Ergebnisbericht des Work-streams „Update4Schule“

Studie zu Wissen und Fähigkeiten von Schüler:innen und Lehrer:innen im Bereich Cyber-Sicherheit und Ideensammlung für Bildungsangebote

„Dialog für Cyber-Sicherheit“

Ein Projekt im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Informationen zum Produkt

Dieser Bericht wurde im Rahmen des Projekts „Dialog für Cyber-Sicherheit“ von Juli 2021 bis März 2022 erarbeitet.

Ideengeber des Workstreams waren: Karin Wilhelm (BSI) und Jörg Schüler (Digitale Helden gGmbH), Dominik George (Teckids e.V.)

Mitwirkende Teilnehmer:innen des Workstreams waren: Jörg Schüler (Digitale Helden gGmbH), Mirko de Paoli (Bundesverband Smart City e.V.), Patrick Luzina (Bits & Bäume), Markus Dölle (AK Usable Security & Privacy), Michaela Brauburger (medien-sinnvoll-nutzen.de), Karin Wilhelm (BSI), Harald Niggemann (BSI), Steffen Haschler (CCC Mannheim - assoziierter Berater)

Beteiligte Mitarbeiter:innen der Geschäftsstelle am nexus Institut waren: Justine Kenzler, Eva Sheperd, Franziska Detsch

Der Dialog für Cyber-Sicherheit ist ein Projekt des Bundesamtes für Sicherheit in der Informationstechnik (BSI), das vom Think Tank iRights.Lab und dem nexus Institut durchgeführt wird. Die Auftragnehmer haben dazu eine Geschäftsstelle eingerichtet.

Der Workstream „Update4Schule“, in dem dieser Bericht entstanden ist, wurde im Rahmen eines partizipativen und offenen Austauschs von der Geschäftsstelle und interessierten Dialogpartner:innen (s.o. Ideengeber:innen und mitwirkende Teilnehmer:Innen) durchgeführt. Die Dialogpartner:innen haben das Thema aus dem Bereich Cyber-Sicherheit für den Workstream selbst gewählt.

Das vorliegende Bericht wurde von der Geschäftsstelle und den Workstream-Teilnehmer:innen eigenständig erarbeitet. Die dort wiedergegebenen Ansichten spiegeln nicht zwangsläufig die Ansicht des BSI wider. Das BSI verfolgt mit dem Projekt das Ziel, einen offenen gesellschaftlichen Diskurs zum Thema IT-/Cyber-Sicherheit sowie damit verwandter gesellschaftlicher Themen zu ermöglichen. Das Projekt soll daher ausdrücklich den verschiedenen Meinungen und Ansätzen zur Annäherung an das Thema Cyber-Sicherheit aus Sicht der Zivilgesellschaft Raum und die Möglichkeit zum Austausch geben, ohne dies durch eine engmaschige Steuerung des BSI zu beschränken.

Weitere Informationen zum „Dialog für Cyber-Sicherheit“:
www.dialog-cybersicherheit.de
Kontakt Geschäftsstelle (iRights.Lab und nexus Institut):
kontakt@dialog-cybersicherheit.de

Stand: April 2022

Ein Projekt im Auftrag des:

iRights.Lab
Think Tank für die digitale Welt

nexus

Bundesamt für Sicherheit in der Informationstechnik

Executive Summary

Die vorliegende qualitative Studie ist im Rahmen des Projektes „Dialog für Cyber-Sicherheit“ im Workstream „Update4Schule“ entstanden. Sie befasst sich aufgrund der marginalen empirischen Datenlage mit der Erforschung des Wissensstands, der Kompetenzen und Sensibilität von Schüler:innen und Lehrer:innen in Deutschland zum Thema Cyber- und Datensicherheit.

Die Studie zeigt auf, dass grundlegende Begrifflichkeiten und Thematiken zu Cyber- und Datensicherheit sowohl Schüler:innen als auch Lehrer:innen bekannt sind, jedoch die zugrundeliegenden – und oft komplexeren – Zusammenhänge meist nicht erklärt werden können. Das führt im Verhalten und auch bewussten Handeln der Befragten nicht selten dazu, dass IT-Sicherheit im Umgang mit ihren digitalen Geräten und ihren Daten eine eher untergeordnete Rolle spielt. Vor allem bei den Handlungsmöglichkeiten zum Selbst- und Fremdschutz (Prävention von Cyber-Angriffen) oder nach einem Cyber-Sicherheitsangriff auf das eigene Gerät weisen die Befragten Wissenslücken auf.

Die Teilnehmer:innen der Befragung sowie die am Workstream beteiligten Expert:innen stimmen darin überein, dass Angebote zu Cyber- und Datensicherheit in der schulischen Bildung bislang massiv unterrepräsentiert sind und dass technische Expertise aufgebaut werden muss. Eine Forderung für ein mögliches Folge-Projekt von „Update4Schule“ besteht daher darin, bestehende Angebote zu sichten, zu vernetzen und weiterzuentwickeln sowie finanziell besser auszustatten. Bei der Entwicklung von Lehr-/Lernangeboten sollte außerdem darauf geachtet werden, interaktive und realitätsnahe Formate zu entwerfen und die Zielgruppen bei der Konzeption aktiv mitwirken zu lassen. Dafür wurden im Workstream erste Ideen gesammelt und in dieser Studie festgehalten.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Hintergrund des Workstreams „Update4Schule“

Die voranschreitende Digitalisierung in allen Lebensbereichen wirkt sich besonders stark auf den Lebensalltag von Kindern und Jugendlichen aus: Jugendliche in Deutschland im Alter von 12 bis 19 Jahren verbringen mehr und mehr Zeit im Internet - im Jahr 2021 durchschnittlich rund 241 Minuten am Tag. Im Vorjahr 2020 wurde sogar ein Höchstwert von 258 Minuten täglich erreicht – was wahrscheinlich auch auf den Befragungszeitpunkt zurückführen ist, denn so waren im Sommer 2021 wieder mehr Freizeitaktivitäten möglich und auch Kontaktbeschränkungen waren gelockert[1]. Trotzdem war die Corona-Pandemie nicht beendet und somit keine vollständige Normalität im Alltag der Jugendlichen möglich[2]. Ganze 95% der Jugendlichen nutzen das Internet auch in ihrer Freizeit täglich[3], welches eine immer größer werdende Rolle im Leben junger Menschen in Deutschland spielt.

Wissen und Kompetenzen im Bereich Cyber- und Datensicherheit sind auch für Kinder und Jugendliche bereits von großer Bedeutung. Sie nutzen früh digitale Geräte und Anwendungen und können dementsprechend auch Opfer von Cyber-Kriminalität, wie beispielsweise Identitätsdiebstahl und Betrug werden. Cyber- und Datensicherheit sollten daher auch in der schulischen und außerschulischen Bildung mitgedacht werden, um Kinder und Jugendliche zu sensibilisieren und dabei zu unterstützen, frühzeitig digitale Kompetenzen aufzubauen. Cyber-Sicherheit auch bereits im schulischen Bildungsbereich mitzudenken, fordert u.a. die Kultusministerkonferenz[4] und verschiedene Bundesländer versuchen, dies bereits in unterschiedlichsten Formaten in den Schulalltag zu integrieren[5].

Während es bereits Studien zum Wissensstand und Vertrauen im Internet von Erwachsenen gibt[6], finden sich kaum empirische Befunde zu Wissen und Kompetenzen von Schüler:innen und Lehrer:innen beim Thema Cyber- und Datensicherheit. Es ist unklar, welche Fähigkeiten und Erfahrungen Schüler:innen im sicheren Umgang mit Informationstechnik haben oder inwieweit Lehrer:innen ausreichend für die sicherheitsrelevanten Anforderungen der zunehmenden Digitalisierung in Ausbildung und Beruf sensibilisiert sind.

Der Workstream „Update4Schule“ widmete sich daher von Juli 2021 bis März 2022 der empirischen Untersuchung des Bewusstseins und der Bedarfe von Schüler:innen und Lehrer:innen zum Thema Cyber- und Datensicherheit. Die Arbeitsgruppe wurde im Rahmen der „Denkwerkstatt Sichere Informationsgesellschaft“ 2021 von mehreren Stakeholdern ins Leben gerufen. Sie ist damit Teil des „Dialogs für Cyber-Sicherheit“, einem Projekt, das vom nexus Institut und

[1] JIM-Studie (2021): https://www.mpfs.de/fileadmin/files/Studien/JIM/2021/JIM-Studie_2021_barrierefrei.pdf
[2] JIM-Studie (2021): https://www.mpfs.de/fileadmin/files/Studien/JIM/2021/JIM-Studie_2021_barrierefrei.pdf
[3] JIM-Studie (2021): https://www.mpfs.de/fileadmin/files/Studien/JIM/2021/JIM-Studie_2021_barrierefrei.pdf
[4] Strategie der Kultusministerkonferenz „Bildung in der digitalen Welt“ (2017): https://www.kmk.org/fileadmin/pdf/PresseUndAktuelles/2018/Digitalstrategie_2017_mit_Weiterbildung.pdf
[5] Digital? Aber sicher! – Hacker-Experten kommen an Sachsens Schulen (2022): https://www.medienservice.sachsen.de/medien/news/1037296
[6] vgl. Bitkom (2012). Vertrauen und Sicherheit im Netz: https://www.bitkom.org/sites/main/files/file/import/Vertrauen-und-Sicherheit-im-Netz.pdf
DIVSI (2012). Milieu-Studie zu Vertrauen und Sicherheit im Internet: https://www.divsi.de/publikationen/studien/divsi-milieu-studie/einstellungen-zum-thema-vertrauen-und-sicherheit-im-internet-in-der-bevoelkerung-2/index.html

dem iRights.Lab im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) durchgeführt wird.

1.2 Ziele und Fragestellungen

Aufgrund der geschilderten Ausgangslage war es das Ziel des Workstreams „Update4Schule“, eine erste explorative Untersuchung des Wissensstandes von Schüler:innen und Lehrer:innen durchzuführen. Mittels einer qualitativen Datenerhebung an deutschen Schulen zum Thema Cyber-Sicherheit und Datensicherheit in Form von Fokusgruppeninterviews sollten das Wissen, die Erfahrungen und Fähigkeiten sowie die Bedarfe an Bildungsangeboten ermittelt werden. Die langfristige Vision des Workstreams ist es, dass Cyber- und Datensicherheit perspektivisch ein höherer Stellenwert in der Schulbildung eingeräumt wird.

Die Ergebnisse der Studie und die daraus ableitbaren Handlungsempfehlungen richten sich an verschiedene Akteure der Bildungslandschaft und sollen für die Thematik sensibilisieren und dabei unterstützen, zielgruppengerechte Bildungsangebote zu fördern, zu entwickeln und umzusetzen. Gleichzeitig können die Erkenntnisse dieser explorativen Untersuchung als Ausgangspunkt für vertiefende qualitative und quantitative Erhebungen genutzt werden.

Folgende zentrale Fragestellungen sollen im Rahmen dieser Studie untersucht werden:

- Was ist der Wissensstand zum Thema Cyber-Sicherheit, Datensicherheit und Datenschutz bei Schüler:innen und Lehrer:innen in Deutschland?
- Wo sehen die Zielgruppen Wissensbedarfe bzw. Wissenslücken?
- Wie müssen Bildungsangebote gestaltet sein, um von den Zielgruppen optimal umgesetzt werden zu können?
- Welche Herausforderungen bestehen bzgl. der Umsetzung von (potenziellen) Bildungsangeboten vonseiten der Zielgruppen?

2 Methodisches Vorgehen

2.1 Studiendesign und Stakeholdermitwirkung

Die Studie wurde insgesamt in sieben Phasen umgesetzt. Die ehrenamtlich engagierten Workstream-Teilnehmer:innen haben an den verschiedenen Phasen in unterschiedlichen Funktionen teilgenommen. Dies wird in dem nachfolgenden Studiendesign anhand der orangefarbenen Pfeile abgebildet:

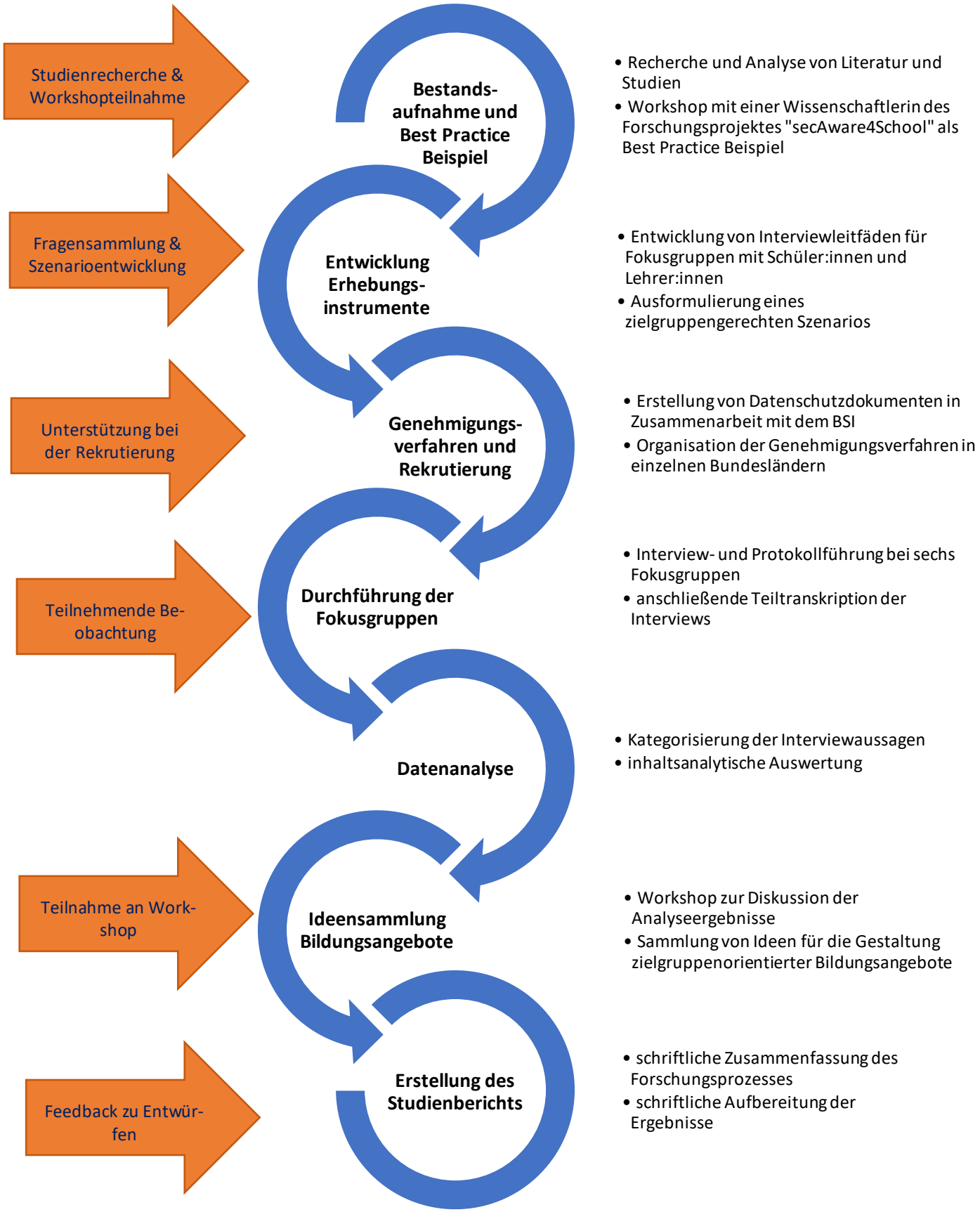

Abbildung 1: Forschungsdesign und Mitwirkung der Stakeholder:innen im Workstream „Update4Schule“

