UNIVERSITÄT KOBLENZ · LANDAU
Fachbereich 4: Informatik

Erstellung von Aufgaben zu Datenschutz und Datensicherheit von Smartphone-Applikationen für Informatik im Kontext

Bachelorarbeit

zur Erlangung des Grades eines Bachelor of Education
im Studiengang Lehramt Informatik

vorgelegt von

Marco Böhm

Erstgutachter:	Prof. Dr. Rüdiger Grimm Institut für Wirtschafts- und Verwaltungsinformatik - IT Risk Management
Zweitgutachter:	Alexander Hug Institut für Wirtschafts- und Verwaltungsinformatik - Fachdidaktik Informatik

Koblenz, im Mai 2015

Erklärung

Hiermit bestätige ich, dass die vorliegende Arbeit von mir selbstständig 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).

	Ja	Nein
Mit der Einstellung der Arbeit in die Bibliothek bin ich einverstanden.	☐	☐
Der Veröffentlichung dieser Arbeit im Internet stimme ich zu.	☐	☐

.....

(Ort, Datum) (Marco Böhm)

Zusammenfassung

Mit der rasant fortschreitenden Entwicklung von Informatiksystemen und Algorithmen ist die Erfassung und Verarbeitung von Daten in immer größeren Umfang möglich. Verschiedene Initiativen haben sich dadurch motiviert zur Aufgabe gemacht, über die daraus resultierenden Gefahren für die Persönlichkeitsrechte und die Meinungsfreiheit aufzuklären. Dies soll einen bewussteren Umgang mit personenbezogenen Daten zur Folge haben. Zum Schutz der Grundrechte bedarf es aufgeklärter und informierter Nutzer, diese Aufgabe können die Initiativen allerdings nicht alleine leisten. Die staatlichen Bildungseinrichtungen und besonders die Schulen, stehen hier in der Pflicht sich an der Lösung des Problems zu beteiligen. Um ihrem Bildungsauftrag im vollen Ausmaß gerecht zu werden, bedarf es struktureller Änderungen, wie der Änderung von Lehrplänen. Solange diese allerdings nicht erfolgt sind, muss in und mit den gegebenen Strukturen gearbeitet werden. Eine Plattform dafür bietet der schulische Informatikunterricht.

Die vorliegende Arbeit stellt eine Unterrichtsreihe zur Behandlung von Datenschutz und Datensicherheit vor. Es wurde dabei ein kontextorientierter Ansatz nach Vorbild von *Informatik im Kontext* gewählt. Die Reihe *Smartphone-Applikationen* beinhaltet über die genannten primären Themen der Unterrichtsreihe hinaus weitere Dimensionen, die bei der Nutzung von Smartphones auftreten. Durch den direkten Bezug zum Alltag der Schüler soll dabei eine möglichst hohe Betroffenheit erzeugt werden. Dadurch sollen die Schüler ihr bisheriges Nutzungsverhalten überdenken und im besten Fall ihren Altersgenossen als Vorbilder dienen. Die Prüfung der Durchführbarkeit der Reihe im Unterricht steht noch aus. Diese war im Rahmen dieser Arbeit, begründet durch die begrenzte Bearbeitungszeit, nicht zu leisten.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Kapitel 1

Einleitung

Seit 1998 jährlich durchgeführt, beschäftigt sich die JIM-Studie [FPR14] unter anderem mit Freizeitaktivitäten, Mediennutzung und -besitz von Kindern und Jugendlichen im Alter von 12 bis 19 Jahren. Dadurch lassen sich Entwicklungen beim Konsum von Medien erkennen, bezüglich Smartphones sind drei in Tabelle 1.1 dargestellt[1].

	2014	2013	2012	2011
Haushalte mit Smartphones	94 %	81 %	63 %	43 %
Besitz eines Smartphones	88 %	72 %	47 %	35 %
Internetnutzung via Handy/Smartphone	86 %	73 %	49 %	29 %

Tabelle 1.1 Entwicklungen bei der Medienausstattung und -nutzung von Kindern und Jugendlichen [FPR14]

Mit einer Steigerung um 13 Prozentpunkte (PP) im Vergleich zum Vorjahr, ist das Smartphone mittlerweile in 94 % der deutschen Haushalte zu finden. 97 % der Befragten sind sogar in Besitz eines eigenen Mobiltelefons, wobei 88 % dieser Geräte internetfähige Smartphones sind, was einer Steigerung um 16 PP entspricht. Genutzt werden diese von 93 % mehrmals wöchentlich, was einer Zunahme um 3 PP entspricht. Die 100 %-Marke und damit eine Vollausstattung mit Smartphones wird in Deutschland aufgrund der anhaltenden Entwicklung in naher Zukunft erreicht sein. Damit haben sich auch die Gewohnheiten bei der Nutzung

[1]Dabei wurden für eine bessere Darstellung der Entwicklung die Werte der Studien von 2011-2013 ergänzt.

verändert. Die Benutzung des mobilen Internets ist mit 75 % an zweiter Stelle nach der Nutzung von Musik und vor dem Telefonieren. Bei der Internetnutzung zeigt sich eine steigende Tendenz, +57 PP seit der Studie von 2011. Als Viertes steht mit 63 % die Nutzung von Communities bzw. deren Applikationen. Die Smartphone-Nutzung birgt allerdings auch Risiken, denn neben unerwünschten Begleiterscheinungen des Internets ist das Ausmaß der Funktionalität diverser Anwendungen den Schülern[2] nicht bewusst. Begleiterscheinungen können bspw. Mobbing oder das Versenden von gewalttätigen bzw. pornographischen Filmen sein. Diese sind nicht zu unterschätzen, da deren Häufigkeit und Effekte sich durch die ständige Verfügbarkeit der mobilen Geräte verstärken können. Obwohl 80 % der Befragten zumindest bekannt ist, dass einige Apps Daten auslesen und an die Anbieter weiterleiten, haben nur 56 % die Übertragung von Ortungsdaten generell ausgeschaltet. Weitere Fragen bzgl. der Smartphone-Anwendungen werden in der JIM-Studie nicht gestellt, sodass über ein generelles Bewusstsein für die Funktionsweise und Datennutzung eben dieser keine Aussage getroffen werden kann.

Es zeigt sich jedoch deutlich, dass das Medium Smartphone von sehr hoher Bedeutung für die heutige Jugend ist und dass es bezüglich einiger Funktionen und Risiken potentiell noch erheblicher Aufklärungsbedarf besteht. Ziel dieser Arbeit ist die Wichtigkeit des Datenschutzes für den Informatikunterricht herauszuarbeiten und kontextbezogene Aufgaben zum Thema *Smartphone-Applikationen* zu entwickeln. Nachdem die Idee des kontextbezogenen Unterrichts vorgestellt wurde, werden die technischen Grundlagen zu Smartphones thematisiert. Die potentiellen Angriffsmöglichkeiten auf mobile Geräte und mögliche Gegenmaßnahmen bilden die Grundlage für einen Unterrichtsentwurf im Kontext *Smartphone-Applikationen*. Die Schüler sollen im Laufe der Reihe ein verbessertes Verständnis von der Funktionsweise ihres Smartphones und den installierten Applikationen erhalten und sich möglicher Konsequenzen bei der Nutzung bewusst werden.

[2]Im Folgenden bezieht sich die maskuline Form immer auf die Angehörigen beider Geschlechter.

1.1 Die Wichtigkeit des Datenschutzes

Unter anderem Jadin und Farthofer [JF14] stellen im Abschlussbericht ihrer Begleitforschung zu dem Projekt *Netkompass für Social Web*[3] fest, dass vielen Jugendlichen mögliche Risiken bzgl. der Vernetzung in sozialen Netzwerke und der Verwendung des mobilen Internets oftmals nicht bekannt sind. Das ein mangelndes Verständnis von und fahrlässiger Umgang mit dem Datenschutz weitreichende Folgen haben kann zeigt das Projekt Datenschutz [Pro]. Dieses führt eine interessante Liste von Datenschutzvorfällen in deutschen Behörden und Unternehmen. Diese Vorfälle reichen von Akten im Papiermüll bis hin zu frei im Internet zugänglichen Kundendaten. Die Bedeutung des Datenschutzes verlangt nach einem angemessenen Bildungskonzept, denn über alle Generationen hinweg gibt es Defizite beim Verhalten bzgl. des Datenschutzes.

1.1.1 Datenschutz als Bildungsaufgabe

Um sich selbst und seine Daten schützen zu können, sind Kenntnisse über die Datenverarbeitung erforderlich. Das Bundesverfassungsgericht stellte bereits bei seinem Urteil aus dem Jahre 1983 zur Volkszählung fest, *dass jeder wissen soll, wer was, wann und bei welcher Gelegenheit über ihn weiß* [Mes14]. Dazu Bedarf es nach Mester [Mes14] Aufklärung, welche Möglichkeiten der Information es gibt und wie man seine Daten schützen kann, denn ohne das Wissen um die Gefahren des Datenmissbrauchs kann Datenschutz nicht durchgesetzt werden.

Der Landesbeauftrage für Datenschutz in Rheinland-Pfalz Edgar Wagner erklärte 2012 den Datenschutz zum Bildungs- und Erziehungsauftrag. Die Bürger müssen in der Lage sein verantwortungsvoll mit persönlichen Daten von sich selbst und anderen umzugehen, da die Möglichkeiten des Gesetzgebers im Web 2.0 an ihre Grenzen stoßen. Die *Aktivisten des Web 2.0* [Wag12, S. 83] hinterlassen überall Datenspuren, über deren Speicherung schnell der Überblick verloren gehen kann. Auch das Bewusstsein, dass Daten im Netz schwer bis nicht zu löschen sind und deshalb auch in ferner Zukunft noch abrufbar sind, fehlt größtenteils. Hinzu kommt eine Überforderung der Nutzer, die den technischen Entwicklungen nicht mehr folgen können.

[3] Eine nähere Beschreibung folgt in 1.1.2

Der Schaden, der unter anderem durch Kommerzialisierung von Daten durch die Wirtschaft angerichtet wird, trifft dabei nicht nur die eigene Privatsphäre, sondern kann sich auch zur Bedrohung der demokratischen Ordnung entwickeln, wenn die gesellschaftlichen Grundwerte bedroht sind. Dies beschreibt Thilo Weichert, Landesbeauftragter für Datenschutz in Schleswig-Holstein, in seinen Ausführungen zu Big Data [Wei13]. Mit ihren Überwachungsprogrammen haben die Vereinigten Staaten von Amerika die Möglichkeit der Analyse von unvorstellbar großen Datenmengen[4] und damit des Bildens von Rückschlüssen auf Vermögen, Interessen oder Konsumverhalten, was eine Bildung von individuellen Profilen ermöglicht. Die erfolgte Nutzung dieser Möglichkeiten und daraus folgende Konsequenzen für die Grundrechte der informationellen Selbstbestimmung und Meinungsfreiheit lassen sich nur erahnen.

Somit ist es unbedingt erforderlich, dass die Bürger sich eine eigene Meinung bilden können, denn das *wirkungsvollste Mittel zum Grundrechtsschutz im Internet ist der aufgeklärte und informierte Nutzer* [Wag12, S. 84]. Daraus abgeleitet sieht Wagner die Notwendigkeit, dass ein Bewusstsein für digitale Zusammenhänge geschaffen werden muss, Rechte und Pflichten beim Datenschutz bekannt sein müssen und ein werteorientiertes Bewusstsein geschaffen werden muss. Dazu müssen alle Bildungsinstitutionen mit einbezogen werden, da alle Generationen durch die stetige Entwicklung der Technik betroffen sind, wobei die Schule laut Wagner [Wag12] am stärksten in der Pflicht steht.

Bei Jugendlichen besteht folglich ein erhöhter Bedarf an Aufklärung. Ein Versuch diese Aufklärungsarbeit zu leisten bilden verschiedene Initiativen, von denen einige exemplarisch vorgestellt werden.

1.1.2 Vorhandene Initiativen

Es existieren bereits verschiedene Projekte von verschiedenen Initiatoren, die sich der Schaffung eines Bewusstsein bei Jugendlichen für Datenschutz und Datensicherheit auf die Fahne geschrieben haben. Exemplarisch sollen hier einige Initiativen kurz vorgestellt werden.

[4] 97 Milliarden Dateneinheiten alleine im März 2013 durch die NSA [Wei13]

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.[5] ist eine Interessenvertretung für Datenschutzbeauftragte und Datenschutzberater in Deutschland. Aus der Satzung geht hervor:

> *Zweck des Vereins ist auf Verbandsebene die Interessen der betrieblichen und behördlichen Datenschutzbeauftragten im Sinne einer dem Stand der Technik angemessenen Realisierung von Datenschutz und Datensicherung zu fördern.*

Eine Maßnahme dazu ist die im Jahr 2008 ins Leben gerufene Initiative *Datenschutz geht zur Schule*. Der BvD versucht damit dem oft lockere Umgang mit privaten und Unternehmensdaten entgegenzuwirken. Die Initiative setzt bei Schülern an, denn je früher die Sensibilisierung stattfindet, desto besser. Es werden dazu von fachkundigen und geschulten, ehrenamtlichen Dozenten Workshops zu verschiedenen Themen des Datenschutzes an interessierten Schulen durchgeführt. Am Ende sollen die Schüler ein besseres Bewusstsein für ihre Daten und deren Sicherheit entwickeln, sowie ihr Verhalten anpassen. Für Eltern und Lehrer gibt es ebenfalls Angebote und Materialien, damit sie die Schüler beim Lernprozess unterstützen können [KS14].

Beim Projekt *Netkompass für Social Web*[6] erstellen Schüler von Partnerschulen der FH Oberösterreich unter Anleitung von Studenten Informationsmaterialien zu den Themenfeldern Privatsphäre und Datenschutz im Social Web. Diese Materialien dienen der Bereitstellung einer Informationsplattform für Jugendliche zur Selbstinformation. Da es sich hierbei um Arbeiten von Schülern handelt, fallen die Ergebnisse sehr unterschiedlich aus: sie reichen von Fotostorys über Podcasts bis zu selbstgedrehten Videos. Für die partizipierenden Schüler ist durch die aktive Beschäftigung mit Themen des Datenschutzes ein Mehrwert zu erwarten, zur Selbstinformation eignen sich die Materialien nach Meinung des Autors nur bedingt. Besonders Bilder und Fotostorys sind zwar anschaulich, können für eine ausführliche Behandlung von Fragen des Datenschutzes allerdings nur als Aufhänger dienen[7]. Im Rahmen der Begleitstudie von Jadin und Farthofer sind

[5] https://www.bvdnet.de/dsgzs.html Stand: 24.03.2015

[6] http://www.netkompass.at Stand: 24.03.2015

[7] Vgl. dazu http://www.netkompass.at/wp-content/uploads/2013/04/Kathrin-Gutenbrunner.jpg, http://www.netkompass.at/wp-content/uploads/2013/04/Schestauber-olivia.jpg und http://www.netkompass.at/wp-content/uploads/2013/04/cybermobing.jpg. Stand: 21.05.2015

die Medienkompetenzen und der Umgang mit Privatsphäre und Datenschutz bei den Schülern sehr unterschiedlich ausgeprägt und reicht von sehr freizügig bis reflektierend und überlegt. Ein Wissenstransfer auf ähnliche Anwendungen findet nicht statt, was die Frage offen lässt, ob die Jugendlichen die Medienkompetenz besitzen, oder sich nur an ein Nutzungsmuster gewöhnt haben. Ein weiteres Ergebnis ist die hohe Bedeutung von *Peer-to-Peer learning*, die sich bei der Durchführung des Projekts herausgestellt hat. Lernen von *Gleichaltrigen zu Gleichaltrigen* bedeutet, dass die Schüler voneinander lernen und ihr Wissen untereinander teilen. Besonders im Verhalten in sozialen Netzwerken und der Privatsphäre passen die Jugendlichen ihr Verhalten entsprechend im Freundeskreis erlebter Dinge an. Inhalte, die sie von Anderen nicht sehen wollen zeigen sie in der Regel auch nicht von sich. Sie entwickeln demnach anhand gemachter Erfahrungen ihre eigenen Strategien zum Datenschutz [JF14]. Bei der Bewältigung der in 1.1.1 genannten Aufgabe für die Bildungsinstitutionen sollte die Ausnutzung dieses positiven Effektes angestrebt werden, um die Wirkung der Aufklärungsarbeit zu erhöhen.

