name: | Klasse 6.2 | Lehrkraft: J.Thielen

Bewegungsprofil – Wie man unbemerkte Ortung verhindert

Der Zugriff von Apps auf den Standort ist eine der am häufigsten geforderten Berechtigungen. Viele benötigen sie zur Bereitstellung bestimmter Funktionen, manche jedoch missbrauchen sie zur Erstellung von Bewegungsprofilen. Dazu werden viele Aufenthaltspunkte des Smartphones verknüpft und zu einem Profil zusammengefasst. Technisch möglich wird dies aufgrund der Tatsache, dass moderne Smartphones mit einer Vielzahl von Sensoren ausgestattet sind. Damit kann das Gerät bis auf mehrere Kilometer (über das Mobilfunknetz) oder sogar wenige Meter (mit WLAN oder GPS) geortet werden.

Was passiert mit den gesammelten Daten?

Bei vielen Apps ist die Nutzung der jeweiligen Berechtigungen sinnvoll, z. B. die Ortung für Navigation oder Stauerkennung. Natürlich können diese sensiblen Daten aber auch missbraucht werden. Über den Aufenthaltsort können Rückschlüsse über den Wohnort, die Schule, den Arbeitsplatz und das Freizeitverhalten ermittelt werden – und das unbemerkt und ohne aktives Teilen von Informationen durch den Nutzer. Die gesammelten Daten sind also besonders attraktiv für Werbetreibende, die sich für die Gewohnheiten ihrer Zielgruppen interessieren.

Wie kann die Ortung verhindert werden?

Bei Smartphones mit iOS-Betriebssystem oder Android ab Version 6 kann der Zugriff auf den Standort für jede App einzeln freigegeben werden. Siehe Station 4. Eine weitere Möglichkeit ist außerdem die Ortungsfunktion/GPS allgemein auszuschalten.

Aufgabe 1. Schaue mit deinem Partner das Video: https://bit.ly/2OEEZtq an.

Aufgabe 2. Stelle deinem Partner / deiner Partnerin schriftlich drei Fragen zu dem Video oder dem Text, welche er / sie dann beantworten soll.

1. Frage

2. Frage

3. Frage

AB: Software für Datenschutz Thema Datenschutz 09.08.2018

Name: Klasse 6.2 Lehrkraft: J.Thielen

An den anderen Stationen lernst du verschiedene, teils negative Dinge in Bezug auf Datenschutz kennen. Hier wollen wir nun Add-Ons und Programme kennenlernen, mit denen wir uns dagegen wehren können.

Aufgabe 1: Finde heraus, welche Funktion die Add-Ons / Programme haben und aus welchen Gründen man sie nutzen kann oder sollte. Ergänze hierzu die Tabelle.
(Suche dafür im Internet oder nutze beiliegendes Informationsblatt.)

Add-Ons	Funktion	Nutzen für:
Ad-Blocker		
Ghostery	Ghostery ist eine Software, die den Anwender beim Surfen auf versteckte Dienste hinweist, die im Hintergrund private Daten an Seitenbetreiber übermitteln, und diese auf Wunsch blockiert.	Schützen der privaten Daten, durch Blockieren versteckter Datensammel-Dienste
Lightbeam	Dem Benutzer zeigen, welche Cookies von welchen Seiten geladen wurden. Zeigt auch Seiten, die auf dasselbe Cookie zugreifen.	Tracking nachvollziehen und verhindern.
Self-Destroying Cookies		
Privacy Badger	Das Add-On unterdrückt die gängigsten Werbe-Tracker und verhindert so, dass Ihr Surf-Verhalten aufgezeichnet wird.	Verhindert personalisierte Werbung sowie das Speichern von Cookies
Flagfox		

Programme	Funktion	Nutzen für:
KeePassX	Safe für Passwörter	Speichert Passwörter sicher auf dem Computer.
TOR	Browser, mit dem man anonym das Internet nutzen kann	Anonymes Surfen
Antiviren-Software	Schütz den Computer / das Handy vor Viren und anderer Schadsoftware	Abwehr von Viren und anderer Schadsoftware

AB: Software für Datenschutz Thema Datenschutz 09.08.2018

Name: Klasse 6.2 Lehrkraft: J.Thielen

Nun geht es um die praktische Erprobung der Tools.

Bearbeite folgende Aufgaben und beobachte das Verhalten der Tools.

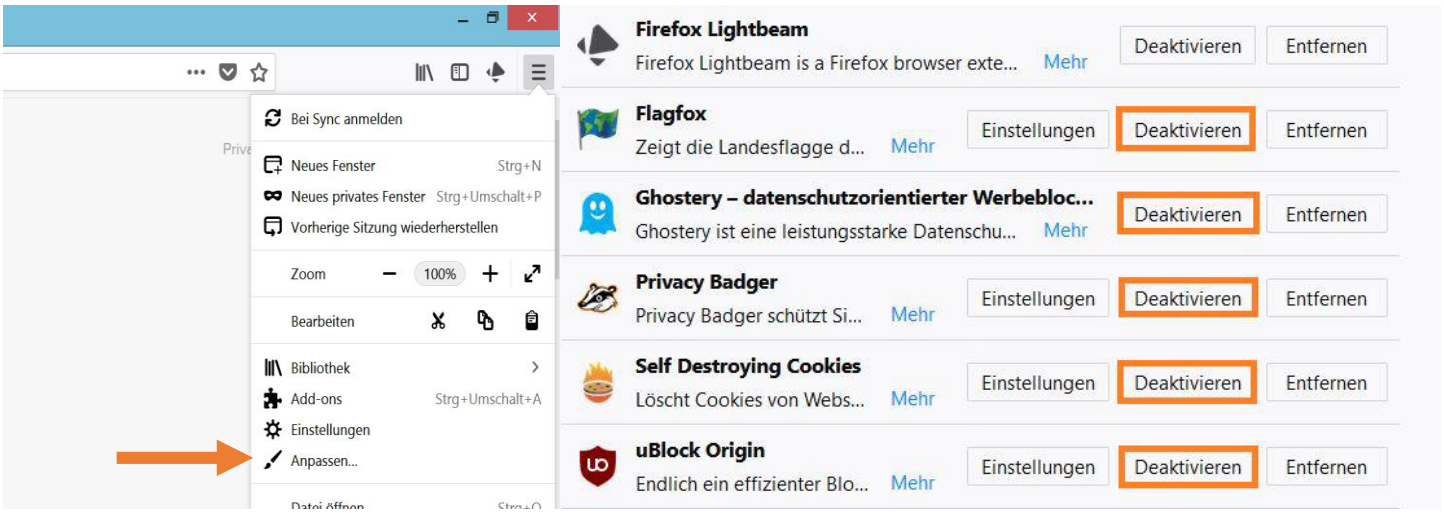
Aufgabe 2: Klicke im Browser Firefox auf das Lightbeam-Symbol. Klicke Links auf Reset Data.

Aufgabe 3: An den PCs sind die Add-Ons installiert, surfe ein wenig (2-3min) im Internet.
Besuche die Seiten: Youtube.com, Google.de, Booking.com, rhein-zeitung.de, musical.ly, instagram.com

Aufgabe 4: Beschreibe das Verhalten der Add-Ons (was zeigen dir die Addons an?) und ergänze die Tabelle auf der anderen Seite.

Aufgabe 5: Lasse dir in Lightbeam anzeigen, welche Cookies geladen wurden. Notiere dir hier die Anzahl an geladenen Cookies:

Aufgabe 6: Deaktiviere alle Add-Ons bis auf Lightbeam und wiederhole Aufgabe 2-5.
Wie viele Cookies wurden nun geladen?



Anhang A. 12. Rollenspiel inklusive Beizettel (3.Seiten)

Rollenspiel Cookies und Browserverlauf[39]

Du: Hey Browser, ich will mal wieder in den Urlaub. Kannst du mir bitte mal booking.com aufrufen?

➔ Booking.com-Aufruf an Browser geben.

Dein Browser: Ja klar, das mache ich sofort! Hey booking.com, mein Meister will Inhalte von dir. Gib mir deine Startseite!

booking.com: Klar, hier hast du die gewünschten Inhalte. Ich binde übrigens externe Inhalte mit ein, bspw. von Google. Kennst du „Google Analytics"? Das ist voll praktisch für meinen Betreiber!

Dein Browser: Nee, kenn ich nicht, und ist mir auch egal. Ich möchte nur das, was mein Meister mir befiehlt. Sag einfach, was ich laden soll, er wird ungeduldig.

➔ Booking.com-Inhalte an Browser geben.

booking.com: Ja ja, hier sind deine Inhalte. Ach, übrigens, damit ich dich später wiedererkenne, gebe ich dir diese kleine Textdatei, ein Cookie. Wenn du noch was von mir willst, zeig mir den. So erinnere ich mich an dich, und du musst Formulardaten nicht neu eingeben, oder ich habe vielleicht gerade ein Sonderangebot für deinen Meister, das ihm gefällt.

➔ Booking.com-Cookie an Browser geben.

Dein Browser: Das klingt praktisch, den speichere ich mir ab. Jetzt kann ich meinem Nutzer schneller Inhalte von dir ausliefern, das macht ihn sicher glücklich.

booking.com: Ach, hier sind übrigens noch ein paar Cookies von Anbietern, mit denen ich zusammenarbeite. Sie schalten manchmal Sonderangebote auf anderen Seiten. Damit sie dich ebenfalls wiedererkennen können, habe ich auch von denen Cookies, die ich dir gerne geben würde.

➔ Google-Cookie an Browser geben.

Dein Browser: Klingt sinnvoll, die nehme ich auch, danke. Meister, hier sind die von dir gewünschten Inhalte von booking.com! Was wünschst du jetzt?

➔ Booking.com-Inhalte an „Du" geben.

Du: Danke, Browser. Jetzt hätte ich gerne, dass du mir die neuesten Nachrichten von dieser „BildZeitung" anzeigst. Die habe ich bisher noch nie angeschaut.

➔ bild.de-Aufruf an Browser geben.

Dein Browser: Wird sofort erledigt! He, bild.de, zeig mal, was es Neues gibt!

bild.de: Klar, gerne doch. Ich binde dir aber Werbung ein, denn damit verdiene ich mein Geld. So kann ich deinem Meister meine Inhalte kostenlos anbieten!

Dein Browser: Das klingt nur fair. Hoffentlich interessiert sich mein Meister für diese Werbung …

bild.de: Aber sicher doch! Kennen wir uns denn schon? Denn dann kann ich dir definitiv passende Werbung einblenden.

Dein Browser: Ich schau mal in meinen Cookies nach … keiner von bild.de. Ich war noch nie bei dir.

bild.de: Wir kennen uns noch nicht, aber ich arbeite unter anderem mit Google zusammen. Die schalten auch Werbung für uns. Vielleicht kennt Google dich?

Dein Browser: Ah, da ist ein Google-Cookie.

➔ Google-Cookie bild.de zeigen.

bild.de: Sei unbesorgt: Die Werbung, die dein Meister zu sehen bekommt, wird ihm gefallen. Google kennt ihn bereits (woher auch immer, das weiß ich nicht, und ist mir auch egal) und kann für ihn gezielt Werbung einblenden.

➔ bild.de-Inhalte an Browser geben.

Dein Browser: Hier Meister, die von dir gewünschten Inhalte von bild.de, inklusive personalisierter Werbung

➔ bild.de-Inhalte an „Du" geben.

Du: Wow, wie geht das denn? Ich bin noch nie auf bild.de gewesen mit dem Browser, aber trotzdem kommt da jetzt Werbung von booking.com? Echt krass!

[39] Dieses Rollenspiel entstammt aus Haschler 2017, S. 18 und wurde minimal abgeändert um die Schüler enaktiv handeln zu lassen. Dabei erhielt jede Rolle diese Seite mit markierten Textstellen der jeweiligen Rolle.
Auch die Schrift war zur besseren Lesbarkeit größer und wurde nur in diesem Anhang verkleinert.

Booking.com-Aufruf

Booking.com

Booking.com-Inhalte

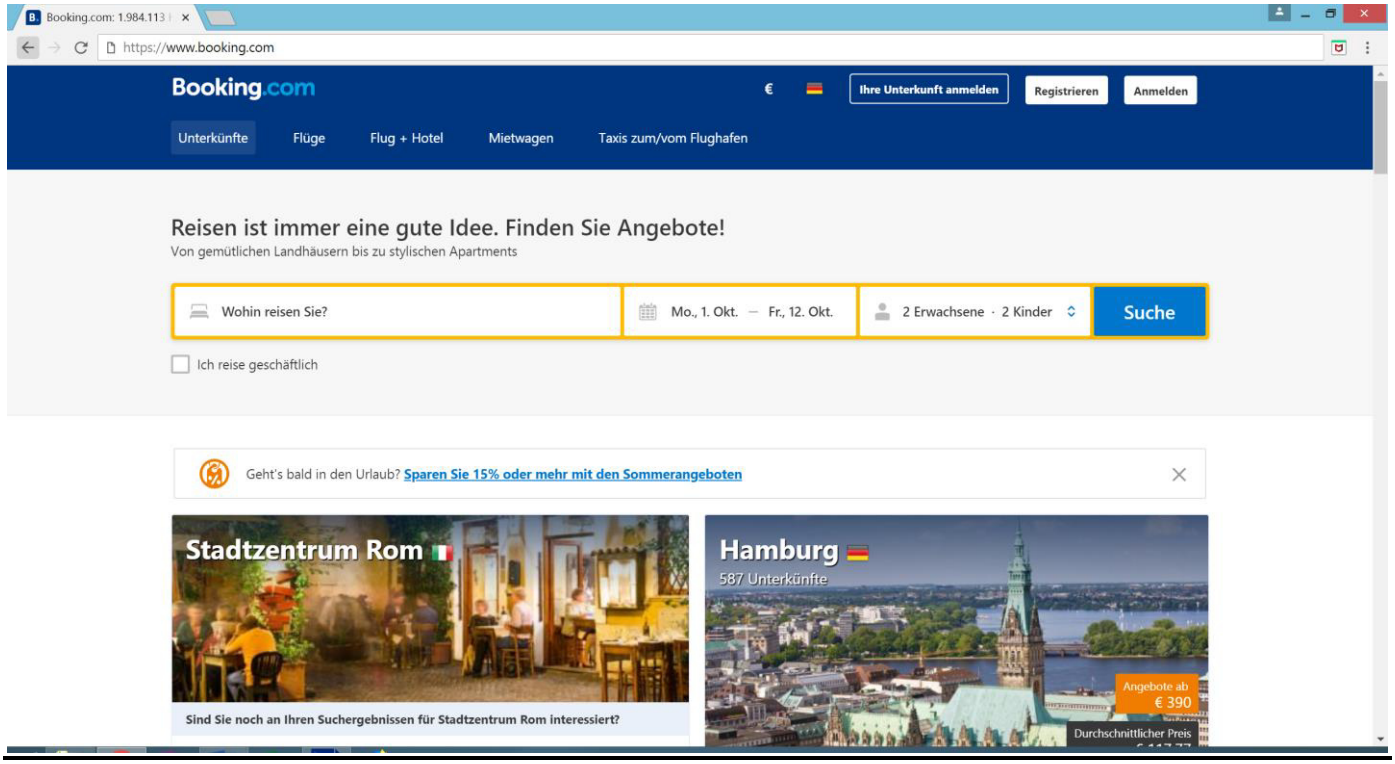
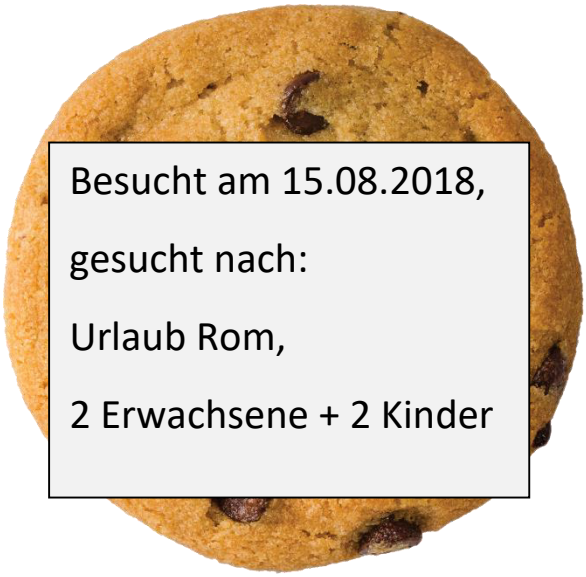


