Ergebnisbericht des Work-streams „UpSchooling“

„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 Projektes „Dialog für Cyber-Sicherheit“ von November 2022 bis August 2023 erarbeitet.

Ideengeber des Workstreams waren Patrick Luzina (Bits und Bäume, Privacy Week Berlin) und Markus Saborowski (Bundesverband Smart City e.V.).

Mitwirkende Teilnehmer:innen des Workstreams waren (nach Nachnamen aufsteigend): Fatma Geisler (thefuturepast), Larissa Bläser, Hanna Heuer (BSI), Michaela Brauburger (Pädagogisches Landesinstitut Rheinland-Pfalz), Mirko de Paoli (Bundesverband Smart City e.V.), Markus Dölle (Privacy Week Berlin), Michael Große (Bundesinstitut für Risikobewertung), Laura Guntrum (Technische Universität Darmstadt), Anne Hennig (Karlsruher Institut für Technologie, KIT), Daniela Jäger-Biela (Fraunhofer IAIS), Bettina Kloppig (Bundesarbeitsgemeinschaft der Senioren-Organisationen, BAGSO), Claudius Link (Agile Security Consultant & Coach), Patrick Luzina (Bits und Bäume, Privacy Week Berlin), Nadja Menz (Fraunhofer FOKUS), Dror-John Röcher (intcube GmbH), Markus Saborowski (Bundesverband Smart City e.V.), Holger Schlösser (Fraunhofer FOKUS), Jörg Schüler (Digitale Helden gGmbH), Vivian Simon (selbstständige Dozentin und Autorin), Jolanda Todt (Freie Kommunikationsdesignerin), externe Beratung durch Steffen Haschler (CCC Mannheim).

Der Dialog für Cyber-Sicherheit ist ein Projekt des Bundesamtes für Sicherheit in der Informationstechnik (BSI), das vom Thinktank iRights.Lab und dem nexus Institut durchgeführt wird. Die Auftragnehmer haben dazu eine Geschäftsstelle eingerichtet. Beteiligte Mitarbeiter:innen der Geschäftsstelle am nexus Institut waren Maria Jacob, Justine Kenzler, Philipp Offermann, Luana Thor sowie Dr. Daniel Guagnin (Projektleitung) und Claudia Haas (stv. Projektleitung).

Der Workstream „UpSchooling“ wurde im Rahmen eines partizipativen und offenen Austauschs zwischen der Geschäftsstelle und den Teilnehmer:innen durchgeführt, die das Thema aus dem Bereich Cyber-Sicherheit für den Workstream im Rahmen der Denkwerkstatt gewählt haben.

Die vorliegende Dokumentation des Workstreams wurde von der Geschäftsstelle eigenständig erarbeitet. Die wiedergegebenen Ansichten spiegeln nicht zwangsläufig die Ansicht des BSI bzw. jedes einzelnen Teilnehmenden 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“:
http://www.dialog-cybersicherheit.de
Kontakt Geschäftsstelle (iRights.Lab und nexus Institut):
kontakt@dialog-cybersicherheit.de

Stand: Oktober 2023

Ein Projekt im Auftrag des:

iRights.Lab
Think Tank für die digitale Welt

nexus

Bundesamt für Sicherheit in der Informationstechnik

Executive Summary

Die Bedeutung von Cyber-Sicherheit für Schülerinnen und Schüler (SuS) wächst mit der zunehmenden Nutzung digitaler Endgeräte sowohl im privaten als auch im schulischen Kontext. Die Schülerinnen und Schüler sind in einer digitalisierten Welt Risiken und Gefahren ausgesetzt, die ihre Geräte, Daten und persönliche Sicherheit betreffen. Die Sensibilisierung für Cyber-Sicherheit und das Erlernen von technischen und sozialen Grundlagen sind für junge Menschen essenziell, um Sicherheitsrisiken einschätzen zu können und einen souveränen Umgang mit dem Internet zu entwickeln.

Aufbauend auf den Erfahrungen und Ergebnissen des Workstreams „Update4Schule“ im Rahmen des Dialogs für Cyber-Sicherheit 2021 wurde das Ziel des Workstreams „UpSchooling“ definiert. Es zielt darauf ab, Jugendliche zwischen 13 und 18 Jahren durch partizipative Workshops für Cyber-Sicherheitsthemen zu sensibilisieren. Die Schüler:innen sollen befähigt werden, Präventivmaßnahmen zum persönlichen Schutz umzusetzen und bei Cyber-Sicherheitsvorfällen angemessen zu handeln. Lerneinheiten, die von den Beteiligten mit bestehenden Lernangeboten entwickelt wurden, wurden in einem partizipativen Workshop mit den SuS getestet und unter Berücksichtigung ihrer Bedarfe weiterentwickelt.

Die Integration des Themas Cyber-Sicherheit in Schulen hat sich als äußerst positiv erwiesen. Engagierte Stakeholder:innen und gut durchdachte Ansätze haben dazu beigetragen, dass die Schüler:innen für das Thema sensibilisiert und für einen sicheren Umgang mit der digitalen Welt gestärkt wurden. Die Verwendung von nachhaltigem und zielgruppenspezifischem Material hat dazu beigetragen, die entwickelten Lerninhalte anschaulich und relevant zu gestalten.

Damit das Thema Cyber-Sicherheit nicht als isoliertes Projekt behandelt wird, ist es wichtig, solche Angebote in die Lehrpläne der Schulen zu integrieren. Eine kontinuierliche Wissensvermittlung ist essenziell, damit die nächste Generation gut informiert und verantwortungsbewusst mit Cyber-Sicherheitsthemen umgeht.

Inhalt

Abbildungsverzeichnis

1 Einleitung

Die Bedeutung von Cyber-Sicherheit für Schülerinnen und Schüler (SuS) wächst mit der steigenden Nutzung digitaler Endgeräte. Die Digitalisierung bei Jugendlichen betrifft sowohl ihr Privatleben als auch den schulischen Kontext, denn insbesondere im Zuge der Coronapandemie wurde der Schulalltag vermehrt digitalisiert. Doch ganz gleich, ob privater oder schulischer Kontext, Risiken und Gefahren bestehen bei der Nutzung einer Vielzahl von netzwerkfähigen Geräten hinsichtlich der Integrität des verwendeten Geräts und der Vertraulichkeit und Verfügbarkeit damit in Verbindung stehender Daten. Eine Sensibilisierung für Cyber-Sicherheit durch das Erlernen der technischen und sozialen Grundlagen der aktiven und passiven Nutzung des Internets und ein Grundverständnis der damit einhergehenden Cyber-Sicherheitsrisiken seitens der SuS ist aufgrund der besonderen Schutzbedürftigkeit junger Menschen essenziell. Ein souveräner Umgang mit dem Internet, die Einschätzung und die Bekämpfung von Sicherheitsrisiken sollten möglichst früh erlernt werden.

Aufbauend auf den Erfahrungen und Ergebnissen des Workstreams „Update4Schule“ im Rahmen des Dialogs für Cyber-Sicherheit 2021 ist das Ziel des Workstreams „UpSchooling“, Jugendliche zwischen 13 und 18 Jahren für Themen der Cyber-Sicherheit zu sensibilisieren und sie über entsprechende Risiken aufzuklären. Die SuS sollen befähigt werden, Präventivmaßnahmen zum persönlichen Schutz umzusetzen und auf Handlungsempfehlungen bei Cyber-Sicherheitsvorfällen zurückgreifen zu können. Deshalb sollen in einem partizipativen Workshop mit den Schüler:innen bestehende Lernangebote getestet und unter Einbezug der zielgruppenspezifischen Bedarfe weiterentwickelt werden.

2 Methodisches Vorgehen

2.1 Studiendesign und Stakeholder-Mitwirkung

Die Workstream-Arbeit wurde in drei Phasen umgesetzt. Die ehrenamtlich engagierten Stakeholder:innen haben an den verschiedenen Phasen in unterschiedlichen Funktionen teilgenommen.

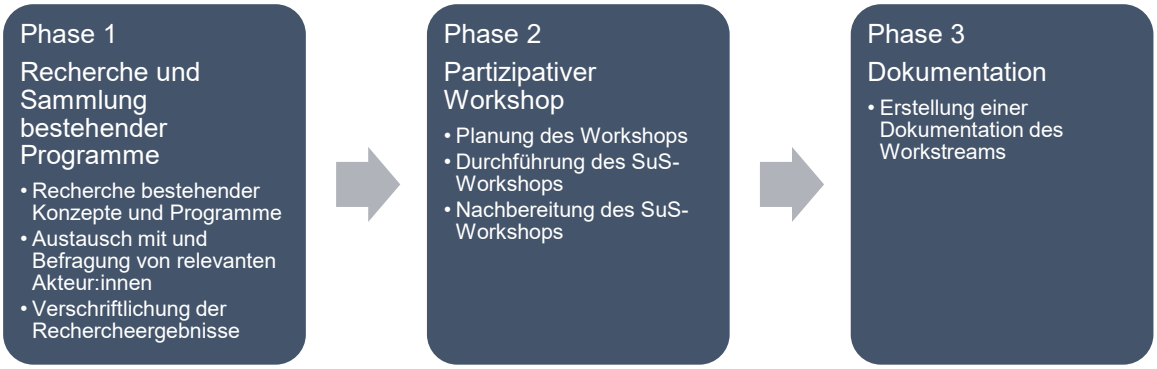


Abbildung 1: Phasen des Workstreams „UpSchooling“

2.2 Recherche bestehender Programme und Austausch mit Anbietern

In der ersten Phase wurde eine umfangreiche Recherche der bestehenden Lernangebote und vorhandenen Anbieter durchgeführt. Diese wurden im Workstream evaluiert und priorisiert. Nachdem mehrere Gespräche mit Anbietern geführt worden waren, wurde sich auf eine Priorisierung von acht Anbietern geeinigt. Diese umfasste: *Bildung, Bits und Bäume, Chaos macht Schule, DigiBits – Digitale Bildung trifft Schule, Digitale Helden, Gesellschaft für Medienpädagogik und Kommunikationskultur in der Bundesrepublik Deutschland e.V. (GMK), ISuMiS – IT-Sicherheit- und Medienkompetenz, JUUUPORT e.V.* sowie *klicksafe*.

