4school SecAware

Informationssicherheits-bewusstsein für den Schulalltag

SecAware4school

Gefördert von
HGS Horst Görtz Stiftung

Technische Hochschule Wildau
Technical University of Applied Sciences

Margit Scholl (Hrsg.)

Informationssicherheitsbewusstsein für den Schulalltag

SecAware4school

Margit Scholl (Hrsg.)

Informationssicherheitsbewusstsein für den Schulalltag

SecAware4school

Buchwelten Verlag
FRANKFURT AM MAIN

Bibliografische Informationen der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Empfohlene Zitierweise:
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.

Informationssicherheitsbewusstsein für den Schulalltag
SecAware4school

Imprint
Informationssicherheitsbewusstsein für den Schulalltag
SecAware4school

1.Auflage 2020
eBook-Ausgabe 2020

Printed in Germany.
© 2020 by Bubans Buchwelten Verlag,
Frankfurt am Main
Published by
Bubans Buchwelten Verlag
Hugo-Sinzheimer-Straße 15
Frankfurt am Main
http://www.buchwelten-verlag.de

ISBN: 978-3-945740-13-2

Informationssicherheit für den Schultag

(SecAware4school)

Projektlaufzeit 01.09.2018 – 31.12.2020

Schuktomow, Regina

Scholl, Margit (Prof. Dr.)

Koppatz, Peter

Edich, Denis

Gube, Stefanie

Gerlach, Josephine

4school SecAware

GEFÖRDERT VON HGS Horst Görtz Stiftung

Technische Hochschule Wildau Technical University of Applied Sciences WILDAU

Inhalt

Abkürzungsverzeichnis

AL.....Accelerated Learning

AT ..... Awareness Training

DG ..... Durchgang/Durchgänge

FSG.....Friedrich-Schiller-Gymnasium Königs Wusterhausen

FWG .....Friedrich-Wilhelm-Gymnasium Königs Wusterhausen

GBL .....Game-based Learning

GKW.....Staatliche Gesamtschule Königs Wusterhausen

(ehem. Dr. Hans Bredow Oberschule)

HGB .....Humboldt-Gymnasium Berlin

HGO.....Dr. Hans Bredow Oberschule Königs Wusterhausen

LS ..... Lernszenario

MA ..... Mitarbeitende

RVO..... Rudolf-Virchow-Oberschule Berlin

TH Wildau.....Technische Hochschule Wildau

ZIT-BB .....Brandenburgischer IT-Dienstleister

IT-SiBe.....Informationssicherheitsbeauftragte/r

Abbildungsverzeichnis

Tabellenverzeichnis

Kurzdarstellung

Die Nutzung von digitalen und smarten Endgeräten wie Tablets, Smartphones, Smartwatches etc. ist nicht mehr aus dem Alltag wegzudenken. Alles in unserer Umgebung wird smarter und so schreitet die Digitalisierung unserer Gesellschaft voran. Es ist praktisch unmöglich, Kinder und Jugendliche in einem gut entwickelten Industrieland, wie Deutschland, ohne den Einfluss von Internet aufwachsen zu lassen. Umso wichtiger ist es, sie für die Nutzung von Internetservices zu sensibilisieren. Das Projekt „Informationssicherheitsbewusstsein für den Schulalltag (SecAware4school)“, gefördert durch die Horst Görtz Stiftung, möchte Schülerinnen und Schülern eine eigene Risikobewertung ermöglichen und sie spielerisch im sorgsamen Umgang mit personenbezogenen Daten bei der Nutzung von Internet Services und sozialen Netzwerken schulen. An der Technischen Hochschule Wildau (TH) wurden in den vergangenen zwei Jahren Konzepte und innovative Lernszenarien mit Zertifizierung entwickelt, die als Maßnahmen zur Sensibilisierung des Bewusstseins und der Kompetenzen bezüglich Informationssicherheit von ca. 600 Schülerinnen und Schülern wie auch Lehrenden und Eltern erprobt und durchgeführt wurden.

In der Pilotgruppe aus fünf Schulen in Berlin und Brandenburg waren Schülerinnen und Schüler unterschiedlichen Alters der Klassenstufen 6 bis 11 vertreten. Dem variierenden Wissensstand zwischen den Altersgruppen wurden wir gerecht, indem die einzelnen Lernszenarien für drei Schwierigkeitsstufen (angepasst an die Klassenstufe) entwickelt wurden. Um das komplexe Thema der Informationssicherheit den Teilnehmenden leicht begreifbar, haptisch und erlebbar zu vermitteln, wurde ein methodischer Ansatz für die Sensibilisierung gewählt, der möglichst viele kreative und interaktive Lehr- und Lernmethoden beinhaltet. Aus Erfahrung vorangegangener Projekte und auf Basis aktueller Forschungserkenntnisse zur Wirksamkeit von Sensibilisierungsmaßnahmen wurden gemäß dem *Game-based Learning* Ansatz analoge und digitale spielbasierte Lernszenarien, auch *Serious Games* genannt, entwickelt, erprobt und evaluiert. Im Projekt SecAware4school wurden insgesamt 36 Lernszenarien zur Informationssicherheit entwickelt: acht analoge und vier digitale Lernszenarien in jeweils drei unterschiedlichen Schwierigkeitsgraden. Alle Lernszenarien in SecAware4school wurden mit hohem Einsatz im Forschungsprojekt konzipiert und entwickelt. Nach dem Projektende sind alle digitalen Simulationen über die Webseite (https://secaware4school.wildau.biz) abrufbar und kostenfrei nutzbar. Die Anleitungen zum Ausdrucken der analogen Lernszenarien stehen auch auf der Internetseite allen Interessierten kostenfrei zur Verfügung.

Die wissenschaftliche Begleitforschung zur Wirksamkeit der Sensibilisierungsmaßnahmen und der entwickelten Lernszenarien zeigt, dass die teilnehmenden Schülerinnen und Schüler mit dem methodischen Ansatz ausgesprochen zufrieden sind. Auf Grundlage der Projekterfolge wird angestrebt, in Schulen „Informationssicherheit“ als Unterrichtsfach und/oder Projekttage zu etablieren.

Der methodische Schwerpunkt basiert dabei auf einem Game-based Learning (GBL)-Ansatz, mit dem Lehr- und Lernmethoden in analoger und digitaler Form zu Themen der Informationssicherheit entwickelt wurden. Dieser GBL-Ansatz basiert auf psychologischen Erkenntnissen aus der betrieblichen Awarenessforschung (Helisch und Pokoyski 2009) (Pokoyski 2009) (Haucke 2018) und konnte bereits in zwei vorangegangenen Forschungsprojekten (SecAware4job[1], Security[2]) mit anderen Zielgruppen erfolgreich umgesetzt werden. Im Sinne des Authentic Learning- und Accelerated Learning-Ansatzes sind Anpassungen von spielbasierten Lernszenarien an den konkreten Schwierigkeitsgrad und ihre Bezüge für den Lernerfolg von großer Bedeutung. Neben der Spezifizierung von Inhalten auf die von Teilnehmenden gewünschten Themenbereiche der Informationssicherheit sind auch kulturelle und sprachliche Aspekte zu berücksichtigen. Die drei Schwierigkeitsgrade unterscheiden sich nicht nur durch die Inhalte, die an den Wissensstand der Teilnehmenden angepasst sind, sondern auch in ihrer vereinfachten Sprache für die jüngeren Klassenstufen. Zusätzlich wurde bereits eines der digitalen Lernszenarien vom Projekt SecAware4school auf Englisch konzipiert. Damit fördert und unterstützt das Projekt SecAware4school neben der an die Bedürfnisse und Altersunterschiede angepasste Wissensvermittlung auch die Internationalisierung an den Schulen.

[1] http://secaware4job.th-wildau.de/
[2] https://security.wildau.biz/de.html

1 Ausgangssituation

Längst ist ein Hacker-Angriff nicht nur für Informatiker und Programmierer eine Gefahr. Immer häufiger werden Menschen im privaten Bereich zu Opfern der Angriffe, um auch an das eigentliche Ziel, das Unternehmen, heranzukommen (Schonschek 2020). Die Analyse/Aufarbeitung solcher Angriffe zeigt, dass der Faktor Mensch der größte Angriffssektor ist, denn menschliche Unwissenheit und die damit verbundenen Schwachstellen können leicht ausgenutzt werden. Alle Cyberattacken beziehen sich auf den Missbrauch von Daten oder auf die Störung von IT-Systemen (Security Awareness 2020). Informationen sind nutzbringend, weswegen z. B. unzählige Unternehmen die Daten der Kunden sammeln und auswerten, um sich gewinnbringende Handlungsmaßnahmen zu verschaffen. Das Ausspähen der Informationen erstreckt sich vom Surfen im Internet über Onlineeinkäufe bis hin zur Speicherung der personenbezogenen Daten auf fremden externen Servern. Der Schutz personenbeziehbarer und personenbezogener Daten sowie sensibler Informationen stellt eine Herausforderung in der heutigen voranschreitenden Digitalisierung dar.

Umso wichtiger ist der achtsame Umgang mit Informationen. Voraussetzung dafür sind die Kenntnisse über die Grundwerte der Informationssicherheit: Vertraulichkeit, der Schutz vor unbefugter Preisgabe und Kenntnisnahme von Informationen, Integrität, die Sicherherstellung der Korrektheit von Informationen und der korrekten Funktionsweise von Systemen, und Verfügbarkeit, die Möglichkeit zu jedem vorgesehenen Zeitpunkt Daten, Informationen, Dienstleistungen, Netze und Komponenten nutzen zu können (BAköV 2016, 13). Je nach Anwendungszweck sind weitere Schutzziele sinnvoll oder juristisch notwendig: so z. B. die Authentizität als Gewährleistung, dass eine Person oder IT-Komponente oder eine Anwendung tatsächlich diejenige ist, die sie vorgibt zu sein (BAköV 2016, 13). Auch die Nichtabstreitbarkeit als Nachweisbarkeit des Versands oder Empfangs von Informationen, wie z. B. E-Mails, kann eines dieser Ziele darstellen. Durch Schwachstellen, d.h. Lücken in der Sicherheit von Systemen, können Systeme anfällig für allgemeine Bedrohungen werden und es kann zu konkreten Gefährdungen kommen (BAköV 2016, 14). Schwachstellen resultieren beispielsweise durch Produktmängel, fehlerhafte Implementierungen oder auch fehlerhafte Nutzung. Menschen, seien es Produktions- Softwareentwickler oder „nur“ Konsumenten, müssen stärker in den Mittelpunkt der Sensibilisierung für Informationssicherheit rücken (Dark 2006) (Workman 2007) (Singh, et al. 2013) (Styles 2013, 197-206) (Kim 2014) (Beyer, et al. 2016). Da die Bedrohungen sowohl technischer (z. B. Hacking) als auch zwischenmenschlicher (z. B. Social Engineering) Natur sein können, sind ein höheres Bewusstsein und verbesserte Kenntnisse der Menschen hinsichtlich der mit der Digitalisierung einhergehenden Gefahren

und entsprechenden Schutzmechanismen für das Privat-, Schul- und Arbeitsleben unerlässlich. Darüber hinaus kann die Aufklärung über Informationssicherheit nicht früh genug erfolgen.
Mit 97 Prozent besitzen nahezu alle 12- bis 19-Jährigen ein eigenes Smartphone (Feierabend, Rathgeb und Reutter 2018, 8). Dies geht aus der JIM-Studie hervor, mit der der Medienpädagogische Forschungsverbund Südwest (mpfs) seit 1998 den Medienalltag Jugendlicher in Deutschland untersucht (Feierabend, Rathgeb und Reutter 2018, 3). Social Media-Plattformen, wie WhatsApp, Instagram und Snapchat, gehören wie der Musikstreaming-Dienst Spotify oder das Videoportal YouTube zum Alltag der Jugendlichen (Feierabend, Rathgeb und Reutter 2018, 22,38,51). An einer entsprechenden Vermittlung von Kenntnissen zur Funktionsweise dieser Dienste und daraus resultierenden möglichen Gefährdungen und notwendigen Schutzmöglichkeiten fehlt es oft noch im (Schul-)Alltag. In der Studie „Digitale Schule – vernetztes Lernen“ der BITKOM aus dem Jahr 2015 stimmten 89 Prozent der befragten Schülerinnen und Schüler zwischen 14 und 19 Jahren sowie Lehrende der Aussage „Medienkompetenz sollte stärker im Unterricht vermittelt werden [...]“ zu (Bitkom Research GmbH 2015, 47). Die befragten Eltern der nachfolgenden Studie aus 2016 wünschten sich vor allem mehr Unterricht zu den Lerninhalten „Datenschutz im Internet“ (73 %), „Richtiges Verhalten in Chats und sozialen Netzwerken“ (65 %) und „Rechtliche Grundlagen im Internet“ (53 %) (Berg 2016, 12).

2 Zielsetzung von SecAware4school

Zentrales Ziel des Forschungsprojekts ist die Sensibilisierung von Schülerinnen und Schülern für das Thema Informationssicherheit im Schulalltag über erlebnisorientierte Awareness-Lernszenarien. Darüber hinaus sollen Freiwillige zu jugendlichen Sicherheitsberater/innen ausgebildet werden. Die jeweils älteren Schülerinnen und Schüler der 6., 9. und 11. Jahrgangsstufe sollen ihr Wissen adäquat an jüngere weitergeben und als Moderatorinnen und Moderatoren durch die entwickelten Lernszenarien leiten können. Parallel werden ihre Bezugspersonen, die Lehrerinnen und Lehrer, trainiert und die Eltern spezifisch informiert. Im Vordergrund der analogen und digitalen Lernszenarien stehen vor allem die Berücksichtigung konkreter Alltagssituationen, die Interessen der Zielgruppen und deren Emotionalisierung für Informationssicherheitsthemen. Die Lernszenarien basieren auf der Integration von drei Lernmethoden: Game-based, Accelerated und Authentic Learning.
Ein weiteres Ziel des Projektes ist die Einbeziehung ihrer Bezugspersonen, der Lehrenden und Eltern. Im Vordergrund stehen dabei vor allem die Berücksichtigung konkreter Alltagssituationen und die Interessen der Zielgruppen, um z. B. für einen sorgsamen Umgang

mit personenbezogenen Daten bei der Nutzung von Internet Services und sozialen Netzwerken zu sensibilisieren. Weitergehend soll den Schülerinnen und Schülern der beteiligten Klassen ermöglicht werden, sich zu jugendlichen Sicherheitsberaterinnen und -beratern im Rahmen eines Mentoren-/Coaching-Konzeptes ausbilden zu lassen. Diese Ausbildung befähigt sie zur Weitergabe ihres Wissens und ihrer Erfahrungen an Mitschülerinnen und Mitschüler der jeweils darunterliegenden Klassenstufen. Einen Teil ihrer Ausbildung stellt die Teilnahme an Vorbereitungsschulungen und die Prüfung nach dem Internationalen Computerführerschein (ICDL), im Modul „IT-Sicherheit“, dar. Darüber hinaus werden sie in den Kreativworkshops bestärkt, Anpassungs- und Verbesserungsvorschläge für bereits bestehende analoge und digitale erlebnisorientierte Lernszenarien vorzunehmen, die Probleme und Bedürfnisse in ihrem Alltag widerspiegeln. Die Moderation der entwickelnden Lernszenarien gegenüber den Eltern gehört ebenfalls zu den Aufgaben der jugendlichen Sicherheitsberaterinnen und -beratern.

Die Jugendlichen sollen als Nutzer von Internet Services und sozialen Netzwerken spielerisch an den sorgsamen Umgang mit sensiblen Daten herangeführt werden und in gleicher Weise ihre digitale Kompetenz und ihr technisches Verständnis weiterentwickeln. Sie sollen sich in der Lage sehen, sich selbstbestimmt und bewusst auch in der digitalisierten Welt zu bewegen. Zu den Fähigkeiten zählen zum Beispiel, selbstständig die potenziellen Gefahren im Netz zu erkennen, Risiken zu bewerten und präventiv Schutzmaßnahmen zu ergreifen. Dabei soll die Erfahrung nicht auf das Individuum begrenzt werden, sondern vielmehr zu einem in sich geschlossenen Kreislauf der Wissensvermittlung und -erhaltung der Schülerinnen und Schüler untereinander führen. Während jüngere Teilnehmende so von der Erfahrung älterer profitieren, festigen diese ihr Wissen durch die spätere selbstständige Moderation und Begleitung der Lernszenarien in ihrer Schule. Die Qualifikation der Schülerinnen und Schüler zu sogenannten jugendlichen Sicherheitsberaterinnen und -beratern bildet somit einen weiteren wichtigen Grundstein dieses Projekts.

Essenziell stellt sich hier auch der Einbezug des erwachsenen Umfelds der Jugendlichen dar, wie den Eltern und den Lehrenden. Im Rahmen des Projekts wurden die erlebnisorientierten Lernszenarien durch die Schülerinnen und Schüler vermittelt, während den Lehrenden eine beratende und unterstützende Aufgabe zuteilwurde, um die Nachhaltigkeit der Projektziele zu gewährleisten. Jeweils eine Lehrerin bzw. ein Lehrer pro beteiligter Pilotschule wurde zudem zur/ zum Informationssicherheitsbeauftragten ausgebildet.

Folgende Pilotschulen in Berlin und Brandenburg nahmen am Projekt teil:

- Humboldt-Gymnasium Berlin (HGB)
- Rudolf-Virchow-Oberschule Berlin (RVO)

- Friedrich-Schiller-Gymnasium Königs Wusterhausen (FSG)
- Friedrich-Wilhelm-Gymnasium Königs Wusterhausen (FWG)
- Staatliche Gesamtschule Königs Wusterhausen (GKW) (ehem. Dr. Hans Bredow Oberschule Königs Wusterhausen)

3 Methodische Grundlagen

3.1 Security Awareness

Wissenstransfer wird in deutschen Schulen für gewöhnlich über Vorträge, Präsentationen und Plakate vermittelt – Frontalunterricht ist hier das Stichwort. Die Sensibilisierung für Informationssicherheit, wenn diese an Schulen überhaupt stattfindet, beschränkt sich oft auf diese gängigen Formen des Wissenstransfers. Um die Inhalte der Informationssicherheit erlebbar und nachhaltig begreifbar zu vermitteln, wurden die bereits in vorangegangenen Projekten verwendeten Methoden des erlebnisorientierten Ansatzes gewählt.
Aus der psychologisch-basierten betrieblichen Awareness-Forschung ist bekannt, dass mögliche Sensibilisierungsmaßnahmen einerseits eine Emotionalisierung der Menschen bewirken und andererseits einen Erfahrungsaustausch ermöglichen sollten (Scholl, Fuhrmann und Pokoyski 2016) (Haucke 2018). Eine nachhaltige Bewusstseinsförderung bedarf somit einer emotionalen Einbindung der Zielgruppen in die Diskussionen um die Themen zur Informationssicherheit in konkreten Situationen. Die entwickelnden Maßnahmen sind als erlebnisorientierte Lernszenarien aus dem Alltag der Zielgruppen konzipiert und in analoger und digitaler Form entwickelt worden sowie mit unterschiedlichen Teams erprobt und mit Coaching- und Mentoren-Konzepte ergänzt.

3.2 Game-based Learning

Zur Realisierung der dargelegten Ziele wurden die Lernansätze Game-based und Accelerated Learning (AL) kombiniert. Neben der abwechslungsreichen und animierenden Form des Lernens (Linek und Albert 2009) ermöglicht GBL den Schülerinnen und Schülern den Blick auf ein gesetztes Ziel und ein direktes Feedback (Fang, Zhang und Chan 2013). Die drei unterschiedlich geplanten Anforderungsstufen der spielbasierten Lernszenarien fördern die Weiterentwicklung der Teilnehmenden, ohne ihnen zu viel abzuverlangen (Bressler und Bodzin 2013). Das AL hingegen fordert den Schüler/innen über die passive Wahrnehmung hinaus das aktive Erschaffen von Wissen ab (Bandura 1969) (Mataric 1994) (Rose & Nicholl 1998) (Boyd 2004). Der Ansatz verfolgt das Ziel, dass die Lernenden bestimmte Fähigkeiten selbstständig

und langfristig verinnerlichen. Unter den vielen Lernmethoden stellt sich das narrative Lernen für Kinder und Jugendliche als besonders effektiv heraus. Diese Methode ermöglicht es, die Sprachfähigkeiten weiterzuentwickeln und sich gleichzeitig mit dem Thema der Informationssicherheit auseinanderzusetzen.

Erlebnisorientierte, spiel- und teambasierte Lernszenarien als Sensibilisierungsmaßnahmen erlauben den Lernenden, Fehler zu begehen, zu experimentieren und den sicheren Umgang mit einem potenziellen Unsicherheitsfaktor zu erlernen (Trybus 2014). Die Teilnehmenden arbeiten auf ein Ziel hin, wählen und führen Aktionen aus und erleben unmittelbar die daraus resultierenden Konsequenzen. Der perspektivische Vorteil dieser Projektmaßnahmen mit jugendlichen Moderatorinnen und Moderatoren besteht vor allem darin, dass die Wissensvermittlung durch beinahe Gleichaltrige oftmals glaubwürdiger und authentischer empfunden wird als durch Erwachsene. Hiermit wird auf das Prinzip Peer-Involvement zurückgegriffen (Damon 1984) (Piaget 2003) (DuBois und Karcher 2013). Denn *Peer Group* ist ein längst etablierter Begriff und Gegenstand psychologischer und erziehungswissenschaftlicher Forschung. Diese Methode der Schulung von Gleichaltrigen hat sich bereits im früheren 19. Jahrhundert bewährt (Schmidt 2002, 127-140). Die Herangehensweise des gesamten Projekts bietet weitergehende Vorzüge, wie die Förderung der Kommunikations- und Kooperationsfähigkeit, die Verknüpfung mit realen Problemen aus dem Leben der Schülerinnen und Schüler und die Reduzierung der Komplexität von anspruchsvollen auf erlebbare Lerninhalte.

Narration bedeutet, etwas in der erzählenden Form darzustellen, z.B. das Erzählen einer Geschichte, und steht im direkten Zusammenhang mit dem Lese- und Schreibvermögen. Vergangene Ereignisse werden beim Erzählen narrativ rekonstruiert und sind mit Erinnerungen verbunden. Die dabei rekonstruierten Fakten werden durch die Wiedergabe neu interpretiert, selektiert und evaluiert (Busch 2013, 33). Erzählungen beruhen auf autobiografischen Erinnerungen, Erfahrungen und Erwartungen.

Nach Fingerhut ist die Narration eine Form des Lernens, die zur Erweiterung der sprachlichen Kompetenzen beiträgt. So entwickeln Kinder und Jugendliche geschlechtsspezifische Verhaltensmuster und nehmen in ihrer Fantasie künftige Ereignisse vorweg. Deshalb sind die Teilnehmerinnen und Teilnehmer der Lernstationen beim narrativen Lernen Zuhörer und gleichzeitig affektiv Beteiligte, wodurch das Erzählte nahezu ikonisch abgespeichert wird (Fingerhut o.J.). Es ist festzuhalten, dass die aktive Vorstellungskraft ein wichtiger Bestandteil der Narrative ist. Narration wird als Sprache entwickelnde und sprachgestützte Lernweise

verstanden. Die erzählten Sachverhalte werden als Ereignisse, die man erleben kann, modelliert und somit zum ereignishaften Lernen geformt.
Die Kombination der Methoden findet in Form von erlebnisorientierten Lernszenarien im Schulalltag durch emotionalisierende, motivierende analoge und digitale Spiele im Projekt SecAware4school Anwendung.

4 Meilensteine des Projektes

Das Ziel der Sensibilisierungsmaßnahme – Stärkung des Bewusstseins für Informationssicherheit und entsprechender Kenntnisse – wurde durch vier große Schritte und parallel laufende Tätigkeiten erreicht. Einen Überblick dazu bietet Abbildung 1. Neben einer Online-Umfrage, Informationsveranstaltungen, Awareness Trainings (AT), Kreativworkshops (KW) und der Ausbildung der Lehrerinnen und Lehrer zu Informationssicherheitsberater/innen wurden parallel die Lernszenarien entwickelt, erprobt und finalisiert.

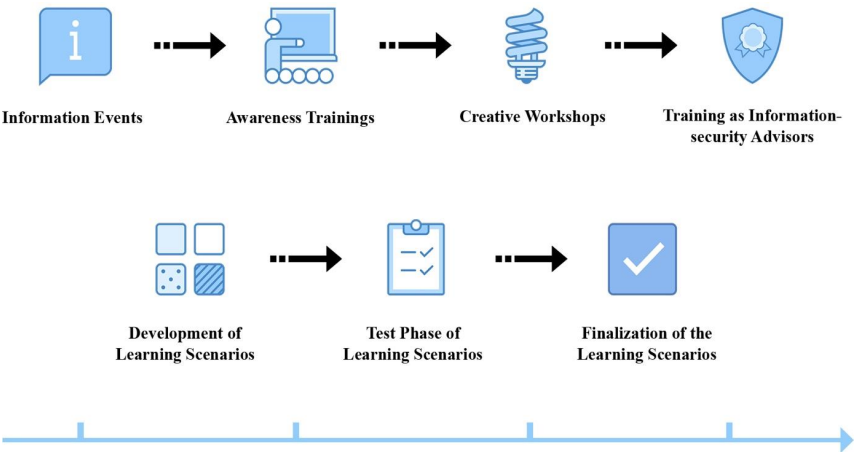


Abbildung 1: Projektmeilensteine in SecAware4school

Der Entwicklung unterschiedlicher, auf die Zielgruppen abgestimmter Maßnahmen liegt die Erforschung des Ist-Zustandes zugrunde. Eine Online-Umfrage im September 2018 diente als Basis für die Themenfindung und den zu entwickelnden Lernszenarien. Darauf aufbauend wurden den Schülerinnen und Schülern bei Informationsveranstaltungen nicht nur das Projekt vorgestellt, sondern auch deren spezifische Bedürfnisse und Fragen mittels Beobachtung und aktivem Austausch analysiert. Die gewonnenen Erkenntnisse flossen in die Entwicklung acht

neuer und Modifizierung vier vorhandener spielbasierter Lernszenarien aus vorangegangenen Projekten ein. Dies erfolgte unter Berücksichtigung konkreter Alltagssituationen der Jugendlichen, ihrer Sprache und ihres Alters. An den Schulen erfolgten im nächsten Schritt die Awareness Trainings, die aus bis zu zehn verschiedenen spielbasierten Lernszenarien bestanden, welche die Grundlagen der Informationssicherheit vermittelten. Um die Eltern rechtzeitig über das Forschungsprojekt zu informieren, wurde im Vorfeld der ersten Informationsveranstaltungen und der ersten Sensibilisierungsmaßnahmen ein Informationsblatt ausgeteilt, welches im Anhang zu finden ist.

4.1 Umfrage zur Themenfindung

Das Interesse an den geplanten erlebnisorientierten Lernszenarien in den Schulen zu wecken, war bereits ein Ziel der vorbereitenden Informationsveranstaltungen in den Klassen. Die vielen Fragen zum Projekt und zum Vorhaben offenbarten deutlich das Interesse der Schülerinnen und Schüler. Eine Umfrage in den Schulen gab zusätzlich Aufschluss darüber, für welche Themen sich die Teilnehmenden interessieren. Die Themen wurden in erlebnisorientierten Lernszenarien umgesetzt, die in drei Schwierigkeitsniveaus entwickelt und in Klassen der 6., 9. und 11. Jahrgangsstufe der teilnehmenden Pilotschulen erprobt wurden. Die Umfrage bestand aus insgesamt neun Fragen.

Die ersten Fragen dienten zur Erfassung der demografischen Angaben. Die Beteiligung an den Schulen fiel sehr unterschiedlich aus: Die höchste Anzahl verzeichnet das HGB mit 396 Teilnehmenden. Gefolgt wird es vom FWG mit 232, der RVO mit 107 und dem FSG mit 28 online befragten Personen. Abbildung 2 zeigt die prozentuale Teilnahme jeder Schule gegenüber der Gesamtmenge an erfolgreich Befragten.

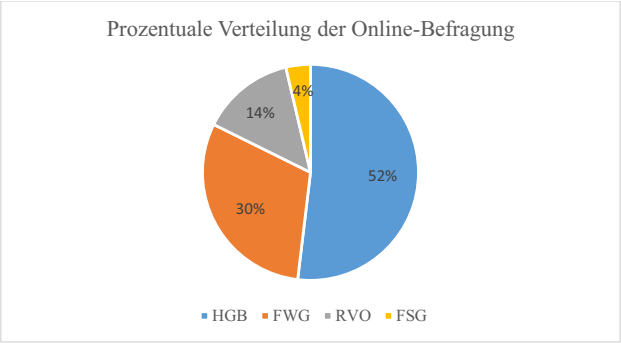


Abbildung 2: Beteiligung an der Online-Befragung

Aufgrund der zeitlich verkürzten Möglichkeit zur Teilnahme liegt die GKW (ehem. HBO) mit 0,65 Prozent (5 Personen) an letzter Stelle der teilnehmenden Pilotschulen. Daher wurde sie bei Vergleichsauswertungen aus Datenschutzgründen, aufgrund der niedrigen Teilnehmerzahl, nicht berücksichtigt. Nach eigener Angabe nahmen insgesamt 481 Schüler/innen (62,5 %), 84 Lehrende (11 %) und 204 Eltern (26,5 %) teil.

Die einleitende Frage nach den Merkmalen eines sicheren Passwortes und der als sicher geltenden Anzahl der Zeichen wurde wie folgt beantwortet (s. Abbildung 3): Eine deutliche Mehrheit von 606 Personen, 84 Prozent von 723 Teilnehmern/innen dieser Frage, hat die richtige Antwort gewählt. Nur 20 Personen (3 %) entschieden sich für fünf Zeichen. Mit acht Zeichen gilt ein Kennwort als noch relativ sicher – von Experten werden allerdings mehr und unterschiedlich kombinierte Zeichen empfohlen. Das Ergebnis der Teilnehmenden ließe vorerst die Schlussfolgerung zu, dass die meisten über Kenn- und Passwörter gut informiert sind. Im weiteren Austausch während der Informationsveranstaltungen und Awareness Trainings wurde dem SecAware4school-Team allerdings deutlich, dass (geschätzt) weniger als die Hälfte der Befragten tatsächlich ein Passwort mit acht oder mehr Zeichen benutzt. Allein dieses Ergebnis verdeutlicht einen Sensibilisierungsbedarf, denn es gibt offenbar eine Diskrepanz zwischen Wissen und Verhalten. Dies entspricht durchaus den Erkenntnissen aus der betrieblichen Awareness-Forschung (Scholl, Fuhrmann und Pokoyski 2016) (Haucke 2018).

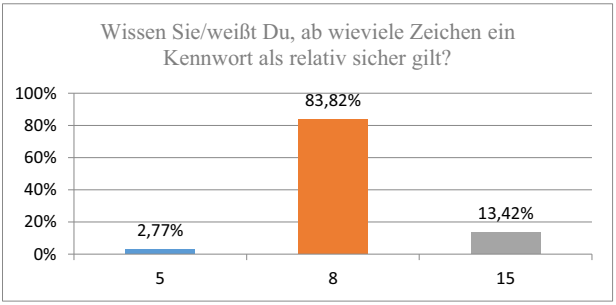


Abbildung 3: Frage nach der Passwortlänge

Frage 5: Wissen Sie/weißt Du, wie man die eigene Privatsphäre im Internet schützen kann?

Bei der fünften Frage waren drei Antwortmöglichkeiten vorgegeben: *Ja/Nein/Teilweise*. In Abbildung 4 sind ihre Häufigkeiten aufgeführt. 390 von 722 an dieser Frage teilnehmende Personen haben angegeben, dass sie nur teilweise wissen, wie die eigene Privatsphäre im Internet geschützt werden kann. Dies entspricht mit 54 Prozent der Mehrheit aller Befragten.

