Datensatz – Datenschatz?

Warum Datenschutz und Datensicherheit wichtig sind

In Kooperation mit

CMS CHAOS MACHT SCHULE

klicksafe TO GO

Titel:
Datensatz – Datenschatz?
Warum Datenschutz und Datensicherheit wichtig sind
aus der Reihe klicksafe to go

Autorinnen und Autoren:
Steffen Haschler (Bildungsprojekt „Chaos macht Schule“, Chaos Computer Club Mannheim) unter Mitarbeit von Benjamin Schlüter (Bildungsprojekt „Chaos macht Schule“, Chaos Computer Club Berlin) und Stefanie Rack (klicksafe)
Verantwortlich: Birgit Kimmel

Der Autor, Steffen Haschler, ist Lehrer und hält Fortbildungen zu den Themen Datenschutz, Urheberrecht und Medienwelten für das Regierungspräsidium Karlsruhe und engagiert sich in seiner Freizeit im Projekt „Chaos macht Schule“ des Chaos Computer Clubs. Ziel dieses Projekts ist es, Schüler, Eltern und Lehrer in den Bereichen Medienkompetenz und Technikverständnis zu stärken. Kontakt: schulprojekt@ccc-mannheim.de

Herausgeber:
klicksafe ist das deutsche Awareness Centre im CEF Telecom Programm der Europäischen Union. klicksafe wird gemeinsam von der medienanstalt rlp (Koordination) und der Landesanstalt für Medien NRW umgesetzt. klicksafe ist Teil des Safer Internet DE Verbundes (https://saferinternet.de). Diesem gehören neben klicksafe die Internet-Hotlines internet-beschwerdestelle.de (durchgeführt von eco und FSM) und jugendschutz.net sowie die Nummer gegen Kummer (Helpline) an.

Koordinatorinnen klicksafe:
Birgit Kimmel, Deborah Woldemichael

The project is co-funded by the Connecting Europa Facility of the European Union · http://ec.europa.eu/saferinternet

2. Auflage März 2020

klicksafe to go ist ein Format, in dem aktuelle medienpädagogisch relevante Themen aufgegriffen und für Schule und Unterricht kompakt aufbereitet werden.

Bezugsadresse:
klicksafe
c/o Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz
Direktor: Dr. Marc Jan Eumann
Turmstraße 10
67059 Ludwigshafen
Tel: 0621 5202-271
E-Mail: info@klicksafe.de
URL: https://klicksafe.de

Layout und Umschlaggestaltung:
Vanessa Buffy

Verwendete Symbole:
- Tipp
- Information
- Exkurs

Vorwort

Unser Alltag ist nicht mehr in Analoges und Digitales zu unterteilen. Wir sind umgeben von Geräten, die unsere Daten erheben, verarbeiten, speichern und weiterleiten. Täglich nehmen uns Überwachungskameras auf, der Hersteller unseres Autos kennt dank GPS unseren Standort und mit „electronic cash“ wird nachvollziehbar, was wir wann und wo gekauft haben. Das Fitnessarmband, ein sogenanntes Wearable, weiß, wie viel wir heute gelaufen sind und kennt unseren allgemeinen Gesundheitszustand.

Unsere Handys sind Minicomputer mit zahlreichen Apps, die viele Berechtigungen besitzen, wie den Zugriff auf unsere Bilder, unsere Kontakte, was wir sprechen oder in unseren Browser eingeben.

Im Internet hinterlassen wir weitere Datenspuren: Zum einen offensichtliche, indem wir etwas in Sozialen Netzwerken posten, zum anderen unbewusste, wenn Firmen unser Surfverhalten tracken und die dabei gewonnenen Informationen langfristig speichern.

Daten, die einmal zu einem bestimmten Zweck erhoben wurden, werden später häufig unzulässigerweise miteinander verknüpft, um neue Informationen zu gewinnen. So entstehen mit der Zeit detailreiche Personenprofile. Diese werden international und meist intransparent gehandelt und sind nicht nur für Firmen und Behörden, sondern auch für Kriminelle interessant – etwa zum Identitätsklau oder um Menschen zu erpressen.

Die Zahl der „großen“ Hackerangriffe nimmt zu, wie beispielsweise die Ransomware-Attacke WannaCry, die im Mai 2017 zehntausende Rechner weltweit infizierte oder der Doxing-Angriff auf hunderte im Bundestag vertretenen Politiker, von denen im Januar 2019 umfangreiche Informationen wie private Kontaktdaten oder Chatverläufe der Öffentlichkeit zugänglich gemacht wurden. Auch häuften sich in den letzten Jahren die Meldungen rund um schwerwiegende Datenschutzpannen bei Facebook.

Die im Januar 2016 verabschiedete und im Mai 2018 in Kraft getretene europäische Datenschutzgrundverordnung (EU-DSGVO) vereinheitlicht den Datenschutz innerhalb der Europäischen Union über die Ländergrenzen hinweg, indem Anbieter von Internetdiensten gewisse Standards einhalten müssen. Bei Zuwiderhandlungen können hohe Bußgelder verhängt werden. Doch unsere Datenschutzgesetze gelten nicht weltweit und werden oft von international agierenden Konzernen ignoriert, oder es wird fahrlässig mit der Datensicherheit umgegangen, da eine bewusste Auseinandersetzung damit Geld und Zeit kostet und so Gewinne und Marktanteile schmälert. Datensicherheit bedeutet dabei unter anderem, dass Datenverlust, -manipulation und unberechtigter Zugriff verhindert werden.

Als Verbraucher sollte man selbst tätig werden und neben dem kritischen Hinterfragen eigener Kaufentscheidungen Vorkehrungen treffen, die die eigenen Daten schützen.

Die zu diesem Material erstellten Arbeitsblätter sollen junge Menschen dabei unterstützen, sich bewusster, sicherer und damit mündiger im digitalen Raum zu bewegen.

Quelle: fotolia

Sachinformation

Datenschutzgesetze: International, in der EU, in Deutschland

Was Datenschutz bedeutet, wird weltweit unterschiedlich betrachtet. Das Internet kennt im digitalen Zeitalter keine Ländergrenzen, und so ergeben sich schnell Probleme, wenn persönliche Daten häufig durch mehrere Länder wandern. Das Demo-Tool „Traceroute“[1] macht den internationalen Weg von Daten eindrucksvoll sichtbar. Um die Daten der eigenen Bürger zu schützen, gibt es zwischen Ländern Abkommen wie das „EU-US Privacy Shield“[2]. Dieses Abkommen regelt den Austausch zwischen den USA sowie der Schweiz und Europa in Bezug auf Datenverarbeitung.

Bereits Ende 1983 – also lange vor dem Entstehen des kommerziellen Internets in den 1990er-Jahren – hat das deutsche Bundesverfassungsgericht ein „Recht auf informationelle Selbstbestimmung“[3] aus den Artikeln 1 und 2 des Grundgesetzes abgeleitet. Es spricht jedem Menschen das Recht zu, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, bis auf notwendige, im Gesetz klar geregelte Ausnahmen. „Datenschutz“ ist ein relativ neuer Rechtsbegriff aus den 1970er Jahren und findet sich daher nicht im Grundgesetz. Das Bundesland Hessen war Vorreiter, als es das weltweit erste Datenschutzgesetz verabschiedete.

