IQ.SH

Institut für Qualitätsentwicklung
an Schulen Schleswig-Holstein

Medienkompetenz vermitteln

Digitale Mündigkeit

Schleswig-Holstein. Der echte Norden.

Impressum

Medienkompetenz vermitteln
Digitale Mündigkeit

Herausgeber
Institut für Qualitätsentwicklung an Schulen
Schleswig-Holstein (IQSH)
Dr. Gesa Ramm, Direktorin
Schreberweg 5, 24119 Kronshagen
http://www.iqsh.schleswig-holstein.de
https://twitter.com/_IQSH

Bestellungen
Onlineshop: https://publikationen.iqsh.de
Tel. +49 (0)431 5403-148
Fax +49 (0)431 988-6230-200
E-Mail: publikationen@iqsh.landsh.de

Autorinnen
Yuliya Kolesnykova, Sonja Reimer

Unter Mitarbeit von
Maximilian Groß, Svea Hundertmark, Jana Labahn

Gestaltung
Christoph Valentowicz

Lektorat
Petra Haars, Stefanie Pape

Titelbild
Regina Schaller

Publikationsmanagement
Petra Haars, Stefanie Pape

Auflage Juni 24

Broschüre Nr. 10/2024
Das IQSH ist laut Satzung eine dem Bildungsministerium unmittelbar nachgeordnete, nicht rechtsfähige Anstalt des öffentlichen Rechts.

Medienkompetenz vermitteln

Digitale Mündigkeit

Inhalt

Medienberatung des IQSH:
https://medienberatung.iqsh.de/start.html

1 Einführung

Unter Bezug auf die Strategie der Kultusministerkonferenz „Bildung in der digitalen Welt“[1] von 2016 hat das Land Schleswig-Holstein 2018 eine „Ergänzung zu den Fachanforderungen“[2] herausgegeben beziehungsweise Medienkompetenz als Bestandteil der Fachanforderungen für die Grundschule[3] aufgenommen. Hier werden Kompetenzen benannt, die Schülerinnen und Schüler zum Ende von Jahrgangsstufe 4 beziehungsweise mit dem Abschluss der Sekundarstufe I erworben haben sollten. Medienkompetenzvermittlung bildet allerdings kein eigenes Fach, sondern soll integrativer Bestandteil aller Fächer sein.

Das vorliegende Papier ist Teil einer Reihe von Handreichungen, die den Einstieg in die Vermittlung von Medienkompetenz erleichtern sollen. Die einzelnen Handreichungen greifen dabei die sechs Kompetenzbereiche der KMK[4] auf, ordnen diese jedoch inhaltlich folgenden elf Themen zu:

- Funktionsweise von Computern und dem Internet
- Den persönlichen Medieneinsatz weiterentwickeln und digitale Medien zum Lernen nutzen
- **Digitale Mündigkeit**
- Recherchieren: suchen und finden, bewerten und filtern
- Mit Medien kommunizieren und kollaborieren
- Medienproduktion und Präsentation
- Rechtsgrundlagen bei der Medienproduktion
- Gesundheit im Medienkontext
- Wirtschaft, Umwelt und Nachhaltigkeit im Medienkontext
- Politik und Gesellschaft im Medienkontext
- Jugend- und Verbraucherschutz

Jede der elf Handreichungen bietet einen Einstieg in das jeweilige Thema. Eine Vertiefung kann eigenständig mithilfe der weiterführenden Literaturhinweise erfolgen. Die Handreichungen richten sich an Lehrkräfte, wobei die beschriebenen Inhalte die Grundlage für den Kompetenzerwerb der Schülerinnen und Schüler bilden.

Die Einbindung der Inhalte in das jeweilige Fach muss durch die Lehrkraft und in Passung mit der jeweiligen Lerngruppe sowie dem schulinternen Fachcurriculum erfolgen. Die Vermittlung von Medienkompetenz ist eine gesamtschulische Aufgabe. Eine Aufteilung auf die Fächer kann diesen Prozess unterstützen, sodass die Inhalte in den jeweiligen Fachkonferenzen im Team erarbeitet werden können. Gleichzeitig bietet es sich an, Medienkompetenz in Form von fächerübergreifenden Projekten zu erarbeiten. Sie bietet somit einen geeigneten Anknüpfungspunkt für die Öffnung der Fächer und das Denken außerhalb von Fachgrenzen.

Zur Illustration enthält jede Handreichung neben der inhaltlichen Darstellung des Themas einige Ideen zur unterrichtlichen Umsetzung, teilweise als methodische Hinweise, teilweise in Form etwas detaillierterer Vorschläge. Diese stellen jeweils einen Bezug zu den in den Fachanforderungen beziehungsweise in deren Ergänzung dargestellten Kompetenzen her und greifen zudem die in den jeweiligen Anhängen beschriebene Entwicklung der Medienkompetenz auf. Eine Anpassung an den eigenen Unterricht und an das eigene Fach muss in jedem Fall vorgenommen werden. Zu beachten ist auch, dass es sich nicht immer um Einführungsaufgaben handelt, sondern sich die Ideen auf die drei verschiedenen Anforderungsbereiche verteilen. Dementsprechend muss zum Teil bereits ein gewisses Maß an Anwendungskompetenz oder Inhaltswissen bei den Schülerinnen und Schülern vorhanden sein, um manche der Ideen mit einer Lerngruppe umsetzen zu können.

Generell eignen sich die Handreichungen auch als Grundlage für Prozesse der Schulentwicklung beziehungsweise für die Arbeit in Fachschaften. Die konkreteren Inhalte können dabei vor allem bei der Einbindung

---

1 KMK: Bildung in der digitalen Welt Strategie der Kultusministerkonferenz. 2016, Berlin. URL: https://www.kmk.org/themen/bildung-in-der-digitalen-welt/strategie-bildung-in-der-digitalen-welt.html (24.01.2024).

2 Ministerium für Bildung, Wissenschaft und Kultur des Landes Schleswig-Holstein (Hg.): Ergänzung zu den Fachanforderungen Medienkompetenz. Lernen mit digitalen Medien. Allgemein bildende Schulen Sekundarstufe I Sekundarstufe II. 2018, Kiel. URL: https://fachportal.lernnetz.de/sh/fachanforderungen.html (24.01.2024). [unter „Fachübergreifende Ergänzungen“].

3 vgl. https://fachportal.lernnetz.de/sh/fachanforderungen.html (unter dem jeweiligen Unterrichtsfach).

4 KMK: Kompetenzen in der digitalen Welt. 2016, Berlin. URL: https://www.kmk.org/themen/bildung-in-der-digitalen-welt/strategie-bildung-in-der-digitalen-welt.html (24.01.2024). [unter „Schulen und berufliche Bildung“ – „Kompetenzrahmen“].

der KMK-Kompetenzen in das schulinterne Fachcurriculum hilfreich sein.

Im Rahmen der Fortbildungsplanung an der Schule können die Handreichungen in Kombination mit dem IQSH-Papier „Lehren und Lernen in der digitalen Welt. Perspektiven zur Kompetenzentwicklung in der Aus- und Fortbildung von Lehrkräften an allgemeinbildenden Schulen in Schleswig-Holstein“[5] außerdem einen Ausgangspunkt für die Personalentwicklung im Bereich Medienbildung darstellen.

[5] Institut für Qualitätsentwicklung an Schulen Schleswig-Holstein (IQSH): Lehren und Lernen in der digitalen Welt. Perspektiven zur Kompetenzentwicklung in der Aus- und Fortbildung von Lehrkräften an allgemeinbildenden Schulen in Schleswig-Holstein. 2023, Kiel. URL: https://publikationen.iqsh.de/lernen-mit-digitalen-medien/lehren-und-lernen-in-der-digitalen-welt.html (24.01.2024).

2 Kompetenzeinordnung

Datenschutz ist in den Fachanforderungen beziehungsweise in deren Ergänzung im Kompetenzbereich „K4 Schützen und sicher Agieren" verankert. Gleichzeitig ist auch die Fähigkeit, Medien zu analysieren und zu reflektieren, wichtig, um bewusst mit den eigenen Daten umgehen zu können. Daher bezieht sich die vorliegende Handreichung ebenfalls auf den Kompetenzbereich „K6 Analysieren und Reflektieren".

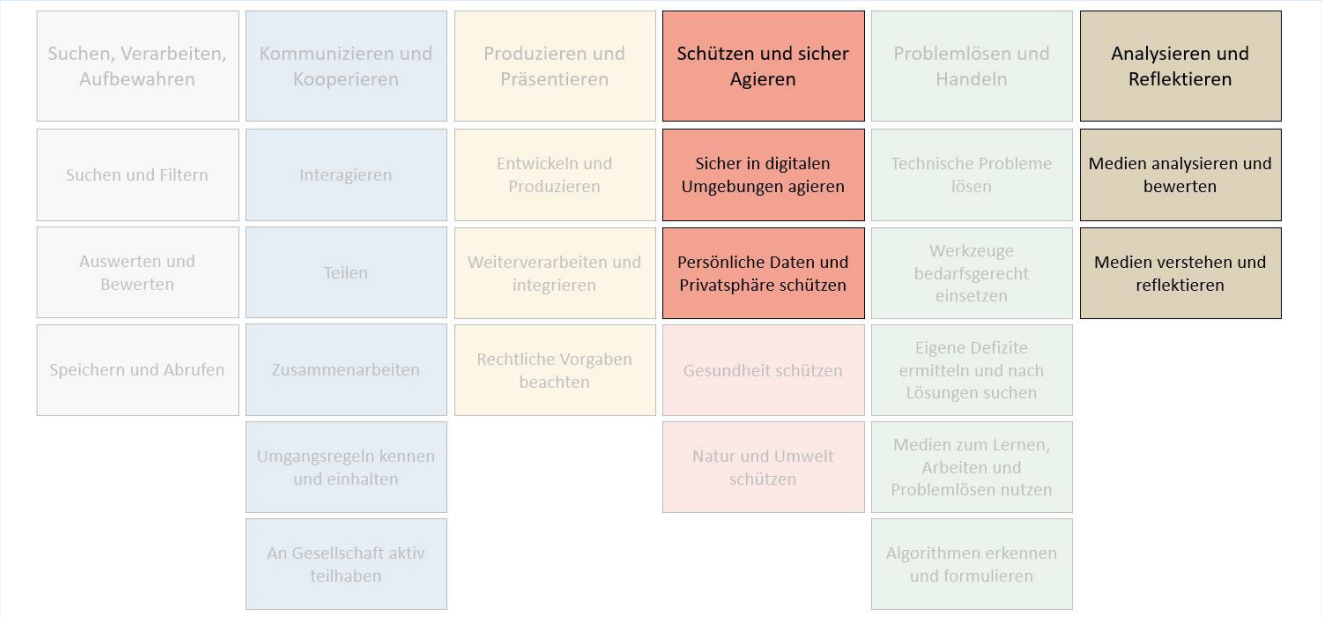

Abbildung 1: Einordnung der Handreichung in die sechs Kompetenzbereiche der KMK; CC BY-NC 4.0 Jens Lindström, IQSH

Die vorliegende Handreichung nimmt das Thema „Digitale Mündigkeit" in den Blick. Es geht dabei darum, Verantwortung für das eigene Handeln im digitalen Raum zu übernehmen. Eine wichtige Voraussetzung dafür ist, selbstbestimmt mit den eigenen Daten umgehen zu können. Daher ist Datenschutz ein zentraler Aspekt der folgenden Ausführungen. Dabei wird zunächst auf die Möglichkeiten zur Erhebung von Daten und die Gründe, aus denen diese Erhebungen vorgenommen werden, eingegangen. Anschließend stehen Möglichkeiten, wie man Daten selbst schützen kann, im Fokus.

Im Umgang mit diesem Thema ist eine kritische Haltung gegenüber der Erfassung und gegebenenfalls Speicherung persönlicher Daten, zum Beispiel durch Unternehmen, angelegt. Dementsprechend wird im Folgenden auf viele Gefahren des Missbrauchs von Daten eingegangen. Gleichzeitig soll an dieser Stelle darauf hingewiesen werden, dass es viele gute Gründe gibt, Daten zu verarbeiten. Zudem handelt es sich beim Datenschutz um ein Persönlichkeits-, also Individualrecht. Häufig hängt es somit auch vom Individuum ab, ob eine Datenverarbeitung als positiv, negativ oder neutral angesehen wird. Beispielsweise kann die langfristige Speicherung von Cookies den Komfort bei der Bedienung einer durch den Nutzer beziehungsweise die Nutzerin häufig besuchten Webseite erhöhen, zeitgleich werden dem Webseitenbetreiber gegenüber gegebenenfalls mehr Daten als nötig offengelegt. Ebenso freuen sich einige Menschen über personalisierte Werbung und Kaufvorschläge, während andere Menschen vielleicht befürchten müssen, aufgrund von personalisierter Werbung zum Beispiel als transgender[6] geoutet zu werden.