Recherche und Sammlung bestehender Programme

Bildung, Bits und Bäume

Bildung, Bits und Bäume ist ein zweitägiges, jährliches Lernfestival, bei dem Studierende und Dozent:innen pädagogischer Studiengänge, Lehrkräfte, Schulleitungen und Schüler:innen gemeinsam konkrete Ideen entwickeln, wie Zukunftsthemen rund um Nachhaltigkeit und Digitalisierung in Schulen thematisiert werden können. Ein anderer Themenschwerpunkt ist zudem der Ausbau der Digitalisierung im Bildungsbereich. Hierzu werden während der zwei Festivaltage kostenfreie Workshops, Talks, Panels, Ideenlabore und Werkstätten angeboten. Das letzte Festival fand vom 30. September 2022 bis zum 01. Oktober 2022 statt. Der Termin für 2023 steht laut Webseite noch nicht fest.

Chaos macht Schule

Die Initiative „Chaos macht Schule“ des *Chaos Computer Club* hat sich als Ziel gesetzt, die Medienkompetenz und das Technikverständnis von Schüler:innen, Eltern und Lehrer:innen zu stärken. Das Projekt hilft Bildungsinstitutionen dabei, sich an die schnelle und vielfältige Entwicklung der neuen Medien und des Internets anzupassen, einen selbstverständlichen und trotzdem kritischen Umgang mit moderner Technik zu vermitteln und über Möglichkeiten, Risiken und Grenzen aufzuklären. Zu diesem Zweck bietet die Initiative ein eigenständiges Vortrags-, Workshop- und Schulungsangebot zu Themen wie Internetnutzung, Risiken sozialer Netze, Datenschutz, Urheberrecht im Netz und verwandten Themen an. Als konkrete Angebote für Jugendliche gibt es die Projekte „Rundgang durchs Internet“ und „Planspiel Datenschutz“ sowie Vorträge und offene Fragerunden. Zudem können Schüler:innen zu Medienscouts ausgebildet werden. Die Ansprechpartner:innen (Erfa-Kreise) sind regional verschieden.

DigiBits – Digitale Bildung trifft Schule

Das kostenfreie Angebot „DigiBits (Digitale Bildung trifft Schule)“ des gemeinnützigen Vereins *Deutschland sicher im Netz e.V.* richtet sich an Lehrkräfte und Schulen. Lehrkräfte sollen motiviert und befähigt werden, digitale Kompetenzen von Schüler:innen im Fachunterricht zu fördern. Zudem sollen Lehrende bei der Herausforderung, ihren Unterricht lehrplankonform an die Kultur der Digitalität anzupassen, unterstützt werden. Um Medienkompetenzen zu erwerben, zu vernetzen und zu unterrichten, prüft und bündelt „DigiBits“ didaktische Materialien und entwickelt daraus Unterrichtskonzepte. Darüber hinaus werden praxisorientierte Workshops, Austausch und Vernetzung sowie eine persönliche Begleitung der Partnerschulen angeboten. Es gibt einen Materialpool im Bereich Medienbildung mit Unterrichtsmaterialien zu Apps, Sicherheit im Netz, sicherem Suchen, Cybermobbing etc. Der „DigiBits“-Materialkoffer existiert in zwei Ausführungen: als Ordner- oder als Koffer-Materialmappe mit Lehrmaterialien zu fünf

Fachbereichen (einschließlich Medienbildung). Der Materialkoffer ist nur von Partnerschulen nutzbar.

Digitale Helden

Das gemeinnützige Unternehmen *Digitale Helden* vermittelt Wissen über den Umgang mit persönlichen Daten im Netz, die Vermeidung von Cybermobbing und andere aktuelle Online-Themen. Hierdurch soll die Medienmündigkeit und digitale Empathie von Jugendlichen gestärkt werden. Konkret werden kostenlose Webinare für Eltern und Pädagog:innen und kostenlose Online-Kurse für Schüler:innen zu Netz-Themen wie Stress im Klassenchat, Mobbing, Hass, Fake-Profile und radikale Meinung im Netz angeboten. Ergänzend gibt es ein Mentorenprogramm, das Schüler:innen der Klassenstufen 8 bis 10 zu Expert:innen der digitalen Welt ausbildet. Das Projekt „Digitaler Notfall" unterstützt Pädagog:innen dabei, mit digitalen Konflikten ihrer Schüler:innen umzugehen.

Gesellschaft für Medienpädagogik und Kommunikationskultur in der Bundesrepublik Deutschland e.V. (GMK)

Die *Gesellschaft für Medienpädagogik und Kommunikationskultur in der Bundesrepublik Deutschland e.V. (GMK)* setzt sich für die Förderung einer ganzheitlichen, umfassenden Medienpädagogik und Medienkompetenz ein. Hierbei sollen soziale, ethische, kulturelle, kreative und politische Aspekte mit technischen Kompetenzen und Voraussetzungen verknüpft werden. Die thematischen Schwerpunkte des Vereins richten sich an alle gesellschaftlichen Gruppen und werden in Projekten und Veranstaltungen vermittelt. Diese umfassen Medienkompetenz und Medienpädagogik, mediale Beteiligung, die Förderung von Kreativität und Kritikfähigkeit, den Dialog zwischen Medienforschung und Praxis, Medienbildung, die Unterstützung pädagogischer Fachkräfte, die Förderung junger Wissenschaft, Politikberatung sowie mediale Globalisierung. Konkret gibt es zwei Projekte, in denen die Medienpraxis von Geflüchteten (Kindern, Jugendlichen und Erwachsenen) sowie Kita-Kindern und Grundschüler:innen („MekoKitaService") geschult werden soll. Andere Projekte der GMK haben einen regionalen Bezug. Für die beiden genannten Projekte stehen Materialien zum Download bereit.

ISuMiS – IT-Sicherheit- und Medienkompetenz

Das vom Bundesministerium für Bildung und Forschung geförderte Projekt „IT-Sicherheit- und Medienkompetenz in Schulen" (ISuMiS) der *Fraunhofer-Institute FOKUS und IAIS* in Kooperation mit der *Hochschule für Technik und Wirtschaft Berlin* sowie *Junge Tüftler*innen gGmbH* möchte IT-Sicherheit und Datenschutz für Schüler:innen und Eltern praktisch erfahrbar machen und in den Schulunterricht integrieren. In den bereitgestellten Bildungs- und Begleitmaterialien geht es vor allem um sichere Informationstechnik, Sensibilisierung für Cybergefahren und Fragen zu IT-Sicherheit und Datenschutz. Die „ISuMiS"-Box beinhaltet frei nutzbare Lehrmaterialien zum Thema IT- und Datenschutz-Gefahren. Diese soll jedoch erst nach dem Projektabschluss im Jahr 2025 externen Partner:innen zur Verfügung stehen.

JUUUPORT e.V.

JUUUPORT e.V. ist ein Verein, der schnelle Hilfe und Beratung von Jugendlichen für Jugendliche anbietet. Der Fokus liegt vor allem auf den Themen Cybermobbing, Sexting, Cybergrooming, Hass im Netz, Mediensucht sowie Fake-News. Zu diesen Themen werden Beratung und Hilfestellung angeboten. Zusätzlich sollen Fragen zu Datenschutz und Bildrechten im Netz, Datenklau, Datenmissbrauch, Abzocke und Social-Media-Plattformen beantwortet werden. Der Verein bietet eine Reihe von kostenlosen Infomaterialien zu diesen Themen an. Zudem gibt es die Möglichkeit, sich als sogenannte *JUUUPORT*-Scouts ausbilden zu lassen.

klicksafe

Die EU-Initiative *klicksafe* verfolgt das Ziel, die Online-Kompetenz von Menschen aller Altersgruppen zu fördern und diese bei einem kompetenten und kritischen Umgang mit dem Internet zu unterstützen. Themenschwerpunkte sind Cybergrooming, Digital Wellbeing, Cybermobbing, Hate Speech, Medienerziehung und Privatsphäre. Diese Themen sollen den Zielgruppen durch Printmaterialien, visuelle, auditive und interaktive Medien, Materialien für pädagogische Fachkräfte, Elternarbeit sowie in Webinaren nahegebracht werden. Obwohl das Projekt bereits im Schuljahr 2017/18 durchgeführt wurde, stehen die Projektergebnisse und Unterrichtsmaterialien weiterhin zur Verfügung.