281 Personen (39 %) haben diese Frage bejaht und 51 Personen (7 %) verneint. Die Ergebnisse der einzelnen Pilotschulen wurden zusätzlich miteinander verglichen. Dabei ist interessant, dass beim FWG 79 Prozent der Teilnehmenden als Antwort *Teilweise* und nur 10 Prozent *Ja* auswählten. Dieses Ergebnis unterscheidet sich deutlich von den anderen Pilotschulen, bei denen 37 bis 46 Prozent der Befragten *Ja* angaben. Es wurde angestrebt, die Belastbarkeit dieser Umfragedaten im Projektverlauf zu verfolgen.

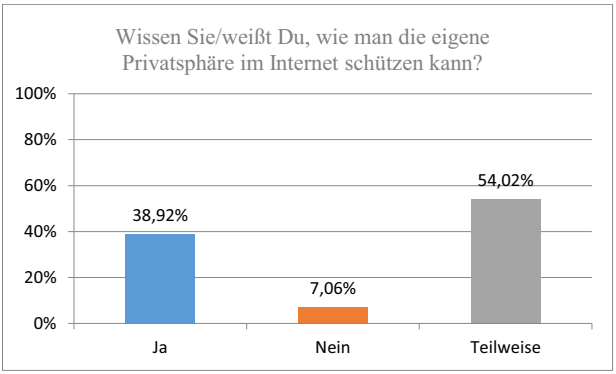


Abbildung 4: Frage nach dem Schutz der Privatsphäre

In Abbildung 5 ist die Frage über den Schutz der Privatsphäre im Vergleich zu den einzelnen Pilotschulen dargestellt. Eine Abweichung von den anderen Schulen ist beim Friedrich-Wilhelm-Gymnasium zu beobachten: 79 Prozent der Befragten gaben an, sich teilweise mit dem Schutz der eigenen Privatsphäre im Internet auszukennen. Die Teilnehmenden der anderen Schulen wählten die Antwortmöglichkeit wesentlich seltener aus.

Eine weitere Auffälligkeit zeigt sich bei der Häufigkeit der Antwortmöglichkeit *Ja* in der Befragung des Friedrich-Wilhelm-Gymnasiums: Nur 10 Prozent schätzten ihre Kenntnisse als genügend in diesem Bereich ein. Die Differenz zum Humboldt-Gymnasium, das Platz drei bei dieser Antwortmöglichkeit erreicht, beträgt mehr als 26 Prozent.

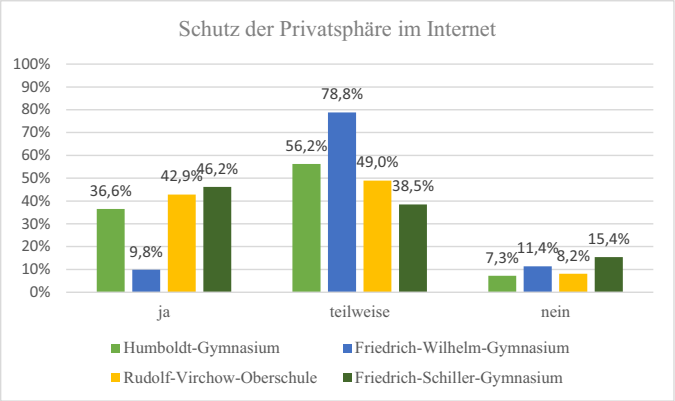


Abbildung 5: Schutz der Privatsphäre im Vergleich der Schulen

Frage 6: Wie oft nutzen Sie/nutzt Du Bilder aus dem Internet, z.B. für Referate?

Die sechste Frage wurde in der Online-Umfrage aufgenommen, um der Vermutung, dass sorglos mit Bildern aus dem Internet umgegangen wird, nachzugehen und daraus ggf. ein mögliches Thema für eines der Lernszenarien zu entwickeln. Drei Antwortmöglichkeiten waren hier vorgegeben: *Nie/Selten/Oft*. 410 der Befragten gaben an, dass sie oft Bilder aus dem Internet nutzen, dies entspricht knapp 57 Prozent. 264 Personen (37 %) nutzen selten Bilder aus dem Internet und nur 7 Prozent (48 Personen) gaben an, dass sie nie Bilder für den eigenen Gebrauch aus dem Internet nutzen (s. Abbildung 6). Die Abweichungen bei der Beantwortung der Frage der einzelnen Pilotschulen fallen im direkten Vergleich geringfügig aus: Bei allen nutzen 54 bis 65 Prozent oft Bilder aus dem Internet. Dieses Ergebnis zeigt die Relevanz des Themas *Bildnutzungsrechte* für den Aufbau eines Lernszenarios im Forschungsprojekt. Darüber hinaus kann dieses Thema leicht mit der Bedeutung eines sicheren Verhaltens in sozialen Netzwerken verknüpft werden. 67 Prozent aller Befragten gaben an, sich mittel oder sehr für Alternativen zu bekannten sozialen Netzwerken zu interessieren (s. Abbildung 8).

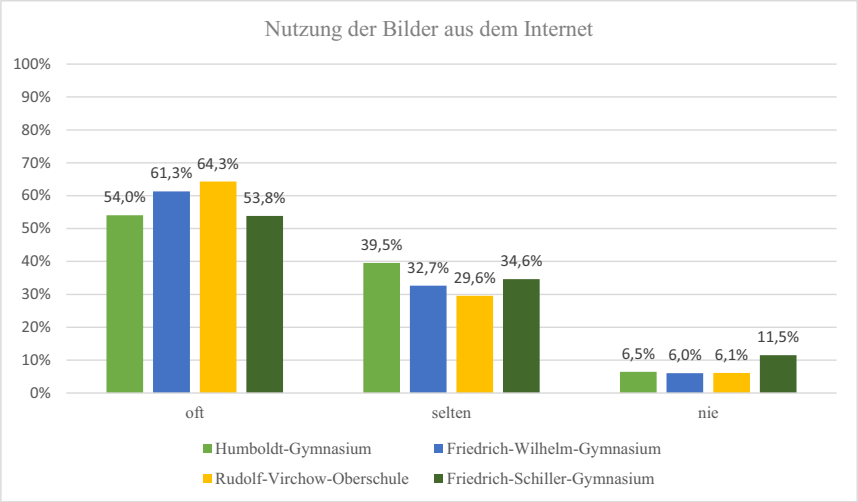


Abbildung 6: Nutzung der Bilder aus dem Internet im Vergleich der Schulen

Frage 7: Wurden Sie/ wurdest Du schon mal Opfer von Datendiebstahl (z.B.: Anmeldedaten wurden gestohlen)?

Die siebte Frage wurde von 723 Personen beantwortet. Abbildung 7 ist zu entnehmen, dass davon durchschnittlich 72 Prozent diese Frage mit *Nein* beantwortet haben, dies entspricht 520 der befragten Personen. 17 Prozent (125 Personen) gaben an, sich nicht sicher zu sein. Lediglich 11 Prozent der Befragten (78 Personen) bejahten die Frage. Vergleichend liegen alle Pilotschulen zwischen 58 und 74 Prozent mit der Einschätzung, bislang kein Opfer von Datendiebstahl gewesen zu sein. Es bleibt im Projektverlauf abzuwarten, ob und wie sich diese persönlichen Einschätzungen ändern. An dieser Stelle scheint es sinnvoll, auch Awareness-Messungen im Forschungsprojekt einzuplanen, die allerdings eine sehr komplexe Angelegenheit darstellen und bislang selten durchgeführt wurden (Scholl, K. und Fuhrmann 2017).

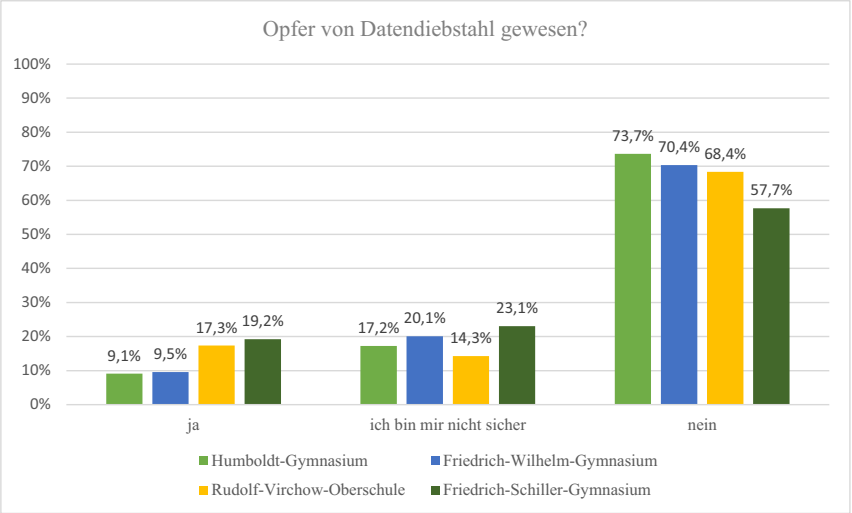
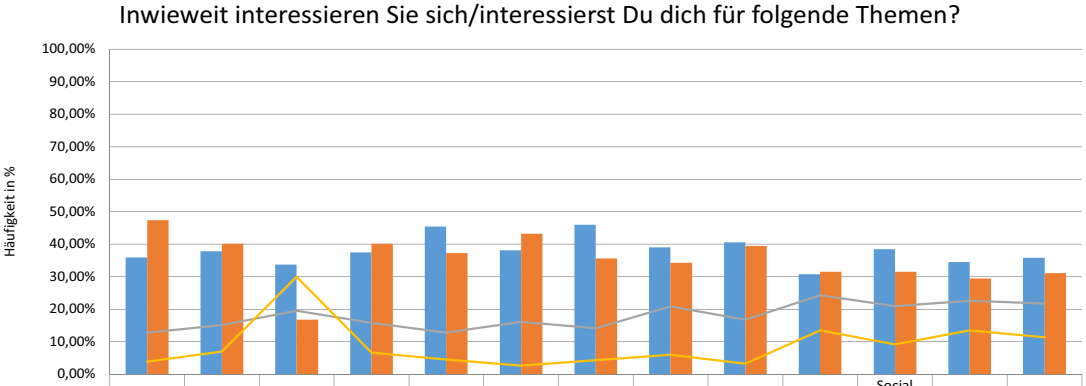


Abbildung 7: Opfer von Datendiebstahl im Vergleich der Schulen

Frage 8: Inwieweit interessieren Sie sich/ interessierst Du dich für folgende Themen?

Bei der achten Frage wurden 13 Themen der Informationssicherheit (s. Abbildung 8) vorgegeben mit den vier Antwortmöglichkeiten: *Sehr/Mittel/Wenig/Gar nicht*. Sie wurde von 722 Personen beantwortet. Das größte Interesse der online Befragten gilt dem Thema Sichere Passwörter und führt daher auf die Einstiegsfrage und deren widersprüchliche Beantwortung zurück: 331 Personen (46 %) haben bei der achten Frage die Antwortmöglichkeit *Sehr* gewählt. In den später durchgeführten Informationsveranstaltungen vor Ort wurde die Verwendung von Passwortmanagern meist verneint und korreliert sicherlich mit der geringen Anzahl von Passwörtern, die von Schüler/innen nach eigenen Angaben verwendet werden. Allerdings bleibt noch ungeklärt, ob tatsächlich für alle Dienste unterschiedliche Passwörter genutzt werden. Zudem wäre die Beantwortung einer weiteren Frage darüber interessant, mit welcher Regelmäßigkeit die Passwörter zurückgesetzt werden − eine wichtige Ergänzung zur Untersuchung des Benutzerverhaltens.



	Informationssicherheit (Schutz persönlicher Daten und Informationen)	Fake-News (Das Erkennen von vertrauenswürdigen Quellen)	Videospiele	Sicheres Verhalten in sozialen Netzwerken	Sichere Bedienung des Smartphones	Apps (Allgemein)	Sichere Passwörter	Verschlüsselung (Methoden, um Informationen geheim zu halten)	Schutzmaßnahmen gegenüber Gefahren im Internet	Phishing (Alles rund um E-Mail-Betrug)	Social Engineering (Manipulation von Menschen, um an vertrauliche Informationen zu kommen)	Cyber-Mobbing	Alternativen zu bekannten sozialen Netzwerken (z.B. Whats App, Google, etc.)
Sehr	35,92%	37,86%	33,70%	37,45%	45,42%	38,09%	45,97%	38,97%	40,56%	30,79%	38,42%	34,54%	35,83%
Mittel	47,43%	40,08%	16,78%	40,08%	37,22%	43,21%	35,56%	34,26%	39,44%	31,48%	31,48%	29,40%	31,11%
Wenig	12,76%	15,12%	19,56%	15,81%	12,78%	16,07%	14,17%	20,80%	16,81%	24,27%	20,94%	22,61%	21,67%
Gar nicht	3,88%	6,93%	29,96%	6,66%	4,58%	2,63%	4,31%	5,96%	3,19%	13,45%	9,15%	13,45%	11,39%

Abbildung 8: Interesse an Themen der Informationssicherheit

Nur knapp hinter *Sichere Passwörter* steht an zweiter Stelle das Interesse am Thema *Sichere Bedienung des Smartphones*: 327 Personen (45 %) gaben an, sich für das Thema sehr zu interessieren. An dritter Stelle liegt das Thema *Schutzmaßnahmen gegenüber Gefahren im Internet*: 292 Personen (41 %) interessieren sich sehr dafür. Darüber hinaus gaben 281 der Befragten (39 %) ein verstärktes Interesse am Thema *Verschlüsselung* an. Diese Ergebnisse entsprechen durchaus den bisherigen Erfahrungen des Forschungsteams. Zum einen entsprechen diese Themen Problemfeldern im Bereich Informationssicherheit, die von Angreifern seit Jahrzehnten (aus-)genutzt werden und für die sich Anwender/innen sehr konkrete benutzerfreundliche Lösungen im praktischen Gebrauch von Technologien wünschen. Andererseits verdeutlichen diese Ergebnisse, dass über komplexere Themen wie *Verschlüsselung* bislang nur ungenügend Aufklärung betrieben worden ist.

Frage 9: Für welche Themen interessieren Sie sich/ interessierst Du dich noch?
Bei der letzten Frage wurde online ein freies Feld zur Eingabe eingerichtet, um weitere Interessen der Teilnehmenden aufzunehmen. Die Auswertung dieser Frage hat sich als komplex herausgestellt. Sie wurde manuell analysiert, um die Kernthemen herauszufiltern. Hier sind die Favoriten der online befragten Pilotschulen nach Relevanz/Popularität geordnet:

- Informationssicherheit allgemein
- Soziale Netzwerke
- Privatsphäre
- Verschlüsselung
- Fake News
- Schadsoftware
- Programmieren & Hacken

Der letzte Aspekt verdeutlicht den Anreiz, sich in die Denkweise von Angreifern hineinversetzen zu wollen. Dies ist auch in der betrieblichen Awareness-Forschung ein wichtiger Aspekt von Sensibilisierungsmaßnahmen (Haucke 2018). Es bedeutet jedoch nicht, dass die Lernszenarien Anleitungen für Straftaten geben sollen. Vielmehr sollen sie in klarer und verständlicher Kommunikation aufklären über Motivation und Vorgehensweisen der Angreifenden als Täter, damit sich die Opfer qualifiziert sensibilisieren können. Zugleich wird so eine Befähigung aller Lernenden zur Risikoabschätzung der Bedrohungen und Gefährdungen im konkreten Kontext erreicht.

Die Auswertung zum Interesse am Thema *Fake News* (s. Abbildung 9) fiel für alle Befragten der Pilotschulen ähnlich aus: *sehr* bis *mittel interessant.* Auch in der betrieblichen Awareness-Forschung ist dieses Phänomen der Online-Welt inzwischen ein Dauerbrenner, dessen Bedeutung für die Wirtschaft und das eigene Arbeitsumfeld jedoch überwiegend noch erheblich unterschätzt wird (Matas und Pokoyski 2018, 19). Eine aktuelle Studie mit qualitativer Feldforschung dazu zeigt, dass Desinformation keine Folge einer digitalen Überlastung ist, weshalb die bloße Überprüfung der Quelle einer Information unzureichend ist (Take Aware Events (Hrsg.) 2018) (Matas und Pokoyski 2018, 21). Vielmehr muss das Prinzip der Falschmeldung im Kontext der Institution und Situation verstanden und die eigenen Mechanismen im Umgang mit Informationen erkannt werden. Eine Sensibilisierungsmaßnahme, die das berücksichtigt, „geht über ein bloßes Erkennen von richtig und falsch hinaus − sie verlangt vielmehr eine Selbstreflexion und digitale Achtsamkeit." (Matas und Pokoyski 2018, 21).

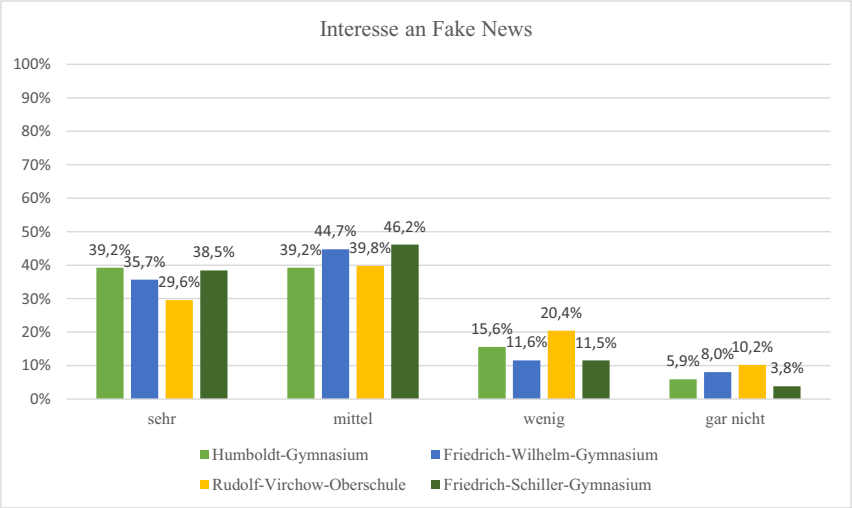


Abbildung 9: Interesse an Fake News im Vergleich der Schulen

Bemerkenswert zeigte sich bei der Schulbefragung zudem, dass das Thema *Videospiele* bei den Befragten nur mit 4 Prozent Unterschied zwischen insgesamt *sehr* (34 %) und *gar nicht* (30 %) bewertet wurde. Die Beantwortung dieser Frage ist zudem schulspezifisch (s. Abbildung 10): Die RVO zeigt mit 52 Prozent der Befragten großes Interesse an Videospielen, gefolgt vom HGB mit 36 Prozent. Das FWG sticht damit heraus, dass sich dort 41 Prozent für das Thema

Videospiele gar nicht interessieren. Das Thema *Videospiele sicher nutzen* ist einerseits ein bislang wenig erforschter Bereich und andererseits gekennzeichnet durch eine sehr spezifische Sprache und Kurzformen, die eigentlich nur aktive Videospieler/innen kennen, sodass die Entwicklung einer spielbasierten Sensibilisierung für alle (ob Spieler/in oder nicht) mit Reduzierung der Komplexität durchaus eine erhebliche Herausforderung darstellt.

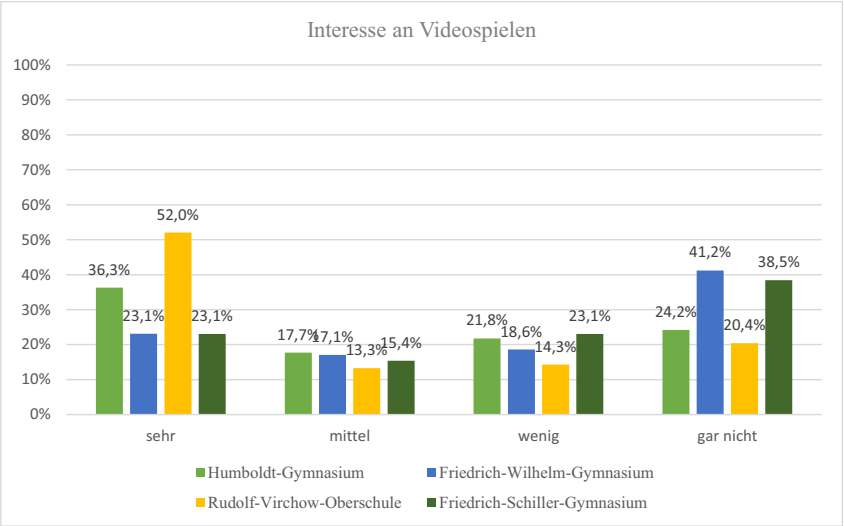


Abbildung 10: Interesse an Videospielen im Vergleich der Schulen

Das Thema *Sichere Smartphone-Bedienung* fällt an allen Pilotschulen ähnlich stark zwischen *sehr* und *mittel* aus, wobei sich die RVO mit 48 Prozent am meisten für das Thema interessiert. Da das Smartphone für Jugendliche zum Alltag gehört, ist es nicht ungewöhnlich, dass über 40 Prozent der Befragten sich für die sichere Bedienung des Smartphones interessieren. Dieses Thema kann darüber hinaus gerade in Blick auf die dritte Schwierigkeitsstufe der zu entwickelnden Lernszenarien recht gut mit den Themen *Verschlüsselung* und *digitale Zertifikate* mobiler Endgeräte gekoppelt werden.

Die Ergebnisse der anonymen Online-Befragung in den Pilotschulen fließen weiterhin in die Entwicklung der ersten Prototypen von analogen und digitalen erlebnisorientierten Lernszenarien im Forschungsprojekt SecAware4school ein. Darüber hinaus können die in den beiden Vorgängerprojekten (Security und SecAware4job) für andere Zielgruppen bereits existierenden Szenarien und Simulationen spezifisch angepasst und zur Erprobung genutzt

werden. Außerdem wird mit dem in SecAware4school Anfang April 2019 stattfindenden Kreativworkshop gemeinsam mit Schüler/innen und Lehrer/innen auch eine Prioritätenliste zur Entwicklung der Lernszenarien in drei Schwierigkeitsniveaus definiert.

4.2 Informationsveranstaltungen

Informationsveranstaltungen fanden in der Zeit zwischen Oktober 2018 und Januar 2020 statt. Für die Vorbereitung der geplanten Sicherheitstrainings, die auch für den Test der neu zu entwickelnden Lernszenarien genutzt werden sollten, wurden in allen Partnerschulen Informationsveranstaltungen durchgeführt. Sie sollten bei sowohl Lehrerinnen und Lehrern als auch Schülerinnen und Schülern Interesse wecken und die geplanten Maßnahmen vorstellen. Als Ausgangspunkt zur inhaltlichen Einführung in die Problematik *Informationssicherheit und Datenschutz* wurden oftmals der Streit um die Bildrechte am „Selfie des Affen Naruto“ (Hertreiter 2018) (Sokolov 2018) und die Methode *Storytelling* genutzt. Im Durchschnitt war einem Schüler oder einer Schülerin die Geschichte in jeder Klasse bekannt. Interessant sind die unterschiedlichen Auslegungen und Darstellungen der Sachverhalte im Vergleich zum Wikipedia-Artikel (Wikimedia Foundation Inc.) gewesen. Durch das Erzählen einer Geschichte soll das Wissen besser verinnerlicht werden – sowohl bei den Erzählenden als auch bei den Zuhörenden (Busch 2013, 33) (Fingerhut o.J.). In der anschließenden Diskussion kamen häufig weitere Fragen auf, die andeuteten, dass fallbasierte Themen ein Schlüssel für die Sensibilisierung und die anschließende weitergehende Wissensvermittlung auch an Schulen sein könnten. Das Projekt wurde positiv und mit großem Interesse sowohl von Schülerinnen und Schülern als auch von Lehrenden aufgenommen. Das Problem der Digitalisierung an deutschen Schulen und der zunehmenden Erreichbarkeit jeder Person durch den ständigen Begleiter, dem Smartphone, hat bei Beteiligten Hoffnung geweckt, mit der Teilnahme besser aufgeklärt und sensibilisiert zu sein für den komplexen Bereich der Informationssicherheit. Die beteiligten Schulen nahmen das Angebot des Projektes positiv auf und waren erfreut über andere Lehr- und Lerninhalte, die Abwechslung in den Schulalltag brachten.

Der Abbildung 11 ist ein erstes Brainstorming zu entnehmen, welches in den Informationsveranstaltungen besprochen wurde. Den meisten Beteiligten der jüngeren Klassenstufen waren die meisten Begriffe unbekannt. Den mittleren und älteren Klassenstufen (8.-11.) waren deutlich mehr Begriffe vom Hörverständnis bekannt, aber nicht inhaltlich nachvollziehbar.

Abbildung 11: Postkarte, die bei Informationsveranstaltungen eingesetzt wurde

Eine erste Auswertung der Vorabbefragung aller Schülerinnen und Schüler konnte ebenfalls präsentiert werden. Hier hat die Frage nach der optimalen Passwortlänge die Defizite hinsichtlich Kenntnisse der Informationssicherheit offengelegt. Grundsätzlich haben alle Schülerinnen und Schüler die Ankündigung der etwas anderen Form eines Sicherheitstrainings begrüßt. Nach den Informationsveranstaltungen wurden Termine für die anschließenden Awareness Trainings mit den Schulen vereinbart.

4.3 Awareness Trainings

Die Awareness Trainings bildeten die Grundlage für die (Weiter-)Entwicklung und Tests der spielbasierten Lernszenarien. In allen Fällen wurde ein Zirkeltraining organisiert, um möglichst unterschiedliche, für den Schulalltag relevante Themen der Informationssicherheit abzudecken. Geplant waren die Awareness Trainings für je 2 Klassen der Klassenstufen 6/7, 8/9 und 10/11. Bei einer erwarteten Klassenstärke von 20 Schülerinnen und Schülern ergibt dies bei fünf teilnehmenden Schulen insgesamt 600 geplante Teilnehmende. Tabelle 1 gibt einen Überblick über die tatsächliche Verteilung. Insgesamt nahmen 21 Klassen an den Awareness Trainings

teil. Die Klassenstärke bzw. -frequenz wich von der ursprünglichen angenommenen Anzahl ab und unterschied sich nach Bundesland und Schultyp. Durchschnittlich betrug die Klassenstärke im Schuljahr 2017/2018 an Berliner Gymnasien 27,6 und den Sekundarstufen 22,7 (Amt für Statistik Berlin-Brandenburg 2019A). In Brandenburg betrug die Klassenstärke im Schuljahr 2018/2019 an Gymnasien 25,5 und an Gesamt- und Oberschulen 22,9 (Amt für Statistik Berlin-Brandenburg 2019). Diese Werte entsprechen in etwa auch den Erfahrungen der Forschungsgruppe in den Schulen, sodass die Werte für die Berechnung der Gesamtteilnehmerzahl herangezogen werden. Durch die Corona-Krise erhielten zwar weniger Klassen ein Awareness Training, dennoch konnten insgesamt etwa 521 Schülerinnen und Schüler daran teilnehmen.

Tabelle 1: Awareness Training - Verteilung der Klassen nach Schulen und Klassenstufen

		Ø Klassen-stärke nach Schultyp	Teilnehmende Klassen			geschätzte Gesamtzahl Schülerinnen und Schüler
			Klassenstufe 7/6	Klassenstufe 8/9	Klassenstufe 10/11	
Projektschulen	HG	27,6	2	2	2	166
	RVO	22,7	2	2	2	136
	FSG	25,5	1	2	0	76
	FWG	25,5	0	1	1	51
	GKW	22,9	4	0	0	92
	Sum.					521

Nach Möglichkeit wurde ein Awareness Training mit einer Klasse durchgeführt, was in der Regel eine Teilnahme von 20 bis 32 Schülerinnen und Schülern pro Durchgang bedeutete. Dies hatte zum einen organisatorische Gründe, wie die zur Verfügung stehenden Räume oder die Personalkapazitäten seitens der Forschungsgruppe. Zum anderen sollte eine übersichtliche Teilnehmeranzahl die Bildung kleinerer Teams erlauben, da diese bessere Teamarbeit zeigen, auch wenn Forschungsergebnisse keine absolute optimale Teamgröße in Bezug auf eine bestimmte Anzahl liefern (Hoegl 2005). Jeder Teilnehmende sollte die Möglichkeit erhalten,

sich aktiv in die spielbasierten Lernszenarien einzubringen. In der Abbildung 12 ist ein typischer Ablaufplan der Awareness Trainings zu sehen.

Maximilian

Durchlauf 1

Lernszenario		Team	Zeit	Punkte
1	Passworthacking	A	08:10-08:30	
2	Phishing	D	08:30-08:50	
3	Phishing	C	08:50-09:10	
4	Passworthacking	D	09:25-09:45	
5	Passworthacking	C	09:45-10:05	
6	Passworthacking	B	10:05-10:25	

Durchlauf 2

Lernszenario		Team	Zeit	Punkte
1	Bildrechte	B	10:55-11:15	
2	Bildrechte	A	11:15-11:35	
3	Phishing	C	11:35-11:55	
4	Passworthacking	D	12:40-13:00	
5	Bildrechte	D	13:00-13:20	
6	Bildrechte	C	13:20-13:40	

Steffi

Durchlauf 1

Lernszenario		Team	Zeit
1	Bildrechte	B	08:10-08:30
2	Bildrechte	A	08:30-08:50
3	Klassenfahrt	D	08:50-09:10
4	Klassenfahrt	C	09:25-09:45
5	Bildrechte	D	09:45-10:05
6	Bildrechte	C	10:05-10:25

Durchlauf 2

Lernszenario		Team	Zeit
1	Passworthacking	A	10:55-11:15
2	Phishing	D	11:15-11:35
3	Klassenfahrt	D	11:35-11:55
4	Klassenfahrt	C	12:40-13:00
5	Passworthacking	C	13:00-13:20
6	Passworthacking	B	13:20-13:40

Abbildung 12: Beispielhafter Ablaufplan der Awareness Trainings in den Schulen

Die Tabelle 2 zeigt eine Übersicht über die Awareness Trainings. Zu Beginn eines Awareness Trainings wurde der Ablauf erläutert und die jeweilige Klasse nach einer kurzen Begrüßung in durchschnittlich 4 Teams á 6 bis 10 Personen aufgeteilt. Anschließend wurden Laufzettel verteilt, sodass jedes Team wusste, welche Station die Nächste ist und wie viele Punkte an der jeweiligen Station erworben wurden. Für die gesamte Phase wurden maximal 10 Minuten eingeplant. Für ein Lernszenario wurden durchschnittlich 20 Minuten veranschlagt, 5 Minuten für eine kurze Einführung mittels Moderationsfragen, 10 Minuten für die eigentliche Durchführung und 5 Minuten für die Auswertung. Das Forschungsteam hat festgestellt, dass 25 bis 30 Minuten optimal wären. Zum einen würde der Stationswechsel dadurch deutlich ruhiger ablaufen und zum anderen hätten die Schülerinnen und Schüler etwas mehr Zeit für Fragen und Diskussionen. Je nach verfügbarer Zeit wurden 3 bis 6 spielbasierte Lernszenarien durchgeführt. Durchschnittlich standen 114 Minuten pro Klasse zur Verfügung. Am Ende eines Awareness Trainings wurden die Teamergebnisse ausgewertet, die entstandenen Geschichten beim *Storytelling* vorgetragen, Feedback eingeholt und die Klasse durch die Moderierenden verabschiedet, wofür etwa 10 Minuten einkalkuliert wurden.