2.2 Recherche und Analyse von Sekundärdaten

Um einen besseren Überblick über die Wissensstände und Kompetenzen zum Thema Cyber- und Datensicherheit von Schüler:innen und Lehrer:innen in Deutschland zu erhalten, wurde im Vorfeld der eigenen empirischen Erhebung eine Bestandsaufnahme in Form einer stichprobenartigen Literatur- und Studienrecherche vorgenommen.

Die Recherche nach empirischen Befunden erfolgte über übliche Suchmaschinen (z.B. Google, DuckDuckGo), spezialisierte Suchmaschinen für Wissenschaftsliteratur (z.B. ResearchGate, Google Scholar) und Universitätsbibliothekskataloge. Eingesetzt wurden unterschiedliche, im Rahmen des Workstreams mit den Teilnehmenden identifizierte Suchbegriffe in unterschiedlichen Kombinationen. In folgender Abbildung sind die verwendeten Suchbegriffe gelistet:

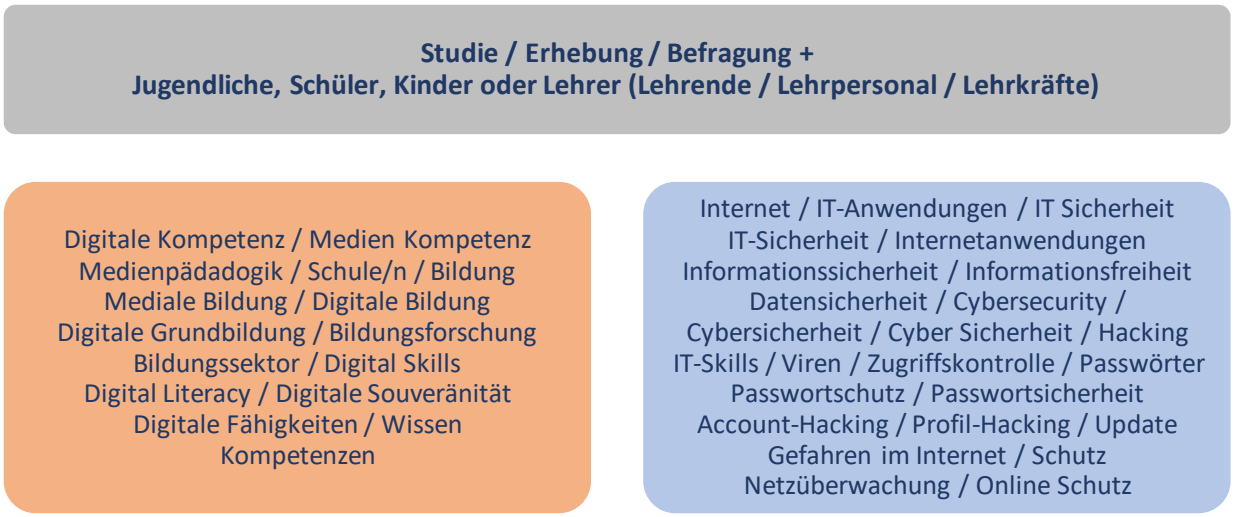

Abbildung 2: Sekundärdatenrecherche - Suchbegriffe und -kombinationen

Es wurden über 40 Studien, Berichte und Dokumente gefunden, welche als möglicherweise relevant für die Fragestellungen erachtet wurden. Nach einem Vorab-Screening wurden 19 Studien davon ausgewählt und detaillierter betrachtet. Elf dieser Studien widmeten sich der Zielgruppe der Schüler:innen und acht enthielten empirische Befunde zur Zielgruppe Lehrkräfte. Die Analyse der recherchierten Studien ergab jedoch, dass es weder in der deutsch- noch in der englischsprachigen wissenschaftlichen Literatur dezidierte qualitative oder quantitative Abfragen zum Wissen, zu den Kompetenzen oder zur Sensibilisierung von Schüler:innen und Lehrer:innen zum Thema Cyber- oder Datensicherheit gibt. Lediglich in der D21-Sonderstudie Schule Digital 2016[7] und im Onlinefragebogen[8] des Projektes der Technischen Universität Wildau „SecAware4School[9]“ wurde das Thema Cyber-Sicherheit anhand mehrerer Items

[7] vgl. Initiative D21 e. V. (2016): Sonderstudie „Schule Digital“. Lernwelt, Lehrwelt, Lebenswelt: Digitale Bildung im Dreieck Schüler:innen, Eltern, Lehrkräfte. Abrufbar unter: https://initiative21.de/publikationen/sonderstudie-schule-digital/

[8] vgl. Schuktomow, R.; Scholl, M.; Gube, S.; Koppatz, P.; Edich, D.; Gerlach, J. (2020): Projektdokumentation Informationssicherheitsbewusstsein für den Schulalltag (SecAware4School). Scholl, M. (Hrsg.). Buchwelten-Verlag: Frankfurt am Main.

[9] https://secaware4school.wildau.biz/de.html

(Fragestellungen) aufgegriffen. Nachfolgend werden die für diese Studie relevanten Items und Ergebnisse dieser zwei Untersuchungen dargestellt.

Relevante Ergebnisse aus „D21 Sonderstudie Schule Digital 2016“

Für die Sonderstudie wurden zwischen August und September 2016 insgesamt 1.116 Schüler:innen weiterführender Schulen sowie deren Eltern (n=1.123) und Lehrkräfte (n=1.425) per Zufallsstichprobe ausgewählt und befragt.[10] Die Ergebnisse zeigen, dass 49% der Schüler:innen und 57% der Lehrer:innen technische Grundlagen (z.B. IT- und Datensicherheit sowie Verschlüsselung) als wichtiges Thema für die Vermittlung im Unterricht bewerten. Ein Bewusstsein für den Bedarf an Wissens- und Informationsvermittlung zu Cyber-Sicherheitsthemen ist folglich bei rund der Hälfte der Schüler:innen und Lehrer:innen vorhanden – und auch ethische Grundlagen und kritischer Umgang mit Digitalthemen (z.B. Datenschutz, gesellschaftliche Fragen) sowie rechtliche Grundlagen werden von jeweils 60% der Schüler:innen sowie 86% bzw. 78% der Lehrer:innen als relevant für den Unterricht erachtet. Im Gegensatz dazu bewerten nur 35% bzw. 25% der Schüler:innen Fähigkeiten wie Programmierkenntnisse und Fähigkeiten für Webseiten-Gestaltung als wichtig. Bei den Lehrer:innen liegen beide Themen sogar unter 20%.[11]

Im Umgang mit dem Internet äußern 9 von 10 Lehrer:innen, dass sie Antivirensoftware nutzen und diese regelmäßig aktualisieren. Rund 8 von 10 Schüler:innen stimmen dieser Aussage zu. Ebenfalls 9 von 10 Lehrer:innen stellen aus Datenschutzgründen nur wenige persönliche Daten von sich ins Netz, bei den Schüler:innen bestätigen dies 7 von 10 Befragten. Ihre Passwörter wechseln rund 4% der Lehrer:innen regelmäßig – mindestens alle drei Monate – bei den Schüler:innen tun dies 3%.[12]

Relevante Ergebnisse aus „secAware4school“

Das Projekt „SecAware4school“ wurde zwischen September 2018 und Dezember 2020 an der Technischen Hochschule Wildau durchgeführt. Die Zielsetzung war es, Schüler:innen, Lehrende und Eltern spielerisch im sorgsamen Umgang mit personenbezogenen Daten bei der Nutzung von Internetdiensten und sozialen Netzwerken zu schulen und ein Bewusstsein für das Thema Informationssicherheit zu schaffen. Fünf pilotierende Schulen in Berlin und Brandenburg wurden für die Umsetzung gewonnen. Am Projekt beteiligt waren ca. 600 Schüler:innen der Klassenstufen 6 bis 11 sowie 20 Lehrer:innen.

Einer der Meilensteine des Projektes war eine online durchgeführte „Umfrage zur Themenfindung“. Sie sollte dem Forschungsteam ermöglichen, den Wissensstand der Schüler:innen einzuschätzen und zu erfahren, für welche Themen sie sich interessieren.[13] Das Projektteam entwickelte einen Onlinefragebogen mit 9 Fragen, der an den 5 Pilotschulen zirkuliert wurde. Es wurden insgesamt 800 Fragebögen ausgewertet und eine Zusammenfassung der Ergebnisse im Abschlussbericht des Projektes veröffentlicht.

[10] vgl. Initiative D21 e. V. (2016): Sonderstudie „Schule Digital“. Lernwelt, Lehrwelt, Lebenswelt: Digitale Bildung im Dreieck Schüler:innen, Eltern, Lehrkräfte. S.7. Abrufbar unter: https://initiatived21.de/publikationen/sonderstudie-schule-digital/

[11] vgl. ebd. S.27

[12] vgl. ebd. S.21

[13] vgl. Schuktomow, R.; Scholl, M.; Gube, S.; Koppatz, P.; Edich, D.; Gerlach, J. (2020): Projektdokumentation Informationssicherheitsbewusstsein für den Schulalltag (SecAware4School). Scholl, M. (Hrsg.). Buchwelten-Verlag: Frankfurt am Main.

Eine Frage des Online-Fragebogens zielte auf die Merkmale eines sicheren Passwortes, spezifisch die als sicher geltende Anzahl der Zeichen, ab. Hier wählten 84% der Teilnehmer:innen (Schüler:innen, Lehrende und Eltern) aus den 3 möglichen Antworten die richtige mit „8 Zeichen“ (statt 5 oder 15 Zeichen) aus. In anschließenden Veranstaltungen mit den Zielgruppen stellte das Forschungsteam jedoch fest, dass geschätzt weniger als die Hälfte der Befragten tatsächlich ein Passwort mit 8 oder mehr Zeichen nutzt und eine Diskrepanz zwischen dem Wissen und dem Verhalten besteht.[14]

Eine weitere Frage untersuchte, ob die Proband:innen wussten, wie sie ihre Privatsphäre schützen können. Hierbei antworteten 54%, und damit die Mehrheit der Befragten, dass sie dies teilweise wüssten, 39% bejahten und 7% verneinten die Frage.[15]

Mit der Frage „Wurden Sie/wurdest Du schon mal Opfer von Datendiebstahl (z.B.: Anmeldedaten wurden gestohlen)?“ wurde in der Umfrage direkt auf die eigenen Erfahrungen mit Cyberkriminalität abgezielt. 72% der Befragten beantworteten diese Frage mit Nein, 17% waren sich nicht sicher und lediglich 11% bejahten diese Frage.[16]

Mit einer weiteren Frage wurde nach dem Interesse an 13 Themen der Informationssicherheit mittels einer vierstufigen Skala (sehr/mittel/wenig/gar nicht) gefragt[17]: Das größte Interesse galt dem Thema ‚Sichere Passwörter‘ (46%). Interessant ist hierbei, dass in später durchgeführten Veranstaltungen die Verwendung von Passwortmanagern meist verneint wurde und Schüler:innen nach eigenen Angaben nur eine geringe Anzahl von Passwörtern verwenden. Nur knapp dahinter stand das Interesse am Thema ‚Sichere Bedienung des Smartphones‘ (45%), gefolgt von ‚Schutzmaßnahmen gegenüber Gefahren im Internet‘ (41%). Für das Thema ‚Verschlüsselung (Methoden, um Informationen geheim zu halten)‘ gaben 39% und für ‚Social Engineering (Manipulation von Menschen, um an vertrauliche Informationen zu kommen)‘ 38,5% der Befragten ein sehr hohes Interesse an. Für ‚Sicheres Verhalten in Sozialen Netzwerken‘ zeigten 37,5% ein sehr hohes Interesse, gefolgt von ‚Alternativen zu bekannten Sozialen Netzwerken‘ (36%). Beim allgemein formulierten Item ‚Informationssicherheit (Schutz persönlicher Daten und Informationen)‘ zeigten nur 34% der Befragten ein sehr hohes Interesse, für ‚Phishing (Alles rund um E-Mail-Betrug)‘ sogar nur 31%. Das Forschungsteam von SecAware4School führt diese Ergebnisse darauf zurück, dass sie den bekannten Problemfeldern im Bereich Informationssicherheit entsprechen, die von Angreifern schon lange ausgenutzt werden und in denen sich die Anwender:innen daher benutzerfreundliche Lösungen für ihre Geräte wünschen.