Austausch mit Anbietern

Mit der Priorisierung der vier besten Anbieter wurden von der Geschäftsstelle *Digitale Helden, Chaos macht Schule, DigiBits und Bildung, Bits und Bäume* für ein Austauschgespräch angefragt. Dieser Austausch hatte zum Ziel, einerseits von Erfahrungen der langjährig vernetzten Anbieter zu profitieren, andererseits aber auch Lücken in der Bildungslandschaft zu erfragen, um eine mögliche Positionierung und Ausrichtung des Workstreams zu eruieren. Im Februar 2023 konnten zwei Gespräche mit Jörg Schüler (*Digitale Helden*) und Steffen Haschler (*CCC Mannheim* und „Chaos macht Schule“) geführt werden. Im Folgenden findet sich eine Zusammenfassung der Gespräche. Ausführlich wurden die Gespräche im Zwischenbericht zur Phase 1 (Abrufbar auf der Website des Dialogs: *https://www.dialog-cybersicherheit.de/*) thematisiert.

Jörg Schüler ist Mitbegründer der gemeinnützigen Organisation *Digitale Helden*, die sich zum Ziel gesetzt hat, junge Menschen zu einem sicheren und verantwortungsbewussten Umgang im digitalen Raum zu befähigen. Die Organisation legt den Fokus auf soziale Kompetenzen und behandelt Fragen zur Kommunikation sowie zur Erkennung und Lösung kritischer Situationen im Internet. Jörg Schüler betont die Dringlichkeit einer guten Cyber-Sicherheitsschulung für Schüler:innen, Eltern und Lehrkräfte, da eine Sensibilität für bestimmte Risiken oft fehlt und kompetente Hilfe bei Cyber-Sicherheitsvorfällen häufig nicht vorhanden ist. Als mögliche Schwierigkeiten nennt er den Zeitmangel der Lehrkräfte und die bereits bestehenden, aber kaum genutzten Angebote zu Digital-Themen.

Weiterhin schlägt er vor, spielerische Angebote wie Quiz oder digitale Schnitzeljagden zu entwickeln und Inhalte in kleinen Häppchen zu vermitteln, um die Jugendlichen zu erreichen. Die Befähigung der Lehrkräfte und der menschliche Faktor sind entscheidend für den Erfolg der Schulungen. Die Inhalte sollen die digitale Lebensrealität der Jugendlichen ansprechen und interessante Themen aufgreifen. Dabei ist es wichtig, auch blinde Flecken zu berücksichtigen. Eine mögliche Kollaboration mit Jugendidolen wie Influencern wird ebenfalls erwähnt.

Das Gespräch mit Jörg Schüler bestätigt den Plan des Workstreams, spielerische Ansätze zu verwenden sowie gute und umfassende IT-Sicherheitsangebote für Schulen zu entwickeln, die sinnvoll in den Schulalltag integriert werden können. Solche Angebote fehlen Jörg Schüler zufolge bislang in der aktuellen digitalen Bildungslandschaft.

Steffen Haschler ist Lehrer für Mathematik, Informatik und Physik und ehrenamtlich im *CCC Mannheim* aktiv. Er unterstützt das Projekt „Chaos macht Schule“ im Rhein-Neckar-Gebiet und im gesamten DACH-Raum. „Chaos macht Schule“ ist eine Initiative des *CCC*, die Lehrkräfte, Eltern und Schüler:innen dabei unterstützt, Medienkompetenzen und Technikverständnis aufzubauen. Die Angebote und Aktivitäten der Initiative variieren je nach Engagement der Ehren-

amtlichen und können Workshops für Schüler:innen und Lehrkräfte oder politische und pressebezogene Arbeit umfassen. Das Hauptziel der Initiative ist, die digitale Mündigkeit der Jugendlichen zu stärken und sie zu kritischen und produktiven Anwender:innen digitaler Technologien zu machen.

Die Workshops von „Chaos macht Schule“ orientieren sich an den Interessen der Lehrkräfte und den Anknüpfungspunkten zum Lehrplan. Die Vertiefung der Themen während der Workshops mit Schüler:innen erfolgt entlang ihrer Lebensrealität und Interessen. Die Veranstaltungen dienen in erster Linie der Bewusstseinsbildung und sind weniger geeignet, um nachhaltig Wissen zu vermitteln.

Die Materialien für die Workshops werden von den Engagierten selbst bereitgestellt oder stammen aus verschiedenen frei zugänglichen Ressourcen. Dem Austausch und der Verfügbarkeit der Materialien liegen persönliche Vernetzung und eigenes Engagement zugrunde, sodass die Qualität der Materialien unterschiedlich sein kann.

Zur wirksamen Vermittlung von Inhalten zur Cyber-Sicherheit sind lebensnahe und eindrucksvolle Beispiele wichtig, um die kurze Aufmerksamkeitsspanne der SuS zu berücksichtigen. Qualitätvolle und niedrigschwellige Materialien sollten Lehrkräften vermittelt werden, damit sie die Inhalte erfolgreich an ihre Schüler:innen weitergeben können. Strukturell bedingte Ressourcenhemmnisse müssen bei der Ausgestaltung des Angebots berücksichtigt werden und es sollte an bestehende Netzwerke angeknüpft werden, um möglichst nachhaltige Ergebnisse bei der Verbreitung des Angebots zu erzielen. Gleichzeitig müssen Lehrkräfte über grundlegende Kenntnisse und ein gewisses Interesse verfügen, um Cyber-Sicherheitsthemen nachhaltig in den Unterricht integrieren zu können. Aspekte, die nicht im Lehrplan stehen, können selten in den schulischen Alltag eingebaut werden. Steffen Haschler empfiehlt daher, digitale Kompetenzen über die Lehrpläne zu vermitteln und Lehrkräfte entsprechend zu befähigen.

2.3 Konzeption der Lerneinheiten und Durchführung der SuS-Workshops

Auf der Grundlage der zusammengetragenen Lernangebote und der gewonnenen Einblicke aus den Anbietergesprächen wurde die zweite Phase des Workstreams angegangen. Diese umfasste die Planung und Konzeptionierung der Lerneinheiten und des partizipativen Workshops mit Jugendlichen an zwei Schulen. Hierbei sollten einerseits bestehende Materialien genutzt und ausgewertet werden und andererseits der Raum geschaffen werden, um Themen zu erörtern, die die Jugendlichen interessieren, sowie Methoden zu erproben, mit denen sie diese gut erlernen können. Die genaue Ausgestaltung dieser Workshops und die Konzeptualisierung der Lerneinheiten fand in mehreren Workstream-Treffen sowie einem längeren analogen Arbeitstreffen in Berlin statt.

Nach der Vorbereitung umfasste das Konzept für den ersten Workshop in Magdeburg fünf Lerneinheiten. Diese wurden für die Durchführung in zwei Blöcke á 45 Minuten aufgeteilt. Der erste Block umfasste die Module „Das Internet vergisst nicht“, „Smartphone- und App-Sicherheit“ sowie „Datenschutz und Nutzungsbedingungen“. Zum zweiten Block gehörten die Module „Sichere Passwörter“ und „Phishing“. Diese Aufteilung sollte sicherstellen, dass alle SuS ein grundlegenderes, theoretisches Thema aus dem ersten Block und ein spezifischeres, anwendungsbezogenes Thema aus dem zweiten Block belegt haben. An diese Lernphase schloss sich eine 90-minütige Reflexionsphase an, in der umfassendes Feedback der SuS zur Gestaltung der Module eingeholt wurde.

In der Konzeption der Lernmodule wurde darauf geachtet, einen Methoden-Mix zu verwenden und die Einheiten interessant und abwechslungsreich zu gestalten. Für den zu vermittelnden Input wurden deshalb im besonderen Maße visuelle und partizipative Methoden herangezogen. Neben der Nutzung kurzer Informationsvideos wurden (selbsterstellte) Quiz verwendet, um die SuS zu aktivieren und für das jeweilige Thema zu interessieren. Auch eigene Rechercheaufträge wurden in kurzen Selbstlerneinheiten vergeben. So sollten die SuS beispielsweise die Sicherheit verschiedener Passwörter in einem Passwort-Check eigenständig testen, die Traceroutes (Serververbindungen) verschiedener Webseiten verfolgen oder die Berechtigungen verschiedener Apps auf ihren Smartphones überprüfen. Alle in den Modulbeschreibungen genannten Quellen sind den beigefügten Handouts zu entnehmen.

Die Mitarbeiter:innen der Geschäftsstelle haben gemeinsam mit den Stakeholdern die beiden Workshops durchgeführt. Der erste Workshop fand am 19.06.2023 mit einer 10. Klasse des Editha-Gymnasiums Magdeburg statt. Der Workshop ging über fünf Schulstunden, von der zweiten bis zur sechsten Stunde. Die SuS wurden den beiden Lernblöcken zufällig zugeteilt, um Gruppenbildung und die Überbelegung einzelner Module zu vermeiden.