bild.de-Aufruf

bild.de

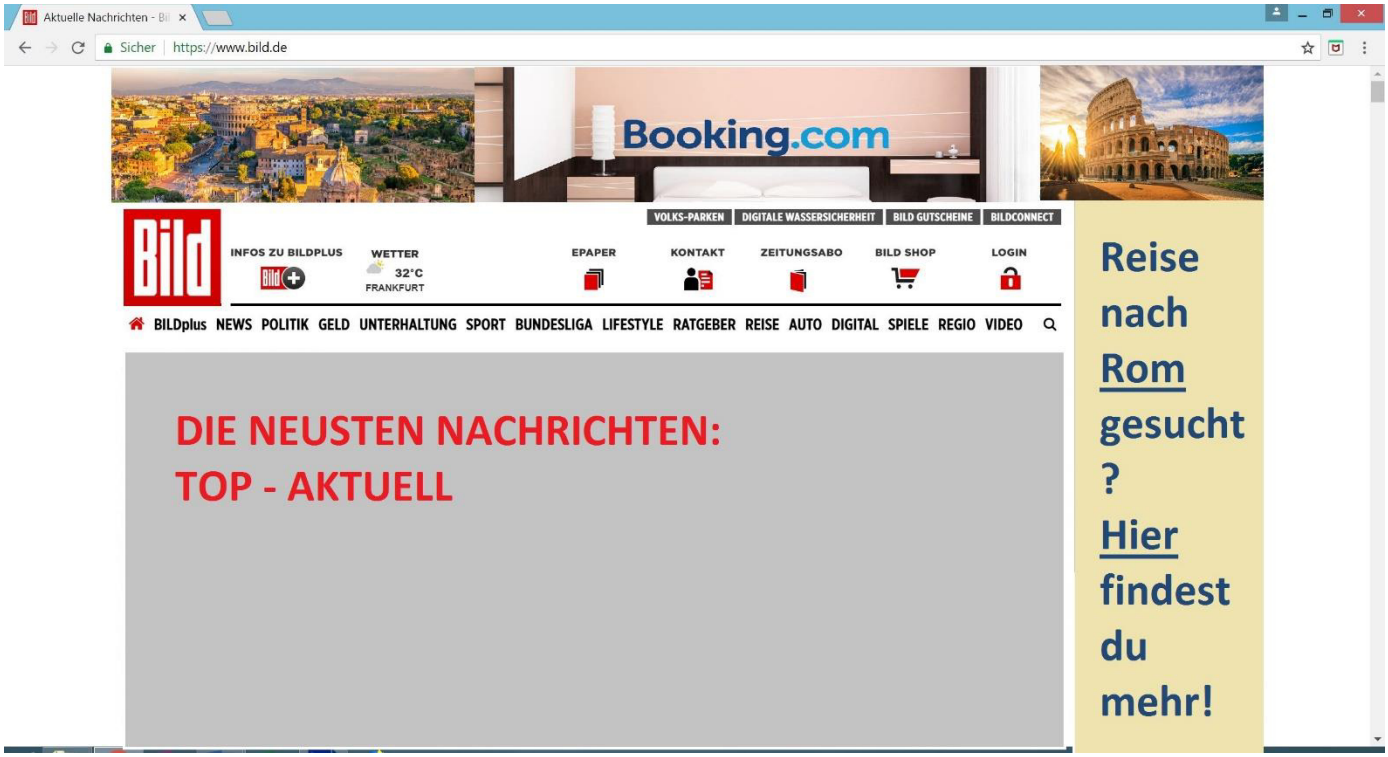
Booking.com-Cookie



Google-Cookie

---

bild.de-Inhalte



Ich habe an der Station 1 zu Viren und Trojanern gelernt:


1._____

2._____

3._____

Ich habe an der Station 2 zu Rechte und Gesetze gelernt:

1._____

2._____

3._____

Ich habe an der Station 3 zu Cookies und Browserverlauf gelernt:

1._____

2._____

3._____

Ich habe an der Station 5 zu Bewegungsdaten gelernt:

1._____

2._____

3._____

Ich habe an der Station 6 zu Software zum Datenschutz gelernt:

1._____

2._____

3._____

Deckblatt

Thema Datenschutz

09.08.2018

Name: Klasse 6.2 Lehrkraft: J.Thielen

In diesem Hefter befinden sich alle Arbeitsblätter der Stationenarbeit zum Thema Datenschutz.

Da nicht alle Bereiche zum Thema Datenschutz bearbeitet werden können, findest du auf folgenden Seite interessante Informationen und auch Videos:

Allgemeines:

https://www.handysektor.de/
Welche Apps soll oder darf man denn dann noch nutzen?
Auf Handysektor findest du alles rund ums Handy in Texten und Videos erklärt. Dort findest du auch einen App-Check (App-Alarm), der verrät, was die Apps machen und wie man sie nutzen sollte ohne zu viel über sich preiszugeben.

http://netla.ch/
Hier findest du das Thema Datenschutz im Comicstyle aufgearbeitet, sowie ein Quizz zum Thema Datenschutz.

https://www.youngdata.de/
Du möchtest dich mit einer offiziellen Seite der Datenschutzbehörde informieren? Hier findest du eine Seite für Jugendliche zum Thema Datenschutz.

https://www.scroller.de/Gut_gemacht/Taffe_Tipps/1357_Datenschutz_Tipps.htm
Scroller ist ein Medienmagazin für Kinder und Jugendliche, mit einer Zeitschrift zum Thema Datenschutz

Videos:

https://www.youtube.com/watch?v=WZwoaL-ydi4
Oder sucht auf YouTube nach „SnapChat“ und „Daten sammeln“,
dort findet ihr ein interessantes Video, warum SnapChat Daten sammelt.

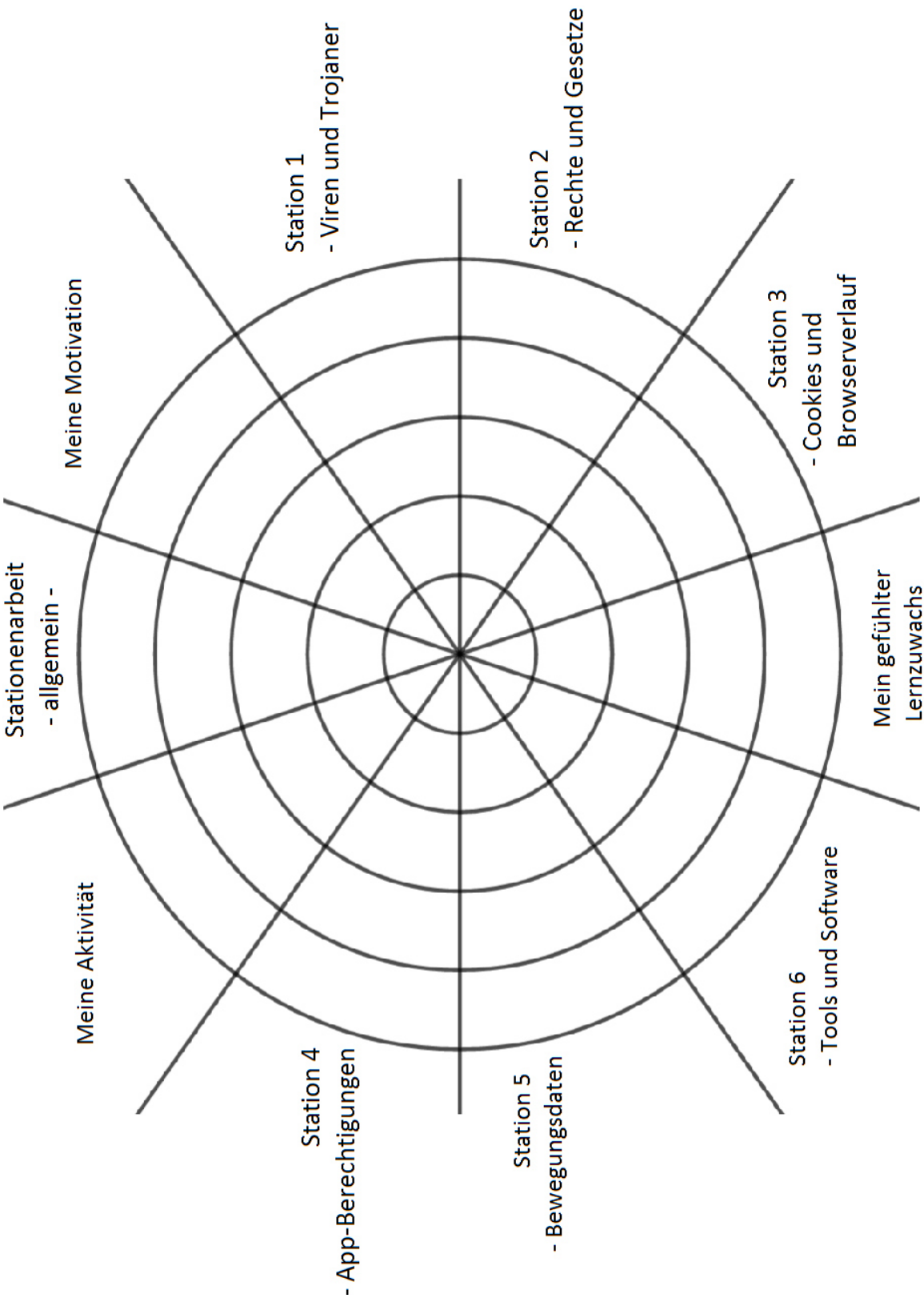
https://www1.wdr.de/fernsehen/quarks/bigdatatalk-kassenbon100.html
Ein Video zum Thema BigData. Warum es für einen Supermarkt interessant ist, welche Kunden schwanger sind und wie der Supermarkt das sogar durch Datenauswertung herausbekommt.

Spiele:

http://datadealer.com/de
Einmal selbst Datensammler sein? Hier findest du ein Computerspiel zum Thema Datendealer (Dealer bedeutet auf Deutsch Händler).

http://panopti.com.onreact.com/swf/
Ein kleines Spiel zum Thema Überwachung. Wie man uns mit Daten kontrollieren kann.

Anhang A. 15. Evaluationszielscheibe



Zahlenschlösser - Anzahl an möglichen Pins

Stellen	Ziffern	Rechnung	Anzahl an Möglichkeiten
1	10		10
2	10	$10 * 10 = 10^2 =$	100
3	10	$10 * 10 * 10 = 10^3 =$	1000

Zahlenschloss mit Hinweisen

Hinweis	Positionen der Zahl	Anzahl weiterer Stellen	Anzahl der Ziffern der anderen Stellen	Rechnung
Größte Zahl die 7, welche genau einmal vorkommt:	**3**	**2**	**7**	3 * 7 * 7 = 147 Möglichkeiten
Kleinste Zahl die 1, welche genau einmal vorkommt:	3	2	8	3*8*8 = 192 Möglichkeiten
Der PIN enthält die 5 sowie eine größere und eine kleinere Zahl.:	**3**	**2 aber mit**	**5 bzw. 4 Ziffern**	daher 3 * 2*5 * 4 = 120 Möglichkeiten
An der letzten Stelle die größte Zahl.	1	2	abhängig von der Zahl	1*9*9 + 1*8*8+ … + 1*2*2+ 1*1*1 = 285 Möglichkeiten
An der ersten Stelle die kleinste Zahl.	1	2	abhängig von der Zahl	1*1*1+ 1*2*2+ … + 1*8*8 + 1*9*9 = 285 Möglichkeiten
Nur mit ungeraden Zahlen gesperrt.	-	3	5	5 * 5 *5 = 125 Möglichkeiten
Keine Zahl doppelt.	-	3	mit 10 / 9 / 8 Ziffern	10 * 9 * 8 = 720 Möglichkeiten

AB: Zahlenschloss Kombinatorik Thema Datenschutz 09.08.2018

Name: Klasse 6.2 Lehrkraft: J.Thielen

Aufgabe 1:

Wie viele Möglichkeiten an Pins gibt es bei einem Zahlenschloss mit einem Rad? _____

Wie viele Möglichkeiten gibt es bei einem Zahlenschloss mit zwei Rädern? _____

Aufgabe 2:

Versucht das vor euch liegende Zahlenschloss zu öffnen.

Wie viele Möglichkeiten gibt es ohne Hinweis? _____

Daher bekommt ihr folgenden Hinweis:

Hier steht einer der Hinweise aus Anhang A 17

Wie viele Möglichkeiten gibt es jetzt noch? Schätze einmal: _____

Hinweis für Schnelle:
Der PIN eures Zahlenschlosses hat die Quersumme 13.

Aufgabe 3:

Wie viele Möglichkeiten gibt es bei einem dreistelligen Schloss, wenn anstelle der Ziffern von 0-9, das kleine Alphabet (26 Buchstaben) steht? _____

Wie viele Möglichkeiten gibt es bei einem dreistelligen Schloss, wenn Ziffern (0-9) und das kleine Alphabet (26 Buchstaben) existieren? _____

AB: Passwortregeln	Thema Datenschutz	09.08.2018
Name:	Klasse 6.2	Lehrkraft: J.Thielen

Aufgabe 4: Regeln für ein sicheres Passwort

1._____

2._____

3._____

4._____

5._____

6._____

Aufgabe 5:
Einige dich mit deiner Gruppe auf die wichtigsten Regeln zu Passwörtern.
Gestalte dazu mit deiner Gruppe ein Dokument am PC.
Das Dokument soll am Ende vorgestellt werden!