YOUNGDATA[8] ist ebenfalls ein Portal zur Information für Jugendliche bzw. Schüler. Es wurde initiiert von den Datenschutzbeauftragten des Bundes und der Länder. Hier werden Fakten und Informationen, aber auch Verhaltensvorschläge zu Themen wie Datenschutz, Facebook, Videoüberwachung und Informationsfreiheit bereitgestellt. Die Sammlung ist umfangreicher als die von *Netkompass* und die Aufmachung der Inhalte ist deutlich professioneller gestaltet, da hier nicht wie bei Netkompass die Ergebnisse von Schülerarbeiten präsentiert, sondern konkrete Informationen bereitgestellt werden. Die Beschäftigung mit dem Themenfeld soll demnach über die Materialien der Webseite erfolgen und nicht bei der Erstellung von Informationsmaterial. Dafür fehlen hier die Vorteile des Peer-to-Peer Lernens, was einen nicht unerheblichen Nachteil darstellt.

klicksafe[9] ist eine 2009 von der EU-Kommission gestartete Kampagne, welche die Medienkompetenz von Kindern und Jugendlichen im Umgang mit dem Internet verbessern soll. Dazu werden primär Materialien für dieses Publikum bereitgestellt, die allerdings auch für Eltern oder Lehrer geeignet sind, um die Zielgruppe möglichst umfangreich über Risiken und problematische Inhalte im Internet aufzuklären. Mögliche Risiken sind unter anderem Gewaltverherrlichung, Pornografie und Computerspiel- bzw. Internetsucht. Zu den Materialien zählen

[8] http://www.youngdata.de Stand: 24.03.2015
[9] http://klicksafe.de Stand: 21.05.2015

nicht nur Informationen und Verhaltenstipps zum Selbststudium auf den Internetseiten von *klicksafe*, sondern auch Broschüren für Eltern und Unterrichtsmaterialien. Für den Unterricht steht eine Fülle an Informationsmaterialien und Arbeitsblättern für ganze Unterrichtstunden bzw. -einheiten zur Verfügung, die mit methodisch-didaktischen Hinweisen versehen sind. Dabei wird auf einen Bezug zur Lebenswelt der Schüler geachtet. So werden z.B. Bild- und Urheberrechte beim Einsatz in Referaten oder privates Streamen von Videos thematisiert [KRF11].

Diese Projekte haben nach Berendt et al. [BDDP15] oft den Nachteil, dass ihre sinnvollen Aufrufe überwiegend nicht beachtet werden. Gründe dafür lassen sich nach deren Aussage in der Privacy-Forschung finden: viele der Materialien greifen zu kurz, denn die Abdeckung der gesamten Breite des Themenfeldes ist oft durch zu starke Fokussierung auf einzelne Aspekte nicht gewährleistet. Nach Berendt et al. ist die geschützte Privatsphäre bzw. Privacy nicht nur mit Blick auf soziale Aspekte zu betrachten, sondern auch auf institutionelle. Bei der sozialen Privacy liegt der Blick auf dem Schutz der Privatsphäre gegenüber den Mitmenschen, wie bspw. Mitschüler, Eltern oder Lehrer. Die gängigen Informations- und Aufklärungsmaterialien befassen sich dabei überwiegend mit der richtigen Konfiguration von Privacy-Settings in sozialen Netzwerken. Datenvermeidung und die Auswahl des Publikums für verschiedene Inhalte stehen im Vordergrund. Bei institutioneller Privacy geht es hingegen um den Schutz vor Überwachung durch den Staat und seine Geheimdienste, aber auch um die Datensammlung durch Medienkonzerne, wie Google und Facebook. In diesem Zusammenhang steht auch das Data Mining.

Eine von Berendt et al. [BDDP15] entworfene Unterrichtsreihe befasst sich hauptsächlich mit der institutionellen Privacy, speziell mit den Prinzipien und Folgen von Profilbildung durch Tracking und Datensammlung durch Internet-Großkonzerne für eine staatliche Ordnung. Die genannten Nachteile der Projekte und Initiativen treten hier ebenfalls auf. Die Kommentare einer Schülerin im Nachgang eben dieser Unterrichtsreihe bestärkt die oben angeführten Aussagen der Privacy-Forschung. Ihre Kritik bezieht sich auf die Orientierung der Inhalte an *Erwachsenen-Kriterien* [BDDP15, S. 53]. Das Mitteilungsbedürfnis ist stärker als die Angst vor theoretischen Auswirkungen auf das spätere Leben. Besonders die Fragen bzgl. der Folgen für die demokratische Ordnung und Werte werden von den Schülern zwar verstanden, Konsequenzen werden von ihnen daraus jedoch

trotzdem keine gezogen, da die direkte Betroffenheit für sie nicht erkennbar ist. Die realen Konsequenzen und die in der Reihe genannten Folgen sind für die Schüler nicht unmittelbar erkennbar und zudem zu unpersönlich, weshalb diese für sie sehr abstrakt wirken. Die behandelten Inhalte sind zwar sinnvoll und wichtig, aufgrund des fehlenden direkten Bezugs zur aktuellen Lebenswelt der Schüler entsteht nur ein geringer Kompetenzzuwachs.

Berendt et al. ziehen daher das Fazit, dass der Ansatz der Datensparsamkeit für die heutige Schülergeneration nicht die richtige Vorgehensweise zu sein scheint. Ein zu starker Fokus auf einen Aspekt von Privacy ist genauso wenig zielführend, wie die Ratschläge zur Datenvermeidung und bewussten Datenpreisgabe. Die bei der Datensammlung und -verarbeitung verwendeten Algorithmen arbeiten nicht nach kausalen Mustern, sodass die daraus gemachten Vorhersagen nicht den Vorstellungen der Nutzer entsprechen und die Appelle zur Datensparsamkeit widersprechen dem Mitteilungsbedürfnis der Anwender. Eine verantwortungsvoller Umgang mit seinen Daten muss deshalb unter anderem mit der Aufklärung über die verwendete Software einhergehen und der Erkenntnis, dass Privacy nicht nur reine Privatsache des Einzelnen ist, sondern im gleichen Maße politische Lösungen erfordert. Sie kommen zu dem Schluss, dass Verschlüsselung und Anonymisierung von Kommunikation zur Vermeidung von Identifikation der Anwender in den Mittelpunkt gerückt werden sollte.

Die im Rahmen dieser Arbeit zu erstellende Unterrichtsreihe soll sich zum einen an den gerade benannten Erkenntnissen orientieren und zum anderen kontextorientiert sein. Deshalb wird im Folgenden das Unterrichtskonzept *Informatik im Kontext* kurz vorgestellt. Dieses wurden nicht explizit für das Thema Datenschutz entwickelt, dennoch weisen einige bereits vorhandenen Unterrichtsreihen thematischen Bezügen dazu auf. Diese Reihen werden ebenfalls kurz erläutert, um später die Inhalte der neuen Reihe bestimmen zu können.

1.2 Das Projekt *Informatik im Kontext*

Informatik im Kontext (IniK) ist den Kontext-Projekten aus den Naturwissenschaften Chemie, Physik und Biologie nachempfunden und hat sich zur Aufgabe gemacht, Schüler für die Informatik zu begeistern. Durch die Behandlung von informatischen Themen und Fragestellungen innerhalb eines bestimmten Kontextes

wird versucht die Schüler in ihrer Lebenswelt abzuholen und damit die Inhalte des Informatikunterrichts interessanter zu gestalten. Initiiert wurde IniK von Bildungsverantwortlichen (vornehmlich Lehrer) in Berlin und Brandenburg im Rahmen des Modellversuchs SINUS (Steigerung der Effizienz des mathematisch-naturwissenschaftlichen Unterrichts), beziehungsweise dessen Weiterentwicklung SINUS-Transfer[10] und hat sich zu einem bundesweiten Projekt weiterentwickelt.

Dem Konzept von IniK liegen drei Prinzipien zu Grunde:

- Die Kontexte stammen aus der Lebenswelt der Schüler und haben eine Bedeutung für diese. Während des gesamten Unterrichtsverlaufs wird in diesem Kontext gearbeitet.
- Die Inhalte orientieren sich an den von der Gesellschaft für Informatik empfohlenen Bildungsstandards für den Informatikunterricht der Sekundarstufe I.
- Die verwendeten Methoden innerhalb der Unterrichtsreihe sollen sowohl schüleraktivierend und kooperativ, als auch abwechselnd sein.

Es besteht bereits eine Reihe von verschiedenen Unterrichtsentwürfen in diversen Entwicklungsstadien und zu unterschiedlichen Themenbereichen. So existieren unter anderem fertige und mehrfach getestete Unterrichtseinheiten zu *Chatbots und Sprachdialogsystemen*, sowie nur teilweise ausgearbeitete Entwürfe zu Themen wie *Filesharing* und *Soziale Netze*.

Viele der vorhandenen Kontexte haben einen mehr oder weniger starken Bezug zum Thema Datenschutz und Datensicherheit. So findet sich im Kontext *RFID* ein Abschnitt *Datenschutz und Recht*, der Schüler für Einsatz- und Missbrauchsmöglichkeiten bei der Nutzung von RFID sensibilisieren soll, der Kontext *Cybermobbing* thematisiert im *Planspiel Web 2.0* unter anderem den Umgang mit persönlichen Daten und Passwörtern. Aufgrund des starken thematischen Bezuges zum Datenschutz werden drei dieser Kontexte im Folgenden genauer betrachtet:

1. Die Reihe *E-Mail (nur?) für Dich*

   E-Mails sind ein zentraler Bestandteil der modernen Kommunikation, weshalb ein Kontext dazu naheliegend ist. 41 % der Jugendlichen kommunizieren mehrmals in der Woche per E-Mail. Allerdings haben das Chatten mit

[10] http://sinus-transfer.uni-bayreuth.de/ Stand: 01.05.2015

80 % und soziale Netzwerke mit 62 % im Jahr 2014 eine vergleichsweise deutliche höhere Bedeutung bei den Jugendlichen [FPR14, S. 26].

Die behandelten Fragestellungen und Themen der Unterrichtsreihe lassen sich gut aus Abbildung 1.1 ablesen. Die auf 20 Schulstunden ausgelegte

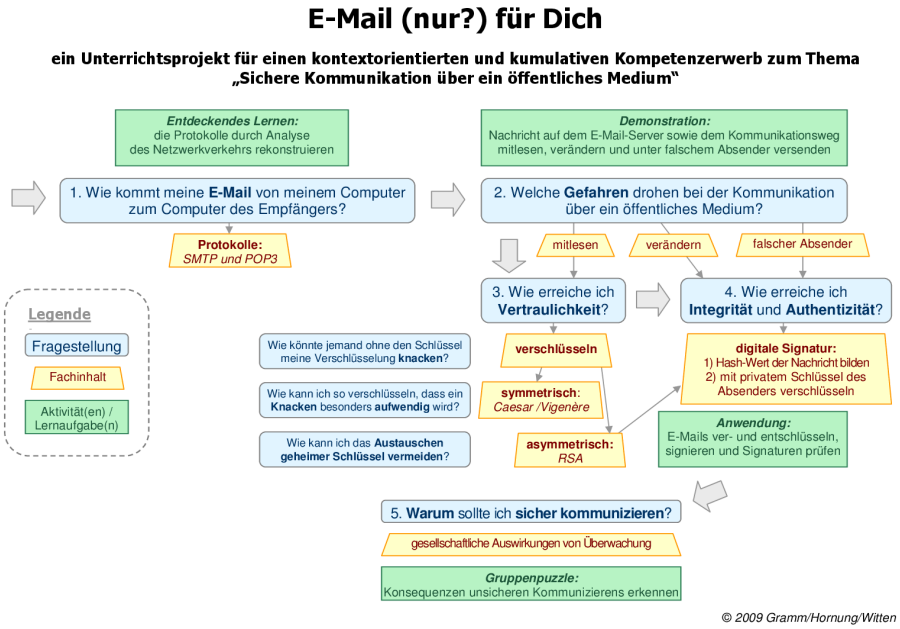

Abbildung 1.1 Überblick über die Unterrichtsreihe *E-Mail (nur?) für Dich* - Gramm/Hornung/Witten, 2009 [Ini]

Unterrichtsreihe beginnt mit dem Kennenlernen von Protokollen bei der Versendung von E-Mails, um die technischen Abläufe zu verstehen. Danach wird auf Gefahren bei der Kommunikation über öffentliche Medien eingegangen. Die Hälfte der angesetzten Zeit wird auf die Behandlung kryptographischer Verfahren mit dem Ziel verwendet, dass die Schüler in der Lage sind E-Mails zu ver- und entschlüsseln. Vor- und Nachteile verschiedener Verschlüsselungstechniken, sowie Angriffsmöglichkeiten werden genauso thematisiert, wie mathematische Grundlagen. Es folgt eine Behandlung von Authentizität, digitalen Signaturen und Zertifikaten. Zum Abschluss werden Gründe für eine sichere Kommunikation besprochen und die Risiken, die es entgegen der landläufigen Meinung *Ich habe doch*

nichts zu verbergen! gibt, die man bei der Kommunikation leicht außer Acht lassen kann. Die Schüler sollen über Gefahren der Kommunikation aufgeklärt werden.

2. Die Reihe *Planspiel Datenschutz*

   Das *Planspiel Datenschutz* behandelt die zentrale Fragestellung *Wer weiß was über mich im Internet?* und ist auf 7 bis 10 Unterrichtsstunden ausgelegt, deren Ablauf in Abbildung 1.2 dargestellt ist. Grundlage für das Planspiel ist

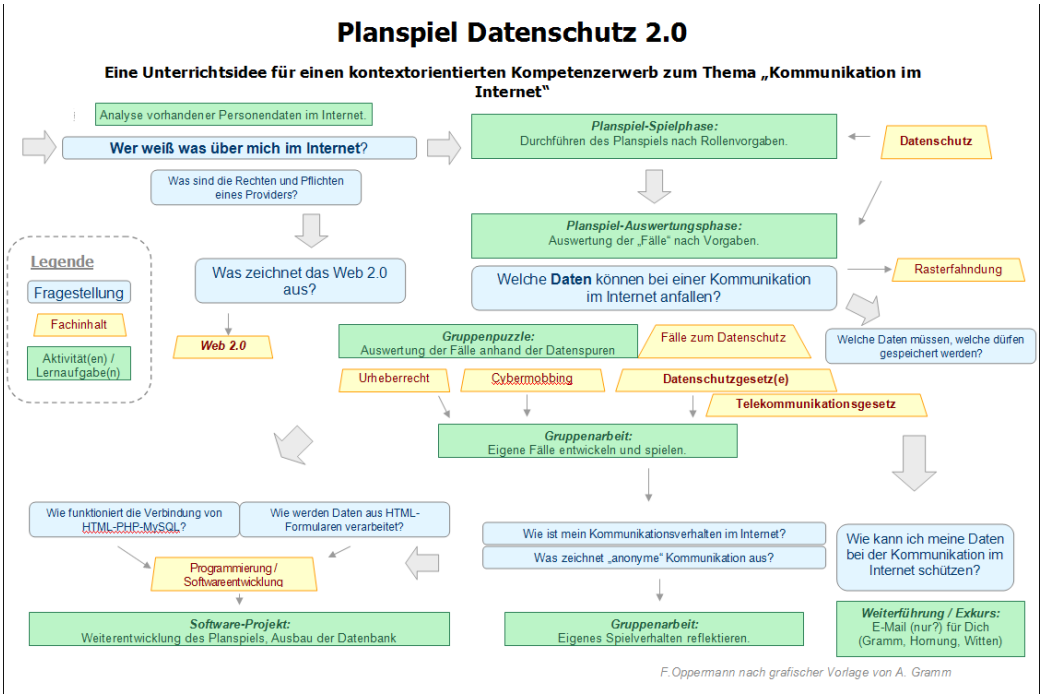

Abbildung 1.2 Überblick über die Unterrichtsreihe *Planspiel Datenschutz* - F. Oppermann/A. Gramm [Ini]

die Einrichtung eines fiktiven Providers durch den Lehrer, was sich mit Hilfe der bereitgestellten Materialien und des zur Verfügung gestellten Webspaces auf einem Server in Berlin einfach gestaltet. Die Klasse wird in verschiedene Gruppen aufgeteilt und jeder Schüler erhält eine Rollenbeschreibung für einen bestimmten Charakter in einer vorgegebenen Geschichten. In der ersten Phase, der *Spielphase* des Online-Spiels, handeln die Schüler nach den Vorgaben der Beschreibung und hinterlassen bei der Interaktion mit dem bereitgestellten Provider Spuren. In der nun folgenden *ersten Aus-*

wertungsphase untersuchen zwei Gruppen wechselseitig die Fälle einer anderen Gruppe. Dabei werden die Daten des Providers ausgewertet. Diese reichen von Blogs und Foreneinträgen, über gesehene Videos und Einträge in Chats. Die Schüler sehen die Handlungen im Netz unter einem anderen Blickwinkel und verfassen eine begründete Antwort auf die zu Beginn gegebene Fragestellung (*Wer soll warum den Praktikumsplatz erhalten?*, *Wer ist der Dieb des Camcorders?*). In der *zweiten Auswertungsphase* stellen die Ermittler den Protagonisten des Falls ihre Ergebnisse vor und diskutieren diese. Im Anschluss bereiten die beiden Gruppen, unter Berücksichtigung zur Verfügung gestellter Materialien und einer Internetrecherche, eine Vorstellung ihrer Fälle für den Rest der Klasse vor. Hier kommen unter anderem auch gesellschaftliche und rechtliche Fragestellungen mit ins Spiel. In der *Vernetzungsphase* können eigene Rollen und Fälle entwickelt werden, sowie weitergehende Fragestellungen behandelt werden wie z.B.: *Was ist der Sinn des Datenschutzgesetzes?*, *Was versteht man unter dem Recht auf informationelle Selbstbestimmung?* oder *Welche Rechte hat ein Bürger in Bezug auf Auskunft, Berichtigung und Löschung gespeicherter Daten?*. Im Anschluss können auch technische Aspekte, beispielsweise mit der Reihe *E-Mail (nur?) für dich*, aufgegriffen werden.