Wichtig im Kontext der digitalen Mündigkeit ist, dass die Entscheidung – etwa über die Inanspruchnahme eines be-

[6] Queer Lexikon: „Transgender", 08.06.2017. URL: https://queer-lexikon.net/2017/06/08/transgender/ (24.01.2024).

stimmten Angebots oder die Angabe bestimmter Daten – unter Berücksichtigung der möglichen Konsequenzen für einen selbst und die Gesellschaft getroffen wird. Hierzu gehört unter anderem, sich mit den verschiedenen Gründen auseinandergesetzt zu haben, die dafür sprechen, sorgsam mit den eigenen Daten und den Daten anderer im digitalen Raum umzugehen: Zum Beispiel könnten Firmen ein Interesse daran haben, Personen entsprechend der gewonnenen Daten Werbung anzuzeigen, wofür sie gegebenenfalls detaillierte Persönlichkeitsprofile erstellen. Staaten könnten durch das Erheben von Daten die Einhaltung ihrer Gesetze sicherstellen. Je nachdem, in welchem Staat ein Mensch lebt, kann das mehr oder weniger problematisch sein. Betrüger könnten gestohlene oder anderweitig erworbene Daten so nutzen, dass sie sich von den betroffenen Menschen Geld erschleichen können. Digitale Straftäterinnen und Straftäter könnten die Geräte und Accounts ihrer Opfer und dadurch die Opfer selbst mithilfe von Schadsoftware kontrollieren. Zu all diesen potenziellen Szenarien gibt es im Folgenden kleine Beispiele um zu zeigen, dass der Schutz von Daten vor allem dem Schutz von Menschen dient.

3 Wozu werden Daten im digitalen Raum erhoben?

Wenn es um die Erhebung von Daten im digitalen Raum, insbesondere dem Internet, geht, ist es wichtig zu wissen, dass nicht nur die Daten erfasst werden, die Nutzende bewusst preisgeben, zum Beispiel, wenn sie sich bei einem Dienst registrieren. Einige Daten werden beispielsweise auch beim regulären „Surfen" über den Web-Browser erhoben. Hierzu gehören unter anderem die IP-Adresse[7], der Zugriffszeitpunkt, die Browser-Version und die Bildschirmauflösung. Darüber hinaus gibt es viele weitere Daten, die angebotsabhängig erfasst werden können wie zum Beispiel die Verweildauer auf einer Seite, die Mausbewegungen während des Webseitenbesuchs, der Pausier- oder Abbruchzeitpunkt bei einem Video sowie der Gerätestandort des genutzten Endgerätes.

Je mehr Informationen die Nutzenden zusätzlich zu den automatisch erfassten Daten bei verschiedenen Diensten im Internet hinterlegen, desto umfassender wird das Bild, dass diese Dienste über sie und gegebenenfalls auch ihr Umfeld[8] erhalten. Beispiele hierfür sind Adressdaten, Zahlungsdaten[9], Informationen über die eigenen Interessen[10], politische Ansichten, Verbindungen zu anderen Menschen und je nachdem, bei welchem Anbieter eine Person ist, werden gegebenenfalls sogar E-Mail-Inhalte ausgewertet.

Diese Informationen sammeln Unternehmen und Organisationen aus verschiedenen Gründen, etwa um ihre Produkte und Dienstleistungen zu verbessern, Trends und Muster in der Gesellschaft zu erkennen oder auch, um einzelne Personen oder Personengruppen gezielter ansprechen zu können. Dabei ist die Erhebung von Daten nicht grundsätzlich problematisch. Viele Dienstleistungen sind ohne das Verarbeiten von Daten gar nicht möglich. Um die Interessen von Unternehmen, Organisationen, Behörden und Nutzenden in Einklang zu bringen gibt es Datenschutzgesetze wie die Datenschutz-Grundverordnung (DSGVO); auf diese wird in Kapitel 4 näher eingegangen. Zur digitalen Mündigkeit gehört wiederum, dass die Nutzenden selbst in der Lage sind abzuwägen, ob bestimmte Angebotsbedingungen ihrer Ansicht nach vertretbar sind und ob sie das Angebot entsprechend uneingeschränkt, nach Ergreifung zusätzlicher technischer Maßnahmen (zum Beispiel anonymer Browser, Adblocker, Pseudonym) oder auch gar nicht nutzen möchten.

Mehr Informationen

Weitere Informationen zum Thema „Datenerhebung im Internet" finden sich beim Projekt „Datenparty" des Landesjugendring-Saar e. V.: https://www.jugendserver-saar.de/fileadmin/datenparty/index653c.html?id=1948 (13.02.2024)

[7] „IP" steht für „Internet Protocol". Dabei handelt es sich um eine individuelle Adresse pro Haushalt bzw. Standort, die Geräten zugeordnet wird, wenn sie mit dem Internet verbunden sind.

[8] Die im Smartphone gespeicherten Kontakte können von Apps, beispielsweise Messengern, genutzt werden um herauszufinden, wer in der Kontaktliste ebenfalls die entsprechende App nutzt. Es werden jedoch auch die Kontakte derjenigen erfasst, die diese App nicht nutzen und dies vielleicht auch nicht möchten.

[9] Wer in einem Onlineshop einkaufen möchte, muss dort meistens die eigenen Zahlungsinformationen hinterlegen, zum Beispiel eine IBAN für den Lastschrifteinzug, eine Kreditkarte oder eine PayPal-Adresse.

[10] Musikgeschmack, Lieblingsfilme und dergleichen mehr werden vor allem in Social-Media-Accounts eingegeben. Ist die Einsicht in das Profil nicht auf einen begrenzten Personenkreis eingestellt, ist dieses dann öffentlich zugänglich (mindestens innerhalb des jeweiligen Netzwerks).

3.1 Welchen Einfluss kann personalisierte Werbung haben?

Viele Firmen (zum Beispiel Google, Netflix und Meta[11]) haben ein Interesse an personenbezogenen Daten der Nutzenden. Je mehr Daten einer Firma zur Verfügung stehen, desto genauere Profile können über einzelne Personen oder Personengruppen erstellt werden. Je größer zum Beispiel ein soziales Netzwerk ist, desto mehr Daten stehen zur Analyse zur Verfügung (Kontakte, Likes, Antworten aus Persönlichkeitstests, Standortdaten und so weiter). Diese Datensätze können durch hinzugekaufte Datensätze anderer Firmen ergänzt und vergrößert werden. Auf diese Weise entstehen sehr große Datenmengen (Big Data), die mithilfe künstlicher Intelligenz (KI) ausgewertet werden. Bei der Analyse dieser großen Menge an Informationen ist die KI in der Lage, Zusammenhänge zwischen den Daten zu erkennen, die ein Mensch nicht entdecken würde. Dadurch können sehr genaue Persönlichkeitsprofile aller Nutzenden erstellt werden. Je besser eine Firma eine Userin beziehungsweise einen User kennt, desto besser kann sie versuchen, diese Person zu beeinflussen, zum Beispiel über gezielte und gesteuerte Werbung oder über besonders anregende Inhalte. So versuchen viele Firmen, die Nutzenden so lange und so oft wie möglich auf ihren Seiten zu haben, entweder, weil sie direkt Geld bezahlen, um das Angebot zu nutzen, oder damit sie so viel Werbung wie möglich zu sehen bekommen. Denn wenn Firmen kein Geld von den Nutzenden nehmen, finanzieren sie sich in der Regel damit, Werbung zu schalten oder die Daten der Nutzenden an Werbeunternehmen zu verkaufen.[12] Die Werbetreibenden wiederum können potenziell Einfluss auf die Kaufentscheidungen der Nutzenden nehmen, ihren Blick auf die Welt beeinflussen und ihre politischen Ansichten manipulieren. Dass diese Beeinflussungsversuche ein reales Risiko sind, zeigt sich immer wieder.

Wie persönliche Daten zur Generierung von Werbung genutzt werden, zeigt eine Aktion der Non-Profit-Organisation „Signal". Diese hat im Jahr 2021 Instagram-Werbeflächen gekauft, um sichtbar zu machen, wie personalisierte Werbung funktioniert. Hierfür hat sie in ihren Werbeanzeigen einige der höchst persönlichen Kriterien dargestellt, nach denen ausgewählt wird, warum eine bestimmte Person eine bestimmte Werbung angezeigt bekommt. So lautetet eine dieser Werbeanzeigen (frei übersetzt): „Du siehst diese Werbung, weil du ein frisch verheirateter Pilates Lehrer bist und Cartoons liebst. Diese Werbung hat deine Ortsfreigabe genutzt, um zu sehen, dass du dich in La Jolla befindest. Du liest gerne Blogs zu Elternschaft und denkst über LGBTQ Adoption nach". Die Aktion wurde auf dem englischsprachigen Signal-Blog dokumentiert.[13]

Ein Beispiel der politischen Meinungsmanipulation mithilfe von Werbung unter anderem in den sozialen Medien liefert der 2018 aufgedeckte „Cambridge-Analytica-Skandal". Hierbei handelt es sich um einen der bekanntesten dokumentierten Fälle von sogenanntem politischen Micro-Targeting. In diesem Fall „[wurde] ein ganzes Informationsökosystem von Webseiten und Blogs aufgesetzt […], die nicht als Teil der Trump-Kampagne erkennbar waren. Sie seien genutzt worden, um Wähler gezielt mit vermeintlich unabhängigen Informationen zu versorgen, für die sie laut ihrem Profil besonders ansprechbar sind. So seien Wähler immer genau mit den Forderungen und Versprechen Trumps bespielt worden, die bei ihnen die größte Wirkung erzielen würden."[14] Zeitgleich sollten Trump gegenüber skeptisch einstellte Personengruppen mithilfe gezielter Anzeigen demotiviert werden, ihre Stimme überhaupt abzugeben.

Der Schutz der eigenen Daten ist also unter anderem ein Schutz davor, zum Spielball der Interessen anderer zu werden. Er verhilft Menschen dazu, Entscheidungen selbstbestimmt zu fällen, ihre Interessen zu vertreten und diese gegenüber anderen durchzusetzen.

Mehr Informationen

Im Abschnitt „Weiterführende Literaturhinweise und Angebote" finden sich einige jugendgerechte Videos des Funk-Formats „SoManyTabs" darüber, welche Daten verschiedene Konzerne über ihre Nutzenden sammeln.

[11] Meta ist der Konzern, zu dem Facebook, Instagram und WhatsApp gehören.

[12] Netzpolitik.org: „Datenhändler verticken Handy-Standorte von EU-Bürger*innen", 17.01.2024. URL: https://netzpolitik.org/2024/berliner-unternehmen-datenhaendler-verticken-handy-standorte-von-eu-buergerinnen/ (31.01.2024).

[13] Signal Blog: „The Instagram ads Facebook won't show you", 04.05.2021. URL: https://signal.org/blog/the-instagram-ads-you-will-never-see/ (16.01.2024).

[14] Netzpolitik.org: „Was wir über den Skandal um Facebook und Cambridge Analytica wissen", 21.03.2018. URL: https://netzpolitik.org/2018/cambridge-analytica-was-wir-ueber-das-groesste-datenleck-in-der-geschichte-von-facebook-wissen/ (16.01.2024).

Ein Beispiel dafür, wie die vermeintlich problemlose Erhebung von Daten auf einmal das eigene Leben beeinflussen kann, ist die neue Situation in den USA, nachdem dort das Abtreibungsrecht gekippt wurde: Plötzlich können Informationen, die zum Beispiel in Menstruations-Apps gesammelt werden, von Interesse für Strafverfolgungsbehörden sein.[15] Eine digital dokumentierte ausbleibende Periode kann einen Hinweis darauf liefern, dass eine Person schwanger ist beziehungsweise schwanger war. Deswegen rufen Pro-Choice-Aktivistinnen in den USA dazu auf, Menstruations-Apps zu löschen. Welche Fülle an Daten solche Apps sammeln, wurde bereits 2021 von „SoManyTabs" in einem Video beleuchtet.[16]

Ein extremes Beispiel dafür, wie durch veränderte Umstände eine unter guten Absichten erstellte Datensammlung für die Betroffenen gefährlich werden kann, ist der Systemwechsel in Afghanistan. Das US-Militär hat während des Hilfseinsatzes bis 2021 biometrische Daten (zum Beispiel Fingerabdrücke, Iris-Scans) sogenannter Ortskräfte erfasst. Das sind Menschen vor Ort, die das US-Militär unterstützt haben. Nach dem Abzug der Truppen und der Machtübernahme durch die Taliban haben die Taliban von den US-Truppen zurückgelassene biometrische Gesichts-Scanner beschlagnahmt. Dadurch haben die Taliban potenziell Zugriff auf die gesamte Datenbank erlangt und wurden dadurch möglicherweise in die Lage versetzt, in Afghanistan verbliebene Ortskräfte bei Kontrollen zu identifizieren. So wurde die Sicherheit der verbliebenen Ortskräfte gefährdet. Auch vermeintlich harmlose Online-Profile in sozialen Netzwerken können den Menschen in Afghanistan nach dem Machtwechsel gefährlich werden.[17] Dieser Punkt wird auch für Menschen hier in Deutschland relevant. Denn alle können dazu beitragen, andere Personen nicht unnötig zu gefährden, indem sie überlegen, ob Informationen, die sie über andere oder mit anderen per Messenger oder in den sozialen Netzwerken teilen, eine Gefahr für diese Menschen darstellen können.