Die Ergebnisse des Schulworkshops in Magdeburg wurden mithilfe eines Gallery Walks, einer Strahlenbewertung der einzelnen Lernmodule und der Möglichkeit, Kommentare auf Moderationskarten zu verfassen, zusammengetragen. Im Gallery Walk hatten die SuS 30 Minuten Zeit, sich allein mit den verschiedenen Stationen zu befassen. Einzelne SuS, die die Stationen bearbeitet hatten, stellten diese den übrigen Mitschüler:innen vor. Parallel wurden den SuS fünfundzwanzig Klebepunkte ausgehändigt, mit denen sie an jeder Station fünf Fragen beantworten sollten:

1. Ich finde das Thema…überhaupt nicht bis sehr interessant.
2. Ich finde die angewandte Methode…überhaupt nicht bis sehr geeignet.
3. Ich finde die vermittelten Inhalte…überhaupt nicht bis total spannend.
4. Ich finde das Thema für mich als Schüler:in…überhaupt nicht bis total relevant.
5. Diesem Modul würde ich folgende Schulnote geben: (1-6)

Zusätzlich gab es die Möglichkeit, Gedanken und Kommentare auf Moderationskarten festzuhalten. Im Anschluss fanden sich die SuS in Kleingruppen zusammen und besprachen, wie einzelne Lernmodule oder auch der Workshop an sich verbessert werden könnten. Diese Erkenntnisse wurde auf weiteren Moderationskarten notiert und im Anschluss von den SuS im Plenum vorgestellt. Abschließend wurde ein kurzes Blitzlicht durchgeführt. Hierbei sollten die SuS sinnbildlich notieren, was für sie in den „Papierkorb“ gehört, was sie im „Koffer“ mitnehmen und wozu sie noch immer „Fragezeichen“ haben.

Ein zweiter Workshop mit SuS einer 8. Klasse des Englischen Instituts in Heidelberg fand am 20.07.2023 statt. Aufbauend auf den Rückmeldungen der Magdeburger Schüler:innen wurden die Module im Vorfeld angepasst. Gemeinsam mit den Stakeholdern des Workstreams konnten fünf Module umgesetzt werden. „Das Internet vergisst nicht“ war Grundmodul für alle SuS. In einem ersten Block fanden daran anschließend, dieses Mal mit freiwilliger Zuteilung, parallel die Module „Smartphone- und App-Sicherheit“ und „Datenschutz und Nutzungsbedingungen“ statt. Der zweite Block beinhaltete die Module „Sichere Passwörter“ und „ChatGPT/KI“. Anders als noch in Magdeburg mit Blöcken à 45 Minuten wurden in Heidelberg die Module in 60 Minuten durchgeführt. Dieses Vorgehen entsprach ebenfalls etwa fünf Schulstunden.

Auch bei diesem Workshop folgte auf die Lerneinheiten eine Reflexionsphase, in der die SuS ihre Eindrücke und Rückmeldungen zu den Formaten mitteilen konnten. Im Anschluss an jedes Lernmodul wurde ein QR-Code bzw. Link geteilt, über den die SuS mittels eines Befragungstools die Module bewerten konnten. Die Fragen glichen denen, die auch in Magdeburg gestellt wurden. Mit Beginn der Reflexionsphase wurden die Ergebnisse im Plenum besprochen, mündliche Nachträge wurden dokumentiert. Auf die Methodik des Gallery Walks wurde in Heidelberg verzichtet, vielmehr wurden in moderierten Kleingruppen inhaltliche Verbesserungen sowie fehlende und für die SuS interessante Themen gesammelt. Abgeschlossen wurde auch dieser Workshop mit einem Blitzlicht.

3 Ergebnisse

Die im Vorfeld definierten Ergebnisse des Workstreams umfassen angelehnt an die drei Phasen des Workstreams:

- eine **Sammlung bestehender Programme** (Selbstlernangebote, Workshops etc.) und Übersicht relevanter Themenbereiche zu Cyber-Sicherheit oder verwandter Themen für Schüler:innen bzw. Schulen,
- einen **partizipativen Workshop mit SuS**, anhand dessen Lernmaterialien (z. B. bestehende freie Bildungsmaterialien oder von den Workstream-Teilnehmenden (weiter-) entwickelte Materialien) zum Thema Cyber-Sicherheit evaluativ und integrativ entwickelt sowie weitere Erkenntnisse über den Bedarf (in Bezug auf die Themenauswahl und die geeigneten Methoden der Materialien) der SuS gewonnen werden und
- eine **Zusammenfassung** des methodischen Vorgehens im Workstream und der dabei gesammelten Erkenntnisse in einer Dokumentation.
- Optional wird ein Konzept bzw. ein geeigneter Rahmen für die Bereitstellung bzw. Veröffentlichung der von den Stakeholdern zusammengestellten Lernmaterialien zum Themenkomplex Cyber-Sicherheit entwickelt.

Die in Phase 1 erfolgte Sammlung bestehender Programme wurde in Form eines Zwischenberichts angelegt. Dieser Bericht umfasst die Dokumentationen der Anbietergespräche und der recherchierten Lernangebote und Anbieter, die im Laufe der Workstream-Zeit fortlaufend nachgetragen wurden. Auf diese Weise entwickelte sich als erstes Ergebnis des Workstreams ein umfassendes Dokument über die Angebotslandschaft zum Thema Cyber-Sicherheit für SuS. Dieses ist auf der Webseite des Projektes einzusehen (Link: *https://www.dialog-cybersicherheit.de/*).

Diese Zusammenfassung der Arbeit und der Projektschritte sowie die Ergebnisse der Workshops, in Form ausgearbeiteter Lerneinheiten, sind die wesentlichen Ergebnisse des Workstreams. Anders als zunächst geplant, ergab sich durch den Kontakt zu Steffen Haschler die Möglichkeit, einen zweiten partizipativen Workshop durchzuführen. Die beiden ganztägig durchgeführten Workshops mit SuS in Magdeburg und Heidelberg führten bei der Geschäftsstelle sowie den Stakeholdern zu hilfreichen Erkenntnissen über die wahrgenommenen relevanten Themen der jungen Zielgruppe. Sie ermöglichten die Weiterentwicklung der Lernmaterialien bzw. -module. Weiterhin konnte das optional geplante Konzept zur Bereitstellung bzw. zur Veröffentlichung der konzipierten Lernmaterialien durch die Initiative einiger Stakeholder:innen ausgearbeitet werden. In Form von drei Videos werden die Informationen aus drei ausgewählten Lerneinheiten für die Zielgruppe bereitgestellt. Somit gilt auch das optionale Konzept zur Bereitstellung von Lernmaterialien als Ergebnis des Workstreams.

Im Folgenden werden die sechs entwickelten Lernmodule mit ihren thematischen und methodischen Schwerpunkten beschrieben. Die entsprechenden Materialien zur Durchführung eines Moduls, die ausführlichen Moderationspläne sowie die PowerPoint-Präsentationen sind auf der Webseite des „Dialog für Cyber-Sicherheit“ zu finden. Zunächst werden die wesentlichen Methoden und Inhalte der Lernmodule dargestellt (Kapitel 3.1). Aufbauend auf dem Feedback der SuS wurden die Lernmodule zwischen den Workshops in Magdeburg und Heidelberg teilweise umgebaut, die Anpassungen werden ebenfalls beschrieben. Die Rückmeldungen der SuS werden im Kapitel 3.2 thematisiert. Stimmungsbild, Rückmeldungen zur Eignung der Module und Kommentare im Abschlussblitzlicht geben Aufschluss über die Einstellungen und Bedenken der SuS und sollen an dieser Stelle abgebildet werden.

3.1 Entwickelte Lernmodule

Das Internet vergisst nicht

In diesem Modul werden die Schüler:innen auf eine spannende Reise durch die Welt des Internets und seine vielfältigen Herausforderungen mitgenommen. Ziel des Moduls ist, dass die SuS ein umfassendes Verständnis für die historische Entwicklung des dezentralen Internets und die damit einhergehenden Risiken für ihren Alltag entwickeln.

Im Verlauf des Moduls werden die SuS mit einem faszinierenden Artefakt konfrontiert: dem Internetarchiv. Sie erfahren und begreifen, dass das Internet Informationen unwiderruflich speichert und somit nichts vergisst. Darüber hinaus werden sie über die Unterschiede zwischen clearweb, deepweb und darkweb informiert.

Ein weiterer wichtiger Aspekt des Moduls ist die Auseinandersetzung mit der komplexen Rechtslage im World Wide Web. Die SuS lernen, dass ihre Aktivitäten im Internet mit rechtlichen Konsequenzen verbunden sein können und dass Ländergrenzen nicht wie in der realen Welt funktionieren. Dies können die SuS mit verschiedenen Tools zu „traceroutes“ ausprobieren und erlangen so selbstwirksam neues Wissen.

Ein besonderer Fokus liegt auf der (Pseudo-)Anonymität im Netz. Die SuS erfahren, wie ihre Online-Aktivitäten nachverfolgt werden können und welche Möglichkeiten es gibt, sich zumindest teilweise anonym zu bewegen. Hieraus leiten sie angemessene Verhaltensweisen ab, um sich selbst und andere im digitalen Raum zu schützen.

Das Modul „Das Internet vergisst nicht“ vermittelt den SuS somit wichtige Kompetenzen, um sich sicher, selbstbestimmt und verantwortungsbewusst in der digitalen Welt zu bewegen. Es unterstützt sie dabei, die Chancen des Internets zu erkennen und gleichzeitig mögliche Risiken zu minimieren. Die erworbenen Kenntnisse und Verhaltensweisen sind nicht nur im schulischen Kontext, sondern auch im privaten und späteren beruflichen Leben von großer Bedeutung. Aus diesem Grund wurde das Modul beim zweiten Workshop in Heidelberg zum Grundmodul für alle SuS erklärt und der Arbeit in Kleingruppen vorangestellt.