Auf EU-Ebene gilt seit dem 25. Mai 2018 mit der Datenschutzgrundverordnung“ eine EU-weite Vereinheitlichung der Regeln für die Verarbeitung von personenbezogenen Daten durch Behörden und private Unternehmen. Diese definiert über die Ländergrenzen hinweg die Rechte der Verbraucher und verpflichtet Firmen, den Verbrauchern Auskunft über die über sie gespeicherten Daten zu erteilen. Außerdem können hohe Bußgelder bei Verstößen verhängt werden. Auf Basis der DSGVO wurde beispielsweise eine Strafe von 50 Millionen Euro gegen Google in Frankreich verhängt, die Immobiliengesellschaft Deutsche Wohnen muss 14,5 Millionen Euro wegen Datenschutzverstößen zahlen.

IP-Routing und -Adressen: Möchten sich Geräte in Computernetzwerken verbinden bzw. Daten, auch international, austauschen, müssen sie füreinander erreichbar sein. Ähnlich wie unsere Postadressen bzw. unsere Telefonnummern gibt es dazu im Internet IP-Adressen. Welche IP-Adresse Ihnen gerade von Ihrem Provider zugeordnet ist, können Sie auf einer Seite wie www.utrace.de sehen.

Recht an den eigenen Daten

Die Datenschutzgesetze schützen Menschen, indem sie die Verarbeitung ihrer personenbezogenen Daten beschränken. Das sind Daten, die eine Person direkt bestimmen oder durch weitere Informationen bestimmbar machen. Dies kann der eigene Name, ein WhatsApp-Chat oder auch nur die Augenfarbe sein.

Mit dem „Recht auf informationelle Selbstbestimmung“ brauchen Dritte in Deutschland immer die Einwilligung des Betroffenen, um seine Daten verarbeiten zu dürfen. Allerdings gibt es gesetzlich geregelte Ausnahmen, z. B. für Steuerbehörden oder Schulen, die personenbezogene Daten verarbeiten müssen, um ihre Aufgaben erfüllen zu können. Dabei ist die Verhältnismäßigkeit (legitimer Zweck, Geeignetheit, Erforderlichkeit, Angemessenheit) zu achten. Werden personenbezogene Daten verarbeitet, hat man immer ein Auskunftsrecht und ein Recht auf Berichtigung, Löschung oder Sperrung dieser Daten, falls sie nicht korrekt erhoben wurden. Das „Recht auf Selbstauskunft“ kann jeder Bürger bei staatlichen Behörden oder Firmen geltend machen, über einen Generator[4] lässt sich leicht ein Auskunftsersuchen erstellen.

Auf sozialen Netzwerken wie beispielsweise Instagram[5] oder Facebook gibt es einen Download-Link, über den man alle Daten abrufen kann, die die jeweilige Plattform über die eigene Person gespeichert hat.

1 https://ogy.de/ajst
2 https://ogy.de/oqwq
3 https://ogy.de/ej1h
4 https://datenschmutz.de/cgi-bin/auskunft
5 https://spiegel.de/netzwelt/apps/instagram-wie-laedt-man-seine-daten-herunter-a-1204683.html

Eine einmal erteilte Einwilligung zur Verarbeitung der eigenen Daten kann widerrufen werden oder ist gegebenenfalls gar nicht gültig. Insbesondere junge Menschen gelten nicht immer als einwilligungsfähig, da man davon ausgeht, dass sie noch nicht einschätzen können, welche Auswirkungen ihr heutiges Handeln auf ihre Zukunft hat. Aber auch von Erwachsenen erteilte Einwilligungen können unwirksam sein, wenn es keine umfängliche Aufklärung gab. Es reicht beispielsweise nicht, Eltern zu fragen, ob sie damit einverstanden sind, wenn ein Foto ihre Kindes auf der Schulhomepage veröffentlicht wird. Sie müssen vorher darüber aufgeklärt werden, dass einmal ins Internet hochgeladene Inhalte nicht mehr kontrollierbar sind, da viele Kopien angelegt werden können und dort normalerweise dauerhaft verbleiben.

Automatisierte Datenverarbeitung und Big Data
Daten werden heute meist automatisiert verarbeitet, was deren Verfügbarkeit erhöht und ermöglicht, zu verschiedenen Zwecken erhobene Daten einfach zu verknüpfen und damit neue Informationen zu gewinnen. Dies ist nach deutschem Recht unzulässig. Natürlich wäre ein Kreditgeber daran interessiert, den genauen Gesundheitszustand eines Bürgers zu kennen, bevor sein Kredit freigegeben wird. Gesundheitsdaten werden jedoch erhoben, damit Ärzte den Menschen besser behandeln können, und nicht, um anderen damit zu ermöglichen, ihre Geschäftsrisiken zu minimieren.

Auch kann man Daten über Daten sammeln, sogenannte Metadaten, die zusätzliche interessante Rückschlüsse auf Personen ermöglichen. Ein Beispiel sind Verbindungsdaten von Telefonen. Die eigentlichen Gespräche sind unbekannt, aber anhand von Zeiten und Kontakten können viele Rückschlüsse auf den Nutzer gezogen werden. Telefoniert eine Person beispielsweise regelmäßig mit einem Psychologen, liegt die Vermutung nahe, dass sich die Person dort in Therapie befindet.

Data Mining
Falls Sie interessiert, wie solches „Data Mining“, also das automatisierte Auswerten großer Datenmengen, funktioniert, und eine Stunde investieren können, schauen Sie sich den Vortrag[6] eines Fachmannes an. Alternativ können Sie sich die Visualisierung der Vorratsdaten von Malte Spitz[7] ansehen, die er bei der Telekom eingeklagt hat.

Datensicherheit durch Verschlüsselung und Signatur
Beim Verarbeiten von Daten muss darauf geachtet werden, dass sie nicht in die Hände Unberechtigter fallen, zerstört oder manipuliert werden. Diese Datensicherheit ist eine technische Voraussetzung dafür, dass Datenschutzgesetze eingehalten werden können.

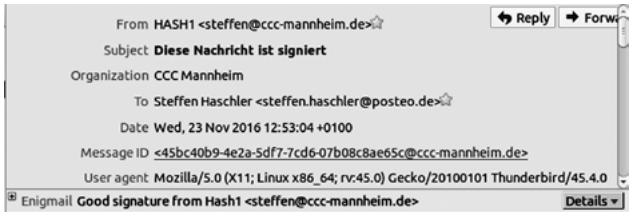
Analoge Datensätze werden deswegen in Firmen und Behörden oft in Aktenschränken weggeschlossen und an mehreren Orten aufbewahrt. Für das Übertragen der Daten kommen oft besondere Kuriere zum Einsatz. In der digitalen Welt verschlüsselt und signiert man die Daten mit kryptografischen Verfahren und legt Sicherheitskopien an.