Tabelle 2: Awareness Trainings - Übersicht

Datum	Schule	Anzahl Klassen	Stufe	Anzahl DG	Teams/ DG	Anzahl LS	MA TH Wildau	Zeit gesamt	Zeit/ LS
24.01.19	FSG	2	9	2	4	4	4	60 min	13 min
28.01.19	FSG	1	6	1	3	3	3	90 min	23 min
22.03.19	HG	2	8, 6	2	4	6	4	135 min 120 min	20 min 17 min
25.03.19	HG	2	8, 10	2	4	6	4	135 min 120 min	20 min 17 min
01.04.19	RVO	2	7	1	4	4	4	90 min	18 min
02.04.19	HG	1	6	1	4	6	4	120 min	17 min
03.04.19	RVO	4	2x9, 2x11	2	6	2x3	5	90 min	23 min
10.04.19	FWG	2	8, 10	2	4	4	4	90 min	17 min
12.04.19	HG	1	10	1	4	4	3	120 min	25 min
24.10.19	GKW	2	7	2	3	3	3	140 min 130 min	20 min 25 min
07.11.19	GKW	2	7	2	3	3	3	140 min 130 min	20 min 25 min
Gesamt	5	21		**Ø**	4	4	4	114 min	20 min

Für die Awareness Trainings wurden bereits im Projekt „Gendersensible Studien- und Berufsorientierung für den Beruf Security Spezialistin (Security)“ entwickelte Lernszenarien wie *Klassenfahrt – Sicher unterwegs*, *Password Hacking* und *Bildrechte* genutzt. Im Laufe der Zeit kamen die im Projekt SecAware4school entwickelten, spielbasierten Lernszenarien *Informationssicherheit: Schnelles Begrifferaten*, *Storytelling in der Informationssicherheit* und *Bildrechte (digital)* zum Einsatz. Das Feedback der Schülerinnen und Schüler sowie der Lehrenden floss in die Weiterentwicklung der Lernszenarien ein, sodass deren Endfassungen durch eine Integration in den normalen Unterricht eingesetzt oder als Workshop-Konzept realisiert werden können.

An vier der am Projekt teilnehmenden Schulen fanden die Awareness Trainings im Januar, März und April 2019 statt. Aufgrund einer anstehenden Fusion war es für die ehemalige Hans-Bredow-Oberschule, jetzt Staatliche Gesamtschule Königs Wusterhausen, organisatorisch nicht möglich, in diesem Zeitraum teilzunehmen. Im Rahmen einer Bachelorarbeit wurden nachträglich Awareness Maßnahmen in vier 7. Klassen an zwei Terminen im Oktober und November durchgeführt. Diesen Trainings ging eine auf 15 Minuten gekürzte Informationsveranstaltung voraus, da die Zeit für das Projekt aufgrund der internen und komplexen Umstrukturierung der Schule sehr begrenzt war. Vor und nach dem eigentlichen Awareness Training nahmen die Schülerinnen und Schüler an einer Online-Umfrage teil. Diese enthielt eine Selbsteinschätzung bezüglich des Wissens, Verhaltens und der Einstellung zu den Themen *Soziale Netzwerke*, *sichere Passwörter*, *Phishing* und *Bildrechte* und diente dazu, einen Vorher-Nachher-Vergleich des Wissensstandes zu ermöglichen.

4.4 Kreativworkshops

Ziel der Kreativworkshops war es, die bereits in der Entwicklung befindlichen spielbasierten Lernszenarien entsprechend der Zielgruppen weiterzuentwickeln und neue Ideen zu geplanten Themen zu entfalten. Die Schülerinnen und Schüler sollten sich in die Rolle der „Entwickler“ reinversetzen und überlegen, wie sie ein bestimmtes Thema der Informationssicherhit jüngeren Schülerinnen und Schülern verständlich und erlebnisorientiert vermitteln könnten.
Der erste Kreativworkshop fand am 05. April 2019 zwischen 9 und 14 Uhr an der Technischen Hochschule Wildau statt. Das Konzept entstand in Zusammenarbeit mit dem Projektpartner known_sense. Den Auftakt bildete ein Impulsvortrag. Anschließend sollten sich die 19 Schülerinnen und Schüler von vier Projektschulen in drei Gruppen aufteilen und sich hierfür zwischen den Themen *Privatsphäre*, *Soziale Netzwerke* und *Knigge* entscheiden. Ein Überblick zum Veranstaltungsverlauf ist Abbildung 13 zu entnehmen.
Die sieben Lehrerinnen und Lehrer wurden ebenfalls in den Kreativworkshop integriert, sie wurden dem Thema *Fake News* zugeteilt. Eine gemischte Gruppe aus Lehrer/-innen und Schüler/-innen schien nicht erfolgsversprechend, da aufgrund bestehender Rollen- sowie Altersunterschieden mit erheblichen Hemmungen bzw. Zurückhaltung seitens der Schülerinnen und Schüler zu rechnen war. Jeder Gruppe war ein Team aus einer moderierenden sowie einer beobachtenden und dokumentierenden Person zugeordnet.

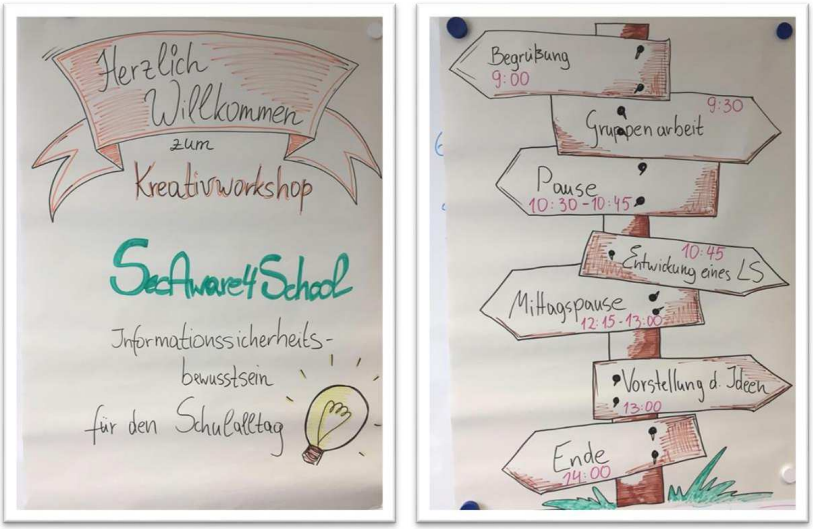


Abbildung 13: Kreativworkshop - Agenda

In jeder einzelnen Gruppe wurde eine Vorstellungsrunde mithilfe von askitMeta-Bildkarten durchgeführt. Bei diesem 10-minütigen assoziativen Warm-up sollten die Teilnehmenden unter anderem jeweils eine Bildkarte auswählen, die für ihn oder sie persönlich das Thema *Informationssicherheit* repräsentiert. Die nächste Kreativübung bestand darin, Collagen zu dem Thema *Sicherheitslandschaft Schule – heute und morgen* zu kreieren (s. Abbildung 14). Die Teilnehmenden erhielten hierfür zwei Sätze aus Landschaftsbildern, Bilderbögen und entsprechendes Zubehör. Die aktuelle und zukünftige Situation in Bezug auf Informationssicherheit an der jeweiligen Schule wurde anhand der Collage von denen der jeweiligen Teilnehmenden erläutert (s. Abbildung 15).

Abbildung 14: Kreativworkshops – Impression Kreativübung Collage

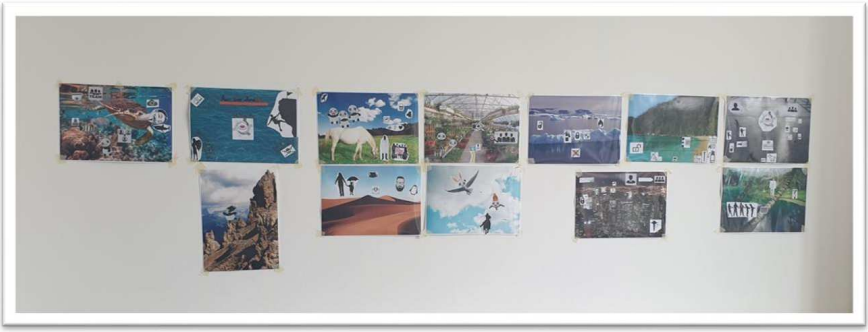


Abbildung 15: Kreativworkshop – Collage: Sichere Schule

Das Herz des Kreativworkshops bildeten die *Brain Stations*. Zu diesem Zweck wurden pro Gruppe fünf Flipchartpaper an den Wänden platziert, auf denen jeweils eine für die Entwicklung eines Lernszenarios relevante Frage stand. Die Teilnehmenden wurden nachfolgend aufgefordert, sich vor den fünf Plakaten zu verteilen und innerhalb von drei Minuten jeweils drei bis fünf kurze spontane Aussagen auf Klebezetteln zu notieren und anzuheften (s. Abbildung 16). Anschließend wechselten die Teilnehmenden zum nächsten Plakat, bis alle Teilnehmenden jede Frage mit ihren Kommentaren versehen hatten. Hieran schloss sich das Mapping an, bei dem die Ergebnisse in Gruppenarbeit zusammengefasst wurden. Die Gruppenarbeit sollte in eine Diskussion zur Optimierung bzw. Neuentwicklung der thematisierten Lernstationen überführt werden. Zum Ende der Veranstaltungen wurden die entwickelten Ideen den anderen Gruppen vorgestellt (s. Abbildung 17).

Abbildung 16: Kreativworkshop – Brain Stations

Abbildung 17: Kreativworkshops – Ergebnisse Mapping nach Brain Stations

Der Kreativworkshop wurde mithilfe der Methode *Brain Stations* ausgewertet. Die ersten beiden Übungen ermöglichten den Teilnehmenden einen kreativen Zugang zu den Themen und bildeten ein erfolgreiches und notwendiges Warm-up. Die *Brain Stations* selbst haben gezeigt, dass die Fragen für die Schülerinnen und Schüler zu abstrakt waren und sie Beispiele und bildhafte Unterstützung benötigen. Ein für die Entwicklung von Lernszenarien notwendiges Vorwissen war nur bedingt vorhanden. Die Zeit für die eigentliche Ideenentwicklung war zudem sehr knapp bemessen. Für weitere Kreativworkshops sollten daher die Übungen besser aufeinander abgestimmt werden.

Am 14. Mai 2019 fanden zwei halbtags Kreativworkshops mit jeweils einer 9. Klasse des Friedrich-Schiller-Gymnasiums statt. Als Warm-up wurde ein visuelles Brainstorming zum Begriff „Smart“ durchgeführt, dessen Ergebnisse in Abbildung 18 zu sehen sind. Im Anschluss wurde die Idee zum Thema *Soziale Netzwerke* aus dem vorherigen Kreativworkshop vorgestellt, daran weitergearbeitet und das Ergebnis zum Ende der Veranstaltung präsentiert. Diejenigen Schülerinnen und Schüler, die nicht kreativ werden wollten, wurden als Gametester aktiv.

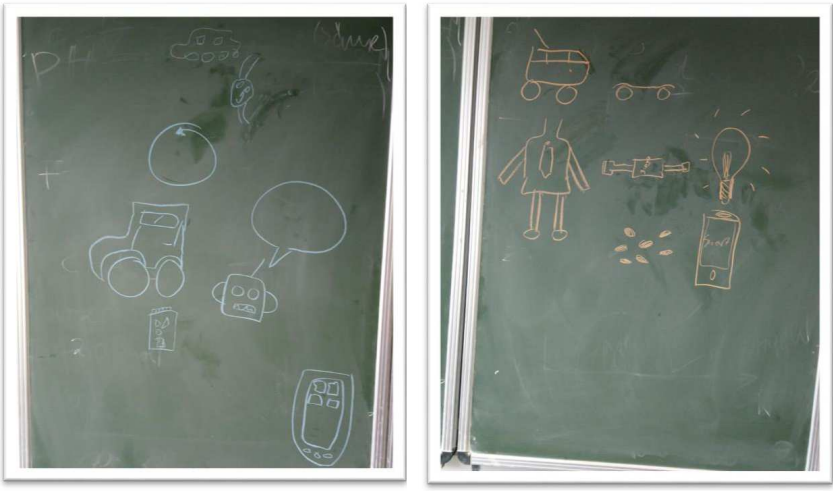


Abbildung 18: Kreativworkshop – Warm-up zum Begriff "smart"

Der Kreativworkshop am 06. Juni 2019 baute ebenfalls auf den Ergebnissen der vorherigen Workshops auf. Die Teilnehmenden berichteten über interessante Themen und kreative Methoden, die sie in ihrer kreativen Denkweise weitergebracht und das Thema *Informationssicherheit* erlebbar gemacht haben. Als Feedback (s. Abbildung 19) für das durchführende Forschungsteam wurden Punkte für die Organisation und Durchführung vergeben.

Abbildung 19: Kreativworkshop - Feedback

4.5 Gametest

Die spielbasierten Lernszenarien *Informationssicherheit: Schnelles Begrifferaten* und *Storytelling* wurden bereits während der Awareness Trainings ausreichend getestet und immer wieder angepasst. Die weiteren im Projekt entwickelten Lernszenarien waren zur Zeit der Awareness Trainings noch nicht ausgereift, sodass zusätzliche Termine für eine Testung eingerechnet wurden. Lernszenarien wie *Security Surfer*, *Digital Sozial*, *Security Duell*, *Fake or Real* und *Storytelling (digital)* wurden in diesem Zusammenhang getestet.

Ein erster Test fand im Rahmen des Kreativworkshops mit Schülerinnen und Schülern zweier 9. Klassen des Friedrich-Schiller-Gymnasiums statt, die sich nicht an der Entwicklung eines Lernszenarios beteiligen wollten. Getestet wurden die Lernszenarien *Bildrechte (digital)* (Arbeitstitel *Snapshot*), *Informationssicherheit: Schnelles Begrifferaten* (Arbeitstitel *Blitzer*), *Digital sozial – Internetregeln erkennen* (Arbeitstitel *Knigge*) und *Security Surfer – Gefahren und Schutzmaßnahmen erkennen* (Arbeitstitel *Hexa Surf*). Der hierfür entwickelte Fragebogen enthielt 20 Fragen, die mit einer 3er-Likert-Skala in der *Ausprägung 1=trifft nicht zu, 2=kann man gelten lassen und 3=trifft zu* beantwortet werden konnten. Das zusätzliche Bemerkungsfeld war für die Weiterentwicklung der Lernszenarien besonders nützlich. Die Fragebögen wurden von den Teilnehmenden nicht wie geplant einzeln, sondern in den Teams gemeinsam ausgefüllt.

Die erste Fragebogengeneration hat dahingehend Mängel gezeigt, dass die Bemerkungsfelder häufig ungenutzt blieben. Zudem stellte sich die 3er-Likert-Skala für einige Fragetypen als unpassend heraus, sodass der Fragebogen designtechnisch für die nächsten Tests überarbeitet wurde. Bei einem Teil der Fragen wurden zusätzlich universell verständliche Smileys zu der Ausprägung herangezogen. Des Weiteren wurden alle offenen Fragen hintenangestellt.

Mit sechs Fachinformatik-Auszubildenden des ZIT-BB wurde ein weiterer Test am 16. August 2019 durchgeführt. Getestet wurden *Fake or Real*, *Security Surfer*, *Bildrechte (digital)*, die englische Version von *Informationssicherheit: Schnelles Begrifferaten* sowie *Storytelling*. Der Test des ersten Prototypen von *Fake or Real* ergab, dass den Testenden vor allem Zusatzinformationen fehlten, um nicht lediglich bei der Zuordnung raten zu müssen. Besonders positiv wurden das bewusste Lesen und die Anregung zur Diskussion bewertet. Es wurde mehrfach vorgeschlagen, die Themen altersgerecht zum Beispiel aus den Bereichen Natur/Umwelt sowie Sport zu wählen. Des Weiteren wurde eine digitale Version angeregt.

Der zweite Prototyp von *Security Surfer* erwies sich bereits während des Tests als überarbeitungsbedürftig. Dies spiegelte sich auch im Feedback wider. So waren die Regeln

speziell hinsichtlich des in dieser Version vorgesehenen Hackerangriffs für die Teilnehmenden unklar. Besonders positiv wurden die grafische Umsetzung und der Brettspielcharakter bewertet. Als konkrete Veränderung wurde die Anpassung der Werte vorschlagen.

Das Feedback zur englischen Version von *Informationssicherheit: Schnelles Begrifferaten* fiel, wie bereits die deutsche Version in den Awareness Trainings, sehr positiv aus. Einzig der Umstand, dass die Komplexität der Begriffe innerhalb desselben Schwierigkeitsgrades abweicht, wurde angemerkt.

Um die Wiederspielbarkeit zu erhöhen, regten die Testenden von *Bildrechte (digital)* an, mehr Motive hinzuzufügen. Des Weiteren wurde eine statistische Auswertung am Ende als Verbesserung vorgeschlagen.

Storytelling wurde zwar bereits ausreichend hinsichtlich der Spielemechanik getestet, jedoch ist hierzu bisher keine Befragung erfolgt. Die Testenden bewerteten den kreativen Einstieg in die Thematik, das Spiel im Team und die leichte Anpassbarkeit und Erweiterbarkeit als besonders positiv. Kritisiert wurden vor allem der Papierverbrauch, die Kürze der vorgegebenen Spielzeit und der hohe Schreibaufwand, um abschließende Geschichten zu kreieren. Dieses Feedback floss direkt in die Finalversion ein, wobei der Aspekt des Schreibens im Hinblick auf einen pädagogischen Nebeneffekt beibehalten wurde.

Ein Feedback zum Fragebogen selbst zeigte, dass die Teilnehmenden eher eine 5er-Likert-Skala bevorzugen, um Nuancen besser darstellen zu können. Um den Auswertungsumfang zu minimieren, wurde für weitere Tests eine angepasste digitale Version erstellt.

Am 04.09.2019 fand ein Gametest von *Bildrechte (digital)* mit 13 Teilnehmenden statt, deren Bewertung bereits über den digitalisierten Fragebogen erfolgte.

Ein weiterer größerer Test erfolgte im Rahmen des am 28.01.2020 stattfindenden Fachtages der TH Wildau. Im Fokus standen die Lernszenarien *Digital sozial*, *Security Duell* und *Storytelling* (digital). Aufgrund des engen Zeitrahmens wurde auf das Ausfüllen eines Fragebogens verzichtet und stattdessen ein Gruppeninterview auf Basis des Fragebogens geführt. Bei *Digital sozial* bewies sich das Puzzle in zwei Durchläufen zwar als gutes Warm-up, jedoch mit einer sehr unterschiedlichen Bearbeitungszeit. Die Teilnehmenden begrüßten vor allem den Erfahrungsaustausch, die Argumentation und das Kennenlernen unterschiedlicher Sichtweisen. Die Fairness wurde im Schwierigkeitsgrad 3 als nicht gegeben gesehen, da Mogeln leicht durch Abschauen und Nachahmen vom anderen Team möglich scheint.

Da aufgrund der COVID-19 Krise geplante Workshops auf unbestimmte Zeit verschoben werden mussten, konnten keine weiteren umfangreichen Tests der Lernszenarien erfolgen. Um jedoch ein weiteres Lernszenario zum Thema *Fake News* zu testen, fand am 05.06.2020 ein

außerplanmäßiger Test mit vier Fachinformatik-Auszubildenden im zweiten Lehrjahr des ZIT-BB statt, die bereits 2019 am Test von Lernszenarien an der TH Wildau teilgenommen hatten. Bei diesem Test wurden der Prototyp eines Kartensatzes verwendet und zwei Teams gebildet, die gegeneinander spielten. Als Ergänzung zum Spiel stand ein Wiki in Papier- und elektronischer Form zur Verfügung. Die Papierversion wurde nicht in Anspruch genommen und die Webversion nur kurz getestet. Die erweiterten Erklärungen zu den im Spiel genannten Fällen wurden mündlich vorgetragen. Die Notwendigkeit für ein Wiki hat sich bestätigt, weil die genannten Fälle nur zum Teil bekannt waren und in anderen Fällen Erklärungsbedarf bestand. Es ist davon auszugehen, dass die Teilnehmenden dank ihres Vorwissens weniger auf ein Nachschlagewerk angewiesen waren, als es bei der tatsächlichen Zielgruppe der Fall sein dürfte. Mit der Offline-Version ist aber ein Spiel ohne Multimedia-Unterstützung möglich.
Die Regeln waren zum Zeitpunkt des Tests noch nicht festgeschrieben und wurden später überarbeitet. Bemängelt wurde z. B. der noch fehlende Wettbewerbscharakter, der jedoch nicht das primäre Ziel des Lernszenarios darstellt. Vielmehr sollten die Jugendlichen in den Erfahrungsaustausch treten und über die im Lernszenario genannten realen Fälle gezielt über die Aspekte von Fake News, Fehlinformation und Betrug diskutieren. Im Test erwies sich diese Zielstellung als erfüllt. Eine Erweiterung der Fälle wurde zwar von den Testenden angeregt, jedoch wird dies durch die vorherige Festlegung auf die Größe eines klassischen Kartensatzes von 32 Karten nicht mehr im Projekt SecAware4school realisiert. Im Test zeigte sich, dass 20 bis 30 Minuten für dieses Lernszenario unzureichend sind. Da die Diskussion komplexer Zusammenhänge ein elementarer Bestandteil des Lernszenarios ist, wird empfohlen genügend Zeit von mindestens einer Schulstunde einzuplanen.

5 Serious Games – analoge und digitale spielbasierte Lernszenarien

Zur Entwicklung und Modifizierung digitaler Simulationen und analoger Lernszenarien wurden Inhalte aus den Ergebnissen der Umfrage eingefügt, die Ideen aus den Kreativworkshops einbezogen und die Erfahrung vorangegangener Projekte genutzt.
Im Prozess der Entwicklung wurden mehrere Stationen berücksichtigt. Nach der Ist-Analyse und Zieldefinierung ausgewählter Themenbereiche der Informationssicherheit folgte die Kreativphase. In der Kreativphase sollen die Ideen innerhalb des Teams zu bestimmten inhaltlichen Themen gesammelt werden. Dabei wurde oft die Methode des *Design Thinking*

Process angewandt. Diese wurde an die Gegebenheiten angepasst, sodass für die Schülerinnen und Schüler, die in Abbildung 20 aufgeführten Arbeitsschritte festgelegt wurden.

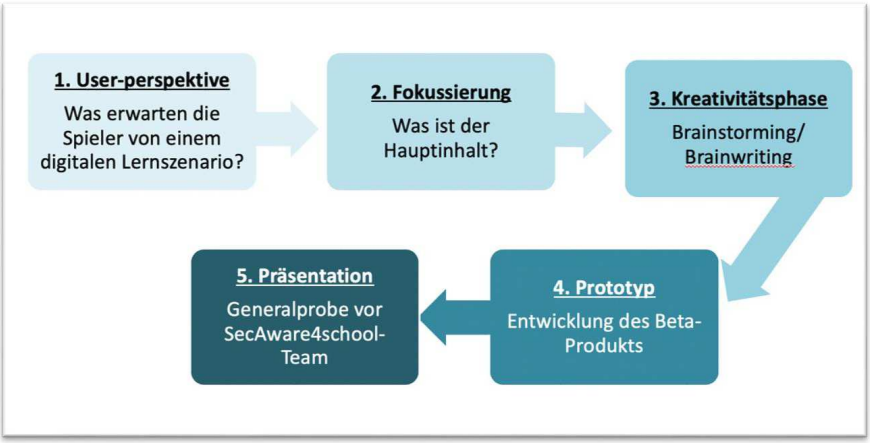


Abbildung 20: Angepasster Design Thinking Prozess

Die wichtigsten Punkte bei der Entwicklung von Lernszenarien sind: die Perspektive der Nutzer; Konkretisierung des wichtigsten Inhaltes; das Sammeln der Ideen; das Entwickeln eines Prototyps und das Testen und Evaluieren des Lernszenarios. Diesem Konzept sind das Team SecAware4school sowie die am Projekt beteiligten Schülerinnen und Schüler des Seminarkurses bei der Entwicklung der Lernszenarien nachgegangen.

5.1 Informationssicherheit: Schnelles Begrifferaten

Beim Lernszenario *Informationssicherheit: Schnelles Begrifferaten* wird der sichere Gebrauch von Fachbegriffen im Begriffsfeld *Informationssicherheit* geübt. Durch die zunehmende Menge an online verfügbaren Informationen und Diensten ist es von Bedeutung, sich mit Fachbegriffen der Informationssicherheit vertraut zu machen.

Ziel des Lernszenarios ist es, anhand von Hinweisen Fachbegriffe nach dem „Galgenmännchen"-Prinzip zu erraten. Die Spielenden haben etwa 15 Minuten Zeit, den Stapel an Karten in ihrem Schwierigkeitsgrad abzuarbeiten. Pro Karte gibt es nur drei Fehlversuche. Ein Ausschnitt aus einem Awareness Training ist in der Abbildung 21 zu sehen.

Abbildung 21: LS Informationssicherheit Schnelles Begrifferaten

5.2 Digital sozial – Internetregeln erkennen

Ein Anliegen des Forschungsteams war es, neben den klassischen informationssicherheitsspezifischen Aspekten auch eine soziale Komponente in ein Lernszenario aufzunehmen. Im Vordergrund der Entwicklung stand daher weniger das Wissen, sondern viel mehr die Einstellung und das Verhalten der Schülerinnen und Schüler. Aus der Idee heraus ein Lernszenario zum „Internet-Knigge“ zu entwickeln, wurde zu den Wünschen und Bedürfnissen zur „Netiquette“ (Regeln für das richtige Benehmen im Internet) von Internetnutzenden recherchiert. Die daraus entstandenen Aussagen wurden in einem ersten Versuch in Wortgruppen zerlegt und sollten wieder in sinnvolle Aussagen zusammengesetzt werden (s. Abbildung 22). Diese allererste Version stellte sich jedoch selbst bei Kenntnis der Aussagen als äußerst schwierig heraus. Daraus entwickelte sich die Idee eines Puzzles. Hierfür wurde ein Teil der Aussagen bildlich dargestellt. Ein erster Prototyp ist in Abbildung 23 dargestellt.

Abbildung 22: LS Digital sozial – Test der ersten Idee

Abbildung 23: LS Digital sozial – Erster Prototyp

Das Puzzle sollte als Warm-up den Teilnehmenden die Gelegenheit bieten, sich mit der Thematik auf spielerische Art vertraut zu machen. Das fertige Puzzle war ursprünglich als Spielunterlage angedacht. In verschiedenen Tests zeigte sich jedoch die zum Teil stark variierende Bearbeitungszeit. Zudem war nicht ersichtlich, inwieweit durch das Puzzeln der Inhalt bereits wahrgenommen wurde. Sowohl diese Aspekte als auch eine nachträgliche Kürzung des Projektbudgets führten zu der Entscheidung, die Puzzleidee als solche zu verwerfen.

In der Endfassung dienen die Motive als Spielunterlage (s. Abbildung 24, 25 und 26). Um Schülerinnen und Schüler für das Thema zu sensibilisieren, wurden Fragen zu den Aussagen entwickelt, die zum Austausch und zur Diskussion anregen sollen. Dank dieser Interaktion soll die Thematik aus verschiedenen Perspektiven betrachtet werden.

Die Spielunterlage zur Schwierigkeitsstufe 1 (s. Abbildung 24) funktioniert ähnlich wie ein klassisches Brettspiel – die Teams würfeln, setzen ihre Figur, ziehen eine Karte, beantworten die Frage aus ihrer Erfahrung und diskutieren, zu welcher Aussage diese Frage passt. Bei der

richtigen Zuordnung erhält das Team einen Punkt. Die Spielunterlagen zu den Schwierigkeitsgraden 2 und 3 unterschieden sich inhaltlich nur geringfügig voneinander. Der Darstellung liegt die Form eines Netzwerkes in Anlehnung eines sozialen Netzwerkes zugrunde. Die beiden Versionen wurden um je vier Aussagen erweitert und kommen ohne Würfel aus. Im Unterschied zu Schwierigkeitsgrad 1 und 2 passen zu einer Frage des Schwierigkeitsgrades 3 mehrere Aussagen. Dies soll die Argumentationsfähigkeit der Teilnehmenden fördern und dazu führen, dass sich diese noch umfassender mit den Fragen und Aussagen auseinandersetzen.

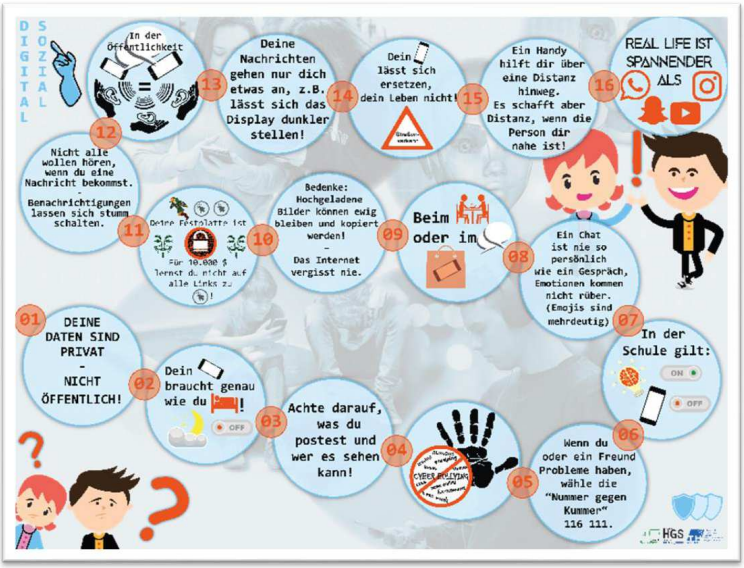


Abbildung 24: LS Digital sozial – Spielunterlage Schwierigkeitsgrad 1

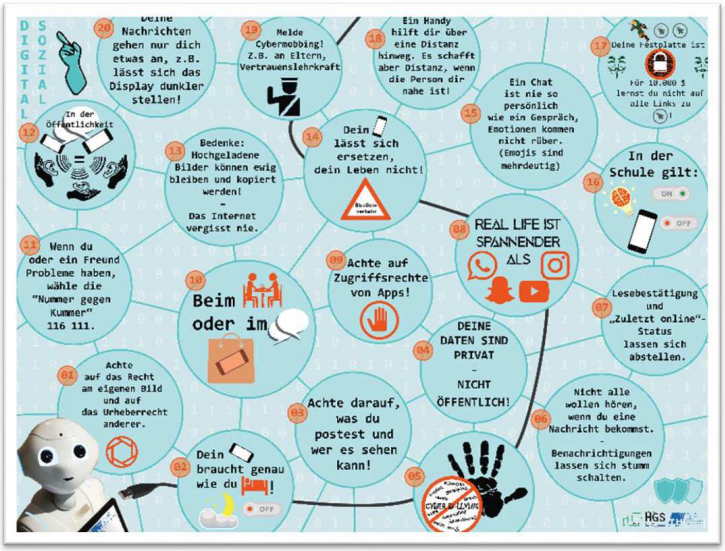


Abbildung 25: LS Digital sozial – Spielunterlage Schwierigkeitsgrad 2

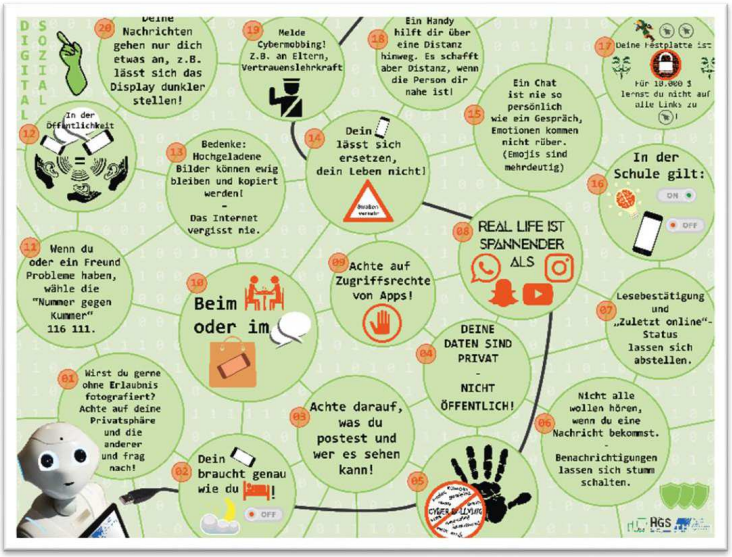


Abbildung 26: LS Digital sozial – Spielunterlage Schwierigkeitsgrad 3

5.3 Security Surfer – Gefahren und Schutzmaßnahmen erkennen

Das Motiv des Meeres und der Inseln als Symbol des Internets ist durch den Begriff „Internetsurfen“ nach Brainstorming- und Assoziationsübungen des Forschungsteams entstanden. Der Begriff wurde unter anderem durch einen Artikel „Surfing the Internet“ geprägt, der 1992 von der US-amerikanischen Bibliothekarin Jean Armour Polly veröffentlicht wurde (Digital-Kompas, & Deutschland sicher im Netz e.V. (Hrsg.)). Der Begriff „Security Surfer“ betitelt das Lernszenario hingegen im Sinne eines sicheren Surfens im Internet. Ziel des Lernszenarios ist es, dass Teilnehmende ein Bewusstsein für die Gefahren im Internet in verschiedenen Bereichen wie Soziale Netzwerke, Onlinespiele und Onlineshopping entwickeln sowie Schutzmaßnahmen kennen und ergreifen können.