3.2 Wofür nutzen Kriminelle die eigenen Daten und wie kann man sich schützen?

Fast alle Menschen, die eine E-Mail-Adresse besitzen und diese in verschiedenen Online-Accounts hinterlegt haben, haben schon einmal sogenannte Phishing-E-Mails erhalten. Ein häufiges Ziel von Phishing ist es, die betroffenen Personen unbemerkt dazu zu bringen, persönliche Zugangsdaten zum Beispiel zu ihrem Online-Banking oder zu Online-Zahlungsdiensten wie PayPal preiszugeben. Hierfür erstellen die Kriminellen eine Webseite, die so aussieht wie die Login-Seite zum Beispiel von PayPal oder der Postbank. Dann verschicken sie massenhaft E-Mails, die zum Beispiel besagen, dass ein unbefugter Zugriff auf das eigene Konto stattgefunden hat und dass daher das Passwort umgehend geändert werden sollte. Die Phishing-E-Mail enthält dann einen Link zu der gefälschten Seite. Wenn die Empfängerinnen und Empfänger der Aufforderung folgen und den gefälschten Link nutzen, um sich in ihren vermeintlichen Account einzuloggen, werden die Zugangsdaten an die Betrügenden übertragen. Diese können die Daten dann nutzen, um über das Geld auf dem Konto zu verfügen. Phishing kann aber auch für andere Zwecke genutzt werden, zum Beispiel um an die Zugangsdaten von Social-Media-Accounts zu kommen und die betroffenen Personen zu erpressen, öffentlich bloßzustellen oder über den Account an andere mit der „gehackten" Person verbundene Kontakte heranzukommen. Das Funk-Video „Passwort-Fails – die FÜNF größten EVER" zeigt, dass das Erschleichen von Zugangsdaten per Phishing auch ohne das Versenden von E-Mails funktionieren kann (ab 3:16 Min, Passwort-Fail Nummer 3 – Wie Twitter zum Phishing-Opfer wurde).[18]

Phishing ist zudem auch eine mögliche Methode, mit der digitale Gewalttäterinnen und Gewalttäter, wie zum Beispiel Stalker und Stalkerinnen, versuchen, näher an ihre Opfer heranzukommen. Wenn die Täter ihre Opfer bereits persönlich gut kennen oder es sich um digitale häusliche Gewalt handelt, gibt es hierfür auch direktere Methoden, wie zum Beispiel den Missbrauch von AirTags beziehungsweise der „find my phone"-Funktion zum Ver-

[15] Netzpolitik.org: „Viele Menstruations- und Schwangerschaftsapps erfassen sensible Daten", 23.08.2022. URL: https://netzpolitik.org/2022/datenschutz-viele-menstruations-und-schwangerschaftsapps-erfassen-sensible-daten/ (16.01.2024).

[16] SoManyTabs: „Können wir Menstruations-Apps wie Flo & Co trauen?", 05.05.2021. URL: https://www.funk.net/channel/somanytabs-12189/koennen-wir-menstruationsapps-wie-flo-co-trauen-mit-maria-von-aufklo-1736478 (16.01.2024).

[17] Netzpolitik.org: „Vom Facebook-Profil auf die Verhaftungslisten der Taliban", 25.08.2021. URL: https://netzpolitik.org/2021/afghanistan-vom-facebook-profil-auf-die-verhaftungslisten-der-taliban/ (16.01.2024).

[18] SoManyTabs: „Passwort-Fails – die FÜNF größten EVER", 26.07.2021. URL: https://www.funk.net/channel/somanytabs-12189/passwortfails-die-fuenf-groessten-ever-1755783 (16.01.2024).

folgen von Personen oder das Installieren sogenannter „Stalkerware" auf den Geräten der Opfer.[19] Häufig wird Stalkerware in Deutschland legal, zum Beispiel als Kinderschutzsoftware, verkauft und dann missbraucht. Solche Apps sind etwa in der Lage, den Standort des Smartphones der Opfer sowie alle über das Smartphone gesendeten Nachrichten und Suchanfragen live an das Gerät des Täters beziehungsweise der Täterin zu übermitteln, ohne dass die Opfer wissen, dass diese Software auf ihren Geräten installiert ist. Daher ist es sehr wichtig, dass jedes Smartphone mit einer Zugangssperre (zum Beispiel Passwort, PIN oder Muster) versehen ist und der Zugang mit niemandem geteilt wird. Außerdem sollten Menschen in die Lage versetzt werden, ihre Geräte eigenständig einzurichten und upzudaten, sodass potenzielle Straftäter und Straftäterinnen nicht aus vermeintlicher Hilfsbereitschaft heraus Zugang zum Gerät erhalten.

In der ersten Folge von „Game of Phones" berichtet ein Betroffener davon, wie es sich für ihn angefühlt hat, als sein E-Mail-Account und in der Folge auch seine sozialen Medien gehackt wurden.[20]

Maßnahmen gegen Phishing und digitale Übergriffe:

- Für Seiten, die man nur einmal nutzen möchte, aber für welche ein Account nötig ist, kann zum Beispiel ein E-Mail-Alias oder eine „Wegwerf-E-Mail-Adresse" eingerichtet werden.[21]
- Bevor man auf einen Link in einer E-Mail oder SMS klickt, sollte die Glaubwürdigkeit des Absenders / der Absenderin überprüft werden.
- Gelangt man über einen Link in einer E-Mail beispielsweise zu der Internetseite eines Zahlungsdienstleisters, auf der man aufgefordert wird, das Passwort einzugeben, dann sollte man misstrauisch werden und stattdessen die Seite des Zahlungsdienstleisters direkt aufrufen und sich in den Account einloggen. Wichtige Benachrichtigungen sollten auch hier angezeigt werden.
- Wichtige Accounts, wie zum Beispiel der E-Mail-Account, sollten immer mit einem individuellen, sicheren Passwort geschützt sein, welches nirgendwo anders verwendet wird und niemand anderem bekannt ist (siehe hierzu auch Kapitel 4.2.1).
- Alle wichtigen Accounts sollten nach Möglichkeit mit einem zweiten Faktor abgesichert sein (siehe hierzu ebenfalls Kapitel 4.2.1).
- Wenn man seinen Standort mit einer anderen Person teilen möchte, dann sollte man das ausschließlich situationsabhängig tun, niemals durch eine generelle Freigabe.

Mehr Informationen

Ausführliche Informationen und Hilfsangebote zu (digitaler) Gewalt gibt es im Abschnitt „Weiterführende Literaturhinweise und Angebote".

[19] Süddeutsche Zeitung: „Wenn der Ex das ganze Leben überwacht", 23.12.2019. URL: https://www.sueddeutsche.de/digital/spionage-smartphone-stalkerware-stalking-app-1.4733070 (16.01.2024).

[20] Game of Phones: „Nicht gehackt werden! Sicherheit im Netz - Mit Fabian Siegismund", 02.05.2019. URL: https://soundcloud.com/gameofphones/folge-1 (16.01.2024).

[21] Wikipedia – die freie Enzyklopädie: „E-Mail-Konto", 15.12.2023. URL: https://de.wikipedia.org/w/index.php?title=E-Mail-Konto&oldid=240222772#Alias-Adressen_und_Wegwerf-E-Mail-Adressen (16.01.2024).

4 Digitale Souveränität und digitale Mündigkeit

Der Begriff „digitale Souveränität" hat verschiedene Auslegungen, je nachdem, wer ihn benutzt. Eine mögliche Auslegung ist eine politische, nationalstaatliche digitale Souveränität. Hierbei ist das Ziel, dass einzelne Staaten und gegebenenfalls verbündete Nationen eine von dritten Ländern unabhängige Infrastruktur haben. Ein Beispiel: Das Ziel der staatlichen digitalen Souveränität ist, dass Deutschland sein Mobilfunknetz eigenständig und ohne Einfluss anderer Staaten betreiben kann.

Daneben gibt es eine auf das Individuum bezogene Auslegung von digitaler Souveränität. Bei dieser geht es um die Fähigkeit einer Person, sich frei, selbstbestimmt und ohne Überwachung im Netz zu bewegen sowie die eigenen digitalen Geräte zu nutzen. Damit diese Souveränität erreicht werden kann, müssen einerseits gesetzliche Regelungen existieren und umgesetzt werden. Andererseits müssen Menschen eigenständig oder durch Unterstützung befähigt werden, informierte und bewusste Entscheidungen in der digitalen Welt zu treffen. Somit können sie auch Verantwortung für das eigene Handeln übernehmen. Letzteres wird auch unter dem Begriff „digitale Mündigkeit" zusammengefasst.

Die Sachinformationen, die zur digitalen Mündigkeit führen, lassen sich grob in die Themenbereiche „Datenschutz" und „Datensicherheit" aufteilen.

4.1 Datenschutz und informationelle Selbstbestimmung

Hinter dem Begriff „Datenschutz" versteckt sich das Recht auf informationelle Selbstbestimmung. Dieses Recht ist im Rahmen der gesellschaftlichen und gerichtlichen Auseinandersetzung über die für 1983 geplante Volkszählung und der zunehmenden elektronischen Datenverarbeitung ausformuliert worden. Das Bundesverfassungsgericht hat in der zugehörigen Entscheidung, dem sogenannten „Volkszählungsurteil", die informationelle Selbstbestimmung als Grundrecht definiert, abgeleitet vom allgemeinen Persönlichkeitsrecht und der Menschenwürde, also direkt aus dem Grundgesetz (GG). Anbei zwei kleine Abschnitte aus der Urteilsbegründung, die heute immer noch hochaktuell sind: „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen." Das Gericht warnt hier also vor sogenannten „Chilling Effects", einer Verhaltensanpassung an gesellschaftliche Normen aus Angst vor negativen Konsequenzen. Weiter heißt es: „Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus."[22]

Die informationelle Selbstbestimmung auf Basis des Grundgesetzes ist also nicht ein Recht neben vielen anderen, sondern hat ein besonderes Gewicht. Zusammenfassend heißt das, dass es das Ziel des Datenschutzes ist, das Recht auf informationelle Selbstbestimmung zu gewährleisten. Der Schutz der personenbezogenen Daten ist dabei nur das Mittel für diesen Zweck, denn es geht im Kern um den Schutz von Menschen. In der Europäischen Grundrechtecharta ist das Recht in Artikel 8 explizit definiert und es wird durch die Datenschutzgrundverordnung (DSGVO) konkretisiert.

[22] BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209/83 -, Rn. 1-215. URL: https://www.bverfg.de/e/rs19831215_1bvr020983.html (16.01.2024).

4.1.1 Datenschutzgrundverordnung (DSGVO)

Die DSGVO wurde von der Europäischen Union (EU) eingeführt, um die Grundrechte der Menschen in der EU (also auch in Deutschland) sicherzustellen. Alle Menschen sollen selber darüber entscheiden können, welche Informationen (personenbezogene Daten) sie mit anderen Menschen und vor allem auch Behörden und Unternehmen teilen und welche nicht. Die DSGVO gilt nicht im persönlichen oder familiären Bereich. Ein Beispiel für diese sogenannte „Haushaltsausnahme" ist das Teilen von Bildern in der Familie oder unter Freunden. Wenn die Bilder allerdings einer größeren Gruppe zur Verfügung gestellt werden, gilt sie schon.

Wenn die DSGVO greift, gilt erst einmal: Jede Verarbeitung[23] von personenbezogenen Daten[24] ist verboten. Damit die eigenen personenbezogenen Daten doch durch andere verarbeitet werden dürfen, muss zunächst einmal klar sein, was (welche Daten) warum (Zweck) verarbeitet werden soll. Außerdem bedarf es einer Ausnahme (der sogenannten Rechtsgrundlage). Alle Rechtsgrundlagen stehen in Artikel 6 der DSGVO. Diese können gegebenenfalls durch Regelungen in nationalen Gesetzen wie dem Bundesdatenschutzgesetz (BDSG), dem Landesdatenschutzgesetz (LDSG) oder auch der Schuldatenschutzverordnung (SchulDSVO)[25] konkretisiert werden.