Aufgabe 6:

Überlege dir ein Passwort, welches du nur für diese Aufgabe nutzt, und notiere es hier:

Überprüfe die stärke deines Passwortes mit dem Passwortüberprüfer:

https://www.passwortcheck.ch/

Gib dort NIEMALS deine richtigen Passwörter ein!

Wer schafft das komplizierteste Passwort?

Hinweise zum Öffnen eines dreistelligen Zahlenschlosses[40]

Der PIN eures Zahlenschlosses enthält die 5 sowie eine größere und eine kleinere Zahl.: Drei Möglichkeiten für die Stellung der 5 sowie dazu jeweils zwei Möglichkeiten der Reihenfolge der größeren und der kleineren Zahl. Dies entspricht auch der Anzahl an Permutationen von 3 Objekten. Des Weiteren gibt es für die kleinere Zahl fünf Ziffern von 0 bis 4 und vier Ziffern für die größere Zahl von 6 bis 9.

3 * 2*5 * 4 = 120 Möglichkeiten

Der PIN eures Zahlenschlosses hat als größte Zahl die 7, welche genau einmal vorkommt: Drei Möglichkeiten für die Stellung der 7 sowie dazu jeweils 7 Möglichkeiten für die Ziffern der anderen beiden Stellen.

3 * 7 * 7 = 147 Möglichkeiten

Der PIN eures Zahlenschlosses hat als kleinste Zahl eine 1, welche genau einmal vorkommt:

3*8*8 = 192 Möglichkeiten

Der PIN eures Zahlenschlosses hat an der letzten Stelle die größte Zahl.

9*9+8*8+7*7+6*6+5*5+4*4+3*3+2*2+1*1 = 285 Möglichkeiten

Der PIN eures Zahlenschlosses hat an der ersten Stelle die kleinste Zahl.

Siehe oben = 285 Möglichkeiten

Der PIN eures Zahlenschlosses hat keine Zahl doppelt.
Urnenmodell Ziehen ohne zurücklegen 3 aus 10.

10 * 9 * 8 = 720 Möglichkeiten

Euer Zahlenschloss wurde nur mit ungeraden Zahlen gesperrt.

5 * 5 * 5 = 125 Möglichkeiten

Hinweis für Schnelle: Der PIN eures Zahlenschlosses hat die Quersumme 13.

[40] Dieses Blatt erhielt nur die Lehrkraft.

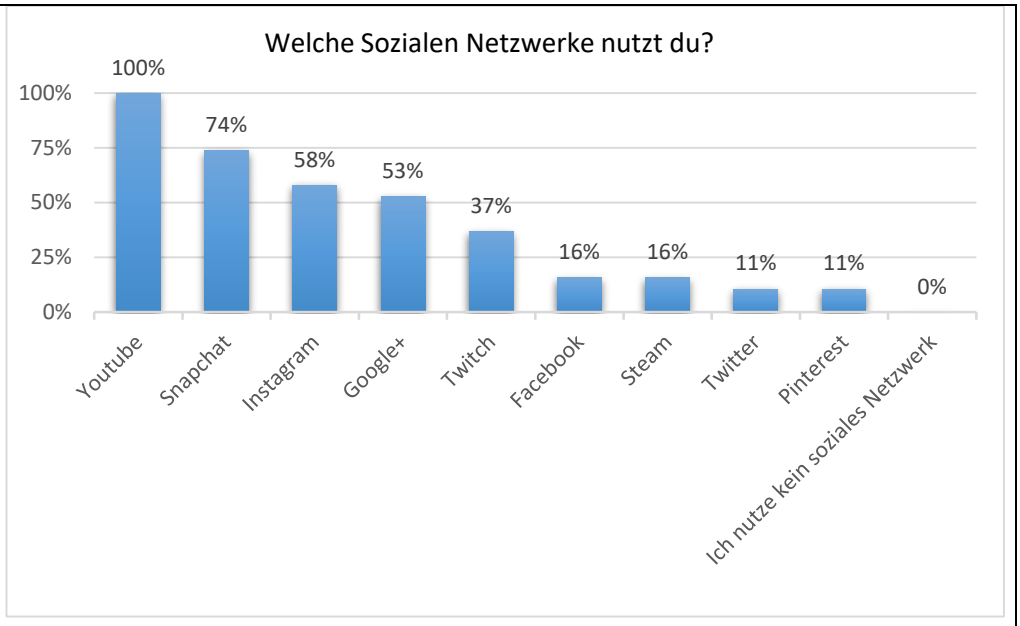
Anhang A. 19. Ergebnisse der Überprüfungen (11.Seiten)

Diese Überprüfung wurde anhand des Fragebogens aus der Studie von Hug 2017 erstellt.

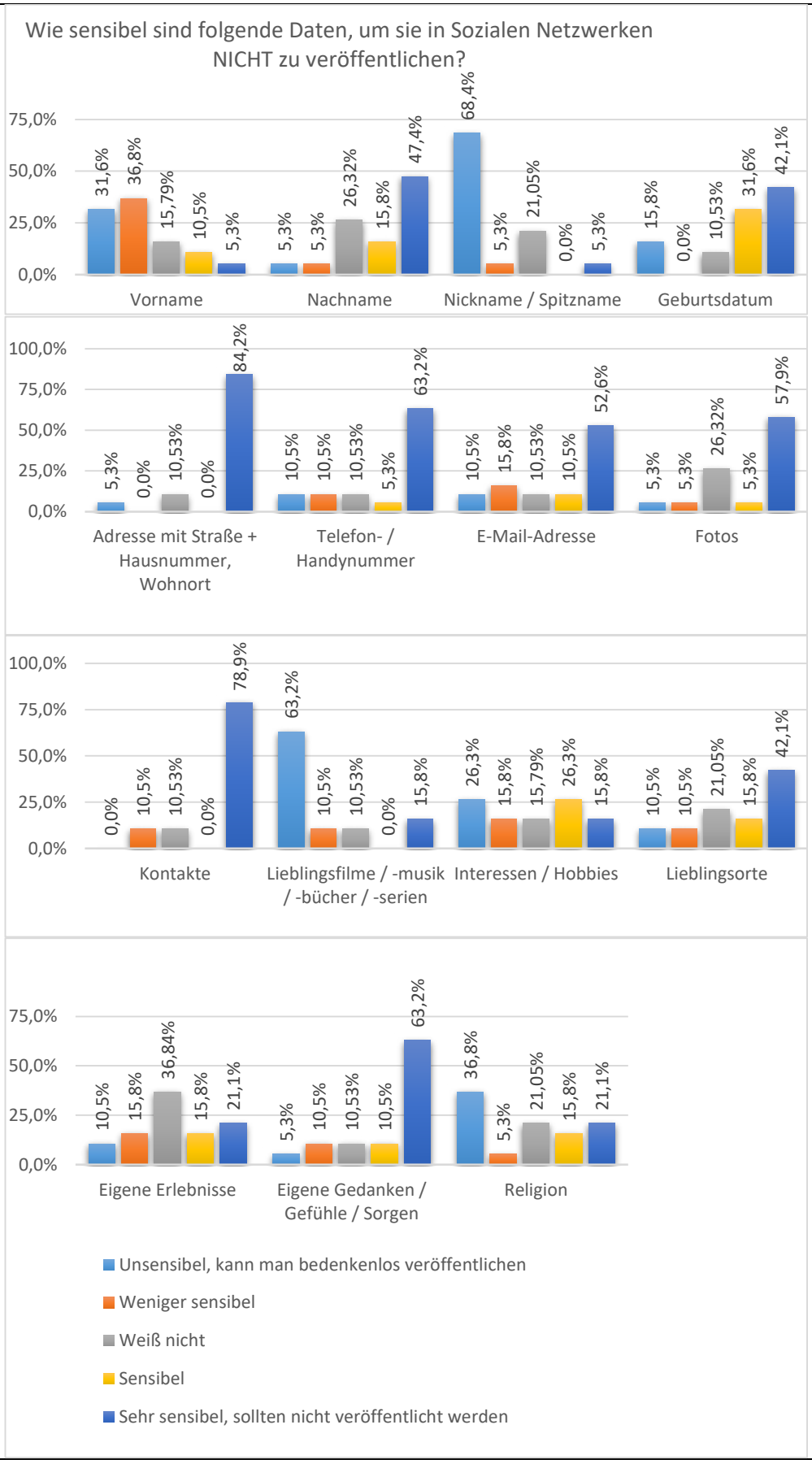
Bezüglich der genauen Items siehe WIPSCE QUELLE.

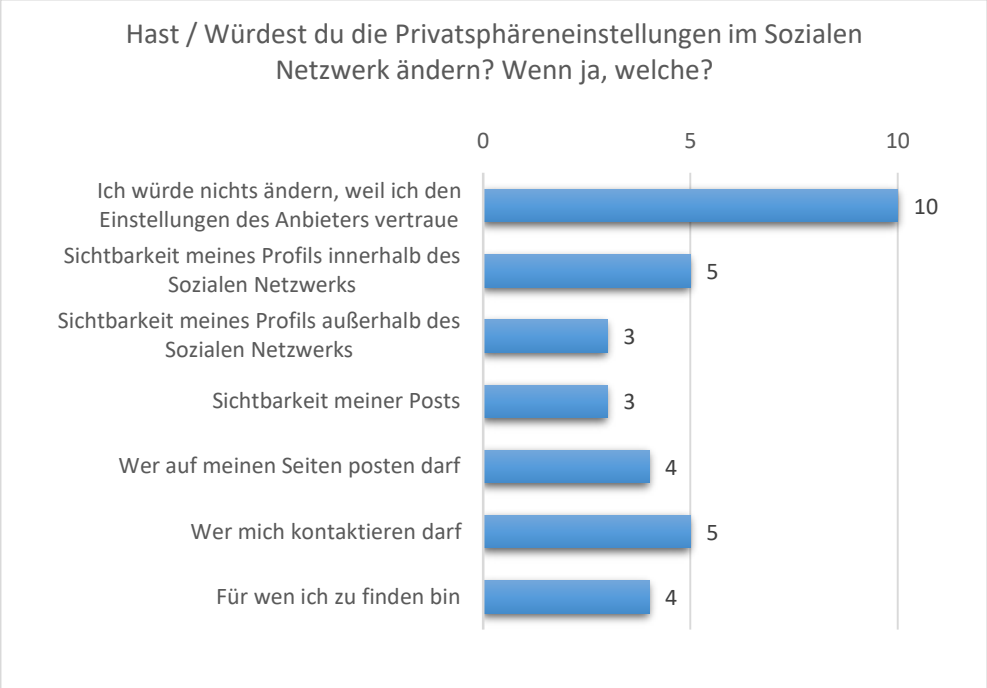
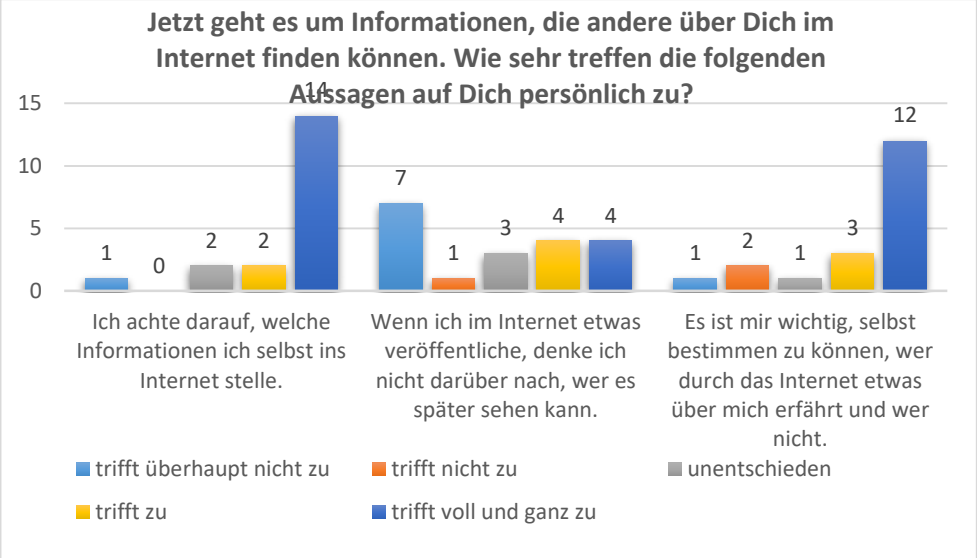
Teilnehmer der Studie:	19
davon männlich:	12
davon weiblich:	7

Die Altersverteilung:	
10 Jahre:	2
11 Jahre:	8
12 Jahre:	2
ohne Angabe:	7

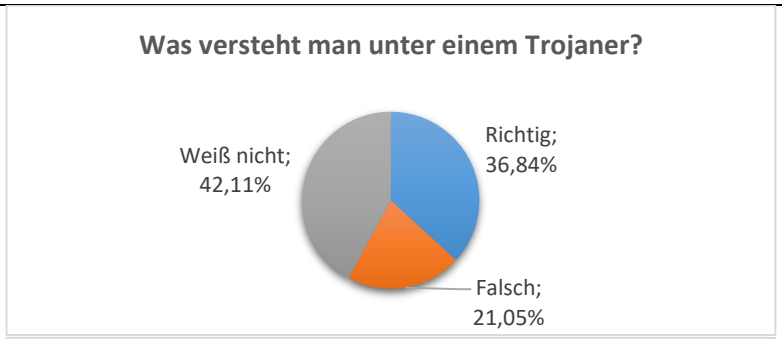
A18.3 Mehrfachnennung war möglich	

A18.4

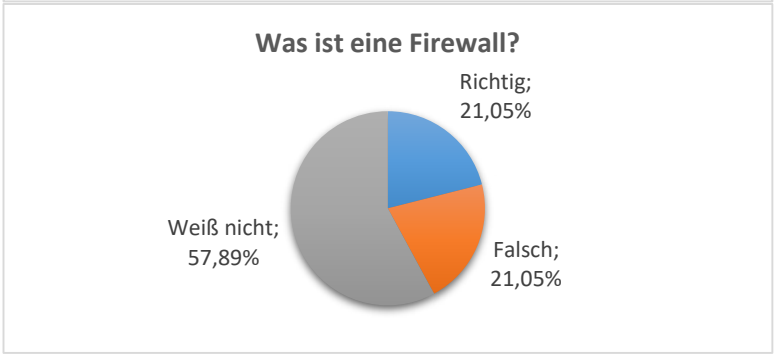

Wie sensibel sind folgende Daten, um sie in Sozialen Netzwerken NICHT zu veröffentlichen?
75,0%
50,0%
25,0%
0,0%
31,6%
36,8%
15,79%
10,5%
5,3%
5,3%
5,3%
26,32%
15,8%
47,4%
68,4%
5,3%
21,05%
0,0%
5,3%
15,8%
0,0%
10,53%
31,6%
42,1%
Vorname
Nachname
Nickname / Spitzname
Geburtsdatum
100,0%
75,0%
50,0%
25,0%
0,0%
5,3%
0,0%
10,53%
0,0%
84,2%
10,5%
10,5%
10,53%
5,3%
63,2%
10,5%
15,8%
10,53%
10,5%
52,6%
5,3%
5,3%
26,32%
5,3%
57,9%
Adresse mit Straße + Hausnummer, Wohnort
Telefon- / Handynummer
E-Mail-Adresse
Fotos
100,0%
75,0%
50,0%
25,0%
0,0%
0,0%
10,5%
10,53%
0,0%
78,9%
63,2%
10,5%
10,53%
0,0%
15,8%
26,3%
15,8%
15,79%
26,3%
15,8%
10,5%
10,5%
21,05%
15,8%
42,1%
Kontakte
Lieblingsfilme / -musik / -bücher / -serien
Interessen / Hobbies
Lieblingsorte
75,0%
50,0%
25,0%
0,0%
10,5%
15,8%
36,84%
15,8%
21,1%
5,3%
10,5%
10,53%
10,5%
63,2%
36,8%
5,3%
21,05%
15,8%
21,1%
Eigene Erlebnisse
Eigene Gedanken / Gefühle / Sorgen
Religion
Unsensibel, kann man bedenkenlos veröffentlichen
Weniger sensibel
Weiß nicht
Sensibel
Sehr sensibel, sollten nicht veröffentlicht werden