Das Lernszenario *Security Surfer* durchlief viele Entwicklungsstufen. Zu Beginn der Entwicklung des Lernszenarios stand bereits sein Thema *Gefahren im Internet und mögliche Schutzmaßen* fest. Die erste Grundidee griff die Entwicklung eines unechten Memospiels auf, bei dem Gefahren passenden Schutzmaßnahmen zugeordnet werden sollten (s. Abbildung 27).

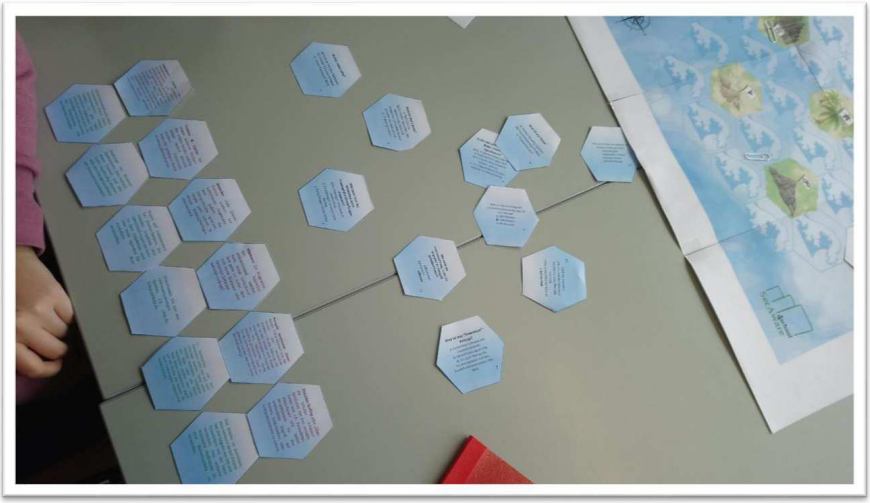


Abbildung 27: LS Security Surfer – Idee: Entwicklung eines unechten Memospiels

In der späteren Weiterentwicklung wurden die Karten in Form eines achtseitigen Polygons konzipiert. Dieses Design ermöglicht es, einer Gefahr verschiedene Schutzmaßnahmen zuzuordnen. Bei Recherchen zur Umsetzbarkeit der Polygonidee fanden sich Druckereien, die zwar keine achteckigen Polygone, jedoch aber sechseckige Polygone in einer für Spielkarten angemessenen Größe produzieren. Die Kartengröße wurde angepasst, da für die Entwicklung

der Karten die Forschungsgruppe die für das populäre Spiel „Die Siedler von Catan“ verwendete Kartengröße mit einer Kantenlänge von 45 Millimeter wählte. Die Größe der Hexagone bestimmt somit die Größe des Spielfeldes. Der Aspekt der Umsetzbarkeit sollte bei der Entwicklung kreativer Spielideen, die nicht in klassischen Formaten konzipiert werden, unbedingt nach den ersten Entwicklungsschritten beachtet werden, um möglichst hohe Produktions- bzw. Änderungskosten des Designs zu vermeiden. Grundsätzlich entscheidet die Auflage bei den meisten Druckaufträgen darüber, welches Druckverfahren angewendet werden kann. Für Aufträge in Kleinstauflage, wie es in diesem Projekt der Fall ist, bieten die Druckereien häufig nur Standardformate an. Die Alternative ist ein entsprechend hoher Stückpreis.

Abbildung 28: LS: Security Surfer - Erster Prototyp

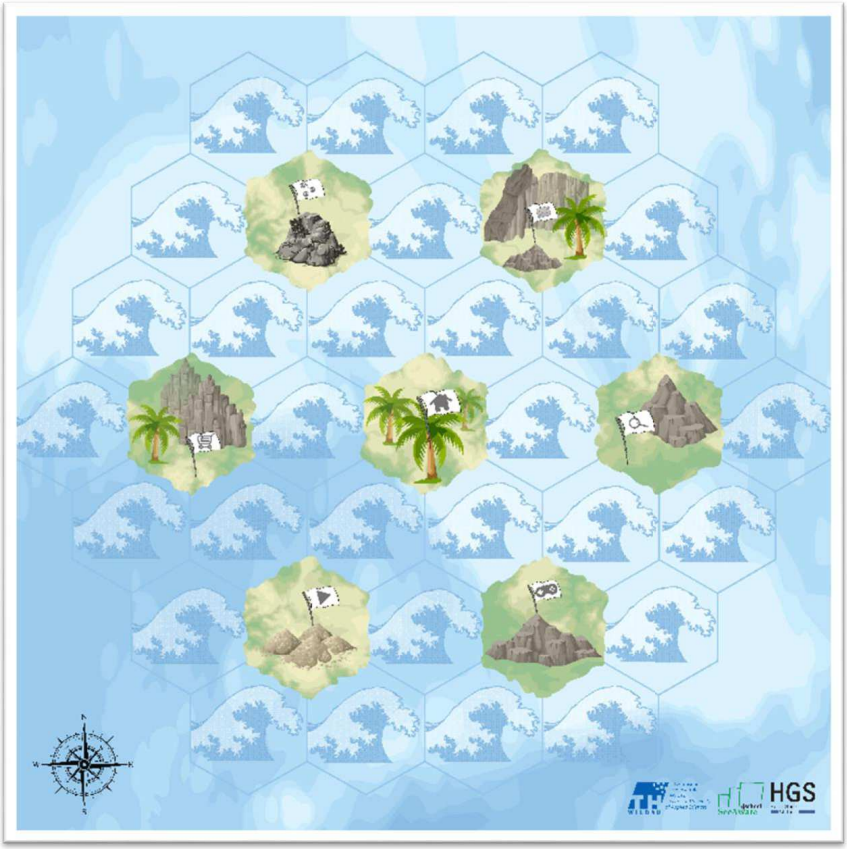


Abbildung 29: LS Security Surfer - Eine Weiterentwicklung

Der erste Prototyp ist in Abbildung 28 dargestellt, Abbildung 29 zeigt eine Weiterentwicklung. Bei ersten Tests dieser Prototypen stellte sich schnell heraus, dass die Spielemechanik in der Realität nicht optimal funktioniert. Dies verdeutlicht umso mehr, wie bedeutend regelmäßige Tests für die Weiterentwicklung (s. Abbildung 30) sind. Erreichen die Lernszenarien eine fortgeschrittene Entwicklungsstufe und Reife, ist das Testen durch die jeweilige Zielgruppe unerlässlich (s. Abbildung 31). Diese Lernszenario wurde auch mit einer Studierendengruppe getestet. Nur so ist eine sowohl inhaltliche als auch ausdruckstechnische Anpassung an die Zielgruppe möglich. Nach der Überarbeitung der ersten Prototypen wurde überprüft, ob der Sensibilisierungscharakter erfüllt ist. Eine Sensibilisierungsmaßnahme sollte Aspekte enthalten, die das Wissen (= Knowledge), die Einstellung (= Attitude) und das Verhalten

(= Behavior) (Khan, et al. 2011) der Teilnehmenden ansprechen. Die Vermittlung von Wissen, zum Beispiel hinsichtlich von Fachbegriffen, bildet die Basis einer Sensibilisierung (M. Scholl 2018, 31). Diese ermöglicht den Teilnehmenden, in einem aktiven Austausch mit anderen ihre Einstellung zu informationssicherheitsrelevanten Themen zu reflektieren. Erst diese Reflektion der eigenen Einstellung lässt eine spätere/folgende Verhaltensänderung zu. Da bis zu diesem Entwicklungstand vorwiegend nur das Wissen im Vordergrund stand, musste umfangreich inhaltlich nachgebessert werden. Die ursprüngliche Idee des unechten Memos wurde zu diesem Zeitpunkt gänzlich verworfen.

Abbildung 30: LS Security Surfer - Zweite Entwicklungsstufe

Abbildung 31: LS Security Surfer – Test der zweiten Entwicklungsstufe mit Fragekarten

Des Weiteren wurde die bis dato sehr komplexe und strategisch ausgerichtete Spielemechanik um ein Vielfaches vereinfacht. Gerade eine komplexe Spielemechanik kann sich bei einem kurzweiligen Lernszenario negativ auf die Spielbarkeit auswirken, da viel Zeit für das Verstehen der Spielregeln aufgebracht werden muss. In der Endversion (s. Abbildung 32) stehen die ersten sechs Felder des Spielfeldes für Wissen.

Abbildung 32: LS Security Surfer – finale Version. Spielfeld

Hier erfahren die Teilnehmenden, was sich hinter bestimmten Begriffen verbirgt. Die häufig offenen Fragestellungen im weiteren Spielverlauf führen die Teilnehmenden in einen Erfahrungsaustausch im Rahmen einer Diskussion, der die Reflexion der eigenen Einstellung und eine Verhaltensänderung ermöglicht.

5.4 Verhalten in sozialen Netzwerken – Internetregeln erkennen

Die allererste Idee zum Wunschthema der teilnehmenden Schülerinnen und Schüler entstand im Kreativworkshop von einer Gruppe Neuntklässlern aus dem Friedrich-Schiller-Gymnasium Königs Wusterhausen. Im Kreativworkshop im Rahmen des Projektes SecAware4school wurden verschiedene Themen behandelt. Nach der Frage, wie richtiges Verhalten in den sozialen Netzwerken erlern- und vermittelbar gestaltet werden kann, wurden Ideen zum Lernszenario entwickelt und präsentiert. Nach der Idee der Schülergruppe war das Lernszenario interaktiv und interessant zu gestalten.

Das Lernszenario zum Thema *Soziale Netzwerke* sollte dazu beitragen, sich bewusst über das eigene Verhalten in sozialen Netzwerken zu werden. Dazu gehört, sich in der Umgangsform im Internet zu reflektieren und über das eigene Verhalten kritisch nachzudenken. Des Weiteren umfasst das Lernszenario Themen wie *Mobbing* und Notsituationen, die gemeldet werden sollten. Hierbei soll abgewägt werden, wie kritisch die vorgegebene Situation ist und welche Handlungsmaßnahmen eingeleitet werden sollten. Als Ausgangsbasis wurden dazu Ideen aus verschiedenen bekannten Gesellschaftsspielen zusammengetragen und zu einem Ganzen kombiniert. Der Abbildung 33 ist zu entnehmen, dass sich das Lernszenario aus mehreren Kategorien zusammensetzt. An der Idee der Schülergruppe wurde im SecAware4school-Team weiter gearbeitet und getestet.

Abbildungen 33: LS Verhalten in sozialen Netzwerken - Erste Idee der Schülerinnen und Schüler des Friedrich-Schiller-Gymnasiums Königs Wusterhausen

In Abbildung 34 ist die überarbeitete Idee des Forschungsteams dargestellt und in Abbildungen 35 und 36 die Überarbeitung und Evaluation.

Abbildung 34: LS Verhalten in sozialen Netzwerken - Idee des Forschungsteams

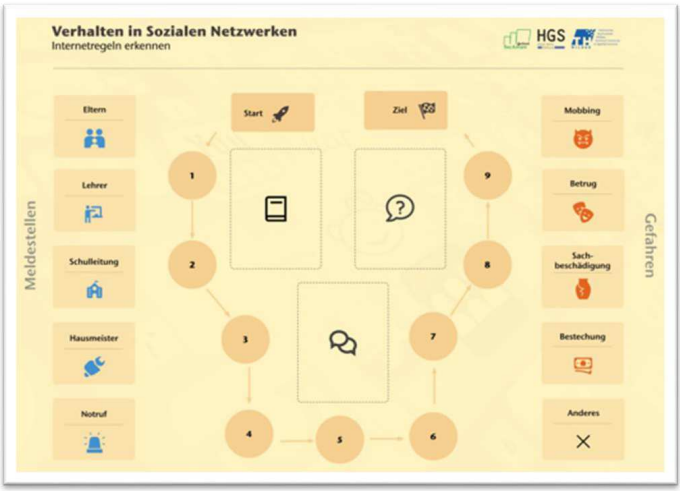


Abbildung 35: LS Verhalten in sozialen Netzwerken - Überarbeitung der Idee

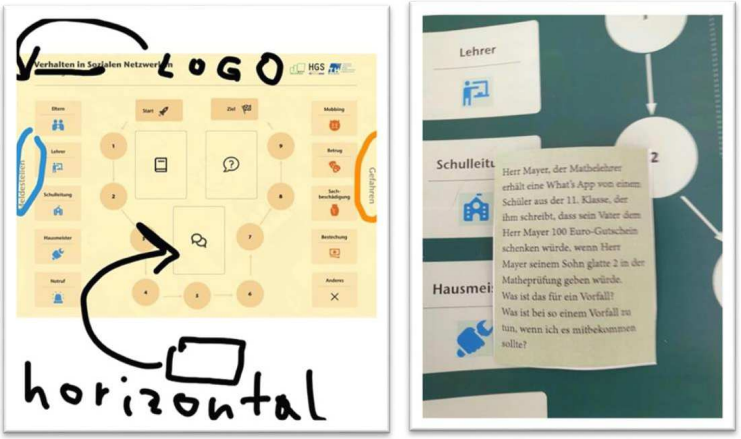


Abbildung 36: LS Verhalten in sozialen Netzwerken - Evaluierung des Lernszenarios

Die Testungen mit verschiedenen Altersgruppen haben gezeigt, dass die Komplexität des Lernszenarios heruntergebrochen werden muss, um das Interesse und die Aufmerksamkeit der Zielgruppe aufrechtzuerhalten. Nach dieser Erkenntnis wurden die finale Version des Lernszenarios erstellt und die Inhalte überarbeitet (s. Abbildung 37). Das Ziel des Lernszenarios wurde somit präzisiert auf die Bewusstmachung und Kenntnis potenzieller Sicherheitsgefahren sowie entsprechender Schutzmaßnahmen in sozialen Netzwerken und im Schulalltag. Hierbei werden sowohl Themen der Informationssicherheit als auch der physischen Sicherheit angesprochen. Dieses Lernszenario wurde für drei Altersgruppen in verschiedenen Schwierigkeitsgraden konzipiert.

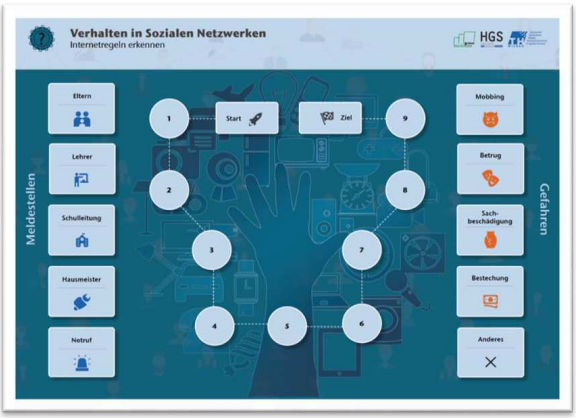


Abbildung 37: LS Verhalten in sozialen Netzwerken - finale Version

5.5 Storytelling und Storytelling digital

Das Erzählen von Geschichten ist nicht nur für die Fantasie anregend, sondern auch für die Entwicklung von sprachlichen Kompetenzen und für das Verinnerlichen spezifischer Inhalte. Beim Formulieren und Erzählen von Geschichten werden vergangene Ereignisse rekonstruiert und mit Erinnerungen verbunden. Die dabei rekonstruierten Fakten werden durch das Neuformulieren bzw. Darstellen neu interpretiert, selektiert und evaluiert (Busch 2013). Das Spielprinzip für *Storytelling* ist einfach: Symbole werden in eine Geschichte eingebaut. Erweitert um Vorgaben, wie z.B. Fachbegriffe aus den Bereichen Sicherheit, Datenschutz oder Privatsphäre, kommt es zu einer intensiven Auseinandersetzung mit dem vorgegebenen Thema. Die Geschichte kann lustig, ernst oder ausgefallen sein. Vielmehr zielt dieses Prinzip auf einen Effekt ab, der als „Mnemonik" bekannt ist. Er beschreibt die Verbesserung der Merkfähigkeit, wenn Begriffe und deren Bedeutung gezielt in eine kleine Geschichte eingebaut werden. Um das Lernziel nicht zu verfehlen, ist es daher wichtig, möglichst alle vorgegebenen Symbole in die Geschichte einzubinden. Diese Regel soll zusätzlich die Fantasie und Kreativität der Teilnehmenden anregen. Im Projekt SecAware4school liegt der Fokus auf dem Thema *Informationssicherheit*. Dieses Lernszenario ist jedoch nicht allein auf die Informationssicherheit beschränkt und kann für beliebige Themen adaptiert werden.
Auf der analogen Version beruhend begann die Entwicklung einer digitalen Variante, die eine Investition in analoges Spielmaterial entbehrlich macht und somit einen geringen Aufwand in der Vorbereitung bedeutet. Darüber hinaus sollte die digitale Version ein „Schummeln" bei der Auswahl der Symbole verhindern. Ausgehend von den genannten Vorbedingungen wurden unterschiedliche Varianten des Spiels entwickelt.

Variante I

Mit einer einfachen Webapplikation (Vue.js) kann ein Thema und die Anzahl der zufällig generierten Symbole festgelegt werden. Die Symbole werden nach dem „Wurf" angezeigt. Davon kann ein Bildschirmfoto erstellt und ausgedruckt werden (s. Abbildung 38). Die Vorbereitungszeit für eine Lerneinheit ist damit sehr gering, was die moderierende Person entlasten sollte. Diese Variante steht online zur Verfügung und kann unter der URL https://story-telling.methopedia.eu/ aufgerufen werden.

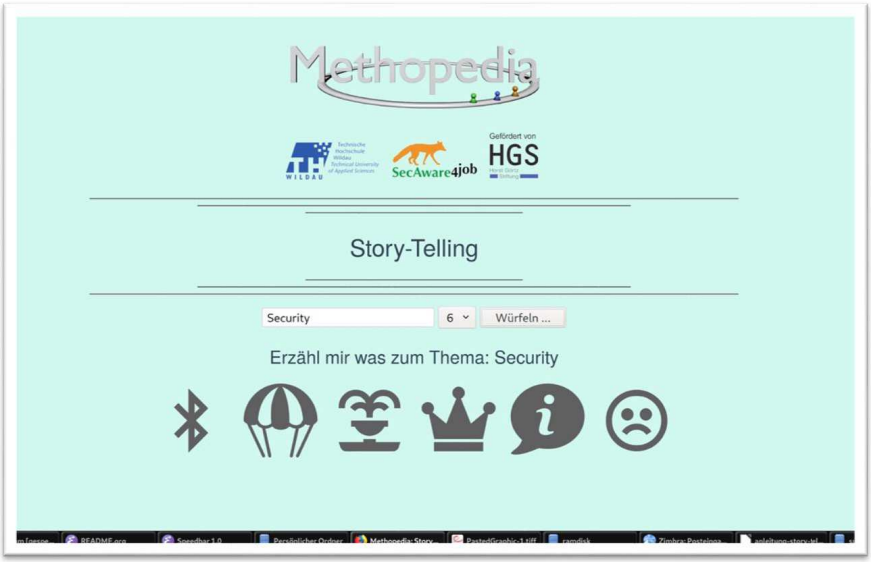


Abbildung 38: LS Storytelling digital - Variante 1

Die digitale Variante ist mit der analogen Variante verknüpfbar, indem die Symbole ausgedruckt und ausgeschnitten bzw. abgezeichnet und direkt in den geschriebenen Text eingearbeitet werden können (s. Abbildung 39).

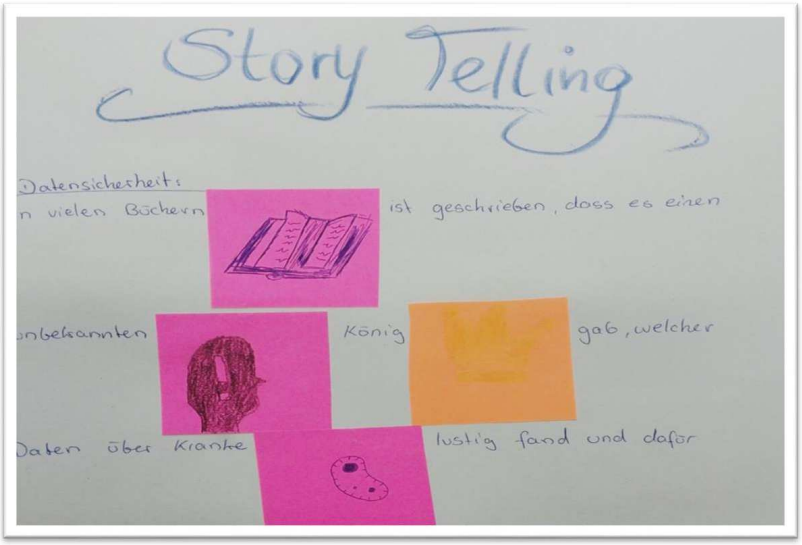


Abbildung 39: LS Storytelling analog - Bsp. aus einem Awareness Training

Variante II

Die Spielentwicklung ist eng mit dem Testen neuer Technologien verknüpft. So ist im Spielesektor eine Zunahme im Bereich der 3D-Visualisierung zu beobachten. Nachteilig für den allgemeinen Einsatz in Schulen sind die anspruchsvollen Voraussetzungen, wie hoher Investitions- und Installationsaufwand, oft verbunden mit kostenpflichtigen Optionen und nicht freien Lizenzen. Ein duales System wie kostenlose Installation und Nutzung einer Software für erste Tests und die Evaluation neuer Technologien sind hilfreich und erleichtern den Einstieg. Die Weiterentwicklung wurde aus Zeit- und Kostengründen nicht weitergeführt. Ein Prototyp (s. Abbildung 40) kann unter der URL https://story-telling-3d.methopedia.eu/ aufgerufen werden.

Abbildung 40: LS Storytelling digital aus dem vorangegangenen Projekt SecAware4job

Variante III (SecAware4school-Projekt)

Die finale Variante, die im SecAware4school an die vorhandenen Versionen anknüpft, soll ebenfalls ohne die Verwendung von Papier auskommen. In dieser Variante kam das Entwicklertool „Godot“ zum Einsatz. Nun bietet die dritte Variante neben der zufälligen Auswahl von Symbolen auch eine Möglichkeit, mittels Drag & Drop sowohl die Symbole als auch Text-Schnipsel wie bei der analogen Version anzuordnen (s. Abbildung 41).

Das Spiel steht online zur Verfügung und kann unter folgender URL aufgerufen werden: https://szenarien.wildau.biz/storytelling/storytelling.html

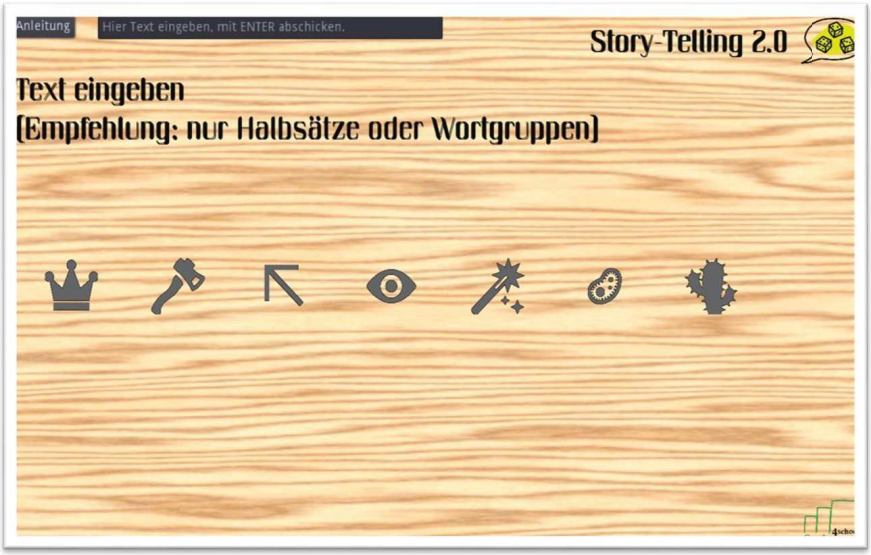


Abbildung 41: LS Storytelling digital im Projekt SecAware4school

Hybrider Ansatz zwischen digitalen und analogen Lernszenarien

Die digitalen Varianten bieten den Vorteil, dass die Vorbereitung von Materialen entfällt. Sie bieten einen schnellen Start in die Bearbeitung der Aufgabe, wenn eine entsprechende Technik zur Verfügung steht. Während auf dem Papier Korrekturen nur eingeschränkt möglich sind, können in der Applikation Texte jederzeit verbessert werden.

Nachteilig ist, dass bei Gruppenübungen nur ein Gruppenmitglied die Tastatur bedienen kann, während alle anderen Gruppenmitglieder nur als beratende Zuschauer fungieren. Des Weiteren entfällt, wie bei vielen digitalen Anwendungen und Spielen, das Trainieren der Handschrift, das als wichtige Übung für Gehirn und Feinmotorik gilt. Um diesen Nachteil auszugleichen, wäre eine Kombination aus Werfen der Symbole und Bildschirmfoto (Variante I oder II) möglich. Das Bildschirmfoto oder einzelne Bilder werden in ein kollaboratives Schreibprogramm eingefügt. Alle Gruppenmitglieder haben dann die Möglichkeit, gemeinschaftlich den Text zu bearbeiten. Das eben beschriebene Verfahren wurde im Rahmen des Projektes SecAware4school noch nicht evaluiert, aber als weiterführende wissenschaftliche Forschung ins Visier genommen. Dagegen stehen oft die Datenschutzbestimmungen an den Schulen und der Zwang, sich auf einer Plattform anmelden zu müssen. Genau dies wollen wir mit unseren

Programmen vermeiden. Auch die Schul-Cloud des Landes Brandenburg bietet das gemeinsame Bearbeiten von Inhalten noch nicht an.

5.6 Fake or real? Fake News erkennen

Das Lernszenarios zielt auf das Aneignen eines bewussten Umgangs mit Fake News ab und soll durch Übungen die Fähigkeit vermitteln, Fake News von Wahrheiten unterscheiden zu können. Folgende Teillernziele waren für das Szenario angestrebt:

- Funktion/Intention von Fake News. Wissen ist Macht und beeinflusst Menschen in ihrer Meinung und Handlung.
- Hinterfragen von Informationen, d. h. Schülerinnen und Schüler sollten Informationen kritisch bewerten und dafür sensibilisiert werden, nicht alles zu glauben, was in den Medien geschrieben und gesagt wird. Integration des Wertes von Informationen in das eigene Wertebewusstsein einbeziehen, Entschleunigung von Informationsweitergabe bewirken.
- Definition, Synonyme und Arten von Fake News kennenlernen.
- Merkmale und Erkennungsstrategien von Fake News erkennen und anwenden. Z.B.: *Wie unterscheide ich wahre und gefälschte Aussagen und/oder Bilder? Welche Fragen sollte ich mir stellen, wenn ich nicht sicher bin, ob die Nachricht in den Medien richtig ist?*

Um das Erlebnis und die Spielbarkeit zu gewährleisten, waren weitere Bedingungen für dieses Lernszenario formuliert: Die Bearbeitungszeit für die Lernstation sollte 20 Minuten nicht überschreiten und trotz dessen die Option der Skalierbarkeit als „Präsenztraining“ (d.h. Verlängerung bis zu einer Schulstunde von Spiel und Moderationsteilen) ermöglichen. Außerdem sollten Form und Ansprache analog realisiert werden. Der Vorteil der analogen Umsetzung dieses Themas ist, dass die Station verzögerungsfrei und relativ glatt *out of the box* funktioniert, ohne die Abhängigkeit von digitaler Infrastruktur (bzw. deren Fehleranfälligkeit).

Die Idee zu diesem Lernszenario entstand gemeinsam mit dem Projektpartner, der Firma known_sense unter der Leitung von Dietmar Pokoyski, der das Lernszenario fertigstellte. Bilder und sog. *News,* also Nachrichten, müssen entsprechend unterschieden und sortiert werden. Die Karten mit den Bildern bzw. News müssen entsprechend ihres vermuteten Wahrheitsgehalts auf eine rote (falsch) oder grüne (wahr) Decke gelegt werden. Die Zuordnung der Nachrichten erfordert somit eine eigene Bewertung des Wahrheitsgehalts der Informationen.

Die Bedingung, ein analoges Lernszenario zu kreieren, zeigt auch in Hinblick auf die Erforderlichkeit eines pragmatischen Fallback-Szenarios und der Handlungsfähigkeit im *worst case* ihre Berechtigung. Wie bei anderen Lernszenarien wurde auch hier ein Moderationsleitfaden verfasst.

Zunächst wurde das Konzept „Domino" als zusätzliche Aufwärmphase angeregt. In jedem Fall sollte der methodische Aspekt „Erkennungsmerkmale" vor dem eigentlichen Beginn des Spielens mitbewegt werden – idealerweise als eine Art Präambel Game (ähnlich wie das Quasi-Domino bei der Station „Internet Services, Apps & Co" oder die Bildkarten bei „Social Media" aus dem vorangegangenen Projekt SecAware4job). Von enormer Wichtigkeit war die Realisierung des Lernszenarios für drei Zielgruppen nach Alterskompatibilität. Dafür wurden die Inhalte nach zwei Aspekten in einer 50/50 Aufteilung ausgewählt: a) generischer Content mit News für alle mit allgemein verständlichen Informationen (z.B. Nachrichten über große globale Themen, etwa Informationen zu Friday4Future-Demos etc.) und b) spezifische Nachrichten analog der Reife (z. B. Nachrichten orientiert am peergruppengerechten Interesse wie Popkultur oder variierender Komplexität bei politischen Themen).

Aus der 50:50-Quotierung ergab sich, dass bei den z. B. erstrebten 30 Nachrichten für jede Zielgruppe insgesamt 60 aufbereitet werden müssten (15 generische und je 15 spezifische für die 3 Zielgruppen). Im Ergebnis wurden jeweils 16 Karten für jeden Schwierigkeitsgrad präpariert. Um Fake News nachzuvollziehen, wurden reale Nachrichten umgeschrieben. Dabei kam die Überlegung auf, einen analogen Katalog als Quelle zu reichen, in dem die realen Nachrichten (in verkürzter Form) aufgeführt sind. Diese verkürzten, wahren Nachrichten sollten dann mit denen auf den Karten abgeglichen werden. Diese Idee wurde hier nicht weiterverfolgt, um die Komplexität des Lernszenarios gering zu halten und die Spielbarkeit in einer vorgegebenen Zeit im Schulunterricht zu gewährleisten. Stattdessen wurde sie in der Gestaltung des Lernszenarios *Fake News. Mit Fake News richtig umgehen* berücksichtigt.