Beispiele für Rechtsgrundlagen:

- Vertragserfüllung: Wenn jemand eine Pizza nach Hause bestellt, geht das nur, wenn die Person ihren Nachnamen und ihre Adresse angibt.
- Einwilligung: Wenn jemand bei einer Müllsammelaktion eines Umweltvereins mitmacht und vorher unterschreibt, dass Fotos von ihr oder ihm beim Müllsammeln im Blog des Vereins veröffentlicht werden dürfen.
  - Einwilligungen, wie sie laut DSGVO gestaltet sein sollten:
    - freiwillig (man hat eine echte Wahl; kein Zwang/Machtgefälle)
    - informiert (man hat ausreichend Informationen, um mögliche Konsequenzen einer Einwilligung abschätzen zu können)
    - endlich (man kann die Einwilligung jederzeit zurückziehen)
- Erfüllung rechtlicher Verpflichtungen: Die Schule darf einige Daten von Schülerinnen und Schülern verarbeiten, weil sie einen pädagogischen Auftrag hat, und die Schulpflicht gilt.
  - Dies sind beispielsweise der vollständige Name, die Adresse, die Telefonnummer, Konfession und rechtliche Besonderheiten (zum Beispiel in Bezug auf das Sorgerecht oder bestehende Kontaktverbote).[26]

Der Verarbeitungszweck, die Rechtsgrundlagen, welche Daten verarbeitet werden sollen und einige weitere Pflichtinformationen müssen den Betroffenen vor der Verarbeitung der Daten mitgeteilt werden, zum Beispiel über eine Datenschutzerklärung auf der Webseite einer Firma. Diese Informationen brauchen die Nutzenden, damit sie beurteilen können, ob sie ihre Daten zum Beispiel an ein soziales Netzwerk weitergeben möchten und welche Konsequenzen das Teilen der Daten für sie haben kann.

Mehr Informationen

Im Abschnitt „Weiterführende Literaturhinweise und Angebote" gibt es einige Quellen, mit deren Hilfe Datenschutz kinder- und jugendgerecht vermittelt werden kann.

[23] In der DSGVO gilt als „Verarbeitung" alles, was mit Daten gemacht werden kann: Erheben, Speichern, Übermitteln, Ändern, Löschen usw. Dabei geht es nicht nur um digitale Verarbeitung, sondern zum Beispiel auch um Papierakten.

[24] Alle Informationen, die allein oder in der Kombination mit anderen Informationen eine Person identifizierbar machen (zum Beispiel: Name, Pseudonyme, IP-Adressen, Geburtsdatum, Geschlecht, Gesundheitsdaten), sind „personenbezogene Daten".

[25] Landesverordnung über die Verarbeitung personenbezogener Daten an öffentlichen Schulen (Schul-Datenschutzverordnung – SchulDSVO) vom 18. Juni 2018. URL: https://www.gesetze-rechtsprechung.sh.juris.de/bssh/document/jlr-SchulDSVSH2018rahmen (16.01.2024).

[26] Eine vollständige Liste kann der Anlage 2 der SchulDSVO entnommen werden.

4.1.2 Allgemeine Geschäftsbedingungen (AGB)

Unternehmen haben das Recht, Regeln aufzustellen, die dann bei jeder Vertragsbeziehung, die sie eingehen, gelten. Wenn jemand zum Beispiel eine App oder einen Dienst, für den man sich registrieren muss (zum Beispiel ein soziales Netzwerk), nutzen möchte, muss die Person vorher meistens den AGB zustimmen. Diese sollte man theoretisch vor der Zustimmung gelesen haben. Praktisch tut dies aber fast niemand. In den AGB könnte aber vieles stehen, dem man eigentlich gar nicht zustimmen möchte. Deswegen ist es sinnvoll, sich zumindest grundlegend zu informieren. Hierfür eignen sich die Zusammenfassungen der wichtigsten Punkte, die zum Beispiel auf der Seite „Datenparty“[27] frei zur Verfügung stehen. Für soziale Netzwerke finden sich folgende Beispiele:

- Facebook: https://www.jugendserver-saar.de/fileadmin/datenparty/indexff06.html?id=1984 (13.02.2024)
- Instagram: https://www.jugendserver-saar.de/fileadmin/datenparty/index3652.html?id=2300 (13.02.2024)
- Snapchat: https://www.jugendserver-saar.de/fileadmin/datenparty/index405d.html?id=2301 (13.02.2024)
- TikTok: https://www.jugendserver-saar.de/fileadmin/datenparty/index8dcb.html?id=2302 (13.02.2024)

Unabhängig davon werden Menschen in Deutschland aber auch durch das Gesetz geschützt. Im Bürgerlichen Gesetzbuch (BGB) ist geregelt, was in AGB stehen darf und was nicht. AGB dürfen zum Beispiel nicht überraschend sein. Wenn man einem sozialen Netzwerk beitritt und in den AGB steht, dass man mit dem Beitritt auch ein Auto kauft, dann konnte man das nicht erwarten und genau der Teil der AGB, der den Autokauf beinhaltet, ist dann ungültig.

4.1.3 Datensparsamkeit

Die beste Möglichkeit zu verhindern, dass andere Informationen über die eigene Person bekommen, die sie nicht haben sollen, ist, diese Informationen gar nicht erst zu erzeugen. Wenn man zum Beispiel nicht möchte, dass eine App weiß, wo man sich befindet, dann kann man in den Smartphone-/Tablet-Einstellungen die Ortsfreigabe für diese App verbieten. Wenn es eine alternative App mit derselben Funktionalität gibt, die weniger Daten von den Nutzenden haben möchte, dann kann diese Alternative benutzt und die wissbegierige App deinstalliert werden. In den sozialen Medien kann man einstellen, welcher Personenkreis die eigenen Inhalte sehen darf: die eigenen Freunde oder alle Menschen, die dasselbe soziale Netzwerk nutzen. Trotz der maximalen Privatsphäre-Einstellungen kann es vorkommen, dass dem genutzten Dienst Daten gestohlen und diese dann verkauft oder öffentlich ins Internet gestellt werden. Daher gilt auch bei vermeintlich privaten Daten im Internet, dass ein Datenleck nie zu 100 % ausgeschlossen werden kann. Man sollte sich also bereits vor dem Hochladen immer die Fragen stellen, was wäre, wenn diese Daten sichtbar im Netz landen würden. Wäre das in Ordnung?

Falls es doch einmal vorkommen sollte, dass private Daten im Netz gelandet sind, gibt es verschiedene Dinge, die man tun kann:

- Wenn man selbst die Inhalte online gestellt hat: Löschen.
- Wenn andere Personen Bilder/Inhalte veröffentlicht haben:
  - Beweise per Screenshot sichern: Wichtig ist, dass Datum, Uhrzeit und URL auf dem Screenshot zu sehen sind.
  - Inhalte melden, falls es eine Meldefunktion gibt.
  - Zusätzlich zum Melden per Kontaktformular beziehungsweise über die im Impressum angegebenen Kontaktdaten zum Löschen auffordern.

Eine ausführliche Anleitung, was bei Nacktbildern im Netz zu tun ist, gibt es bei „Anna Nackt“.[28] Die beschriebenen Schritte gelten aber auch für andere Inhalte, die ohne Einverständnis geteilt wurden. Ebenfalls empfehlenswert ist das jugendgerechte Video „Nackt im Netz: Was tun?! (Sexting, geleakte Fotos)“ des Funk-Formats

[27] Hierbei handelt es sich um ein Projekt des Landesjugendring-Saar e. V.

[28] Anna nackt: Was-tun-Guide. URL: https://annanackt.com/was-tun (16.01.2024).

„SoManyTabs".[29] Das Video beinhaltet einerseits Tipps zur Vorbeugung von Leaks beim Versand intimer Bilder, sogenanntes „Safer Sexting". Andererseits gibt es Hinweise zum Umgang mit bereits veröffentlichten Bildern. Diese Tipps sind ebenfalls auf andere Arten von sensiblen Daten übertragbar.

Neben möglichen Datenpannen ist es auch wichtig, dass man den Menschen vertraut, mit denen man private Informationen teilt. Wenn man zum Beispiel ein Foto in einer Chat-Gruppe postet, sollte man darauf achten, ob alle Menschen in dieser Gruppe sensibel mit den eigenen Daten umgehen und diese zum Beispiel nicht ungefragt an andere weiterleiten. Man kann dem Bild gegebenenfalls den Hinweis hinzufügen, dass es die Gruppe nicht verlassen soll. Sobald ein Foto / eine Information / eine Nachricht das eigene Handy oder den Computer verlässt, kann sie von anderen Menschen/Computern gesehen/gespeichert worden sein. Egal wie lang oder kurz sie am anderen Ort verfügbar war. Auch technische Hilfen wie selbstlöschende Nachrichten bieten keinen Schutz, wenn die Person am anderen Ende die Information vorher anderweitig gespeichert hat.

Beim Thema Datensparsamkeit geht es auch um den verantwortungsvollen Umgang mit den Daten anderer Menschen. Wenn sich zum Beispiel eine Person bewusst gegen die Nutzung sozialer Medien entscheidet, sollte man nicht einfach (ungefragt) Bilder oder Videos, auf denen diese Person zu sehen ist, in die sozialen Medien hochladen.[30] Im schlimmsten Fall versucht die Person, sich zum Beispiel vor einem Stalker oder einer Stalkerin zu schützen und das geteilte Foto (inklusive Location) verrät ihm oder ihr, wo das Opfer sich befindet.

Mehr Informationen

In dem beschriebenen Beispiel ist auch allgemein das Recht am eigenen Bild zu beachten. Weitere Informationen hierzu finden sich in der Handreichung „Rechtsgrundlagen der Medienproduktion".
Sie finden die Handreichung im Publikationsshop des IQSH auf der Seite: https://publikationen.iqsh.de/dm-medienbildung.html. Die Handreichungen zur Medienkompetenz werden sukzessive eingestellt.

Mehr Informationen

Weitere Denkanstöße und praktische Tipps zur bewussteren Nutzung digitaler Ressourcen gibt es zum Beispiel im Rahmen des Data Detox Kits unter https://datadetoxkit.org/de/home.[31]

4.1.4 Cookies

Wenn man eine Webseite aufruft, werden durch diese Webseite häufig Cookies gesetzt. Cookies sind Textdateien mit Informationen über die Nutzerin oder den Nutzer beziehungsweise das genutzte Gerät, die im Browser gespeichert werden. Es gibt aber auch Webseiten, die ganz ohne Cookies auskommen.

Cookies haben ganz unterschiedliche Funktionen. Ein klassischer Grund für Webseitenbetreiber, Cookies zu benutzen, ist, die persönliche Online-Erfahrung angenehmer zu gestalten. Wenn man zum Beispiel einen Online-Shop nutzt und einen Artikel in den Warenkorb legt, wird diese Information in einem Cookie gespeichert. Würde das nicht passieren, müsste man bei jedem Aufruf einer neuen Unterseite, zum Beispiel der Seite zum Bezahlen, erneut sagen, was man kaufen wollte.[32]

Jede Person, jeder Verein, jede Firma und jede Behörde, die eine öffentliche Webseite betreibt, ist durch EU-Gesetze dazu verpflichtet, die Besucherinnen und Besucher

[29] SoManyTabs: „Nackt im Netz: Was tun?! (Sexting, geleakte Fotos)", 06.05.2021. URL: https://www.funk.net/channel/somanytabs-12189/nackt-im-netz-was-tun-sexting-geleakte-fotos-1745187 (16.01.2024).

[30] YoungData: Das „Recht am eigenen Bild". URL: https://www.youngdata.de/recht-am-eigenen-bild/ (16.01.2024).

[31] Tactical Tech: „Data Detox Kit", 20.09.2021. URL: https://datadetoxkit.org/de/home (16.01.2024).

[32] Verbraucherportal Baden-Württemberg: „Cookies – hilfreich oder gefährlich", 09.02.2023. URL: https://www.verbraucherportal-bw.de/,Lde/Startseite/Verbraucherschutz/Cookies+_+hilfreich+oder+gefaehrlich_ (16.01.2024).

der Seite über alle Cookies aufzuklären, die verwendet werden sollen. Außerdem dürfen ohne Einwilligung rein rechtlich keine Cookies im Browser gespeichert werden, es sei denn, es handelt sich um sogenannte technisch notwendige Cookies. Deswegen liefert fast jede Webseite direkt nach dem Aufrufen ein sogenanntes Cookie-Consent-Banner, mit dessen Hilfe man die eigenen Cookie-Einstellungen für die Webseite festlegen kann. Wie lange ein Cookie gespeichert wird, wird durch den Webseitenbetreiber festgelegt. Man kann Cookies in den Browser-Einstellungen aber auch manuell löschen, eine maximale Lebensdauer festlegen oder einstellen, dass alle Cookies bei jedem Schließen des Browsers gelöscht werden.