Datenschutz und Nutzungsbedingungen/ Datenschutz als Selbstverteidigung

In diesem Lernmodul geht es darum, die SuS für den Schutz ihrer persönlichen Daten zu sensibilisieren. Das Modul zielt darauf ab, das Bewusstsein der Teilnehmenden für Datenschutzfragen zu schärfen und sie zu informierten Entscheidungen über ihre Daten zu ermutigen.

Zunächst wird ein Video über Datenschutz gezeigt, dass die Bedeutung des Datenschutzes und die Risiken der Datenverarbeitung erklärt. Anschließend nehmen die Teilnehmenden an

einem Quiz teil, um ihren Datenschutztyp zu ermitteln und über ihre Einwilligung in die Datenerhebung und -verarbeitung nachzudenken. Im Gruppengespräch werden anschließend verschiedene Datenschutzthemen diskutiert, etwa Messenger-Apps, App-Rechte, Ortungsdienste, digitale Sprachassistenten und Zahlungsmethoden. Es werden auch Punkte angesprochen, die zum Nachdenken anregen, wie die Nutzung von WhatsApp im Vergleich zu Signal, das Ausloggen bei Diensten oder die Wichtigkeit des Speicherorts von Terminkalendern und Fotos. Abschließend wird die Bedeutung von Nutzungsbedingungen hervorgehoben und die Teilnehmenden werden ermutigt, offene Fragen zu stellen und weitere Materialien zu diesem Thema zu erkunden.

Dieses Modul wurde im Anschluss an den Workshop in Magdeburg umfassend umstrukturiert und legte mit dem Workshop in Heidelberg den Fokus auf Selbstschutz und die Selbstverteidigung im Digitalen.

Zu Beginn werden die Teilnehmenden anhand dreier Fallvignetten dafür sensibilisiert, wie sie sich selbst schützen können und wie wichtig ihnen ihre Privatsphäre ist. Anschließend erfolgt eine Übertragung auf das Internet, um zu erfahren, wie die Teilnehmenden sich dort bislang schützen und wie gut ihr Wissenstand in diesem Bereich ist. Ein Video informiert darüber, welche Daten Unternehmen sammeln und wofür sie diese nutzen. In einem Gruppengespräch werden die Themen aus dem Quiz diskutiert und Rückfragen geklärt. Es erfolgt eine Zusammenfassung der Datenschutzmöglichkeiten mit einer offenen Diskussion darüber, warum Geheimnisse wichtig sind. Es wird auch über die weiteren Risiken im Netz gesprochen, insbesondere in Bezug auf personenbezogene Daten, die in Cookies und Berechtigungen abgefragt werden können. Ein weiteres Video klärt über Cookie-Einstellungen und deren Änderungsmöglichkeiten auf. Ein Quiz und eine Diskussion darüber, welche Apps bedenkenlos installiert werden könnten, sind ebenfalls Teil des Moduls. Gemeinsam werden abschließend Handlungsstrategien erarbeitet.

Sichere Passwörter

Das Modul „Sichere Passwörter“ widmet sich dem wichtigen Thema der Passwortsicherheit und zusätzlicher Schutzmaßnahmen für Online-Konten und ihrer Zugänge. In dem interaktiven Modul werden die SuS ermutigt, sich bewusst mit der Sicherheit ihrer Passwörter auseinanderzusetzen und den Schutz ihrer digitalen Identität zu stärken. Das Ziel des Moduls besteht darin, ein Verständnis für gute Passwörter zu vermitteln, Wege aufzuzeigen, wie man sichere Passwörter aufbewahren kann, und die Bedeutung eines zweiten Faktors für zusätzlichen Schutz zu erläutern. Das Modul vermittelt den jungen Erwachsenen wichtige Kompetenzen, um ihre Online-Konten besser zu schützen und sich sicher im Internet zu bewegen. Es fördert das Verständnis für die Bedeutung starker Passwörter und zusätzlicher Sicherheitsmaßnahmen, mit denen sie sich vor möglichen Gefahren im digitalen Raum schützen können.

Der Modulablauf sieht wie folgt aus: Das Modul beginnt mit einer offenen Abfrage der Anzahl der vorhandenen Accounts und Art der verwendeten Passwörter der SuS. Dabei wird ermittelt, wie die SuS derzeit mit ihren Passwörtern umgehen, sowohl bezüglich der Güte der Passwörter als auch der ungefähren Länge.

Anschließend werden die SuS in das Thema eingeführt, indem ihnen die essenzielle Bedeutung von Passwörtern zum Schutz ihrer Konten und Zugänge verdeutlicht wird. Die Analogie eines Zahlenschlosses für Fahrräder veranschaulicht die enorme Bedeutung sicherer Passwörter: mehr Stellen und ein größerer Zeichensatz erhöhen die Sicherheit signifikant. Gemeinsam werden die Kennzeichen eines guten Passworts sowie kritischer Passwörter erarbeitet.

In diesem Kontext werden die beliebtesten Passwörter in Deutschland aus dem 2022 diskutiert.

Ein Video ergänzt die Inhalte des Moduls und fördert das Verständnis für die Thematik. Gleichzeitig lernen die SuS eine Webseite kennen, auf der sie ein neues Passwort eingeben und auf dessen Sicherheit hin überprüfen lassen können.

Ein weiterer Schwerpunkt liegt auf der sicheren Aufbewahrung guter Passwörter. Die SuS erhalten eine Empfehlung für die Passwort-Datenbank-Software „KeePassXC“ und lernen anhand einer Demonstration, wie sie Einträge anlegen, Passwörter generieren und die Auto-Login-Funktion nutzen können.

Die Bedeutung eines zweiten Faktors (2FA) für die zusätzliche Absicherung von Accounts wird thematisiert. Verschiedene Beispiele für eine Zwei-Faktor-Authentifizierung werden erläutert, darunter SMS/Einmalcode, Yubikey, Authenticator App, Trusted Device, TAN und Biometrie. Die SuS werden dazu angehalten, die Vor- und Nachteile der verschiedenen Optionen abzuwägen.

Das Modul schließt mit einer Zusammenfassung und Sicherung der vermittelten Inhalte. Die SuS erhalten ein Checkblatt mit den wichtigsten Punkten. Idealerweise haben sie ein Bewusstsein dafür aufgebaut, dass kein System absolut sicher ist. Es wird betont, dass es dennoch wichtig ist, die Sicherheit der Bequemlichkeit in puncto Accountschutz vorzuziehen.

Die wesentlichen Änderungen im zweiten Modul „Sichere Passwörter“ liegen vor allem in der Verfeinerung der Inhalte und der Schwerpunktsetzung. Durch die Anpassung der Modulzeit von 45 auf 60 Minuten werden die einzelnen Punkte verlängert. Diese Anpassungen und Präzisierungen wurden vorgenommen, um den Inhalt des Moduls zielgerichteter zu vermitteln und die SuS optimal auf das Thema Passwortsicherheit vorzubereiten. Durch die Betonung bestimmter Aspekte sollen die Schüler:innen ein tieferes Verständnis für die Sicherheitsmaßnahmen im digitalen Raum entwickeln und besser darauf vorbereitet werden, ihre Online-Konten sicher zu verwalten.

Smartphone- und App-Sicherheit

Das Lernmodul „Smartphone- und App-Sicherheit“ führt die SuS spielerisch und interaktiv in das Thema ein und vermittelt ihnen wichtige Kenntnisse über die Bedeutung von App-Berechtigungen, den Umgang mit Apps und die Sicherheit beim Umgang mit Smartphones. Es fördert einen bewussten Umgang mit Apps und sensibilisiert für mögliche Risiken und Gefahren im digitalen Raum.

Zunächst wird eine lebendige Statistik erstellt, indem die SuS aufstehen, wenn eine Aussage zu ihren Erfahrungen mit App-Berechtigungen zutrifft. Dies dient dazu, sich gegenseitig kennenzulernen und das Thema auf lockere Weise einzuleiten.

Anschließend wird gemeinsam ein kurzes Video angeschaut, um das Thema App-Berechtigungen zu vertiefen. Dabei haben die Schüler:innen die Möglichkeit, Rückfragen zu stellen und Unklarheiten zu klären.

Im weiteren Verlauf des Moduls sollen die Schüler:innen überprüfen, welche Berechtigungen verschiedene Apps auf ihren Handys haben. Dazu teilen sie sich in Kleingruppen ein und untersuchen die Berechtigungen ihrer meistgenutzten Apps. Auf einem Arbeitsblatt können sie ihre Ergebnisse darstellen. Anschließend erfolgt die Vorstellung der Kleingruppenergebnisse und es wird darüber diskutiert, was die Schüler:innen dabei überrascht hat. Es werden erste Überlegungen gesammelt, warum es wichtig ist, über App-Berechtigungen Bescheid zu wissen.

Weiterführend wird ein Poster erstellt, auf dem relevante Informationen gesammelt werden. Die Schüler:innen erarbeiten gemeinsam, wo Apps heruntergeladen werden können, welche Informationen bei der Installation von Apps wichtig sind und welche zusätzlichen Informationsmöglichkeiten es gibt. Es werden Aspekte besprochen, auf die bei der Nutzung von Apps geachtet werden sollte, beispielsweise Kosten, das Mindestalter, In-App-Käufe, das Vermeiden von Werbung, das regelmäßige Aktualisieren von Apps und das Deinstallieren von nicht mehr verwendeten Apps.