6 https://ogy.de/k6x6
7 https://ogy.de/56ub

E-Mail-Verschlüsselung und -signatur
Unverschlüsselte E-Mails sind mit Postkarten vergleichbar. Denn anders als durch Umschläge geschützte Briefe können Postkarten unterwegs von jedem gelesen werden, etwa vom Postboten bei der Zustellung. Daher sollte man E-Mails verschlüsseln, denn die Verschlüsselung entspricht einem Briefumschlag. Gleichzeitig verhindert die digitale Signatur, dass der Absender gefälscht wird. Sie entspricht der analogen Unterschrift unter dem Brief. Wer seine E-Mails verschlüsseln will, schaut sich die Textanleitung[8] von netzpolitik.org an.

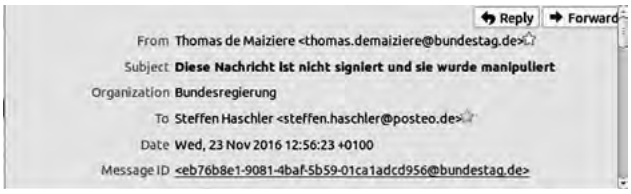
Um die Manipulation von digitalen Daten zu verhindern, verwendet man – ähnlich wie dies Stempel und Unterschriften im Analogen gewährleisten sollen – erneut kryptografische Verfahren. Im Folgenden sehen Sie ein Beispiel für einen solchen digitalen Stempel, auch „Signatur" genannt:

Die E-Mail unten stammt scheinbar von „steffen@ccc-mannheim.de". Sie wurde digital signiert, was ein Programm wie Enigmail erkennt, prüft und verifiziert.



Der Absender ist überprüfbar, da diese Mail eine digitale Unterschrift enthält (Quelle: Screenshot von Steffen Haschler, mit Thunderbird erstellt)

Anders ist es bei der folgenden Nachricht:



Sie stammt nicht vom ehemaligen Bundesinnenminister, ohne Signatur lässt sich dies kaum feststellen (Screenshot von Steffen Haschler, mit Thunderbird erstellt)

Hier stammt die Nachricht scheinbar von „thomas.demaiziere@bundestag.de", also vom ehemaligen Bundesinnenminister. Da E-Mails immer noch nicht standardmäßig signiert werden, kann man solch eine Fälschung nur schwer erkennen.

Ransomware, Bundestags-Trojaner und weltweite Hacks: Das Zeitalter der Cyberkriege?
Genauso, wie es Einbrüche in Gebäude gibt, werden digitale Speicherplätze angegriffen. Cloudspeicher und Netzwerke von Unternehmen sind aus praktischen Gründen oft weltweit erreichbar. Sie können damit auch von überallher angegriffen werden. Die eingesetzten IT-Systeme weisen fast immer Sicherheitslücken auf oder werden falsch genutzt, sodass viele solcher Angriffe erfolgreich sind. Dabei kann es sich um den Diebstahl von Informationen handeln, wie beim Bundestag-Hack im Jahr 2015. Durch eine infizierte E-Mail, die von Abgeordneten geöffnet wurde, verschafften sich die Angreifer Zugang zum Bundestagsnetz und einigen Abgeordnetenkonten.

Auch wenn bis heute unklar ist, wer hinter dem Angriff steckt und welche Daten dabei entwendet wurden, besteht auch nach Jahren noch das Risiko, dass diese Daten an die Öffentlichkeit gelangen. Diese könnten Einfluss auf zukünftige politische Debatten haben, ähnlich wie die Veröffentlichungen geheimer E-Mails von Hillary Clinton während ihres US-Wahlkampfes 2016.

Ein weiteres lohnendes Geschäftsmodell der Hacker ist es, die Daten, auf die sie Zugriff erlangen, als Geisel zu nehmen und Lösegeld zu fordern. Eine solche Ransomware-Attacke ist WannaCry[9]. Mitte 2017 wurden Zehntausende Rechner weltweit infiziert, u. a. auch Rechner der Deutschen Bahn. Die Schadsoftware verschlüsselt dabei Daten, auf die sie Zugriff bekommt, und gibt den Schlüssel zu ihrer Wiederherstellung nur gegen Zahlung einer Geldsumme heraus.

8 https://ogy.de/nr99
9 https://ogy.de/zb7q

Exploits, die „Brechstangen“ des Hackers:
Ein modernes Betriebssystem wie Windows besteht aus vielen Millionen Zeilen Code – damit erhöht sich die Wahrscheinlichkeit, dass er Fehler aufweist. Ein Browser alleine besteht schon aus vielen Hunderttausend Codezeilen. Manchmal ermöglicht dies, in das System einzubrechen. Es gibt verschiedene Arten solcher Exploits, die ähnlich wie Brechstangen im Analogen dazu verwendet werden, die Kontrolle über Computer[10] zu erlangen. Dabei werden neben bekannten Sicherheitslücken auch Lücken ausgenutzt, die der Allgemeinheit unbekannt sind, jedoch bspw. von Geheimdiensten[11] genutzt werden („Zero-Day-Exploits“).

Cookies und andere Arten von Tracking

Oft werden sogenannte „Cookies“ dazu verwendet, um das Surfverhalten von Nutzern auszuspionieren. Dies nennt man „Tracking“. Insbesondere bei kostenfreien Diensten findet es Anwendung. Cookies sind einfache Textdateien, die von Webseiten gelesen und geschrieben werden können. Sie werden dabei lokal im eigenen Browser hinterlegt. Sie gewährleisten, dass eine Webseite einen Besucher wiedererkennt. Das ist praktisch, weil man sich nicht immer wieder „ausweisen“ muss, indem man sich mit seinem Namen und Passwort erneut einloggt.

Der Nachteil ist, dass viele Seiten Inhalte von Drittanbietern einbinden, z. B. von Google Analytics oder Facebook. Die besuchte Webseite liefert dann nicht nur den eigenen (praktischen) Cookie aus, sondern auch die Cookies dieser anderen Anbieter. Da solche Drittanbieter mit vielen Seiten zusammenarbeiten, erhalten sie so Informationen über fast alle Besuche, die ein Nutzer diversen Seiten abstattet.

Neben Cookies gibt es viele weitere Methoden wie das „digitale Fingerprinting“, um einen Nutzer anhand seiner Browsereinstellungen wiederzuerkennen (Einstellungen wie benutztes Betriebssystem, Do-Not-Track-Informationen, die Bildschirmauflösung oder die Wahl bestimmter Adblocker). Die Werbenetzwerke sind hier kreativ.[12] Mit der Vielzahl an Methoden und deren geschickter Kombination ergeben sich detaillierte Nutzerprofile, die dann gehandelt und für das Ausliefern personalisierter Werbung genutzt werden.