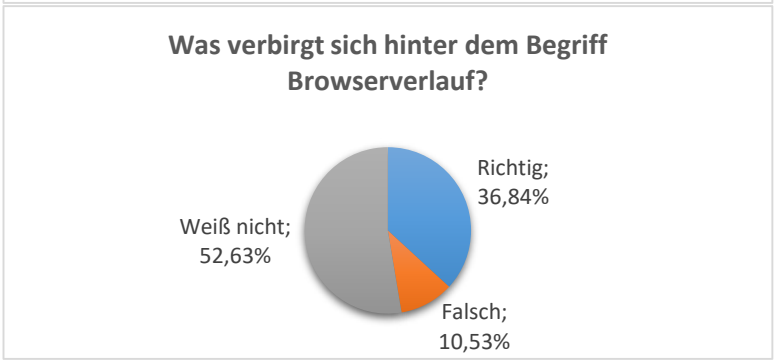
A18.5 Mehrfachnennung war möglich!	
A18.6	

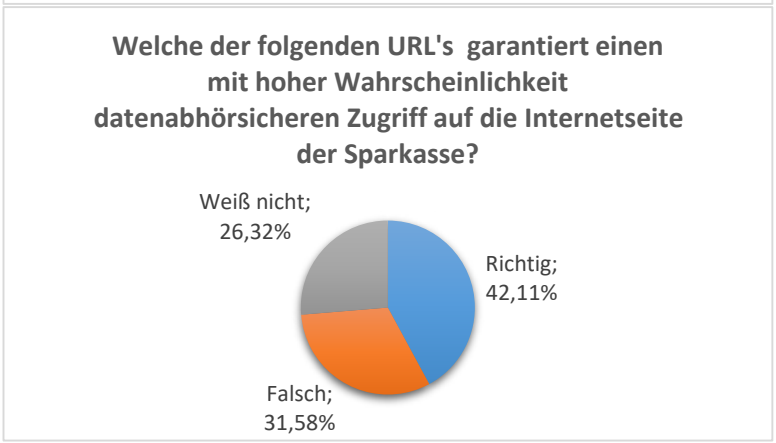
A18.7


Was versteht man unter einem Trojaner?
Weiß nicht; 42,11%
Richtig; 36,84%
Falsch; 21,05%

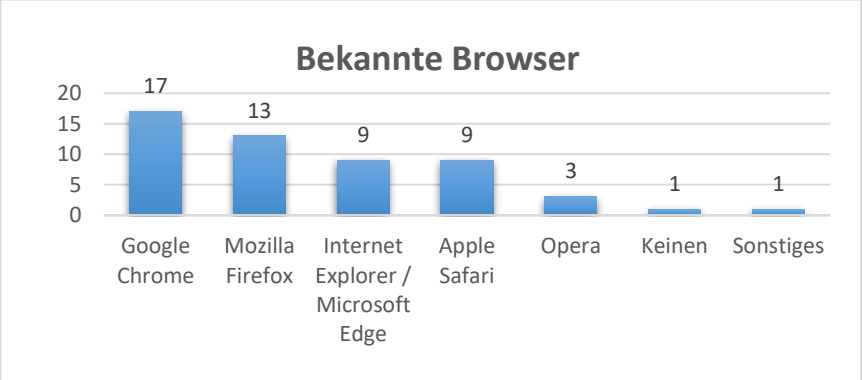

Was ist ein Cookie?
Richtig; 26,32%
Weiß nicht; 47,37%
Falsch; 26,32%

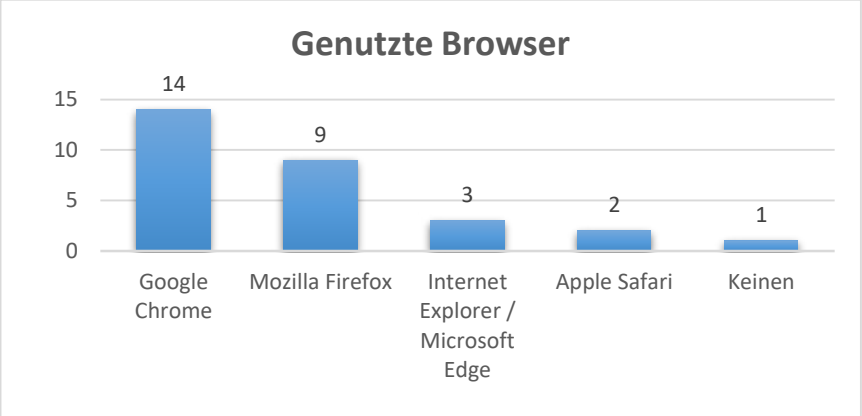

Was ist eine Firewall?
Richtig; 21,05%
Weiß nicht; 57,89%
Falsch; 21,05%


Was verbirgt sich hinter dem Begriff Browserverlauf?
Richtig; 36,84%
Weiß nicht; 52,63%
Falsch; 10,53%

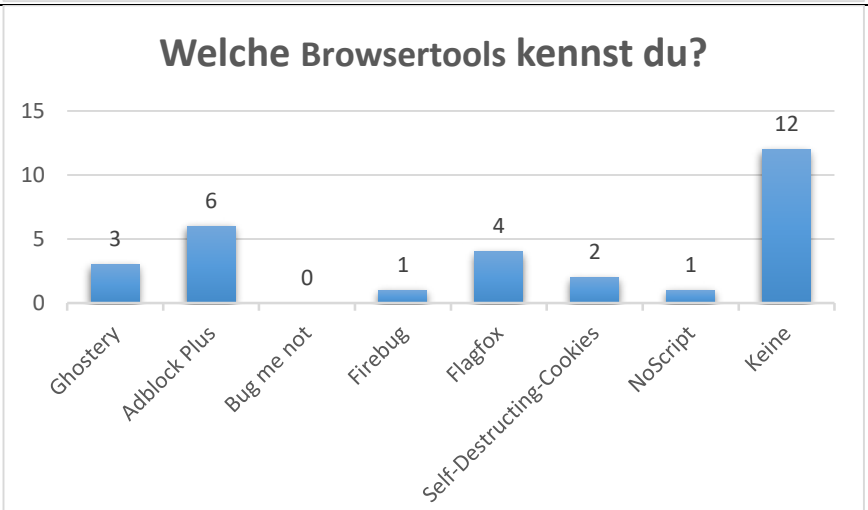

Welche der folgenden URL's garantiert einen mit hoher Wahrscheinlichkeit datenabhörsicheren Zugriff auf die Internetseite der Sparkasse?
Weiß nicht; 26,32%
Richtig; 42,11%
Falsch; 31,58%

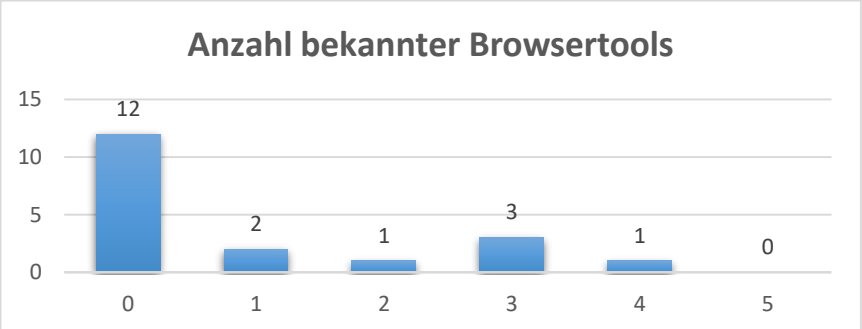
A18.8

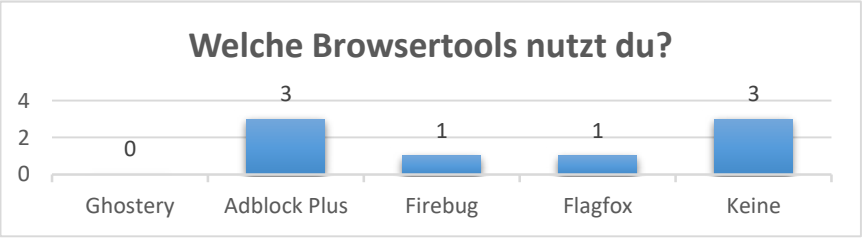

Bekannte Browser
20
15
10
5
0
17
13
9
9
3
1
1
Google Chrome
Mozilla Firefox
Internet Explorer / Microsoft Edge
Apple Safari
Opera
Keinen
Sonstiges

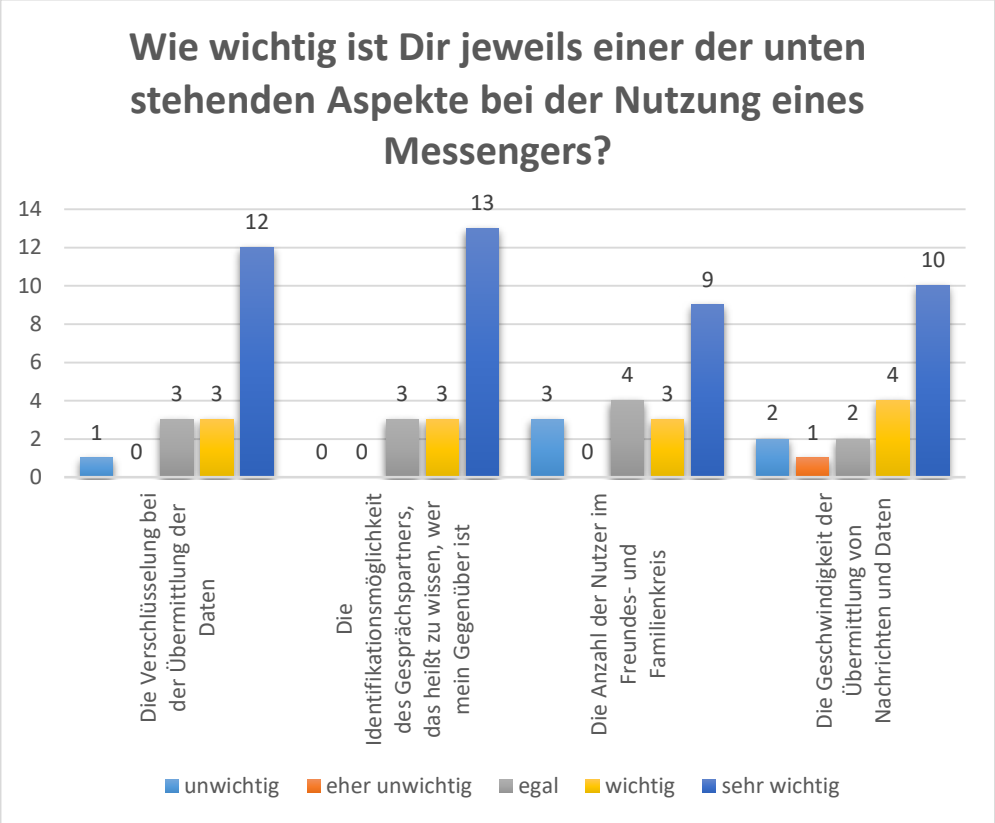

Genutzte Browser
15
10
5
0
14
9
3
2
1
Google Chrome
Mozilla Firefox
Internet Explorer / Microsoft Edge
Apple Safari
Keinen

A18.9


Welche Browsertools kennst du?
15
10
5
0
3
6
0
1
4
2
1
12
Ghostery
Adblock Plus
Bug me not
Firebug
Flagfox
Self-Destructing-Cookies
NoScript
Keine