2.3 Konzeption und Durchführung von Fokusgruppen-Interviews

Erhebungsinstrument Fokusgruppe

Die vorliegende Studie wurde in Form von Fokusgruppen-Befragungen durchgeführt. Fokusgruppen sind moderierte Gruppeninterviews, bei denen eine Kleingruppe mithilfe eines Leitfadens mit offenen Fragen zur Diskussion über ein bestimmtes Thema angeregt wird. Sie sind

[14] vgl. Schuktomow, R.; Scholl, M.; Gube, S.; Koppatz, P.; Edich, D.; Gerlach, J. (2020): Projektdokumentation Informationssicherheitsbewusstsein für den Schulalltag (SecAware4School). Scholl, M. (Hrsg.). Buchwelten-Verlag: Frankfurt am Main. S. 10

[15] vgl. ebd. S.11

[16] vgl. ebd. S. 13

[17] vgl. ebd. S.14f.

ein typisches und ressourcenschonendes Erhebungsinstrument für die Erkundung eines unbekannten Forschungsfeldes[18], wie etwa im vorliegenden Fall, wenn Erkenntnisse über den Wissensstand, die subjektive Risikowahrnehmung und die Erfahrungen von Proband:innen im Bereich Cyber-Sicherheit generiert werden sollen. Fokusgruppen sind darüber hinaus auch eine geeignete Methode in der partizipativen Forschung[19], denn der Einsatz dieses Forschungsinstruments dient neben dem Ziel des Erkenntnisgewinns auch dem Ermächtigungsprozess (Empowerment) der Teilnehmenden[20]. In der Ergebnisdarstellung wird darauf eingegangen, wie diese Wirkung in ersten Ansätzen bereits bei der Durchführung der Fokusgruppen zu bemerken war.

Leitfaden-Entwicklung

Gemeinsam mit den im Workstream aktiven Stakeholder:innen wurden für die Befragungen der Schüler:innen wie auch der Lehrkräfte jeweils szenariobasierte Leitfäden entwickelt (siehe Anhang). Durch verschiedene lebensweltnahe Szenarien, wie beispielsweise den Empfang eines Spam-Links, den Umgang mit einem von einem Virus infizierten Gerät oder einem Datenleck im Schulsetting, wurde anhand von rund 20 Leit- und Unterfragen eine Wissens-, Bewusstseins-, Verhaltens- und Bedarfsabfrage durchgeführt. Die Fragen wurden entlang übergeordneter Themenaspekte zu Cyber-Sicherheit entwickelt (z.B. Wissen um technische Zusammenhänge und Handlungsoptionen, Risikoverständnis, Informationsquellen), welche in Diskussionen der teilnehmenden Stakeholder:innen gemeinsam mit Expert:innen aus Forschung und dem BSI als besonders relevant für die explorative Erhebung identifiziert wurden.

Fallauswahl und Rekrutierung

Für die Rekrutierung von Teilnehmenden für die Schüler:innen-Fokusgruppen wurden Schulen in Sachsen-Anhalt, Nordrhein-Westfalen, Berlin und Hessen telefonisch und per E-Mail durch die Geschäftsstelle (nexus Institut), das BSI sowie teilnehmende Stakeholder:innen des Workstreams angefragt. Die Entscheidung für die Eingrenzung auf diese Bundesländer wurde aufgrund folgender Faktoren getroffen:

- günstiger Feldzugang zu Schulen aufgrund vorhandener beruflicher Kontakte der an der Durchführung beteiligten Organisationen
- Berücksichtigung einer möglichst kurzen Zeitspanne des offiziellen Genehmigungsverfahrens, um die Erhebung im zeitlichen Rahmen des Workstreams umsetzen zu können.

Ein weiteres Kriterium für die Fallauswahl der Schulen und die Auswahl der Teilnehmer:innen waren der Einbezug unterschiedlicher Schultypen (Gymnasium bzw. Gesamtschule / Realbzw. Hauptschule / Berufsschule), um hier eine mögliche Varianz in den Antworten erheben zu können. Die teilnehmenden Schüler:innen sollten sich zudem in der Jahrgangsstufe 9 und

[18] Schulz, M. (2012). Quick and easy!? Fokusgruppen in der angewandten Sozialwissenschaft. In Schulz et al. (Eds.), Fokusgruppen in der empirischen Sozialwissenschaft (pp. 9-10). Springer VS.

[19] Bär. G., Kasberg, A., Geers, S., Clar, C. (2020). Fokusgruppen in der partizipativen Forschung. In: Hartung, S., Wihofszky, P. & Wright, Michael T. Hrsg. (2020). Partizipative Forschung. Ein Forschungsansatz für Gesundheit und seine Methoden, S. 207 – 232. Wiesbaden: Springer VS.

[20] Bär. G., Kasberg, A., Geers, S., Clar, C. (2020). Fokusgruppen in der partizipativen Forschung. In: Hartung, S., Wihofszky, P. & Wright, Michael T. Hrsg. (2020). Partizipative Forschung. Ein Forschungsansatz für Gesundheit und seine Methoden, S. 207 – 232. Wiesbaden: Springer VS.

aufwärts (Sekundarstufe I) befinden, da über 90% der Jugendlichen in diesem Alter bereits ein Smartphone besitzen und eigenständig und weitestgehend autonom damit umgehen[21].

Es wurden von Februar bis März 2022 insgesamt fünf Schüler:innen-Fokusgruppen und eine Lehrer:innen-Fokusgruppe durchgeführt. Da sich die Rekrutierung von interessierten Schulen aufgrund der starken organisationalen Belastungen bedingt durch die Corona-Pandemie als sehr schwierig erwies, konnten die Schüler:innen-Fokusgruppen nur in den Bundesländern Sachsen-Anhalt und Nordrhein-Westfalen durchgeführt werden. Hinzu kam eine Fokusgruppe mit Lehrer:innen von unterschiedlichen Bundesländern und Schultypen. Ressourcenbedingt wurde in dieser Studie der Schwerpunkt auf die Untersuchung der Schüler:innen gelegt – eine extern möglichst heterogene Lehrer:innen-Fokusgruppe versprach hier daher den größten zusätzlichen Erkenntnisgewinn für diese Zielgruppe. Die Fokusgruppen hatten eine Dauer von 1,5 bis 2 Stunden und es nahmen jeweils zwischen fünf und elf Schüler:innen bzw. Lehrer:innen teil.

Zielgruppe	Bundesland	Schultyp	Alter TN	Anzahl TN
Schüler:innen	Sachsen-Anhalt	Berufsschule	16-20	7
Schüler:innen	Sachsen-Anhalt	Berufsschule	17-20	11
Schüler:innen	Sachsen-Anhalt	Gymnasium	14-15	6
Schüler:innen	Nordrhein-Westfalen	Gesamtschule	15-16	6
Schüler:innen	Nordrhein-Westfalen	Gymnasium	14-16	6
Lehrer:innen	Berlin, Sachsen-Anhalt, Nordrhein-Westfalen	Berufsschule, Gesamtschule, Gymnasium	k.E.	5

Tabelle 1: Charakteristika der rekrutierten Fokusgruppen

2.4 Auswertungsmethodik

Die Fokusgruppeninterviews wurden per Videokonferenz von einer geschulten Interviewerin des nexus Instituts anhand des szenariobasierten Leitfadens geführt. Die Gesprächsinhalte wurden parallel durch eine wissenschaftliche Mitarbeiterin stichpunktartig protokolliert. Zudem wurden die Fokusgruppen-Interviews für die weiterführende wissenschaftliche Auswertung als Audioaufnahme aufgezeichnet und im Nachgang aus datenschutzrechtlichen Gründen gelöscht. Die Gesprächsprotokolle wurden im Nachgang durch einen erneuten Abgleich mit den digitale Audioaufzeichnung ergänzt und finalisiert. Zudem wurden zentrale Zitate transkribiert. Diese Verfahrensweise wird typischerweise bei wissenschaftlich begleiteten Gruppendiskussionen, die anhand eines Leitfadens geführt wurden, angewendet.[22]

Die Auswertung der Fokusgruppen-Interviews erfolgte anhand des inhaltsanalytischen Vorgehens[23]. Dieses beinhaltet die Identifikation zentraler Themen und Aspekte des Gesprächs sowie eine Beschreibung, Einordnung und Erklärung der verschiedenen Aussagen[24]: Anhand

[21] Kinder bekommen zwischen 6 und 11 Jahren am häufigsten ihr erstes Smartphone. YouGov. https://yougov.de/news/2021/11/25/kinder-bekommen-zwischen-6-und-11-jahren-am-haufig/

[22] Ruddat, M. (2012). Auswertung von Fokusgruppen mittels Zusammenfassung zentraler Diskussionsaspekte. In Schulz et al. (Eds.), Fokusgruppen in der empirischen Sozialwissenschaft (pp. 9-10). Springer VS.

[23] Mayring, P. & Fenzl, T. (2019). Qualitative Inhaltsanalyse. In N. Baur & J. Blasius (Hrsg.), Handbuch Methoden der empirischen Sozialforschung (pp.633-637). Springer, https://doi.org/10.1007/978-3-658-21308-4_42

[24] Schulz, M. (2012). Quick and easy!? Fokusgruppen in der angewandten Sozialwissenschaft. In Schulz et al. (Eds.), Fokusgruppen in der empirischen Sozialwissenschaft (pp. 9-10). Springer VS.

der Leitfragen der Interviewleitfäden wurden dazu in einem ersten Schritt die grundlegenden Antwortkategorien für die Analyse gebildet und Aussagen der Teilnehmer:innen wurden diesen Kategorien in einer tabellarischen Übersicht zugeordnet (deduktives Kodieren). In den Gesprächsprotokollen darüber hinaus identifizierte relevante inhaltliche Aspekte wurden in einem zweiten Schritt in neu gebildeten Kategorien aufgenommen (induktives Kodieren). Die folgende Abbildung zeigt das Vorgehen der Analyse:

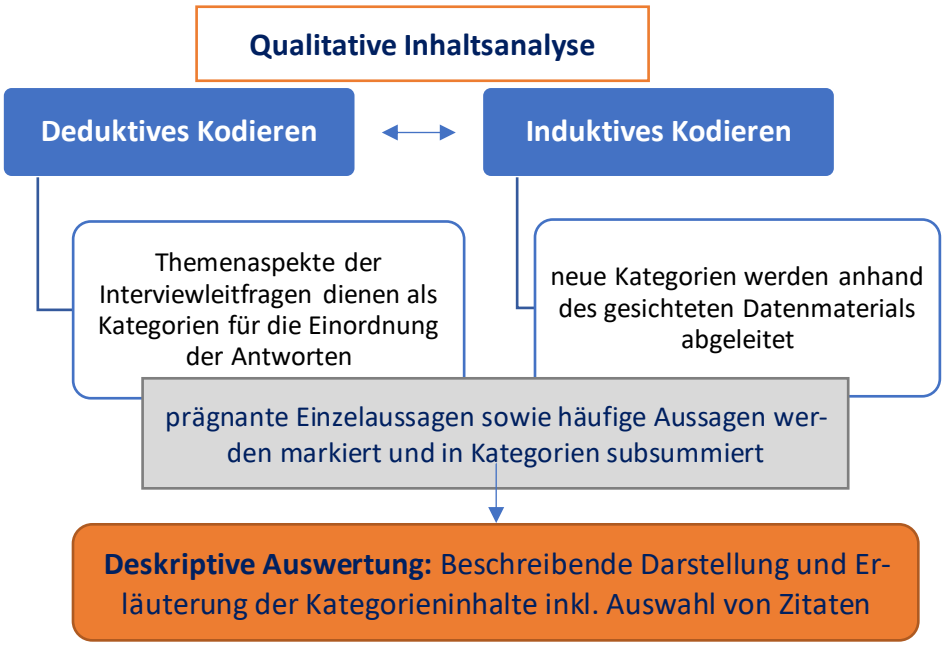

Abbildung 3: Ablauf Qualitative Inhaltsanalyse

3 Forschungsergebnisse

3.1 Einführung in die Ergebnisse

Die Fokusgruppenleitfäden orientieren sich an den drei Grundwerten der Informationssicherheit: Vertraulichkeit, Integrität (Unverfälschtheit) und Verfügbarkeit. Alle drei Grundwerte finden sich in unterschiedlichen Graden in den Leitfäden wieder. Aus den Vorgesprächen mit den Workstream-Teilnehmenden und Expert:innen ergaben sich folgende Kategorien, zu denen Leitfragen entwickelt wurden:

- Wissen zum Themenfeld
- persönliche Risikowahrnehmung im digitalen Raum
- Erfahrungen mit Sicherheitsvorfällen
- Informationsquellen zu Cyber- und Datensicherheit
- persönliche Bedeutung von Cyber- und Datensicherheit
- Handlungsoptionen für sichere Internetnutzung
- Ideen für Bildungsangebote zu Cyber-Sicherheit

Von Interesse waren Einsichten in den Umgang mit unterschiedlichen Internetanwendungen (z.B. Apps generell, Webseiten, spezifische Soziale Netzwerke) und Geräten wie u.a. Smartphone, Laptop, Tablet und PC im schulischen, wie im privaten Bereich.