Generell sei der Hinweis angebracht, dass die meiste Software kontinuierlich weiterentwickelt wird. Nahezu alle Browserhersteller werben heute damit, die Privatsphäre ihrer Nutzer immer besser zu schützen, so lassen sich bei nahezu allen Browsern mittlerweile die Cookies von Drittanbietern sperren. Auf der anderen Seite entwickeln kommerzielle Anbieter immer neue Tracking-Methoden. Es ist zu empfehlen, die Entwicklungen im Auge zu behalten.

Datenschutzgrundverordnung

Galten traditionell in jedem Land eigene Datenschutzgesetze, wurde mit der Europäischen Datenschutzgrundverordnung (DSGVO) ab dem 25. Mai 2018 ein EU-weiter Standard verabschiedet. Dies ist sinnvoll, schließlich spielen Ländergrenzen bei der Internetnutzung keine Rolle. Die DSGVO räumt den Verbrauchern zusätzliche Rechte ein und definiert zusätzliche Pflichten für die Unternehmen. Verbraucher haben ein Recht auf Auskunft, welche Daten ein Unternehmen über sie gespeichert hat, für welchen Zweck diese Daten verarbeitet werden und das Recht, diese ggf. zu korrigieren. Auf der Webseite „Deine Daten, deine Rechte“[13] können sich Verbraucher über ihre Rechte bzgl. der Speicherung und Verarbeitung ihrer personenbezogener Daten informieren. Bei Zuwiderhandlungen empfiehlt es sich, eine Beschwerde bei den Datenschutzbauftragten des jeweiligen Bundeslandes einzureichen.

Verständliche Erklärvideos zur DSGVO findet man auf https://deinedatendeinerechte.de (abgerufen am 17. 2. 2020)

10 https://ogy.de/djtm
11 https://ogy.de/xpsu
12 https://ogy.de/5w2l
13 https://deinedatendeinerechte.de

Selbstdatenschutz und die Problematik kostenfreier Dienste

Es gibt für den Verbraucher einige Möglichkeiten, sich zu schützen; doch genauso wie im analogen Leben gibt es auch in der digitalen Welt keine Garantien und keine absolute Sicherheit.

- Um Angriffen zu entgehen, sollte man seine Software immer auf dem aktuellsten Stand halten. Leider liefern viele Hersteller die dazu nötigen Sicherheits-Updates („Patches“) nur verspätet oder gar nicht aus. Dann bleibt nur der Wechsel zu einem zuverlässigeren Anbieter. Insbesondere bei mobilen Endgeräten ist das ein Problem. Geräte mit Internetanbindung, die keine Sicherheitsupdates mehr erhalten, sollte man entsprechend nicht mehr einsetzen.
- Man sollte regelmäßig eine Datensicherungskopie („Back-up“) der eigenen Daten erstellen, um Datenverlust vorzubeugen. Wenn Sie sich nicht damit auskennen, finden Sie hierzu beim Bundesamt für Sicherheit in der Informationstechnik ausführliche Informationen.[14]
- Die eigenen Daten sollten immer verschlüsselt verschickt und abgelegt werden, damit sie für Fremde nicht direkt lesbar sind. Dies gilt insbesondere dann, wenn man weder den Transportweg noch die Speicherorte genau kennt – und das ist im Internet eigentlich immer der Fall. In dieser Einheit lernen die Schülerinnen und Schüler (SuS) „Veracrypt“ kennen[15], welches primär für das Ablegen von Daten auf Rechnern und mobilen Speichermedien wie USB-Sticks gedacht ist und auch für Sie als Lehrer interessant sein könnte. Sie können zum Thema Verschlüsselung eine „Crypto-Party“[16] in Ihrer (Nachbar-)Stadt besuchen, um von Experten mehr darüber zu erfahren und sich schließlich selbst besser schützen zu können.
- Man sollte auf kommerzielle, aber kostenfreie Dienste, z. B. WhatsApp, verzichten, da man durch die Einwilligung zur monetären Nutzung der eigenen Daten immer das Produkt und nicht der Kunde sein wird. Denn die Firmen haben Ausgaben und müssen daher ihren Geldgebern etwas vorlegen. Nutzt man solche Dienste, sollte man sich dieser Problematik zumindest bewusst sein.
- Datensparsamkeit: Es sollten immer nur so viele Daten herausgegeben werden wie unbedingt erforderlich. Dies gilt gegenüber Behörden und Firmen, aber auch gegenüber Fremden in Sozialen Netzwerken.

Sicher(er) surfen mit HTTPS:

Der Großteil aller Webseiten wird heute über „https“ (statt wie noch vor ein paar Jahren über „http“) ausgeliefert. Wenn man sich die Adresse im Adressfeld des Browsers vollständig anzeigen lässt, sieht man, ob sie mit http oder https beginnt. Unterschiedliche Browser stellen die aufgerufenen Adressen unterschiedlich dar, die meisten Browser zeigen in ihrer aktuellen Version ein kleines Schloss neben den https-Adressen an. Wie der eigene Browser http- und https-Verbindungen darstellt, lässt sich über die Webseite httpvshttps.com testen:

Daten, die mittels „https“ ausgetauscht werden, sind verschlüsselt und daher nicht so einfach einsehbar. Dies ist insbesondere von Bedeutung, wenn Passwörter in fremden Netzwerken (Hotel, Café usw.) übertragen werden. Ein informatives Erklärvideo[17] hierzu hat Alexander Lehmann erstellt. Ist man regelmäßig in fremden Netzen unterwegs, empfiehlt sich der Einsatz eines VPN wie IPredator[18], um gesichert aus dem unbekannten Netzwerk zu kommen.

14 https://ogy.de/dbkz
15 https://veracrypt.fr
16 https://cryptoparty.in
17 https://ogy.de/siby
18 https://ipredator.se

Daten, Daten, immer mehr Daten

Bei allen hier betrachteten Beispielen sei außerdem angemerkt, dass die Menschheit kontinuierlich mehr Daten produziert. Bis vor 10 Jahren passierte dies hauptsächlich an PCs. Dann kamen Smartphones dazu, deren Apps zusätzliche Daten generieren und zu den Clouds der Anbieter transferieren. Ans Internet der Dinge sind längst nicht mehr nur Smartwatches angeschlossen, die unsere Pulsfrequenz und Bewegungsprofile erfassen. Überwachungskameras erfassen das Geschehen in der Öffentlichkeit oder in Geschäften und speichern die Aufnahmen in der Cloud. Nicht immer sind diese gegen den ungewünschten Zugriff Dritter ausreichend geschützt. Wurden beispielsweise im Jahre 2013 noch etwa 660 Milliarden Fotos aufgenommen, hat sich die Zahl im Jahr 2017 mit 1,2 Billionen Bildern fast verdoppelt. In diesem Kontext können die aufgeworfenen Fragestellungen diskutiert werden.

Datensparsamkeit: „Das Internet vergisst nicht“

Problematisieren Sie im Unterricht, dass sich Daten im Netz, egal ob verschlüsselt oder unverschlüsselt, für immer außerhalb der eigenen Kontrolle befinden. Sie können diese Problematik mit der WayBack Machine[19] verdeutlichen.