Die wesentlichen Änderungen im Modul „Smartphone- und App-Sicherheit“ im Nachgang des Magdeburger Workshops sind zum einen dadurch bedingt, dass in Heidelberg mehr Zeit zur Verfügung steht, zum anderen auch durch den Wunsch der SuS nach mehr inhaltlicher Tiefe. Daher wurde in einem kurzen thematischen Input zusätzlich auf die Bedeutung von Big Data eingegangen und gemeinsam eine Collage zur Veranschaulichung von Datenflüssen erarbeitet. Die interaktive Gestaltung des Moduls mit der lebendigen Statistik und der Collage fördern das Mitwirken der SuS und ermöglichen eine aktive Auseinandersetzung mit dem Thema.

Insgesamt wurden die Modulinhalte erweitert und präzisiert, um den Fokus stärker auf die Thematik der App-Berechtigungen und deren Auswirkungen auf die Datensicherheit und Privatsphäre der Nutzer:innen zu legen.

Phishing

Das Modul bezweckt zum einen die Sensibilisierung für das Thema Phishing, zum anderen sollen den SuS die Merkmale von Phishing-Mails aufgezeigt und gemeinsam Schutzstrategien erarbeitet werden. Der Aufbau des Moduls fördert das Mitdenken und aktive Einbringen der Teilnehmenden, sodass sie besser für die Gefahren des Phishings sensibilisiert werden und praktische Schutzmaßnahmen erlernen.

Nach einem offenen Einstieg, der den Kenntnisstand der SuS abfragt, wird gemeinsam ein kurzes Video angeschaut, das das Thema Phishing erklärt. Eventuelle Verständnisfragen werden anschließend beantwortet. In der Problematisierungsphase werden den Schüler:innen Beispiele von Phishing-Mails gezeigt. Die SuS sollen diese Mails in Partnerarbeit analysieren und festhalten, welche Hinweise auf Phishing in den Mails vorhanden sind. Diese können auf einem Arbeitsblatt gesammelt werden.

Die erste Sicherung erfolgt im Plenum, die gesammelten Hinweise werden auf Moderationskarten festgehalten, geclustert und auf einem Plakat befestigt. Dabei werden Fragen zum Begriff Phishing, seiner Funktionsweise und den Merkmalen von Phishing-Mails diskutiert. Darauf aufbauend entwickeln die SuS Strategien, wie sie sich zukünftig vor Phishing-Mails schützen können. Diese werden ebenfalls schriftlich festgehalten und bei Bedarf ergänzt.

In den Rückmeldungen der SuS zeigte sich, dass das Modul thematisch nicht der Lebensrealität der Zielgruppe entspricht. Im Alter von ungefähr 16 Jahren haben die wenigsten eigene Bankkonten oder E-Mail-Postfächer, in der Regel werden diese von den Erziehungsberechtigten betreut. Trotzdem empfanden sie das Modul als interessant und spannend (siehe Feedback der SuS 3.2). Dennoch entschieden die Stakeholder:innen und die Geschäftsstelle, dass dieses Modul in der 8. Klasse in Heidelberg nicht angeboten wird. Für zukünftige Entwicklungen der Lerneinheit bietet sich die thematische Ausrichtung des Moduls an „Smishing“ (Phishing per SMS/Textnachricht) und Phishing-Nachrichten in den sozialen Medien an.

ChatGPT

Dieses Modul wurde nur in Heidelberg durchgeführt. Das Feedback der SuS in Magdeburg war Grundlage für diese Entscheidung. Das Thema ChatGPT wurde als relevanter als das

Thema Phishing bewertet und sollte durch die Teilnahme der zuständigen Stakeholderin in Heidelberg angeboten werden.

Das Modul zielt darauf ab, die Schüler:innen über lernende Modelle wie ChatGPT zu informieren, ihnen die Grundlagen der Funktionsweise zu vermitteln und sie aktiv in die Thematik einzubeziehen. Interaktive Elemente und eine Debatte befördern das Verständnis und ermöglichen den Teilnehmenden eine kritische Auseinandersetzung mit dem Einsatz selbstlernender Sprachmodelle im Unterricht.

Das Modul beginnt mit einer interaktiven Quizrunde, bei der die SuS Aussagen als richtig oder falsch einordnen, z. B. „In der Regel werden als Künstliche Intelligenz insbesondere Methoden des maschinellen Lernens bezeichnet“ (Antwort: richtig). Anschließend reflektieren sie die Quizfragen. Die erste Erarbeitung veranschaulicht, wie neuronale Netze funktionieren, indem die Schüler:innen eine einfache Bildererkennung in Gruppen durchführen. Die Idee ist, ein neuronales Netzwerk nachzubilden, in dem ein:e Schüler:in ein Bild nachzeichnet (z. B: eine Katze oder ein Auto), ein:e andere:r die Informationen sammelt (Kreise, Rechtecke, Dreiecke) und eine dritte Person die Informationen auswertet und auf das ursprüngliche Motiv zurückzuführen versucht.

In der Erklärungsphase wird mithilfe eines Videos verdeutlicht, wie ein neuronales Netz Daten analysiert und so die Ergebnisse generiert. Mit diesem gemeinsamen Verständnis zur Funktionsweise von Sprachmodellen findet eine Pro-Contra-Debatte über die Frage statt, ob selbstlernende Sprachmodelle wie ChatGPT im Unterricht eingesetzt werden sollten. Die SuS bilden zwei Gruppen und erarbeiten Argumente für oder gegen den Einsatz von ChatGPT im Unterricht. Mit einer vorgegebenen Zeit von wenigen Minuten werden die wesentlichen Argumente dargelegt und diskutiert. Ernannte Juror:innen verfolgen die Debatte und fällen abschließend ein Urteil.

3.2 Feedback der SuS

Stimmungsbild

Zu Beginn der Workshops in Magdeburg und Heidelberg haben die Jugendlichen ein vielfältiges Stimmungsbild abgegeben, indem sie ihre Einstellungen, Sorgen, wahrgenommenen Vorteile und Gedanken zum Thema Cyber-Sicherheit verschiedenen Emojis zuordnen konnten.

Wenige Jugendliche zeigten sich **skeptisch** und äußerten Bedenken bezüglich der Gefahr durch Viren und Trojaner. Sie betonten die Wichtigkeit von Datenschutzmaßnahmen auf Webseiten, die wichtig sind, um Vertrauen zum jeweiligen Anbieter aufzubauen.

Ein großer Teil der SuS war **nachdenklich** und verband mit dem Thema viele Fragen. Die SuS beschäftigten sich mit den Chancen und Risiken von Künstlicher Intelligenz, zum Beispiel im Bereich des autonomen Fahrens. Sie sprachen über die zunehmende Nutzung von KI und erwähnten Whistleblower wie Edward Snowden. Datenschutz, die Sorge vor Datenverlust und bürokratische Hürden in Schulen waren ebenfalls Thema, ebenso wie Bedenken über Unwissenheit im Umgang mit digitalen Technologien und die wirklichen Nutznießenden von Datensammlungen. Begriffe wie ChatGPT, Digitalisierung, Notwendigkeit, Schutz und Cookies wurden genannt und führten zusammen mit Fragen nach Nachteilen und ethischen Aspekten zum Schlagwort des gläsernen Menschen.

Eine Person zeigte sich **traurig** über die bestehende Unwissenheit bezüglich Cyber-Sicherheit und eine sogar **entsetzt**, dass Informationen gehackt werden können, die nicht bewusst preisgegeben werden.

Es gab aber auch Schüler:innen, die sich **zufrieden**, **froh** und sich sicher mit dem Thema fühlten, da bisher noch nichts Schlimmes passiert sei. Sie schätzten die Möglichkeit, etwas über das Thema zu lernen, und freuten sich darüber, dass man über das Internet neue Menschen kennenlernen kann und sie auf viele Informationen zugreifen können. Die Existenz von Zwei-Faktor-Authentisierung und Pop-up-Benachrichtigungen, insgesamt von einem guten Schutz vor Cyber-Attacken, wurde positiv bewertet.

Zusammenfassend zeigt das Stimmungsbild, dass die Jugendlichen ein breites Spektrum an Einstellungen und Gefühlen bezüglich Cyber-Sicherheit haben. Einige sind skeptisch und besorgt, während andere nachdenklich und interessiert sind. Neben positiven Empfindungen bleibt die Sorge um mangelhafte Kenntnisse und den Schutz der eigenen Daten präsent.

Eignung der Module

Bei den beiden Workshops mit Schüler:innen in Magdeburg und Heidelberg wurden die verschiedenen Module bewertet. Anhand von fünf Aussagen auf einer Strahlen- bzw. digitalen Sternebewertung konnten die SuS ihre Meinung abgeben.

1. Ich finde das Thema…überhaupt nicht bis sehr interessant.
2. Ich finde die angewandte Methode…überhaupt nicht bis sehr geeignet
3. Ich finde die vermittelten Inhalte…überhaupt nicht bis total spannend.
4. Ich finde das Thema für mich als Schüler:in…überhaupt nicht bis total relevant.
5. Diesem Modul würde ich folgende Schulnote geben: (1-6)

Die Bewertungen für die Eignung der jeweiligen Module sieht insgesamt wie folgt aus:

Das Modul „Internet vergisst nicht“ stieß bei den Schüler:innen auf mittleres bis sehr starkes Interesse. Die vermittelten Inhalte wurden als mittel bis total spannend empfunden. Das Thema wurde als relevant bis total relevant bewertet und die angewandte Methode wurde insgesamt als mittel bis geeignet angesehen.