Die Herausforderung bei der Analyse von Fokusgruppen-Interviews ist es, einen bestimmten Gruppentonus herauszufiltern und nicht einzelnen Stimmen besonders viel Gewicht zu geben. Dabei ist an dieser Stelle anzumerken, dass in jeder Gruppe mindestens eine Person ein besonders tiefgehendes Wissen im Bereich der Technik im Allgemeinen – wie der Cyber-Sicherheit im Spezifischen – aufwies. Genauso gab es in jeder Gruppe einzelne Schüler:innen, die sich nur sehr oberflächlich mit den abgefragten Themen auskannten. Ziel der Inhaltsanalyse ist es, einen Querschnitt der unterschiedlichen Perspektiven abzubilden und die Differenzen herauszuarbeiten.

Die befragten Schüler:innen-Gruppen zeichneten sich durch einen hohen Grad an Heterogenität aus: Durch unterschiedliche Lehrpläne der Bundesländer, verschiedene beteiligte Schulformen und die Diversität der sozialen Hintergründe der Teilnehmenden konnte ein breites Spektrum der empirischen Lage abgedeckt werden. Besonders auffällig war, dass trotz einiger sprachlicher Hürden, insbesondere bei Nicht-Muttersprachler:innen, sowie sehr unterschiedlicher technischer Voraussetzungen für die digitale Befragung alle Gruppen ein großes Interesse und Engagement (z.T. nach der regulären Schulzeit) für die Befragung zeigten.

Die im Rahmen einer Fokusgruppe gemeinsam befragten Lehrer:innen unterrichteten in unterschiedlichen Bundesländern und Schulformen und waren relativ heterogen hinsichtlich der Altersstruktur und des IT-Kompetenzlevels.

Für die Lehrer:innen-Gruppe wurde der Leitfaden für die Befragung nur leicht angepasst, die Fragen blieben aber grundlegend bestehen. Im Folgenden werden die Ergebnisse der Befragung der Schüler:innen und Lehrer:innen getrennt vorgestellt. Die Ergebnisse der deskriptiven Analyse werden anhand von anschaulichen Zitaten aus den Befragungen ergänzt, um die Teilnehmenden mit ihren ganz persönlichen Perspektiven und Meinungen zu Wort kommen zu lassen.

3.2 Wissen und Risikosensibilität von Schüler:innen

Was ist Cyber-Sicherheit?

Auf die Frage, was für sie Cyber-Sicherheit bedeutet, haben die Teilnehmer:innen sehr unterschiedliche Antworten gegeben. Diese reichten von „ich habe keine Ahnung, was das heißt“, über „dass man sicher durchs Internet geht“ bis hin zu „vor Viren schützen und vor fremdem Eingriff auf das eigene Gerät schützen und die eigenen Daten schützen“. Bereits bei dieser Einstiegsfrage zeigte sich somit das Spektrum des Wissens über die Fokusgruppen hinweg aber auch innerhalb derselbigen.

Privatsphäre und Datendiebstahl

Im Szenario des Fokusgruppenleitfadens war der Ausgangspunkt, dass Daten im schulischen wie im privaten Bereich durch ein Datenleck bzw. einen Hack offen im Internet verfügbar sind. Personenbezogene Daten, wie unter anderem Name, E-Mail-Adresse, Wohnort, Geburtsdatum und Klasse, die bei einem Angriff auf die Schulplattform öffentlich zugänglich wären, wurden von den Schüler:innen aufgezählt aber überwiegend nicht als besonders schützenswert

eingestuft: Zwar war das Wissen um die Existenz dieser personenbezogenen Daten im digitalen Raum in den meisten Fällen vorhanden, eine Sensibilität für das Risiko, welches entstehen kann, wenn diese Informationen ungeschützt im Internet kursieren, wiesen jedoch nur wenige der befragten Schüler:innen auf. Dies verdeutlichen die folgenden zwei Beiträge:

„Ich habe nichts zu verbergen."

„Was sollen Leute denn mit meiner Adresse?"

Weitaus stärker war das Risikobewusstsein der Schüler:innen hingegen dann vorhanden, wenn es um den Diebstahl und die Veröffentlichung von privaten Nachrichten, Chatverläufen und Bildern sowie Daten und Kommunikationsverläufe aus den Sozialen Netzwerken ging. So äußern sich zwei Teilnehmende:

„Wenn jemand sagt ‚Ich habe dein E-Mail-Passwort' […] ja, private Sachen finde ich viel schlimmer, als irgendwelche Passwörter, weil Passwörter sind änderbar. Aber private Sachen sind halt privat."

„Ich fände es wirklich unangenehm, wenn irgendwelche Menschen darauf zugreifen könnten, was ich gegoogelt habe, wann ich es gegoogelt habe und welche Internetseiten ich nutze."

An mehreren Stellen in den Gesprächen wurde deutlich, dass Privatsphäre bei den Schüler:innen im privaten Bereich einen besonders hohen Stellenwert hat und als äußerst schützenswert wahrgenommen wird. Es kann daher eine Diskrepanz hinsichtlich des Risikobewusstseins zwischen den als ‚persönlich' wahrgenommenen Daten und personenbezogenen sowie weiteren Daten, die explizit im schulischen Kontext anfallen, festgestellt werden: So wurde der Zugriff Externer auf schulische Inhalte (z.B. Hausaufgaben, Chatverläufe mit Lehrkräften, Noten, Stundenpläne) – wie auch bei den personenbezogenen Daten – ebenfalls als wenig bis gar nicht sicherheitskritisch eingestuft. Nur wenige Schüler:innen waren der Ansicht, dass anhand der auf einer Schulplattform verfügbaren Daten ein ernsthafter Schaden angerichtet werden könne.

Anspruch an Sicherheit von schulischen Tools

Einige Schüler:innen formulierten einen hohen Sicherheitsanspruch an ihre Schulen und die zur Verfügung gestellten Online-Dienste, wie z.B. Lernplattformen. Sie schenkten der Institution Schule und den jeweilig genutzten Anbietern von Software-Tools grundlegendes Vertrauen. Die Möglichkeit eines effektiven Angriffs auf die dort hinterlegten Daten wurde daher oft als nicht realistisch wahrgenommen. Entsprechend groß wäre aus Sicht einiger der befragten Schüler:innen die Empörung, wenn die eigene Schule und der von ihr bereitgestellte Online-Dienst keine ausreichende Sicherheit gewährleisten würden. Insbesondere weil die Nutzung der Online-Tools für die Teilnahme am Schulalltag oft verpflichtend sei, wurde ein unzureichendes Sicherheitsniveau hier als besonders kritisch empfunden.

Monetarisierung von Daten

In den Interviews wurde auch mehrfach das Narrativ des „Mithörens" oder „Abhörens" aufgeführt, häufig in Bezug auf personalisierte Werbung. Ein:e Teilnehmende:r formulierte es so:

„Ich finde es erschreckend zu wissen; Okay, das Handy hört mit."

Personalisierte Werbung wurde meist mit gemischten Gefühlen betrachtet. Während sie von manchen als legitimes Mittel der Plattformlogik registriert und akzeptiert wurde, wurde sie von einigen Teilnehmenden auch als „gruselig" empfunden und stark kritisiert. Damit einhergehend

wurde bei einigen Teilnehmenden auch ein differenziertes Wissen über Metadaten, Tracking und eine Kritik an der Monetarisierung von Daten deutlich, wie folgendes Zitat verdeutlicht:

„Früher haben normale Leute den Daten, die wir online stellen, gar nicht so viel Aufmerksamkeit gegeben. Aber jetzt wissen wir – [Daten] sind ein Schatz. Jetzt werden wir auf [Messenger- und Social Media-Diensten] oder beim Chatten analysiert. [Unsere Daten] werden verkauft. Ich finde, das ist ein sehr großes Problem.“

3.3 Erfahrung mit Cyber-Sicherheitsvorfällen und Informationsquellen

Umgang mit Gefahren und Sicherheitsvorfällen

Fast alle der befragten Schüler:innen haben von persönlichen Erfahrungen mit Cyber-Sicherheitsvorfällen berichtet oder kannten eine Person in ihrem engeren Umfeld, die Opfer eines Cyber-Angriffs geworden war. Während die meisten Schüler:innen hierbei von Schadprogrammen auf ihren Geräten berichteten, hatten einige Erfahrungen mit Delikten wie Daten- und Identitätsdiebstahl sowie damit verbundenen ungerechtfertigten Zahlungsaufforderungen an sie gemacht. Dies führte dann z.T. auch zum Einholen von juristischer Unterstützung durch die Eltern.

Die Schüler:innen weisen aufgrund ihrer eigenen Erlebnisse mit Hacking-Angriffen auf private Accounts und Spam- und Phishing-Nachrichten per SMS oder E-Mail bereits einige Sensibilität für mögliche Sicherheitsvorfälle auf. Einzelne Schüler:innen benannten auch spezifische Begriffe wie Scam (Onlinebetrug) oder DoS-Angriffe (Denial-of-Service) als Varianten von Cyber-Attacken.

Gleichzeitig verhielten sich die Schüler:innen aber im Szenario der Befragung beim Erhalt eines unbekannten Links, der einen potenziellen Hacking-Versuch abbilden sollte, unvorsichtiger. Mehrere Schüler:innen hätten auf den - von einer wissenschaftlichen Mitarbeiterin im Chat gepostеten - Link „yourtube.de“ geklickt, wenn dieser von einer befreundeten Person gestammt hätte. Es wurde von vielen der Befragten betont, dass man einem Link von einem Freund oder einer Freundin grundsätzlich vertraue und diesen eigentlich nicht prüfe. Hier besteht demnach ein besonderes Risiko für Schüler:innen, da Cyber-Kriminelle solche Vertrauensverhältnisse zunehmend ausnutzen (z.B. Social Engineering, Deepfakes).

In diesem Kontext wurde den Schüler:innen bewusst, dass sie im Fall eines Cyber-Sicherheitsvorfalls unsicher sind, was dann zu tun sei. Die ersten Reaktionen reichten von Panik (Smartphone ausmachen und sich ablenken) über Polizei anrufen bis hin zu App löschen, Smartphone neustarten und neu in der App anmelden.

Anlaufstellen bei Sicherheitsvorfällen

Bei der Frage, an wen sie sich bei einer Virusinfektion ihres Smartphones als erstes wenden würden, war die erste Erkenntnis in vielen Fällen, dass sie nicht wüssten, wer ihnen am besten helfen könnte. Wenig überraschend wurden die Eltern daher oft als erste Ansprechpersonen genannt, auch wenn dies selten mit der Hoffnung verbunden war, dass sie bei der technischen Lösung des Problems helfen könnten. Mehrere der befragten Schüler:innen benannten dann jedoch noch eine Person in ihrem Familien- oder Bekanntenkreis, die eine gewisse Technikexpertise vorweisen und als Anlaufstelle für konkrete technische Hilfestellungen dienen könne. Dies waren oft ältere Geschwister oder Arbeitskolleg:innen bzw. Bekannte der Eltern. Auch

der nächste Handyshop wurde als Anlaufstelle für Hilfe bei einem Cyber-Sicherheitsvorfall benannt.

Ein weiterer Impuls der Schüler:innen war es, den Support des gehackten Dienstes zu kontaktieren, wenngleich hier nicht immer klar war, ob dieser Support überhaupt existiere und wie er ggf. kontaktiert werden könne. Von den Jugendlichen wurde sich daher vielfach mehr Transparenz von den Anbietern gewünscht, sowie parallel mehr Aufklärung, vor allem im schulischen Bereich. Ein:e Schüler:in formuliert es wie folgt:

„Cyber-Sicherheit, Social-Media und alles ums Thema Technik kommt in der Schule viel zu kurz. Man weiß, wie man eine Story posten kann, aber mehr dann halt auch nicht – und das ist vor allem eine Gefahr für sich selbst. Darauf muss in der Schule mehr eingegangen werden."

Ein:e Schüler:in formulierte, es würde sicherlich ein höheres Amt geben, bei dem man „Informationssachen" erhalten könne.

3.4 Persönliche Bedeutung von Cyber-Sicherheit und Handlungsoptionen

Eigenes Sicherheitsgefühl

Auf die Frage „Wie sicher fühlst du dich im Netz?" (quantitative Abfrage im Chat, Skala von 1 bis 5; 1 = sehr sicher, 5 = sehr unsicher) lag der Durchschnitt bei 3. Hier gab es nur wenige Ausreißer, die sich sehr oder gar nicht sicher fühlten. Dies bestätigt die Erkenntnisse der Analyse, dass zwar ein grundlegendes Verständnis von Cyber-Sicherheit und Interesse am Thema bei vielen Teilnehmer:innen vorhanden ist, jedoch eine nicht unerhebliche Hilflosigkeit empfunden wird, hinsichtlich des (Selbst-)Schutzes vor Cyber-Attacken und bestehenden Sicherheitslücken. So betont ein:e Schüler:in:

„Ich wüsste gar nicht, wie ich mich schützen soll."

Auch der Umgang vieler Online-Dienstleister mit persönlichen Daten, insbesondere die unwissentliche bzw. ungewollte Weitergabe der Daten an Dritte sowie deren Verkauf wurden kritisiert (siehe hierzu Kap. 3.2). Neben der Unzufriedenheit mit konkreten Apps aufgrund der Intransparenz der Daten(weiter)verwendung wurden hierbei auch datenbasierte Services oder Produktverbesserungen kritisiert. Das folgende Zitat fasst die Kritik zusammen:

„Ich kann mich so sehr schützen wie ich möchte und so viele AGBs lesen wie ich möchte, wenn ich dann der Daten[nutzung] zustimme, sie im Endeffekt aber noch für etwas ganz anderes genutzt werden – das liegt dann ja nicht mehr in meiner Hand. Das passiert heutzutage leider ziemlich häufig, weil es da dann nur noch ums Geld geht."