3. Die Reihe *Cybermobbing*

   Die Reihe *Cybermobbing* beinhaltet drei Unterrichtsentwürfe zu singulären Stunden. Zu jedem Entwurf gibt es eine Geschichte, bei der verschiedene Formen des Cybermobbings behandelt werden. Beim ersten Entwurf wird das anonyme Versenden von Nachrichten thematisiert, beim Zweiten die Erstellung und Verbreitung einer Fotomontage. Spezifische technische Aspekte, wie die Rückverfolgung einer SMS zu ihrem Urheber oder Möglichkeiten der Fotomontage, werden bei beiden Szenarien genauso wie rechtliche Fragen - unter anderem bzgl. AGBs oder dem Recht am eigenen Bild - betrachtet. Der dritte Entwurf ist ein analoges Planspiel. Beim *Planspiel Web 2.0* schlüpfen die Schüler in vorgegebene Rollen, wobei das Hinterlassen von Datenspuren hier bewusst mit Stift und Papier erfolgt.

   Gemeinsam haben alle drei die Betrachtung der Opfer und welche Möglichkeiten es für diese gibt sich zu wehren. Zudem werden ebenfalls die Intentionen der Täter analysiert und diskutiert. Ziel ist es, Schüler für die

Gefahren des Cybermobbings und mögliche Konsequenzen zu sensibilisieren. Darüber hinaus werden auch rechtliche Aspekte, wie die Bedeutung des Persönlichkeits- oder Urheberrechts thematisiert.

Im ersten Kapitel wurde zunächst der Stellenwert des Smartphones innerhalb der Lebenswelt von Schülern herausgestellt. Daran anschließend folgte eine Betrachtung des Datenschutzes und dessen Bedeutung. Schulen müssen sich dieser Thematik annehmen, um ihren Bildungsauftrag gerecht zu werden. Die Bemühungen verschiedener Initiativen reichen nicht aus, das geforderte werteorientierte Bewusstsein für die digitalen Zusammenhänge zu schaffen. Die Vorstellung der vorhandenen Kontexte zeigt, dass der Lebensweltbezug durch technische bzw. gesellschaftliche Entwicklungen in Teilen verloren gehen kann und daher eine Anpassung der vorhandenen Kontexte oder die Neuschaffung einer neuen Unterrichtsreihe notwendig sind.

Kapitel 2

Smartphone-Applikationen

Das Smartphone spielt bei der Aufklärung von Jugendlichen über den Datenschutz eine nicht unwesentliche Rolle. Es ist ein ständiger Begleiter und sehr persönlicher Gegenstand und Kontrolle des Nutzungsverhaltens, bzgl. der Häufigkeit und der Inhalte, durch die Eltern findet kaum statt. Die vorhandenen Schutzmaßnahmen sind nicht ausgereift bzw. werden nicht angenommen. Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. [1] [KS14] sieht in diesem Zusammenhang eine Sensibilisierung der Jugend, die so früh wie möglich stattfinden sollte, als unbedingt notwendig an. Gerade mit Blick auf die *Bring your own device* Praktik vieler Betriebe, ist das Erlernen eines verantwortungsvollen Umgangs mit mobilen Geräten von entscheidender Bedeutung. Der Wert von personenbezogenen Daten muss bewusst und der Umgang mit den Medien kritischer werden.

Die Nutzungsmöglichkeiten von Smartphones lassen sich durch Applikationen (Apps) um viele Funktionen erweitern, besonders durch die hohe Verfügbarkeit des mobilen Internets. Laut der JIM-Studie [FPR14] installieren Jugendliche zusätzlich zu den vorinstallierten Programmen im Schnitt weitere 18 Applikationen, die meisten davon sind kostenlos. Auf 94 % der Smartphones ist *WhatsApp* zu finden (+25 PP im Vegleich zum Vorjahr) und hat mittlerweile sogar *Facebook* überholt. *WhatsApp* ersetzt aufgrund seiner Funktionalität und der geringeren

[1] Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. wurde 1989 mit dem Ziel gegründet, die beruflichen Interessen der betrieblichen und behördlichen Datenschutzbeauftragten zu unterstützen

Kosten[2] immer mehr die klassische SMS. Die Sicherheit ihrer Daten schätzen gerade die Jüngeren am sichersten ein, die Älteren haben eine etwas höhere Sensibilität entwickelt und die Gruppe derer, die ihre Daten als eher sicher ansehen, ist insgesamt um zehn PP, auf 46 % gefallen.

Im Folgenden werden erst Grundlagen zur Funktionsweise von Smartphones und Apps erklärt und darauf aufbauend mögliche Angriffsvektoren aufgezeigt. Abschließend werden Schutzmaßnahmen gegenüber diesen Angriffen vorgestellt. Der Schwerpunkt liegt auf dem Betriebssystem *Android*, denn von den im Monat Januar des Jahres 2015 in Deutschland abgesetzten Smartphones hat Android einen Marktanteil von 72,7 %[3]. Der Anteil des zweitplatzierten Betriebssystems iOS von Apple hingegen beläuft sich nur auf 17,4 %.

2.1 Technische Grundlagen

Verantwortungsvoller Umgang setzt ein grundlegendes Verständnis der technischen Gegebenheiten voraus. Aus diesem Grund wird nun auf die Funktionsweise von Android und seinen Apps eingegangen, im Zusammenhang mit den zu entwickelnden Materialien allerdings allgemein gehalten.

Nach den von Hoog in [Hoo12, Kapitel 1] beschriebenen *Android Features* gehört zu den wichtigsten Eigenschaften des Betriebssystems die Auslegung auf einen jederzeit möglichen Online-Betrieb. Die Bedienung erfolgt je nach Gerät per Touchscreen oder integrierter Tastatur, sowie über Tasten für das Ein-/Ausschalten des Gerätes oder die Lautstärkeregelung. Ein weiteres dieser Features ist das Speichern von Daten auf dem internen Flash-Speicher und externen SD-Karten, die den Speicherplatz der Geräte erhöhen. Weitere Kernkomponenten von Smartphones sind nach [Hoo12, Abschnitt 2.2] Schnittstellen für GPS[4], drahtlose Netzwerke, Kamera und Mikrofon, sowie Bewegungssensoren.

Die Funktionalität des Smartphones wird über Apps erweitert, wobei dies überwiegend über eine vorinstallierte *Market App* den *Google Play Store* erfolgt.

[2] *WhatsApp*-Nachrichten werden über die Internetverbindung gesendet, daher fallen nur die monatlichen Kosten der Datenflatrate, sowie ein geringer Jahresbetrag an.

[3] http://de.statista.com/statistik/daten/studie/256790/umfrage/marktanteile-von-android-und-ios-am-smartphone-absatz-in-deutschland Stand: 03.05.2015

[4] Global Positioning System

Dies ist die offizielle und zu einem gewissen Grad kontrollierte Bezugsquelle der Firma Google. Darüber hinaus existieren weitere Marktplätze, die aufgrund fehlender Kontrollen mehr oder minder vertrauenswürdige Inhalte bereitstellen. Der *Amazon Appstore* und *Fireplace* sind zwei dieser Alternativen. Um eine App aus dem Play Store beziehen zu können, muss sich der Nutzer mit einen Gmail-Account bei dem Marktplatz anmelden. Danach kann er aus kostenlosen und kostenpflichtigen Angeboten auswählen. Vor der Installation auf seinem Smartphone werden dem Nutzer unter anderem Informationen über das Produkt gezeigt: eine Beschreibung der Funktionalität, Nutzerbewertungen der App, Anzahl erfolgter Downloads und Nutzerkommentare. Auf die bei der Installation eingeforderten Rechte wird im Laufe dieses Abschnitts explizit eingegangen. Nach Download und Installation[5] stehen das Programm und seine Funktionen bis zu seiner Deinstallation auf dem Gerät zur Verfügung.

Die Schöpfer des Betriebssystems, die im Jahr 2003 gegründete Firma Android Inc., wurde samt des entwickelten Systems im Juli 2005 von der Firma Google übernommen. Google gibt sich selbst folgenden Auftrag[6]:

> *Das Ziel von Google ist es, die Informationen der Welt zu organisieren und für alle zu jeder Zeit zugänglich und nutzbar zu machen.*

Dieser Hintergrund ist für die Bemühungen des Datenschutzes für sich bereits problematisch, denn das primär durch Werbung finanzierte Geschäftsmodell des Unternehmens verlangt nach möglichst vielen Daten der Nutzer. Durch diese Daten werden die Werbemaßnahmen personalisierter und damit erfolgreicher.

Der Aufbau des Systems ist in Abb. 2.1 veranschaulicht. Die Basis von Android stellt der Linux-Kernel dar, der die Gerätetreiber enthält und die Verwaltung von Energieverbrauch, Speicher und Prozessen übernimmt. Die Laufzeit-Umgebung wird von der DVM (*Dalvik Virtual Machine*) übernommen. Für jede Anwendung wird in einem eigenen Betriebssystemprozess eine separate DVM gestartet, innerhalb der die Anwendung läuft. Dies ist ressourcenintensiv, aber sinnvoll im Bezug auf die Sicherheit. Die Bibliotheken stellen die für die Ausführung notwendigen Funktionalitäten (Grafikbibliotheken, Oberflächenkomponenten, Webzugriff etc.) zur Verfügung. Der Anwendungsrahmen erlaubt den

[5] Auf *mobilen Code* (Programme die nicht auf dem eigenen Gerät installiert, sondern nur ausgeführt werden) wird in dieser Arbeit keinen Bezug genommen. Bei Eckert [Eck13, 2.7.1] lassen sich Informationen über das Bedrohungspotential finden.

[6] https://www.google.de/intl/de/about Stand: 07.05.2015

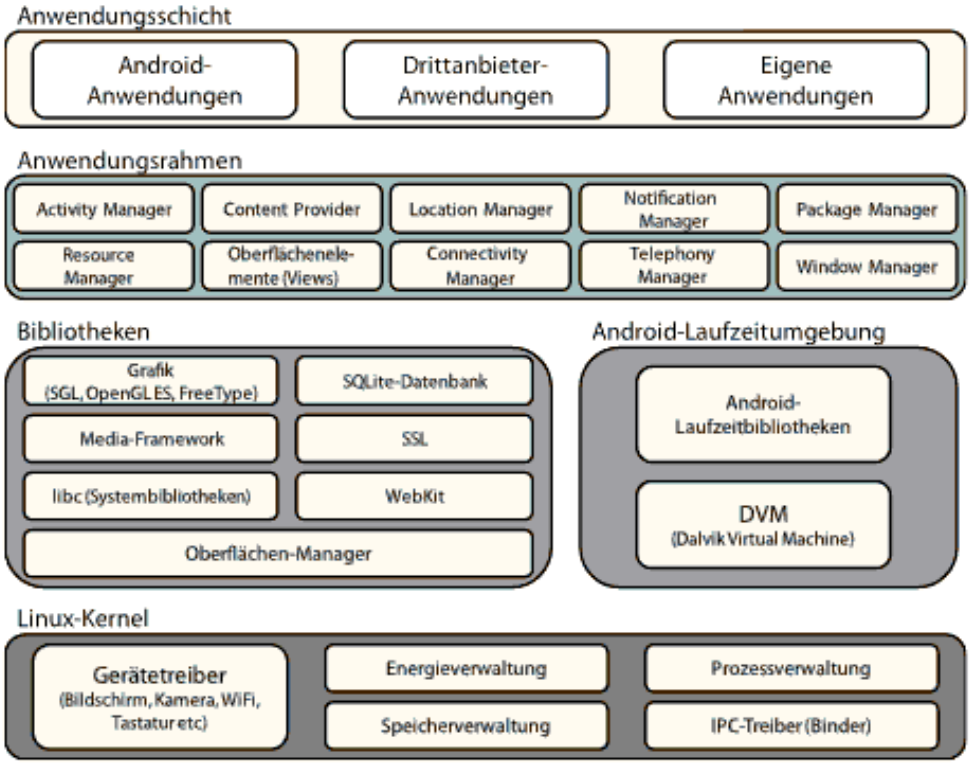

Abbildung 2.1 Die Android-Systemarchitektur - [BP14, Kapitel 2]

Zugriff auf Hardwarekomponenten seitens der Anwendungen und greift selbst auf die Bibliotheken zu. Der Nutzer interagiert mit der Anwendung mit Hilfe der Anwendungsschicht, in der auch die Anwendungen untereinander kommunizieren bzw. auf die Programmierstellen der darunterliegenden Ebenen zugreifen [BP14, Kapitel 2].

Durch diese Architektur ist das *Sandbox-Prinzip*, sowie das Berechtigungssystem von Android möglich [BP14, Kapitel 3]: Eine Sandbox ist eine DVM mit eingeschränkten Funktionen. Alle Daten der Applikation sind dabei vor Zugriff von anderen Anwendungen geschützt und jede App hat ihren eigenen Speicher, sodass eine fehlerhaft ausgeführte Anwendung keinen Einfluss auf die Funktion der Übrigen hat. Dadurch wird ebenfalls ein direkter Zugriff auf das Betriebssystem verhindert. Dabei nutzt Android das Berechtigungssystem von Linux: auf Betriebssystemebene wird jeder Anwendung ein eigener Benutzer zugeordnet, der beim Nutzen der App in einem eigenen Prozess startet. Diese Prozesse sind

dabei vor Zugriff nach außen geschützt und eine Applikation kann die Sandbox nur durch explizite Erteilung von Berechtigungen verlassen. Um bspw. eine Verbindung mit dem Internet aufzubauen sind der Zugriff auf Systemfunktionen bzw. Ressourcen außerhalb der Sandbox notwendig. Bei der Installation werden im Android-Manifest der Anwendung hinterlegte Berechtigungen angefordert, sodass die App bei Bedarf kontrolliert auf Funktionen außerhalb der Sandbox zugreifen kann. Laut [BP14, S. 35] gibt es über 100 unterschiedliche Berechtigungen.

Apps fordern demnach spezifische Zugriffsrechte, um ihre Funktionen ausführen zu können. Diese bestimmen den Umfang des Zugriffs auf Informationen und die Hardware. Diese Praxis erlaubt den Apps allerdings mit denen ihnen zugestandenen Rechten Aktionen auszuführen, ohne dass der Besitzer davon Kenntnis haben muss [PBP14, S.8-10]. Die Rechtevergabe ist demnach allgemeingültig und nicht an die aktive Nutzung der Applikation geknüpft. Diese Zugriffsvergabe hat im Gegenzug den Vorteil, dass der Besitzer nur im begrenzten Rahmen seiner Soft- und Hardware Schaden zufügen kann.

Durch *Rooten* ist es möglich viele dieser Beschränkungen aufzuheben und vollständige Administratorrechte zu erhalten. Neben Änderungen am System kann auch die Hardware beeinflusst werden. Dies kann sowohl zu gewollten Effekten, als auch Schäden am Gerät führen ([PBP14]. Da dies in der Regel zu Garantieverlust führt, ist vom Rooten abzuraten. Dieses Verfahren spielt allerdings bei den nun folgenden Angriffsvektoren eine Rolle.