Beim Modul „Smartphone- und App-Sicherheit“ gaben die Schüler:innen an, dass sie das Thema von interessant bis sehr interessant einschätzten. Die Inhalte wurden als mittel bis spannend empfunden und das Thema wurde als mittel bis relevant für ihre Zielgruppe bewertet. Die angewandte Methode wurde ebenfalls als mittel bis total geeignet wahrgenommen.

Dem Modul „Datenschutz und Nutzungsbedingungen“ standen die Schüler:innen aufgeschlossen gegenüber und fanden das Thema mehrheitlich sehr interessant. Die vermittelten Inhalte wurden als spannend bis sehr spannend bewertet, das Thema wurde als relevant empfunden. Die angewandte Methode erhielt eine insgesamt positive Bewertung und wurde als geeignet eingestuft.

„Sichere Passwörter“ wurde als interessantes Thema gewertet. Die SuS empfanden die Inhalte als spannend bis sehr spannend. Das Thema erhielt eine Bewertung von relevant bis sehr relevant, die angewandte Methode wurde als geeignet wahrgenommen.

Das Modul „Phishing“ wurde von den Magdeburger Schüler:innen als besonders interessant bis sehr interessant empfunden. Die vermittelten Inhalte wurden als spannend bis sehr span-

nend bewertet und das Thema erhielt, anders als in dem mündlichen Feedback in der Umfrage, eine hohe Relevanzbewertung. Die angewandte Methode zur Vermittlung wurde jedoch unterschiedlich bewertet: einige Teilnehmende sahen sie als nicht geeignet, andere als mittel bis geeignet an.

Schließlich wurde das Modul „ChatGPT“, das nur in Heidelberg angeboten wurde, von den SuS als sehr interessant und sehr relevant für die Zielgruppe eingestuft. Durchwachsen war die Bewertung der angewandten Methoden, mit einer positiven Tendenz zur guten Eignung, sowie die Bewertung der vermittelten Inhalte von mittel bis sehr spannend.

Die Bewertungen zeigen, dass die Schüler:innen unterschiedliche Interessen und Meinungen zu den verschiedenen Modulen haben. Es ist wichtig, diese Rückmeldungen zu berücksichtigen, um zukünftige Workshops zu verbessern und die Bedürfnisse der jungen Zielgruppe besser zu erfüllen. Durch eine gezielte Anpassung der Methoden und Inhalte können noch effektivere und ansprechendere Lernmaterialien geschaffen werden, die das Interesse und Wissen der Schüler:innen zum Thema Cyber-Sicherheit weiter steigern können.

Abschlussblitzlicht

Im Abschlussblitzlicht der Workshops zur Cyber-Sicherheit in Magdeburg und Heidelberg haben die Schüler:innen ihre Gedanken und abschließende Bewertung zum Workshop anhand der Kofferreflexion geäußert. Der Koffer entspricht symbolisch der Frage „Was nehme ich mit?“, der Papierkorb der Frage „Was war nicht so gut?“ und das Fragezeichen der Frage „Was ist mir noch unklar?“. Die SuS schrieben ihre Gedanken auf Moderationskarten und sortierten sie dann den drei Kategorien zu. Die Karten wurden im Nachgang von den Mitarbeitenden der Geschäftsstelle digitalisiert und in einer Tabelle geclustert (5.3 und 5.4).

Das im Abschlussblitzlicht in **Magdeburg** zusammengetragene Feedback der SuS zeichnet folgendes Bild: Die SuS nehmen die Wichtigkeit und Komplexität von Cyber-Sicherheit als Thema wahr. Generell gibt es das Grundgefühl, etwas gelernt zu haben und sich somit sicherer im Internet bewegen zu können. Explizit wurden folgende neue Lerninhalte hervorgehoben: Phishing-Strategien, Verständnis über Datenumgang und -missbrauch, Kenntnis über die Funktionsweise und Einstellung von App-Berechtigungen, die Wichtigkeit von 2FA und Datenschutz. Besonders das Modul zu sicheren Passwörtern hat einen nachhaltigen Eindruck bei den SuS hinterlassen. Dies spiegelt sich auch in der Strahlenbewertung wider, bei der das Modul mit einer Schulnote 1-2 am besten von den SuS bewertet wurde. Platz zwei teilen sich mit der Note 2 die Module „Smartphone- und App-Sicherheit“ und „Datenschutz und Nutzungsbedingungen“. Auf dem letzten Platz liegen mit einer Bewertung von 2-3 die Module „Das Internet vergisst nicht“ und „Phishing“. Dies scheint jedoch nicht an einem mangelnden inhaltlichen Interesse, sondern an den nur als mittelmäßig geeignet eingestuften Methoden gelegen zu haben.

Auf die Frage, welche Fragen die SuS noch zum Thema Cyber-Sicherheit haben, konzentrierten sich diese vor allem auf das Thema Hacking und die Nutzung der eigenen Daten. Hacking und der Diebstahl persönlicher Daten werden als akute Bedrohung wahrgenommen, bei der sich Fragen einer angemessenen Reaktion stellen. Den SuS wissen nicht, was mit ihren Daten passiert oder wie diese genutzt/ missbraucht werden könnten.

Negativ ist den SuS vor allem die fehlende Zeit aufgefallen. Dadurch sei eine nur oberflächliche Behandlung der Themen möglich gewesen. Außerdem wurde die zufällige Zuordnung in die Gruppen leicht kritisiert, da so keine Wahl nach eigenem Interesse möglich gewesen sei. Zudem wünschten die Schüler:innen, mehr auf die sozialen Auswirkungen und Gefahren von Social Media einzugehen.

Die SuS in **Heidelberg** haben gelernt, welche Gefahren im Internet lauern und wie wichtig es ist, auf die Sicherheit ihrer Daten zu achten. Sie haben Handlungs- und Umgangsstrategien kennengelernt, beispielsweise wie sie sich besser um ihre Apps kümmern können und welche Datenschutzmaßnahmen zu beachten sind. Besonderes Augenmerk wurde auf die Passwortsicherheit gelegt, die als essenziell betrachtet wurde.

Ein weiterer Punkt, der von den Schüler:innen hervorgehoben wurde, war das erworbene neue Wissen. Insbesondere das Verständnis für Traceroutes und die Möglichkeit, zu verfolgen, welchen Weg die Datenpakete physisch zurücklegen, wurden positiv bewertet. Obwohl einige Inhalte bereits bekannt waren, gab es dennoch neue Erkenntnisse, insbesondere in Bezug auf individuelle Interessensgebiete.

Die Diskussion über ChatGPT, bei der sowohl positive als auch negative Aspekte beleuchtet wurden, hinterließ ebenfalls Eindruck. Es wurde deutlich, dass der Workshop den Schüler:innen eine breitere Perspektive auf Künstliche Intelligenz und deren Auswirkungen ermöglichte.

Ein weiterer wichtiger Punkt war das Verständnis für Daten und deren Bedeutung. Die Schüler:innen erkannten, wie der Datenstrom verläuft und dass Daten sowohl gut als auch wichtig sind. Sie gewannen Einsichten in das Marketing mit Daten und unterstrichen die Wichtigkeit der Datensicherheit.

Insgesamt zeigten sich die Schüler:innen mit dem Workshop zufrieden, da viele ihrer Fragen geklärt wurden und sie sich besser auf den digitalen Raum vorbereitet fühlen. Der Workshop hat dazu beigetragen, ihr Bewusstsein für Cyber-Sicherheit zu stärken und ihnen wertvolle Werkzeuge an die Hand zu geben, mit denen sie sich vor den Gefahren im Internet schützen und verantwortungsvoll mit ihren Daten umgehen können.

3.3 Nachbereitung und Veröffentlichung der Lernmodule und -materialien

Nach den beiden durchgeführten Workshops wurden die Lernmodule und -materialien von der Geschäftsstelle und den beteiligten Stakeholdern aufbereitet. Handouts, die die wesentlichen Quellen und auch weiterführende Links umfassen, wurden den Schüler:innen im Nachgang der Workshops digital bereitgestellt. Sie lassen sich auf der Webseite des Projektes (*https://www.dialog-cybersicherheit.de/*) einsehen und herunterladen.

Zusätzlich zu den bereits dargestellten Ergebnissen des Workstreams „UpSchooling“ werden drei weitere Outcomes als Ergänzung zu den im Workstream entwickelten Selbstlernmodulen für Schüler:innen entwickelt.

Konkret wurden Videos zu drei verschiedenen Themen aus dem Bereich IT-/Cyber-Sicherheit für die Zielgruppe der 13- bis 18-jährigen Schüler:innen produziert, zu denen im Workstream bereits Lernmodule entwickelt und mit Schüler:innen getestet wurden.

Die filmische Umsetzung der im Workstream erarbeiteten Materialien hat zum Ziel, Jugendliche und junge Erwachsene für Themen der Cyber-Sicherheit zu sensibilisieren – die zentrale Aufgabe des Workstreams. Durch die Veröffentlichung auf einer Videoplattform können die Filme als Selbstlernmaterialien eingesetzt werden; zentrale Inhalte der Workshops werden auf diese Art und Weise niederschwellig vermittelt. Zudem können die Videos in dem etablierten Format ein weitreichendes Interesse erzeugen, sich mit den Materialien auseinanderzusetzen und sie im persönlichen und schulischen Alltag in die Anwendung zu bringen.