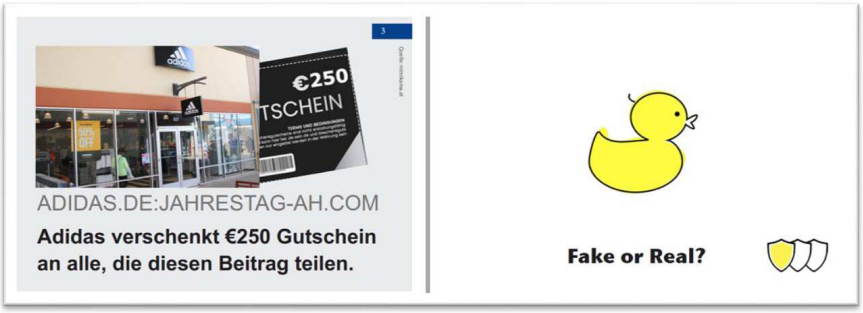


Abbildung 42: LS Fake or real?

Die zu sortierenden Karten wurden nach Schwierigkeitsgraden erstellt und mit einer entsprechenden Markierung versehen (s. Abbildung 42).

Bei *Fake or real?* ist die Aufwärmphase von großer Bedeutung, denn dort fassen die Teilnehmenden ihr Wissen über Fake News zusammen und bekommen neuen Input von der moderierenden Person. Diese moderierende Person trägt die Begriffsdefinition und grundlegende Merkmale vor. Nach der ersten Runde, in der die Karten auf Zeit als wahr oder falsch kategorisiert werden müssen, werden spezifischere Merkmale und Erkennungsstrategien anhand von „Goldenen Regeln" besprochen, die in der zweiten Runde dem Überdenken der getroffenen Entscheidungen dienen. Dies bildet die Grundlage für rege Diskussionsrunden und Austausche, die wiederum für das Thema sensibilisieren.

5.7 Security Duell – Informationssicherheit im Unternehmen

Zum ersten Kennenlernen eines Unternehmensaufbaus in Verbindung mit dem Einsatz von IT-Sicherheitsmaßnahmen wurde das Lernszenario *Security Duell – Informationssicherheit im Unternehmen* entwickelt. Schülerinnen und Schüler lernen hierbei Sicherheitsmaßnahmen kennen, die Organisationen zum Schutz ihrer sensiblen Informationen und ihrer IT-Infrastruktur einsetzen können. Die drei Schwierigkeitsgrade unterscheiden sich bezüglich der Häufigkeit, unbekannte Begriffe in einem extra entwickelten Nachschlagewerk (Wiki) nachschlagen zu dürfen. Nach Testungen wurde deutlich, dass *Security Duell* besonders für die Klassenstufen 8 bis 11 relevant ist.

Auf dem Spielfeld (s. Abbildung 43) sind verschiedene Bereiche eines Unternehmens abgebildet, die vor Angreifenden geschützt werden müssen. Im gegenseitigen Wechsel erfolgen

Angriffe und darauffolgende Verteidigungsaktionen von zwei Teams. Die Aufgabe des Verteidigungsteams ist es, die unterschiedlichen Unternehmensbereiche (z.B. Kundendatenbank, Netzwerk, Personalabteilung) so gut wie möglich mit angepassten Schutzmaßnahmen (z.B. Social Engineering-/ Informationssicherheitsbeauftragter-Schulung) vor den Angreifern zu schützen. Das Angreifer-Team hat die Aufgabe, Schwachstellen in den Unternehmensbereichen zu finden und an sensible Daten zu gelangen.
Im Laufe der Entwicklung und Testphase wurde die Komplexität des Szenarios reduziert, um die Spielmechanik intuitiver zu gestalten und den Rahmen eines Schulunterrichtes nicht zu sprengen.

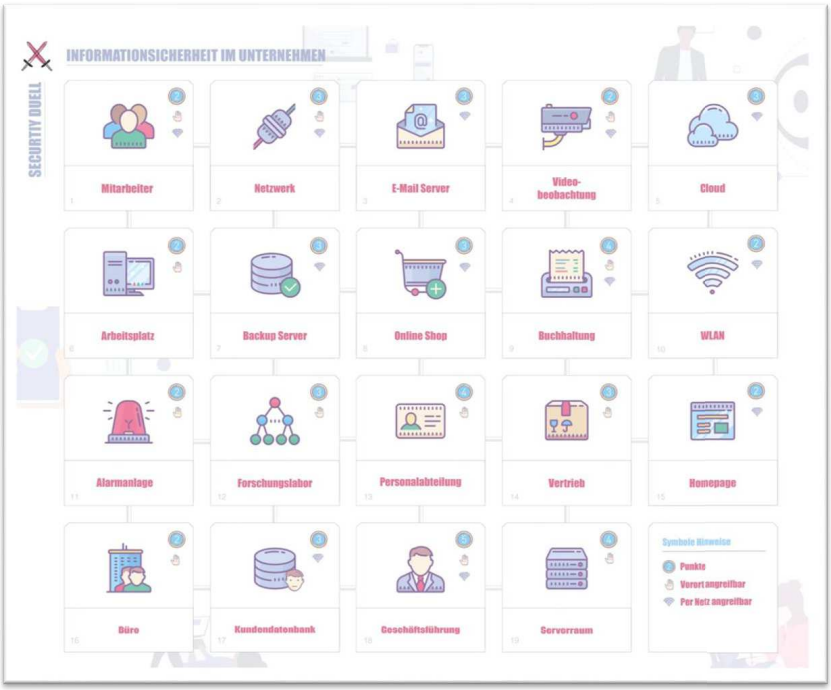


Abbildung 43: LS Security Duell – Informationssicherheit im Unternehmen

5.8 Fake News. Mit Fake News richtig umgehen

Für den bewussten Umgang mit Fake News, der in den Auftaktveranstaltungen als wichtiges Thema benannt wurde, war zu Beginn unklar, wie mehr als eine bloße Wiederholung der

ohnehin schon reichlich vorhandenen Tipps im Internet erreicht werden könnte. Deshalb wurde für den Einstieg eine kleine Fallliste gewählt, die in der Auseinandersetzung mit dem Thema Begrifflichkeiten, Werkzeuge für den Faktencheck sowie bestimmte Verhaltensstrategien einbezieht. Dieses Lernszenario ist auch als eine Erweiterung und Vertiefung für das *Fake or real?*-Lernszenario zu betrachten, erfordert aber keine erweiterten Kenntnisse.

Entstanden ist ein Kartenspiel, das die oben genannten Kategorien verwendet und die Diskussion im Spiel anregt. In der Abbildung 44 ist ein Prototyp zu sehen, in Abbildung 45 die Endversion.

Abbildung 44: LS Fake News: Mit Fake News richtig umgehen - Prototyp

Die Idee der Spielmechanik basiert auf der Problematik, die wahren Nachrichten von Fakes zu unterscheiden. Dabei wurde an der Idee gearbeitet, einen bestimmten Fall durch Strategie und Werkzeuge richtig bewerten zu können.

Ein intensives Testen der Spielemechanik und der Wirkung der Inhalte konnte aufgrund der COVID-19 Pandemie nicht mehr erfolgen. Testrunden haben aber aufgedeckt, dass viele Begriffe, Fallbeispiele und die genannten Werkzeuge unbekannt sind. Deshalb wurde ergänzend zum Lernszenario ein „Wiki“ in zwei Varianten für unterschiedliche Schwierigkeitsgrade entwickelt. Dabei war die Überlegung einen analogen Katalog als Quelle zu geben, in dem die realen Nachrichten (in verkürzter Form) aufgeführt sind, die mit denen auf den Karten abzugleichen sind. Dabei lernen Schülerinnen und Schüler der Quelle nachzugehen und auf ihre Richtigkeit im „Wiki“ zu prüfen.

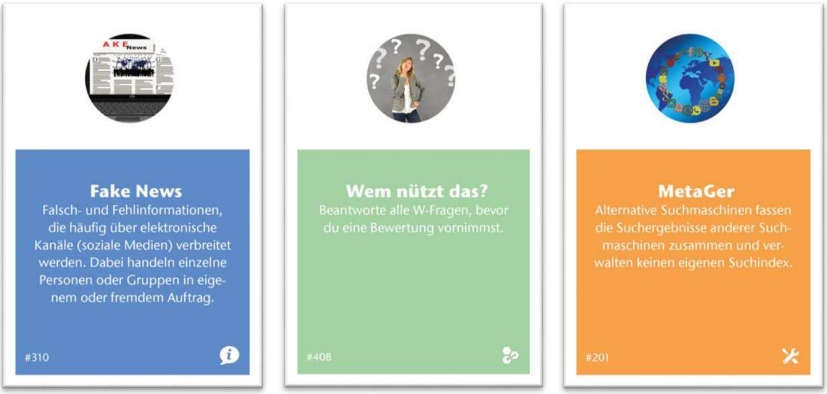


Abbildung 45: LS Fake News: Mit Fake News richtig umgehen - finale Version

Um gezielt unterschiedliche Altersgruppen anzusprechen, unterscheiden sich beide Versionen im Umfang und in der Wortwahl. Beide Wikis stehen auch als Online-Version auf der Projektseite bereit. Die zum Spiel mitgelieferte papiergebundene Wiki-Version soll verhindern, dass der Spielfluss durch eine Onlinesuche unterbrochen wird. Alternativ können, eine optimale Web-Anbindung vorausgesetzt, die Wiki-Einträge über die Projektwebsite z.B. mit einem Beamer projiziert werden. Sollten die Informationen nicht ausreichen, besteht die Möglichkeit, über die weiterführenden Links und Quellenangaben das Thema weiter zu vertiefen. Für den Spielverlauf wären die oft ausführlichen Web-Artikel zu umfangreich. Die gekürzten Wiki-Artikel sollten für den normalen Spielverlauf hinreichend Informationen zur Verfügung stellen.

5.9 Datenspionage – Sicherer Raum (digital)

Die Idee des Lernszenarios *Datenspionage – Sicherer Raum* wurde aus dem vorangegangenen Projekt SecAware4job abgeleitet, welches wiederum aus der *Security-Arena* ins Deutsche übersetzt wurde. In einem früheren Drittmittelprojekt IT-Sicherheit@KMU wurde gemeinsam mit dem Partner known_sense die *Security-Arena* – eine Linie Extender des „SECURITY PARCOURS“ von T-Systems – mit analogen Lernszenario-Stationen entwickelt.
In diesem Lernszenario soll ein Raum so sicher wie möglich verlassen werden. Die wichtigsten Gegenstände sollen für den Fall eines unbefugten Eindringens, einer Datenspionage, vor Mitnahme oder Einsicht geschützt werden. Dafür müssen sämtliche Objekte mit möglichen sensiblen Informationen in kurzer Zeit erkannt, gefunden und sicher aufbewahrt werden.

Die Umgebung der Räumlichkeit wurde visuell als eine Mischung zwischen einem Büroarbeitsplatz und einem häuslichen Arbeitszimmer gestaltet (s. Abbildung 46). Diese Variante wurde gewählt, um Schülerinnen und Schülern einerseits einen vertrauten und anderseits auf die Zukunft vorbereitenden Einblick zu gewähren und für den sicheren Umgang mit sensiblen Informationen am Arbeitsplatz zu trainieren und sensibilisieren. *Datenspionage – Sicherer Raum* ist in drei Schwierigkeitsgraden entwickelt worden, die sich im Zeitlimit unterscheiden.

Die Spielmechanik besteht darin, dass unterschiedliche Objekte im Arbeitszimmer oder im Büro an gewöhnlichen Plätzen verteilt sind. Abhängig vom Schwierigkeitsgrad des Lernszenarios müssen die Teilnehmenden in kürzester Zeit relevante Objekte finden und sich für deren korrekte Verwahrung entscheiden. Alle relevanten Objekte sind mit einer Info-Box verknüpft. Die Info-Box gibt den Zugang zum aktuellen Status des Objektes und wird für die Auswahl einer Aktion für das jeweilige Objekt genutzt (s. Abbildung 47). Dieses Lernszenario ist unter der URL https://szenarien.wildau.biz/secroom/story.html zu finden.

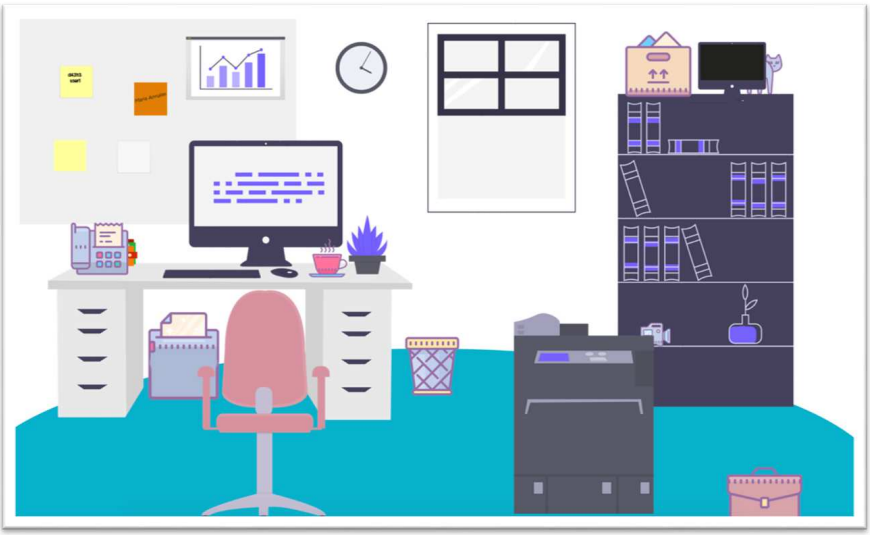


Abbildung 46: LS Datenspionage - Sicherer Raum digital

Jedem ausgewählten Objekt sind individuell wählbare Aktionen zugeschrieben. Dabei hat jede Aktion verschiedene Gewichtpunkte. Objekte, wie der Zettel an der Pinnwand, haben ihren

individuellen Ausgangszustand („Angehängt an der Pinnwand“). In diesem Fall wählbare und nach Punkten gewichtete Aktionen sind: 1) *In den Papierkorb werfen – minus 2 Punkte;* 2) *Schreddern – plus 2 Punkte;* 3) *In der Schublade verstecken – plus 1 Punkt;* 4) *Nichts tun – minus 1 Punkt*.

Die unterschiedliche Gewichtung der Aktionsmöglichkeiten ist den Teilnehmenden nicht ersichtlich, um nicht die korrekte Lösung preiszugeben. Nach Ablauf der Zeit oder Beendigung des Spiels erhält der Teilnehmende eine Übersicht der Wertung seiner Aktionen. Die nicht gefunden Objekte werden am Spielende nicht aufgezählt, um das Lernszenario wiederholen zu können und bessere Ergebnisse zu erreichen. Die Tests in den Schulen haben ähnliche Resonanz gezeigt wie beim Lernszenario *Bildrechte*: Die Schülerinnen und Schüler waren sofort gewillt, das Lernszenario erneut zu spielen, um alle Objekte in der vorgegebenen Zeit zu erkennen und die richtige Aktion auszuwählen.

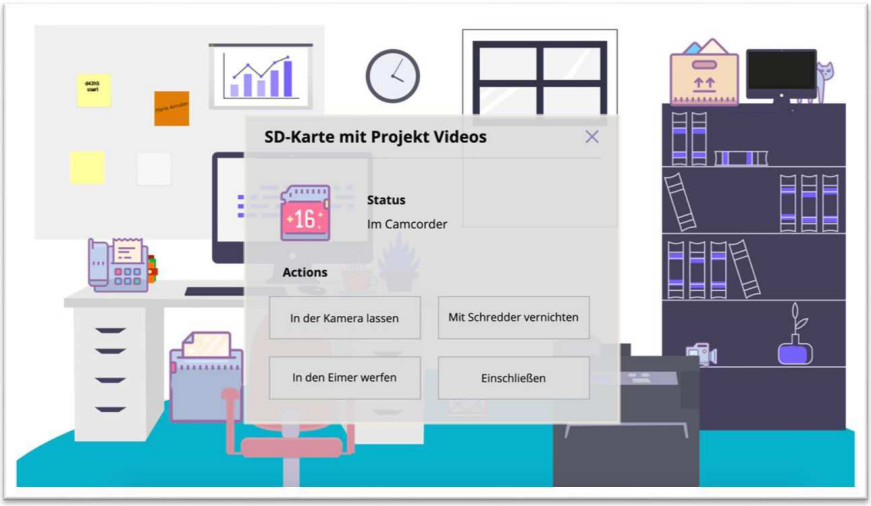


Abbildung 47: LS Datenspionage - Sicherer Raum digital. Info-Box

5.10 Bildrechte (digital)

Um für das wichtige Thema der *Rechte an Bildern* zu sensibilisieren, wurde ein digitales Lernszenario entwickelt und als Quiz konzipiert, dessen Fragen nach unterschiedlichen Schwierigkeitsgraden gruppiert wurden. Im ersten Teil werden Fragen beginnend mit der

Aufnahme bis hin zur Bildnutzung gestellt, wobei die Antworten in der einfachsten Form mit *Ja* bzw. *Nein* zu geben sind. Im zweiten Fragenkomplex geht es um eine genaue Bewertung, die aus drei Auswahlkriterien eine korrekte Zuordnung fordert. Der dritte Teil richtet sich an die höheren Klassenstufen und verlangt einen Zugang zum Netz, um die in den Fragen genannten Urteile bzw. die Rechtslage online prüfen und nachschlagen zu können. Abbildung 48 zeigt die Oberfläche des Spiels.

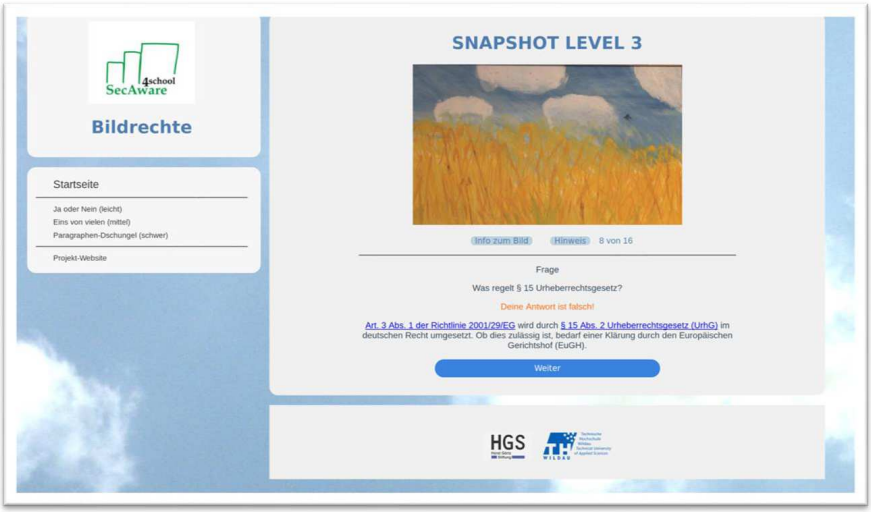


Abbildung 48: LS Bildrechte digital

Für die Überprüfung der Fragen wurden Einzeltests als auch die Abarbeitung in kleinen Gruppen mit drei bis vier Schülerinnen und Schülern durchgeführt. Sehr schnell haben die Tests kleine logische Fehler und Verständnisfragen sichtbar gemacht, die für die Endfassung weitestgehend ausgeräumt wurden. Damit schließt sich, ausgehend von der Informationsveranstaltung, über die im Abschnitt 4.2. berichtet wurde, und dem Rechtsstreit um das Selfie des Makaken „*Naruto*“, der Kreis mit einem Quiz, welches viele Aspekte der Bildrechte berührt.

Auch wenn die schwierigste Stufe sich an die älteren Schülerinnen und Schüler wendet, haben die Jüngeren es nicht versäumt, diesen Teil ebenfalls zu beantworten. Ohne die Auseinandersetzung mit der Gesetzeslage wurde dann eher geraten. Nach kurzer Zeit konnte im Test beobachtet werden, dass Begriffe wie *Bildrecht*, *Recht am eigenen Bild*, *Hausrecht* oder *Privatsphäre* klar zu unterscheiden sind und die Teilnehmenden diese Differenzierung bewusst

anwendeten. Wenn es die Zeit erlaubte, haben einige Schülerinnen und Schüler den Test wiederholt, um im zweiten Versuch eine höhere Punktzahl zu erreichen.
Dieses Lernszenario steht unter der URL https://szenarien.wildau.biz/bildrechte zur direkten Verwendung bereit.

5.11 Hacker Terminal (digital)

Um wichtige Begriffe der Informationssicherheit und deren Bedeutung zu verstehen, wurde das digitale Lernszenario *Hacker Terminal* entwickelt. Dieses Lernszenario ist als eine Ergänzung zum analogen Lernszenario *Schnelles Begrifferaten – Informationssicherheit* anzusehen und eignet sich gut sowohl für das selbstständige Lernen als auch im Team.
Das Ziel ist es, verschlüsselte Kennwörter in Form von Anagrammen mit Hilfe von Hinweisen zu erraten, um in ein System zu gelangen. Visuell wurde eine Oberfläche im Retro-Design (s. Abbildung 49) geschaffen, die den Teilnehmenden erlaubt, sich in die Rolle des Hackers zu versetzen.

Abbildung 49: LS Hacker Terminal digital

5.12 Sketch – Secure Passwords (digital)

Die Praxis in den Schulen hat gezeigt, dass in der Einführung der Awareness Trainings Schülerinnen und Schüler das Lernszenario *Password hacking* am meisten begeistert hat. Dieses Lernszenario wurde im vorhergehenden Projekt „Security - Gendersensible Studien- und Berufsorientierung für den Beruf Security Spezialistin“ entwickelt. Da sich das Thema der Passwortsicherheit in der Umfrage als eines der ausschlaggebendsten herausstellte, wurde ein praxisorientierter Sketch zur Passwortsicherheit entwickelt, um die Teilnehmenden für die sichere Aufbewahrung der Passwörter zu sensibilisieren. In der Rolle als Frau Hackermann müssen sich die Teilnehmenden für eine von vier Optionen (s. Abbildung 50) entscheiden, wie sie ein wichtiges Passwort aufbewahren.

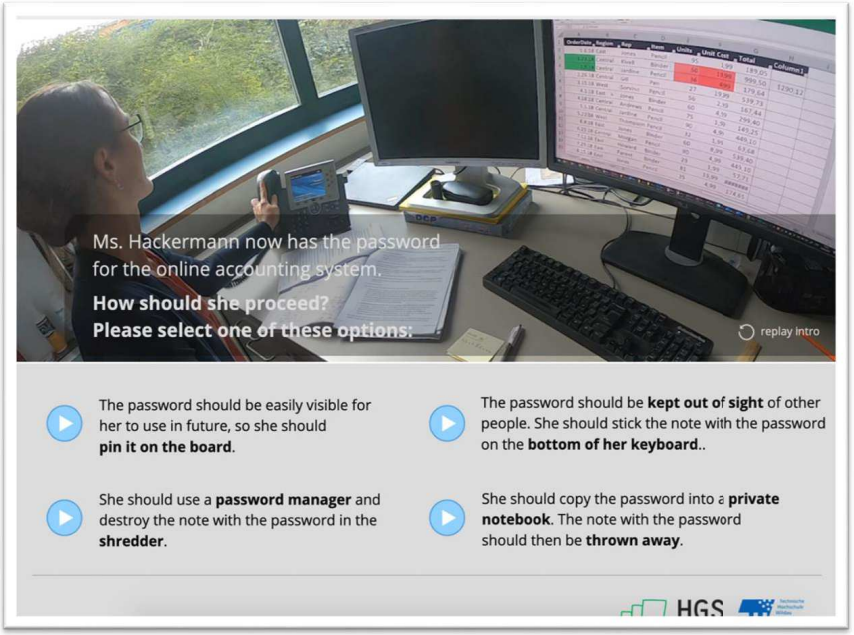


Abbildung 50: LS Password Sketch digital

Im Falle einer falschen Entscheidung wird den Teilnehmenden sogleich auf humorvolle, aber dennoch realistische Weise die Konsequenz von nachlässigem Umgang mit Passwörtern aufgezeigt. Dieses Lernszenario wurde in englischer Sprache entwickelt, um der

Internationalität in den Schulen gerecht zu werden und auch z.B. im Englischunterricht angewendet zu werden.
Dieses Lernszenario steht zur direkten Verwendung unter der URL https://szenarien.wildau.biz/security_sketch_passwords_eng/story_html5.html bereit.

6 Informationssicherheit als Unterrichtsfach

In dem Projekt SecAware4school haben wir die Schülerinnen und Schüler in die Weiterentwicklung der Spiele eingebunden (siehe Awareness Training und Kreativworkshops), die zu diesem Zeitpunkt noch als Prototyp vorgestellt wurden. Das Feedback hat gezeigt, dass bei den Jugendlichen ein großes Interesse geweckt wurde, ein eigenes Spiel zu entwickeln. So haben sich in einer der fünf Partnerschulen, dem Friedrich-Wilhelm-Gymnasium, 12 Schüler aus einer Vielzahl von möglichen Projekten für die Entwicklung eines eigenen digitalen Prototyps entschieden. Die in der Planungsphase präsentierten Ideen zeigen deutlich den Zuwachs an Wissen zum vorgegebenen Thema des Sicherheitsbewusstseins.
Wenn der Wandel vom klassischen Frontalunterricht hin zu Workshop-zentrierter Wissensvermittlung eine Alternative darstellt, so hat unser Projekt den pädagogischen Nutzen des Letztgenannten klar bestätigt. Nicht zu unterschätzen ist der erhöhte Aufwand, wenn Technik und Technologien eingesetzt werden sollen, die noch nicht im Lehrplan involviert sind. Hier ist nicht nur das Engagement der Schülerinnen und Schüler gefragt, sich eigeninitiativ neues Wissen anzueignen, sondern auch das der Lehrkräfte.

6.1 Vorbereitung

Am Friedrich-Wilhelm-Gymnasium Königs Wusterhausen wurde das Thema *Informationssicherheit* erfolgreich im Informatikkurs aufgenommen. Die interessierten Schülerinnen und Schüler haben, angeregt durch einen von der Forschungsgruppe zusätzlich angebotenen Workshop, eigene Ideen entwickelt. Diese sollten im nachfolgenden Schritt zu einem digitalen Prototyp weiterentwickelt werden. Die Empfehlung, die Programmiersprache *Python* und die Bibliothek *PyGame* zu verwenden, wurde weitestgehend angenommen, obwohl Python im Unterricht nicht als Lehrsprache verwendet wird. Als leicht zu erlernende Sprache ist sie dennoch für den schnellen Einstieg und den Informatikunterricht gut geeignet. Das gilt

nur bedingt für die Spieleentwicklung mit der Bibliothek *PyGame*, da hier alle Aspekte der objektorientierten Programmierung zur Anwendung kommen.

6.2 Durchführung

Im ersten Schritt wurde eine Kombination aus Awareness Training und Kreativworkshop für die Ideenfindung durchgeführt. Die eigenständige Weiterentwicklung der Ideen mündete in einer Präsentation, die am 04.03.2020 als Zwischenpräsentation an der TH Wildau stattfand. Hierfür sollte jede Gruppe eine Präsentationsmethode wählen (z.B. Plakat, PowerPoint, Video etc.) und ihre Ideen zu den Lernszenarien vorstellen, inklusive einer Beschreibung der Vorgehensweise und der dabei entwickelten Ideen. Die Funktionsweise sollte allgemeinverständlich sichtbar werden. Die Präsentationen enthielten den Arbeitstitel des Spiels, den Aufbau der Präsentation, die Spielidee, den aktuellen Stand, einen Ausblick sowie die Anteile der jeweiligen Teammitglieder. Ihre Länge sollte zwischen 5 und 10 Minuten betragen. Im Anschluss unterstützte das Team von SecAware4school alle Schülerinnen und Schüler durch Hinweise und Anregungen bei der Weiterentwicklung eines ersten Prototyps.
Die gezeigten Entwürfe, Ideen und die Präsentationen waren von guter bis sehr guter Qualität. Die geforderten Bedingungen wurden erfüllt und bildeten die Voraussetzung für die programmiertechnische Umsetzung der Ideen. Die erste Veranstaltung wurde genutzt, um grundlegende Kenntnisse der Programmiersprache *Python* zu vermitteln, weil diese Sprache für den regulären Informatikunterricht nicht verwendet wird.

6.3 Ergebnisse und Erkenntnisse

Für eine volle Unterstützung der Schülerinnen und Schüler war die Verwendung der Versionsverwaltungssoftware Git geplant. Eine Anleitung zur Software und der gleichzeitige Test am Gymnasium haben aber gezeigt, dass die restriktiven Netzwerkregeln eine Arbeit mit diesem Tool nicht wie geplant oder nur lokal ermöglichen. Die Nutzung der im Land Brandenburg angebotenen Schul-Cloud hat sich für die Entwicklung von Software als nicht geeignet erwiesen, weil es sich um ein Dateiablagesystem handelt, welches den Lehrerinnen und Lehrern lediglich den Austausch über Daten, Termine und Dateien mit Schülerinnen und Schülern ermöglicht. Ein Einsatz als Entwickler-Werkzeug für die Softwareentwicklung, wie es durch *Github* bzw. *Gitlab* angeboten wird, ist nicht möglich.

Die beiden genannten Zielstellungen, Dateiaustausch und Kommunikation auf der einen und Fähigkeiten und Fertigkeiten der Softwareentwicklung auf der anderen Seite, sollten Anlass für weitere Untersuchungen sein. Es gilt die Frage zu beantworten, inwieweit durch die Verwendung von *Git-Repositories* im Vergleich zu einer klassischen Dateiablage und Verwaltung, wie sie die Schul-Cloud bietet, die digitale Kompetenz der Schüler gefördert werden.
Die technischen Hürden haben in der Corona-Krise eine effektive Unterstützung verhindert. Eine Weiterentwicklung der in der ersten Präsentation gezeigten Ideen wird im laufenden Schuljahr weiterverfolgt (siehe auch den Plan zur Entwicklung in der Anlage zu Kapitel 6).

6.4 Erfahrungsberichte zum SecAware4school-Projekt und zur Informationssicherheitsbeauftragten Ausbildung (IT-SiBe)

Ein Flyer zur Ausbildung zum Informationssicherheitsbeauftragten ist im Anhang zum Kapitel 6 zu finden. In der Abbildung 50 sind die Lehrende zu sehen, die erfolgreich die IT-SiBe Prüfung absolviert haben.

Dr. Stephan Hell, Friedrich-Wilhelm-Gymnasium Königs Wusterhausen:

> *In der ersten Hälfte des Jahres 2018 erhielt unsere Schule die Einladung, am Projekt teilzunehmen. Zuerst wurden ausgewählte Klassen im Unterricht durch die Arbeitsgruppe um Prof. Scholl in typische Fragenstellungen der Informationssicherheit eingeführt. Anschließend fuhr eine kleine Gruppe Schüler*innen zu einem Kreativworkshop an die TH Wildau. Hierbei erhielten wir zusammen mit Schüler*innen anderer Schulen einen ersten Einblick in die Herangehensweise und Methoden der Entwicklung einer Spielidee zum Thema Informationssicherheit. Es war für alle eine erfrischende Erfahrung in einer sehr stimulierenden Atmosphäre.*
> *Ausgehend von diesen ersten Erfahrungen entschieden wir uns, das Informatikangebot unserer Schule für die Jahrgangsstufe 11 ab dem Schuljahr 2019/20 in Form eines an das Projekt angelehnten Seminarkurses zu erweitern. Dieser Kurs bestand unter der Leitung von Dr. Hell aus 13 Teilnehmer*innen. Sie wurden in mehreren Workshops durch unseren externen Partner weiter in die Techniken der Spieleentwicklung eingeführt. Im März 2020 kam es zu einer Präsentation der Spielideen durch die einzelnen Teams und einer anschließenden Feedbackrunde an der TH Wildau. Für den August 2020 ist geplant, dass 6 Schüler*innen des Kurses die ECDL-Prüfung IT-Sicherheit ablegen. Alle Teams werden ihre Spielidee bis zum Herbst 2020 weiter realisieren und im Anschluss präsentieren. Der Einsatz dieser Spiele zur Sensibilisierung unserer Schülerschaft in Fragen der Informationssicherheit ist in Planung.*
> *Abschließend möchten wir uns herzlich für die fruchtvolle Zusammenarbeit und neuen Impulse durch die gesamte Arbeitsgruppe bedanken, ganz besonderer Dank an Herrn Koppatz und Frau Schuktomow für ihr Engagement. Die Zusammenarbeit mit unserem externen Partner, der TH Wildau, ermöglicht unseren Schüler*innen neue Einblicke in Studienmöglichkeiten und Thematiken, die wir als Schule in dieser Form nicht leisten können.*

Die Herangehensweise des gesamten Projekts bietet weitergehende Vorzüge, wie die Förderung der Kommunikations- und Kooperationsfähigkeit, die Verknüpfung mit realen Problemen aus dem Leben der Schüler/innen und Reduzierung der Komplexität der Inhalte von anspruchsvollen zu erlebbaren Lerninhalten.