- Als Beispiel können Sie Ihre Schulhomepage oder den Sportverein eines Schülers verwenden und eine kleine Zeitreise unternehmen.
- Verfügen die SuS über eigene Internetzugänge, sollten sie selbst recherchieren.
- Diskutieren Sie die Vor- und Nachteile eines solchen Internetarchives.

Mit diesem Wissen sollte das Prinzip der Datensparsamkeit besser einleuchten. Lassen Sie dazu die SuS bspw. mittels des Merkspruchs „Stop – look – think – post“ Überlegungen dazu anstellen, was man beachten sollte, bevor man etwas hochlädt oder veröffentlicht.
Eine heute noch als sicher geltende Verschlüsselung wird möglicherweise in der Zukunft zu brechen sein, da Computer immer schneller werden oder Sicherheitslücken im Verschlüsselungsverfahren gefunden werden könnten. Somit kann man verschlüsselte Inhalte auch als zeitverzögert lesbar ansehen.

Inhalte der Praxisprojekte

Mit den ersten beiden Projekten erarbeiten sich die SuS anhand des Trackings, dass ihre Daten zum einen sensibel sind und zum anderen ausgewertet werden durch Dritte, wenn diese ihre Daten erlangen.

Das dritte und das vierte Projekt zeigen auf, wieso Verschlüsselung notwendig ist und wie man Daten verschlüsselt, Back-ups erstellt und die anfallenden Passwörter organisieren kann.

Ziel der gesamten Einheit ist es, die digitale Mündigkeit der Jugendlichen zu steigern. Es ist denkbar, diese Einheit an einem Projekttag im Ganzen durchzuführen, da sie für vier Einzelstunden konzipiert ist und sich leicht ausdehnen lässt. Es ist zusätzlich denkbar, den Vortrag von David Kriesel[20] zu schauen oder einen Film wie „Im Rausch der Daten“[21] bzw. „Citizenfour“[22] – je nach Altersstufe und Kenntnisstand der SuS.

19 https://archive.org/web
20 https://ogy.de/6eg3
21 https://ogy.de/30ae
22 https://citizenfourfilm.com

In der Unterrichtseinheit verwendete Dienste:

- **Traceroute**[23] macht die Wege verschickter Daten im Internet sichtbar. Man gibt eine Zielseite, bspw. „instagram.com“, ein. In der Konsole werden die IP-Adressen der Zwischenstationen für diese Anfrage angezeigt. Die ungefähren Standorte dieser Etappen werden auf der Karte ebenfalls sichtbar gemacht.
- **Track This**[24]
  Was Cookies beim täglichen Surfen bedeuten, demonstriert das Mozilla-Projekt „Klick This“ eindrucksvoll. Auf Basis der besuchten Webseiten wird uns bekanntlich über Cookies auf anderen Webseiten auf unsere Interessen zugeschnittene Werbung eingeblendet. Über die Webseite „Klick This“ kann man in die Online-Identität eines Hypebeast, Filthy Rich („Stinkreicher“), Doomsday („Prepper“) oder Influencer schlüpfen und sich ansehen, welche Anzeigen dieser Zielgruppe beim Surfen durchs Netz angezeigt werden. Dafür nimmt man einen Browser ohne Plugins und besondere Privatsphäreeinstellungen und öffnet die Webseite https://trackthis.link. Über die Webseite lassen sich dann automatisiert 100 verschiedene Webseiten öffnen, die auf die Zielgruppe zugeschnitten sind – im Hintergrund speichern diese ihre Cookies auf dem eigenen Rechner. Wer danach durchs Web surft, erhält entsprechende Webeanzeigen. Vor dem Experiment löscht man am besten einmal alle Cookies auf seinem Rechner. Leider ist die Webseite nur auf englisch verfügbar. Wer das Experiment mit unterschiedlichen Identitäten durchführen möchte, sollte beim Wechsel jeweils vorher seine Cookies wieder löschen.
- **Startpage**[25] (auch als Browser-Erweiterung erhältlich) ist eine Suchmaschine, die Ergebnisse von Google ausliefert, jedoch lediglich als „Zwischenstation“. So wird verhindert, dass Google Informationen über jemanden sammelt – denn gerade Suchanfragen können etwas sehr Persönliches sein. Allerdings muss man nun Startpage vertrauen. Da es sich aber um ein europäisches Unternehmen handelt, gilt hier das europäische (Datenschutz-)Recht, und das ist – gegenüber dem US-Konzern Google – ein bedeutender Vorteil.

- **Privacy Badger**[26] (als Firefox-Add-on) schützt vor Tracking, während man surft. Allerdings muss man sich etwas in das Programm einarbeiten.
- **VeraCrypt**[27] ist eine kostenlose Software, die zudem Open Source ist (d. h. der Code kann von jedem eingesehen werden). Sie verschlüsselt Dateien und Speichermedien. Sie ist ein Nachfolgeprojekt des ggf. bekannteren TrueCrypt, das vor Kurzem eingestellt wurde. VeraCrypt läuft plattformunabhängig auf Linux, Windows und MacOS.
- **KeePassX**[28] ist eine kostenlose Open-Source-Software, die Passwörter verwaltet und verschlüsselt ablegt. Sie läuft plattformunabhängig auf Linux, Windows und MacOS. Es gibt mobile Versionen, wobei man mobilen Endgeräten grundsätzlich misstrauen und sensitive Daten wie Passwortsammlungen dort nicht ablegen sollte.

23 www.dnstools.ch/visual-traceroute.html
24 https://trackthis.link
25 https://startpage.com
26 https://mzl.la/2EbVzez
27 https://veracrypt.fr
28 https://keepassx.org