Es wird zwischen verschiedenen Cookies unterschieden. Es gibt sogenannte technisch notwendige oder essenzielle Cookies, ohne die einige Webseiten gar nicht genutzt werden können. Dann gibt es sogenannte funktionale Cookies, die dafür sorgen, dass bestimmte Funktionen der Webseite (komfortabel) nutzbar sind, wie zum Beispiel der Warenkorb. Außerdem gibt es sogenannte Analyse-Cookies, die für statistische Zwecke genutzt werden, zum Beispiel damit die Betreibenden einer Webseite wissen, wie oft die Seite täglich aufgerufen wird oder welche Unterseiten besonders beliebt sind. Diese Daten können anonym oder personenbezogen erfasst werden. Wenn Analysedaten personenbezogen erfasst werden, nutzen die Webseitenbetreibenden sie in der Regel nicht nur für die Verbesserung der jeweiligen Seite, sondern auch, um den Nutzenden passendere Produkte zu zeigen, zum Beispiel um mehr verkaufen zu können oder um die Nutzerinnen und Nutzer länger auf der Webseite zu halten. Eventuell wird das Profil, das so über eine Person erstellt wurde, aber auch an andere Personen oder Unternehmen weiterverkauft. Wenn mithilfe von Cookies nicht nur die Nutzungsdaten der Webseite, auf der man sich befindet, erfasst werden, sondern auch Informationen darüber, welche Webseiten jemand sonst noch besucht, handelt es sich um sogenannte Tracking Cookies.

4.1.5 Tracking und seine Folgen

Tracking lässt sich besonders gut anhand von personalisierter Werbung erklären. Werbung im Internet funktioniert auf den ersten Blick ähnlich wie Werbung auf der Straße oder Werbung in Zeitschriften. Es gibt feste Werbeflächen, die für das Anzeigen von Werbung gekauft werden können. Wenn jemand eine Firma hat, die veganen Fleischersatz verkauft, dann kauft die Person vermutlich Werbeflächen in Stadtteilen, in denen bei der letzten Wahl viele Menschen „die Grünen" oder „die Tierschutzpartei" gewählt haben. Wenn die Person Werbeflächen in Zeitschriften kauft, macht sie das wahrscheinlich eher in einer Zeitschrift, die ökologische Themen behandelt als in einem Comic-Heft für Kinder. Hierbei handelt es sich um kontextualisierte Werbung. Die Produkte beziehungsweise Themen, für die geworben wird, richten sich danach, wo die Werbeflächen sich befinden, weil aus dem Kontext abgeleitet wird, dass möglichst viele Personen der jeweiligen Zielgruppe die Werbung sehen werden. Dieses Prinzip funktioniert online genauso wie offline.

Personalisierte Werbung gibt es dagegen ausschließlich im Internet, weil die Werbeinhalte hierbei von der betrachtenden Person abhängen und nicht vom Ort der Werbefläche. Auf der Straße sehen alle Menschen dieselbe Werbung. Im Internet „weiß" die Werbefläche meistens, wen sie vor sich hat. Deswegen wird jeder Person die Werbung angezeigt, bei der die Wahrscheinlichkeit am größten ist, dass sie das gezeigte Produkt kauft beziehungsweise die ihre Meinung im Interesse der Werbetreibenden formt.

Die Frage ist nun, woher die Online-Werbetafel weiß, wer vor ihr steht und welche Inhalte sie anzeigen soll. Was die Person sieht, wird aufgrund umfangreicher Persönlichkeitsprofile entschieden, die zum Beispiel wie in Kapitel 3.1 beschrieben erstellt werden. Zudem fließen weitere Informationen in das Profil ein. Hierfür werden vor allem Tracking und Fingerprinting genutzt. Der Begriff „Tracking" (engl. Verfolgung) beschreibt ganz allgemein erst einmal die Verfolgung der eigenen Aktivitäten im Netz. Wenn zum Beispiel eine Firma jemanden „trackt", also verfolgt, dann werden alle Informationen, die sie sammelt, in einem Profil über diese Person gespeichert. Mögliche Informationen sind zum Beispiel, welche Webseiten jemand aufruft, was sich die Person auf den Webseiten wie lange anguckt und worauf sie klickt. Eine Möglichkeit, die Aktivitäten einer Person verfolgen zu können, ist das Setzen eines Tracking-Cookies beim Aufruf der Firmenseite. Noch invasiver als das Nutzen von Tracking-Cookies ist das sogenannte „Fingerprinting". Hierbei werden Informationen über das genutzte Gerät (Bildschirmauflösung, Zeit-/Spracheinstellungen, Schriftarten, …) beziehungsweise den genutzten Browser (Typ, installierte Plugins, Sprachen, …) gesammelt und dadurch die Person und ihre genutzten Geräte identifiziert.

Die unter anderem durch Tracking erstellten beziehungsweise ergänzten Persönlichkeitsprofile werden nicht nur durch Werbetreibende genutzt, sondern können zum Beispiel auch zur automatischen Entscheidungsfindung verwendet werden. Ein klassisches Beispiel hierfür ist das sogenannte Scoring, mit dessen Hilfe die Entscheidung darüber vorbereitet wird, ob eine Person einen Kredit bekommt oder nicht. Problematisch hierbei ist, dass die Profile zwar sehr genau sind, doch auch hier Fehler passieren können, indem zum Beispiel Daten falsch zugeordnet werden, oder die KI, die zur Mustererkennung genutzt wurde, fehlerhaft implementiert ist. Dadurch können falsche Zusammenhänge entstehen, die in der Realität gar nicht existieren. Außerdem ist jede KI menschengemacht, das heißt die (unbewussten) Vorurteile der Menschen (Bias), die zum Beispiel in den Trainingsdaten enthalten sein können, fließen so in die KI ein.

Mehr Informationen

Weitere Informationen zu den Problemen, die im Zusammenhang mit künstlicher Intelligenz entstehen können, finden sich in der Handreichung „Recherchieren" im Abschnitt „Exkurs: Recherche mithilfe von Sprachmodellen?". Sie finden die Handreichung im Publikationsshop des IQSH auf der Seite: https://publikationen.iqsh.de/dm-medienbildung.html. Die Handreichungen zur Medienkompetenz werden sukzessive eingestellt.

Was man tun kann, um Tracking zu verhindern:

- Browser-Erweiterungen installieren, die Tracker blocken (zum Beispiel uBlockOrigin, Privacy Badger, Ghostery).
- Dienste, die entweder einen eigenen Account oder einen Login mit Google/Facebook/Microsoft/… anbieten, ausschließlich über einen eigenen Account nutzen.
- Sich aus Accounts wie Google, Amazon, Instagram, Netflix, … ausloggen, wenn man andere Dinge im Netz macht, oder unterschiedliche Browser beziehungsweise Browser-Profile nutzen.
- Den eigenen Apps den Zugriff auf Daten anderer Apps verbieten.

4.1.6 Datenschutzeinstellungen

Menschen, die sich im Internet bewegen und über das Internet miteinander interagieren, kommen nicht umhin, auch Daten über sich selbst preiszugeben. Welche Daten das sind, sollten sie möglichst einfach überblicken und somit im Optimalfall auch entscheiden können. Eine Hilfe dabei sind die Datenschutzeinstellungen. Fast jede App oder Online-Anwendung bietet den Nutzenden die Möglichkeit mitzubestimmen, welche Daten an wen weitergegeben werden. Das fängt bei den Einstellungen über die Analyse zur Verbesserung eines Angebots an und geht bis zu verschiedenen Sichtbarkeitsstufen jedes einzelnen Posts in den sozialen Medien.

Bei den verschiedenen Datenschutzeinstellungen kann vereinfacht zwischen zwei Kategorien unterschieden werden: Nutzung auf dem Smartphone/Tablet und Nutzung über den Desktop-Computer. Auf dem Smartphone oder Tablet gibt es einerseits ganz allgemeine Einstellungen im Betriebssystem (zum Beispiel iOS, iPadOS, Android). Hier kann beispielsweise allen Apps verboten werden, auf den Standort, auf die Kamera, auf Dateien, auf Kontakte und so weiter zuzugreifen, sodass jede App bei der ersten Nutzung den Zugriff für die einzelnen Komponenten anfragen muss und die nutzende Person individuell entscheiden kann, ob eine bestimmte Berechtigung erteilt wird oder nicht. Das hat einen etwas höheren Aufwand bei der Einrichtung eines neuen Gerätes zur Folge. Im eigentlichen Betrieb erzeugt dies allerdings keinen nennenswerten Mehraufwand. Neben diesen grundsätzlichen Einstellungen auf dem Gerät verfügt fast jede App über zusätzliche Datenschutzeinstellungen. Beispielsweise bieten viele Messenger-Apps die Option, den Online-Status, die Lesebestätigung oder auch den Schreib-Indikator zu verstecken.

Im Unterricht: Datenschutzeinstellungen auf dem Smartphone

Jahrgangsstufen: 5 bis 7
zum Beispiel im Rahmen der Themen „Privatsphäre“ und/oder „Datenschutz“

Ablauf:
Die Schülerinnen und Schüler öffnen ihre favorisierte Social-Media-App und rufen ihre Profileinstellungen auf (in der Regel durch Antippen des Profilbilds). In den Einstellungen gibt es bei den meisten sozialen Netzwerken eine eigene Kategorie „Privatsphäre-Einstellungen“. Hier sollten alle Schülerinnen und Schüler einmal durchnavigieren und schauen, ob sie die Einstellungsmöglichkeiten verstehen. Wenn sie irgendetwas nicht verstehen, können sie mit Mitschülerinnen und Mitschülern und der Lehrkraft die Einstellungen genauer erforschen.

Weitere Informationen und Materialien zum Thema:

- Klicksafe und mobilsicher: Social-Media-Apps einstellen – so geht’s!, August 2020. URL: https://www.klicksafe.de/materialien/teil-5-mobil-safe-social-media-apps-einstellen-so-gehts (16.01.2024).
- Klicksafe: Smartphones souverän nutzen, Februar 2020. URL: https://www.klicksafe.de/materialien/smartphones-souveraen-nutzen (16.01.2024).
- Schau hin: Die Faszination sozialer Netzwerke. URL: https://www.schau-hin.info/soziale-netzwerke (16.01.2024).
- Datenschutz geht zur Schule: Datenschutz leicht erklärt. URL: https://www.datenschutz-leicht-erklaert.de/ (16.01.2024).
- Klicksafe: Datenschutz – leicht erklärt, Mai 2022. URL: https://www.klicksafe.de/materialien/datenschutz-leicht-erklaert (16.01.2024).
- Klicksafe: Quiz zum Thema Datenschutz, 2018. URL: https://www.klicksafe.de/materialien/quiz-zum-thema-datenschutz (16.01.2024).

Auf dem Desktop-Computer lassen sich ebenfalls grundlegende Einstellungen am Betriebssystem vornehmen. Insbesondere bei Windows sind die Einstellungsmöglichkeiten allerdings sehr undurchsichtig. Darüber hinaus sind auf dem Desktop vor allem die Browser-Einstellungen interessant. Es kann unter anderem eingestellt werden, wann und ob Cache und Verlauf (welche Seiten wurden wann besucht) gelöscht werden, ob Passwörter und Zahlungsdaten im Browser gespeichert werden dürfen und welche Suchmaschine standardmäßig genutzt wird. Außerdem werden, abhängig von den gewählten Privatsphäre- und Sicherheitseinstellungen, einige Tracking-Cookies und Fingerprinting direkt blockiert. Um möglichst alle Tracker automatisch zu blockieren, sind zusätzliche AddOns, wie zum Beispiel uBlockOrigin, PrivacyBadger oder Ghostery, hilfreich. Auch im Browser ist Learning by Doing die einfachste Methode, um zu verstehen, welche Einstellungen es gibt und was diese für Auswirkungen haben, weshalb Schülerinnen und Schüler dies aktiv erproben sollten.

Viele Dienste sammeln standardmäßig so viele Daten wie möglich. Daher ist es für die selbstbestimmte Verfügung über die eigenen Daten wichtig, dass direkt nach der Installation einer App oder der Kontoeinrichtung einer Online-Anwendung immer zuerst die Privatsphäre- und Sicherheitseinstellungen aufgerufen werden, bevor die eigentliche Nutzung erfolgt.

4.2 Datensicherheit und digitale Selbstverteidigung

Der Begriff „Datensicherheit“ umfasst im Allgemeinen alle technischen und organisatorischen Maßnahmen, die ergriffen werden, um alle in einem System befindlichen Daten jederzeit genau den Personen zugänglich machen zu können, die das Recht dazu haben – unabhängig davon, ob es sich um personenbezogene Daten handelt oder nicht. Technische Maßnahmen, um dies sicherzustellen, sind zum Beispiel passwortgeschützte Accounts, Verschlüsselungen, Backups und verschlossene Serverräume. In einigen Bereichen ergänzen sich Datensicherheit und Datenschutz, in anderen Bereichen stehen die beiden in Konkurrenz zueinander. Beispielsweise vereinfachen umfangreiche und langfristig gespeicherte Server-Logs (Mitschnitte der Aktivitäten auf einem Server) das Aufdecken von verdächtigen Aktivitäten, was zur Erhöhung der Datensicherheit beitragen kann. Aus Datenschutzperspektive ist so eine detaillierte Protokollierung jedoch nicht wünschenswert.