Möglichkeiten zur Erhöhung der Cyber-Sicherheit

Persönliche Schutzmaßnahmen, wie z.B. sichere Passwörter, Anti-Viren-Programme und das Durchführen regelmäßiger Updates, waren den meisten Teilnehmenden bekannt. Die Durchführung wird jedoch vor allem auf mobilen Endgeräten nicht stringent umgesetzt. Während die allermeisten der befragten Schüler:innen auf Computern oder Laptops Anti-Viren-Programme installiert hatten, war dies auf dem Smartphone nur sehr selten der Fall. Genauso wenig wurden durchgängig sichere Passwörter ausgewählt. Hierfür wurden vor allem Unkreativität und Vergesslichkeit als Gründe genannt. Oft erklärten die Schüler:innen, die Sicherheit ihrer Passwörter je nach Wichtigkeit des Online-Dienstes anzupassen – je (subjektiv) wichtiger der Dienst eingestuft wurde, desto komplexer das Passwort. Einige der Befragten gaben an, einen

Passwortmanager zu benutzen, andere wiederum schrieben sich ihre Passwörter lieber handschriftlich auf – z.T. auch weil Passwortmanager als anfällig für Hacking-Angriffe angesehen wurden.

Umgang mit Apps und AGBs

Wenn Datenschutz-Optionen niedrigschwellig sind und eine einfache Opt-Out-Option geboten wird, um seine Daten zu schützen (z.B. bei App-Berechtigungen, die automatisch abgefragt werden), wird dies in den allermeisten Fällen von den Befragten angenommen und individuell konfiguriert: Das Bewusstsein für das Prinzip der Datensparsamkeit war also bei den Schüler:innen durchaus vorhanden. Wenn die Schwelle zum Datenschutz jedoch höher liegt, z.B. durch zu lange und komplizierte AGBs und Datenschutzerklärungen, so sank die Bereitschaft der Schüler:innen, sich damit zu beschäftigen. Eine Erklärung fand sich auch mehrfach darin, dass man eine App aus einem bestimmten Grund herunterladen und nutzen wolle und die Formalitäten dann schlichtweg eine untergeordnete Rolle spielen würden. Dieses Ergebnis steht im Einklang mit dem Verhalten der restlichen deutschen Bevölkerung; der Großteil der teilnehmenden Schüler:innen las die AGBs nie, laut Statista trifft diese Aussage auf 72% der Deutschen zu[25]. Hier wurde von den Schüler:innen die Komplexität und Benutzerunfreundlichkeit (z.B. zu lang, zu unverständlich geschrieben) der AGBs stark kritisiert.

Bei der Frage, ob die Teilnehmer:innen bestimmte Dienste oder Apps aufgrund von Sicherheitsbedenken nicht oder nicht mehr nutzen, gab es sehr gemischte Antworten. Bei den meisten der befragten Schüler:innen spielten die Anbieter hinter den Apps eher keine Rolle und waren oftmals auch nicht bekannt. Das Ausweichen auf Open Source-Alternativen spielte sogar überhaupt keine Rolle bei der Auswahl der Apps. Auch Datenschutzbedenken wurden nur äußerst selten als Grund genannt, bestimmte (vor allem populäre) Dienste nicht (mehr) zu nutzen. Viele der Apps wurden teilweise allein wegen ihrer Popularität als sicher eingestuft:

„Wenn es nicht sicher wäre, würden es ja auch nicht so viele nutzen."

Falls Apps oder Dienste nicht mehr von den Jugendlichen genutzt wurden, spielten statt Sicherheitsbedenken meist nur der fehlende persönliche Mehrwert einer App eine Rolle. Einige der Befragten äußerten, dass sie eine App gelöscht hatten, da ihre Anwendung zu viel Zeit in Anspruch nahm. Das Motiv der Selbstregulierung durch die Deaktivierung einer App trat unerwartet häufig auf.

Das bedeutet aber keinesfalls, dass die Jugendlichen bei der Nutzung verschiedenster Anbieter gar keine Sicherheitsbedenken haben; Zwar wurden Apps nicht immer sofort deinstalliert, aber einige Dienste wurden aufgrund von Datensicherheitsbedenken seltener genutzt. Andere Schüler:innen geben an, alle Apps zu nutzen, die sie möchten, dabei aber ihre Daten so gut wie möglich über die individuellen Einstellungen zu schützen und den Zugriff der Apps auf sämtliche Funktionen des Smartphones zu minimieren.

Awareness vs. Unsicherheit

Einige der Teilnehmenden konnten sogar aktuelle Debatten um datenschutzrechtlich relevante Themen, wie zum Beispiel die Diskussionen um die im Rahmen der COVID-19-Pandemie populär gewordenen Kontaktpersonennachverfolgung, oder auch den Cambridge Analytica Skandal, gut wiedergeben. Sie gaben an, daraus Konsequenzen für ihr eigenes Verhalten

[25] Kunst, A. (2019, November, 6th). *Häufigkeit mit der Online-Käufer die AGBs von Online-Shops lesen in Deutschland 2017*. Statista.

gezogen, App Konten gelöscht und Apps deinstalliert zu haben. Hierbei wurde deutlich, dass die Schüler:innen damit ein Zeichen für mehr Awareness setzten wollten und die Hoffnung hatten, dass andere Personen in ihrem Umfeld ähnliche Konsequenzen ziehen. Dies kann durchaus als eine politische Dimension im Handeln der Jugendlichen gedeutet werden.

Gleichzeitig konnte man bei manchen Jugendlichen eine gewisse Hilflosigkeit bzw. Resignation feststellen und fehlende Ideen zum (Selbst-)Schutz im Internet; teilweise wurde der Besitz eines Smartphones als Sicherheitsrisiko eingestuft, auf welches man kaum Einfluss nehmen könne. In die teilweise empfundene Hilflosigkeit mischte sich aber auch ein Gefühl von Freiheit und Unbefangenheit. So äußerte ein:e Schüler:in:

„Ich fühle mich unglaublich frei. Ich laber‘ über alles auf WhatsApp mit meinen Freunden. Und natürlich, wir wissen alle, dass alles, was man im Internet macht, auch im Internet bleibt.“

Empowerment durch aktivierende Befragung

Zum Abschluss sollte festgehalten werden, dass die Befragung bei allen Schüler:innengruppen dankbar angenommen wurde. So sagte ein:e Schüler:in am Ende der Befragung:

„Ich finde es gut, dass auch mal mit den Schülern gesprochen wird und gefragt wird, wie weit die Schüler sind und was [wir] vielleicht noch brauchen. Ich hatte vorher das Gefühl, dass vor allem was die Technikfrage betrifft nicht richtig mit uns gesprochen wurde. Es wird immer gesagt ‚Die Schüler kennen sich nicht aus‘ und ‚Die jungen Menschen sind so viel im Internet und machen so viel Blödsinn‘ aber keiner geht auf uns zu und sagt uns, was wir denn da beachten müssen.“

Wie an vielen anderen Stellen während der Befragungen wurde hier das grundsätzliche Interesse der Schüler.innen an der Mitgestaltung ihrer eigenen Lebensrealität sowie das Interesse am Thema Cyber-Sicherheit deutlich. Die Jugendlichen zeichneten sich durch ein großes Engagement während der Befragung und vielen Ideen aus, wie Cyber-Sicherheitsthemen attraktiver, präsenter und greifbarer in ihrem Leben verankert werden können (siehe hierzu Kap. 4.2).

3.5 Ergebnisse der Lehrer:innen-Fokusgruppe

Hohes Risikobewusstsein aufgrund von Sicherheitsvorfällen

Die Lehrer:innen wiesen alle ein grundlegendes Verständnis von Begrifflichkeiten rund um das Thema Cyber-Sicherheit auf, kannten gesellschaftliche Debatten rund um das Thema Cyber-Sicherheit und waren sich grundlegender Risiken bewusst. Bei ihnen wurde eine kritische Grundhaltung zu personalisierten Inhalten und der detailgenauen algorithmischen Profilierung und Vorhersage des Nutzungsverhalten deutlich. Vor allem im schulischen Kontext zeigten die Befragten einen sehr hohen Sicherheitsanspruch – deutlich mehr als im privaten Bereich. So waren die Lehrer:innen vor allem sehr sensibel und wachsam für die Risiken, denen Schüler:innen im Umgang mit dem Internet ausgesetzt sind.

Während einige der Befragten noch keine persönlichen Erfahrungen mit Cyber-Sicherheitsvorfällen gemacht haben, haben andere schon unterschiedliche Sicherheitsvorfälle an den Schulen erlebt. So wurde von Vorfällen berichtet, bei denen Passwörter von Lehrer:innen veröffentlicht wurden oder über mehrere Jahre unbemerkt ein offenes WLAN-Netz an einer

Schule verfügbar war, über das einzelne Schüler:innen gehackt wurden. Auch wurde von Außenstehenden berichtet, die sich während der Corona-Pandemie in den Online-Schulunterricht eingeklinkt hätten.

Hoher Bedarf an fachlicher Ausbildung und Ressourcen

Der Umgang mit solchen sicherheitskritischen Situationen ist vor allem aufgrund der mitunter sehr großen ressourcenmäßigen Unterschiede zwischen den Schulen und Bundesländern herausfordernd: Während es an manchen Schulen Fachpersonal gäbe, das sich um den Betrieb des Schulnetzwerkes und etwaige Sicherheitslücken kümmere sowie für Fragen vor Ort zur Verfügung stehe, seien andere Schulen laut den Interviewaussagen ziemlich auf sich allein gestellt: Hier müsse man sich selbst helfen durch autodidaktische Weiterbildung und die Stärkung der Zusammenarbeit zwischen den Schulen. Als Beispiel wurde ein regelmäßiger Austausch-Termin zwischen Lehrer:innen unterschiedlicher Schulen angeführt, damit sie sich gegenseitig mit ihrem Erfahrungswissen unterstützen und Fragen beantworten können.

Trotzdem empfanden die Befragten auch eine Überforderung mit den Anforderungen und Herausforderungen der schnelllebigen digitalen Welt. In diesem Zusammenhang wurde auch Kritik am Bildungssystem laut, welches dem digitalen Wandel auch bei der Ausbildung des pädagogischen Personals hinterherhinke:

„Ich finde es schwierig, dass es davon abhängig ist, ob sich jemand interessiert oder nicht – und wer sich nicht interessiert, der wird darüber wahrscheinlich auch nichts erfahren.“

Eine offizielle, verpflichtende Schulung zum Thema Cyber-Sicherheit wurde bislang an keiner der Schulen der Befragten angeboten. So hinge die Expertise des Lehrpersonals weiterhin vom freiwilligen Interesse und Engagement einzelner Lehrer:innen ab. Die befragten Lehrer:innen wünschten sich vor allem Zeit, um sich weiterzubilden und dass dieses für einen sicheren Schulalltag fundamentale Wissen nicht allein auf Freiwilligkeit basieren dürfe.

Gleichzeitig wurde immer wieder der Lehr- und Fachkräftemangel thematisiert und alle Teilnehmenden waren sich einig, dass es mehr Expertise in den Schulen rund um das Thema Cyber-Sicherheit brauche. So forderte ein:e Lehrer:in:

„Wir brauchen Informatiker an der Schule, die für die Cyber-Sicherheit verantwortlich sind und uns [Lehrer:innen] helfen. Jede Schule braucht einen Informatiker, der Vollzeit arbeitet.“

Zwar waren sich die Lehrer:innen uneinig, ob diese Expertise bestenfalls im eigenen Haus aufgebaut werden solle (d.h. interessiertes pädagogisches Personal spezialisiert sich auf IT-Themen) oder ob externe Informatiker:innen angestellt werden sollen – einig waren sie sich jedoch in der Notwendigkeit von mehr digitalen und sicherheitsrelevanten IT-Kompetenzen im Schulalltag. Zusätzlich stellten die befragten Lehrer:innen den Bedarf der curricularen Verankerung von Cyber-Sicherheits-Themen im Lehrplan fest. Dieses für die Zukunft so relevante Thema könne nicht „einfach in jedem Fach nebenbei unterrichtet werden“.

4 Handlungsansätze

4.1 Best Practice Beispiel „SecAware4school“

Im Verlauf der Literatur- und Studienrecherche im Workstream tat sich mit SecAware4school ein Best-Practice-Beispiel für inspirierende Bildungsangebote im schulischen Lernumfeld auf,

das das Thema Informationssicherheit auf spielerische Weise aufgreift. Es soll an dieser Stelle vorgestellt werden.

Das Projekt „Informationssicherheitsbewusstsein für den Schulalltag – SecAware4school“ wurde von September 2018 bis Dezember 2020 von der Technischen Hochschule Wildau (TH) umgesetzt.[26] Ziel des Forschungsprojektes war es, insbesondere bei Schüler:innen, aber auch bei Lehrer:innen und Eltern Interesse für das Thema Informationssicherheit zu wecken und sie dafür zu sensibilisieren.

Das Forschungsteam von Frau Prof. Dr. Scholl der Technischen Hochschule Wildau setzte SecAware4school in Kooperation mit fünf Pilotschulen in Berlin und Brandenburg um und führte Awareness Trainings, Kreativworkshops sowie Projekttage durch. An ihnen waren insgesamt ca. 600 Schüler:innen sowie ca. 20 Lehrer:innen beteiligt. In einem partizipativen Forschungsdesign wurden gemeinsam 36 Lernszenarien mit und für Schulen entwickelt und erprobt.

Zu Beginn des Projektes wurden alle Teilnehmenden durch Workshops geschult, um eigene Kompetenzen im Bereich Informationssicherheit zu erlangen oder zu erweitern. Dabei wurden die Lehrkräfte darauf vorbereitet, motivierte Schüler:innen als „Sicherheitsberater:innen“ der Peergroup auszubilden, anzuleiten und zu sensibilisieren. Ältere Schüler:innen sollten ihr Wissen adäquat an Jüngere weitergeben und als Moderator:innen durch die entwickelten Lernszenarien leiten können.[27]

Die Lernszenarien sollten die von Schüler:innen und Lehrkräften oftmals als techniklastig und komplex wahrgenommenen Inhalte besser greifbar und einfacher verständlich machen. Durch aktives Erleben der (sowohl digitalen wie auch analogen) Szenarien sollten die Teilnehmenden die Risiken im Internet erkennen und die Folgen ihres Handelns besser einschätzen können. Die Lernszenarien wurden in 12 Themenbereichen mit jeweils drei Schwierigkeitsstufen entwickelt und sind für unterschiedliche Wissensstände und Altersstufen geeignet.