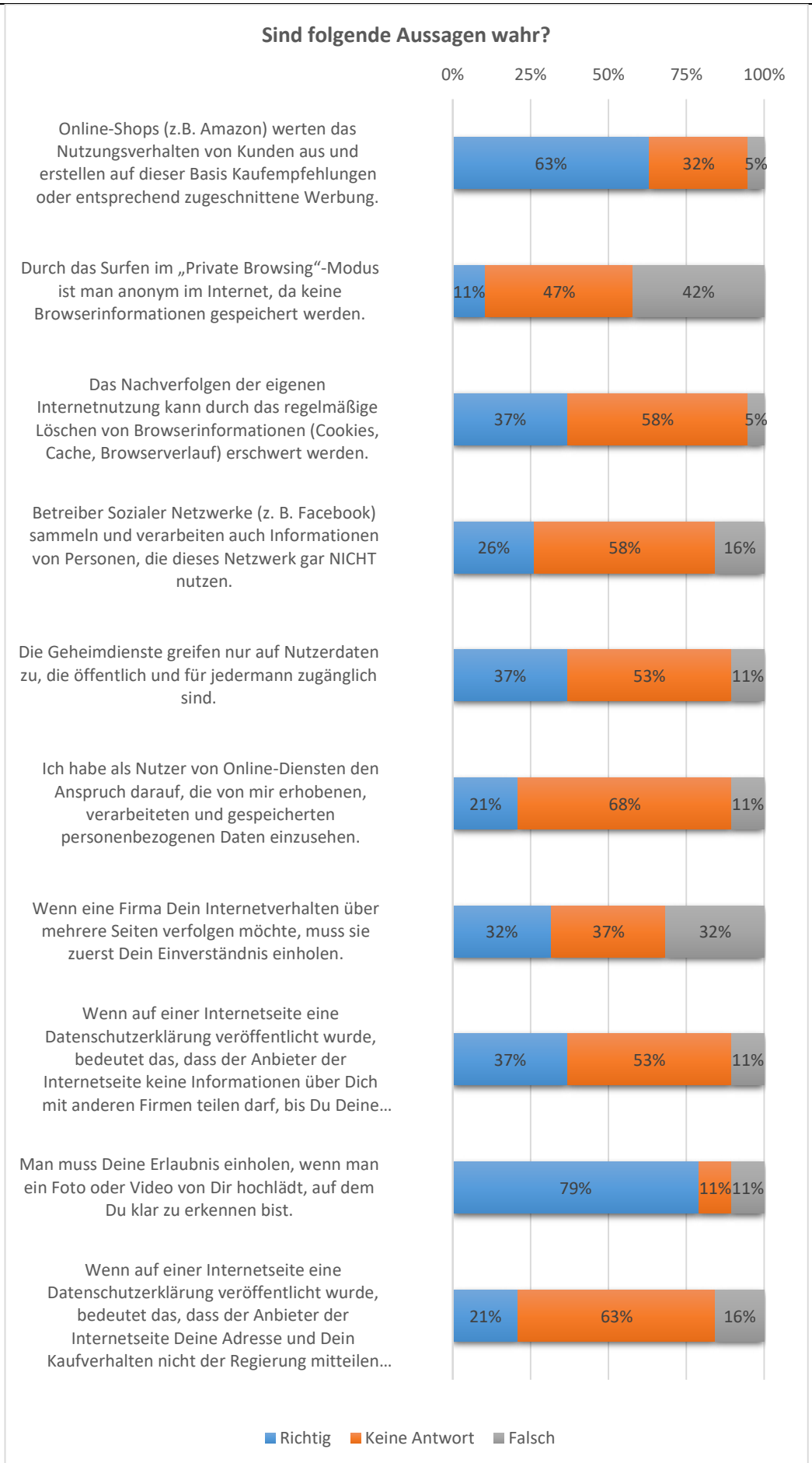

Anzahl bekannter Browsertools
15
10
5
0
12
2
1
3
1
0
0
1
2
3
4
5


Welche Browsertools nutzt du?
4
2
0
0
3
1
1
3
Ghostery
Adblock Plus
Firebug
Flagfox
Keine

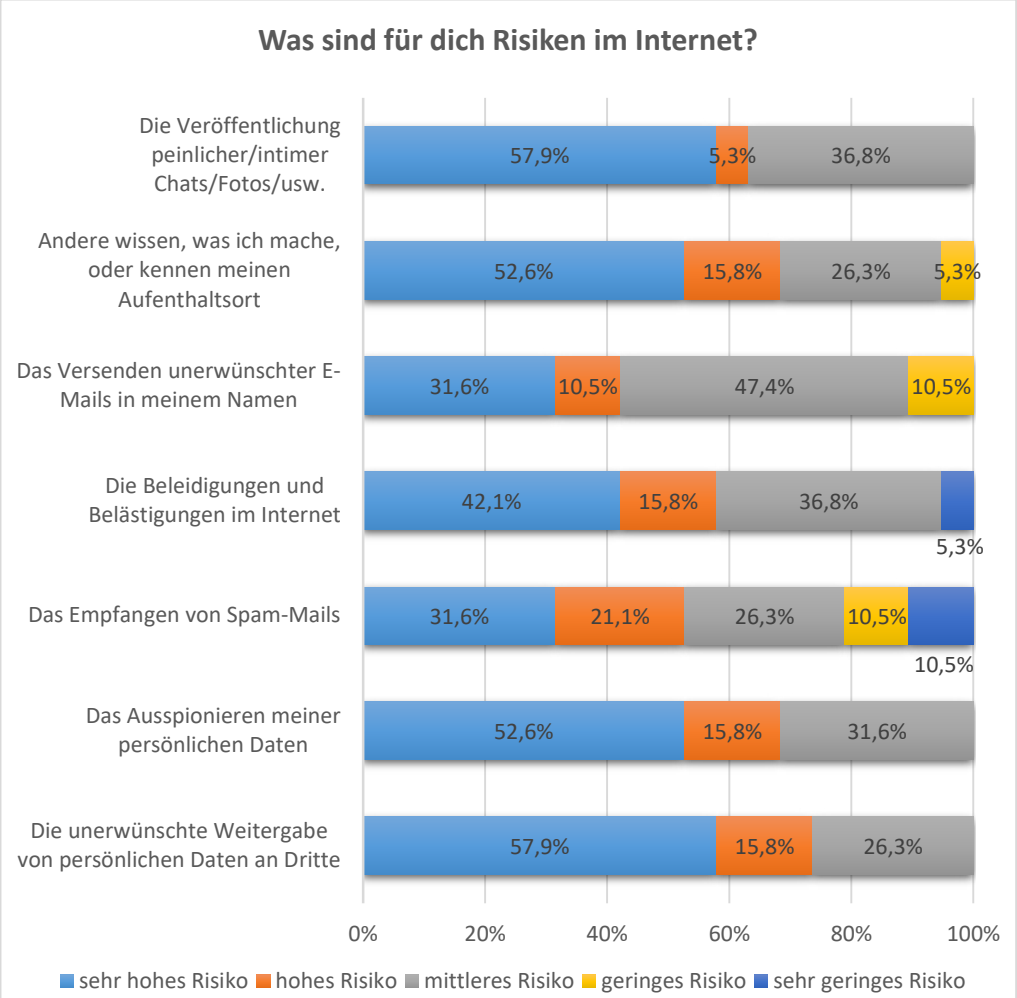
A18.10	

Wie wichtig ist Dir jeweils einer der unten stehenden Aspekte bei der Nutzung eines Messengers?
14
12
10
8
6
4
2
0
1
0
3
3
12
0
0
3
3
13
3
0
4
3
9
2
1
2
4
10
Die Verschlüsselung bei der Übermittlung der Daten
Die Identifikationsmöglichkeit des Gesprächspartners, das heißt zu wissen, wer mein Gegenüber ist
Die Anzahl der Nutzer im Freundes- und Familienkreis
Die Geschwindigkeit der Übermittlung von Nachrichten und Daten
unwichtig
eher unwichtig
egal
wichtig
sehr wichtig

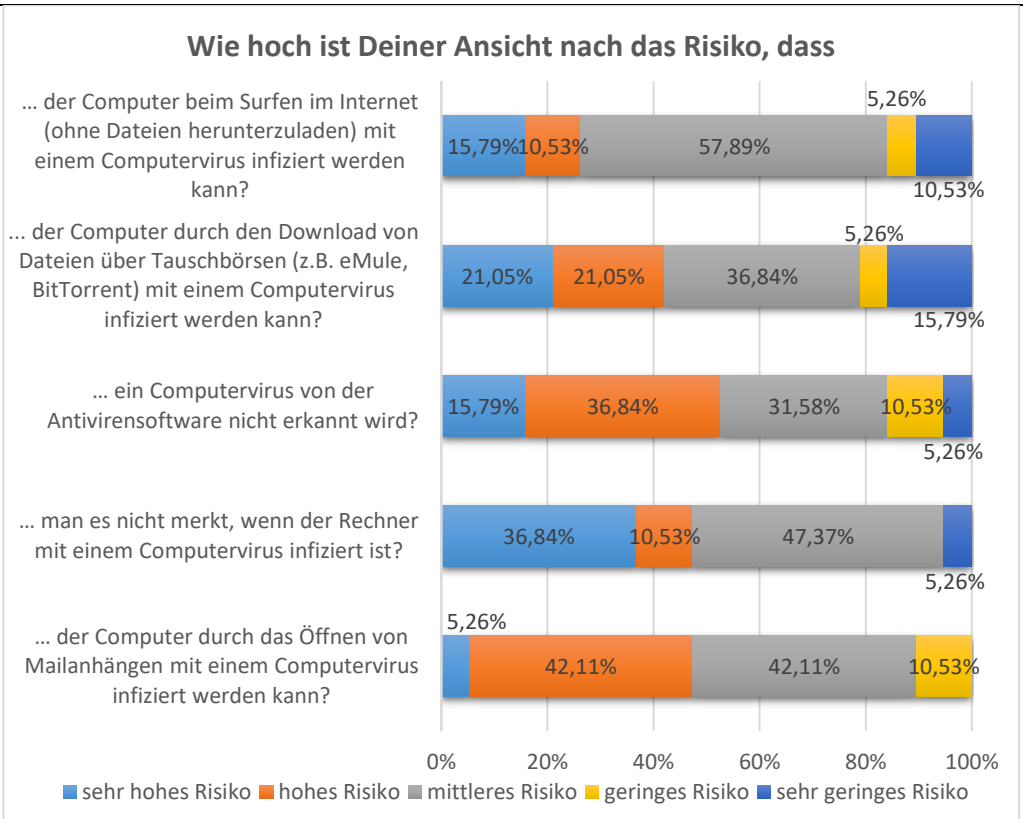
A18.11


Sind folgende Aussagen wahr?
0%
25%
50%
75%
100%
Online-Shops (z.B. Amazon) werten das Nutzungsverhalten von Kunden aus und erstellen auf dieser Basis Kaufempfehlungen oder entsprechend zugeschnittene Werbung.
63%
32%
5%
Durch das Surfen im „Private Browsing“-Modus ist man anonym im Internet, da keine Browserinformationen gespeichert werden.
11%
47%
42%
Das Nachverfolgen der eigenen Internetnutzung kann durch das regelmäßige Löschen von Browserinformationen (Cookies, Cache, Browserverlauf) erschwert werden.
37%
58%
5%
Betreiber Sozialer Netzwerke (z. B. Facebook) sammeln und verarbeiten auch Informationen von Personen, die dieses Netzwerk gar NICHT nutzen.
26%
58%
16%
Die Geheimdienste greifen nur auf Nutzerdaten zu, die öffentlich und für jedermann zugänglich sind.
37%
53%
11%
Ich habe als Nutzer von Online-Diensten den Anspruch darauf, die von mir erhobenen, verarbeiteten und gespeicherten personenbezogenen Daten einzusehen.
21%
68%
11%
Wenn eine Firma Dein Internetverhalten über mehrere Seiten verfolgen möchte, muss sie zuerst Dein Einverständnis einholen.
32%
37%
32%
Wenn auf einer Internetseite eine Datenschutzerklärung veröffentlicht wurde, bedeutet das, dass der Anbieter der Internetseite keine Informationen über Dich mit anderen Firmen teilen darf, bis Du Deine…
37%
53%
11%
Man muss Deine Erlaubnis einholen, wenn man ein Foto oder Video von Dir hochlädt, auf dem Du klar zu erkennen bist.
79%
11%
11%
Wenn auf einer Internetseite eine Datenschutzerklärung veröffentlicht wurde, bedeutet das, dass der Anbieter der Internetseite Deine Adresse und Dein Kaufverhalten nicht der Regierung mitteilen…
21%
63%
16%
Richtig
Keine Antwort
Falsch

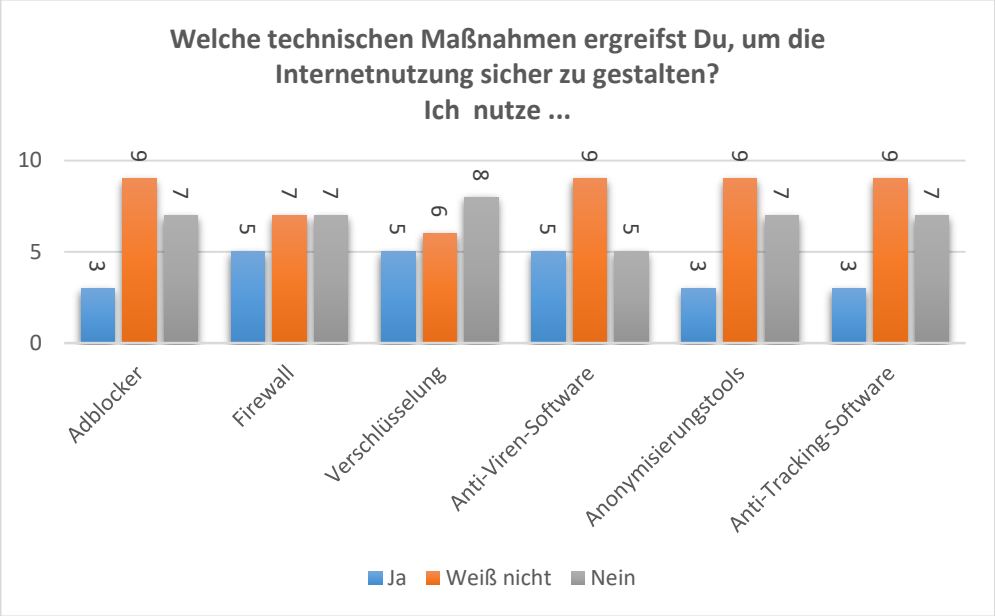
A18.12

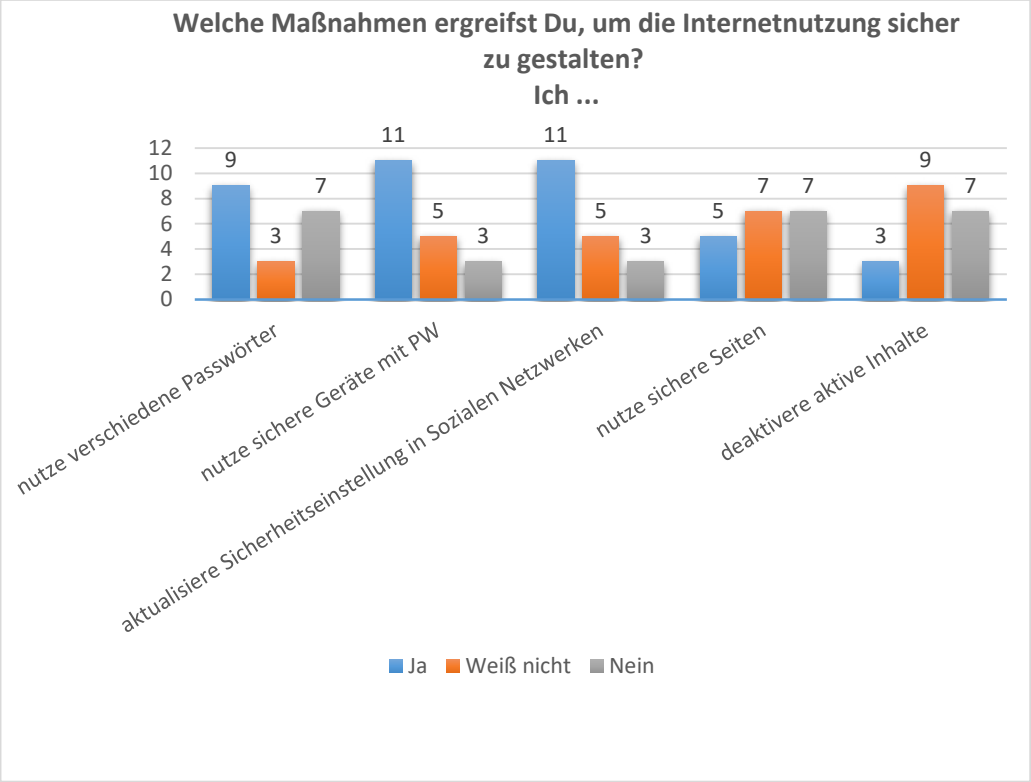

Was sind für dich Risiken im Internet?
Die Veröffentlichung peinlicher/intimer Chats/Fotos/usw.
57,9%
5,3%
36,8%
Andere wissen, was ich mache, oder kennen meinen Aufenthaltsort
52,6%
15,8%
26,3%
5,3%
Das Versenden unerwünschter E-Mails in meinem Namen
31,6%
10,5%
47,4%
10,5%
Die Beleidigungen und Belästigungen im Internet
42,1%
15,8%
36,8%
5,3%
Das Empfangen von Spam-Mails
31,6%
21,1%
26,3%
10,5%
10,5%
Das Ausspionieren meiner persönlichen Daten
52,6%
15,8%
31,6%
Die unerwünschte Weitergabe von persönlichen Daten an Dritte
57,9%
15,8%
26,3%
0%
20%
40%
60%
80%
100%
sehr hohes Risiko
hohes Risiko
mittleres Risiko
geringes Risiko
sehr geringes Risiko