Das Absichern der eigenen Daten vor unerwünschter Manipulation (Lesen, Verändern, Löschen) nennt man auch „digitale Selbstverteidigung". Einige Methoden der digitalen Selbstverteidigung wurden bereits in den vorigen Kapiteln besprochen (zum Beispiel Datensparsamkeit, Datenschutzeinstellungen, Tracking-Schutz und Verhalten bei Phishing-Versuchen). Aus dem Bereich der Datensicherheit kommen noch weitere Möglichkeiten zur digitalen Selbstverteidigung hinzu.

Im Folgenden wird insbesondere auf die Themen Passwörter, Authentisierung und Verschlüsselung eingegangen. Außerdem wird kurz erläutert, was Hacking eigentlich bedeutet und wie Personen oder Organisationen Opfer von Hacking werden können.

Mehr Informationen

Weitere Informationsangebote zur digitalen Selbstverteidigung finden sich im Abschnitt „Weiterführende Literaturhinweise und Angebote".

4.2.1 Passwortsicherheit, Passwortmanager und Zwei-Faktor-Authentisierung (2FA)

Viele Webseiten und Apps sind nur mit einem Account nutzbar. Dieser muss üblicherweise mit einem Benutzernamen und einem Passwort gesichert werden. Damit der Zugang auch wirklich sicher ist, gibt es verschiedene Anforderungen an das Passwort, die sogenannte Passwortrichtlinie, die je nach App beziehungsweise Webseite unterschiedlich sein kann. Eine typische Richtlinie ist, dass das Passwort mindestens acht Zeichen haben muss, unter denen sich je ein Großbuchstabe, eine Zahl und ein Sonderzeichen befinden. Darüber hinaus gibt es Empfehlungen zur Passwortsicherheit, zum Beispiel vom Bundesamt für Sicherheit in der Informationstechnik (BSI). Die aktuellen Empfehlungen werden über deren Webseite veröffentlicht.[33] Passwortrichtlinien orientieren sich häufig an den Empfehlungen des BSI.

Sichere Passwörter sind

- komplex: Sie beinhalten verschiedene Zeichentypen (Klein-/Großbuchstaben, Zahlen, Sonderzeichen).
- lang: Je weniger komplex sie sind, desto länger müssen sie sein (mind. 8 – 12 Zeichen).
- einzigartig: Jeder Account wird mit einem eigenen Passwort geschützt.
- nicht zu erraten: Sie haben keinen Bezug zur Person (Spitznamen, Geburtsdaten, …) und kommen so nirgendwo anders vor, weder in (Wörter-)Büchern, noch Filmen, noch Musik.

[33] Bundesamt für Sicherheit in der Informationstechnik: Sichere Passwörter erstellen. URL: https://www.bsi.bund.de/dok/6596574 (16.01.2024).

Unterrichtsidee: Passwort in Gefahr – ein Fall für die Internet-Detektive

Jahrgangsstufen: 3 bis 4
Fächerschwerpunkt: Alle Fächer

Hauptintention:
Indem die Schülerinnen und Schüler die Probleme der Roboter mit ihren Passwörtern reflektieren und die Nutzung eines Kochrezepts für sichere Passwörter einüben, erlernen sie einen bewussten Umgang mit ihren Daten in einer digitalen Umgebung.

Zu vermittelnde Medienkompetenzen:
K 4 Schützen und sicher agieren
4.2. Persönliche Daten und Privatsphäre schützen
4.2.1. Maßnahmen für Datensicherheit gegen Datenmissbrauch berücksichtigen
4.2.2. Privatsphäre in digitalen Umgebungen durch geeignete Maßnahmen schützen

Entwicklung der Medienkompetenz laut Fachanforderungen:
Die Schülerinnen und Schüler können …
4.2.1. angeleitet Gefahren von Datenmissbrauch und -verlust vermeiden.
4.2.2. angeleitet die Bedeutung von Passwörtern und Pseudonymen erläutern und diese nutzen.

Arbeitsphasen
- Die Schülerinnen und Schüler lesen als Internet-Detektive in Gruppen je einen „Fall" eines Roboters, der ein Problem mit seinem oder ihrem Passwort hat. Sie überlegen, was mit dem Passwort passiert sein könnte und beantworten die gestellten Fragen.
- Die Gruppen berichten im Plenum über ihren „Fall" und machen Vorschläge zur Lösung des Problems.
- Die Schülerinnen und Schüler lernen in einem zweiten Schritt ein „Kochrezept" für ein sicheres Passwort kennen. Mithilfe des Rezepts finden sie Beispiel-Passwörter heraus, die sich aus einem Merksatz ableiten lassen.

Eine detaillierte Beschreibung dieser und weiterer Unterrichtsideen (auch zu anderen Themen der Medienkompetenzvermittlung) finden Sie hier: https://medienberatung.iqsh.de/medienkompetenz-vermitteln-unterrichtsideen.html. Die Unterrichtsideen sind unter der Überschrift dieser Handreichung in der Reihenfolge ihres Erscheinens im Text sortiert.

Ob die eigenen E-Mail-Adressen und Passwörter schon mal in einem (großen) bekannten Daten-Leak dabei waren, kann mithilfe der Seite „Have I Been Pwned" unter folgendem Link geprüft werden: https://haveibeenpwned.com/.[34]

Alle Anforderungen an sichere Passwörter zu erfüllen und sich dann die große Menge verschiedener Passwörter zu merken, ist den meisten Menschen nicht möglich. Deswegen gibt es Passwortmanager. Dabei handelt es sich um eigenständige oder auch in den Browser integrierte Software, die die eigenen Passwörter für einen verwaltet. Hierbei gibt es unterschiedlich sichere (zum Beispiel verschlüsselt, extra gesichert) und unterschiedlich komfortable (beispielsweise automatische Synchronisierung, integrierter Passwortgenerator) Lösungen. Die folgenden Beiträge geben einen Überblick über die Vor- und Nachteile verschiedener Passwort-Manager:

- SoManyTabs: Nie mehr ÄRGER mit Passwörtern | Passwortmanager-Vergleich, 23.08.2021. URL: https://www.funk.net/channel/somanytabs-12189/nie-mehr-aerger-mit-passwoertern-passwortmanagervergleich-1758083 (16.01.2024).
- Bundesamt für Sicherheit in der Informationstechnik: Passwörter verwalten mit dem Passwort-Manager. URL: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/Passwort-Manager/passwort-manager_node.html (16.01.2024).

Bei der Nutzung von Passwörtern können viele Dinge schiefgehen und nicht alle davon liegen in der eigenen Hand. Wenn zum Beispiel ein soziales Netzwerk die Passwörter seiner Nutzenden schlecht sichert und dieses

[34] Have I Been Pwned: Check if your email address is in a data breach. URL: https://haveibeenpwned.com/ (16.01.2024).

Netzwerk gehackt wird, kann ein Passwort noch so gut sein: Wenn andere es kennen, erfüllt es seinen Zweck nicht mehr. Eines der Hauptprobleme von Passwörtern ist also, dass jede Person, die das Passwort kennt, dieses auch nutzen kann. Deswegen bieten viele Online-Dienste für ihre Accounts inzwischen die Einrichtung einer Zwei-Faktor-Authentisierung (2FA) an. Hierbei wird nach der Passworteingabe mithilfe eines zweiten Faktors geprüft, ob die Person auch wirklich berechtigt ist, sich in den Account einzuloggen. Dieser zweite Faktor kann zum Beispiel ein zeitlich begrenzt gültiger Zahlencode sein, der per SMS an die Handynummer geschickt wird, die bei der Account-Einrichtung hinterlegt wurde. Weit verbreitet ist inzwischen auch die Nutzung von Authentisierungs-Apps, die einen temporären, zufälligen Zahlencode erzeugen. Der zweite Faktor ist also an den Besitz, entweder der SIM-Karte oder des Gerätes gebunden, auf dem die Authentisierungs-App eingerichtet wurde, sodass durch die Kombination aus Wissen (Passwort) und Besitz (2FA) die Wahrscheinlichkeit sehr hoch ist, dass die Person berechtigt ist, den Account zu nutzen. Alle wichtigen Accounts (E-Mail, Online-Banking, soziale Medien) sollten mit einem zweiten Faktor gesichert werden.

Mehr Informationen

Das Bundesamt für Sicherheit in der Informationstechnik hat eine Seite mit Informationen und Erklärvideos zum Thema „Zwei-Faktor-Authentisierung" eingerichtet: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html (13.02.2024).

4.2.2 Verschlüsselung und Backups

Eine weit verbreitete Methode, um die Sicherheit von Daten zu gewährleisten, ist das Verschlüsseln, also das Umwandeln von Klartextdaten in geheime Daten. Die geheimen Daten können dann nur noch mithilfe des passenden Schlüssels gelesen werden. Der Schlüssel ist hierbei zum Beispiel ein Passwort, eine (Zertifikats-)Datei oder auch ein biometrisches Merkmal wie zum Beispiel ein Fingerabdruck. Biometrische Daten als Schlüssel zu verwenden, ist allerdings umstritten, da ihr Vorteil – sie sind eindeutig einer Person zuzuordnen und nicht veränderbar – auch zum Nachteil werden kann. Passwörter dürfen, zumindest in Deutschland, nicht per Zwang ermittelt werden, Fingerabdrücke allerdings schon[35] und geklaute Fingerabdrücke lassen sich nicht ändern.

Es können unter anderem Dateien, Ordner, Speichermedien oder Betriebssysteme verschlüsselt werden. Moderne Desktop- und mobile Betriebssysteme sind standardmäßig verschlüsselt. Sollen einzelne Dateien geschützt werden, ist es am einfachsten, diese mit einem Passwort zu sichern. Alle gängigen Office-Programme bieten die Möglichkeit, beim Speichern einen Passwortschutz zu aktivieren. Dadurch wird die Datei verschlüsselt. Eine andere Methode ist, Dateien oder Ordner mithilfe einer Software wie beispielsweise 7zip zu komprimieren und das entstehende Archiv mit einem Passwort zu schützen. Auf diese Weise verschlüsselte sensible Daten können so zum Beispiel eher auf einem unverschlüsselten USB-Stick gesichert oder als Anhang einer unverschlüsselten E-Mail verschickt werden. Dabei ist jedoch zu beachten, dass auch hier gilt: je besser das Passwort, desto besser der Schutz. Das beste Verschlüsselungsverfahren nützt nichts, wenn das Passwort leicht zu erraten ist.

Sollen externe Speichermedien wie Festplatten oder USB-Sticks verschlüsselt werden, so ist hierfür eine Zusatzsoftware, beispielsweise VeraCrypt, hilfreich.[36] Dies ist vor allem relevant, wenn (sensible) Daten mithilfe eines USB-Sticks von A nach B transportiert oder Daten gegen Verlust gesichert werden sollen. Denn zur Datensicherheit gehört auch, dass die Daten wieder verfügbar gemacht werden können, wenn der Computer oder das mobile Endgerät einmal kaputtgeht. Die bequeme Lösung hierfür sind Cloud-Backups: Hier ist der Aufwand minimal, denn alle Daten werden automatisch synchronisiert und sie liegen zusätzlich an einem anderen physi-

[35] Netzpolitik.org: „Polizei darf Fingerabdrücke nehmen, um Handy zu entsperren", 10.03.2023.URL: https://netzpolitik.org/2023/gerichtsbeschluss-polizei-darf-fingerabdruecke-nehmen-um-handy-zu-entsperren/ (17.01.2024).

[36] Zentrum für Schulqualität und Lehrerbildung (ZSL): Neue Tresordatei anlegen. URL: https://lehrerfortbildung-bw.de/st_digital/medienwerkstatt/dossiers/sicherheit/stickcrypt/vc/3use/ (17.01.2024).

schen Ort, sodass die Daten zum Beispiel auch vor einem Verlust durch Feuer geschützt sind. Dabei gilt es jedoch folgendes zu beachten: Wenn man nicht eine eigene Cloud betreibt, werden die Daten bei fremden Personen beziehungsweise Organisationen gespeichert, denn, vereinfacht ausgedrückt, die Cloud sind die Computer anderer Menschen. Diesen muss man entweder vertrauen, dass sie die Daten nicht missbrauchen und dass die Cloud nach außen sicher verschlüsselt ist, oder die Daten müssen verschlüsselt werden, bevor sie in die Cloud übertragen werden. Auch hierfür kann VeraCrypt genutzt werden.[37] Um besonders sensible Daten vor dem Zugriff fremder Personen zu schützen, sollte ein Backup auf einem lokalen Speichermedium dem Backup in der Cloud vorgezogen werden.