Übersicht über die Projekte

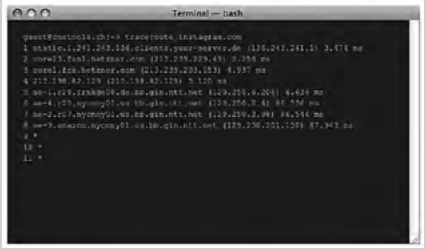
Projekt	1	2	3	4
Titel	**Datensammeln als Geschäft** (ab 13 Jahren)	**Tracking und personalisierte Werbung** (ab 13 Jahren)	**Selbstdatenschutz durch Verschlüsselung** (ab 14 Jahren)	**Passwort-Management und Back-ups** (ab 14 Jahren)
Ziele	Die SuS lernen, wie Datensammeln funktioniert und welche Geschäftsmodelle es gibt.	Die SuS lernen, wie Tracking und personalisierte Werbung funktionieren. Sie erlernen Handlungsmaßnahmen, mit denen sie sich davor schützen können.	Die SuS erarbeiten sich die Notwendigkeit von Selbstdatenschutz und erlernen Verfahren, wie man Daten verschlüsselt.	Die SuS erarbeiten sich die Notwendigkeit von Selbstdatenschutz und erlernen Grundlagen zu Back-up-Lösungen und Passwort-Management.
Unterrichtsstunden à 45 min.	1	1–2	1–2	1–2
Methoden und Material	Video, Gespräch, Screenshot/Live-Demonstration: Google Translate, optional: Live-Demonstration Traceroute	Video, Rollenspiel, Gespräch, Screenshot Lightbeam/optional: Video-Demonstration	Video, Gespräch, Bild Fahrrad (Analogie), Live-Demonstration: Verschlüsselung Word-Dokument, VeraCrypt (https://veracrypt.fr), optional: Zip-Ordner-Verschlüsselung	Video, Gespräch, Live-Demonstration: KeePass (https://keepassx.org bzw. https://keepass.info)
Zugang Internet/PC	ja; die Unterrichtseinheit erfolgt zentral an einem Präsentationsgerät; falls die SuS Internetzugang besitzen, können sie die beiden Demos (Traceroute, Google Translate) selbst ausprobieren	ja; die Unterrichtseinheit erfolgt zentral an einem Präsentationsgerät; alternativ haben die SuS eigene Arbeitsplätze und erledigen die Aufgaben in Partnerarbeit	ja; die Unterrichtseinheit erfolgt zentral an einem Präsentationsgerät; alternativ haben die SuS eigene Arbeitsplätze und erledigen die Aufgaben in Partnerarbeit	ja; die Unterrichtseinheit erfolgt zentral an einem Präsentationsgerät; alternativ haben die SuS eigene Arbeitsplätze und erledigen die Aufgaben in Partnerarbeit

Methodisch-didaktische Hinweise zu AB 1: Datensammeln als Geschäft (ab 13 Jahren)

Titel	**Datensammeln als Geschäft**
Ziele	**Die SuS lernen, wie Datensammeln funktioniert und welche Geschäftsmodelle es gibt.**
Unterrichtsstunden à 45 min.	1
Methoden und Material	Video, Gespräch, Screenshot/Live-Demonstration: Google Translate, optional: Live-Demonstration Traceroute
Zugang Internet/PC	ja; die Unterrichtseinheit erfolgt zentral an einem Präsentationsgerät – falls die SuS Internetzugang besitzen, können sie die beiden Demos (Traceroute, Google Translate) selbst ausprobieren
Einstieg	Stellen Sie den SuS zum Einstieg folgende Fragen: *Habt ihr euch schon mal gefragt, wieso Dienste wie WhatsApp kostenlos sind?* Antwort: Die Betreiber haben hohe Kosten, so müssen sie etwa Entwickler beschäftigen und Rechenzentren bereitstellen, um ihren Dienst anbieten zu können. Als Nutzer bezahlt man kostenlose Dienste meist mit seinen eigenen Daten – wie genau dieses Geschäftsmodell funktioniert, lernen die SuS in dieser Einheit. *Wieso sind eure Daten aber etwas wert? Wir schauen jetzt eine Reportage dazu als Einstieg in unser Thema.* Schauen Sie den 12-minütigen Clip „Nackt im Netz“[1] des NDR, Beitrag von Panorama. Kurzes Nachbesprechen anhand der Leitfragen auf dem Arbeitsblatt: • *Was versprechen die Datensammler-Firmen der Reporterin unter dem Pseudonym Anna Rosenberg?* Datensätze von 3 Mio. Deutschen (ca. 1 von 30 Bürgern ist betroffen → einer in diesem Raum?), lückenlos über 3 Jahre, dauerhaftes Abo für 10.000,– Euro/Monat • *Welche der Personen im Film sind aus deiner Sicht besonders angreifbar und warum?* (bspw. der Richter, der Polizist oder die Politikerin) **Hinweis:** Es kann als Vergleich eine kurze Abstimmung durchgeführt werden, und man lässt je Votum eine Schülerin oder einen Schüler deren Wahl begründen. **Richter:** ist ggf. erpressbar wegen seiner Recherchen zu Sexuellem, insbesondere, wenn er Familie hat **Polizist:** verstößt gegen Datenschutz, riskiert seine Karriere und wird dadurch erpressbar **Verdächtigter:** ist noch nicht verurteilt, ggf. ist er unschuldig, und sein Ruf wird so geschädigt **EU-Abgeordneter:** sein Handeln wird durchschaubar und vorhersagbar, womit man ihn besser beeinflussen oder einschüchtern kann **Politikerin:** es gibt die Möglichkeit, sie bloßzustellen, bspw. im Wahlkampf, aber auch eine Krankenversicherung könnte sich dafür interessieren, dass sie nach Antidepressiva Ausschau hält **gilt für alle:** Falls den oben aufgeführten Personen bewusst ist, dass sie ausspioniert werden, könnten sie sich beobachtet fühlen und sich daher anders verhalten (dieses Phänomen ist im Englischen als „Chilling Effect“ bekannt). • *Glaubt ihr, dass dieser Datenhandel erlaubt ist? Haben die Menschen nicht das Recht zu wissen, wie mit ihren Daten im Internet umgegangen wird?* Es gibt bei uns Datenschutzgesetze; deshalb müssen Menschen bei uns grundsätzlich darüber informiert werden, was mit ihren Daten geschieht. Leider halten sich viele Firmen nicht daran bzw. unsere Gesetze gelten nicht weltweit. Da Daten sich oft durch mehrere Länder bewegen, lässt sich selten garantieren, dass die in Deutschland geltenden Datenschutzgesetze eingehalten werden.

1 https://ogy.de/oazl

Einstieg



Die Wege von Datenströmen im Internet
Um zu veranschaulichen, welche internationalen Wege Daten im Internet zurücklegen, zeigen Sie Traceroute[2] – wenn die SuS selbst Internetzugang haben, können sie diesen Dienst selbst aufrufen. Download des Screenshots auch auf https://klicksafe.de/klicksafetogo

www.dnstools.ch/visual-traceroute.html
mit Domain-Eingabe „instagram.com“
Quelle: Steffen Haschler (abgerufen am 8. 6. 2017)

Die SuS sollen nun das Problem einer verräterischen URL (kurz für „Uniform Resource Locator“ – ein Link, unter dem man einen bestimmten Dienst erreicht) – wie im Film (Polizist) gesehen – nachvollziehen.

Gehen Sie dazu auf Google Translate[3] und geben Sie einen beliebigen Text in das Übersetzungsfenster ein.

Falls keine Internetverbindung vorhanden ist, können Sie vorher diesen Screenshot herunterladen unter https://klicksafe.de/klicksafetogo:

Auf dem Screenshot ist die URL in der Adressleiste zu lesen. Sie wird aus der Eingabe bei Google Translate gebildet. Wer diese URL sieht, kennt auch den Text, der zur Übersetzung eingegeben wurde. Manche Add-ons im Browser oder Apps auf mobilen Endgeräten haben Zugriff auf die URLs. Deren Anbieter können diese speichern und verkaufen. URLs sind ein wichtiger Bestandteil der weltweit gehandelten Datensätze. Achtung: Viele Browser zeigen standardmäßig nicht die vollständige URL an. Eine vollständige Ansicht erhält man durch einen Klick in die Adresszeile.
Die SuS bearbeiten Aufgabe 2, bei der sie in der URL von booking.com markieren sollen, was sie alles über einen Nutzer allein anhand seiner Eingabe in ein Formular erfahren können.