Alexander Dietz, Humboldt-Gymnasium Berlin:

Im Februar und März 2019 fanden in zahlreichen 6., 8., 9. und 10. Klassen Praxisprojekte zum Thema Informationssicherheit statt, die von einem Forschungsteam der TH Wildau vorbereitet und durchgeführt wurden.

Um das abstrakte Thema Informationssicherheit den Schülerinnen und Schülern leicht verständlich und greifbar zu vermitteln, kamen in einem zweistündigen Workshop viele kreative, spielbasierte Lehr- und Lernmethoden an folgenden Stationen zum Einsatz:

- *Password Hacking – Sichere Passwörter*
- *Apps und Risiken – Sichere Smartphone Bedienung*
- *Verschlüsselung und digitale Signatur*
- *Phishing*
- *Bildrechte*
- *Sicher unterwegs auf Klassenfahrten*

Dabei stand die Aneignung des sorgsamen Umgangs mit personenbezogenen Daten bei der Nutzung von Internetdiensten und sozialen Netzwerken im Vordergrund.
Die teilnehmenden Schülerinnen und Schüler empfanden die Lernstationen als sehr motivierend und lehrreich. Die Themen und Inhalte wurden als relevant beurteilt. Es zeigte sich, dass die Vorkenntnisse sehr unterschiedlich waren und die Inhalte im Unterrichtsalltag bisher kaum thematisiert werden.

In einer weiteren Projektphase nahmen ausgewählte Schülerinnen und Schüler an einem Kreativworkshop mit dem Projektteam sowie Schülerinnen und Schüler anderer Projektschulen auf dem Campus der TH Wildau teil. Ziel dieses Workshops war die Entwicklung eines kleinen spielbasierten Lernszenarios für Informationssicherheit für Mitschülerinnen und Mitschüler. Darüber hinaus können interessierte Schülerinnen und Schüler an den ECDL-Prüfungen (Europäischer Computerführerschein) im Modul IT-Sicherheit teilnehmen.

Carsten Hoherz, Rudolf-Virchow-Oberschule Berlin:

Das heutige Arbeitsleben ist digital. Daher ist es ein zentrales Ziel der schulischen Ausbildung, die Schülerinnen und Schüler auf einen digitalen Berufsalltag vorzubereiten. Sicherheitsaspekte sind dabei ein Kernthema und seit Inkrafttreten der DSGVO in aller Munde. Doch schon bald darauf nahm die Aufmerksamkeit für das Thema wieder ab und ist z.T. aus den Köpfen verschwunden. Folglich ist Security-Awareness, also der ständige wache Umgang mit Sicherheit, ein starker Ansatz, um die Heranwachsenden auf zukünftige Herausforderungen und Gefahren der digitalen Welt vorzubereiten. Hier setzt das Projekt SecAware4school an, welches mit einer Vielzahl von spielerisch umgesetzten Lernaufgaben Menschen aller Altersgruppen und insbesondere Schülerinnen und Schüler auf kritische Stellen im Umgang mit sowohl persönlichen als auch betriebszugehörigen Daten aufzeigt.
Die Fokussierung auf die Security-Awareness mit lebensnahen Beispielen bringt die Schülerinnen und Schüler deutlich wirksamer mit dem Thema Security in Kontakt, als es in den vorangegangenen Jahren im Informatikunterricht geschehen ist. Daher sind die Arbeitsergebnisse nicht nur eine andere Ausprägung, sondern eine echte Ergänzung des

Themas in der Schule. Neben den Schülerinnen und Schülern wurden in dem Projekt SecAware4school zusätzlichen Lehrkräften die Ausbildung zum IT-Sicherheitsbeauftragten ermöglicht. Auch wenn Deutschland gegenüber anderen Ländern noch einiges in Sachen Digitalisierung aufzuholen hat, so hat insbesondere auch die herausfordernde Corona-Zeit gezeigt, dass sich in Deutschland hinsichtlich des Themas des digitalen Unterrichts einiges tun wird. Es ist daher klar, dass bei all diesen Unternehmungen Sicherheitsaspekte ständig mitschwingen. Umso dankbarer sind die teilnehmenden Lehrkräfte, da sie durch die umfassende Schulung zum IT-Sicherheitsbeauftragten nun innerhalb der Schulen kompetent mitwirken können. So müssen Hard- und Softwarelösungen für digitalen Unterricht gefunden werden und gleichzeitig der Datenschutz im Auge behalten werden.
Um dabei nicht nur technisch zuverlässig, sondern auch rechtlich formal vorgehen zu können, haben die Teilnehmer innerhalb der Schulung Tools zur Planung und zum Management des Sicherheitssystems Schule kennengelernt. Dabei wurde schnell klar, dass Sicherheit im Hintergrund eine sehr komplexe Aufgabe ist, die ohne geeignetes Tool nur sehr schwer zu bewältigen ist. Es wird einige Zeit dauern, bis alle Aspekte in unserer Schule umgesetzt werden, aber dank der Ausbildung im Rahmen des Projekts ist nun ein Weg aufgezeigt.
Insgesamt freut sich die Rudolf-Virchow-Oberschule darüber, an dem Projekt als Partnerschule teilgenommen zu haben, und steht gern der weiteren Entwicklung von sicherheitsfördernden Lernmaterialien offen gegenüber. Vielen Dank an Frau Professorin Scholl und ihr Team!

Abbildung 51: Lehrer-Kurs IT-SiBe Wintersemester 2019/2020. SecAware4school.

Doris Gerstenberger, Rudolf-Virchow-Oberschule Berlin:

Projekt SecAware4school (gefördert durch die HGS), Ausbildung zur/m Informations-sicherheitsbeauftragten

*SecAware4school – im Herbst 2017 fragen sich Lehrer*innen und Schüler*innen der Rudolf-Virchow-Oberschule was ist das? Security awareness for school – ein Bewusstsein für Sicherheit in Schule (schaffen)? Spielerisch setzten sich Klassen und Projektgruppen mit Fragen zur Daten- und Informationssicherheit auseinander und testen an der TH-Wildau entwickelte Spiele, die ein Gefühl für Sicherheit im Netz schaffen. Den Schüler*innen gefällt sofort ihr Wissensvorsprung auf diesem Gebiet. Ihr Expertenwissen in Sachen soziale Netzwerke können sie dann auch gleich bei der Entwicklung neuer Spiele zum Thema gemeinsam mit Schüler*innen aus anderen Schulen einsetzen. Ein Spiel zu*

*Fake News und deren Gefahren ist ihr erster Gedanke. Und, da sich Eltern und Lehrer fast sofort ebenfalls eine Fortbildung wünschen, entstehen einige Projekte, in denen einzelne Schüler*innen ihr Wissen weitergeben. Auf einem Studientag im November 2019 werden unterschiedliche Workshops zu digitalen Medien angeboten – auch dafür gab das Projekt SecAware4school einen Anstoß. An der Rudolf-Virchow-Oberschule machen wir seit 2002/2003 kontinuierlich die digitale Entwicklung mit (einschließlich einiger Irrwege und viel persönlichem Engagement des pädagogischen Personals, der Eltern und Schüler). Mit der zunehmenden Professionalisierung der Medienbildung an Schulen und dem durchgängigen Einsatz informationsverarbeitender Technologien in Schulorganisation und Unterricht ist ein systematisches Herangehen an Informationssicherheit und Informationsmanagement dringend notwendig geworden. Genau an dieser Stelle ist die Ausbildung zum Informationssicherheitsbeauftragten, begleitend zum Schülerprojekt, für mich sehr spannend gewesen. Sie hat nicht nur ein systematisches und systemisches Herangehen unterstützt, sondern es auch ermöglicht, über den Tellerrand zu schauen und damit die Bewertung eigener Wahrnehmungen zu reflektieren. Durch die gemischte Seminargruppe sind völlig unterschiedliche Sichtweisen deutlich geworden. Für Lehrer sicherlich spannend, um sich der zukünftigen Bedeutung der Informationssicherheit für unsere Schüler*innen im beruflichen Umfeld bewusst zu werden. Meine persönlichen Erwartungen, die Systematisierung und Vertiefung meines Wissens auf dem Gebiet ICT und Informationsmanagement haben sich absolut erfüllt. Ich kann vieles technisch detaillierter einordnen und klarer benennen und damit auch präziser bei Fragen zur Informationssicherheit argumentieren. Mit dem Konzept des Informationssicherheitsmanagements habe ich zudem eine Struktur, die es möglich macht, die in den letzten 15 Jahren immer wieder entstandenen Baustellen in Schulen zu systematisieren und in ihrer Bedeutsamkeit einzuschätzen – eine gute Argumentationsgrundlage für weitere Entwicklungen im Kontext von Medienkonzepten und Medienbildung. In meine Wunschwolke würde ich schreiben: Erfahrungen und Wissen aus den Schülerprojekten nicht versanden lassen, ein gesundes Gefühl für Transparenz, Vertrauen und Sicherheit im schulischen Kontext.*

Rolf Schollbach, Staatliche Gesamtschule Königs Wusterhausen:

Meinung zum Fortbildungslehrgang zum IT-Sicherheitsbeauftragten

Von der TH Wildau wurde die Möglichkeit gegeben, an einem Lehrgang zum IT-SiBe teilzunehmen. Interessant waren für mich die vielen verschiedenen Aspekte, über die ein IT-SiBe Bescheid wissen muss. Mich haben besonders die technischen Fragen interessiert, wie der Aufbau eines sicheren Netzwerks, Datensicherungskonzepte, Bedrohungsszenarien usw..
Überrascht hat mich die Aufgabenfülle eines IT-SiBe bezüglich der administrativen Erfordernisse eines Sicherheitskonzepts nach den BSI-Standards. Diesen Teil empfand ich als relativ schwierig, da ich beruflich mit diesen Dingen bisher nie in Berührung gekommen war. Trotzdem haben uns Frau Prof. Scholl und Herr Ehrlich durch zielgerichtete Fortbildungsinhalte und die angenehme Kursatmosphäre perfekt auf die Prüfung vorbereitet, so dass alle Kursteilnehmer bestanden haben.

Was nehme ich für meine berufliche Tätigkeit aus dieser Fortbildungsreihe mit?

Aus meiner täglichen Arbeit sowohl mit Schülerinnen und Schülern als auch mit Lehrenden weiß ich, dass das Thema IT-Sicherheit aus Bequemlichkeit oder Nichtwissen oft vernachlässigt wird. An dieser Stelle kann ich meine erworbenen Kenntnisse einbringen, um für die Thematik zu sensibilisieren und Verfahren und Lösungswege anzubieten. Die am Ende des Kurses erstellte Belegarbeit „Sensibilisierungskonzept zum Thema E-Mail-Sicherheit“ war dazu ein erster Schritt. Auch sonst werde ich alle zu vermittelnden Inhalte

in meinen eigenen Fortbildungen verstärkt unter dem Aspekt der IT-Sicherheit betrachten. Außerdem habe ich mein privates IT-Nutzungsverhalten nach der Fortbildung verändert. Bewusster Umgang mit Bluetooth und Geotracking gehören inzwischen genauso dazu wie regelmäßige Backups oder Passwort-Manager.

Eyk Kelle, Friedrich-Schiller-Gymnasium Königs Wusterhausen:

Bericht zur Ausbildung zur/m Informationssicherheitsbeauftragten
Im Januar 2020 habe ich die Ausbildung als Informationssicherheitsbeauftragter an der TH Wildau unter der Leitung von Frau Prof. Scholl abgeschlossen. Diese Ausbildung begann ich, da ich als Informatiklehrer, Datenschutzbeauftragter und Fachbereichsleiter für das Fach Informatik am Friedrich-Schiller-Gymnasium Königs Wusterhausen immer häufiger mit dem Thema Datenschutz konfrontiert wurde. Die Ausbildung ist fachlich verständlich und mit multiperspektivischen Methoden aufgebaut. Gerade die vielen Beispiele mit spielerischem Hintergrund haben mir auf eine sehr veranschaulichende und nachvollziehbare Weise die sonst eher „trockenen" Themenbereiche der IT-Sicherheit nähergebracht. Frau Prof. Scholl und Herrn Ehrlich ist es gelungen, das Thema so zu vermitteln, dass ich vom ersten Tag an über praxisnahe Präsentations-Themen nachdenken konnte und zu keinem Zeitpunkt das Gefühl der Überforderung verspürte. Der Mehrwert für meine Tätigkeit an der Schule bezieht sich darauf, mit dem erworbenen Wissen die Kollegen kleinschrittig im Umgang mit IT-Sicherheit zu sensibilisieren. Das spiegelt sich darin wider, dass ich z. B. eine Weiterbildung für alle Kollegen der Schule zum Thema Datensicherheit / IT-Sicherheit am häuslichen Arbeitsplatz anbiete. Durch die Vermittlung rechtlicher Grundlagen hat mir die Ausbildung bei der Ausarbeitung von Nutzungsvereinbarungen, schulischer IT-Arbeitsmittel für die Kollegen, Sicherheit gegeben. Die Nutzung schulischer IT-Systeme ist im Zuge einer Umsetzung des vom Bund initiierten DigitalPakts Schule 2019-2024 im Land Brandenburg, entstanden und wird für die nächsten Jahre immer bedeutender. Überaus hilfreich für die Umsetzung meiner Vorhaben an der Schule ist die Möglichkeit, auf Schulungsunterlagen im Moodle-Bereich der TH-Wildau als „Nachschlagewerk" zurückgreifen zu können.

Mein Wunsch für die Zukunft ist, dass sich die Schüler und Lehrer durch gezielte und klare Richtlinien, im Umgang mit Daten im Allgemeinen aber auch mit bestimmten IT-Systemen, ein Wissensrepertoire angeeignet haben, welches im Kern die Begrifflichkeiten der „Vertraulichkeit", „Integrität" und „Verfügbarkeit" behandelt und ihnen ein sicheres Gefühl im Umgang mit mobilen Endgeräten vermittelt.

7 Sicherheitsberaterinnen und -Beraterausbildung ICDL

Die geplante Sicherheitsberaterinnen und -beraterausbildung mit der Prüfung im Modul IT-Sicherheit des international anerkannten Computerführerscheins ICDL fand aufgrund der COVID-19-Situation und der gelegten Unterrichtszeiten in den Schulen in einem kleinerem Ausmaß als geplant statt. Trotz aller Bemühungen war es den Schulen nicht möglich gewesen, aufgrund der Auflagen zur Eindämmung der Pandemie an die TH Wildau zu kommen, um an der Vorbereitung und an der Prüfung teilnehmen zu können. Eine onlinegestützte

Vorbereitungs- und Prüfungsform wäre an einigen Schulen möglich, allerdings aus Kapazitätsgründen des Forschungsteams von Frau Prof. Scholl nicht mehr umsetzbar gewesen. Dennoch haben am 8. September 2020 6 Schülerinnen und Schüler des Friedrich-Wilhelm-Gymnasiums Königs Wusterhausen die ICDL-Prüfung im Modul IT-Sicherheit erfolgreich abgeschlossen und ein lebenslang gültiges Zertifikat erhalten (s. Abbildung 52). Die Teilnahme war möglich, da es sich um einen Seminarkurs handelt, der Informationssicherheit als Fach und Thema für zwei Jahre innerhalb des regulären Unterrichts behandelt. Das Ergebnis der Schülerinnen und Schüler ist als eine positive Tendenz zu den durchgeführten Maßnahmen in Form von Informationsveranstaltungen, Awareness Trainings und Kreativworkshops zu deuten. Die durchgeführten Maßnahmen haben die Tendenz bestätigt, dass eine nachhaltige Verinnerlichung zur Stärkung des Bewusstseins der Informationssicherheit möglich ist.

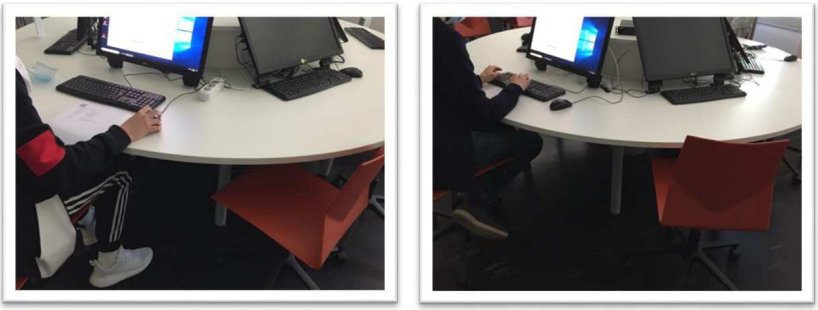


Abbildung 52: ICDL-Prüfung an der TH Wildau

8 Bekanntmachung des Projektes und der Projektergebnisse

8.1 Öffentlichkeitsarbeit

Für das Projekt wurden grafische Elemente und Informationen, wie z.B. Bildmarken und Logo entworfen, um es von anderen Projekten abzuheben. Da das Projekt SecAware4school auf der Idee des vorhergehenden Projektes beruht, wurden im Logo das „SecAware“ angeglichen (s. Abbildung 53).

Abbildung 53: Erste Logoentwürfe (links) und die finale Version (rechts)

Das Projektlogo wurde mit der Unterstützung einer externen Grafikerin entwickelt und ist mit uneingeschränkten Nutzungsrechten versehen. Als Bestandteil des Logos wurden die drei Säulen ausgewählt, die drei Schulgebäude unterschiedlicher Größe symbolisieren. Diese deuten auf die unterschiedlichen Altersgruppen genau wie auf die drei Schwierigkeitsgrade für die Zielgruppen des Projektes hin. Auf die Zugehörigkeit des Projektes zur TH Wildau und auf die Förderung des Projektes durch die Horst Görtz Stiftung wurde jeweils mit den entsprechenden Logos verwiesen (vgl. z.B. Titel der Projektdokumentation).

Für die Lernszenarien wurden Bildmarken entwickelt, die dem Thema des Lernszenarios entsprechen:

Abbildung 54: Bildmarken

Zur Bekanntmachung des Projektes wurde zu Beginn eine Webseite konzipiert und programmiert, auf der Interessierte aktuelle Informationen zu SecAware4school in Deutsch und Englisch abrufen können. Alle digitalen Lernszenarien sowie die Anleitungen zu den analogen Lernszenarien können über die Projektwebseite kostenfrei abgerufen und genutzt werden.
Neben Plakaten mit der Ausgangssituation der Problematik und den Zielen wurden auch Poster, Flyer und Broschüre entwickelt, die den Verlauf des Projektes aufzeigen und öffentlich präsentieren. Das Projekt SecAware4school wurde auch im Forschungsbericht der TH Wildau 2019 und 2020 vorgestellt. Es wurden Presseberichte erstellt, die die wichtigen Meilensteine im Projekt festhalten. Dies geschah zum Projektstart und zu den Krea-tivworkshops. Zum erfolgreichen Abschluss des Projektes wird erneut eine Berichterstattung erstellt. Eine Liste mit allen wissenschaftlichen und nicht wissenschaftlichen Publikationen ist unter Punkt 8.2. zu finden.

8.2 Wissenschaftliche Konferenzen und Publikationen

Tabelle 3: Veröffentlichungen im Zusammenhang mit dem Projekt SecAware4school

Flyer SecAware4school **2020** (im Anhang zu Kapitel 8)
Plakate SecAware4school **2018 – 2020** (im Anhang zu Kapitel 8)
Scholl, M. (Hrsg.) (2020). Broschüre. SecAware4school - Spielbasierte Sensibilisierung zum Thema Informationssicherheit im Schulunterricht. ISBN: 978-3-9819225-1-6 (im Anhang zu Kapitel 8)
Scholl, M. (2021). What competencies do we need in the digitized world? Keynote + Experimental Workshop. Eingereicht bei WMSCI 2020, Florida/USA, für Februar 2020, wegen aktueller Corona-Situation in Absprache mit dem Veranstalter auf 2021 verschoben.
Schuktomow, R., Gube, S., Scholl, M. (Hrsg.), Koppatz, P. & Edich, D. (2020). Lernszenarien – Anleitungen. Sensibilisierung von Schülerinnen und Schülern zum bewussten Umgang mit Informationssicherheit durch erlebnisorientierte Lernszenarien. ISBN: 978-3-9819225-4-7
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.
Scholl, M., & Schuktomow, R. (2020). Smart School in a Smart City: An Experience with Information Security in Schools. In *Proceedings International Journal of E-Planning Research (IJEPR)*, Lisbon, Portugal, Virtual Conference.
Scholl, M., & Schuktomow, R. (2020). Information Security Awareness from Toddler to Grandma: A Target-Group-Oriented, Gender-Specific, and Intergenerational Challenge of Interdisciplinary Interest. In IICE 2020 Dublin, Ireland Virtual Conference.
Scholl, M., & Schuktomow, R. (2020). Information Security at Schools: A Practical Game-Based Application with Sustained Impact. In Nagib CALLAOS, Elina GAILE-SARKANE, Jeremy HORNE, Belkis SANCHEZ, *Proceedings of the 24th World Multi-Conference on Systemics, Cybernetics and Informatics WMSCI 2020 (pp. 24-29)*. USA, Florida: (VOLUME 3 Post-Conference Edition – YEAR 2020) Virtual Conference.
Scholl, M., & Ehrlich, E. (2020). *Information Security Officer: Job profile, necessary qualifications, and awareness raising explained in a practical way*. Frankfurt am Main: Buchwelten Verlag.
Scholl, M., & Schuktomow, R. (2020). Information Security at Schools: A Practical Game-Based Application with Sustained Impact. In Nagib CALLAOS, Jeremy HORNE, and Michael SAVOIE, *Proceedings of the 24th World Multi-Conference on Systemics, Cybernetics and Informatics: WMSCI 2020* (pp. 13ff). Florida, USA: International Institute of Informatics and Systemics (IIIS).

Scholl, M., & Ehrlich, E. (2020). *Informationssicherheitsbeauftragte: Aufgaben, notwendige Qualifizierung und Sensibilisierung praxisnah erklärt*. Frankfurt am Main: Buchwelten Verlag.
Schuktomow, R., Scholl, M., Koppatz, P., & Edich, D. (2020). PLAY THE GAME AND BE AWARE: INFORMATION SECURITY PROJECT WITH SCHOOLS. In Katherine Blashki, Noroff University College, Norway, *14th International Conference on Interfaces and Human Computer Interaction*, Zagreb, Croatia, 59-66.
Scholl, M. (2019). SecAware4school: Information Security Awareness in Everyday School Life. In Professor Charles A. Shoniregun, *London International Conference on Education (LICE-2019)*, London, 38-40.
Scholl, M., & Schuktomow, R. (2019). Participatory Research with Schools to Develop Serious Games for Information Security Awareness. In Nagib CALLAOS, Jeremy HORNE, and Michael SAVOIE, *Invited Papers of the Plenary Keynote Speakers at WMSCI/IMCIC 2019 and their collocated events* (pp. 1-8). USA: Journal of Systemics, Cybernetics and Informatics (VOLUME 17 – NUMBER 5 – YEAR 2019).
Scholl, M. (2019). Information Security Awareness School Projects: Are they transferable to the health sector? In Maria Manuela Cruz-Cunha, Ricardo Martinho, Rui Rijo, Faiez Gargouri, Angappa Gunasekaran, and Altamiro Pereira (Eds.), *Book of industry papers, poster papers and abstracts of the CENTERIS 2019 – Conference on Enterprise Information Systems / ProjMAN 2019 – International Conference on Project Management / Hcist 2019 – International Conference on Health and Social Care Information Systems and Technologies* (pp. 228-231). Sousse, Tunisian: SciKA.
Scholl, M. (2019). Participative Dialogue with Schools to Raise Information Security Awareness through Gamification. In Program committee, *23rd World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2019)* (pp. 50-51). Orlando, Florida, USA: InternationaI lnstitute of Informatics and Systemics (IIIS).
Scholl, M., Schuktomow, R., Koppatz P., Gube, S., Edich, D. (2019). SecAware4school: Informationssicherheitsbewusstsein für den Schulalltag. In Prof. Dr. Melzer, K.-M. (Hrsg.), Bericht Forschung und Transfer 2019 Forschung, Entwicklung, Transfer. Projekte und Publikationen der TH Wildau, S. 39.

Tabelle 4: Teilnahmen an Konferenzen und Messen zum Thema Informationssicherheit

Konferenz/ Messe	Teilnehmende	Datum	Ort
it-sa 2018	Regina Schuktomow, Denis Edich	Oktober 2018	Nürnberg, Messegelände
Glienicker Gespräche	Regina Schuktomow	Mai 2019	Berlin, HWR
15. Landeskonferenz: Digitalisierung im Gesundheitswesen	Regina Schuktomow, Peter Koppatz	Februar 2020	Potsdam, Universität Potsdam

Tabelle 5: Pressemitteilungen SecAware4school

Magazin	Artikel	Datum
Märkische Allgemeine Zeitung	Abschluss des Projektes SecAware4school	Dezember 2020
TH Wildau News	Informationssicherheit für den Schulalltag – Projekt SecAware4school der TH Wildau stellt Ergebnisse aus Zusammenarbeit mit Berliner und Brandenburger Schulen vor	Dezember 2020
Märkische Allgemeine Zeitung	Schüler in Sachen Datenschutz sensibilisieren	April 2019
TH Wildau News	Erster Kreativworkshop zum Sicherheitsbewusstsein im Schulalltag mit Pilotschulen an der TH Wildau	April 2019
Märkische Allgemeine Zeitung	Neues Projekt für Informationssicherheitsbewusstsein	März 2019
Märkische Allgemeine Zeitung	Hilfreich für Bewerbungen. Prüfzentrum für den Europäischen Computerführerschein an der TH Wildau.	Januar 2019
TH Wildau News	Neues Projekt für mehr Informationssicherheitsbewusstsein im Schulalltag	November 2018
Märkische Allgemeine Zeitung	Informationssicherheit auf dem Stundenplan – Königs Wusterhausener Bredow-Oberschüler beteiligen sich an der Pilotmaßnahme eines Projektes der TH Wildau	September 2018

9 Ausblick

Das Ziel dieser Projektdokumentation ist zu zeigen, dass das Vorhaben des Projektes erfüllt wurde und die Ziele an Beispielen von Pilotschulen umgesetzt wurden. Von allen beteiligten Akteuren haben wir starke positive Resonanz erhalten. Schulen sind offen für die im Projekt vorgestellten Methoden und gewillt, an einer Kooperation mit Forschungsprojekten zur Informationssicherheit teilzunehmen.

Das eigentliche Hindernis ist die Organisationskultur der Schulen. Diese bietet wenig Raum für freies Handeln im Unterrichtsfach für Lehrende. Die Lehrpläne müssen stark eingehalten werden und aufgrund zahlreicher Unterrichtsausfälle wegen mangelnder Lehrerschaft bleibt wenig Zeit für zusätzliche Informationssicherheits-Angebote. Jedoch haben alle im Projekt beteiligten Lehrende den Wunsch geäußert, mehr solcher Projekte mit den Schulen und für die Schulen zu fördern, um die heute wichtigen Kompetenzen für die Digitalisierung den

Schülerinnen und Schülern schonend beizubringen und gleichzeitig für Informationssicherheit zu sensibilisieren.

Es ist daher wichtig „Informationssicherheit“ in den Schulen und anderen Bildungseinrichtungen zu etablieren (z.B. als reguläre Projekttage, Seminare, im Unterricht etc.) und das Konzept *train the trainer* anzuwenden, denn dadurch erhöht sich die Sensibilisierung bei den einzelnen Schülerinnen und Schülern und bei den Lehrenden. Die Sensibilisierung sollte so früh wie nur möglich beginnen, denn die Digitalisierung schreitet stetig und allumfassend voran. Es bleibt nur wenig Zeit, die heranwachsende Gesellschaft nachhaltig und effektiv für den bewussten Umgang mit sensiblen Daten und Informationen zu sensibilisieren.

Nachhaltige Nutzung der entwickelten Lernszenarien und Methoden in und außerhalb der Schule

Die weitere Verwendung der Projektergebnisse und somit die Nachhaltigkeit des Projektes SecAware4school ist durch die Möglichkeit der kostenfreien Nutzung der entwickelten Lernszenarien inklusive Moderationsanleitungsbuches, in dem alle Anleitungen gebündelt sind, zu deren Einsatz gesichert. Alle entwickelten Materialien, (u.a. Moderationsanleitung, Flyer und Broschüre), können von der Webseite als PDF kostenfrei heruntergeladen werden. Alle digitalen Lernszenarien können direkt von der Webseite abgerufen und gespielt werden.

Die Pilotschulen bekommen jeweils ein Set von 36 analogen und digitalen Lernszenarien, die sie zur Sensibilisierung von Schülerinnen und Schüler im Unterricht oder bei Projekttagen einsetzen können.

Literatur

Amt für Statistik Berlin-Brandenburg. 2019A. *Statistischer Bericht B | 1 - j / 17: Allgemeinbildende Schulen im Land Berlin Schuljahr 2017/18.* Herausgeber: Amt für Statistik Berlin-Brandenburg. Potsdam. Zugriff am 30. Juni 2020. https://www.statistik-berlin-brandenburg.de/publikationen/stat_berichte/2019/SB_B01-01-00_2017j01_BE.pdf.

Amt für Statistik Berlin-Brandenburg 2019. *Statistischer Bericht B | 1 - j / 18: Allgemeinbildende Schulen im Land Brandenburg Schuljahr 2018/19.* Herausgeber: Amt für Statistik Berlin-Brandenburg. Berlin. Zugriff am 30. Juni 2020. https://www.statistik-berlin-brandenburg.de/publikationen/stat_berichte/2019/SB_B01-01-00_2018j01_BB.pdf.

BAköV, Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern. 2016. *Handbuch IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung.* Herausgeber: BAköV. Bd. Version 5.0.

Berg, A. 2016. „Digitale Schule - vernetztes Lernen." Von BITKOM e.V. Hrsg. Berlin.

Beyer, M., S. Ahmed, K. Doerlemann, S. Arnell, S. Parkin, A. Sasse, und N. Passingham. 2016. „Awareness is only the first step. A framework for progressive engagement of staff in cyber security." *Business white paper* (Hewlett Packard).

Bitkom Research GmbH. 2015. „Digitale Schule - vernetztes Lernen." In *Ergebnisse repräsentativer Schüler- und Lehrbeauftragungen zum Einsatz digitaler Medien im Schulunterricht*, von BITKOM e.V. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien Hrsg. Berlin.

Bressler, D., und A. Bodzin. 2013. „A Mixed Methods Assessment of Students' Flow Experiences During a Mobile Augmented Reality Science Game." *Journal of Computer Assisted Learning*, 505-517.

Busch, Brigitta. 2013. *Mehrsprachigkeit.* Wien: Facultas.

Damon, W. 1984. „Peer education: The untapped potential." *Journal of Applied Developmental Psychology* (http://www.sciencedirect.com/science/article/pii/0193397384900066) 5 (4): 331-343.

Dark, M.J. 2006. „Security Education, Training and Awareness from a Human Performance Technology Point of View." In *Readings and Cases in Management of Information Security, Course Technology*, von M.E. Whitman und H.J. (Hrsg.) Mattord, 86-104. Mason.