2.2 Gefahren bei der Smartphone Nutzung

In allen Lebensbereichen wird das Smartphone verstärkt eingesetzt, da es fast überall genutzt werden kann und leicht mitzuführen ist. Seine vielseitigen Einsatzmöglichkeiten beschränken sich nicht nur auf Telefonie und Nachrichtenaustausch, sondern ermöglichen bspw. die Nutzung als Kalender, Notizbuch, Musik- und Video-Player. Durch die Vielzahl an Ansatzpunkten für einen Angriff, wird es vermehrt zum Zielobjekt eben dieser. Diese können der Spionage oder dem Identitätsdiebstahl, aber auch dem Tracking und Erstellen von Nutzerprofilen dienen. Der Einsatz im Unternehmensumfeld eröffnet darüber hinaus weitere Angriffsgründe [PBP14, S. 7]. *Kaspersky Lab* hat mehr als zehn Millionen potentiell schädliche Apps in offiziellen und inoffiziellen App-Marktplätzen ausgemacht.

99 % zielen auf das Betriebssystem Android ab und verbreiten verschiedene Formen von Schadcode [DuD14]. Die Handhabung der Zertifikate bei Android ist dabei kein Sicherheitsmerkmal. Jede Anwendung muss zwar signiert werden, das dazu notwendige Zertifikat kann jeder Entwickler allerdings selbst erstellen und muss nicht beglaubigt sein. Die Signaturen dienen nicht den Nutzern zur Überprüfung der Seriosität der Hersteller, sondern dem Betriebssystem. Wenn die vergebenen Berechtigungen der Apps es erlauben können Anwendungen mit gleichen Zertifikaten sich eine Sandbox teilen, da anzunehmen ist, dass sie vom selben Anbieter entwickelt wurden.

Das deutsche *Bundesamt für Sicherheit in der Informationstechnik* (BSI) hat in seinem Grundschutz-Katalog[7] für sogenannte *Bausteine* die *Gefährdungslage* und *Maßnahmenempfehlungen* aufgelistet. Die Bausteine *B 3.404 Mobiltelefon* und *B 3.405 Smartphones, Tablets und PDAs* geben eine umfassende Liste möglicher Gefahren, die bei der Nutzung der mobilen Geräte. Der Katalog dient in erster Linie als Vorgabe für Behörden und Empfehlung für die Wirtschaft, bietet dem privaten Nutzer allerdings auch nützliche Hinweise. Die Inhalte sind in der Rubrik *BSI für Bürger* für durchschnittlich Versierte verständlich aufgearbeitet.

Petersen et al. [PBP14, S. 8-10] stellen einige der unterschiedliche Gefahren und Angriffsmöglichkeiten auf die mobilen Geräte vor:

Software wird von Menschen programmiert wird und ist deshalb nie frei von Fehlern. Beliebte und weit verbreitete Software rückt aus diesem Grund schnell in den Blick von Kriminellen, die deren Programmierung nach Lücken untersucht und für Angriffe nutzt. Noch funktionstüchtige Geräte können dabei durch die fehlende Updates[8] in das Visier der Angreifer geraten, da aufgedeckte Lücken nicht geschlossen werden. Nicht weiter vom Hersteller betreute und damit aktualisierte Software ist in erhöhtem Maße gefährdet Sicherheitsmängel aufzuweisen. Darüber hinaus müssen die Nutzer nach Eckert [Eck13, S. 89 f.] der Qualitätskontrolle der Marktplätze vertrauen. Besonders Apps für Android sind durch die mangelhafte Kontrolle erhebliche Sicherheitsrisiken gegeben. Laut Hoog [Hoo12,

[7] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html Stand: 20.05.2015

[8] Durch regelmäßige Pflege und Updates können Sicherheitsrisiken verringert werden. Wegen den anfallenden Personalkosten wird ein Produkt allerdings nur eine gewissen Zeit diese Behandlung zu Teil, denn nur mit neuen Geräten und Software verdienen die Hersteller Geld. Aus diesem Grund wird der Support von Altgeräten in der Regel nur zeitlich begrenzt unterstützt.

Abschnitt 1.6] nutzt Google die Bewertungen der Nutzer als Haupt-Qualitätsmerkmal einer App. Die Vergabe von Rechten soll dabei für die nötige Transparenz sorgen. Durch die Rechteverwaltung können theoretisch gespeicherte Daten, persönliche Inhalte wie Bilder oder identifizierende Informationen über das Gerät von Apps unbemerkt an einen Server gesendet werden. Ein Angreifer kann durch einen *Root-Exploit*, eine Schwachstelle im Betriebssystem, das Sicherheitssystem von Android umgehen und mit dem Rooten des Geräts Schaden verursachen. Neben physischen Schäden kann auf diesem Weg unbemerkt Schadsoftware wie Malware und Spionage- Apps installiert werden. Diese können ebenfalls durch einen Download des Nutzers auf das Smartphone gelangen. In der unüberschaubaren Menge von angebotenen Apps verlangen einige Applikationen mehr Zugriffsrechte als sie für ihren eigentlichen Zweck benötigen. Neben Datendiebstahl können dies auch vom PC bekannte Schadsoftware, wie ein Trojaner sein.

Die meisten Apps kommunizieren mit dem Internet. Neben Updates und Nachrichtenkommunikation kann dies auch störende Werbung und ungewollte Übertragung von Daten sein. Dieses Übertragen von ausgespähten Informationen ist für den normalen Nutzer nicht erkennbar. Im schlimmsten Fall kann ein Angreifer durch Schadsoftware die vollständige Kontrolle über ein Gerät erlangen. Neben den Schwachstellen in der Software kann das Kommunizieren über unsichere Verbindungen wie öffentliche WLAN-Hotspots eine Angriffsfläche bieten, weil die Kommunikation über unverschlüsselte Verbindungen mitgelesen werden kann. Im Falle eines durch einen *Man-in-the-middle-Angriffs* hat der Angreifer Zugriff auf alle versendeten Daten über dieses Netz. Durch Identitätsdiebstahl kann im Namen eines unwissenden Benutzers gesetzwidrige Handlung vollzogen werden. Eine weitere Möglichkeit Kontrolle über ein fremdes Smartphone zu gelangen ist der Diebstahl oder das Finden des Geräts nach Verlust. Ziele sind hier unter anderem das Ausspähen von Passwörtern und die E-Mail- bzw. Chat-Korrespondenz. Firmendaten sind ein weiteres beliebtes Ziel von Angriffen und eine Art der Wirtschaftsspionage.

Die Verbreitung von QR-Codes eröffnet Angreifern eine weitere Option. Der Inhalt des auf Werbetafeln und in Zeitungen angebrachten Grafiken ist für das menschliche Auge nicht ersichtlich. Anstatt der suggerierten Weiterleitung auf eine Internetadresse mit weiteren Informationen über ein Produkt oder einer Fir-

ma, kann der Code auf infizierte Webseiten verweisen, die Schadsoftware installieren oder schlimmstenfalls irreversible Schäden am Gerät verursachen.

Die Vielzahl an möglichen Angriffsvektoren deutet das Ausmaß der Bedrohungslage für Smartphones und andere mobile Geräte an. Im folgenden Abschnitt sollen die Zugriffsrechten der Applikationen genauer betrachtet werden. Dazu wird exemplarisch die Anwendungen *WhatsApp*, aufgrund seiner im Beginn dieses Kapitels erwähnten Bedeutung für die Kommunikation der Schüler, auf ihre eingeforderten Rechte untersucht und deren Notwendigkeit für die Funktionalität überprüft. Es soll geklärt werden, ob diese Rechte für die Funktion der Anwendungen nötig sind und welches Gefahrenpotenzial für den Nutzer besteht.

2.3 Rechte von Apps

Nach Eckert [Eck13, S. 91 f.] ist Googles Philosophie für Android, dass den Entwicklern und deren Apps nicht vertraut werden kann. Daher begründet sich die bereits beschriebene Rechtevergabe. Die speziellen Schnittstellen zum System müssen bei der Installation eingefordert werden und durch den Nutzer bestätigt werden. Dies erzeugt ein gewisses Maß an Transparenz, wälzt aber die Verantwortung dabei auf den Benutzer ab. Ein angemessenes Problembewusstsein seitens der Konsumenten ist daher notwendig.

Exemplarisch werden nun die geforderten Zugriffsrechte von WhatsApp betrachtet. Die Messenger App erfreut sich nicht nur bei Jugendlichen sehr großer Beliebtheit, über 1 Milliarde Downloads kann die Anwendung verzeichnen. Ihre Funktionalität (Senden von Texten, Sprachnachrichten, Bildern, Videos oder Gruppenchats) verlangen Zugriff auf diverse Schnittstellen des Systems. Die bei Installation verlangten Zugriffsrechte im Google Play Store lauten:

- *In App Käufe*: Google Play-Rechnungsdienst
- *Geräte und App Verlauf*: ausgeführte Anwendungen abrufen
- *Identität*: Bekannte Konten erkennen, Kontenliste verwalten
- *Kontakte*: Kontaktdaten lesen und schreiben
- *Standort*: Allgemeiner (netzwerkbasierter) und genauer (GPS) Standort

- *SMS*: SMS empfangen und senden
- *Fotos/Medien/Dateien*: SD Karteninhalte bearbeiten oder löschen
- *Kamera*: Fotos und Videos aufnehmen
- *Mikrofon*: Audio aufnehmen
- *WLAN-Verbindungsinformationen*: WLAN-Status anzeigen
- *Geräte-ID & Anrufinformatonen*: Telefonstatus und Identität lesen
- *Sonstiges*: Als Konto-Authentifizierer agieren, Start automatisch starten, Sticky-Broadcast senden, Schlafmodus verhindern, Netzwerkstatus anzeigen, Shortcut installieren, Authentifizierungsberechtigungen für Konto verwenden, Shortcuts deinstallieren, Audioeinstellungen ändern, Google-Servicekonfiguration lesen, Sync-Einstellungen schreiben, Globale Systemeinstellungen ändern, vollständiger Internetzugriff, Bluetooth-Verbindungen erstellen, WLAN-Status ändern, Sync-Einstellungen lesen, Vibrationsfunktion steuern

Aus dieser Auflistung ist das Ausmaß an erforderlichen Berechtigungen erkennbar und die Tatsache, dass sie für den Verbraucher nicht unbedingt ersichtlich sind. Dazu gehören bspw. die Bedeutung von *Sticky-Broadcasts* oder *Sync-Einstellungen*. Fest steht, dass die Angaben bei der Installation bzw. allgemein bei den Informationen über die installierten Anwendungen auf dem Smartphone unpräzise sind, da die Zweckmäßigkeit der Rechte nicht explizit genannt wird und daher ist es nicht exakt nachvollziehbar für was eine App ihre Rechte tatsächlich nutzt. Ob dies *WhatsApp* zur *Superwanze* macht, war unter anderem Thema in einem Artikel der Westdeutsche Allgemeine Zeitung[9] vom Februar 2014, die vor den Gefahren der App warnt. Als Begründung dieses Vorwurfs werden unter anderem die umfangreichen Rechte der App angeführt. Ein Autor von *GIGA APPLE* unterstellt dem Artikel hingegen Panikmache[10]. Ein Autor[11] von *mimikama*,

[9] http://www.derwesten.de/staedte/hohenlimburg/jeder-vierte-schleppt-superwanze-mit-sich-id8973421.html Stand: 17.05.2015

[10] http://www.giga.de/downloads/WhatsApp-fuer-iphone/news/super-wanze-WhatsApp-man-kann-es-auch-uebertreiben/?PageSpeed=noscript Stand: 17.05.2015

[11] http://www.mimikama.at/allgemein/WhatsApp-die-superwanze-kein-fake/ Stand: 17.05.2015

ein Verein zur Aufklärung über Internetmissbrauch, geht im Zuge dieser Diskussion auf die vergebenen Rechte ein und findet für jede eine Daseinsberechtigung für jede dieser Rechte bzgl. der Funktionen von *WhatsApp*. Gerade mit Blick auf die Kommunikationsabwicklung über amerikanische Server lässt sich keine hundertprozentige Gewissheit erlangen, die Verwendung der Applikation als Wanze scheint allerdings äußerst unwahrscheinlich. Weitere Aufmerksamkeit erlangte die App im April 2015 durch mögliche lokale Speicherung von Gesprächen beim Telefonieren mit *WhatsApp*. Eine genauere Betrachtung lässt sich ebenfalls bei mimikama[12] finden. Hier werden die unterschiedlichen Rechtsauffassungen in den Vereinigten Staaten und Deutschland deutlich: Das Speichern lokaler Daten stellt eine Straftat nach § 201 des Strafgesetzbuches dar, auch wenn dies ohne Vorsatz durch den Nutzer geschieht. Im Rahmen des Themenschwerpunktes zu *WhatsApp* in dem Magazin *c't* berichten die Autoren Eikenberg und Schmidt [ES15] über die angewendete Verschlüsselung bei der App. Durch öffentlichen Druck hat *WhatsApp* eine Ende-zu-Ende-Verschlüsselung eingeführt, welche die Nachrichten ausschließlich Sender und Empfänger zugänglich machen. Problematisch ist allerdings die inkonsistente Handhabung seitens *WhatsApp*: Es ist für den Anwender nicht ersichtlich, wann diese Verschlüsselung angewendet wird, denn der Betreiber kann theoretisch jederzeit und unbemerkt auf unverschlüsselte Kommunikation umstellen und da den Inhalt der Nachrichten mitlesen. Die im Februar 2015 von *heise Security* vorgestellte Möglichkeit[13] die Onlinezeiten von Nutzern wegen fehlerhafter Sicherheitseinstellungen mit kostenlosen Programmen aufzeichnen zu können, rundet das negative Bild von *WhatsApp* bzgl. des Datenschutzes ab.

Die Handhabung des Datenschutzes seitens *WhatsApp* ist besonders wegen der umfangreich eingeforderten Rechte äußerst bedenklich. Der folgende Abschnitt soll Maßnahmen aufzeigen, die der Nutzer zum Schutz seiner Daten ergreifen kann.

[12] http://www.mimikama.at/allgemein/speichert-whatsapp-seine-calls-lokal-ab/ Stand: 17.05.2015

[13] http://www.heise.de/security/meldung/WhatsSpy-Beliebige-WhatsApp-Nutzer-rund-um-die-Uhr-ueberwachen-2543968.html Stand: 17.05.2015

2.4 Schutzmaßnahmen

Zu einigen der in Abschnitt 2.2 genannten Angriffsmöglichkeiten sollen nun mögliche Schutzmaßnahmen vorgestellt und bewertet werden. Hierbei stehen die Maßnahmen der Eigentümer zum Selbstdatenschutz im Vordergrund, denn beispielsweise ein Unternehmen zur Fortführung seines Supports zu verpflichten, ist nicht möglich.

Nach Hoog [Hoo12, Abschnitt 1.6] kann Google schadhafte Apps nicht nur aus dem Marktplatz entfernen, sondern auch von den Android-Geräten selbst[14]. Dennoch sollten Anwender aufmerksam sein. Zum einen helfen die Aktualisierung von Betriebssystem und Anwendungssoftware durch den Hersteller geschlossene Lücken auf dem eigenen Gerät ebenfalls zu schließen, zum anderen können Virenschutzprogramme vor Schadcode schützen. Das *AV-TEST Institut*, unabhängiger Anbieter von Services im Bereich IT-Sicherheit und Antiviren-Forschung, führt eine stetig aktualisierte Liste[15] von zuverlässigen Antiviren-Programmen für Android. Auf der Webpräsenz der Heise Medien GmbH & Co. KG [16] findet sich ebenfalls eine solche Liste. Dass deren Nutzen allerdings nur begrenzt ist, stellt Mike Kuketz[17] in seinem Blog-Eintrag über Antivirus-Apps für Android fest. Des Weiteren sind Rezensionen über Anwendungen - bspw. durch *CHIP* oder *heise Security* - als Qualitätsmerkmal aussagekräftiger, als die Anzahl der Downloads. Hier wird in der Regel auch ein kritischer Blick auf die geforderten Rechte geworfen. Der interessierte Nutzer kann allerdings vor dem Download einer App selbst abwägen, ob das Ausmaß der Rechte für den Einsatz der Anwendung notwendig ist, unter der Voraussetzung, das er diese versteht.

Auf Rooten sollte grundsätzlich verzichtet werden, denn die dadurch gewonnenen Vorteile bieten ihrerseits Angriffsfläche für weitertere Angriffe und bedeuteten in der Regel Garantieverlust. Darüber hinaus verletzt das Verändern von Software in den meisten Fällen auch das Urheberrecht der Entwickler (vgl. hierzu

[14] Im Juni 2010 wurde eine App auf diese Weise gelöscht, die weitere Apps herunterladen und installieren konnte.