Sollen keine ruhenden Daten, sondern zum Beispiel Kommunikationsdaten, verschlüsselt werden, so muss auf die Ende-zu-Ende-Verschlüsselung zurückgegriffen werden. Hierbei werden die Kommunikationsinhalte beim Sender verschlüsselt und erst beim Empfänger wieder entschlüsselt. Heutzutage gibt es verschiedene Messenger, die eine Ende-zu-Ende-Verschlüsselung umsetzen. Hierzu gehören zum Beispiel Signal, Threema und Matrix/Element. WhatsApp ist ebenfalls Ende-zu-Ende-verschlüsselt, wobei zu beachten ist, dass Backups unverschlüsselt gespeichert werden. Allerdings reicht eine Ende-zu-Ende-Verschlüsselung nicht aus, um tatsächlich privat zu kommunizieren, denn sogenannte Metadaten – Zusatzinformationen beispielsweise darüber, wer, wann, wie lange, mit wem kommuniziert – verraten bereits eine Menge. Das FBI hat hierzu eine Tabelle veröffentlicht, auf welche Informationen der Nutzenden die Behörde bei verschiedenen Messengern zugreifen kann.[38]

Nach wie vor sehr relevant in der digitalen Kommunikation sind natürlich auch E-Mails. Diese sind allerdings nicht Ende-zu-Ende-verschlüsselt. Mithilfe von PGP/MIME kann eine Ende-zu-Ende-Verschlüsselung hergestellt werden.[39] Beispielsweise bietet der E-Mail-Client Thunderbird diese Funktionalität nativ an. Da jedoch viele Menschen Schwierigkeiten bei der Nutzung des Programms PGP (Pretty Good Privacy, engl. für „ziemliche gute Privatsphäre") haben, hat sich diese Technik nicht im Alltag durchgesetzt. Einfacher ist es, wie oben beschrieben, sensible Inhalte als Dateien zu verschlüsseln und im Anhang zu senden.

Das Gegenstück zur Ende-zu-Ende-Verschlüsselung ist die Punkt-zu-Punkt-Verschlüsselung. Hierbei wird nicht der Kommunikationsinhalt, sondern der Kanal zwischen zwei Geräten verschlüsselt. Im Kontext der E-Mail-Kommunikation bedeutet dies, dass zwar der Transportweg verschlüsselt ist, allerdings wird die E-Mail auf dem Weg zum Empfänger möglicherweise von verschiedenen Zwischenstationen (Servern) weitergeleitet. Alle diese Zwischenstationen können den Inhalt der E-Mail lesen und gegebenenfalls wird er auch zwischengespeichert.

Wenn es um die Verschlüsselung von E-Mails geht, ist zudem besonders die Wahl des Anbieters zu beachten, denn diese können die Nachrichten mitlesen. Stellvertretend für die lange Reihe an sogenannten Freemailern sei an dieser Stelle Google Mail (Gmail) genannt: „Als Gmail-Nutzer sollte man sich vor Augen führen, dass **jede** ein- und ausgehende E-Mail von Google automatisiert gescannt beziehungsweise analysiert wird."[40]

Was ist Hacking und wie kann man sich dagegen schützen?

Im allgemeinen Sprachgebrauch meint der Begriff „Hacking" heute meist das Eindringen in fremde Computer und das Entwenden oder die Manipulation von fremden Daten, um kriminelle Zwecke zu verfolgen. Ursprünglich war der Begriff jedoch eher wertfrei oder sogar positiv besetzt. Eine allgemeinere Definition könnte daher lauten: Hacking ist das kreative Lösen von Problemen mithilfe technischer Mittel. Eine große europäische Hackervereinigung ist der Chaos Computer Club. Auf ihrer Webseite kann die sogenannte Hackerethik nachgelesen werden, die beschreibt, wie Hacking einen gesellschaftlichen Mehrwert mit sich bringen kann.[41] Die Hackerethik entwickelt sich ständig weiter, da sich auch die Gesellschaft ständig weiterentwickelt. Aus dem Grundsatz „öffentliche Daten nützen, private Daten schützen" lässt sich ableiten, dass Hacker, sobald sie Sicherheitslücken finden, diese nicht ausnutzen, sondern im Zuge eines sogenannten „Responsible Disclosures" melden sollten.

---

[37] Zentrum für Schulqualität und Lehrerbildung (ZSL): Programmauswahl https://lehrerfortbildung-bw.de/st_digital/medienwerkstatt/dossiers/sicherheit/stickcrypt/progs/ (17.01.2024).

[38] Netzpoltik.org: „Diese sicheren Messenger empfiehlt das FBI", 06.12.2021. URL: https://netzpolitik.org/2021/der-grosse-app-vergleich-diese-sicheren-messenger-empfiehlt-das-fbi/ (17.01.2024).

[39] Eine Anleitung gibt es beispielsweise auf folgender Seite. Digitalcourage: „E-Mails verschlüsseln mit OpenPGP", 07.12.2023. URL: https://digitalcourage.de/digitale-selbstverteidigung/e-mail-verschluesselung (17.01.2024).

[40] Kuketz IT Security: „Gmail: Google liest eure E-Mails mit", 24.03.2023. URL: https://www.kuketz-blog.de/gmail-google-liest-eure-e-mails-mit/ (17.01.2024).

[41] Chaos Computer Club: Hackerethik. URL: https://www.ccc.de/de/hackerethics (17.01.2023).

Mehr Informationen

Was Responsible Disclosures sind, wie sie funktionieren und was für Gefahren hierbei existieren, wurde in dem gemeinsamen Vortrag „Deine Software, die Sicherheitslücken und ich" des Forschungskollektivs „Zerforschung" und dem IT-Sicherheitsexperten Linus Neumann erläutert.[42]

Neben dieser konstruktiven Form des Hackings gibt es aber leider auch die eingangs erwähnte destruktive, kriminelle Form, bei der Sicherheitslücken ausgenutzt werden, zum Beispiel um Geld zu erpressen. Die Sicherheitslücken, die hierbei ausgenutzt werden, entstehen häufig erst durch sogenanntes Social Engineering (engl. in etwa „soziales Konstruieren"), das heißt die angreifenden Personen versuchen im ersten Schritt, die Menschen zu manipulieren, die Zugriff auf das System haben, in das sie einbrechen wollen, um dann über diese Menschen ebenfalls Zugriff zu erhalten.

Mehr Informationen

Wie das konkret funktionieren kann, wird einerseits in dem Funk-Video „So funktioniert Hacking wirklich! (Serien vs. Realität)"[43] anschaulich und knapp aufbereitet. Andererseits gibt der Vortrag „Hirne Hacken – menschliche Faktoren der IT-Sicherheit"[44] einen tieferen Einblick in diesen Bereich.

Der beste Schutz vor Hacking ist also, neben den bereits erläuterten technischen Tipps, immer mit einer gesunden Portion Misstrauen an außergewöhnliche, aber auch alltägliche Situationen im Internet, am Telefon und auf der Straße heranzugehen:

- Keine Links anklicken, die man nicht kennt beziehungsweise einordnen kann.
- Account-Daten nicht auf Webseiten eingeben, die über einen Link per E-Mail oder SMS aufgerufen wurden.
- USB-Sticks nicht in unbekannte Geräte stecken.
- Keine Anhänge von unbekannten Absende-Adressen öffnen beziehungsweise überprüfen, ob diese echt sind, wenn der Anhang unerwartet kommt.
- Login-Daten nicht per Telefon (oder auf andere Weise) weitergeben.
- Keine Quizzes ausfüllen, in denen nach Informationen gefragt wird, die auch als Antwort auf eine Sicherheitsfrage (statt Passwort) genutzt werden könnten, zum Beispiel der Name der ersten besuchten Grundschule, der Name des ersten Haustieres, das Geburtsjahr des Vaters, usw.

Im Unterricht: KryptoKids

Eine Möglichkeit, die Themen Datenschutz und Datensicherheit mit Kindern im Alter zwischen acht und zwölf Jahren spielerisch zu erarbeiten, bietet das Projekt „KryptoKids und die Datenkraken". Mit einer Kombination aus App und analogen Materialien können die Schülerinnen und Schüler für die Notwendigkeit von Sicherheitsmaßnahmen im Internet sensibilisiert werden.
Weitere Informationen und Materialien finden sich unter www.krypto-kids.de (13.02.2024).[45]
Das Projekt kann kostenfrei und selbstständig durchgeführt werden.

[42] Chaos Computer Club: „Deine Software, die Sicherheitslücken und ich", 04.01.2022. URL: https://media.ccc.de/v/rc3-2021-xhain-278-deine-software-die-si (17.01.2024).

[43] SoManyTabs: „So funktioniert Hacking wirklich! (Serien vs. Realität)", 19.11.2020. URL: https://www.funk.net/channel/somanytabs-12189/so-funktioniert-hacking-wirklich-serien-vs-realitaet-1721043 (17.01.2024).

[44] Chaos Computer Club: „Hirne Hacken. Menschliche Faktoren der IT-Sicherheit", 30.12.2019. URL: https://media.ccc.de/v/36c3-11175-hirne_hacken (17.01.2024).

[45] Für Lehrkräfte in Schleswig-Holstein steht die App auch im Hub für die Lehrkräfteendgeräte zur Verfügung.

Bibliographie

Weiterführende Literaturhinweise und Angebote

Videos des Funk-Formats „SoManyTabs“: Welche Daten sammeln die verschiedene Konzerne über ihre Nutzenden?

Angebot	Link
Netflix	https://www.funk.net/channel/somanytabs-12189/das-weiss-netflix-ueber-dich-1720593
Spotify	https://www.funk.net/channel/somanytabs-12189/das-weiss-spotify-ueber-dich-luna-exposed-ihre-daten-1745180
Siri, Alexa und Co.	https://www.funk.net/channel/somanytabs-12189/siri-alexa-co-wie-privat-sind-unsere-gespraeche-wirklich-1728354
Instagram	https://www.funk.net/channel/somanytabs-12189/hoert-instagram-was-ich-sage-so-funktioniert-ad-targeting-wirklich-1723899
WhatsApp	https://www.funk.net/channel/somanytabs-12189/wie-geheim-sind-meine-whatsapp-chats-wirklich-1725138
WhatsApp Alternativen	https://www.funk.net/channel/somanytabs-12189/beste-whatsapp-alternative-signal-threema-wire-und-telegram-im-vergleich-1737531
Google Alternativen	https://www.funk.net/channel/somanytabs-12189/leben-ohne-google-geht-das-alternativen-fuer-gmail-chrome-maps-mit-mrwissen2go-1742682

Informationen und Hilfsangebote zu (digitaler) Gewalt

Angebot	Link	Kurzbeschreibung
Coalition Against Stalkerware	https://stopstalkerware.org/de/	Internetseite der Koalition gegen Stalkerware
Juuuport	https://www.juuuport.de/beratung/eure-fragen	Internetseite der bundesweiten Online-Beratungsplattform für junge Menschen
Nummer gegen Kummer	https://www.nummergegenkummer.de/	Internetseite der Nummer gegen Kummer
Jugendschutz.net	https://www.jugendschutz.net/themen/sexualisierte-gewalt	Infoseite zu sexualisierter Gewalt des Kompetenzzentrums zum Schutz von Kindern und Jugendlichen im Internet
Technische Hilfe gegen Cyberstalking	https://antistalking.haecksen.org/	Das Projekt richtet sich an Menschen, die gestalkt werden, dies vermuten oder die präventiv tätig werden wollen.

DSGVO / Datenschutz

Angebot	Link	Kurzbeschreibung
Internet-ABC	https://www.internet-abc.de/kinder/lexikon/a-g/datenschutz/	Das Internet-ABC ist ein Angebot aller Landesmedienanstalten, mithilfe dessen Kinder den Umgang mit dem Internet erlernen können. Die Internetseite richtet sich zusätzlich auch an Eltern und Lehrkräfte. Den Text zum Datenschutz kann man sich auch vorlesen lassen.
Klicksafe	https://www.klicksafe.de/themen/datenschutz/datenschutz-grundverordnung/	Klicksafe ist eine EU-Initiative, die sich dafür einsetzt, dass Menschen befähigt werden, kompetent und selbstbestimmt mit dem Internet umzugehen.
YoungData	https://www.youngdata.de/datenschutz/	YoungData ist das Jugendportal der unabhängigen Datenschutzbehörden des Bundes und der Länder sowie des Kantons Zürich.
„Pixi Wissen – Was ist Datenschutz?“	www.bfdi.bund.de/pixi	Ein Heft, das aus einer Kooperation von Pixi-Wissen, Carlsen und BfDI (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) entstanden ist. Dieses und weitere Hefte können unter dem Link kostenlos bestellt werden.