Digital-Kompas, & Deutschland sicher im Netz e.V. (Hrsg.). 2019. *Surfen im Internet - ZuHause und mobil.* Übersetzung: Abgerufen am 11.06.20 https://www.digital-kompass.de/sites/default/files/material/files/handreichung_2_surfen_2019_druck.pdf.

DuBois, D.L., und M.J. Karcher. 2013. *Handbook of youth mentoring.* Sage Publications.

Fang, X., J. Zhang, und S. S. Chan. 2013. „Development of an Instrument for Studying Flow in Computer Game Play." *International Journal of Human-Computer Interaction*, 456-47.

Feierabend, S., T. Rathgeb, und T. Reutter. 2018. „JIM-Studie 2018 - Jugend, Information, Medien." In *Basisuntersuchung zum Medienumgang 12- bis 19-Jähriger.*, von Medienpädagogischer Forschungsverbund Südwest Hrsg.

Fingerhut, K. o.J. *Narration als Lernform im Fachunterricht und die Eweiterung von Sprachkompetenz im Fachunterricht.* o.O.

Haucke, A: Pokoyski, D. 2018. „Mea culpa - Schuld, Scham und Opferrolle bei Social Engineering." *kes* (1): 6-8.

Helisch, M., und D. (Hrsg.) Pokoyski. 2009. *Security Awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung.* Wiesbaden: Vieweg + Teubner.

Hertreiter, L. 2018. „Der unendliche Prozess um ein Selfie." *Sueddeutsche Zeitung (Hrsg.)* https://www.sueddeutsche.de/panorama/david-slater-der-unendliche-prozess-um-ein-selfie-1.3946613.

Hoegl, M. 2005. „Smaller teams - better teamwork: How to keep project teams small." *Business Horizons*, 209-214. . doi:10.1016/j.bushor.2004.10.013.

Khan, Bilal , Khaled S. Alghathbar, Syed Irfan Nabi, und Muhammad Khurram Khan. 2011. „Effectiveness of information security awareness methods based on psychological theories." In *African Journal of Business Management*, 10862-10868. doi:10.5897/AJBM11.067.

Kim, E.B. 2014. *Recomendations for information security training for college students, Information Management & Computer Security.* Bd. 22(1).

KnowBe4 Human error. Conquered. 2020. „Security Awareness." *Der Mensch ist das Angriffsziel Nummer 1. Security Awareness als Teil des Risikomanagements. CBT: Wie sich Mitarbeiter sensibilisieren lassen.* Berlin, Mai.

Linek, S. B., und D. Albert. 2009. „Game-based Learning: Gender-specific Aspects of Parasocial Interaction and Identification." *Conference: International Technology, Education and Development Conference (INTED).*

Matas, I., und D. Pokoyski. 2018. „Von der Ente zur End-Täuschung." *Kes*, 10: 19-23.

Piaget, J. 2003. *Meine Theorie der geistigen Entwicklung.* Beltz.

Pokoyski, D. 2009. „Security Awareness: Von der Oldscholl in die Next Generation - eine Einführung." In *Security Aeareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung*, von M. Helisch und D.(Hrsg.) Pokoyski, 1-8. Wiesbaden: Vieweg + Teubner.

Schmidt, B. 2002. „Peer-Intervention-Peer-Involvement-Peer-Support: Möglichkeiten und Grenzen peergestützter Ansätze für die Prävention riskanter Drogenkonsumformen in der Partyszene." In *Drogenkonsum in der Partyszene: Entwicklungen und aktueller Kenntnisstand*, 127-140. Bundeszentrale für für gesundheitliche Aufklärung (BZgA) (Hrsg.).

Scholl, M., F. Fuhrmann, und D. Pokoyski. 2016. „Information security awareness 3.0 for job beginners.“ In *Proceedings of the Conference on ENTERprise Information Systems*, von J.E. (Varajão, M.M. Cruz-Cunha, R. Martinho, R. Rijo, N. Bjørn-Andersen, R. Turner und D. (Hrsg.) Alves, 433-436.

Scholl, M., Leiner K., und F. Fuhrmann. 2017. „Blind spot: Do you know the effectiveness of your information security awareness-raising program?“ *Journal of Systemics, Informatics and Cybernetics*, 58-62.

Scholl, Margit. 2018. „Information Security Awareness in Public Administrations.“ In *Public Management and Administration*, Herausgeber: Ubaldo Comite, 27-55. Wildau: IntechOpen. doi:10.5772/intechopen.74572.

Schonschek, Oliver. 2020. „Der Mensch ist das Angriffsziel Nummer 1.“ In *Security-Insider*, 3-5. Berlin: Vogel IT-medien GmbH.

Singh, A.N., A. Picot, J. Kranz, M.P. Cupta, und A. Ojha. 2013. „Information security management (ism) practices: Lessons from select cases from India and Germany.“ *Global Journal of Flexible Systems Management*, 225-239.

Sokolov, Daniel AJ. 2018. *Affen-Selfie: Affe Naruto bekommt keine Copyright-Tantiemen.* Herausgeber: heise online. 24. April. Zugriff am 05. November 2020. https://www.heise.de/newsticker/meldung/Affen-Selfie-Affe-Naruto-bekommt-keine-Copyright-Tantiemen-4030277.html.

Styles, M. 2013. *Constructing Positive Influences for User Security Decisions to Counter Corporate or State Sponsored Computer Espionage Threats.* Bd. Vol. 8030, in *HAS 2013 Lecture Notes in Computer Science*, von L. Marinos und I. (Hrsg.) Askoxylakis. Springer.

Take Aware Events (Hrsg.). 2018. „Von der Ente zur End-Täuschung. Studie, veröffentlicht anlässlich der 2. Social Engineering-Konferenz.“ *BLUFF CITY.* Köln.

Trybus, J. 2014. „Game-Based Learning: What it is, Why it Works, and Where it's Going.“ Zugriff am 06 2017. http://newmedia.org/game-based-learning--what-it-is-why-it-works-and-where-its-going.html.

Wikimedia Foundation Inc. kein Datum. *Wikipedia.* Zugriff am 07. 03 2019. https://de.wikipedia.org/wiki/Selfie. .

Workman, M. 2007. *Gaining Access with Social Engineering: An Empirical Study of the Threat, Information Systems Security.* Bd. 16 (6).

Projektmitarbeitende

Margit C. Scholl (Prof. Dr. rer. Nat.)

Professorin für Wirtschafts- und Verwaltungsinformatik an der Technischen Hochschule Wildau, Fachbereich Wirtschaft, Informatik, Recht. Sie ist verantwortlich für die Projektleitung und das Projektmanagement von SecAware4school.

Regina Schuktomow (M.A.)

Wissenschaftliche Mitarbeiterin und operative Projektleiterin im Projekt SecAware4school.

Denis Edich (M.Sc.)

Wissenschaftlicher Mitarbeiter im Projekt SecAware4school und zuständig für digitale Anwendungen, Web-Entwicklung und Design.

Peter Koppatz

Wissenschaftlicher Mitarbeiter im Projekt SecAware4school und zuständig für digitale Anwendungen und Web-Entwicklung. Er ist freier Trainer und Software-Entwickler.

Stefanie Gube

Wissenschaftliche Mitarbeiterin im Projekt SecAware4school und zuständig für Recherche, Umsetzung und Entwicklung der analogen Lernszenarien.

Ernst-Peter Ehrlich

Labor-Ingenieur

Josephine Gerlach

Studentische Mitarbeiterin mit Schwerpunkt Recherche und Lektorat.

Clara Paetow

Studentische Mitarbeiterin mit Schwerpunkt Recherche und Umsetzung und Entwicklung der analogen Lernszenarien.

Christin Walch

Studentische Mitarbeiterin mit Schwerpunkt Umsetzung und Unterstützung.

Anhang

Anhang zu Kapitel 4

Informationsblatt für die Eltern

Fotokollage Forschungsgruppe Prof. Margit Scholl 2019

Informationsblatt für die Eltern

Das Projekt „SecAware4school“ Informationssicherheit in der Schule

Zielsetzung des Projektes
Frau Prof. Dr. Scholl und ihr Forschungsteam von der Technischen Hochschule Wildau möchten mit dem Projekt „SecAware4school“, gefördert von der privaten Horst Görtz Stiftung, Schüler/innen und ihre Bezugspersonen (Lehrende und Eltern) für das Thema der Informationssicherheit sensibilisieren. Der sorgsame Umgang mit personenbezogenen Daten bei der Nutzung von Internetdiensten und sozialen Netzwerken wird dabei geschult. Es ist vorgesehen jugendliche Sicherheitsberater/innen auszubilden, um nach dem Projekt mit Unterstützung der Lehrer/innen ihr Wissen und ihre Kenntnisse vor allem auch in der eigenen Anwendung der erlebnisorientierten/spielbasierten Lernszenarien an Schüler/innen weiterzugeben.

Umsetzung des Projektes
An dem Projekt beteiligen sich 5 Pilotschulen mit ausgewählten Klassenstufen 7 bis 11. Die Projektdauer ist zwei Jahre (bis August 2020). Die Interessen der Befragten wurden in einer Umfrage ermittelt und berücksichtigt. In der Pilotmaßnahme erleben Schüler/innen aktiv Sensibilisierungsmaßnahmen zum Thema der Informationssicherheit durch analoge und digitale spielbasierte Lernszenarien. Dadurch lernen sie bereits ein wichtiges Aufgabenfeld einer Sicherheitsberaterin/eines Sicherheitsberaters kennen: die Initiierung, Planung und Durchführung von Sensibilisierungs- und Schulungsmaßnahmen für Informationssicherheit. Des Weiteren können Schüler/innen an Kreativworkshops für die Entwicklung spielbasierter Lernszenarien teilnehmen. Über den aktuellen Stand und das weitere Vorgehen wird an Informationsveranstaltungen für Schüler/innen, Lehrende und Eltern berichtet.

Zusätzliches Angebot
Im Modul „IT-Sicherheit“ haben Schüler/innen die Möglichkeit der kostenlosen Prüfung zum Europäischen Computerführerschein (ECDL) mit einer lebenslang gültigen CERT-ID.
Weitere Informationen finden Sie auf der Projektwebseite: http://secaware4school.wildau.biz
SecAware4school-Team

Forschungsgruppe Prof. Dr. Margit Scholl im Jahr 2019 beim Kreativworkshop.

Anhang zu Kapitel 6

Flyer Ausbildung zur Informationssicherheitsbeauftragten 1

Flyer, Ausbildung zur Informationssicherheitsbeauftragten 1

Anhang zu Kapitel 8

Flyer SecAware4school

Broschüre SecAware4school

Poster SecAware4school auf Deutsch

Poster SecAware4school auf Englisch

Plakate aller Lernszenarien von SecAware4school

Auszüge aus Pressemitteilungen

Auszug aus dem Forschungsbericht 2019

Besuch der IT-Messe it-sa 2018 Nürnberg

Bild aus dem Kreativworkshop von SecAware4school

Technische Hochschule Wildau
Hochschulring 1
15745 Wildau

Ansprechpartner

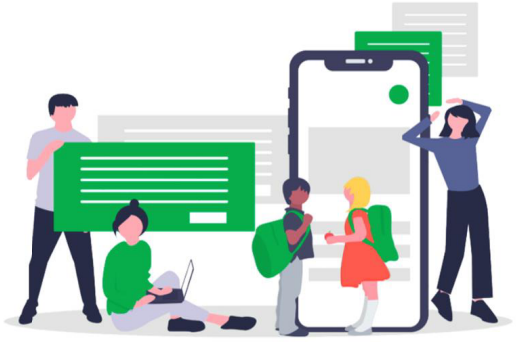
Frau Prof. Dr. rer. nat. Margit Scholl
margit.scholl@th-wildau.de

Regina Schuktomow
regina.schuktomow@th-wildau.de

Projektwebseite: **https://secaware4school.wildau.biz**

Mehr Sicherheit an Schulen! Informationssicherheitsbewusstsein für den Schulalltag:

SecAware4school



SecAware 4school

GEFÖRDERT VON HGS Horst Görtz Stiftung

Technische Hochschule Wildau Technical University of Applied Sciences WILDAU

Flyer SecAware4schoolh

600
Schülerinnen und Schüler aus 5 Schulen

36
analoge und digitale Lernszenarien

12
Themenbereiche

3
Schwierigkeitsgrade

Informationssicherheitsbewusstsein für den Schulalltag

Ausgangssituation

SecAware4school ermöglicht Schülerinnen und Schülern einen bewussten und sicheren Umgang mit Informationen verschiedenster Art. Die Stärkung des Bewusstseins und der Kompetenzen bezüglich Informationssicherheit wurde durch analoge und digitale erlebnisorientierte Lernszenarien gefördert. Bewusster Umgang mit eigenen und personenbezogenen Daten wird heutzutage als eine wichtige Kompetenz angesehen, die jeder erlangen kann!

Ziele

- Ausbildung der Schülerinnen und Schüler zu Sicherheitsberaterinnen und Sicherheitsberatern im Modul IT-Sicherheit (ICDL)
- Aneignung von Fähigkeiten für den sorgsamen Umgang mit personenbezogenen Daten bei der Nutzung von Internetdiensten und sozialen Netzwerken
- Durch spielerische und erlebnisorientierte Lernszenarien Bewusstsein für Informationssicherheit erforschen und schulen

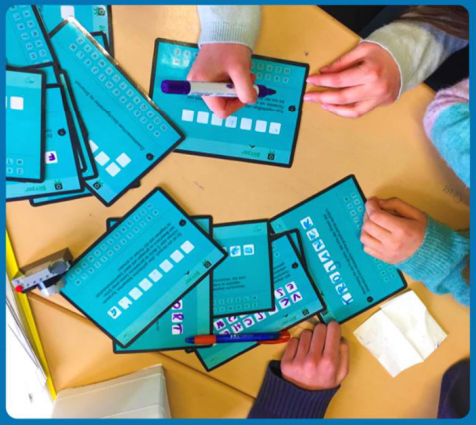
Methoden

Die Lernansätze **Game-based Learning**, **Accelerated Learning**, **Authentic Learning** und **Narratives Lernen** liegen den erlebnisorientierten Lernszenarien im Bereich der Informationssicherheit zugrunde.

Angewandte Methoden

- fördern die Kommunikationsfähigkeit, soziale Interaktion und Zusammenarbeit
- greifen reale (Problem-) Situationen aus dem beruflichen Alltag auf
- lassen komplexe und abstrakte Lerninhalte greif- und erlebbar werden
- bieten direktes Feedback zum Lernfortschritt
- ermöglichen den Lernenden durch Ausprobieren, Fehler zu machen und die Übung zu wiederholen
- orientieren sich an dem Wissensstand und den Bedürfnissen der Lernenden
- unterstützen die Weitergabe und den Austausch von Wissen

Pro Pilotschule nahmen jeweils zwei Klassen aus den Jahrgangsstufen 6, 9 und 11 mit je 20 Schülerinnen und Schülern teil. Diese wurden für ihr jeweiliges Klassenstufenniveau ausgebildet, um die erlernten digitalen Kompetenzen an jüngere Klassenstufen weiterzugeben.



SecAware4school -
Spielbasierte Sensibilisierung zum Thema Informationssicherheit im Schulunterricht

Im Projekt SecAware4school wurden insgesamt 36 analoge und digitale spielbasierte Lernszenarien in drei Schwierigkeitsgraden entwickelt und mit Pilotschulen erprobt. In Kreativworkshops wurden Ideen für Lernszenarien entwickelt, die zu verschiedenen Bereichen der Informationssicherheit sensibilisieren und im Schulunterricht eingesetzt werden.

Spielbasierte Lernszenarien

Erlebnisorientierte und interaktive Methoden wurden bei der Entwicklung der analogen und digitalen Lernszenarien eingesetzt.

Schülerinnen und Schülern sowie deren Bezugspersonen, den Lehrenden und Eltern, ist es möglich, sich spielerisch über Themen wie Verhalten in sozialen Netzwerken, Internet, Mobbing, Umgang mit Passwörtern, Bildrechten und Fake News zu sensibilisieren.

In ihrer Gesamtheit vermitteln die Lernszenarien den achtsamen und sicheren Umgang mit sensiblen Informationen und persönlichen Daten.

Drei Schwierigkeitsniveaus

Am Projekt waren Klassenstufen zwischen der 6. und 11. involviert. Um die Lernszenarien für alle Beteiligten gleichermaßen interessant zu gestalten, wurden 3 Schwierigkeitsgrade festgelegt: Der erste und somit leichteste Schwierigkeitsgrad eignet sich für die Klassenstufen 6 bis 7, der mittlere für die 8. und 9. Klassenstufen und der höchste Schwierigkeitsgrad ist den Klassenstufen 10 und 11 zuzuordnen.

Durch die Anpassung der Lernszenarien in jeweils drei Schwierigkeitsgrade wird neuer Input an den vorhandenen Wissensstand der Beteiligten angeknüpft.

Verhalten in sozialen Netzwerken

An dieser Lernstation geht es darum, Lösungen und Ansprechpartner in verschiedenen Situationen zu finden und sich einen adäquaten und freundlichen Umgang in sozialen Netzwerken anzueignen.

Fake or real?

Fake News ist der moderne Ausdruck für eine Information, die von allgemein bekannten Tatsachen ablenken und diese im Extremfall verfälschen soll. An diesem Lernszenario soll die Wahrnehmung für richtige oder falsche Nachrichten sensibilisiert werden.

Fake News

Das Ziel des Lernszenarios ist das Finden und Herstellen der Zusammenhänge zwischen den Fake News-Fällen, die ein konkretes Ereignis beschreiben. In Gruppendiskussionen muss eine Übereinstimmung gefunden werden, die die logische Zusammengehörigkeit von angewandtem Werkzeug, den Begriffen und der Strategie zum betrachteten Fall sinnvoll erscheinen lässt.

Storytelling

Das Lernszenario „Storytelling“ fördert gleichzeitig Kreativität und die Verknüpfung erlernter Begriffe, indem eine kurze Geschichte zu einem bestimmten Thema der Informationssicherheit erfunden und die gewürfelten Symbole darin eingebaut werden sollen.

Security Sketch

In der Rolle einer/s Büromitarbeitenden sollen die richtigen Entscheidungen in Bezug auf die Passwortsicherheit getroffen werden. Beispielsweise soll entschieden werden, wie mit einem neu erhaltenen Passwort umgegangen werden soll und ob/ wo dieses notiert wird. Dieses digitale Lernszenario dient dazu, für den richtigen Umgang mit Passwörtern zu sensibilisieren. Neben der deutschen Version wurde dieses Lernszenario auch in englischer Sprache umgesetzt, um der Internationalisierung an den Schulen gerecht zu werden.

Bildrechte

Dieses digitale Lernszenario hilft bei der Auseinandersetzung rund mit dem Thema Bildrechte. Der allgemein sorglose Umgang mit Multimediainhalten wirft zahlreiche Fragen auf. Ein Leitfaden für das rechtskonforme Verhalten sensibilisiert die Teilnehmenden.

Hacker Terminal

In diesem digitalen Lernszenario werden grundlegende Begriffe der Informationssicherheit wiederholt und vertieft. In der Rolle der Retro-Hacker sollen anhand von Hinweisen „verschlüsselte" Kennwörter erraten werden, um an Zugänge und ins System zu gelangen.

Datenspionage

Das digitale Lernszenario dient der Bewusstmachung möglicher Sicherheitsobjekte am Arbeitsplatz, die einer besonderen Aufbewahrung bedürfen. Objekte mit sensiblen Informationen sollen erkannt und auf sichere Weise am Arbeitsplatz aufbewahrt werden.

Security Surfer

In diesem analogen Lernszenario wird das globale Thema Internet aufgegriffen und die Möglichkeiten, die das Internet bietet, näher beleuchtet. Beim Surfen im weiten Meer des Internets sollen die Gefahren erkannt und die passenden Schutzmaßnahmen gefunden werden.

Schnelles Begrifferaten

Dieses Lernszenario trainiert den sicheren Gebrauch von Fachbegriffen im Bereich der Informationssicherheit. Aufgrund der zunehmenden Menge an online verfügbaren Informationen und Diensten ist es von Bedeutung, sich mit Fachbegriffen der Informationssicherheit vertraut zu machen.

Zur Benutzung der spielbasierten Lernszenarien im Unterricht finden Sie eine Anleitung zum Selbsterstellen der Lernszenarien auf der Website des Projektes:
https://secaware4school.wildau.biz

Security Surfer

In diesem analogen Lernszenario wird das globale Thema Internet aufgegriffen und die Möglichkeiten, die das Internet bietet, näher beleuchtet. Beim Surfen im weiten Meer des Internets sollen die Gefahren erkannt und die passenden Schutzmaßnahmen gefunden werden.

Schnelles Begrifferaten

Dieses Lernszenario trainiert den sicheren Gebrauch von Fachbegriffen im Bereich der Informationssicherheit. Aufgrund der zunehmenden Menge an online verfügbaren Informationen und Diensten ist es von Bedeutung, sich mit Fachbegriffen der Informationssicherheit vertraut zu machen.

Zur Benutzung der spielbasierten Lernszenarien im Unterricht finden Sie eine Anleitung zum Selbsterstellen der Lernszenarien auf der Website des Projektes:
https://secaware4school.wildau.biz

Digital sozial

Bei diesem analogen Lernszenario geht es um das Verhalten im und mit dem Internet sowie den Umgang mit dem Smartphone in der eigenen Umwelt. Es soll zur Diskussion bezüglich des Verhaltens gegenüber anderen Personen anregen und für den kritischen Umgang mit den „neuen" Medien sensibilisieren.

Security Duell

Dieses Lernszenario bietet die Möglichkeit, potenzielle Angriffspunkte in einem Unternehmen zu erkennen und passende Schutzmaßnahmen zu fnden.

Veranstaltungsblock im Projekt

1. Informationsveranstaltungen
2. Awareness Trainings
3. Kreativworkshops
4. Ausbildung zur/zum Sicherheitsbeauftragten

Digital sozial

Bei diesem analogen Lernszenario geht es um das Verhalten im und mit dem Internet sowie den Umgang mit dem Smartphone in der eigenen Umwelt. Es soll zur Diskussion bezüglich des Verhaltens gegenüber anderen Personen anregen und für den kritischen Umgang mit den „neuen" Medien sensibilisieren.

Security Duell

Dieses Lernszenario bietet die Möglichkeit, potenzielle Angriffspunkte in einem Unternehmen zu erkennen und passende Schutzmaßnahmen zu fnden.

Veranstaltungsblock im Projekt

1. Informationsveranstaltungen
2. Awareness Trainings
3. Kreativworkshops
4. Ausbildung zur/zum Sicherheitsbeauftragten

Materialien und mehr Informationen unter
https://secaware4school.wildau.biz

Das Forschungsprojekt SecAware4school ist ein Projekt unter partizipatorischer Beteiligung von fünf Pilotschulen aus Berlin und Brandenburg. Es wurde an der Technischen Hochschule Wildau mit dem folgenden Forschungsteam von Frau Prof. Dr. Margit Scholl durchgeführt: Regina Schuktomow (operative Projektleitung), Peter Koppatz (technische Leitung), Denis Edich, Stefanie Gube und Josephine Gerlach. Wir danken zudem Peter Ehrlich als Labor-Ingenieur für wichtige Impulse und Clara Paetow als zeitweilige studentische Mitarbeiterin. Wir danken vor allem der Horst Görtz Stiftung (HGS) für die Förderung.

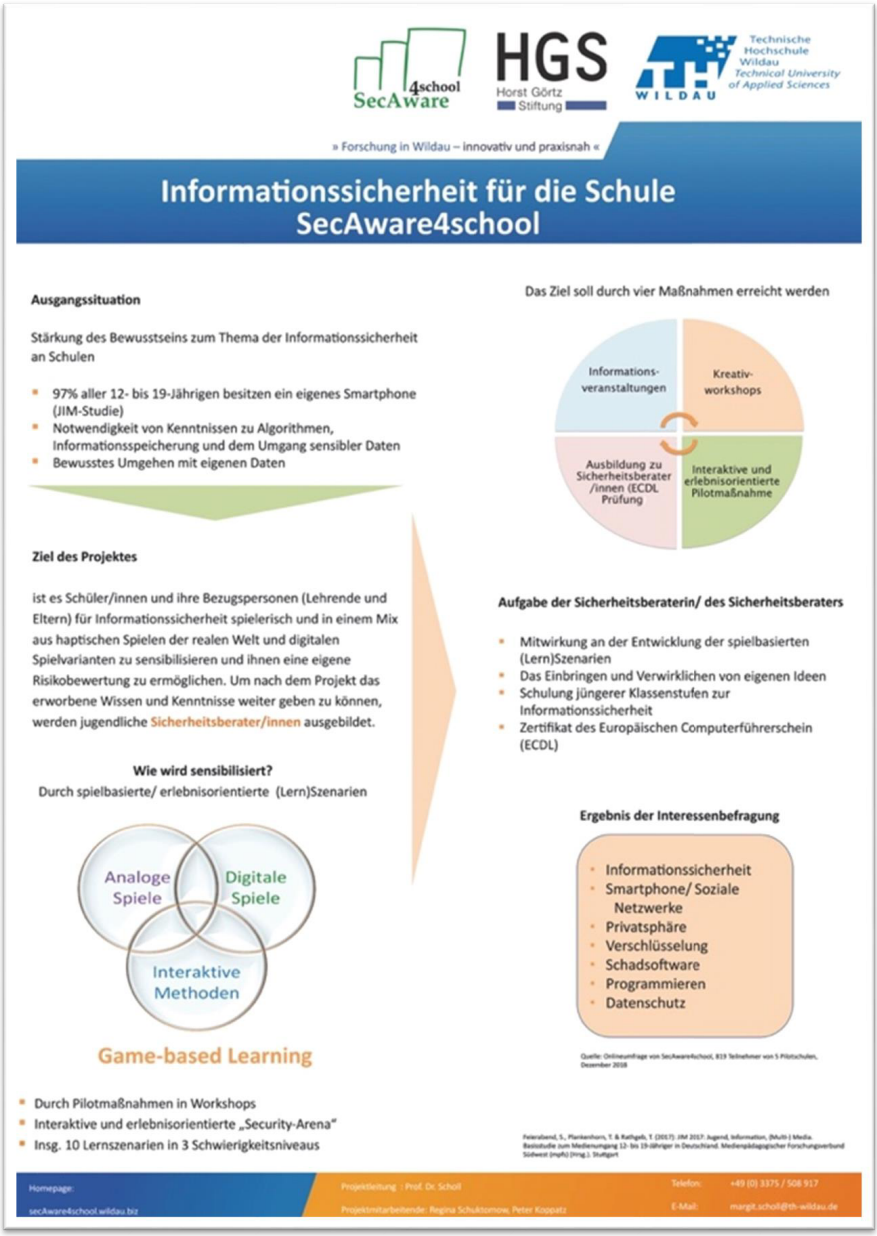
Kontakt
Technische Hochschule Wildau
Hochschulring 1
15745 Wildau

Prof. Dr. Margit Scholl (Hrsg.)
margit.scholl@th-wildau.de

Projektlaufzeit: 01.09.2018 – 31.12.2020
Das Projekt „Informationssicherheitsbewusstsein für den Schulalltag (SecAware4school)" wird aus Mitteln der Horst Görtz Stiftung gefördert.

ISBN: 978-3-9819225-1-6

Poster SecAware4school



Research in Wildau – Innovative and Practical «

Information Security Awareness for Daily Life at School (2018–2020)
SecAware4school

The project is focused on sensitizing pupils and their adult reference persons to issues surrounding information security.

As users of Internet services and social media, the young people are introduced to the careful handling of personal data in a playful manner, in the process developing their digital skills and technical understanding.

Ultimately, the students should find themselves in a position where their actions in the digital world are self-determined and aware.

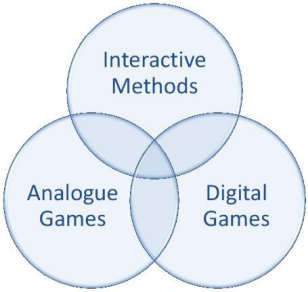
The skills taught include the ability to independently recognize the potential dangers in the network and assess risks, while also taking preventive protective measures.

How is awareness raised?

Through game-based / experience-oriented (learning) scenarios

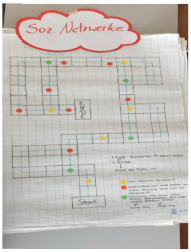
Information Events

Awareness Trainings



Serious Games:
Game-Based Learning

Creative Workshops



Sustainable Implementation

- Training of young security consultants, including ECDL/ICDL exam and certification of teachers
- Establishing the topic of information security in schools in the form of seminars and project days

secaware4school.wildau.biz

Project management: Prof. Dr. Margit Scholl
Operative project lead: Regina Schuktomow
Technical project lead: Peter Koppatz

E-mail: margit.scholl@th-wildau.de
Phone: +49 (0) 3375 / 508 239

Poster der Lernszenarien

SecAware 4school

HGS Horst Görtz Stiftung

Technische Hochschule Wildau
Technical University of Applied Sciences

» Forschung in Wildau – innovativ und praxisnah «

Digital sozial – Internetregeln erkennen

Kritischer Umgang mit neuen Medien

Vorgehen

Situationen diskutieren und Richtigkeit bewerten.

Ziel des Lernszenarios

Richtiges Verhalten auf sozialen Plattformen im Internet sowie den angemessenen Umgang mit dem Smartphone erlernen.
Anregung zur Diskussion über das eigene Verhalten und das Verhalten untereinander.

Mehrwert

- Lerneffekt durch Selbstreflexion
- Richtiges Verhalten im Internet und mit dem Smartphone üben und anwenden
- Spiel- und Spaßfaktor
- Sensibilisierung auf 3 Schwierigkeitsniveaus

secaware4school.wildau.biz

Projektleitung: Prof. Dr. Margit Scholl
Operative Leitung: Regina Schuktomow
Technische Leitung: Peter Koppatz

E-Mail: margit.scholl@th-wildau.de
Telefon: +49 (0) 3375 / 508 239

» Forschung in Wildau – innovativ und praxisnah «

Security Surfer
Gefahren und Schutzmaßnahmen erkennen

Das globale Thema Internet und seine Untiefen

Vorgehen

Die Inseln schützen, indem Fragen zum Thema sicheres Surfen im Internet beantwortet und Schutzmaßnahmen gefunden werden.

Ziel des Lernszenarios

Beim Surfen durch das World Wide Web von Insel zu Insel mögliche Gefahren erkennen, Schutzmaßnahmen anwenden und eine Strategie entwickeln, um so viele Inseln wie möglich zu schützen.

Mehrwert

- Lerneffekt durch strategisches Denken
- Erkennen und Vermeiden von Gefahren im Internet
- Hoher Spiel- und Spaßfaktor dank kreativem Design
- Sensibilisierung auf 3 Schwierigkeitsniveaus

secaware4school.wildau.biz

Projektleitung: Prof. Dr. Margit Scholl
Operative Leitung: Regina Schuktomow
Technische Leitung: Peter Koppatz

E-Mail: margit.scholl@th-wildau.de
Telefon: +49 (0) 3375 / 508 239

SecAware 4school

HGS Horst Görtz Stiftung

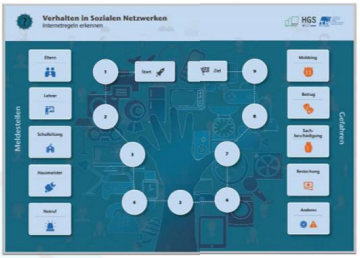
Technische Hochschule Wildau
Technical University of Applied Sciences
WILDAU

» Forschung in Wildau – innovativ und praxisnah «

Verhalten in sozialen Netzwerken – Internetregeln erkennen

Behandle andere so, wie du selbst behandelt werden möchtest!

Diese Regel gilt sowohl im wirklichen Leben als auch in sozialen Netzwerken.



Vorgehen

Für Fälle richtige Lösungen und Ansprechpartner finden, Fragen zu sozialen Netzwerken beantworten und Begriffe dazu erklären.