A18.13

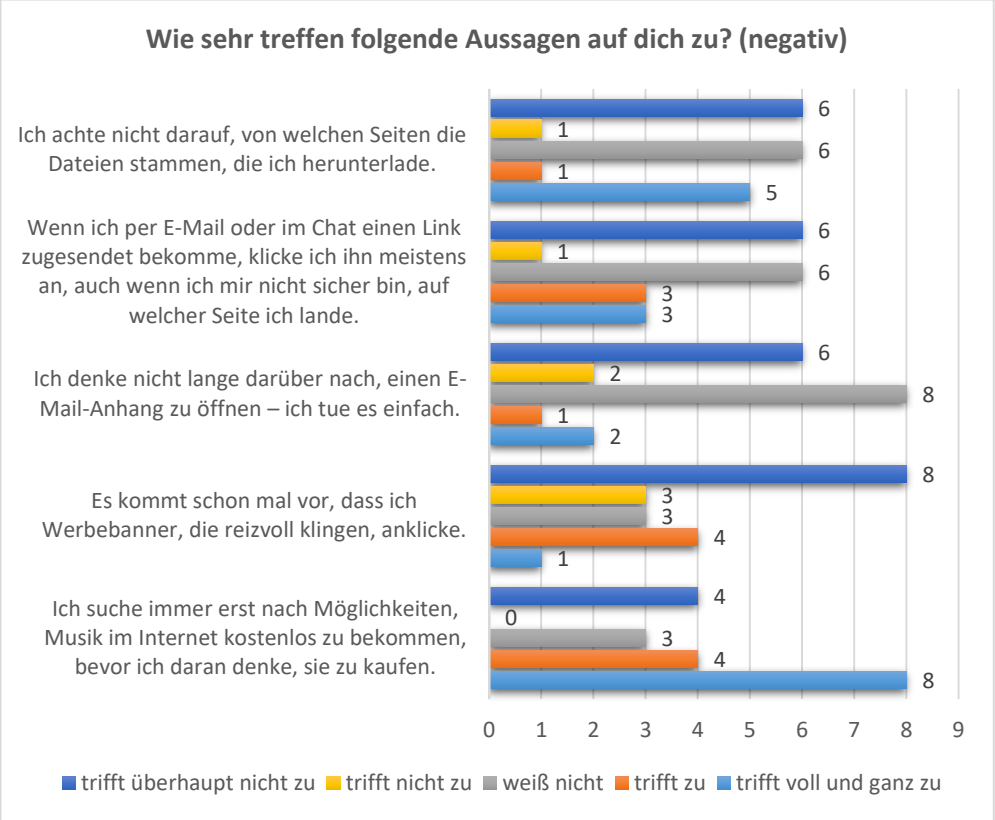

Wie hoch ist Deiner Ansicht nach das Risiko, dass
... der Computer beim Surfen im Internet (ohne Dateien herunterzuladen) mit einem Computervirus infiziert werden kann?
15,79%
10,53%
57,89%
5,26%
10,53%
... der Computer durch den Download von Dateien über Tauschbörsen (z.B. eMule, BitTorrent) mit einem Computervirus infiziert werden kann?
21,05%
21,05%
36,84%
5,26%
15,79%
... ein Computervirus von der Antivirensoftware nicht erkannt wird?
15,79%
36,84%
31,58%
10,53%
5,26%
... man es nicht merkt, wenn der Rechner mit einem Computervirus infiziert ist?
36,84%
10,53%
47,37%
5,26%
... der Computer durch das Öffnen von Mailanhängen mit einem Computervirus infiziert werden kann?
5,26%
42,11%
42,11%
10,53%
0%
20%
40%
60%
80%
100%
sehr hohes Risiko
hohes Risiko
mittleres Risiko
geringes Risiko
sehr geringes Risiko

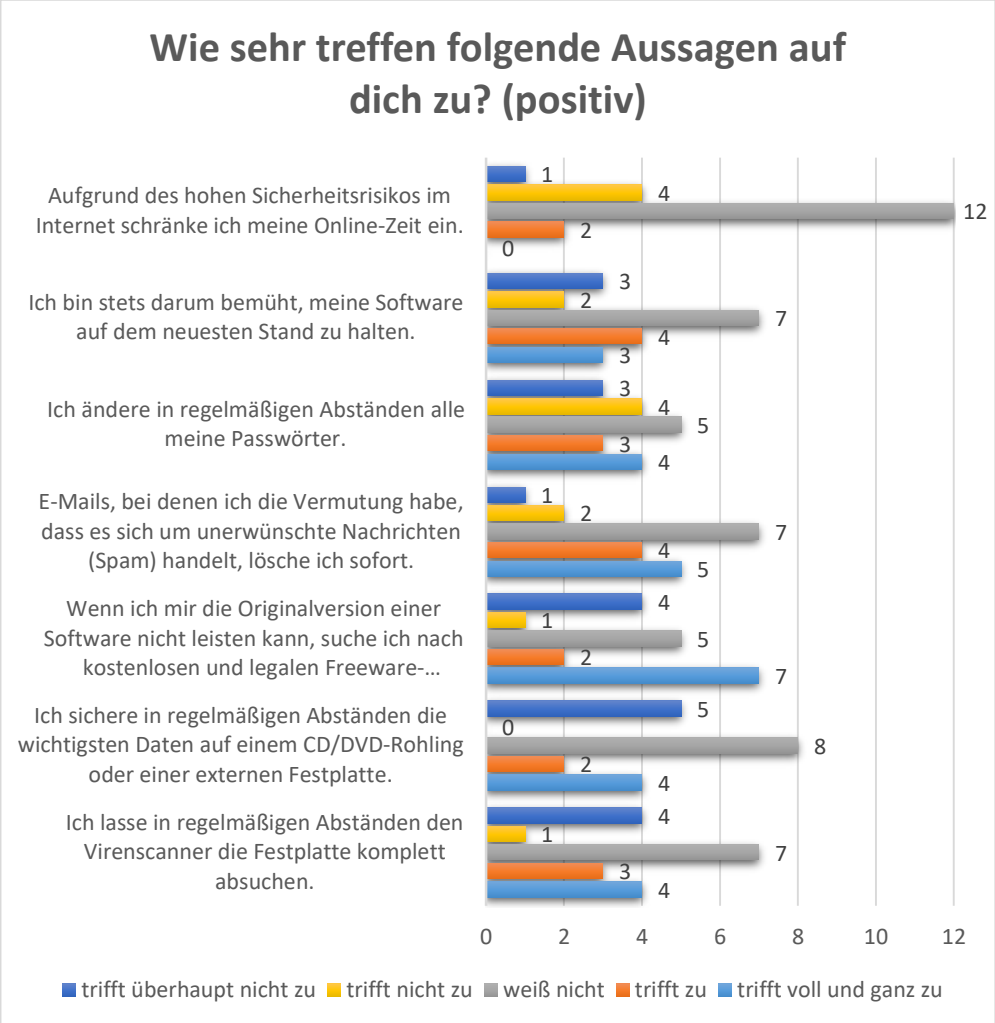
A18.14


Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten?
Ich nutze ...
10
5
0
3
9
7
5
7
7
5
6
8
5
9
5
3
9
7
3
9
7
Adblocker
Firewall
Verschlüsselung
Anti-Viren-Software
Anonymisierungstools
Anti-Tracking-Software
Ja
Weiß nicht
Nein

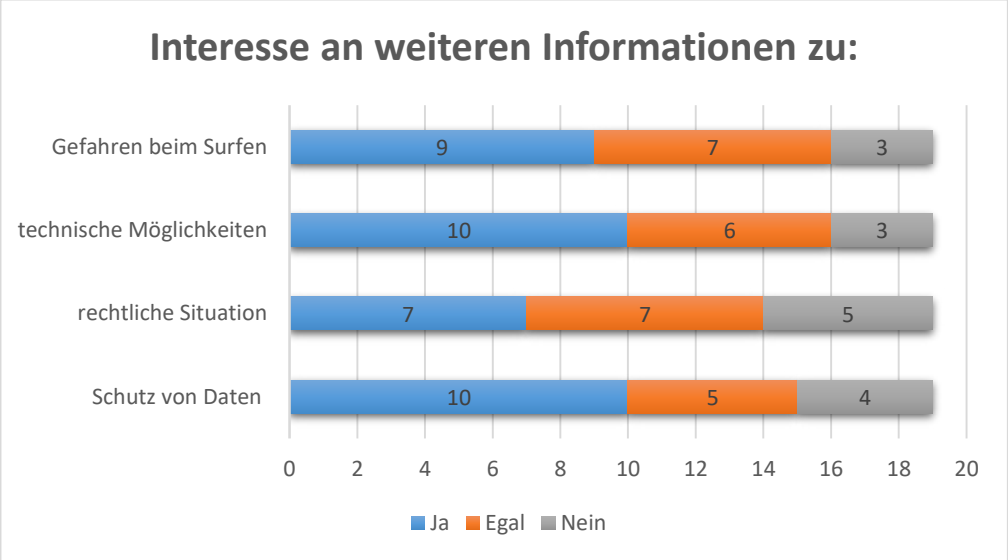

Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten?
Ich ...
12
10
8
6
4
2
0
9
3
7
11
5
3
11
5
3
5
7
7
3
9
7
nutze verschiedene Passwörter
nutze sichere Geräte mit PW
aktualisiere Sicherheitseinstellung in Sozialen Netzwerken
nutze sichere Seiten
deaktivere aktive Inhalte
Ja
Weiß nicht
Nein

A18.15


Wie sehr treffen folgende Aussagen auf dich zu? (negativ)
Ich achte nicht darauf, von welchen Seiten die Dateien stammen, die ich herunterlade.
6
1
6
1
5
Wenn ich per E-Mail oder im Chat einen Link zugesendet bekomme, klicke ich ihn meistens an, auch wenn ich mir nicht sicher bin, auf welcher Seite ich lande.
6
1
6
3
3
Ich denke nicht lange darüber nach, einen E-Mail-Anhang zu öffnen – ich tue es einfach.
6
2
8
1
2
Es kommt schon mal vor, dass ich Werbebanner, die reizvoll klingen, anklicke.
8
3
3
4
1
Ich suche immer erst nach Möglichkeiten, Musik im Internet kostenlos zu bekommen, bevor ich daran denke, sie zu kaufen.
4
0
3
4
8
0 1 2 3 4 5 6 7 8 9
trifft überhaupt nicht zu
trifft nicht zu
weiß nicht
trifft zu
trifft voll und ganz zu


Wie sehr treffen folgende Aussagen auf dich zu? (positiv)
Aufgrund des hohen Sicherheitsrisikos im Internet schränke ich meine Online-Zeit ein.
1
4
12
2
0
Ich bin stets darum bemüht, meine Software auf dem neuesten Stand zu halten.
3
2
7
4
3
Ich ändere in regelmäßigen Abständen alle meine Passwörter.
3
4
5
3
4
E-Mails, bei denen ich die Vermutung habe, dass es sich um unerwünschte Nachrichten (Spam) handelt, lösche ich sofort.
1
2
7
4
5
Wenn ich mir die Originalversion einer Software nicht leisten kann, suche ich nach kostenlosen und legalen Freeware-…
4
1
5
2
7
Ich sichere in regelmäßigen Abständen die wichtigsten Daten auf einem CD/DVD-Rohling oder einer externen Festplatte.
5
0
8
2
4
Ich lasse in regelmäßigen Abständen den Virenscanner die Festplatte komplett absuchen.
4
1
7
3
4
0 2 4 6 8 10 12
trifft überhaupt nicht zu
trifft nicht zu
weiß nicht
trifft zu
trifft voll und ganz zu

A18.16



A18.17

Erreichte Werte der Dimensionen im Vergleich zur Studie von Alexander Hug

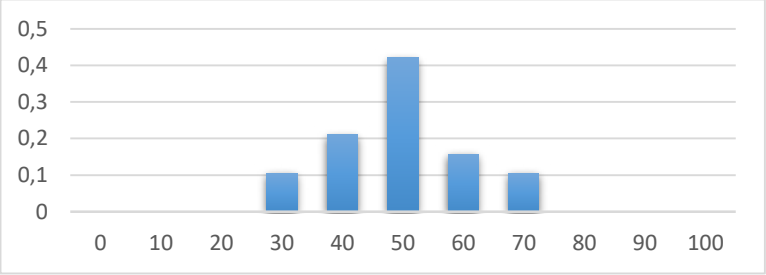
Untersuchung Thielen	W	RK	ANK	UK	HK	Mittelwert aller Dimensionen
Mittelwerte	35,1	62,6	31,9	58,8	58,1	49,3
MAX	66,7	95,4	87,5	100,0	84,4	71,2
MIN	0,0	45,5	0,0	25,0	25,0	29,1