Digitale Selbstverteidigung

Angebot	Link	Kurzbeschreibung
Podcast „D wie Digital“	https://difue.de/news/internet/podcast-dwiedigital-digitale-selbstverteidigung/	Podcast Folge mit dem Thema „Wie geht digitale Selbstverteidigung?“
Digitalcourage	https://digitalcourage.de/digitale-selbstverteidigung	Informationssammlung zur digitalen Selbstverteidigung.

Cybersicherheit im Schulalltag

Angebot	Link	Kurzbeschreibung
Cybersicherheit in der Schule, in Bildungseinrichtungen und zuhause	https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Sicher-im-digitalen-Schulalltag/digitaler-schulalltag_node.html	Infoseite des Bundesamts für Sicherheit in der Informationstechnik zur Cybersicherheit im Schulalltag

Weitere Informationen und Materialien finden Sie auch in der IQSH-Mediathek: http://sh.edupool.de.

Verlagsmaterial für den Unterricht

Gels, David & Nuxoll, Florian: Eine Reise zu den digital Natives. Medienwelten. Für Lehrende und Eltern. 2017, Braunschweig: Bildungshaus Schulbuchverlage Westermann Schroedel Diesterweg Schöningh Winklers.

Materialien für die Primarstufe

Bülow, Sandra & Grotehusmann, Sarah: Medienkompetenz. Klasse 1-4, Band 1. Schritt für Schritt. Smartphones, Tablets, Blogs, Coding. 2018, Berlin: Cornelsen Verlag.

Bülow, Sandra & Grotehusmann, Sarah: Mein Medienpass 2. Zu Einstern und Einsterns Schwester. 2020, Berlin: Cornelsen Verlag.

Bülow, Sandra & Grotehusmann, Sarah: Mein Medienpass 3. Zu Einstern und Einsterns Schwester. 2020, Berlin: Cornelsen Verlag.

Bülow, Sandra & Grotehusmann, Sarah: Mein Medienpass 4. Zu Einstern und Einsterns Schwester. 2021, Berlin: Cornelsen Verlag.

Datz, Margret & Schwabe, Rainer Walter: PC-Führerschein für Kinder. Heft 1. 2016, Offenburg: Mildenberger Verlag.

Datz, Margret & Schwabe, Rainer Walter: PC-Führerschein. Lehrerheft. 2016, Offenburg: Mildenberger Verlag.

Köhler, Katja & Schmid, Ute & Weiß, Lorenz & Weitz, Katharina: Pixel & Co. Informatik in der Grundschule. Arbeitsheft. 2020, Braunschweig: Bildungshaus Schulbuchverlage Westermann Schroedel Diesterweg Schöningh Winklers.

Matthies, Sabrina: Medienheft. Grundschule 3/4. 2022, Braunschweig: Westermann Bildungsmedien Verlag.

Nuxoll, Florian (Hg.): Medienbildung in der Grundschule. Leitfaden für Unterricht und Elternarbeit. 2020, Braunschweig: Westermann Bildungsmedien Verlag.

Nuxoll, Florian (Hg.): Medienwelten Grundschule. Arbeitsheft 3/4. 2018, Braunschweig: Bildungshaus Schulbuchverlage Westermann Schroedel Diesterweg Schöningh Winklers.

Nuxoll, Florian (Hg.): Medienwelten Grundschule. Lehrerhandreichungen 3/4. 2019, Braunschweig: Bildungshaus Schulbuchverlage Westermann Schroedel Diesterweg Schöningh Winklers.

Materialien für die Sekundarstufe

Hancl, Mirek: Informatische Bildung. Klasse 7/8. Coding, Making und vernetzte Welten. 2018, Berlin: Cornelsen Verlag.

Hancl, Mirek: Informatische Bildung. Klasse 9/10. Menschen, Daten und digitale Maschinen. 2018, Berlin: Cornelsen Verlag.

Nuxoll, Florian (Hg.): Medienwelten 2. Entdecken - Verstehen - Gestalten. Arbeitsheft. 2017, Braunschweig: Bildungshaus Schulbuchverlage Westermann Schroedel Diesterweg Schöningh Winklers.

Nuxoll, Florian (Hg.): Medienwelten 2. Entdecken - Verstehen - Gestalten. Lehrerhandreichungen. 2017, Braunschweig: Bildungshaus Schulbuchverlage Westermann Schroedel Diesterweg Schöningh Winklers.

Nuxoll, Florian (Hg.): Medienwelten 3. Entdecken - Verstehen - Gestalten. Arbeitsheft. 2019, Braunschweig: Bildungshaus Schulbuchverlage Westermann Schroedel Diesterweg Schöningh Winklers.

Nuxoll, Florian (Hg.): Medienwelten 3. Entdecken - Verstehen - Gestalten. Lehrerhandreichungen. 2019, Braunschweig: Bildungshaus Schulbuchverlage Westermann Schroedel Diesterweg Schöningh Winklers.

Wiemken, Jens: Webcoach. Soziale Netzwerke. Lehrerband. 2012, Stuttgart: Ernst Klett Verlag GmbH.

Grundlegende Informationen

Institut für Qualitätsentwicklung an Schulen Schleswig-Holstein (IQSH): Lehren und Lernen in der digitalen Welt. Perspektiven zur Kompetenzentwicklung in der Aus- und Fortbildung von Lehrkräften an allgemeinbildenden Schulen in Schleswig-Holstein. 2023, Kiel. URL: https://publikationen.iqsh.de/dm-medienbildung/id-02-2023.html (24.01.2024).

KMK: Bildung in der digitalen Welt Strategie der Kultusministerkonferenz. 2016, Berlin. URL: https://www.kmk.org/themen/bildung-in-der-digitalen-welt/strategie-bildung-in-der-digitalen-welt.html (24.01.2024).

KMK: Lehren und Lernen in der digitalen Welt: Ergänzung zur Strategie der Kultusministerkonferenz „Bildung in der digitalen Welt". 2021, Berlin. URL: https://www.kmk.org/themen/bildung-in-der-digitalen-welt/strategie-bildung-in-der-digitalen-welt.html (24.01.2024).

Ministerium für Bildung, Wissenschaft und Kultur des Landes Schleswig-Holstein (Hg.): Ergänzung zu den Fachanforderungen Medienkompetenz. Lernen mit digitalen Medien. Allgemein bildende Schulen Sekundarstufe I Sekundarstufe II. 2018, Kiel. URL: https://fachportal.lernnetz.de/sh/fachanforderungen.html (24.01.2024).

Verwendete Quellen

Anna nackt: Was-tun-Guide. URL: https://annanackt.com/was-tun (16.01.2024).

Bundesamt für Sicherheit in der Informationstechnik: Sichere Passwörter erstellen. URL: https://www.bsi.bund.de/dok/6596574 (16.01.2024).

BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209/83 -, Rn. 1-215. URL: https://www.bverfg.de/e/rs19831215_1bvr020983.html (16.01.2024).

Chaos Computer Club: „Deine Software, die Sicherheitslücken und ich", 04.01.2022. URL: https://media.ccc.de/v/rc3-2021-xhain-278-deine-software-die-si (17.01.2024).

Chaos Computer Club: Hackerethik. URL: https://www.ccc.de/de/hackerethics (17.01.2023).

Chaos Computer Club: „Hirne Hacken. Menschliche Faktoren der IT-Sicherheit", 30.12.2019. URL: https://media.ccc.de/v/36c3-11175-hirne_hacken (17.01.2024).

Game of Phones: „Nicht gehackt werden! Sicherheit im Netz - Mit Fabian Siegismund", 02.05.2019. URL: https://soundcloud.com/gameofphones/folge-1 (16.01.2024).

Kuketz IT Security: „Gmail: Google liest eure E-Mails mit", 24.03.2023. URL: https://www.kuketz-blog.de/gmail-google-liest-eure-e-mails-mit/ (17.01.2024).

Landesverordnung über die Verarbeitung personenbezogener Daten an öffentlichen Schulen (Schul-Datenschutzverordnung - SchulDSVO) Vom 18. Juni 2018. URL: https://www.gesetze-rechtsprechung.sh.juris.de/bssh/document/jlr-SchulDSVSH2018rahmen (16.01.2024).

Netzpolitik.org: „Datenhändler verticken Handy-Standorte von EU-Bürger*innen", 17.01.2024. URL: https://netzpolitik.org/2024/berliner-unternehmen-datenhaendler-verticken-handy-standorte-von-eu-buergerinnen/ (31.02.2024).

Netzpoltik.org: „Diese sicheren Messenger empfiehlt das FBI", 06.12.2021. URL: https://netzpolitik.org/2021/der-grosse-app-vergleich-diese-sicheren-messenger-empfiehlt-das-fbi/ (17.01.2024).

Netzpolitik.org: „Polizei darf Fingerabdrücke nehmen, um Handy zu entsperren", 10.03.2023.URL: https://netzpolitik.org/2023/gerichtsbeschluss-polizei-darf-fingerabdruecke-nehmen-um-handy-zu-entsperren/ (17.01.2024).

Netzpolitik.org: „Viele Menstruations- und Schwangerschaftsapps erfassen sensible Daten", 23.08.2022. URL: https://netzpolitik.org/2022/datenschutz-viele-menstruations-und-schwangerschaftsapps-erfassen-sensible-daten/ (16.01.2024).

Netzpolitik.org: „Vom Facebook-Profil auf die Verhaftungslisten der Taliban", 25.08.2021. URL: https://netzpolitik.org/2021/afghanistan-vom-facebook-profil-auf-die-verhaftungslisten-der-taliban/ (16.01.2024).

Netzpolitik.org: „Was wir über den Skandal um Facebook und Cambridge Analytica wissen", 21.03.2018. URL: https://netzpolitik.org/2018/cambridge-analytica-was-wir-ueber-das-groesste-datenleck-in-der-geschichte-von-facebook-wissen/ (16.01.2024).

Signal Blog: „The Instagram ads Facebook won't show you", 04.05.2021. URL: https://signal.org/blog/the-instagram-ads-you-will-never-see/ (16.01.2024).

SoManyTabs: „Können wir Menstruations-Apps wie Flo & Co trauen?", 05.05.2021. URL: https://www.funk.net/channel/somanytabs-12189/koennen-wir-menstruationsapps-wie-flo-co-trauen-mit-maria-von-aufklo-1736478 (16.01.2024).

SoManyTabs: „Nackt im Netz: Was tun?! (Sexting, geleakte Fotos)", 06.50.2021. URL: https://www.funk.net/channel/somanytabs-12189/nackt-im-netz-was-tun-sexting-geleakte-fotos-1745187 (16.01.2024).

SoManyTabs: „Passwort-Fails - die FÜNF größten EVER", 26.07.2021. URL: https://www.funk.net/channel/somanytabs-12189/passwortfails-die-fuenf-groessten-ever-1755783 (16.01.2024).

SoManyTabs: „So funktioniert Hacking wirklich! (Serien vs. Realität)", 19.11.2020. URL: https://www.funk.net/channel/somanytabs-12189/so-funktioniert-hacking-wirklich-serien-vs-realitaet-1721043 (17.01.2024).

Süddeutsche Zeitung: „Wenn der Ex das ganze Leben überwacht", 23.12.2019. URL: https://www.sueddeutsche.de/digital/spionage-smartphone-stalkerware-stalking-app-1.4733070 (16.01.2024).

Verbraucherportal Baden-Württemberg: „Cookies - hilfreich oder gefährlich", 09.02.2023. URL: https://www.verbraucherportal-bw.de/,Lde/Startseite/Verbraucherschutz/Cookies+_+hilfreich+oder+gefaehrlich_ (16.01.2024).

Wikipedia – die freie Enzyklopädie: „E-Mail-Konto", 15.12.2023. URL: https://de.wikipedia.org/w/index.php?title=E-Mail-Konto&oldid=240222772#Alias-Adressen_und_Wegwerf-E-Mail-Adressen (16.01.2024).

YoungData: Das „Recht am eigenen Bild". URL: https://www.youngdata.de/recht-am-eigenen-bild/ (16.01.2024).

Zentrum für Schulqualität und Lehrerbildung (ZSL): Neue Tresordatei anlegen. URL: https://lehrerfortbildung-bw.de/st_digital/medienwerkstatt/dossiers/sicherheit/stickcrypt/vc/3use/ (17.01.2024).

Zentrum für Schulqualität und Lehrerbildung (ZSL): Programmauswahl https://lehrerfortbildung-bw.de/st_digital/medienwerkstatt/dossiers/sicherheit/stickcrypt/progs/ (17.01.2024).

IQSH
Institut für Qualitätsentwicklung
an Schulen Schleswig-Holstein

Schreberweg 5
24119 Kronshagen
Telefon: 0431 5403-0
Fax: 0431 988-6230-200
info@iqsh.landsh.de
www.iqsh.schleswig-holstein.de