Alle Lernszenarien sind kostenfrei und unter freier Lizenz auf der Projektwebsite erhältlich.[28] Digitale Simulationen können direkt auf der Website aufgerufen und durchgespielt werden. Analoge Szenarien stehen mitsamt Umsetzungsanleitungen und begleitenden Materialien zum Ausdrucken zur Verfügung. Sie können von interessierten Bildungseinrichtungen, zivilgesellschaftlichen Institutionen und Einzelnen heruntergeladen und weiterentwickelt werden. Da sich die Lernszenarien gut für den Einsatz im schulischen Umfeld eignen, sind insbesondere Schulen hierzu eingeladen.

4.2 Ideensammlung für Bildungsangebote

Sowohl Schüler:innen als auch Lehrer:innen zeigten bei den Fokusgruppen-Interviews einen großen Ideenreichtum für mögliche Bildungsangebote und beide Gruppen sahen die Schule (und insbesondere den fachlichen Unterricht) als geeigneten Ort an, um Bildungsangebote im Bereich der Cyber-Sicherheit umzusetzen. Hierfür müssten jedoch geeignete Rahmenbedingungen geschaffen werden, beispielsweise zielgruppengerechte Lehr-Lern-Formate sowie

[26] Eine umfassende Projektbeschreibung, Informationsbroschüren, Lernszenarien und Umsetzungsanleitungen sind abrufbar unter: https://secaware4school.wildau.biz/de.html.

[27] Vgl. Schuktomow, Scholl, Gube, Koppatz, Edich, Gerlach (2020): Projektdokumentation Informationssicherheitsbewusstsein für den Schulalltag (SecAware4School), Seite 67 ff.

[28] Abrufbar unter: https://secaware4school.wildau.biz/de.html.

ausreichend Ressourcen bei den Lehrenden für die Umsetzung eben dieser. Es wurden immer wieder die Aspekte Freiwilligkeit bzw. curriculare Verankerung sowie Regelmäßigkeit hervorgehoben: Wissen darüber, wie man sich sicher im Internet bewegt, dürfe nicht länger nur auf privatem Engagement und persönlichen Interesse beruhen, sondern sollte ein fester Bestandteil des Schulcurriculums werden, so die überwiegende Meinung der befragten Schüler:innen und Lehrkräfte. Freiwillige Angebote, wie beispielsweise AGs, könnten zwar ein zusätzliches Angebot für besonders Interessierte sein, sollten aber keinesfalls den Erwerb des Grundwissens für alle ersetzen. Darüber hinaus wurde die Schnelllebigkeit des Internets oft hervorgehoben – Bildungsangebote müssten also regelmäßig stattfinden und inhaltlich angepasst werden, um hier immer auf dem neusten Stand zu bleiben.

Vor allem im Bereich rund um das Internet, ist es besonders wichtig, das Lernen im eigenen Tempo und die Binnendifferenzierung von Lehr-Lern-Prozessen nach Interessen, Vorkenntnissen, Inhalten, Lösungsstrategien, Schwierigkeiten, Umfang oder Zeit zu berücksichtigen und dementsprechend flexible Angebote zu schaffen.[29] Die in den Fokusgruppen vorgeschlagenen Bildungsangebote nehmen diese Forderung der Kultusministerkonferenz indirekt auf und gestalten sich dementsprechend vielfältig: So wurden individuelle, schulisch-institutionelle und sogar politische Lösungen vorgeschlagen. Die Jugendlichen wünschen sich vor allem konkrete Hilfestellungen und Beratungen, die nah an der Realität sind. Außerdem wurde immer wieder ein Praxisbezug und der Wunsch nach interaktiven Formaten betont. So wünschte sich eine Schülerin:

„Was spannend wäre, wären mehrere Projekttage, an denen auch realistische Situationen [mit Cyber-Security-Vorfällen] vorgestellt werden. Wo man lernt, was passiert ist und was für Ausläufe das haben kann.“

Auch bei der Schülerschaft wurde der Wunsch nach kompetentem Personal laut:

„Man sollte […] Lehrer schulen, jemanden der auch wirklich Zeit dafür hat, und [die] den Kindern helfen können – [die] quasi Cyberberater sind.“

Hierbei ergeben sich durch das Lehren und Lernen in der digitalen Welt erweiterte Möglichkeiten zu kreativen und produktorientierten Aufgaben in allen Schulstufen und Fächern, wie zum Beispiel dem Erstellen von Podcasts und Videos, Bildverarbeitung, Gestaltung von Websites und Online-Journalen, Modellierungen und Simulationen, Verfahrenstests oder technische Prüfverfahren.[30] Dabei sollten vor allem bestehende Strukturen besser genutzt werden. So wurde oftmals in den Fokusgruppen der Informatikunterricht kritisiert und der Wunsch geäußert, dass dieser realitätsnahes Wissen auf spannende Art und Weise vermitteln solle. Die befragten Schüler:innen forderten auch, dass im Informatikunterricht behandelt werden sollte, wie sie sich selbst besser für Gefahren im digitalen Raum schützen und in sicherheitskritischen Situationen handeln können.

Besonders interessant war der ganzheitliche Ansatz einiger der jungen Teilnehmer:innen, der über das klassische Schulsetting hinausging und die Komplexität der modernen Informationsgesellschaft in den Blick nahm:

[29] Kultusministerkonferenz (2021, December 9th). Strategie „Bildung in der digitalen Welt“. https://www.kmk.org/themen/bildung-in-der-digitalen-welt/strategie-bildung-in-der-digitalen-welt.html

[30] Kultusministerkonferenz (2021, December 9th). Strategie „Bildung in der digitalen Welt“. https://www.kmk.org/themen/bildung-in-der-digitalen-welt/strategie-bildung-in-der-digitalen-welt.html

„Wenn es an jeder Schule einen [IT-Manager] gäbe – dann gäbe es auch mehr Arbeitsplätze und auch mehr Leute, die in der Zukunft in dieser Richtung arbeiten wollen. Und das ist doch eigentlich das, was gebraucht wird und nötig ist in Deutschland."

Neben diesem Blick für die Probleme in einer digitalisierten Welt, hatten die Jugendlichen auch innovative politische Ideen und forderten mehr politisches Handeln und Weichenstellungen für eine zukunftsfähige vernetzte europäische Gesellschaft. So schlug eine junge Teilnehmerin eine „Ständige Europäische Cyber-Kommission", ähnlich der „Ständigen Impfkommission", vor. Diese solle Empfehlungen aussprechen können, die Sicherheit von Diensten überprüfen und eine Anlaufstelle für Opfer von Cyber-Kriminalität bieten.

Die Lehrer:innen traten zwar weniger idealistisch in der Befragung auf, dafür aber nicht weniger kreativ: Sie schlugen beispielsweise einen in Lernplattformen integrierbaren, auf Open-Source Software basierenden Online-Kurs zu Cyber-Security, inklusive der Möglichkeit für einen Zertifikaterwerb, vor. Hinzu kamen Ideen für interaktive Workshoptage zum Erlernen von Programmierfähigkeiten sowie die Konzeption und Umsetzung eigener YouTube-Lernvideos. Weiterhin wurden thematische Escape-Rooms vorgeschlagen, bei denen spielerisch sicheres oder unsicheres Handeln im Internet erlernt werden könne sowie der etwas klassischere Ansatz der Durchführung von Medienkompetenzprogrammen an den Schulen.

In einem Kreativworkshop im Workstream ‚Update4Schule' im März 2022 wurden die Ergebnisse der qualitativen Erhebung mit den Workstream-Teilnehmer:innen, die insbesondere die Sicht der organisierten Zivilgesellschaft vertreten, diskutiert und weiterentwickelt. Während einige Ideen aus den Fokusgruppen aufgegriffen und weitergedacht wurden, wurde auch auf schon bestehende Bildungsformate hingewiesen. Diese sollten vor allem gestärkt und weiterentwickelt werden, anstatt einen Flickenteppich an Projekten entstehen zu lassen, so die Forderung der Workstream-Teilnehmer:innen. Es gebe zum Beispiel schon Cyber-Sicherheitskurse für Schüler:innen[31] oder einen kostenfreien digitalen Führerschein[32], der von der Initiative Deutschland sicher im Netz entwickelt wurde und mit dem Nutzer:innen ihre Internet- und Sicherheitskompetenz testen können. Auch schulübergreifende Arbeitsgruppen, die Wissen im Bereich Informationstechnologie und Datenschutz speziell an Mädchen vermitteln wollen, sind bereits in der Pilotphase[33]. Weiterhin werden auch Online-Webinare zum Thema Cyber-Mobbing[34] angeboten. Finanzielle und personelle Ressourcen sollten neben der Entwicklung innovativer Lehr-Lernangebote daher auch darauf verwendet werden, bestehende Angebote zu bündeln, zu optimieren, ihre Sichtbarkeit zu stärken und ihre Anwendung zu verbreiten.

Einige der im Workshop bei „Update4Schule" gesammelten Ideen für Bildungsangebote werden nachfolgend genauer dargestellt:

[31] https://www.lehrer-online.de/unterricht/sekundarstufen/naturwissenschaften/informatik/unterrichtseinheit/ue/online-kurs-cyber-sicherheit/
[32] https://difü.de/
[33] https://it-security-girls.eu/
[34] https://digitale-helden.de/angebote/webinare/webinar-rechtsfragen-was-tun-bei-cybermobbing/

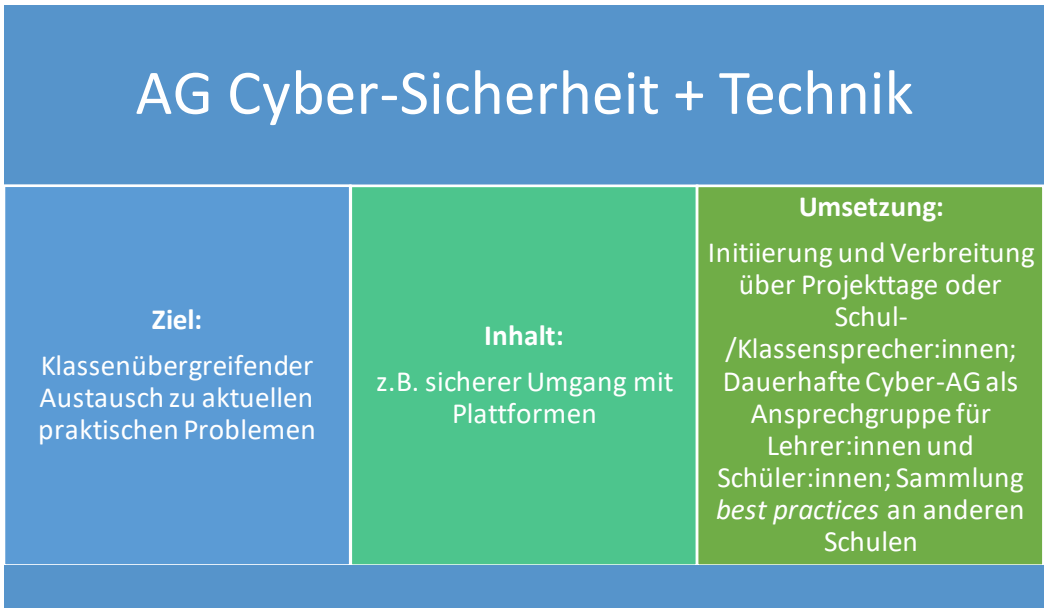

Abbildung 4: Bildungsangebot-Idee "AG Cyber-Sicherheit + Technik"

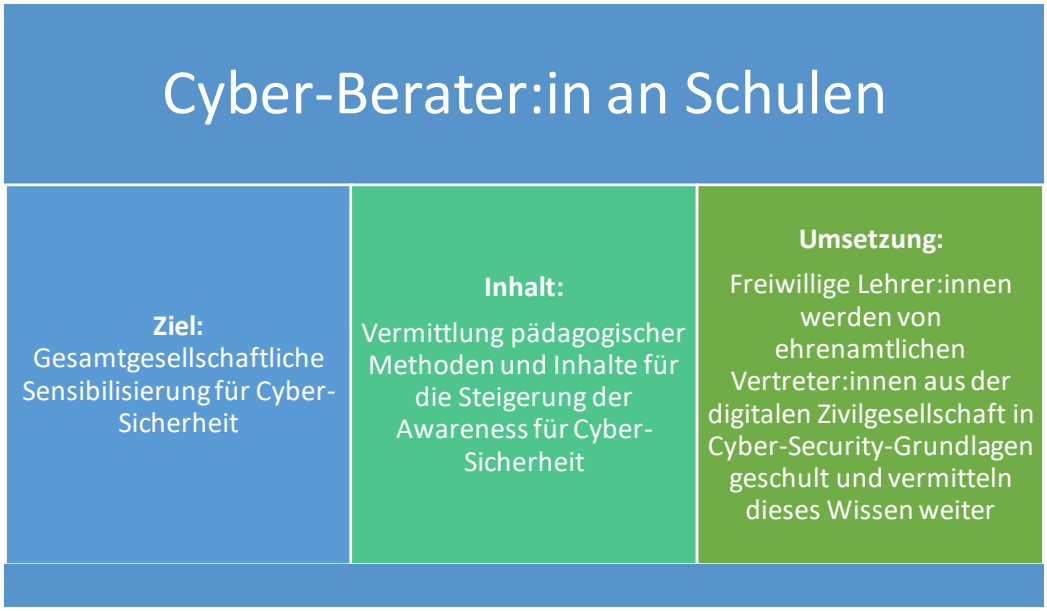

Abbildung 5: Bildungsangebot-Idee "Cyber-Berater:in an Schulen"