[15] http://www.av-test.org/de/antivirus/mobilgeraete/ Stand: 17.05.2015

[16] http://www.heise.de/download/android/sicherheit/virenscanner-50284301183/ Stand: 17.05.2015

[17] http://www.kuketz-WhatsApp.de/antivirus-apps-fuer-android-sinnvoll-oder-nutzlos/ Stand: 23.05.2015. Kuketz ist Lehrbeauftragter an der dualen Hochschule Karlsruhe im Bereich IT-Sicherheit und freier Referent für das Landesmedienzentrum Baden-Württemberg.

[BRRR13]). Bei Heise gibt es darüber hinaus noch weitere, bewertete Sicherheits-Software, dazu zählen Anwendungen zur Analyse und Passwortverwaltung oder Firewalls, sowie zur Verschlüsselung der Daten.

Für alle Gefährdungen gilt, dass ein Großteil durch eine entsprechende Aufklärung und Bewusstseinsschaffung vermieden werden können, da durch unwissendes und unbedarftes Handeln viele Angriffe erst möglich gemacht werden. Folien[18] einer Präsentation von Helmut Eiermann, Mitarbeiters des Datenschutzbeauftragten von Rheinland-Pfalz, zu Datenschutzeinstellungen bei Smartphones zeigen, wie durch simple Änderungen von Einstellungen die Sicherheit von Nutzerdaten verstärkt werden kann.

Effektives Mittel zum Schutz der Daten auf dem Smartphone, sowie der Kommunikation bietet Verschlüsselung bzw. der Einsatz von Applikationen, die eine verschlüsselte Kommunikation gewährleisten. Hierbei gibt es jedoch Qualitative Unterschiede. So schützt eine Transportverschlüsselung zwar vor Lauschangriffen innerhalb eines Netzwerkes, gewährleistet hingegen nicht, dass der App-Anbieter die Nachricht mitliest oder auf seinen Servern speichert. Dagegen hilft nur eine Ende-zu-Ende-Verschlüsselung.

2.5 Zusammenfassung

Die ständige Verfügbarkeit und Vielzahl an Einsatzmöglichkeiten eines Smartphones, sowie eine dauerhafte Verbindung mit dem Internet bergen ein hohes Gefährdungspotenzial bei leichtfertiger Nutzung. Besonders die Nutzung unbekannter drahtloser Netzwerke ist mit Risiken behaftet, die zu Teilen durch die installierten Apps hervorgerufen werden. Die aus Sicherheitsgründen eingeführte Rechtevergabe kann bei unsachgemäßer Handhabung oder Befall durch Schadcode zur Preisgabe vieler Informationen führen. Die Handhabung ist für einen Otto-Normal-Verbraucher aufgrund mangelnden Verständnisses dieser Rechte erheblich erschwert. Persönliche Daten geben bereits viele Anwender freiwillig heraus (in sozialen Netzwerken bspw.). Neben den nicht abzusehenden, langfristigen Konsequenzen für die Gesellschaft sind materielle Schäden auf privater Ebene (Verlust des Gerätes, finanzielle Kosten), sowie innerhalb des Berufsumfeldes nicht zu unterschätzen. Der Verlust von Firmendaten kann nicht nur Anse-

[18] http://www.youngdata.de/fileadmin/youngdata/HM_smartphones/00_seiteninhalt/dateien/Datenschutzeinstellungen_bei_Smartphones_Android.pdf Stand: 17.05.2015

hensverlust beim Kunden, sondern auch Wettbewerbsnachteile durch Spionage seitens der Konkurrenz bedeuten. Welche Entwicklungen eine Gesellschaft nehmen kann, zeigt die gesetzlich verordnete Überwachung[19] der mobilen Geräte von Minderjährigen durch ihre Eltern in Südkorea. Grundlegende Kenntnisse der Funktionsweise der Geräte und der Anwendungen sind elementar für ein Verständnis von und der Teilnahme an Diskussionen über den Datenschutz, der im Alltag unserer Gesellschaft eine immer stärker werdende Bedeutung einnimmt. Beispiel dafür sind die kontroversen Sichtweisen innerhalb der Diskussion um *WhatsApp*, die sich für den Verbraucher nur nachvollziehen lassen, wenn er entsprechende Kompetenzen erworben hat. Selbiges gilt für die Schutzmaßnahmen seiner Privatsphäre. Die breite Palette an zur Verfügung stehenden Apps lässt sich nur mit ausreichendem Wissen bewerten und einsetzen. Andererseits wird immer ein gewisses Maß an Vertrauen gegenüber der bewertenden Instanzen bzw. Experten geben, welches allerdings nicht blind sei darf. Ein Grundniveau an Sicherheit lässt sich bereits durch für Datenschutz sensibilisiertes Handeln erreichen.

Mit den bisher gewonnen Erkenntnissen soll im nächsten Kapitel die Grundlage für eine kontextorientierte Unterrichtsreihe zu Smartphone-Applikationen geschaffen werden, die sich im Kern mit Datenschutz und Datensicherheit befassen soll.

[19] http://www.heute.de/suedkorea-verpflichtet-eltern-zur-online-ueberwachung-ihrer-kinder-38485674.html Stand: 17.05.2015

Kapitel 3

Die Unterrichtsreihe

Im Folgenden werden zuerst einige Vorüberlegungen zu der Einheit gemacht, die das Erstellen eines neuen Kontextes rechtfertigen und dessen Intentionen festlegen sollen. Daran anschließend werden die Vorgaben von IniK an einen Kontext knapp vorgestellt und überprüft, sowie konkrete Inhalte und Kompetenzen ausgewählt. Mit Hilfe der IniK-Kriterien und der getätigten Auswahl wird der Ablauf der Reihe dargestellt, begründet und mit den Vorgaben in Bezug gesetzt. Sowohl die Notwendigkeit bzw. Möglichkeit einer Reduktion der für einen Grundkurs bestimmten Inhalte werden diskutiert, als auch mögliche Anknüpfungspunkte an die in 1.2 vorgestellten Kontexte, sowie ein Ausblick auf potentielle Erweiterungen des neu geschaffenen Kontextes.

3.1 Vorüberlegungen

Die in 1.1.2 von Berendt et al. [BDDP15] genannten Defizite an bisherigen Materialien und die daraus resultierenden Schlussfolgerungen spielen eine zentrale Rolle bei der Konzeption der neuen Unterrichtsreihe. Aufgrund der von Berendt et al. genannten Überkomplexität des Themenfeldes, scheint es nicht ratsam alle Aspekte der sozialen und institutionellen Privacy innerhalb einer Reihe behandeln zu wollen. Sie nennen darüber hinaus, dass die Inhalte wegen der Interdisziplinarität von Privacy nur schwer für Lehrer eines einzelnen Faches handhabbar sind, denn es ergeben sich zwangsläufig eine Fülle von gesellschaftlichen und informatischen Fragen. Aus diesen Gründen scheint es illusorisch, die vollstän-

dige Breite des Themenfeldes in einer einzelnen Unterrichtsreihe behandeln zu wollen.

Die in 1.1.2 beschriebene Kritik einer Schülerin stellt fest, dass es gerade wegen fehlender Zusammenhänge an Konsequenzen beim Nutzungsverhalten fehlt. So war ein bzgl. des Data-Mining genannter Zusammenhang zwischen dem Liken einer Donuts-Kette und späteren Auswirkungen für das verdiente Gehalt zu abstrakt. Der direkte Bezug für die Schüler ist deshalb elementar für die Inhalte der Unterrichtsreihe. Darüber hinaus widersprechen Ratschläge zur Datenvermeidung dem Mitteilungsbedürfnis der Nutzer, weshalb die Verschlüsselung und Anonymisierung von Kommunikation stärker in die Bemühungen der Bildungsinstitutionen einfließen sollten.

Aufgrund fehlender Einbettung des Datenschutz in die Lehrplänen der Sekundarstufe I[1] muss davon ausgegangen werden, dass die Reihe innerhalb des Unterrichts den ersten Kontakt mit dem Datenschutz für die Schüler darstellt. Deshalb sollte weder versucht noch erwartet werden, dass das Themenfeld in vollem Umfang behandelt werden kann. Vielmehr ist das Ziel eine solide Grundlage zu schaffen auf der weitere Maßnahmen aufbauen können. Darunter fallen bspw. weitere Unterrichtsinhalte und betriebliche Fortbildungen, denn nach Aussagen des Datenschutzbeauftragte von Rheinland-Pfalz ist die Erziehung zu aufgeklärten und informierten Nutzern[2] eine generationenübergreifende Aufgabe der Bildungsinstitutionen.

Die Durchführung des IniK-Projekts *Planspiel Datenschutz 2.0*, unter Leitung eines Wissenschaftlichen Mitarbeiters des Arbeitsgebietes Didaktik der Informatik[3] der Universität Koblenz-Landau, mit einem Grundkurs Informatik der Stufe 11 eines Gymnasiums, ergab ein ähnliches Bild: Die Schüler zeigen Interesse an der Thematik und fühlen sich auch betroffen, halten das Thema Privacy allerdings erst für später wichtig. Argumente wie *Denke, dass ich nicht viel preis gebe* oder *Ich mache doch nichts terroristisches!* werden hier von den Schülern angeführt. Ihr Interesse galt überwiegend der Verschlüsselung und wünschten sich, dass aktives Verschlüsseln Teil des Planspiels würde.

[1] In den rheinland-pfälzischen Lehrplänen der Sek. I taucht der Suchbegriff *Datenschutz* nicht bzw. nur unzureichend auf.

[2] vgl. dazu auch 1.1.1

[3] Teil der Arbeitsgruppe IT Risk Management am Campus Koblenz

Die beim Planspiel fehlende Anwendung von Verschlüsselung wird in der IniK-Reihe *E-Mail (nur?) für Dich behandelt*. Da die E-Mail nach den Erkenntnissen der JIM-Studie nicht erste Wahl bei der jetzigen Schülergeneration ist, geht hier jedoch der direkte Bezug verloren. Die Behandlung der kryptographischen Verfahren lassen sich in diesem Kontext gut behandeln, zum Einstieg in das Themenfeld ist er wegen der fehlenden Aktualität jedoch nur noch bedingt zu gebrauchen. Deshalb scheint es naheliegend einen neuen Kontext mit aktuellem Lebensweltbezug für die Schüler zu erstellen.

Daraus folgen inhaltliche Konsequenzen bei der vom Autor zu erstellenden Unterrichtsreihe. Die zu behandelnden Inhalte benötigen einen direkten Bezug zur Lebenswelt der Schüler, damit eventuelle Auswirkungen für sie greifbar sind. Fragen zur Demokratie und Sammelaktivitäten der Datenindustrie sind wichtig, sollten dennoch überwiegend erst in einem nächsten Schritt bzw. im Anschluss an diese Reihe behandelt werden, nachdem ein gewisses Bewusstsein für die Thematik hergestellt wurde. Nach dem Fazit von Berendt et al., beschrieben in 1.1.2, sollte Kommunikation, sowie deren Verschlüsselung und Anonymisierung, stärker betrachtet werden. Das grundlegende Verständnis soll durch eine hohe Eigenaktivität der Schüler geschaffen werden. Daran anschließend soll versucht werden, das in 1.1.2 beschriebene Peer-to-Peer Lernen zu initiieren: Sollten die Schüler durch die Aktivität im Unterricht ihr Verhalten ändern, so wird diese Verhaltensänderung im besten Fall von Altersgenossen übernommen werden.

Erstes Ziel der Einheit soll sein, dass die Schüler Risiken bei der Smartphone-Nutzung erkennen und vermeiden. Dabei soll bewusst nicht der gesamte Umfang an möglichen Konsequenzen behandelt werden. wie bspw. Auswirkungen des Data-Minings auf das Berufsleben. Vielmehr soll ein Bewusstsein beim Einsatz von mobilen Medien entstehen und nach Möglichkeit anschließend ein bewussteres Nutzungsverhalten bei den Schülern einsetzen. Für die Entwicklung der Reihe werden nun zuerst die Kriterien von IniK an einen Kontext genauer betrachtet.

3.1.1 Kriterien von IniK

Über die Beachtung der in 1.2 genannten Prinzipien von IniK müssen nach Diethelm et al. [DKW11] bei der Erstellung eines Kontextes folgende fünf Kriterien erfüllt werden:

1. Mehrdimensionalität:
   Ein Kontext hat immer mehrere Dimensionen, z.B. eine rechtliche, ökonomische, ökologische, ethische oder informatische Dimension [DKW11, S. 102].

2. Breite:
   Die vieldimensionale Ausformung eines Kontextes soll gesellschaftlich relevant und nicht nur technisch-mathematisch interessant sein [DKW11, S. 102].

3. Tiefe:
   Der Kontext muss informatisch relevant sein, d.h. es ist ein solides Hintergrundwissen aus der Informatik notwendig, um die Phänomene, die den Kontext ausmachen zu verstehen [DKW11, S. 102].

4. Lebenswelt:
   Ein Kontext für IniK soll direkten Bezug und Handlungsrahmen in der Lebenswelt Schülerinnen und Schüler aufweisen. Genderaspekte sind hier zu beachten [DKW11, S. 102].

5. Stabilität:
   Der Kontext und die ihm innewohnenden informatischen Prinzipien und die mit ihm vermittelten Kompetenzen sollen über einen längeren Zeitraum Bestand haben [DKW11, S. 102 f.].

Nach Koubek et al. [KSSW09, S. 273] hat kontextorientierter Informatikunterricht verschiedene Optionen zur Ausgestaltung. Der im Rahmen dieser Arbeit ausgewählte Ansatz versteht Informatikunterricht dabei als gesellschaftliches Fach, der sich mit der bereits genannten Definition von Mehrdimensionalität deckt und damit die Wechselwirkungen zwischen Informationstechnik und Gesellschaft berücksichtigt. Die Blickrichtung vom Kontext auf das Fach spielt ebenfalls eine wesentliche Rolle. Das heißt es werden nicht Beispiele zu Fachinhalten gesucht, sondern die Fachinhalte mit Bezug auf die Lebenswelt gefunden.

Zu den in 1.2 genannten Prinzipien gehören vielfältige und schüleraktivierende Methoden. Nach Koubek et al. sind u.a. besonders geeignet: *Experimente und Erkundungen des Kontexts* und *Recherche, ggf. in arbeisteiligen Gruppen* [KSSW09, S. 275].

Für die Struktur der Entwürfe empfehlen Koubek et al.:

1) Analyse des Kontextes mit Rücksicht auf die Lebenswelt der Schüler und gesellschaftliche Relevanz.

2) Kompetenzerwartungen bzw. Inhalts- und Prozessbereiche auflisten.

3) Mögliche Dekontextualisierungen.

4) Planung der Unterrichtsphasen.

5) Verknüpfungsmöglichkeiten zu anderen Fächern.

1) wurde in Kapitel 1 ausführlich beschrieben. Die Punkte 2) bis 5) werden in den folgenden Abschnitten thematisiert.

3.1.2 Kompetenzerwartungen

Edgar Wagner [Wag12] nennt inhaltliche Anforderungen an ein Bildungskonzept, das dem Bildungsauftrag gerecht werden will. Dazu gehört, dass die Bürger ein Bewusstsein für die Zusammenhänge in der digitalen Welt erlangen müssen. Es geht nicht darum jedes technische Detail zu beherrschen, sondern Vorstellungen der Vorgänge und der damit bedrohten gesellschaftlichen Werte zu erlangen. Durch diese Aufklärung sollen selbstverantwortliche Entscheidungen ermöglicht und der Blick für die Bedeutung der Technik für die Persönlichkeitsrechte und die Grundwerte der Demokratie geschärft werden. Daran anschließend muss der Selbstdatenschutz Teil des Konzepts sein - Datenschutz kann nicht zentral geregelt werden, sondern muss aktiv mit der Nutzung von (u.a.) Smartphones betrieben werden. Dies bezieht die ständige Weiterentwicklung der technischen Entwicklungen mit ein. Die Inhalte dürfen nicht auf spezifische Ausprägungen eines Problems abzielen, sondern müssen allgemeine Regeln vermitteln, die eine Anwendung auf weitere Entwicklungen möglich machen. Besonders in der Schule ist dies wesentlich, denn für die Schüler müssen hier die Grundlagen geschaffen werden, die (im Idealfall) im Berufsleben weiter ausgebaut werden.

Bezüglich der im vorherigen Abschnitt genannten Tiefe, wird der Bezug zu den Bildungsstandards der Sekundarstufe I empfohlen, was aufgrund der bisher fehlenden Aufnahme des Informatikunterrichts in die Reihe der verpflichtenden Unterrichtsfächer und der daraus resultierenden Schülerzahlen, für die Konzeption von Unterrichtsreihen allerdings nur bedingt hilfreich ist.