Studie Hug	W	RK	ANK	UK	HK	Mittelwert aller Dimensionen
Mittelwerte	30,2	67,3	30,4	58,6	58,6	49,0
MAX	93,3	100,0	93,8	100,0	100,0	83,3
MIN	0,0	25,0	0,0	0,0	12,5	17,7

Veränderung	W	RK	ANK	UK	HK	Mittelwert aller Dimensionen
Mittelwerte	4,9	-4,7	1,5	0,2	-0,6	0,3
MAX	-26,7	-4,6	-6,3	0,0	-15,6	-12,2
MIN	0,0	20,5	0,0	25,0	12,5	11,4

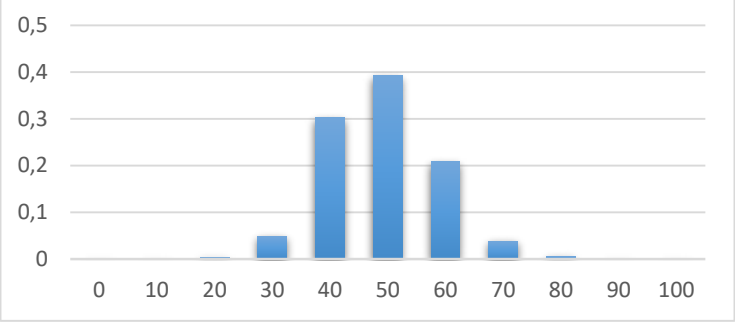
A18.18

Gerundeten Mittelwerte alle Schüler

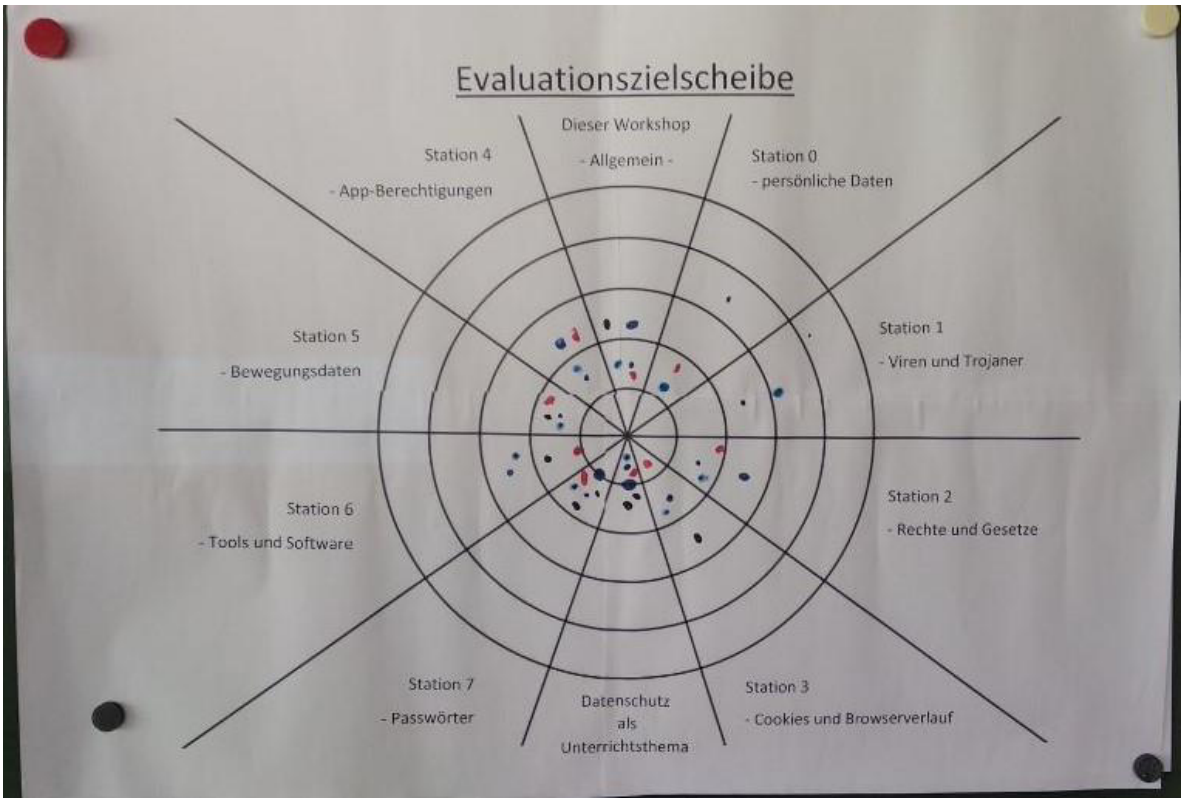


A18.19

Zum Vergleich die gerundeten Mittelwerte aller Schüler aus der Studie von Hug



Anhang A. 20. Evaluationszielscheibe - Auswertung des Workshops



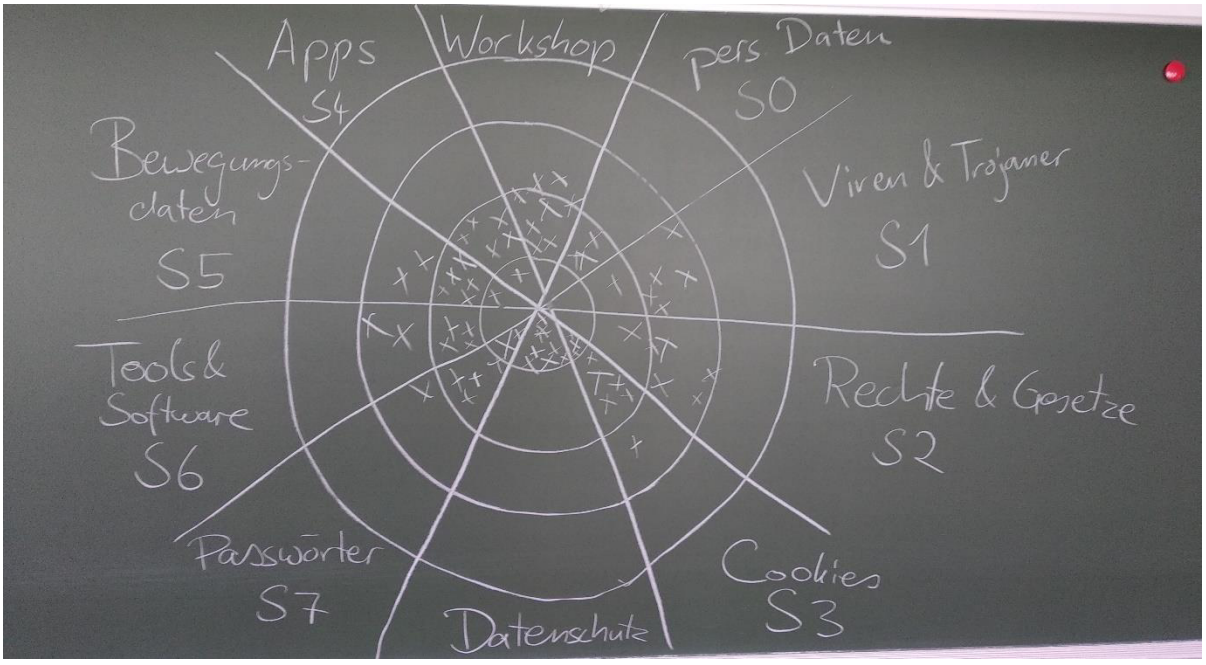


Abbildung 4. Evaluation Workshop

7. Literaturverzeichnis

Andersen, Uwe; Woyke, Wichard (Hg.) (2013): Handwörterbuch des politischen Systems der Bundesrepublik Deutschland. 7., vollständig aktualisierte Aufl. Wiesbaden: Springer VS.

Bastian, Johannes; Combe, Arno; Langer, Roman (2016): Feedback-Methoden. Erprobte Konzepte, evaluierte Erfahrungen. 4., erweiterte und überarbeitete Aufl. Weinheim, Basel: Beltz.

Bauer, Roland (2008): Schülergerechtes Arbeiten in der Sekundarstufe I. Lernen an Stationen. 6. Aufl. Berlin: Cornelsen Scriptor.

Bengesser, Cathrin (2017): Warum Datenschutz? MediaCulture-Online in Zusammenarbeit mit dem Landesmedienzentrum. Online verfügbar unter https://www.lmz-bw.de/warum-datenschutz.html, zuletzt geprüft am 27.08.2018.

Brandt, Friedemann; Heinzerling, Harald; Kempny, Günther (1991): Jugend im Datennetz. Ein Planspiel. In: *Materialien zum Unterricht, Sekundarstufe 1,* Band 105, Hrsg. Hessisches Institut für Bildungsplanung und Schulentwicklung. Online verfügbar unter http://medienwissenschaft.uni-bayreuth.de/unterrichtsmaterial/JugendImDatennetz.pdf, zuletzt geprüft am 10.08.2018.

Bredel, Ursula; Maaß, Christiane (2016): Leichte Sprache. Theoretische Grundlagen, Orientierung für die Praxis. 1. Aufl. Berlin: Dudenverlag.

Brenner, Gerd; Brenner, Kira (2010): Fundgrube Methoden. 3. Aufl. Berlin: Cornelsen Scriptor.

Brüning, Ludger; Saum, Tobias (2008): Strategien zur Schüleraktivierung. 4., überarb. Aufl. Essen: Neue Deutsche Schule Verlagsgesellschaft.

Bundesamt für Sicherheit in der Informationstechnik (2011): BSI gibt Tipps für sichere Passwörter. Bonn. Online verfügbar unter https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2011/Passwortsicherheit_27012011.html, zuletzt geprüft am 18.08.2018.

Bundesministeriums der Justiz und für Verbraucherschutz (30.06.2017): Bundesdatenschutzgesetz (BGBl. I S. 2097). BDSG, vom 30.06.2017. Fundstelle: Bundesgesetzblatt, S. 2097. Online verfügbar unter http://www.gesetze-im-internet.de/bdsg_2018/, zuletzt geprüft am 20.08.2018.

Bundesverfassungsgericht, Urteil vom 15.12.1983, Aktenzeichen 1 BvR 209, 269, 362, 420, 440, 484/83. In: *BVerGE 65 - 1*. Online verfügbar unter http://www.servat.unibe.ch/dfr/bv065001.html, zuletzt geprüft am 25.08.2018.

Czernik, Agnieszka: Definition und Unterscheidung der Begriffe Daten, Informationen & Wissen. Online verfügbar unter https://www.datenschutzbeauftragter-info.de/definition-und-unterscheidung-der-begriffe-daten-informationen-wissen/, zuletzt geprüft am 22.08.2018.

Dachwitz, Ingo; Rudl, Tomas; Rebiger, Simon (2018): FAQ: Was wir über den Skandal um Facebook und Cambridge Analytica wissen. Hg. v. Markus Beckedahl. Online verfügbar unter https://netzpolitik.org/2018/cambridge-analytica-was-wir-ueber-das-groesste-datenleck-in-der-geschichte-von-facebook-wissen/, zuletzt geprüft am 22.08.2018.

Dunham, Ken; Abu-Nimeh, Saeed (2009): Mobile malware attacks and defense. The only book for analyzing and mitigating mobile malicious code! ; understand the history and threat landscape of rapidly emerging mobile attacks ; analyze mobile device/platform vulnerabilities and exploits ; mitigate current and future mobile malware threats. Burlington: Syngress Publishing.

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

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

Eggert, Katrin; Heimburger, Ralf; Kramer, Rudi; Spaeing, Frank (Hg.) (2016): Datenschutz geht zur Schule. Sensibler Umgang mit persönlichen Daten. Arbeitsblätter. Berufsverband der Datenschutzbeauftragten. Online verfügbar unter https://klicksafe.de/service/materialien/broschueren-ratgeber/datenschutz-geht-zur-schule/, zuletzt geprüft am 23.09.2018.

Europäische Union (04.05.2016): Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). 2016/679/EU, vom Abl. L119 vom 04.05.2016, S.1. In: *ABl. (Amtsblatt der Europäischen Union)* (L 119), S. 1–88. Online verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=OJ:L:2016:119:TOC, zuletzt geprüft am 22.08.2018.

Feierabend, Sabine; Plankenhorn, Theresa; Rathgeb, Thomas (2016): KIM-Studie 2016. Kindheit, Internet, Medien. Basisuntersuchung zum Medienumgang 6- bis 13-Jähriger. Hg. v. Medienpädagogischer Forschungsverbund Südwest. Online verfügbar unter https://www.mpfs.de/fileadmin/files/Studien/KIM/2016/KIM_2016_Web-PDF.pdf, zuletzt geprüft am 29.08.2018.

Fileccia, Marco; Kimmel, Birgit; Rack, Stefanie; Tatsch, Isabell; Groschup, Friederike (2016): Knowhow für junge User. Mehr Sicherheit im Umgang mit dem World Wide Web. Materialien für den Unterricht. Hg. v. klicksafe. Landeszentrale für Medien und Kommunikation Rheinland-Pfalz (Koordinator); Landesanstalt für Medien Nordrhein-Westfalen. 1. Aufl. Ludwigshafen. Online verfügbar unter https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Lehrerhandbuch/klicksafe_Lehrerhandbuch.pdf, zuletzt geprüft am 27.08.2018.

Fischer, Peter; Hofer, Peter (2011): Lexikon der Informatik. 15., überarb. Aufl. Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg.

Freis, Herbert (2012): Handreichungen zur informatischen Bildung. MINISTERIUM für BILDUNG, FRAUEN und JUGEND. Online verfügbar unter https://informatik.bildung-rp.de/fileadmin/user_upload/informatik.bildung-rp.de/Informatische_Bildung/Handreichung_Informatische_Bildung_S_I_05-09-12.pdf, zuletzt geprüft am 27.08.2018.

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

Grimm, Rüdiger; Simić-Draws, Daniela; Bräunlich, Katharina; Kasten, Andreas; Meletiadou, Anastasia (2016): Referenzmodell für ein Vorgehen bei der IT-Sicherheitsanalyse. In: *Informatik Spektrum* 39 (1), S. 2–20. Online verfügbar unter https://link.springer.com/article/10.1007/s00287-014-0807-3.

Groß, Daniel; Hahn, Katina; Jacob, Harald; Karger, Axel; Pfurtscheller, Stephan; Stingl, Benjamin; Weller, Ricarda (2014): Medien.Konzepte.Kompetenz. Handreichung zur Medienkonzeptentwicklung für die schulische Praxis. Hg. v. Pädagogisches Landesinstitut Rheinland-Pfalz. Bad Kreuznach. Online verfügbar unter https://medienkompass.bildung-rp.de/fileadmin/user_upload/medienkompass.bildung-rp.de/HR_Medienkompetenz_WEB_final.pdf, zuletzt geprüft am 30.08.2018.