Abbildung 6: Bildungsangebot-Idee "Projekttage an Schulen"

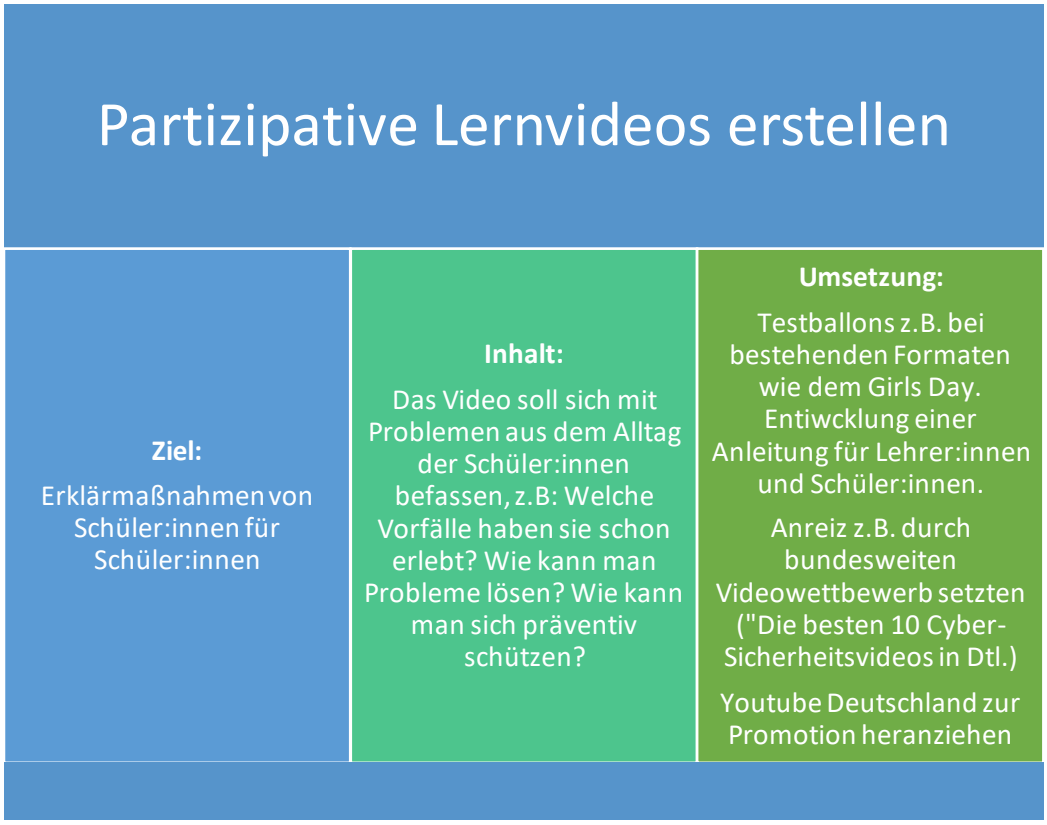

Abbildung 7: Bildungsangebot-Idee "Partizipative Lernvideos erstellen"

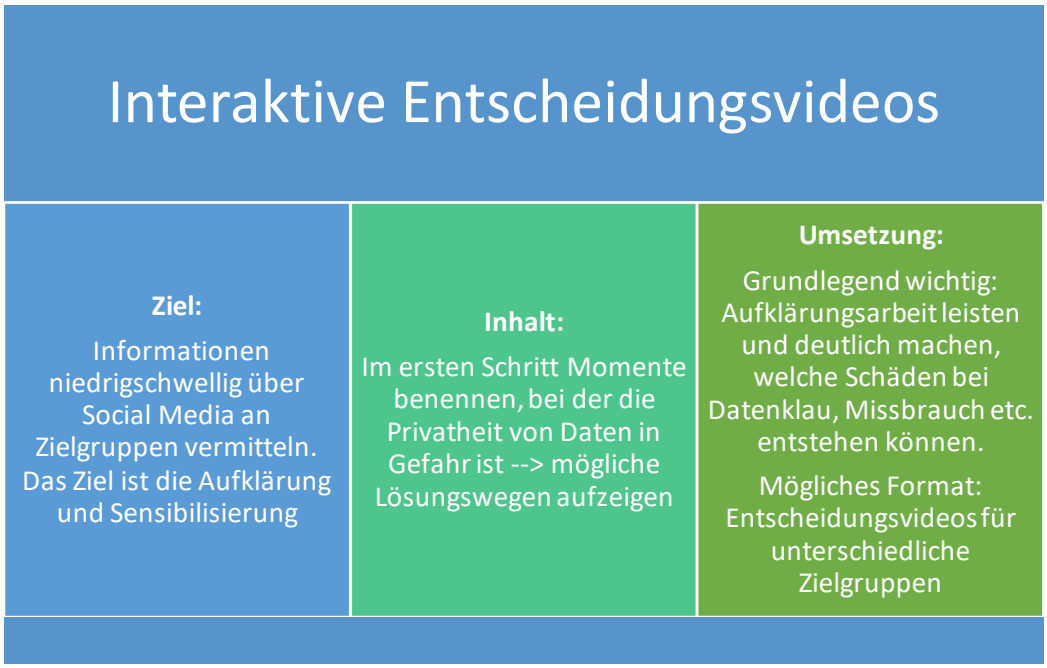

Abbildung 8: Bildungsangebot-Idee "Interaktive Entscheidungsvideos"

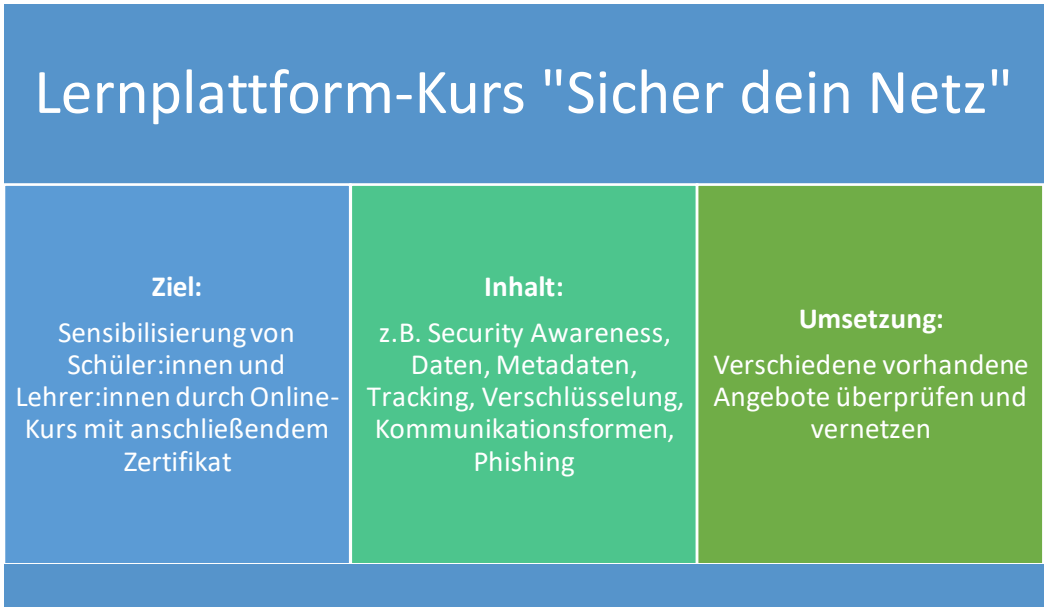

Abbildung 9: Bildungsangebot-Idee "Lernplattform-Kurs 'Sicher dein Netz'"

4.3 Handlungsempfehlungen für Datenerhebungen mit Schüler:innen

Anhand der im Rahmen dieser Studie gesammelten Erfahrung bei der Vorbereitung und Durchführung einer qualitativen Erhebung in Form von (Online-)Fokusgruppen mit Schüler:innen und Lehrer:innen, sollen hier einige Handlungsempfehlungen dargestellt werden:

Vorbereitung der Erhebung

- Es bedarf einer Klärung der länderspezifischen Anforderungen, um wissenschaftliche Erhebungen an Schulen durchführen zu können: Hier gibt es z.T. sehr unterschiedliche

Vorgaben in den Bundesländern, welche auch unterschiedlich viel Zeit für die Durchführung der jeweiligen Genehmigungsverfahrens in Anspruch nehmen. Der persönliche Austausch mit den zuständigen Sachbearbeiter:innen kann hier für eine realistische Zeitplanung hilfreich sein.

- Für die Durchführung einer wissenschaftlichen Erhebung werden Informationsbriefe für die Schulleitung, Eltern und Schüler:innen (sowie ggf. Multiplikator:innen), Datenschutzhinweise, Einwilligungserklärungsvorlagen sowie ein Aufbewahrungs- und Löschkonzept für die erhobenen Daten benötigt. Die Erstellung dieser Dokumente ist relativ zeitaufwendig und das Forschungsteam kann sich hierbei bestenfalls extern beraten lassen.
- Wenn die Erhebung digital durchgeführt werden soll, ist hinsichtlich des zu verwendenden Tools eine Datenschutzerklärung zu erstellen sowie ebenfalls das Einverständnis der Teilnehmenden einzuholen. Alternativ kann ein Tool genutzt werden, welches die Schule bereitstellt.

Befragungssituation

- Von Anfang an sollte der Rahmen der Untersuchung deutlich gemacht werden, das heißt, die wissenschaftliche Befragung klar von einer Testsituation zu unterscheiden und den Teilnehmer:innen zu vermitteln, dass es kein ‚Richtig' und kein ‚Falsch' gibt, sondern es sich ausschließlich um eine wertneutrale Erforschung handelt.
- Die eigene Rolle als interessierte:r Forschende:r sollte von Beginn an deutlich gemacht werden, um sich von der Rolle einer Lehrkraft zu unterscheiden: Hierzu kann hervorgehoben werden, dass es um die Erfahrungen, Meinungen und Perspektiven aus der Lebenswelt der Befragten geht und nicht um eine Wissensabfrage, die sie im schulischen Setting meist gewohnt sind.
- Das persönliche ‚Du' für teilnehmende Schüler:innen anbieten: So können Hemmungen gleich zu Beginn abgebaut und eine angenehme Gesprächsatmosphäre geschaffen werden. Das Ziel der Gesprächseinleitung sollte es sein, Vertrauen zueinander zu schaffen und ein Gespräch auf Augenhöhe zu ermöglichen.
- Moderation der Befragung: In regelmäßigen Abständen sollten alle Teilnehmenden der Gruppe dazu motiviert werden, auf eine Frage zu antworten. So melden sich auch die zurückhaltenden Teilnehmer:innen eher wieder zu Wort.
- Den Teilnehmenden (insbesondere Schüler.innen) sollte verdeutlicht werden, dass sie den Raum haben, ihre eigenen Ideen und Gedanken vorzutragen und mitzugestalten. Durch den Einsatz partizipativer Methoden und deren aktivierende Wirkung kann die Selbstwirksamkeitserfahrung der Teilnehmer:innen gestärkt werden.

5 Fazit

Die vorliegende Studie liefert qualitative Einblicke in den Stand zu Wissen, Fähigkeiten und Sensibilität von Schüler:innen und Lehrer:innen in Deutschland im Bereich Cyber- und Datensicherheit: Sie zeigt auf, dass viele der jugendlichen Schüler:innen über einen grundlegenden Wissensschatz im Bereich Cyber- und Datensicherheit verfügen. Sie wissen, welche Daten von ihnen im schulischen und privaten Kontext entstehen und sind sich der Risiken im digitalen Raum, wie z.B. Hacking-Angriffe, Datendiebstahl und Onlinebetrug, bewusst. Sie kennen be-

reits verschiedene Schutzmöglichkeiten, wie beispielsweise Verschlüsselung, sichere Passwörter, Antiviren-Software und Updates. Diese Ergebnisse waren sehr eindeutig, können jedoch trotzdem, vor allem aufgrund der geringen Teilnehmer:innenzahl, nicht als repräsentativ gesehen werden.

Bei der praktischen Umsetzung von sicherem Verhalten und Schutzmaßnahmen wurde jedoch deutlich, dass noch viele Lücken bestehen und die Sensibilität für das Sicherheitsrisiko sehr unterschiedlich ausgeprägt ist. So wurden z.B. die Privatsphäre und persönliche Daten in Sozialen Netzwerken als schützenswerter empfunden, als auf digitalen Schulplattformen. Es wurde aber auch eine kritische Sicht der Schüler:innen auf den intransparenten Umgang großer Online-Dienste mit persönlichen Daten deutlich und zum Teil Hilflosigkeit bei der Frage, wie sie sich selbst besser im Internet schützen können. Fast alle Teilnehmer:innen hatten bereits Erfahrungen mit verschiedenen Sicherheitsvorfällen, von Phishing bis hin zu Identitätsdiebstahl.

Die Fokusgruppengespräche machten deutlich, dass für Schüler:innen die Handlungsmaxime im digitalen Raum Vertrauen ist: Sie haben Vertrauen in die Sicherheit von vielgenutzten Apps, in die Lernplattform der Schule und in Chat-Nachrichten von Freund:innen. Dieses Grundvertrauen kann leicht für Cyber-Kriminalität ausgenutzt werden, weshalb es umso mehr gilt, sich den mit dieser Studie aufgezeigten Bedarfen anzunehmen und Schüler:innen und Lehrer:innen dabei zu unterstützen, Wissen und Kompetenzen im Bereich Cyber-Sicherheit aus- und aufzubauen. Diese Forderung wurde von den befragten Schüler:innen und Lehrer:innen gestellt: Sie wünschen sich mehr schulische Beratungs- und Lernangebote und mehr Ressourcen für die Umsetzung und den Aufbau von technisch-fachlicher Expertise in den Schulen.