Die Videos werden nach der Veröffentlichung über die Projektwebseite zugänglich gemacht.

4 Fazit

Die Integration des Themas Cyber-Sicherheit in die Schulen hat sich als äußerst positiv erwiesen. Dank guter Ansätze und engagierter Stakeholder:innen ist es gelungen, die Schüler:innen für das Thema zu sensibilisieren und für einen sicheren Umgang mit ihrer zunehmend digitalen Welt zu stärken. Die Verwendung von reichhaltigem und geeignetem Material aus der Zivilgesellschaft hat dabei geholfen, die Lerninhalte anschaulich und zielgruppengerecht aufzubereiten und zu gestalten.

Wenn sichergestellt werden soll, dass das Thema nicht nur als isoliertes Projekt behandelt wird, sondern einen festen Platz im Bildungssystem einnimmt, dann müssen solche und Angebote anderer Anbieter in die Lehrpläne der Schulen übernommen werden. Nur dann kann die Wissensvermittlung kontinuierlich stattfinden und dazu beitragen, dass die nächste Generation gut informiert und verantwortungsbewusst mit Cyber-Sicherheitsthemen umgeht und im digitalen Alltag souverän und selbstbestimmt handelt.

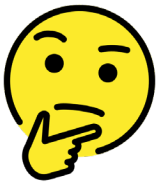
Als besonderer Nachtrag zu den Lernmaterialien, die von den Stakeholdern und der Geschäftsstelle erarbeitet wurden, können die konzipierten Videos auch Schüler:innen erreichen, die nicht an den Workshops teilgenommen haben. Die Videos können eine breite Zielgruppe ansprechen und das Interesse für das Thema auch außerhalb des Unterrichts wecken.

Die bisherigen Ergebnisse sind vielversprechend und es bleibt zu hoffen, dass das Engagement für Cyber-Sicherheit in Schulen wächst, sich etabliert und langfristig positive Auswirkungen auf die Ausbildung von Kompetenzen bei jungen Erwachsenen haben wird.

5 Anhang

5.1 Stimmungsbild Magdeburg

Skeptisch:
Gefahr durch Virus und Trojaner
Vertrauen auf Websites mit Datenschutz



Nachdenklich:
KI (Chancen und Risiken?) z.B. autonomes Fahren
Immer mehr KI-Erstellungen
Whistleblower (Snowden)
Datenschutz und Bürokratie in der Schule
Unwissenheit
ChatGPT?!
Digitalisierung?!
Notwendigkeit?!
Schutz?
Nachteile?
Cookies?!
Ethische Aspekte
Der gläserne Mensch?!

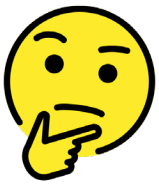
Traurig:
Unwissenheit

Zufrieden:
Nichts passiert bis jetzt
Etwas zu lernen
Wird durch Pop-Ups aufmerksam gemacht
Automatisch abgesichert (2-Faktoren-Authentifizierung)

5.2 Stimmungsbild Heidelberg

Glücklich:
Man kann neue Menschen (Freunde) kennenlernen und sich treffen mit Menschen, die weiter weg wohnen
bringt viele Informationen
Leichtere Kommunikation
Kleidung kaufen wird leichter

Zufrieden:
Ich bin glücklich bzw. neutral, denn wir haben gute Informatikschutz vor cyber attacks.
unpräsent
Eig. merkt man nicht, wie seine Daten benutzt werden. Deswegen finde ich es entspannt und gut
Unpresent
Bin glücklich, weil man alle Artikel, die man will, dort finden kann



Nachdenklich:
Nachdenklich wegen evtl. Datenverlust
Nicht angegebene Daten trotzdem herausgegeben werden
Schwer zu erkennen, wer Daten haben will & wer nicht / bekommt

Entsetzt:
Es können Infos gehackt werden, die nicht preisgegeben wurden

5.3 Abschlussblitzlicht 19.06.2023, Magdeburg

Koffer: Was nehme ich mit?		**Fragezeichen: Was ist mir noch unklar?**		**Papierkorb: Was war nicht so gut?**	
Cluster	**Karte**	**Cluster**	**Karte**	**Cluster**	**Karte**
Relevanz des Themas	Wichtigkeit der Cybersicherheit (Passwörter, Datenschutz), Komplexität des Themas	Datenschutz/-sicherheit	Wie lässt Datenschutz unsere Daten nicht in die Öffentlichkeit? Viele Fachbegriffe bei dem Thema	Themenauswahl	Fehlende Aufklärung über die Gefahren von sozialen Medien
	Dass Cybersicherheit sehr wichtig ist, vor allem Passwörter		Was ist eine IP-Adresse, und wie funktioniert sie		Nicht alle Gruppen (chaotisch)
Neues Wissen	Viel Neues über Cyber-Sachen gelernt, fühle mich sicherer im Umgang mit dem Internet		Wie werden die Daten nach dem Kauf von Unternehmen verwaltet, was genau passiert mit ihnen, & zu welchem Preis werden sie verkauft?		Fehlende Aufklärung über die Auswirkungen von social media und wie es Leben zerstören kann und auch in Schulen & wie Menschen sich dadurch ungewollt oder unwohl fühlen
	Dass Daten sehr schnell von anderen geklaut werden können				
	Dass Cybersicherheit viel mehr umfasst, als einfach nur aufpassen, dass man auf nichts Falsches klickt		Was passiert mit unseren Daten, wenn sie gehackt werden?		„Wahl“ der Module [gemeint: Gruppenzuteilung und Themenauswahl]
	Vorhandenes Wissen hat sich bestätigt. Passwort-Thema war sehr interessant		Gibt es Nachteile durch den Datenschutz?	Gruppenzuteilung	Gruppeneinteilung: dadurch hat man nur einen kleinen Teil der Themen kennengelernt
	Datenschutz kann nervig sein, hilft uns aber	Handlungs- und Umgangsstrategien	Umgang mit den Daten		Gruppeneinteilung und sehr wenig Zeit für sehr umfangreiche Themen
	2FA wichtig!!!		Was tue ich, wenn ich gehackt werde?		Zufall, welche Themen man behandelt; nur 2 von 5 Themen behandelt
	Datenschutz ist viel wert!				

	Viele Infos zu Passwörtern		Was man machen kann, wenn man gehackt wurde		Nicht alle Gruppen (chaotisch)
	Neue Kenntnisse im Thema Datenschutz		Folgen der Internetnutzung, Gefahren	Zeit	Zu wenig Zeit (4x)
Neue Strategien und Umgang erlernt	Passwort dringend ändern	Hacking	Infos zum Hacking		Zeiteinteilung
	Die Strategien der Phisher*innen, um im Vorhinein nicht darauf hereinzufallen				Dass wir so wenig Zeit hatten und alles nur oberflächlich behandelt wurde
	Vorsicht im Netz				Zeitmanagement
	Man muss App-Berechtigungen von Zeit zu Zeit überprüfen				Oberflächlichkeit vieler Themen aufgrund von Zeitmangel
	Sichere Passwörter nutzen				
	Sicherheit bei Passwort wahren				
	Mein Passwort muss erneuert werden				
	Wie ein Passwort sicher wird				
	Auf was ich bei Emails und Passwörtern achte				

5.4 Abschlussblitzlicht 20.07.2023, Heidelberg

Koffer: Was nehme ich mit?	
Cluster	**Karte**
Gefahren im Netz	man sollte auf seine Sicherheit der Daten achten
	Was die Gefahren im Internet sind
	Wissen über Gefahren
Handlungs- und Umgangsstrategien	Alle guten Infos, z.B. wie ich mich mehr um meine Apps kümmere
	Datenschutz: worauf man noch achten kann
	Apps nicht auf alles zugreifen lassen
	Wie ich mich mehr um meine Apps kümmere
	Passwortsicherheit (2x)
Neues Wissen	Traceroute: zu sehen, von wo nach wo die Website geht
	Wissen über traceroutes
	Nicht so viel: meist war der Inhalt schon bekannt
	Mehr Infos über Dinge, die mich interessieren
	Es gibt positive und negative Dinge bei ChatGPT
Daten	Wie der Datenstrom verläuft
	Daten sind gut und wichtig
	Wissen über Marketing mit Daten
	Schauen wo die Daten hingehen
	Datensicherheit ist wichtig
	Die Fragen wurden geklärt! 😊

Fragezeichen: Was ist mir noch unklar?	
Cluster	**Karte**
traceroutes	traceroute
	traceroute
	Dieses trace Teil
Geschichte des Internets	Wie entstand das Internet? Was hat der Erfinder geplant?
Workshop	Was die anderen gemacht haben

Papierkorb: Was war nicht so gut?	
Cluster	**Karte**
Inhaltliche und methodische Kritik	Den ersten Workshop über Datenschutz
	Zu viel über Passwörter
	Es dauert den ganzen Tag
	Funktion von KI muss nicht mehr erklärt werden
	Keine gute Zusammenfassung der anderen [Einheiten]
	Alles war gut
	Man konnte nicht KI UND Passwort machen