Ziel des Lernszenarios

Aufklärung und Kenntnis über potenzielle Sicherheitsgefahren sowie entsprechender Schutzmaßnahmen in sozialen Netzwerken und im Schulalltag.

Mehrwert

- Lerneffekt durch gezielte Konfrontation
- Adäquater und sicherer Umgang miteinander
- Spiel- und Spaßfaktor dank intensiver Interaktion
- Sensibilisierung auf 3 Schwierigkeitsniveaus

secaware4school.wildau.biz

Projektleitung: Prof. Dr. Margit Scholl
Operative Leitung: Regina Schuktomow
Technische Leitung: Peter Koppatz

E-Mail: margit.scholl@th-wildau.de
Telefon: +49 (0) 3375 / 508 239

» Forschung in Wildau – innovativ und praxisnah «

Storytelling in der Informationssicherheit

Zusammenhänge der Informationssicherheit erkennen

Vorgehen

Eine kurze Geschichte zu einem bestimmten Thema der Informationssicherheit erfinden und die gewürfelten Symbole in die Geschichte einbauen.

Ziel des Lernszenarios

Sich mit grundlegenden Begriffen der Informationssicherheit auseinandersetzen und diese in einem kreativen Rahmen anwenden.

Mehrwert

- Lerneffekt gefördert durch Narration
- Auseinandersetzung mit Grundbegriffen
- Spiel- und Spaßfaktor durch Kreativität
- Sensibilisierung auf 3 Schwierigkeitsniveaus
- Analog und digital

secaware4school.wildau.biz

Projektleitung: Prof. Dr. Margit Scholl
Operative Leitung: Regina Schuktomow
Technische Leitung: Peter Koppatz

E-Mail: margit.scholl@th-wildau.de
Telefon: +49 (0) 3375 / 508 239

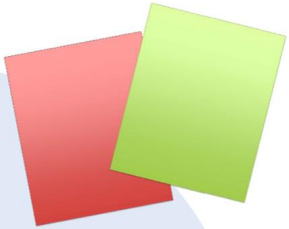
» Forschung in Wildau – innovativ und praxisnah «

Fake or Real – Fake News erkennen

Fake News

Desinformation

Verschwörungstheorien



Vorgehen

Meldungen sollen mithilfe von „Goldenen Regeln" und einer Definitionskarte als falsch (rote Decke) oder richtig (grüne Decke) eingeordnet werden.

Die Goldenen Regeln

Regeln für das Erkennen von falschen und wahren Meldungen

Hinweis	Bemerkung	Prüfungsstrategie
Überschriften	Insbesondere reißerischen Headlines (formal auch mit Großbuchstaben, Ausrufezeichen etc.) sind unseriös.	Überschrift kopieren, in Anführungszeichen setzen und bei Google eingeben: Wenn die Überschrift keine „seriösen" Treffer erzielt, ist sie vermutlich manipuliert.
URLs	Unrechte (z. B. mit minimalen Abweichungen) oder nachahmende URL (z. B. von bekannten Nachricht-enquellen) verifizieren.	Seite aufrufen, um URL mit etablierten Quellen zu vergleichen.
Quellen	Auf Reputation bzw. Image überprüfen, d.h. ist diese bekannt für glaubwürdige Organisationen oder Personen?	Wirkt das Impressum seriös? Gibt es andere Quellen, die Zitate oder Informationen bestätigen? Um die Website kontextuell zu prüfen, kann man bei Google die URL eingeben und „alles" auswählen, damit die Suchmaschine sämtliche Beiträge anzeigt, die auf der Website veröffentlicht wurden. Sind diese sehr einseitig, handelt es sich vermutlich nicht um eine objektive Quelle. Gibt man die URL in Anführungszeichen ein, erhält man Treffer, bei denen ÜBER diese Website von anderen Seiten berichtet wird.

Ziel des Lernszenarios

Existenz von Fehlinformationen im Internet soll realisiert werden. Dabei werden Regeln und Hintergrundrecherche zur ihrer Identifikation erlernt.

Mehrwert

- Lerneffekt durch Analyse konkreter Fälle
- Anwendung und Lernen von Regeln zum Umgang mit Fake News im Internet
- Spiel- und Spaßfaktor durch konzentrierte Gruppenarbeit
- Sensibilisierung auf 2 Schwierigkeitsniveaus

secaware4school.wildau.biz

Projektleitung: Prof. Dr. Margit Scholl
Operative Leitung: Regina Schuktomow
Technische Leitung: Peter Koppatz

E-Mail: margit.scholl@th-wildau.de
Telefon: +49 (0) 3375 / 508 239

» Forschung in Wildau – innovativ und praxisnah «

Fake News
Mit Fake News richtig umgehen

Umgang mit
verfälschten Bildern
und Nachrichten

Vorgehen

In einer Gruppendiskussion werden Fälle mithilfe passender Begriffs-, Werkzeug- und/oder Strategiekarten gelöst.

Ziel des Lernszenarios

Finden und Herstellen der Zusammenhänge zwischen konkreten Ereignissen und den passenden Gegenmaßnahmen, Begriffen oder Strategien.

Mehrwert

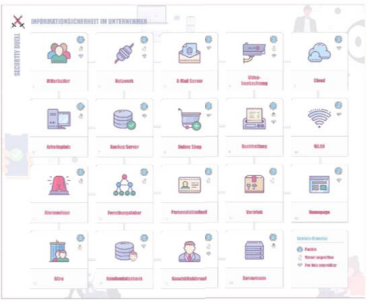
- Lerneffekt durch Erkennen von logischen Zusammenhängen
- Richtigen Umgang mit Fake News im Internet üben
- Spiel- und Spaßfaktor durch aktuellen Bezug
- 2 Schwierigkeitsniveaus

secaware4school.wildau.biz
Projektleitung: Prof. Dr. Margit Scholl
Operative Leitung: Regina Schuktomow
Technische Leitung: Peter Koppatz
E-Mail: margit.scholl@th-wildau.de
Telefon: +49 (0) 3375 / 508 239

» Forschung in Wildau – innovativ und praxisnah «

Security Duell
Informationssicherheit im Unternehmen

Potenzielle Angriffspunkte im Unternehmen erkennen



Vorgehen

Durch Angriffs-Aktionen sind Schwachstellen des Unternehmens zu finden, um diese auszunutzen. Mit Verteidigungs-Aktionen muss das Unternehmen geschützt werden. So viele erfolgreiche Aktionen wie möglich sollen durchführt werden.

Ziel des Lernszenarios

Mögliche Sicherheitsobjekte kennenlernen, Schwachstellen erkennen und Schutzmaßnahmen gegen potenzielle Angriffe finden.

Mehrwert

- Erlernen präventiver Denkweise durch Perspektivwechsel
- Angriffe voraussehen und wirksame Gegenmaßnahmen ergreifen
- Hoher Spaßfaktor dank ausgeprägter Spieldynamik
- Sensibilisierung auf 3 Schwierigkeitsniveaus

secaware4school.wildau.biz
Projektleitung: Prof. Dr. Margit Scholl
Operative Leitung: Regina Schuktomow
Technische Leitung: Peter Koppatz
E-Mail: margit.scholl@th-wildau.de
Telefon: +49 (0) 3375 / 508 239

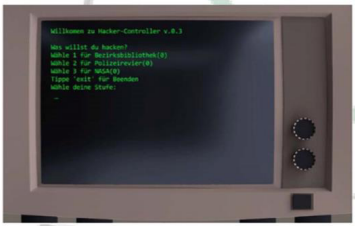
» Forschung in Wildau – innovativ und praxisnah «

Hacker Terminal

Vertiefung und Wiederholung von Begriffen der Informationssicherheit

Vorgehen

Anhand von Hinweisen „verschlüsselte" Kennwörter erraten, um unbefugt an einen Zugang zum System zu gelangen.



Ziel des Lernszenarios

Fachbegriffe und deren Bedeutung lernen. Dabei wird die assoziative Kette verstärkt.

Mehrwert

- Erlernen von Fachbegriffen und deren Definitionen
- Hoher Spaßfaktor dank Rätselcharakter
- Einzeln oder in der Gruppe spielbar (Digital)

secaware4school.wildau.biz

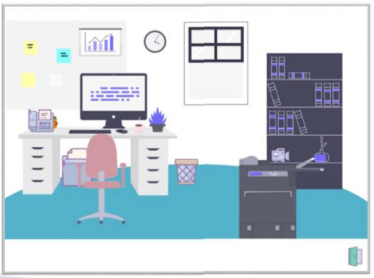
Projektleitung: Prof. Dr. Margit Scholl
Operative Leitung: Regina Schuktomow
Technische Leitung: Peter Koppatz

E-Mail: margit.scholl@th-wildau.de
Telefon: +49 (0) 3375 / 508 239

» Forschung in Wildau – innovativ und praxisnah «

Datenspionage – sicherer Raum

Bewusstmachung möglicher sicherheitsrelevanter Objekte am Arbeitsplatz

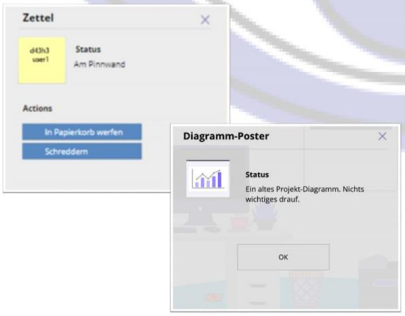


Vorgehen

Die verschiedenen Sicherheitsobjekte erkennen und diese sachgerecht verstauen, um Datendiebstahl vorzubeugen.

Ziel des Lernszenarios

Identifikation und sachgerechte Aufbewahrung sicherheitsrelevanter Objekte am Arbeitsplatz.



Mehrwert

- Lerneffekt dank realitätsnahem Aufbau
- Sensibilisierung im Umgang mit Sicherheitsobjekten und empfindlichen Informationen
- Hoher Spaßfaktor durch ansprechende Visualisierung
- Einzeln oder in Gruppen spielbar
- 3 Schwierigkeitsniveaus

secaware4school.wildau.biz

Projektleitung: Prof. Dr. Margit Scholl
Operative Leitung: Regina Schuktomow
Technische Leitung: Peter Koppatz

E-Mail: margit.scholl@th-wildau.de
Telefon: +49 (0) 3375 / 508 239

» Forschung in Wildau – innovativ und praxisnah «

Bildrechte

Richtiger Umgang mit Multimediainhalten und rechtskonformes Verhalten

Vorgehen

Fragen zum Thema Bildrechte müssen als digitales Quiz beantwortet werden.

Ziel des Lernszenarios

Kompetenzen in den Bereichen Urheberrecht und Quellennachweis verbessern sowie den rechtskonformen Umgang mit Bildmaterial und multimedialen Inhalten im Allgemeinen üben.

Mehrwert

- Lerneffekt durch starken Bezug zum Alltag
- Kompetenz im rechtskonformen Umgang mit Bildern erlangen
- Sensibilisierung auf 3 Schwierigkeitsniveaus
- Digitale Umsetzung

secaware4school.wildau.biz
Projektleitung: Prof. Dr. Margit Scholl
Operative Leitung: Regina Schuldtomow
Technische Leitung: Peter Koppatz
E-Mail: margit.scholl@th-wildau.de
Telefon: +49 (0) 3375 / 508 239

» Forschung in Wildau – innovativ und praxisnah «

Sketch - Secure Passwords

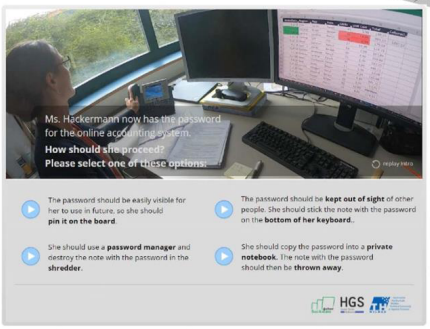
Kritischer Umgang mit Passwörtern

Vorgehen

Verhaltensbeispiele im Umgang mit Passwörtern sollen nach ihrer Korrektheit bewertet werden.

Ziel des Lernszenarios

Richtiges Verhalten und angemessener Umgang mit Passwörtern aufzeigen.



Mehrwert

- Lerneffekt dank visueller Unterstützung
- Sensibilisierung bei Wahl und Schutz von Passwörtern
- In Englisch verfügbar
- Einzeln und in Gruppen spielbar (digital)

secaware4school.wildau.biz

Projektleitung: Prof. Dr. Margit Scholl
Operative Leitung: Regina Schuktomow
Technische Leitung: Peter Koppatz

E-Mail: margit.scholl@th-wildau.de
Telefon +49 (0) 3375 / 508 239

Auszüge aus Pressemitteilungen

NEUES PROJEKT FÜR MEHR INFORMATIONSSICHERHEITSBEWUSSTSEIN IM SCHULALLTAG

12. NOVEMBER 2018 | DIPL.-ING. BERND SCHLÜTTER

Neues Projekt für mehr Informationssicherheitsbewusstsein im Schulalltag

Zwar haben Smartphones längst die Schulhöfe und -gebäude erobert, doch Fragen der Informationssicherheit und der Gefährdungen in Online-Medien sowie eine entsprechende Sensibilisierung dafür gehören an Schulen häufig noch nicht zum Alltag. Das Team „Verwaltungsinformatik und digitale Medien" von Forschungsprofessorin *Dr. Margit Scholl* am Fachbereich Wirtschaft, Informatik, Recht der Technischen Hochschule Wildau rückt dieses Thema jetzt in den Fokus der Aufmerksamkeit von Schülerinnen und Schülern, Lehrenden und Eltern. Dazu wurde das von der privaten Horst Görtz Stiftung geförderte Forschungsprojekt „Informationssicherheitsbewusstsein für den Schulalltag (SecAware4school)" gestartet.

Laut einer ersten Umfrage mit insgesamt 819 Teilnehmerinnen und Teilnehmern aus fünf Pilotschulen in den Ländern Brandenburg und Berlin interessieren sich immerhin 47,3 Prozent der Zielgruppe für die Themen Informationssicherheit und Schutz persönlicher Daten – aber eben mehr als die Hälfte nicht. Deshalb entwickelt und erprobt das Forschungsteam spielbasierte (Lern)Szenarien, die das persönliche Verhalten einprägsam reflektieren und so nachhaltig zu einem sorgsamen Umgang mit Internetdiensten und sozialen Netzwerken anregen.

Insgesamt sollen zehn für die Zielgruppen wichtige Themen in drei Schwierigkeitsniveaus aufbereitet werden. Die praxisnahen Lernformen mit vielen Interaktionsmöglichkeiten in Form einer „Security Arena" werden bis August 2020 in den Klassenstufen 6, 9 und 11 der Pilotschulen erprobt.

Schülerlabore der TH Wildau unterstützten MINT-Projekte weiterführender Brandenburger Schulen

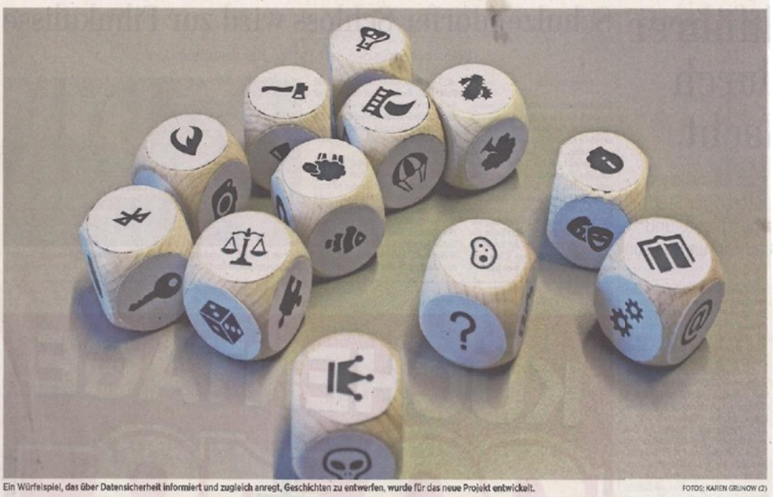
Pressemitteilung • Dez 14, 2018 09:06 CET

Peter Koppatz (l.), Mitarbeiter im Projekt "SecAware4school", betreute das Team des Paul-Fahlisch-Gymnasiums Lübbenau.

Im Rahmen des Brandenburger Verbundformates „**iTechLAB**" haben 2018 sechs weiterführende Schulen mit Hochschulen des Landes zusammengearbeitet, um im MINT-Bereich (**MINT: Mathematik, Informatik, Naturwissenschaften, Technik)** begabte Schülerinnen und Schüler gezielt zu fördern. **Drei Schulprojekte wurden von den Schülerlaboren der Technischen Hochschule Wildau fachlich begleitet.**

Um ihre innovativen Ideen im naturwissenschaftlich-technischen Bereich umzusetzen, erhielten sie Unterstützung durch **Theorie- und Methodenwissen**, aber auch durch **praktische Hilfen bei der Erstellung von Konzepten, Prototypen und Modellen**.

Auf einer Abschlusspräsentation am 7. Dezember 2018 in Potsdam stellten die Schülergruppen ihre Ergebnisse vor. So befasste sich ein Team der **Gesamtschule Treuenbrietzen** in einem Seminarkurs mit dem Thema „Erneuerbare Energien" am Beispiel eines landwirtschaftlichen Betriebes. Begleitet wurde es vom **NaWiTex-**



Ein Würfelspiel, das über Datensicherheit informiert und zugleich anregt, Geschichten zu entwerfen, wurde für das neue Projekt entwickelt. FOTOS: KAREN GRUNOW (2)

Schüler schützen ihre Daten

Projekt an der TH Wildau soll jungen Leuten beim Umgang mit Computer und Handy helfen

Von Karen Grunow

Um die 600 Schüler sind bei dem jüngsten Projekt dabei, das das Team um Margit Scholl, Professorin für Wirtschaft und Verwaltungsinformatik an der Technischen Hochschule Wildau, entwickelt hat. „SecAware4School" heißt es, und es geht dabei um „Informationssicherheitsbewusstsein für den Schulalltag". Neben zwei Berliner Schulen gehören das Friedrich-Wilhelm-Gymnasium, das Schillergymnasium und die Hans-Bredow-Oberschule in Königs Wusterhausen zu den Projektpartnern. „Das Ziel ist, Jugendliche zu sensibilisieren, dass sie sparsamer und bewusster mit den eigenen Daten umgehen", sagt Regina Schuktomow. Sie ist die operative Leiterin des Projektes, das seit September läuft und zwei Jahre dauern wird.

Bisher, sagt sie, habe das Projektteam nur mit motivierten Jugendlichen zu tun gehabt. Das Interesse ist groß, der spielerische Ansatz des von der Horst-Görtz-Stiftung geförderten Projektes gefällt den teilnehmenden Mädchen und Jungen. Ein Ziel ist, an jeder der beteiligten Schulen auch jugendliche Sicherheitsberater auszubilden. Diese können dann künftig selbst jüngere Schüler trainieren. Angesprochen werden mit dem Projekt Sechst- bis Elftklässler. Die große Altersspanne bringt einige zusätzliche Herausforderungen mit sich. So müssen alle spielerischen Lernszenarien für die verschiedenen Altersgruppen konzipiert werden. Das Team, zu dem neben Regina Schuktomow auch Stefanie Gube, Clara Paetow, Denis Edich, Peter Ehrlich und Peter Koppatz gehören, ist dabei, immer drei

> „Das Ziel ist, Jugendliche zu sensibilisieren, dass sie sparsamer und bewusster mit den eigenen Daten umgehen.
>
> **Regina Schuktomow,** operative Projektleiterin

Versionen eines Szenarios zu entwerfen. Zum Teil können sie auf bereits existierende Spiele zurückgreifen, die bereits für die „Security Arena" der TH entwickelt wurden. In dieser können Studierende, aber auch Mitarbeiter von Unternehmen der Region sensibilisiert werden. Beliebt ist beispielsweise das „Phishing-Spiel": Wie beim Fischeangeln wird aus einem den Teich symbolisierenden Karton etwas herausgefischt, in dem Fall E-Mails. Von denen einige echt und einige betrügerische Phishing-Mails sind. Bei den Schülern habe man aber nun gemerkt: „Die Jüngeren können mit E-Mails fast gar nichts mehr anfangen." Stattdessen kommunizieren sie über WhatsApp und Co., darauf müssen sich die „SecAware4School"-Spezialisten einstellen.

Zunächst hatten sie das Projekt in den Schulen vorgestellt und Infoblätter für die Eltern verteilt. Nun aber laufen allmählich die Sensibilisierungsphasen. „Da gehen wir in die Schulen und spielen die Lernszenarien durch", so Schuktomow. In der kommenden Woche ist ein Kreativworkshop vorgesehen, an dem Schulleiter, Lehrer und mindestens drei Schüler von jeder der teilnehmenden Schulen dabei sein sollen. Auch von „Known_sense", dem Vertriebspartner der spielebasierten Lernszenarien, wird jemand da sein. Idee ist, dass gemeinsam neue Lernszenarien entwickelt werden oder bereits existierende altersgemäß überarbeitet. Da sind vor allem die Schüler gefragt. Idealerweise diejenigen, die gern selbst Sicherheitsberater werden möchten. „Der Kreativworkshop ist bereits Teil der Ausbildung", erzählt Regina Schuktomow.

Bis zu zwölf Schüler pro Schule können sich entsprechend ausbilden lassen. An der TH bekommen sie die Möglichkeit, kostenlos den europäischen Computerführerschein zu machen. „Wir möchten ja, dass unser Projekt an den Schulen bleibt", betont Regina Schuktomow. Aber eben nicht als Projekt, sondern künftig als Teil des Unterrichtsangebots. Dass das Interesse am Thema groß ist, zeigte schon eine Online-Umfrage, die vorab unter Schülern durchgeführt wurde. Fast 2000 beteiligten sich daran.

Eines der Königs Wusterhausener Gymnasien wird im Mai bereits an die Hochschule kommen und dann in der Security Arena einen ganzen Projekttag erleben, mit Campus-Rundgang und Bibliothekstour und Essen in der Mensa.

Denis Edich, Peter Ehrlich, Clara Paetow, Stefanie Gube und Regina Schuktomow (v.l.) gehören zum Projekt-Team von TH-Professorin Margit Scholl.

Als neues Lernszenario ist eine Art Puzzle mit dem Arbeitstitel „Knigge" entstanden, es geht dabei um einige aktuelle Benimm-Regeln, etwa, dass Handys in Gesprächen oder beim Essen in den Taschen bleiben sollten. Ein Würfelspiel regt in zum Geschichtenerzählen. Stefanie Gube hat ein neues Brettspiel entwickelt, da geht es um soziale Netzwerke. „Schulen werden die Möglichkeit haben, die Spiele kostenlos auszuleihen", berichtet sie. So zeigt sich die Nachhaltigkeit des Projektes: Jugendliche Sicherheitsberater in den Schulen und die Möglichkeit, künftig selbst im Rahmen des Unterrichts Schülern mit Lernszenarien zu sensibilisieren.

ERSTER WORKSHOP ZUM SICHERHEITSBEWUSSTSEIN IM SCHULALLTAG MIT PILOTSCHULEN AN DER TH WILDAU

25. APRIL 2019 | FORSCHUNGSPROJEKT

Erster Workshop zum Sicherheitsbewusstsein im Schulalltag mit Pilotschulen an der TH Wildau

Am 5. April 2019 lud das Forschungsteam von Frau Prof. Dr. Margit Scholl im Rahmen des Projektes Informationssicherheitsbewusstsein für den Schulalltag („SecAware4school") Schülerinnen und Schüler sowie Lehrende und Schulleitungen aus Berlin und Königs Wusterhausen zum Kreativworkshop an die TH Wildau ein. Das von der Horst Görtz Stiftung geförderte Projekt sensibilisiert spielerisch Schülerinnen und Schüler zum Thema Informationssicherheit.

Im ersten Kreativworkshop von SecAware4school entwickelten die 25 Teilnehmenden vielfältige Ideen für Sensibilisierungsmaßnahmen zur Informationssicherheit im Schulalltag. Für die eigene Sensibilisierung und damit für ein besseres Verständnis rund um die Konzeption von Lernszenarien, hatten viele der Teilnehmenden bereits im Vorfeld an Informationsveranstaltungen und Awareness-Trainings mit erlebnisorientierten Lernszenarien des Forschungsteams teilgenommen.

Die neu zu entwickelnden analogen und digitalen Lernszenarien für Informationssicherheit in den Schulen sind nach dem Projektende im August 2020 auf der Projektwebsite abrufbar und können auch ausgeliehen werden.

Fachliche Ansprechpersonen:

Projektmanagement
Frau Prof. Dr. Margit Scholl
Tel. +49 3375 508-917
E-Mail: margit.scholl(at)th-wildau.de

Neues Projekt für Informationssicherheitsbewusstsein

Schüler lernen sensiblen Umgang mit ihren Daten in dem neuen Projekt „SecAware4School“ an der Technischen Hochschule Wildau. Drei Königs Wusterhausener Schulen gehören zu den Projektpartnern.

Ein Würfelspiel, das über Datensicherheit informiert und zugleich anregt, Geschichten zu entwerfen, wurde für das neue Projekt entwickelt. Quelle: Karen Grunow

Wildau

Um die 600 Schüler sind bei dem jüngsten Projekt dabei, das das Team um Margit Scholl, Professorin für Wirtschaft und Verwaltungsinformatik an der Technischen Hochschule Wildau, entwickelt hat. „SecAware4School“ heißt

Märkische Allgemeine

RND
REDAKTIONSNETZWERK DEUTSCHLAND

Wildau / Wildau

14:08 Uhr / 15.04.2019

Schüler in Sachen Datenschutz sensibilisieren

Um das Informationssicherheitsbewusstsein von Schülern im Alltag zu fördern, fand in der TH Wildau ein Kreativworkshop statt. Warum das Thema Datenschutz so wichtig ist und was es Aktuelles aus der Forschung gibt lesen Sie hier.

Professorin Margit Scholl von der TH Wildau. Quelle: Karen Grunow

Wildau. Schüler, Lehrer und Schulleiter von fünf Schulen in Königs Wusterhausen und Berlin beteiligten sich an einem Kreativworkshop an der Technischen Hochschule Wildau. Dieser ist Teil des Projektes „SecAware4School", bei dem es darum geht, Schüler ab Klassenstufe sechs für den Umgang mit ihren persönlichen Daten im Internet zu sensibilisieren, also um ein Informationssicherheitsbewusstsein im Schulalltag.

Forschungsteam begleitete die Gruppen

Zu den am Projekt beteiligten Schulen gehören das Friedrich-Wilhelm-Gymnasium, das Schillergymnasium und die Hans-Bredow-Oberschule in Königs Wusterhausen. Insgesamt 25 Teilnehmer konnte das Forschungsteam um TH-Professorin Margit Scholl zum Kreativworkshop begrüßen. Idee dabei war, dass in kleinerer Runde für das im September gestartete und für zwei Jahre laufende Projekt so genannte Lernszenarien entwickelt werden.

SecAware4School: Informationssicherheits-bewusstsein für den Schulalltag

Projektleitung
Prof. Dr. rer. nat. Margit Scholl

Projektmitarbeiter(innen)
Regina Schuktomow, Peter Koppatz, Stefanie Gube, Denis Edich

Kooperationspartner
Friedrich Schiller Gymnasium Königs-Wusterhausen, Brandenburg; Friedrich Wilhelm Gymnasium Königs-Wusterhausen, Brandenburg; Staatliche Gesamtschule Königs-Wusterhausen, Brandenburg; Humboldt Gymnasium, Berlin; Rudolf-Virchow Oberschule, Berlin

Projektvolumen
305.999 €

Mittelgeber
Horst Görtz Stiftung

Laufzeit
09/2018–08/2020

Abb. 1) Kreativworkshop von SecAware4school

Das von der Horst Görtz Stiftung (HGS) geförderte Projekt „SecAware4school“ (Sep. 2018 bis Aug. 2020), verfolgt das Ziel der Sensibilisierung von Schüler/innen, Lehrer/innen und Eltern für das Thema Informationssicherheit (IS). Wie wichtig ist Kindern und Jugendlichen der Schutz ihrer Daten und wie gehen sie damit um? Welche Kenntnisse sind zu IS vorhanden? Wie kann eine nachhaltige Sensibilisierung zielgruppenorientiert erfolgen? Mit diesen und ähnlichen Fragen beschäftigt sich das Forschungsteam. Eine zu Beginn des Projektes durchgeführte Online-Umfrage, an der ca. 800 Fragebögen ausgewertet werden konnten, verschaffte den Überblick über die Interessen der Teilnehmenden. Diese stehen im Vordergrund, um einen bewussten und sorgsamen Umgang mit Daten bei der Nutzung z. B. von Internet Services zu erreichen. Die Sensibilisierung erfolgt in spezifischen Awareness-Trainings und Kreativworkshops mithilfe von erlebnisorientierten Lernszenarien sowie Coaching- und Mentoren-Konzepten basierend u.a. auf Game Based Learning (GBL). Es handelt sich dabei um analoge und digitale Spielmechanismen zur Förderung der Motivation, um Verhaltensänderungen zu erzielen. Unsere Forschung zeigt dazu auf, dass Sensibilisierung als ein erster Schritt zur Erhöhung des Bewusstseins für IS die Menschen über interaktive Wissensvermittlung emotional einbinden und so motivationsfördernd wirken kann.

Die Lernszenarien werden hinsichtlich konkreter Alltagssituationen, Sprache und drei unterschiedlichen Schwierigkeitsniveaus für die Klassenstufen 6 bis 11 modifiziert bzw. neu entwickelt. Am Forschungsprojekt nehmen insgesamt ca. 600 Schülerinnen und Schüler aus fünf Pilotschulen in Berlin und Brandenburg teil. Um eine Breitenwirksamkeit und Nachhaltigkeit für IS auch nach dem Projektende zu erreichen, werden bis zu 10% der Schülerinnen und Schüler zu Sicherheitsberaterinnen und -beratern ausgebildet. Außerdem etablieren Pilotschulen teilweise komplette Seminare und Projekttage zur IS auf der Grundlage der ausgewählten Methoden des Forschungsprojektes in den Schulalltag. Darüber hinaus wird pro Pilotschule eine Lehrkraft in einer umfassenden Fortbildung zum IS-Beauftragten zertifiziert.

Nach allen durchgeführten erlebnisorientierten Maßnahmen ist bereits vor dem Projektende zu erkennen, dass Schülerinnen und Schülern das wichtige Thema IS (be-)greifbar und dadurch erfolgreich verständlich gemacht wurde.

Homepage:
https://secaware4school.wildau.biz/

Kontakt:
regina.schuktomow@th-wildau.de

Gefördert durch:

HGS

Besuch der IT-Messe it-sa Oktober 2018 in Nürnberg.

Bild aus dem Kreativworkshop von SecAware4school

In der Schule eignen wir uns wertvolles Wissen an. Erlebnisse und Erkenntnisse begleiten uns auf unserem Lebensweg und beeinflussen unsere Zukunft. So ist es von großer Bedeutung Inhalte des Schulunterrichtes an die Entwicklungen der aktuellen Zeit anzupassen.

Die Digitalisierung schreitet voran, und Kinder und Jugendliche wachsen damit auf. Im Projekt *SecAware4school* wurden Schülerinnen und Schüler für das Thema Informationssicherheit durch erlebnisorientierte Lernszenarien sensibilisiert, um sich das Bewusstsein für den sicheren Umgang mit persönlichen Daten anzueignen und zu bestärken.

In der Projektdokumentation werden die einzelnen Schritte der Sensibilisierung und die Erkenntnisse vorgestellt.

Weitere Informationen zum Projekt:
secaware4school.wildau.biz

ISBN 978-3-945740-13-2 € 29,99

9 783945 740132

Projektlaufzeit: 01.09.2018 - 31.12.2020

ISBN 978-3-945740-13-2

Das Projekt "Informationssicherheitsbewusstsein für den Schultag (SecAware4school)" inklusive dieses Buchdruckes der Projektdokumentation wurde gefördert durch die Horst-Görtz-Stiftung (HGS).

Buchwelten Verlag
FRANKFURT AM MAIN