Ein Blick auf die Statistiken[4] der Schülerzahlen der Mainzer Studienstufe zeigen, dass in Rheinland-Pfalz Informatikunterricht in der Sekundarstufe II überwiegend in Grundkursen stattfindet. Wie in Tabelle 3.1 dargestellt, belegten von den insgesamt 49.052 Schülern der MSS im Jahr 2013/14 nur 235 (0,5 %) Schüler Informatik als Leistungsfach und 10.662 (21,7 %), belegten einen Grundkurs (GK). Demnach betrug der Anteil der Teilnehmer an einem Leistungskurs gemessen an der Gesamtmenge der Informatikschüler 2,2 %. Über die Teilnehmer am (freiwilligen) Wahl- bzw. Wahlpflichtfach[5] in den letzten beiden Jahrgangsstufen der Sek. I in Rheinland-Pfalz gibt es keine Zahlen. Die Teilnahme am Wahl(pflicht)fach ist Voraussetzung für eine mögliche Wahl eines Leistungskurs Informatik. Es ist nicht zu erwarten, dass jeder Teilnehmer auch den Leistungskurs wählt, dennoch ist von einem einstelligen Prozentwert gemessen an der Gesamtschülerzahlen auszugehen.

Gesamte MSS	Leistungskurs	verpflichtender GK	freiwilliger GK
49.052 (100 %)	235 (0,5 %)	8.507 (17,3 %)	2.155 (4,4 %)

Tabelle 3.1 Schülerzahlen der MSS im Fach Informatik 2013/2014

Da Informatik in keinem Bundesland verpflichtendes Unterrichtsfach ist, werden sich die Zahlen im Vergleich zu den übrigen Bundesländern ähneln. Eine offizielle, bundesweite Statistik gibt es jedoch nicht. Es ist anzunehmen, dass die Schülerzahlen bzgl. des Faches Informatik zum jetzigen Zeitpunkt in Grundkursen konzentriert sind. Aufgrund fehlender Bildungsstandards für die Sek. II werden die Inhalte und Kompetenzen beispielhaft unter Berücksichtigung des Lehrplans[6] für das Grundfach der Mainzer Studienstufe ausgewählt bzw. legitimiert. Dieser Lehrplan wurde unter Einbeziehung der Bildungsstandards für die Sek. I konzipiert.

[4]Statistischer Bericht über die Mainzer Studienstufe im Schuljahr 2013/2014 http://www.statistik.rlp.de/fileadmin/dokumente/berichte/B1083_201300_1j_K.pdf (Stand: 16.05.2015)

[5]Die Bezeichnung ist abhängig von der Länge der Schulzeit (G9 bzw. G8), die Inhalte sind im Wesentlichen gleich.

[6]http://informatik.bildung-rp.de/lehrplaene.html Stand: 04.05.2015

Die für die kontextorientierte Unterrichtsreihe *Smartphone-Applikationen* relevanten Inhaltsbereiche sind:

1. Kommunikation in Rechnernetzen
2. Informationen und ihre Darstellung
3. Software-Entwicklung

Zu 1. gehören sowohl die Sicherheitsziele Vertraulichkeit, Authentizität und Integrität, als auch die Sicherheitsprobleme bei alltäglicher Kommunikation, sowie deren Brisanz. 2. umfasst die Sammlung, den Missbrauch und den Schutz personenbezogener Daten. 3. beinhaltet die Fehler in Software bzw. Apps und die daraus resultierende Gefährdung der Sicherheitsziele, sowie die Bedeutung von Updates. Der Inhaltsbereich *Aufbau und Funktionsweise eines Rechners* wird im Zuge des Sandboxings von Android nur angeschnitten und deshalb in der Liste nicht aufgeführt.

Daraus resultieren für die Schüler innerhalb der Reihe zu erwerbende Kompetenzen. Die Schüler sollen:

- Datenerhebung unter dem Aspekt Datenschutz bewerten.
- Datensicherheit unter Berücksichtigung kryptologischer Verfahren erklären und beachten.
- Qualitätsmerkmale für Software kennen und beachten.

Sie sollen die Funktionsweise von Smartphones und deren Apps beschreiben können. Die Qualität von Applikationen bzgl. des Datenschutzes soll erkannt und bewertet werden. Darüber hinaus sollen die Schüler die Sicherheit der von ihnen betriebenen Kommunikation einschätzen können. Durch eine kritische Betrachtung von Datenerhebung sollen sie die Gefahren des Missbrauchs ihrer personenbezogenen Daten erkennen, sowie den Schutz dieser Daten durch die Verwendung sicherer Apps verbessern können. Dies bezieht sich auch auf den Umgang mit den mobilen Geräten und deren Anwendungsmöglichkeiten, die sie verantwortungsvoll einsetzten sollen. Durch die informatisch relevanten Inhalte und Kompetenzen, ist das 3. Kriterium von IniK erfüllt.

3.1.3 Dekontextualisierung

Der Kontext befasst sich mit verschiedenen Dimensionen, was das 1. Kriterium von IniK erfüllt. Die technische Ausprägung des Kontextes ist durch die Betrachtung der Funktionsweise der Rechtevergabe von Android und die Qualitätsbetrachtung von Applikation gegeben. Die ethische Dimension befasst sich mit dem Für und Wider der totalen Transparenz und dem Thema Spionage. Ökonomische Aspekte werden durch die Frage nach den Intentionen von Datensammlern betrachtet. Die historische Dimension ist in gewissem Maße durch die Betrachtung möglicher zukünftiger gesellschaftlicher Entwicklungen vorhanden. Dazu kommt die rechtliche Dimension durch Thematisierung des Informationsfreiheitsgesetzes und der informationellen Selbstbestimmung. Die verschiedenen Dimensionen sind nicht nur innerhalb der Informatik, sondern auch für die Gesellschaft relevant. Das 2. IniK-Kriterium ist damit ebenfalls erfüllt.

3.2 Struktur der Unterrichtsreihe

Koubek et al. [KSSW09] regen an, die Reihe in vier Phasen zu gliedern, Diethelm et al. [DKW11] schlagen die Ergänzung um eine 5. Phase vor:

1. Begegnungsphase
2. Neugier- und Planungsphase
3. Erarbeitungsphase
4. Vernetzungs- und Vertiefungsphase
5. Rekontextualisierungsphase

Die Phasen sind dabei als Anregung zu verstehen und nicht verpflichtend, denn in verschiedenen Entwürfen hat sich gezeigt, dass diese hilfreich oder unbrauchbar sein können. Bei der Erstellung der Reihe *Smartphone-Applikationen* wird sich an vorgeschlagenem Schema orientiert.

Die Reihe ist in vier Phasen gegliedert. Die 1. Phase dient Einführung in das Thema und der Herstellung von Lebensweltbezug für die Schüler. Dazu wird die Spionage mit der häufig genutzten Messanger-App *WhatsApp* behandelt. In der 2. Phase befassen die Schüler sich mit der Rechtevergabe von Android, sowie

der Sicherheit von Software, Netzen und Verbindungen. Die 3. Phase thematisiert das Sicherheitsziel Vertraulichkeit und wie man dieses auf dem Smartphone herstellen kann. Zur Vertiefung werden in der letzten Phase Beweggründe für die Sammlung von Daten besprochen und weitergehende Fragen des Datenschutzes thematisiert. Abgeschlossen wird die Phase und damit die Reihe durch eine Rückschau auf die behandelten Inhalte und die Übertragung des Gelernten auf Situationen, die nicht mit der Nutzung des Smartphones zusammenhängen.

Damit wäre auch das 4. Kriterium von IniK, der Bezug zu Lebenswelt, erfüllt. Das 5. Kriterium, die zeitliche Stabilität kann ebenfalls als erfüllt angesehen werden. Besitz und Nutzung von Computern nehmen laut der JIM-Studie tendenziell ab, während bei Smartphones eine steigende Tendenz beobachtet wird. Die Entwicklung der Datenbrille *Google Glass* und *Smartwatches* zeigen, dass es Smartphones bzw. mobile Geräte mit ähnlicher Funktionalität auch in Zukunft geben wird.

Das bei der Konzeption nicht nur die Sicht der Erwachsenen eine Rolle spielen darf, zeigt die Bewertung der Unterrichtsreihe von Berendt et al. einer Schülerin aus Abschnitt 1.1.2. Daraus resultiert, dass der von Wagner [Wag12, Abschnitt 2.7] bzw. Berendt et al. [BDDP15] genannte *erhobene Zeigefinger* nicht zielführend ist, denn der Spaß an der Mediennutzung muss erhalten bleiben.

Da eine Begrenzung der Reihe auf bestimmte Themen des Datenschutzes notwendig ist, um der Überkomplexität entgegenzuwirken, werden viele im Internet zugängliche Materialien verwendet. Dies soll zum einen die Aktualität dieser gewährleisten und zum anderen den Schülern die Möglichkeit aufzeigen sich über die Unterrichtsreihe hinaus mit Datenschutz und Datensicherheit befassen zu können.

3.2.1 1. Phase: Spionage mit dem Smartphone (1h)

Die Schüler lernen die Möglichkeit des Missbrauchs von Informatiksystemen kennen. Im konkreten Fall die Spionage durch das eigene Smartphone. Dies zeigt die Sicherheitsprobleme bei der Nutzung mobiler Geräte und deren Brisanz auf. Das Sicherheitsziel Vertraulichkeit steht im Vordergrund.

In der ersten Phase der Reihe, soll die Einführung des Themas erfolgen und das Interesse der Schüler geweckt werden. Zu Beginn eignet sich eine Frage wie: *Welche Probleme sind euch bei der Nutzung eures Smartphones bekannt?* Die Schüler

sollen dabei ihnen bekannte Beeinträchtigungen im Zusammen mit der Nutzung ihres Smartphones nennen. Dazu zählen bspw. Nicht-Verfügbarkeit des Netzes, Diebstahl und ungewollt aufgenommene Fotos mit der Kamera des Geräts. Die einzelnen Wortmeldungen sollen dabei an der Tafel gesammelt werden. Für den Lehrer bietet der bereits in 2.2 genannte Grundschutzkatalog des BSI eine Übersicht über mögliche Gefährdungslagen bei der Nutzung von Mobiltelefonen bzw. Smartphones. Bei Bedarf kann der Lehrer mit Elementen dieser Liste Impulse setzen, indem er Beispiele nennt, falls von den Schülern keine oder nur wenige Wortmeldungen kommen. Es empfiehlt sich zur besseren Übersicht eine der Gliederung des Kataloges entsprechenden Anordnung nach z.B. technischem Versagen, menschlichen Fehlhandlungen und vorsätzlichen Handlungen. Darüber hinaus sollen die Begriffe Datenschutz und Datensicherheit mit Bezug auf die genannten Gefährdungen voneinander abgegrenzt werden.

Um anschließend den Fokus auf den Datenschutz zu setzen, eignet sich das knapp acht Minuten lange Video *Das Smartphone als Super-Wanze: Wie Handydienste den Datenschutz aushöhlen*[7] von *report München*, welches die Möglichkeit der Überwachung einer Person mit Hilfe seines Smartphones thematisiert. Inhalt des Videos ist zunächst die Installation einer Spionage-App durch eine Studentin auf dem Smartphone eines Freundes, mit der sie diverse private Informationen erhält. Dazu zählen gespeicherte Fotos, das Mithören von Gesprächen und die Ortung des Smartphones. Weitere Inhalte des Videos sind die Vermutung, dass Smartphones bzw. Apps aufgrund ihrer Rechte Wanzen sind und die verschiedenen Interessenten an den so gewonnenen Informationen. Das Szenario könnte sich in einer ähnlichen Form in gleicher Weise bei den Schüler ereignen und die unter Verdacht stehende App *WhatsApp* wird auf fast allen Smartphones installiert sein, was eine direkte Betroffenheit bei ihnen erzeugt.

Aufgrund der Menge an enthaltenen Informationen, sollte der Kurs in zwei Gruppen geteilt werden, die sich während des Videos jeweils auf bestimmte Fragestellungen konzentrieren sollen. Die erste Gruppe beschäftigt sich mit der Frage welche Daten die im Video thematisierte Spionage-App sammelt. Die zweite Gruppe soll die genannte Begründung bzgl. des Wanzen-Vorwurfs nennen können und die Interessenten an den Daten auflisten. Im Anschluss sollen die gewonnen Informationen gesammelt werden und mit Hilfe eines Tafelbildes gesichert werden, das die Schüler übernehmen sollen, da sich im Verlauf der Reihe noch

[7] https://www.youtube.com/watch?v=oJib8x7Mh7I Stand: 24.05.2015

mehrmals darauf bezogen wird. Dabei soll auch das Sicherheitsziel Vertraulichkeit von Kommunikation herausgearbeitet werden.

Ein alternatives Videos zum Einstieg ist bspw. *Smartphones - Spione in der Hosentasche*.[8] Hier wird bereits detaillierter auf die Rechte von Apps eingegangen, das Szenario der Überwachung wirkt allerdings konstruiert. Das Video von *report München* stellt hingegen eine Situation dar, die jedem Schüler widerfahren könnte.

3.2.2 2. Phase: Apps im Sandkasten (3h)

Um die Risiken des Wanzen-Vorwurfs beurteilen zu können, ist zunächst eine Erarbeitung eines grundlegende Verständnisses der technischen Gegebenheiten notwendig. Die Schüler lernen deshalb das Zusammenspiel des Betriebssystems Android mit Applikationen kennen. D.h. die Sandbox und die Prinzipien der Rechtevergabe müssen von den Schülern erklärt werden können. Darüber hinaus sollen sie bzgl. der Kommunikation in (Rechner)Netzen die Möglichkeiten der Standortbestimmung nennen, die Gefahren von öffentlichen Hotspots beurteilen, sowie die Verbindung via Bluetooth kennen lernen. Bzgl. der Qualität von Software sollen sie die Kontrollmechanismen des Play Stores für Malware bewerten, sowie den Vorwurf der Verwendung von WhatsApp als Wanze beurteilen.

Als Material zum Verständnis der Sandbox eignet sich Abschnitt *3. Sandbox* des Blog-Eintrages von Mike Kuketz[9] über Antivirus-Apps für Android. Für die Rechtevergabe empfiehlt sich das drei Minuten lange Video *Handysektor erklärt: Was sind eigentlich App-Berechtigungen?*[10], welches das Prinzip anschaulich erklärt. Die Schüler sollen nun mögliche Vor- und Nachteile des Sandbox-Konzeptes und seiner Rechtevergabe diskutieren. Da die Behandlung von Betriebssystemen für das Grundfach nicht vorgesehen ist, sollte auf eine Betrachtung der Theorie, bspw. der DVM, verzichtet werden.

[8] Zu finden unter https://www.youngdata.de/smartphones/was-duerfen-apps/. Stand: 23.05.2015

[9] http://www.kuketz-WhatsApp.de/antivirus-apps-fuer-android-sinnvoll-oder-nutzlos/ Stand: 23.05.2015.

[10] Zu finden unter https://www.youngdata.de/smartphones/was-duerfen-apps/ Stand: 23.05.2015

Alternativ zu dem Video ist auch eine Internetrecherche möglich, z.B. mit dem *Exkurs: App-Berechtigungen bei Android*[11] des BSI für Bürger. Das Video bietet allerdings eine passende Überleitung zu den weiteren Inhalten dieser Phase und sollte daher bevorzugt werden.

Die Schüler sollen sich nun mit der App *aSpotCat*, empfohlen von *YOUNGDATA* und dem BSI, einen Überblick über die Rechtevergabe der Anwendungen auf ihrem eigenen Smartphone schaffen. Die App führt dabei die Berechtigungen aller durch den Nutzer installierter Applikationen auf, wahlweise geordnet nach Rechtekategorien (bspw. Anruf und Ihr Standort), oder nur für eine einzelne Anwendung. Dies soll den Grad der konkreten Betroffenheit verstärken.