Hartmann, Werner; Näf, Michael; Reichert, Raimond (2007): Informatikunterricht planen und durchführen. 1. korrigierter Nachdruck. Berlin, Heidelberg: Springer.

Haschler, Steffen (2017): Datensatz - Datenschatz? Warum Datenschutz und Datensicherheit wichtig sind. Hg. v. klicksafe. Landeszentrale für Medien und Kommunikation Rheinland-Pfalz (Koordinator); Landesanstalt für Medien Nordrhein-Westfalen. 1. Aufl. Ludwigshafen. Online verfügbar unter https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Allgemein/ks_to_go_Datensatz_-_Datenschatz.pdf, zuletzt geprüft am 27.08.2018.

Hegele, Irmintraut (2016): Stationenarbeit - Ein Einstieg in den offenen Unterricht. In: Wiechmann, Jürgen und Wildhirt, Susanne (Hg.): Zwölf Unterrichtsmethoden. Vielfalt für die Praxis. 6., vollständig überarbeitete Aufl. Weinheim, Basel: Beltz, S. 65–80.

hessenschau.de (2018): Facebook-Party auf Wiesbadener Neroberg eskaliert. In: *hessenschau*, 25.02.2018. Online verfügbar unter https://www.hessenschau.de/panorama/facebook-party-auf-wiesbadener-neroberg-eskaliert,neroberg-randale-100.html, zuletzt geprüft am 23.08.2018.

Heuer, Hanna; Lechner, Julia; Schulz, Mark (2009): Trojanische Pferde. Hg. v. Bundesamt für Sicherheit in der Informationstechnik (BSI). Bonn. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05021.html, zuletzt geprüft am 22.08.2018.

Hilt, Franz; Grüner, Thomas; Schmidt, Jürgen; Beyer, Anna; Kimmel, Birgit; Rack, Stefanie; Tatsch, Isabell (2018): Was tun bei (Cyber)Mobbing? Systematische Intervention und Prävention in der Schule. Hg. v. klicksafe. Ludwigshafen. Online verfügbar unter https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Allgemein/Was_tun_bei_Cybermobbing.pdf, zuletzt geprüft am 13.09.2018.

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

Hug, Alexander (2018a): "I've got nothing to hide!" - Survey on Data Privacy Competence with German Schoolchildren. In: Mühling, Andreas, Cutts, Quintin und Schwill, Andreas (Hg.): Proceedings of the 13th Workshop in Primary and Secondary Computing Education (WiPSCE '18). 13th Workshop in Primary and Secondary Computing Education. Potsdam, 04-06.10.2018: ACM. in Druck.

Hug, Alexander (2018b): Ergebnisse der Studie zur Datenschutzkompetenz Jugendlicher im Alter von 10 bis 13 Jahren. Koblenz, 22.03.2018. mündlich an Johannes Thielen.

Hug, Alexander; Grimm, Rüdiger (2017): Entwicklung eines Datenschutzkompetenzmodells. In: Diethelm, Ira (Hg.): Informatische Bildung zum Verstehen und Gestalten der digitalen Welt. 17. GI-Fachtagung Informatik und Schule ; 13.-15. September 2017 Oldenburg. Bonn: Gesellschaft für Informatik e.V. (GI) (GI-Edition - lecture notes in informatics (LNI) Proceedings, volume P-274), S. 167–170. Online verfügbar unter https://dl.gi.de/bitstream/handle/20.500.12116/4311/paper.pdf?sequence=1&isAllowed=y, zuletzt geprüft am 22.08.2018.

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

Jaax, Liske (2016): Was Arbeitgeber prüfen dürfen. Background-Check von Bewerbern. Online verfügbar unter https://www.impulse.de/recht-steuern/background-check-bewerber/1032765.html, zuletzt geprüft am 22.08.2018.

Koubek, Jochen; Schulte, Carsten; Schulze, Peter; Witten, Helmut (2009): Informatik im Kontext (IniK). Ein integratives Unterrichtskonzept für den Informatikunterricht. In: Koerber, Bernhard (Hg.): Zukunft braucht Herkunft. 25 Jahre "INFOS - Informatik und Schule" ; INFOS 2009, 13. GI-Fachtagung "Informatik und Schule", 21. bis 24. September 2009 an der Freien Universität Berlin. Bonn: Gesellschaft für Informatik e.V. (GI-Edition Proceedings, 156), S. 268–279. Online verfügbar unter https://medienwissenschaft.uni-bayreuth.de/inik/material/InformatikImKontextINFOS2009.pdf, zuletzt geprüft am 15.09.2018.

Kultusministerkonferenz (2016): Bildung in der digitalen Welt. Strategie der Kultusministerkonferenz. Hg. v. Sekretariat der Kultusministerkonferenz. Kultusministerkonferenz. Berlin. Online verfügbar unter https://www.kmk.org/fileadmin/Dateien/pdf/PresseUndAktuelles/2018/Digitalstrategie_2017_mit_Weiterbildung.pdf, zuletzt geprüft am 29.08.2018.

Landesanstalt für Medien Nordrhein-Westfalen (Hg.) (2014): Workshop Handy. Arbeitsblatt. Online verfügbar unter https://www.medienscouts-nrw.de/wp-content/uploads/2014/05/4.2_Handy_Stationen-Stand-10.02.2017.pdf, zuletzt geprüft am 24.07.2018.

Löbering, Christian (Hg.) (2014): Gewinnspiele & Co.: Persönliche Daten werden oft weitergegeben. PC-Welt. Online verfügbar unter https://www.pcwelt.de/news/Gewinnspiele-Co-Persoenliche-Daten-werden-oft-weitergegeben-137835.html, zuletzt geprüft am 15.09.2018.

Makosch, Yeliz (2018): Entwicklung eines Kriterienkatalogs zur Qualität von Unterrichtsmaterialen und Anwendung dessen durch Analyse von Materialien zum Thema Datenschutz. Masterarbeit. Universität Koblenz-Landau, Koblenz. Fachbereich 4 Informatik, Institut Computervisualistik.

Mattes, Wolfgang (2011): Methoden für den Unterricht. Kompakte Übersichten für Lehrende und Lernende. Druck A. Paderborn: Schöningh.

Mayer, Roger C.; Davis, James H.; Schoorman, F. David (1995): An Integrative Model Of Organizational Trust. In: *AMR* 20 (3), S. 709–734.

Meyer, Hilbert (2017): Unterrichtsmethoden. II: Praxisband. 15. Auflage. Berlin: Cornelsen.

Meyer, Hilbert (2018): Leitfaden Unterrichtsvorbereitung. 9. Auflage. Berlin: Cornelsen.

Miklis, Katharina (2011): Facebook-Fans stürmen Geburtstagsparty. Im Vorgarten von Thessa. In: *stern*, 04.06.2011. Online verfügbar unter https://www.stern.de/digital/online/facebook-fans-stuermen-geburtstagsparty-im-vorgarten-von-thessa-3028024.html, zuletzt geprüft am 15.09.2018.

Ministerium für Bildung (Hg.) (2017): Orientierungsrahmen Schulqualität. 5. Aufl. Online verfügbar unter https://ors.bildung-rp.de/fileadmin/user_upload/ors.bildung-rp.de/Broschuere_ORS_2017_WEB.pdf, zuletzt geprüft am 30.08.2018.

Ministerium für Bildung, Wissenschaft und Weiterbildung (Hg.) (1998): Lehrplan Deutsch. (Klassen 5-9/10) Hauptschulen,Realschulen,Gymnasien, Regionale Schulen, Gesamtschulen. Grünstadt. Online verfügbar unter https://lehrplaene.bildung-rp.de/, zuletzt geprüft am 30.08.2018.

Ministerium für Bildung, Wissenschaft und Weiterbildung RLP (Hg.) (2000): Lehrplan Ethik. Sekundarstufe I (Klassen 5 - 9/10) Hauptschule, Realschule, Gymnasium, Regionale Schule, Gesamtschule. Grünstadt. Online verfügbar unter https://lehrplaene.bildung-rp.de/, zuletzt geprüft am 30.08.2018.

Ministerium für Bildung, Wissenschaft, Jugend und Kultur Rheinland-Pfalz (Hg.) (o. J.): Lehrplan Informatik. Wahlfach und Wahlpflichtfach an Gymnasien und Integrierten Gesamtschulen (Sekundarstufe I). Online verfügbar unter https://informatik.bildung-rp.de/lehrplaene.html, zuletzt geprüft am 15.08.2018.

Ministerium für Bildung, Wissenschaft, Jugend und Kultur Rheinland-Pfalz (Hg.) (2010a): Lehrplan Informatik. Grund- und Leistungsfach, Einführungsphase und Qualifikationsphase der gymnasialen Oberstufe (Mainzer Studienstufe). Online verfügbar unter http://informatik.bildung-rp.de/lehrplaene.html, zuletzt geprüft am 25.08.2018.

Ministerium für Bildung, Wissenschaft, Jugend und Kultur Rheinland-Pfalz (Hg.) (2010b): Richtlinie Verbraucherbildung an allgemeinbildenden Schulen in 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 12.09.2018.

Ministerium für Bildung, Wissenschaft, Weiterbildung und Kultur (Hg.) (2016): Lehrplan für die gesellschaftswissenschaftlichen Fächer. Erdkunde, Geschichte, Sozialkunde. Mainz. Online verfügbar unter https://lehrplaene.bildung-rp.de/.

Müsgens, Martin (2015): Datenschutz im (mobilen) Internet. Hg. v. klicksafe und Internet-ABC. 4. Aufl. Düsseldorf. Online verfügbar unter http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Eltern_Allgemein/Datenschutz_im__mobilen__Internet_Brosch%C3%BCre.pdf, zuletzt geprüft am 28.08.2018.

Pariser, Eli (2011): The filter bubble. What the Internet is hiding from you. New York, NY: Penguin Press.

Rack, Stefanie; Fileccia, Marco (2015): Ich bin öffentlich ganz privat. Datenschutz und Persönlichkeitsrecht im Web Materialien für den Unterricht. Zusatzmodul zu Knowhow für junge User Materialien für den Unterricht. Hg. v. klicksafe. 3. Aufl. Ludwigshafen. Online verfügbar unter https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatzmodule/LH_Zusatzmodul_Datenschutz_klicksafe.pdf, zuletzt geprüft am 26.08.2018.

Rack, Stefanie; Sauer, Fabian (2018a): "Safer Smartphone". Sicherheit und Schutz für das Handy. Arbeitsmaterial für den Unterricht Heft II. klicksafe in Zusammenarbeit mit Handysektor. 2. Aufl. Ludwigshafen. Online verfügbar unter https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Always_On/SaferSmartphone.pdf, zuletzt geprüft am 27.08.2018.

Rack, Stefanie; Sauer, Fabian (2018b): Always on. Arbeitsmaterial für den Unterricht - Heft 1. klicksafe in Zusammenarbeit mit Handysektor. 3. Aufl. Ludwigshafen. Online verfügbar unter https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Always_On/AlwaysOn2015.pdf, zuletzt geprüft am 28.08.2018.

Rieger, Frank (2013): Von Daten und Macht - Essay. Hg. v. bpb.de. Bundeszentrale für politische Bildung. Online verfügbar unter http://www.bpb.de/apuz/157538/von-daten-und-macht-essay?p=1, zuletzt geprüft am 23.08.2018.

Ruff, Mathis (o.J.): Gewinnspiel: Was beim Datenschutz zu beachten ist. Berufsverband der Rechtsjournalisten e.V. Online verfügbar unter https://www.datenschutz.org/gewinnspiel/, zuletzt geprüft am 09.09.2018.

Saint-Mont, Uwe (2013): Die Macht der Daten. Wie Information unser Leben bestimmt. Berlin: Springer Spektrum.

Schallaböck, Jan: Rechtsfragen im Netz: Themenreihe von iRights.info + klicksafe. Vom Web-Tracking zum App-Tracking. Hg. v. iRIGHTS info. klicksafe.de. Online verfügbar unter https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/iRights_Themenreihe/Schwerpunkt_31_Vom_Web-Tracking_zum_App-Tracking.pdf, zuletzt geprüft am 26.08.208.

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

Seidel, Ulrich (1970): Persönlichkeitsrechtliche Probleme der elektronischen Speicherung privater Daten. In: *Neue Juristische Wochenschrift*, S. 1581–1583. Online verfügbar unter http://www.fiff.de/publikationen/fiff-kommunikation/fk-2015/fk-2015-2/fk-2015-2-content/fk-2-15-s62.pdf, zuletzt geprüft am 22.08.2018.

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

Six, Ulrike; Gleich, Uli; Gimmler, Roland (Hg.) (2007b): Kommunikationspsychologie -- Medienpsychologie. Lehrbuch. 1. Aufl. Weinheim: BeltzPVU.

Snap Group Limited (2018): Servicebestimmungen der Snap Group Limited. Unter Mitarbeit von David Lewis. Hg. v. Snap Group Limited. Snap Group Limited. London. Online verfügbar unter https://www.snap.com/de-DE/terms/#terms-row, zuletzt geprüft am 23.08.2018.

Stachowiak, Herbert (1973): Allgemeine Modelltheorie. Wien: Springer.

Statista GmbH (2018): Prognose zu den Marktanteilen der Betriebssysteme am Absatz vom Smartphones weltweit in den Jahren 2018 und 2022. Hamburg. Online verfügbar unter https://de.statista.com/statistik/daten/studie/182363/umfrage/prognostizierte-marktanteile-bei-smartphone-betriebssystemen/, zuletzt geprüft am 14.09.2018.

Vereinte Nationen - Generalversammlung (10.12.1948): Resolution der Generalversammlung 217 A (III). Allgemeine Erklärung der Menschenrechte. Online verfügbar unter http://www.un.org/depts/german/menschenrechte/aemr.pdf, zuletzt geprüft am 15.09.2018.

Verwaltungsgericht Köln, Urteil vom 20.04.2018, Aktenzeichen 9 K 7417/17. Online verfügbar unter http://www.vg-koeln.nrw.de/behoerde/presse/Pressemitteilungen/01_180420/index.php, zuletzt geprüft am 24.08.2018.

Vollmert, Markus; Lück, Heike (2015): Google Analytics. Das umfassende Handbuch. 2 Aufl. Bonn: Rheinwerk Computing.

Wiechmann, Jürgen; Wildhirt, Susanne (Hg.) (2016): Zwölf Unterrichtsmethoden. Vielfalt für die Praxis. 6., vollständig überarbeitete Aufl. Weinheim, Basel: Beltz.

Wolf, Thomas (2011): In den Fängen der Datendiebe. Daten bedeuten Macht - und Geld. In: *Focus*, 11.05.2011. Online verfügbar unter https://www.focus.de/finanzen/recht/tid-22263/datenschutz-daten-bedeuten-macht-und-geld_aid_626155.html, zuletzt geprüft am 18.08.2018.