Sicherung

Die Auswertung von Aufgabe 2 erfolgt im Plenum. Informationen über Aufenthaltsort, Reisedaten, Anzahl der Personen und Zimmer können herausgelesen werden.

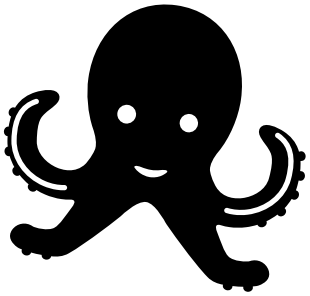
https://www.booking.com/hotel/ae/**emirates-tower**.en-gb.html?label=gen173nr-1DCAsoAkIOZW1pcmF0ZXMtdG93ZXJICVgEaDuIAQGYAQm4AQfIAQ3YAQPoAQH4AQKIAgGoAgO4ApaWrO4FwAIB;all_sr_blocks=7299609_91461414_0_2_0;**checkin=2020-08-01**;**checkout=2020-08-15**;dest_id=-782831;dest_type=city;dist=0;**group_adults=2**;group_children=0;hapos=1;highlighted_blocks=7299609_91461414_0_2_0;hpos=1;**no_rooms=1**;room1=A%2CA;sb_price_type=total;sr_order=popularity;srepoch=1573643145;srpvid=15174e047a6e00a5;type=total;ucfs=1&#hotelTmpl

In dieser Stunde haben die SuS einen Einblick erhalten, wieso Datensammeln lukrativ ist und dass es intransparenten Handel trotz nationaler Gesetze gibt.
Zum eigenen Schutz sollten keine unnötigen Add-ons in ihren Browsern oder Apps auf ihren Geräten installiert sein, da Add-ons und Apps Informationen übertragen können.

2 www.dnstools.ch/visual-traceroute.html
3 https://translate.google.com

klicksafe TO GO

AB 1: Datensammeln als Geschäft



Aufgaben:

1. Beantworte die folgenden Fragen zum Film. Besprecht eure Antworten in der Klasse: Was versprechen die Datensammler-Firmen der Reporterin unter dem Pseudonym Anna Rosenberg?

Welche der Personen im Film ist aus deiner Sicht besonders angreifbar und warum? (bspw. der Richter, der Polizist oder die Politikerin)

Glaubt ihr, dass dieser Datenhandel erlaubt ist? Haben die Menschen nicht das Recht zu wissen, wie mit ihren Daten im Internet umgegangen wird?

2. Was kann man alles aus der folgenden (durch ein booking.com-Formular erzeugten) URL herauslesen? Unterstreiche!

https://www.booking.com/hotel/ae/emirates-tower.en-gb.html?label=gen173nr-1DCAsoAkIOZW1pcmF0ZXMtdG93ZXJICVgEaDuIAQGYAQm4AQfIAQ3YAQPoAQH4AQKIAgGoAgO4ApaWrO4FwAIB;all_sr_blocks=7299609_91461414_0_2_0;checkin=2020-08-01;checkout=2020-08-15;dest_id=-782831;dest_type=city;dist=0;group_adults=2;group_children=0;hapos=1;highlighted_blocks=7299609_91461414_0_2_0;hpos=1;no_rooms=1;room1=A%2CA;sb_price_type=total;sr_order=popularity;srepoch=1573643145;srpvid=15174e047a6e00a5;type=total;ucfs=1&#hotelTmpl

Methodisch-didaktische Hinweise zu AB 2: Tracking und personalisierte Werbung (ab 13 Jahren)

Titel	**Tracking und personalisierte Werbung**
Ziele	**Die SuS lernen, wie Tracking und personalisierte Werbung funktionieren. Sie erlernen Handlungsmaßnahmen, mit denen sie sich davor schützen können.**
Unterrichtsstunden à 45 min.	1–2
Methoden und Material	Video, Rollenspiel, Gespräch, Screenshot Lightbeam/optional: Video-Demonstration
Zugang Internet/PC	ja; die Unterrichtseinheit erfolgt zentral an einem Präsentationsgerät – alternativ haben die SuS eigene Arbeitsplätze und erledigen die Aufgaben in Partnerarbeit
Einstieg	Zeigen Sie den SuS diesen Ausschnitt aus dem Hollywood-Film „Minority Report“: https://ogy.de/28ph. Suche über Suchmaschinen: „Minority report – Mall Scene“

Minority Report
In einer nahen Zukunft werden Mörder mithilfe von Technologien verhaftet, bevor sie ihre Tat begehen können („predictive policing“). Der Hauptdarsteller ist ein Polizist, der solche Verhaftungen durchführt und selbst ins Visier der Fahnder gerät. Da Menschen mittels Augenscannern erkannt werden, muss er sich im Laufe des Filmes einer gefährlichen Augenoperation unterziehen. „predictive policing“ wird bereits heute getestet. Mehr dazu finden Sie hier: https://netzpolitik.org/tag/predictive-policing

Was habt ihr in diesem kurzen Ausschnitt beobachtet?

- ggf. den Film und „predictive policing“ kurz erläutern
- Die Augen des Protagonisten werden gescannt, er wird persönlich begrüßt („Good evening, John Anderton“), und er erhält individuelle Werbung.

Wie im Filmausschnitt geht es heute um personalisierte Werbung. Habt ihr euch schon einmal gefragt, wieso ihr manchmal Werbung im Internet seht von den Dingen, die ihr euch gerade woanders angeschaut habt oder die euch gerade interessieren? Und dass passende Werbung sogar auf Seiten eingeblendet wird, die ihr vorher nie besucht habt?

- Die SuS sollen von ihren Erfahrungen damit berichten.
- Viele Werbefirmen nutzen das sogenannte „Tracking“, um mehr über ihre potenziellen Kunden zu erfahren. Damit können Firmen sie gezielter bewerben. Dies spart Ressourcen und erhöht die Chance, dass eigene Produkt gekauft werden.

Erarbeitung

Um Tracking zu veranschaulichen, wurde in der bisherigen Version des Materials das Firefox-Plugin Lightbeam verwendet, welches es heute leider nicht mehr gibt. Es machte Drittanbieter sichtbar, die ihre Inhalte auf Webseiten platzieren, die wir besuchen. So erfahren diese Firmen, dass wir diese Seiten besucht haben. Drittanbieter sind oft Firmen, die im Hintergrund unsere Daten sammeln und ggf. verwerten bzw. damit handeln.

Zeigen Sie entweder ein Video über Lightbeam[1] oder verwenden Sie den Screenshot in Anhang 1. Er ist auch auf klicksafe.de/klicksafetogo verfügbar.

Schauen wir uns gemeinsam Lightbeam an, welches aufzeigt, wie das Datensammeln funktioniert.
Im Video entsteht nach kurzer Zeit ein Bild, wie in Anhang 1 dargestellt.