Um den Zusammenhang der Rechte mit dem Datenschutz besser zu erkennen, sollen nun folgende Themen, mit Bezugnahme auf das eingangs erstellte Tafelbild, in Kleingruppen erarbeitet werden:

1 Sicherheit von öffentlichen Hotspots bzw. unbekannten WLAN-Netzwerken

2 Standortbestimmung durch GPS und Netzwerke

3 Sicherheit von Verbindungstechniken (z.B. Bluetooth)

4 Softwareupdates, Sicherheit des Play Store und Malware

Hierzu eignen sich die Materialien von (a) *YOUNGDATA*, (b) des BSI (für Bürger) und (c) die Unterrichtsmaterialien von *klicksafe* [Fil08] als erste Informationsquellen für die Schüler. Der gewünschte Umfang bzw. die informatische Tiefe ist vom Lehrer in Abhängigkeit zu der Lerngruppe zu wählen, sodass es weder zur Unter- noch Überforderung kommt. Zur Binnendifferenzierung ist auch die Bereitstellung unterschiedlicher Materialien zum selben Thema denkbar. Es folgt eine Auswahl an möglichen Informationsquellen zu den vier Themen:

zu 1: (a) *Spying Apps*, (b) *Fremde WLANs* und (c) *W-Lan* [Fil08, S. 279 ff.].

zu 2: (a) *Location-Datatracking*.

zu 3: (b) *Verbindungstechniken für mobile Geräte*.

zu 4: (b) *Basisschutz für Smartphone und Co.* bzw. *Basisschutz Apps* und (c) *Viren, Würmer, Trojaner, Spyware* [Fil08, S. 227 ff.].

[11] https://www.bsi-fuer-buerger.de/BSIFB/DE/MobileSicherheit/mobileSicherheit_node.html Stand: 17.05.2015

Besonders die Apps zur Kommunikation benötigen eine Verbindung mit dem Internet. In Ermangelung eines Vertrages oder um das vertraglich begrenzte Datenvolumen zu schonen, werden von Schülern gerne offen zugängliche WLAN-Netzwerke genutzt. Kenntnisse zur Bewertung der Sicherheit dieser Netze sind für den Nutzer von elementarer Bedeutung. Damit einher gehen die dadurch entstehenden Möglichkeiten der Standortbestimmung, die neben positiven Anwendungen auch Gefahren des Missbrauchs bergen. Bei Apps zur Navigation ist der Standort des Nutzer zur Ausführung der Funktion unabdingbar, es können allerdings auch Bewegungsprofile erstellt werden, die Gewohnheiten der Anwender ausspähen. Neben der Möglichkeiten der Datenübertragung über das Datennetz, werden auch weitere Verbindungsarten zwischen Smartphones genutzt, von denen Bluetooth am häufigsten verwendet wird. Dessen Sicherheit sollen die Schüler ebenfalls bewerten können. Darüber hinaus sollten der Zusammenhang von aktualisierter Software mit den Gefahren von Malware beim Einsatz von Smartphones, sowie die Maßnahmen des *Play Stores* gegen schadhafte Software bekannt sein. Als lästig empfundene Aufforderungen zum Update von Apps sollen unter diesen Gesichtspunkten von den Schülern neu beurteilt werden.

Die in den Gruppen gewonnen Erkenntnisse sollen den Mitschülern so präsentiert werden, dass jeder Schüler ein grundlegendes Verständnis der besagten Themen entwickeln kann. D.h. es sollen unbekannte Begriffe erklärt, die Funktionsweisen bzw. Abläufe erläutert, sowie das Gefährdungspotenzial aufgezeigt werden. Eventuelle Gegenmaßnahmen bzw. Vermeidungsstrategien sollen noch nicht Bestandteil der Vorträge sein, da diese erst im weiteren Verlauf der Reihe thematisiert werden. Zur Veranschaulichung der Vortragsinhalte soll von jeder Gruppe ein Plakat erstellt werden, dass die wesentlichen Inhalte zusammenfasst. Bei Verfügbarkeit einer Lernumgebung (z.B. Moodle) bietet es sich an die Plakate dort verfügbar zu machen, da es in der Oberstufe keine festen Klassenräume mehr gibt, sodass sich ein Anbringen der Plakate an der Wand zur Wiederverwendbarkeit nur begrenzt eignet.

Zur Vernetzung soll abschließend mit dem bisher erworbenen Wissen eine Diskussion über den Vorwurf gegen *WhatsApp* geführt werden. Die in 2.3 genannten Berichte von *WAZ*, *GIGA*, *mimikama* und *heise* eignen sich als Diskussionsgrundlage für die Schüler, insofern keine aktuelleren Berichte bekannt werden. Sie befassen sich erst in Kleingruppen mit einer Sichtweise und sollen diese in einer Podiumsdiskussion vertreten. Die Kleingruppen können sich ggf. je nach

Meinungsbild innerhalb der Klasse, diesem Bild entsprechend zusammensetzten. D.h. bspw. die Unterstützer des Wanzen-Vorwurfs bekommen den Artikel der *WAZ*, die Gegner den von *heise* und dazwischen Positionierte den von *mimikama* zur Vorbereitung. An der anschließenden, von einem Schüler (aus einer beliebigen Gruppe) moderierten Diskussion nimmt ein Mitglied aus jeder Gruppe teil. Um positive Effekte bzgl. der Kommunikationskompetenzen der Schüler zu erzielen, sollte der Lehrer eine beobachtende Position einnehmen.

3.2.3 3. Phase: Vertraulichkeit herstellen (3-4h)

Die Erfüllung des in Phase 1 eingeführten Sicherheitsziels Vertraulichkeit ist Thema der dritten Phase. Zur Vermeidung des im Einstiegsvideo gezeigten Fremdzugriffs auf ein Informatiksystem eignen sich u.a. Passwörter, deren Sicherheit sie beurteilen können sollen. An die Diskussion über *WhatsApp* anschließend, soll die verwendete Verschlüsselung der App erarbeitet und bewertet werden. Nach kritischer Betrachtung von Alternativen zu *WhatsApp*, sollen die Schüler die Qualität dieser Softwareprodukte bewerten.

Die Passwortsicherheit lässt sich gut in Partnerarbeit und mit den Materialien *Passwörter* [Fil08, S. 247 ff.] und der dort referenzierten Seite des Datenschutzbeauftragten im Kanton Zürich[12] erarbeiten. Die Materialien des BSI unter der Rubrik *Passwörter* sind hingegen eher Verhaltenstipps. Es fehlt dort an aussagekräftigen Begründungen für die Sicherheit eines Passwortes, sowie Informationen über Möglichkeiten unberechtigt an ein Passwort zu kommen. Die Schüler sollen Angriffsmethoden auf Passwörter, wie z.B. Brute-Force, Phishing und Sniffer, kennenlernen und die Sicherheit von Passwörtern beurteilen können. Sie sollten auch selbst einige Passwörter mit entsprechenden Tools testen, eine Möglichkeit ist ein Passwort-Check, der auf den Internetseiten des züricher Datenschutzbeauftragten zu finden ist. Optional kann ein humoristisches Interview mit dem Whistleblower Edward Snowden zum Einstieg in die Phase verwendet werden: *Edward Snowden über Passwörter*[13].

Im Zuge der Behandlung von Passwörtern wird die Problematik bei der Übertragung von diesen deutlich. Über unsichere Verbindungen übertragene Pass-

[12] https://passwortcheck.ch/ Stand: 23.05.2015

[13] http://www.passwortbibel.de/passwort-knacken/edward-snowden-ueber-passwoerter/4159 Stand: 23.05.2015

wörter können an sich sicher sein, sind allerdings nutzlos, wenn sie als Klartext versendet werden. Zur Einführung in das Thema verschlüsselte Kommunikation eignet sich der Artikel *WhatsApp entschlüsselt* [ES15], da er die Verschlüsselungsverfahren der bereits behandelten Applikation *WhatsApp* thematisiert. Die Sicherheitsziele bei der Kommunikation, Authentizität und Integrität, sollen diskutiert werden.

Eine Möglichkeit die Einhaltung dieser Ziele auf Smartphones zu gewährleisten sind Apps zur verschlüsselten Kommunikation. Aufgrund der Vielzahl an Applikationen, die laut Aussage ihrer Entwickler Datenschutz und Datensicherheit gewährleisten wollen, ist es für die Schüler wichtig die Qualität der Anwendungen beurteilen zu können. Sie sollen explizit Informationen und Bewertungen zu diesen Arten von Apps sammeln, sowie Vor- und Nachteile benennen. Dazu sollen sie zunächst in Partnerarbeit Informationen über eine mögliche Alternative sammeln. Als Quellenhinweise können den Schülern die Bewertungen von *heise* oder *CHIP*[14] empfohlen werden. Alternativen zu *WhatsApp* sind in der *Secure Messaging Scorecard*[15] der *Electronic Frontier Foundation* aufgelistet. Mit Hilfe der gesammelten Informationen sollen die Vor- und Nachteile herausgearbeitet und eine Bewertung für den Rest des Kurses erstellt werden. Zusätzlich zu einer kurzen Vorstellung des Bewertungsergebnisses während des Unterrichts sollen ausführlichere Bewertungen mit Nennung der Argumente auf einer Lernplattform zugänglich gemacht werden. Teil der Argumentation sollten die angewendete Verschlüsselung und die Vertrauenswürdigkeit des Anbieters sein, sowie Kosten und Handhabung der App. Bzgl. des aktiven Ausprobieren der Applikationen kommen voraussichtlich nur kostenfreie Angebote in Frage.

Alternativ eignet sich eine leicht variierende Vorgehensweise. Neben einigen prominenteren Vertretern der *WhatsApp*-Alternativen, wie bspw. *Threema* und *Telegram*, ist im Rahmen der Partnerarbeit auch die Untersuchung von anderen App-Arten möglich. Dazu zählen solche zur Prozessüberwachung, zum Backup bzw. Fernzugriff und zur Kontrolle von Systemkomponenten, die bspw. die Kamera sperren, sowie Virenscanner-Apps. Problematisch an dieser Alternative ist die kontinuierliche Weiterentwicklung des Angebots, denn für keine der weiteren App-Arten haben sich bisher verlässliche Marktführer etabliert. Bzgl. der Prüfung der Handhabung muss der Lehrer demnach genau kontrollieren, ob ei-

[14] http://www.chip.de Stand: 23.05.2015
[15] https://www.eff.org/de/node/82654 Stand: 23.05.2015

ne Installation der Apps ohne Bedenken erfolgen kann. Aufgrund der schnellen Entwicklung des Software-Marktes, gerade im Bereich der Applikationen, bedeutet dies für den Lehrer in beiden Fällen Recherchearbeit. Passende Informationen kann er auf den Webseiten von *heise* und *CHIP* erhalten, die auch Rankings nach App-Arten führen. Die zweite Variante hat hingegen den Vorteil, dass verschieden Arten von Apps ausprobiert werden können und nicht nur Messanger.

3.2.4 4. Phase: Ich habe doch nichts zu verbergen? (1-2h)

Die vierte Phase der Reihe soll der Vertiefung bzw. Vernetzung dienen. Selbst wenn die Möglichkeiten gegeben sind ausgespäht zu werden, bedeutet dies nicht, dass jeder Schüler die Notwendigkeit erkennt sein Verhalten bzgl. der Preisgabe seiner Daten zu ändern. Die Schüler sollen die Notwendigkeit von Verschlüsselung zur Verhinderung von totaler Transparenz kennen. Die Erhebung von Daten soll unter dem Aspekt Datenschutz bewertet werden. Abschließend sollen eine Reflexion und Bewertung der Inhalte dieser Reihe erfolgen, sowie deren Bedeutung in weiteren Lebensbereichen festgestellt werden.

Zum Einstieg empfiehlt sich das drei minütige Video *Sixtus vs. Lobo #13: Totale Transparenz*[16], das Argumente für und wider der Transparenz im Netz aufzeigt. Mit Bezug auf das Tafelbild der 1. Phase soll im Unterrichtsgespräch mögliche Interessenten an Daten und deren Beweggründe besprochen werden. Die folgende Liste dient zur Demonstration der potentiell im Unterricht genannten Datensammler.

- Arbeitgeber: Überwachung bzw. Kontrolle ihrer Arbeitnehmer
- Versicherungen: Aufdecken von Betrug, Erstellung von Risikoprofilen
- Sicherheitsbehörden/ Geheimdienste: Strafverfolgung und -vereitlung
- Krankenkassen: Risikoanalyse
- Firmen: Wirtschaftsspionage
- Betrüger: geldwerte oder materielle Vorteile
- Marktforscher: personalisierte Werbung

[16]http://www.youngdata.de/datenschutz/was-wird-geschuetzt/ Stand: 23.05.2015

- Eltern: Kontrolle der Kinder
- Vermieter: Auswahl der Mieter

Nach Interesse der Schüler sollen nun vereinzelt weitere Fragen bzgl. des Datenschutzes behandelt werden. Dies könnten bzgl. Maßnahmen der Geheimdienste in Deutschland oder den USA gestellt sein, bspw. zur Vorratsdatenspeicherung, dem deutsche Staatstrojaner oder dem amerikanische *PRISM* sein. Quellen dazu sind u.a. Thilo Weicherts Ausführungen zu Big Data [Wei13], *YOUNG-DATA* oder das Datenschutz-Wiki[17] der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Das Recht auf informationelle Selbstbestimmung und das Informationsfreiheitsgesetz bieten sich genauso als Alternativen an, wie die Bedeutung des im Video zur totalen Transparenz angesprochenen sozialen Drucks, der zur Preisgabe von Informationen führen kann.

Durch die genauere Betrachtung von für sie relevanten Fragen, soll das Interesse der Schüler am Datenschutz weiter verstärkt werden und durch das Aufzeigen von verschiedenen Informationsquellen die Möglichkeit zum Selbststudium weiterer Sachverhalte gegeben werden.

Zum Abschluss soll die Behandlung des Datenschutzes in anderen Ländern thematisiert werden ggf. aktuelle Meldungen sind zu bevorzugen. Ein Beispiel ist die bereits in 2.5 angesprochene staatlich verordnete Überwachung von Kindern und Jugendlichen in Südkorea. Durch das Aufzeigen von Entwicklungen der Behandlung des Datenschutzes in anderen Kulturen soll die Bedeutung des Datenschutz noch einmal hervorgehoben werden

Im Zuge des Abschlusses der Reihe soll eine Rekontextualisierung stattfinden. Durch eine Reflexion und Bewertung der behandelten Inhalte soll die Relevanz des neu gelernten für andere Lebensbereiche besprochen werden (vgl. [DKW11]). Dies hat in Ansätzen durch die Auflistung möglicher Datensammler bereits stattgefunden. Die neu gewonnenen Kompetenzen sollen auf andere Kontexte übertragen werden. Dies kann bzgl. der Sicherheitsziele und Qualitätsmerkmale auf das Arbeiten am Computer übertragen werden, sei es privat oder beruflich. Die Sammlung und der Missbrauch von personenbezogenen Daten sind in alltäglichen Situationen, wie dem Abschließen eines Zeitungsabonnements oder allgemein beim Abschluss von Verträgen, zu beachten. Hier sollte darauf geachtet werden, welche Daten zum Vollzug der Geschäftshandlung erforderlich sind.

[17] www.bfdi.bund.de/bfdi_wiki/index.php/Hauptseite Stand: 25.05.2015

3.2.5 Reduktion

Die vorgestellte Reihe ist ohne Bedarf größerer Anpassungen auch in der Sek. I durchführbar. Besonders die Materialien von *klicksafe* zeichnen sich dadurch aus, dass sie in verschiedenen Schwierigkeitsgraden zur Verfügung stehen. Die angesetzte Dauer der Phasen könnte sich durch ein langsameres Arbeitstempo in den niedrigeren Klassenstufen erhöhen. Problematisch ist hier allerdings die Frage, in welchem Fach die Reihe unterrichtet werden soll bzw. auf Kosten welcher Inhalte. Darüber hinaus spielt die zu erwartende mangelnde fachliche Expertise der Kollegen der Sozialwissenschaften eine Rolle, in deren Fächer die Behandlung des Datenschutz möglich wäre. Diese Problematik spielt bei den Verknüpfungsmöglichkeiten zu anderen Fächern ebenfalls eine Rolle.

3.3 Verknüpfungen und Erweiterungen

Die Unterrichtsreihe *Smartphone-Applicationen* bietet einige Anknüpfungspunkte zu bestehenden kontextorientierten IniK-Reihen und zu anderen Fächern. Darüber hinaus bieten sich einige Themen als Erweiterung an.

Mit dem Modul *Vertraulichkeit mit Verschlüsselung herstellen* des Kontextes *E-Mail (nur?) für Dich* können die theoretischen Grundlagen zur Verschlüsselung erarbeitet werden, die bisher nicht thematisiert werden. Das Verständnis von Verschlüsselungstechniken ist plattformunabhängig. Die Durchführung des Moduls birgt allerdings das Problem, dass es keine vergleichbaren und vor allem kostenlosen Apps mit den Funktionen von *Socket Sniff* und *CrypTool* gibt. Ein Vergleich von verschlüsselten mit unverschlüsselten Nachrichten ist damit nicht möglich und die Behandlung der kryptographischen Verfahren verliert an Anschaulichkeit.