Anhand der Fokusgruppen-Interviews und des Austauschs mit den praxisnah tätigen Workstream-Teilnehmer:innen wurden Ideen gesammelt, wie zielgruppenorientierte und praxisnahe Bildungsangebote gestaltet werden können. Fast alle Teilnehmenden stimmten darüber überein, das die Themen Cyber- und Datensicherheit im Lehrplan verankert werden sollten, damit das Wissen hierzu für alle Schüler:innen zugänglich gemacht wird. Vor allem sollten die Lehr-/Lernangebote mit partizipativen Methoden gestaltet werden: Die Befragten und die Workstream-Teilnehmer:innen empfehlen nicht-frontale Formate wie regelmäßige Projekttage, interaktive Workshops, Cyber-Berater:innen, AGs sowie gemeinsam mit Schüler:innen entwickelte Lernvideos. Die Schüler:innen wollen nicht einfach nur „noch ein Buch oder Arbeitsblatt“, sondern anhand von realistischen Szenarien Wissen zu Cyber-Sicherheit erfahren und praktische Empfehlungen für ihren Alltag sammeln.

Hierzu müssten Lehrer:innen entsprechend während ihrer Ausbildung bzw. durch Fortbildungen geschult werden. Der Aufbau von Kompetenzen beim Lehrpersonal dürfe nicht nur auf freiwilliger Basis und in intrinsisch motivierter Eigenleistung „on top“ erfolgen. Diese bislang gängige Praxis sehen die befragten Lehrer:innen als große Herausforderung für die flächendeckende Umsetzung von Informations- und Lernangeboten an den Schulen. Darüber hinaus sei es zentral, bestehende Bildungsangebote zu vernetzen, zu fördern und sie bekannter zu machen.

Die vorliegende Studie zeigt eindrücklich auf, dass sich Schüler:innen, Lehrer:innen und Stakeholder:innen einig darüber sind, dass digitale Teilhabe und Sicherheit im digitalen Raum in der schulischen Bildung verankert werden soll. Eine aktive Mitwirkung an der Entwicklung innovativer Bildungsangebote kann hierzu einen wichtigen Beitrag zum Empowerment von Schüler:innen und Lehrer:innen im Bereich Cyber-Sicherheit leisten.

Anhang

6.1 Leitfaden „Update4Schule“ - Fragenkatalog für Schüler:innen

Szenario: 1 Tag im Internet

Einführung in das Thema der Befragung:

Vor allem für Schüler:innen spielt die **Nutzung des Internets, von Sozialen Netzwerken und Apps** eine wichtige Rolle in ihrer **Freizeit** und zunehmend auch im **Unterricht**. Bislang wissen wir jedoch kaum etwas darüber, was Schüler:innen über die sichere Internetnutzung und die Sicherheit ihrer Daten wissen und was sie selbst für ihren Schutz tun. Dies wollen wir mit unserer Befragung erforschen. Unsere Fragen werden wir anhand einer kleinen Geschichte stellen.

Zuerst möchten wir Dir aber zwei einleitende Fragen stellen:

- *Was bedeutet Cyber-Sicherheit für Dich? oder Was bedeutet Informationssicherheit für Dich?*
- *Wie sicher fühlst Du Dich im Netz?*
  (Quantifizierung und Angabe auf einer Skala von 1 bis 5 (1= sehr sicher / 5 = sehr unsicher) über den Chat)

Vielen Dank, das war ein guter Start!

Beginnen wir die weitere Befragung mit einer kleinen Geschichte: Du verbringst heute einen Tag im Internet.

Morgens

Guten Morgen! Du stehst auf und machst dich fertig für den Schulunterricht. Wegen Corona ist der online. Du setzt dich an den Laptop und öffnest die Startseite der Online-Lernplattform, die deine Schule benutzt. Da bekommst du eine Sicherheitswarnung: Ein Datenleck ist offengelegt worden. Die Daten der Benutzerkonten der Schüler:innen sind frei im Netz verfügbar!

- *Was denkst du? (Wenn nichts kommt: Wie fühlst du dich damit?)*
- *Hattet ihr schon einmal einen ähnlichen Vorfall mit Bezug zu den Themen Cyber-Sicherheit oder Datenschutz? Wie seid ihr Zuhause oder in der Klasse damit umgegangen?*

Kommen wir zurück zu dem Beispiel des Datenlecks bei der Lernplattform deiner Schule.

- *Was glaubst du: welche Daten von dir sind jetzt im Netz verfügbar?*

Auch dein Passwort ist veröffentlicht worden.

- *Welche Gefahren können sich daraus ergeben?*
- *Nachhaken: Wie merkst Du Dir Deine Passwörter?*
- *Falls Thema bei Antworten nicht angeschnitten wird: Benutzt Du dieses Passwort auch für andere Onlinedienste?*

Wir sprachen gerade über die Nutzung einer Lernplattform. Du benutzt im Laufe des Tages aber in der Regel viele unterschiedliche Webseiten und Apps, wie zum Beispiel Instagram. Dabei könnten neben den Daten deines Benutzerkontos noch weitere Daten von Dir gesammelt werden.

- *Welche Daten von dir könnten das sein und warum werden diese gesammelt?*

Weißt du, was verrückt ist? Meistens gibst du selbst dein Einverständnis für die Sammlung dieser Daten. An dieser Stelle finden wir interessant:

- *Wenn du eine App runterlädst, installierst oder in einem anderen Setting nutzt (z.B. Schule): Schaust Du dir die voreingestellten App-Berechtigungen an?*
- *Liest du die AGBs oder Datenschutzbestimmungen?*
- *Nachhaken: Hast Du schon einmal darüber nachgedacht, eine bestimmte App/Online-Dienst (wie beispielsweise TikTok, Instagram, Youtube oder Whatsapp) nicht mehr zu nutzen – und wenn ja, warum? (Frage 4)*

Nachmittags

Nach dem Mittagessen setzt du dich mit dem Smartphone auf die Couch. Du bekommst eine WhatsApp von einem Freund gesendet, der dich auf ein lustiges Video auf „yourtube.de“ aufmerksam macht.

- *Wie reagierst Du darauf?*
- *Wenn von den Proband:innen nicht so recht eine Antwort kommt: Du kannst entweder A: Auf Link klicken oder B: Erstmal nicht klicken, sondern überprüfen. Was machst Du? (Bitte um Angabe der Proband:innen über den Chat)*
- *Wenn du B eingegeben hast: Was machst Du stattdessen und warum? (Offene Frage)*

Wenn Du auf den Link klickst, kommst Du auf eine Seite, die aussieht wie Youtube und siehst dort ein lustiges Video.

- *Noch merkst du nichts… Aber was könnte jetzt schon mit deinem Smartphone passiert sein?*
- *Wie kannst Du das Risiko minimieren, dass Schadsoftware auf dein Smartphone kommt? (Betriebssystem- und App-Updates, Schutzsoftware, Rückfragen an den Versender)*

Du hast Dir mit dem Klick auf den Link einen Virus eingefangen. Du kommst nicht mehr in Deinen Whatsapp-Account rein.

- *Was solltest du jetzt tun?*

Wahrscheinlich wurde Dein Account gehackt; denn Du siehst mit Entsetzen, dass sich irgendwer in Deinen Account einloggt und Hassbotschaften an Deine Freunde verschickt.

- *Du hast keine Ahnung, was zu tun ist. An wen wendest du dich?*
- *Hat Dir der Vorfall mit dem Virus zu denken gegeben?*

Du möchtest dich in Zukunft besser informieren.

- *Was tust Du?*
- *Nachhaken: Was tust du, um dich in Zukunft besser zu schützen?*
- *Wie würdest Du am liebsten Wissen zum Thema Cyber-Sicherheit vermittelt bekommen und wo?*

Das war es schon. Vielen Dank für eure aktive Mitarbeit!

6.2 Leitfaden „Update4Schule“ - Fragenkatalog für Lehrer: innen

Szenario: 1 Tag im Internet

Einführung in das Thema der Befragung:

Die Nutzung des Internets, von Sozialen Netzwerken und Apps spielt auch für Lehrer:innen eine wichtige Rolle: im **Privatleben**, aber auch vorangetrieben durch die **Corona-Pandemie**, zunehmend im **Unterricht**. Bislang wissen wir jedoch kaum etwas darüber, was **Lehrkräfte über sichere Internetnutzung und die Sicherheit ihrer Daten wissen** und was sie selbst für ihren Schutz tun. Dies wollen wir mit unserer Befragung erforschen. Unsere Fragen werden wir anhand einer kleinen Geschichte stellen.

Zuerst möchten wir Ihnen zwei einleitende Fragen stellen:

- *Was bedeutet Cyber-Sicherheit für Sie? oder Was bedeutet Informationssicherheit für Sie?*
- *Wie sicher fühlen Sie sich im Netz?*
- *(Quantifizierung und Angabe auf einer Skala von 1 bis 5 (1= sehr sicher / 5 = sehr unsicher) über den Chat)*

Vielen Dank, das war ein guter Start!

Beginnen wir die weitere Befragung mit einer kleinen Geschichte: Sie verbringen heute einen Tag im Internet.

Morgens

Sie stehen auf und machen sich fertig für den Schulunterricht. Wegen Corona ist der online. Sie setzen sich an den Laptop und öffnen die Startseite der Online-Lernplattform, die Ihre Schule benutzt. Da bekommen Sie eine Sicherheitswarnung: Ein Datenleck ist offengelegt worden. Die Daten der Benutzerkonten der Lehrkräfte und Schüler:innen sind frei im Netz verfügbar!

- *Was denken Sie? (Wenn nichts kommt: Wie fühlen Sie sich damit?)*
- *Hatten Sie schon einmal einen ähnlichen Vorfall mit Bezug zu den Themen Cyber-Sicherheit oder Datenschutz? Wie sind Sie als Lehrer:in damit umgegangen?*

Kommen wir zurück zu dem Beispiel des Datenlecks bei der Lernplattform deiner Schule.

- *Was glauben Sie: welche Daten von Ihnen sind jetzt im Netz verfügbar?*

Auch die Passwörter sind veröffentlicht worden.

- *Welche Gefahren können sich daraus ergeben?*
- *Nachhaken: Wie merken Sie sich Ihre Passwörter?*
- *Benutzen Sie eines oder mehrere Passwörter*
- *Falls Thema bei Antworten nicht angeschnitten wird: Benutzen Sie dieses Passwort auch für andere Onlinedienste?*

Wir sprachen gerade beispielhaft über die Nutzung einer Lernplattform. Die meisten Menschen benutzen im Laufe des Tages viele unterschiedliche Webseiten und Apps wenn Sie im Internet sind. Zum Beispiel, wenn Sie ein Produkt über Amazon kaufen, könnten neben den Daten Ihres Benutzerkontos noch weitere Daten von Ihnen gesammelt werden.

- *Welche Daten könnten das sein und warum werden diese gesammelt?*

Tatsächlich gibt man meistens selbst sein Einverständnis für die Sammlung dieser Daten. An dieser Stelle finden wir interessant:

- *Wenn Sie sich eine App runterladen, installieren oder in einem anderen Setting nutzen (z.B. Schule): Schauen Sie sich die voreingestellten App-Berechtigungen an?*
- *Lesen Sie die AGBs oder Datenschutzbestimmungen?*
- *Nachhaken: Haben Sie schon einmal darüber nachgedacht, eine bestimmte App/Online-Dienst (wie beispielsweise Amazon, Youtube oder Whatsapp) nicht mehr zu nutzen – und wenn ja, warum?*

Nachmittags

Nach Feierabend setzten Sie sich mit dem Smartphone auf die Couch. Sie bekommen eine WhatsApp von eine:m/r Freund:in gesendet, die/der Sie auf ein Video auf „yourtube.de“ aufmerksam macht.

- *Wie reagieren Sie darauf?*
- *Wenn von den Proband:innen nicht so recht eine Antwort kommt: Sie können entweder A: Auf Link klicken oder B: Erstmal nicht klicken, sondern überprüfen. Was machen Sie? (Bitte um Angabe der Proband:innen über den Chat)*
- *Wenn Sie B eingegeben haben: Was machen Sie stattdessen und warum? (Offene Frage)*

Wenn Sie auf den Link klicken, kommen Sie auf eine Seite, die aussieht wie Youtube und Sie sehen dort ein Katzenvideo.

- *Noch merken Sie nichts… Aber was könnte jetzt schon mit Ihrem Smartphone passiert sein?*
- *Wie können Sie das Risiko minimieren, dass Schadsoftware auf Ihr Smartphone kommt? (Betriebs-system- und App-Updates, Schutzsoftware, Rückfragen an den Versender)*

Sie haben sich mit dem Klick auf den Link einen Virus eingefangen. Sie kommen nicht mehr in Ihren Whatsapp-Account rein.

- *Was sollten Sie jetzt tun?*

Wahrscheinlich wurde Ihr Account gehackt; denn Sie sehen mit Entsetzen, dass sich irgendwer in Ihren Account einloggt und Hassbotschaften an Freunde und Bekannte verschickt.

- *Sie haben keine Ahnung, was zu tun ist. An wen wenden Sie sich?*
- *Hat Ihnen der Vorfall mit dem Virus zu denken gegeben?*

Sie möchten sich in Zukunft besser informieren.

- *Was tun Sie?*
- *Tun Sie etwas, um sich in Zukunft besser zu schützen?*
- *Wie würden Sie am liebsten Wissen zum Thema Cyber-Sicherheit vermittelt bekommen und wo?*
- *Nachhaken: Welche Maßnahmen zur Förderung von Kompetenzen von Lehrer:innen im Bereich Cyber-Sicherheit gibt es an Ihrer Schule?*
- *Worin sehen Sie die größten Herausforderungen für die Schulen, Kompetenzen zu Cyber-Sicherheit zu vermitteln?*
- *Welche Art von Bildungsangeboten würden Sie sich für sich und für Schüler:innen wünschen?*
- *Ziel: Bildungsangebote entwickeln*

Unsere Befragung ist nun zu Ende. Vielen Dank für Ihre Mitarbeit!