Für das *Planspiel Datenschutz 2.0* bietet sich die Gestaltung eines Szenarios mit Verwendung von Smartphones an. Denkbar ist auch eine Umstellung des Spiels auf die Benutzung mobiler Geräte, was allerdings erheblichen Aufwand bedeutet. Fraglich ist auch, ob dazu notwendige Anwendungen existieren.

Da das Smartphone elementarer Bestandteil der Kommunikation von Schülern untereinander ist, sind das Auftreten verschiedener Formen des Mobbings nicht auszuschließen. Bei einer Aktualisierung der Entwürfe bietet sich die Behandlung des Smartphones an. Ob im Kontext *Smartphone-Applikationen* die The-

matisierung von Cybermobbing notwendig ist, hängt von der Schule ab. In vielen schulischen Bildungseinrichtungen gibt es außerunterrichtliche Maßnahmen bzw. Konzepte, die sich gezielt mit der Problematik des Mobbings befassen.

Die Einbindung anderer Fächer bei der Behandlung des Kontexts, im Sinne eines fächerverbindenden Unterrichts, ist wünschenswert. So könnte in der Mathematik bspw. auf die Berechnung der Sicherheit von Passwörtern eingegangen werden, in der Physik auf Datenübertragung. In Gemeinschaftskunde eignet sich eine vertiefende Behandlung von informationeller Selbstbestimmung und Informationsfreiheit. Abhängig von den Kompetenzen des Informatiklehrers ist dies auch im fächerübergreifenden Unterricht möglich. Ebenfalls fächerübergreifend ist die Behandlung von Urheberrechten bzgl. des Downloads von Musik vorstellbar, da jedes Smartphone auch die Möglichkeiten dazu bietet. Ein Problem des fächerverbindenden Unterrichts ist jedoch der begrenzte Spielraum für die Behandlung zusätzlicher Inhalte in den übrigen Fächern, sowie fehlende Materialien und mangelndes Know-how über informatische Themen bei den Fachkollegen.

Die Erweiterung der neuen Reihe ist mit verschiedenen Inhalten möglich. Neben der genannten Behandlung von Angriffsmethoden auf Passwörter, können die verschiedenen Arten von Schadprogrammen behandelt werden. Bot-Netze oder Trojaner sind auch im Zusammenhang mit Smartphones möglich. Die Behandlung der Kommunikation in Netzen, sowie Verbindungsarten und -techniken oder Protokollen bietet sich auf mobilen Geräten in gleicher Weise wie beim Computer an.

Die Architektur von Rechnern, die Thematisierung von Hardwarekomponenten und der Arbeitsweise von Betriebssystemen[18] lässt sich bei mobilen Geräten ebenfalls durchführen, einzig die Anschaulichkeit, die beim Öffnen eines Rechners gegeben ist, geht verloren. Da die Nutzung von Computern zu Gunsten mobiler Geräte abnimmt, ist es legitim diese Inhalte am Smartphone zu behandeln. Daran anschließend können Vor- und Nachteile des Rootens, sowie Fragen des Urheberrechts diesbezüglich besprochen werden. Beim Rooten wird ggf. geschützte Software verändert.

Objektorientierte Programmierung von Apps mit Java ist ebenfalls möglich. Martin Jakobs, regionaler Fachberater für Informatik, hat bereits einige Materia-

[18]Die Behandlung von Betriebssystemen ist in Rheinland-Pfalz allerdings nur im Lehrplan des Leistungsfaches vorgesehen.

lien dazu entwickelt und auf seiner Homepage[19] zur Verfügung gestellt. Die Programmierung findet zwar am Computer statt, das Ergebnis kann jedoch auf dem Smartphone getestet werden.

Die Möglichkeiten des E-Commerce in Verbindung mit mobilen Geräte zu betrachten ist bzgl. der Datensicherheit interessant. Weitere Behandlung von Fragen des Datenschutzes bietet sich in diversen Formen an, bspw. die Thematisierung von *Big Data*, ggf. in Verbindung mit der Behandlung von Datenbanken. Berendt et al. stellen in [BDDP15] eine Unterrichtsreihe vor, die neben den üblicherweise verwendeten Algorithmen auch die durch sie generierten Rückschlüsse auf Personen thematisiert. Weitere Aspekte des Datenschutzes sind die genauere Betrachtung von Wirtschafts-Spionage oder der Überwachung von Personen. Bereits jetzt erkennbare Entwicklungen sind das Bestreben von Krankenkassen, die Daten von Schrittzähler- und anderen Gesundheits-Apps zu verwenden, um ggf. die Beiträge in Abhängigkeit zum Lebenswandel einer Person festzusetzen. Die Arbeit der Geheimdienste ist im Zusammenhang mit den Interessenskonflikten bzgl. des Schutz von personenbezogenen Daten im Zuge der 4. Phase denkbar. Dazu zählt auch der Einsatz von Vorratsdatenspeicherung, sowie die möglichen Entwicklungen einer Gesellschaft durch Erschaffung von *gläsernen Bürgern*. Daran schließen sich das Grundrecht der Meinungsfreiheit bzw. die Bedeutung von Meinungspluralismus an, die Weichert in [Wei13] beschreibt.

Ergänzend zu der in Ansätzen vorhandenen Qualitätsbetrachtung von Software sind die Qualitätskontrollen durch Audits im Vergleich zu Open Source Projekten, sowie rechtlicher Fragestellungen. Diese können Urheberrechte und Creativ Commons betreffen, aber auch die Frage nach der Legalität des Einsatzes eines Smartphones als Wanze.

Die Liste möglicher Erweiterungen der Reihe ist lang und bietet noch weitere Ansatzpunkte zur Ausgestaltung. Begründet durch den zeitlichen Rahmen dieser Arbeit, ist eine genauere Betrachtung der Durchführbarkeit dieser Ideen leider nicht zu leisten.

[19] http://www.martinjakobs.de/pages/android-apps-programmieren.php Stand: 23.05.2015

Kapitel 4

Fazit

Für die von Kramer und Spaeing in [KS14] geforderte Begleitung der Schüler auf *ihrem Weg in die digitale Zukunft* [KS14, S. 372] kommt diese Unterrichtsreihe sehr spät. Bereits in den unteren Klassenstufen der Sek. I besitzen die Schüler eigene Smartphones und in Kontakt mit diesen Systemen kommen sie durch die Geräte von Eltern und Verwandten bereits deutlich früher. Besonders in Anbetracht der Tatsache, dass gerade die Jüngeren die Sicherheit ihrer Daten am höchsten einstufen.

Die enormen Anstrengungen, die seit knapp zehn Jahren zur Aufnahme des Faches Informatik in den Kanon der Pflichtfächer unternommen werden, zeigen deutlich, dass eine engere Verzahnung des Datenschutzes in den Schulunterricht voraussichtlich noch längere Zeit auf sich warten lassen wird. Darüber hinaus ist ein politischer Wille dazu nur in überschaubarem Rahmen zu erkennen. Einzig die Datenschutzbeauftragten des Bundes und der Länder zeigen Bemühungen dazu. Der Datenschutz als Teil des politisches Programm wurde seit dem Ausscheiden der FDP aus dem Bundestag in Ansätzen von Bündnis 90/ Die Grünen übernommen. Deren Gestaltungsmöglichkeiten sind als Oppositionspartei jedoch limitiert. Derweil befürworten die Regierungsparteien CDU und CSU bspw. die Vorratsdatenspeicherung und richten sich damit gegen die Ziele des Datenschutzes.

Die Schulen werden nach Wagner [Wag12] durch die digitalen Entwicklungen vor große Herausforderung gestellt, denn durch den fehlenden politischen Willen müssen sie selbstständig versuchen neue Inhalte zum Erlernen der nötigen Kompetenzen in den bereits vorhanden Fächern unterzubringen. Das Be-

handeln neuer Inhalte geht allerdings in der Regel mit einem Verzicht auf bestehende Inhalte einher. Darüber hinaus fehlt es vielen Lehrern an der fachlichen Expertise, sodass bisherige Anstrengungen meist nur eine Anpassung von Verhaltenshinweisen bzw. Ratschläge zur Datenvermeidung beinhalten. Es Bedarf angemessener Aus- und Weiterbildung der Lehrkräfte, sowie eine Aufnahme datenschutzrechtlicher Themen in allen Fächern der Sek. I. Dies soll nicht bedeuten, dass der Datenschutz zwanghaft in alle Unterrichtsthemen eingebunden werden muss, sinnvolle Möglichkeiten zur Einbindung sollten jedoch genutzt werden.

Allerdings werden sich selbst durch etwaige Anpassungen der Lehrpläne niemals alle Fragen des Datenschutzes und der Datensicherheit innerhalb des Unterrichts behandeln lassen. Dies ist alleine der stetigen Weiterentwicklung von Informationstechnik geschuldet. Der Anteil der Fächer an der von Wagner genannten Bildungsaufgabe muss es daher sein, den Schülern eine angemessene Grundlage an die Hand zu geben. Die innerhalb des späteren Berufs notwendigen Vertiefungen müssen die entsprechenden Bildungseinrichtungen bzw. Betriebe übernehmen.

Obwohl er zunächst überwiegend in der Oberstufe zum Einsatz kommen wird, soll der vorliegende Kontext zu Erfüllung dieser Bildungsaufgabe beitragen. Die Schüler sollen mit ihm lernen die Welt durch die *informatische Brille* zu sehen. Die Selbstverständlichkeit der Nutzung von Informatiksystemen bedarf einer Aufklärung der Nutzer. Da durch die ständige Weiterentwicklung Anwenderschulungen unzureichend sind, geht es daher um das Verständnis des Zusammenspiels von Informatiksystemen. Die immer weiter voranschreitende Vernetzung mit Hilfe des Internets, das *Internet der Dinge*, birgt bei unzureichenden Sicherheitsmaßnamen oder unsachgemäßer Handhabung viele Risiken. Da zum jetzigen Zeitpunkt nur eine begrenzte Anzahl von Schülern durch den Informatikunterricht erreicht werden, ist das Initiieren des Peer-to-Peer Lernens von entscheidender Bedeutung. Dadurch kann auch bei den übrigen Schülern eine Steigerung ihrer Kompetenzen erzielt werden. Ggf. wird durch die aktiven Elemente auch das Image der Informatik verbessert. Das Thema Datenschutz bietet im Vergleich zu anderen informatischen Themen, wie bspw. dem Programmieren, einen deutlich weniger abstrakten bzw. kompliziert wirkenden Zugang zu dem Fachgebiet.

Ob die Unterrichtsreihe den gesteckten Zielen gerecht werden, wird sich erst nach praktischen Erprobungen zeigen. Im Zusammenhand damit wird sich zei-

gen, ob die aktiven Elemente der Reihe ausreichen, um das Peer-to-Peer Lernen anzuregen und die Anreize für eine weitere Beschäftigung mit den Inhalten groß genug sind. Besonders die Nutzung der *WhatsApp*-Alternativen als dauerhafter Ersatz für diese App könnte durch äußere Faktoren verhindert werden. So macht es besonders für Schüler nur eingeschränkt Sinn eine Kommunikations-Applikation zu nutzen, mit der man nur einen geringen Teil seines Freundeskreises erreichen kann. In Zusammenarbeit mit den Schülern müssen anschließend ggf. notwendige Anpassungen durchgeführt werden, um den Kompetenzzuwachs der Schüler zu optimieren. Zur Disposition stehen bspw. die angewendeten Methoden und Sozialformen. Auch die Anzahl der eingebundenen Videos könnte für diesen Zeitraum zu hoch sein. Nach erfolgreicher Erprobung und Verbesserung sollte die Reihe um einige der in 3.3 genannten Themen erweitert werden, da das Potential des Kontextes durch den starken Lebensweltbezug sehr groß ist. Es sollte jedoch vermieden werden alle Unterrichtsthemen ausschließlich in Kontexte unterrichten zu wollen, immer gleiche Methoden und Vorgehensweisen langweilen die Lernenden auf Dauer. Abschließend bleibt zu hoffen, dass die Schüler mit den in dieser Reihe erworbenen Kompetenzen ihr Verhalten bzgl. Datenschutz und Datensicherheit im positiven Sinne anpassen und ihren Altersgenossen als Vorbilder dienen.

Literaturverzeichnis

[BDDP15] BERENDT, Bettina ; DETTMAR, Gebhard ; DEMIR, Cihan ; PEETZ, Thomas: Kostenlos ist nicht kostenfrei. In: *LOG IN Heft Nr. 178/179, Seiten 41 - 56* (2015)

[BP14] BECKER, Arno ; PANT, Marcus: *Android 4.4, 3. aktualiserte und erweiterte Auflage*. dpunkt.verlag, 2014

[BRRR13] BODDEN, Prof. Dr. E. ; RASTHOFER, Siegfried ; RICHTER, Dr. P. ; ROSSNAGEL, Prof. Dr. A.: Schutzmaßnahmen gegen datenschutzunfreundliche Smartphone-Apps. In: *DuD - Datenschutz und Datensicherheit, Ausgabe 10, Seiten 671 - 674* (2013)

[DKW11] DIETHEM, Ira ; KOUBEK, Jochen ; WITTEN, Helmut: IniK - Informatik im Kontext. In: *LOG IN Heft Nr. 169/170, Seiten 97 - 105* (2011)

[DuD14] Kaspersky Lab: Sicherheitsregeln beim Download, der Verwaltung und Nutzung von Apps. In: *DuD - Datenschutz und Datensicherheit, Ausgabe 8, Seite 574* (2014)

[Eck13] ECKERT, Prof. Dr. C.: *IT-Sicherheit, 8. aktualisierte und korrigierte Auflage*. Oldenburg Verlag München, 2013

[ES15] EIKENBERG, Ronald ; SCHMIDT, Jürgen: WhatsApp entschlüsselt. In: *c't - Magazin für computer technik, Ausgabe 11 , S. 88* (2015)

[Fil08] FILECCIA, Marco: Knowhow für junge User. In: *Materialien für den Unterricht, 2. Auflage, klicksafe.de* (2008)

[FPR14] FEIERABEND, Sabine ; PLANKENHORN, Theresa ; RATHGEB, Thomas: JIM Studie 2014 - Jugend, Information, (Multi-) Media / Medienpädagogischer Forschungsverbund Südwest. 2014. – Forschungsbericht

[Hoo12] HOOG, Andrew: *Android Forensik - Datenrecherche, Analyse und mobile Sicherheit bei Android*. Franzis Verlag GmbH, München, 2012

[Ini] www.informatik-im-kontext.de Stand: 13.03.2015

[JF14] JADIN, Tanja ; FARTHOFER, Romana: Endverwendungsnachweis für Projekt SPA 04/196 "Netkompass für Social Web" / FH Oberösterreich, Fakultät für Informatik, Kommunikation und Medien, Hagenberg. 2014. – Forschungsbericht

[KRF11] KREUTZER, Dr. T. ; RACK, Stefanie ; FILECCIA, Marco: Nicht alles, was geht, ist auch erlaubt. In: *Materialien für den Unterricht, klicksafe.de* (2011)

[KS14] KRAMER, Rudi ; SPAEING, Frank: "Datenschutz geht zur Schule" - was Hänschen nicht lernt... In: *DuD - Datenschutz und Datensicherheit, Ausgabe 6, Seiten 370 - 374* (2014)

[KSSW09] KOUBEK, Jochen ; SCHULTE, Carsten ; SCHULZE, Peter ; WITTEN, Helmut: Informatik im Kontext (IniK). In: *Lecture Notes in Informatics, Zukunft braucht Herkunft, 25 Jahre INFOS - Informatik an Schulen, S. 268 - 279* (2009)

[Mes14] MESTER, Britta A.: Aufklärung - eine Aufgabe des Datenschutzes? In: *DuD - Datenschutz und Datensicherheit, Ausgabe 6, Seite 361* (2014)

[PBP14] PETERSEN, Dominique ; BARCHNICKI, Sebastian ; POHLMANN, Norbert: Schutz- und Frühwarnsysteme für mobile Anwendungen. In: *DuD - Datenschutz und Datensicherheit, Ausgabe 1, Seiten 7 - 14* (2014)

[Pro] www.projekt-datenschutz.de Stand: 20.03.2015

[Wag12] WAGNER, Edgar: Datenschutz als Bildungsauftrag. In: *DuD - Datenschutz und Datensicherheit, Ausgabe 2, Seiten 83 - 87* (2012)

[Wei13] WEICHERT, Thilo: Big Data - eine Herausforderung für den Datenschutz. In: *Big Data - Das neue Versprechen der Allwissenheit, edition unseld, Seiten 131 - 148* (2013)