Erarbeitung mithilfe von Lightbeam anhand des Screenshots in Anhang 1:

Woher weiß Google, dass der Nutzer, dessen Surfverhalten hier bildlich dargestellt ist, auf bild.de und booking.com war?

- Der Nutzer hat einige Seiten besucht, die in Lightbeam als Kreis (mit Logo) angezeigt werden.
- Diese Webseiten werden von Drittanbietern umgeben, die auf den von ihm besuchten Seiten eigene Inhalte anbieten. Viele von ihnen sind sogenannte „Tracker" und verfolgen ihn über mehrere Seiten hinweg.
- Die Tracker werden als Dreiecke dargestellt und scharen sich um die eigentlich von ihm besuchten Webseiten. Ihre Verbindung zu einer von ihm besuchten Seite wird durch eine Linie dargestellt.
- Im Screenshot im Anhang erkennt man das Google-Logo zwischen bild.de und booking.com. Daran erkennt man, dass beide Seiten Google-Inhalte nachladen (bspw. Google Analytics, ein Analyse-Tool, das auf sehr vielen Seiten für Nutzeranalysen eingebunden wird). Damit weiß Google aber, welche unterschiedlichen Seiten (hier bild.de und booking.com) der gleiche Nutzer besucht, und diese können so personalisiert werben.

Da der technische Ablauf beim Surfen den SuS wahrscheinlich nicht geläufig ist, folgt zur Vertiefung nun das Rollenspiel (Aufgabe 1 des Arbeitsblatts in Anhang 2). Dafür brauchen Sie 4 SuS („du", „dein Browser", die Seite „booking.com" und die Seite „bild.de").

Jetzt versteht ihr, wieso man personalisierte Werbung angezeigt bekommt.

1. Optionale Zusatzaufgabe: Welche Cookies liegen auf meinem Gerät?
Ermutigen Sie die SuS, auf ihren eigenen Geräten in die Browser-Einstellungen zu gehen und dort nach den hinterlegten Cookies zu schauen. Bei Chrome findet man diese bspw. unter „chrome://settings/cookies". Anhand der Cookies kann man, ähnlich wie anhand der Browser-History, auf das Surfverhalten des Nutzers detailliert rückschließen. Daher sollte man die Cookies nicht vor einer Gruppe aufrufen.
Wenn die SuS in den Cookie-Einstellungen sind, können diese direkt angepasst werden. Die jeweiligen Browser bieten hier leider keine einheitlichen Optionen. Um die Privatsphäre zu erhöhen, wird empfohlen Drittanbieter-Cookies zu blockieren sowie Cookies beim Schließen des Browsers zu löschen. Aber Vorsicht: blockiert man automatisch alle Cookies, kann man sich auf vielen Webseiten nicht mehr einloggen!

1 https://tinyurl.com/rbu5ke3

Erarbeitung

2. Optionale Aufgabe: SuS probieren das Tool „Track this“ aus. Erst löschen sie alle Cookies auf ihrem Gerät und entscheiden sich dann für eine der von Track This vorgegebenen Rollen. Nachdem das Tool automatisch zahlreiche Internetseiten geöffnet hat, sollen die SuS Webseiten ansurfen, auf denen Werbeanzeigen eingebunden sind (z.B. Nachrichtenseiten) und die ihnen dort angezeigte Werbung reflektieren.

3. Optionale Aufgabe: Welche Cookies hat Firefox blockiert?
Firefox stellt eine wöchentliche Statistik bereit, welche Cookies blockiert werden (dafür in die Adresszeile „about:protections“ eingeben). Mit dem vorher Gelernten sollen die SuS diskutieren, welche Auswirkungen die blockierten Cookies auf ihre Privatsphäre haben.
Wichtig: die Statistik ist natürlich nur brauchbar, wenn der Browser in den letzten Tagen auch bei der Internetnutzung verwendet wurde.

Wie können wir ein solches (rechtlich z. T. unzulässiges) Tracking verhindern?
Die SuS bearbeiten die Aufgabe 2 des Arbeitsblatts zunächst in Einzelarbeit.

Sicherung

Auswertung von Aufgabe 2 im Plenum oder an der Tafel.
Mögliche Lösungen (über Beamer zeigen oder Tipps kopieren und austeilen): siehe Anhang 2

Live-Demonstration mit der Proxy-Suchmaschine Startpage
Bei ausreichend Zeit können Sie für den 6. Punkt auf Startpage[2] gehen und demonstrieren, wie man direktes „Googeln“ vermeidet. Geben Sie dort einen Begriff wie „Jogginghose“ ein und vergleichen Sie das Suchergebnis mit einer gleichlautenden Anfrage auf Google. Abgesehen davon, dass die Personalisierung wegfällt, sind die Ergebnisse identisch.
Statt dass der Browser Google direkt um Inhalte bittet, fragt man stellvertretend Startpage als „Proxy“ an. Ein Proxy ist dabei eine Zwischenstelle, der man vertraut. Sie sucht stellvertretend nach Inhalten im Netz und liefert diese an uns aus. Vergleichbar wäre, im Restaurant nicht direkt beim Koch zu bestellen, sondern beim Ober als Schnittstelle zwischen Kunde und Hersteller. Der Proxy fragt nun bei Google direkt an und gibt die Inhalte an uns weiter, ohne Google zu verraten, für wen die Inhalte eigentlich sind.
Neues Problem: Jetzt muss man seinem Proxy, hier Startpage, vertrauen!

Zusatzaufgabe oder Hausaufgabe
Pro-und-Kontra-Diskussion „personalisierte Werbung“

Im Folgenden werden Aussagen für und gegen „personalisierte Werbung“ genannt. Lesen Sie diese nacheinander vor oder teilen Sie sie aus und diskutieren Sie mit den SuS, für welche sie sich entscheiden würden. Die SuS können auch eigene Aussagen dazu machen.

Weitere Informationen zu den Themen „Datenschutz“ und „Filterblase“ finden Sie in den Unterrichtsmaterialien „Ethik macht klick“ (Baustein 1) sowie im Material „Fakt oder Fake“ (Projekt 2) auf https://klicksafe.de/materialien.

2 https://startpage.com

a

- Personalisierte Werbung ist harmlos und hat sogar Vorteile, da man die Dinge sieht, die einen interessieren und Anbieter wie bild.de mehr Geld verdienen können.
- Das Problem bei Werbenetzwerken wie Google ist, dass nach und nach detaillierte Nutzerprofile entstehen, die sehr viel über einen Menschen aussagen, weil Informationen, die einzelne Seiten über uns haben, mit-einander verknüpft werden. Firmen wie Versicherer oder Kreditbanken interessieren sich für diese Daten, genauso wie dein zukünftiger Arbeitgeber oder Staaten – sie können dich so besser einschätzen.
- Internetangebote wie soziale Netzwerke oder journalistische Beiträge können durch Werbeeinnahmen im Internet für alle angeboten werden, ohne dass Nutzer dafür Geld zahlen müssen.
- _____
  _____
  _____
  _____
  _____

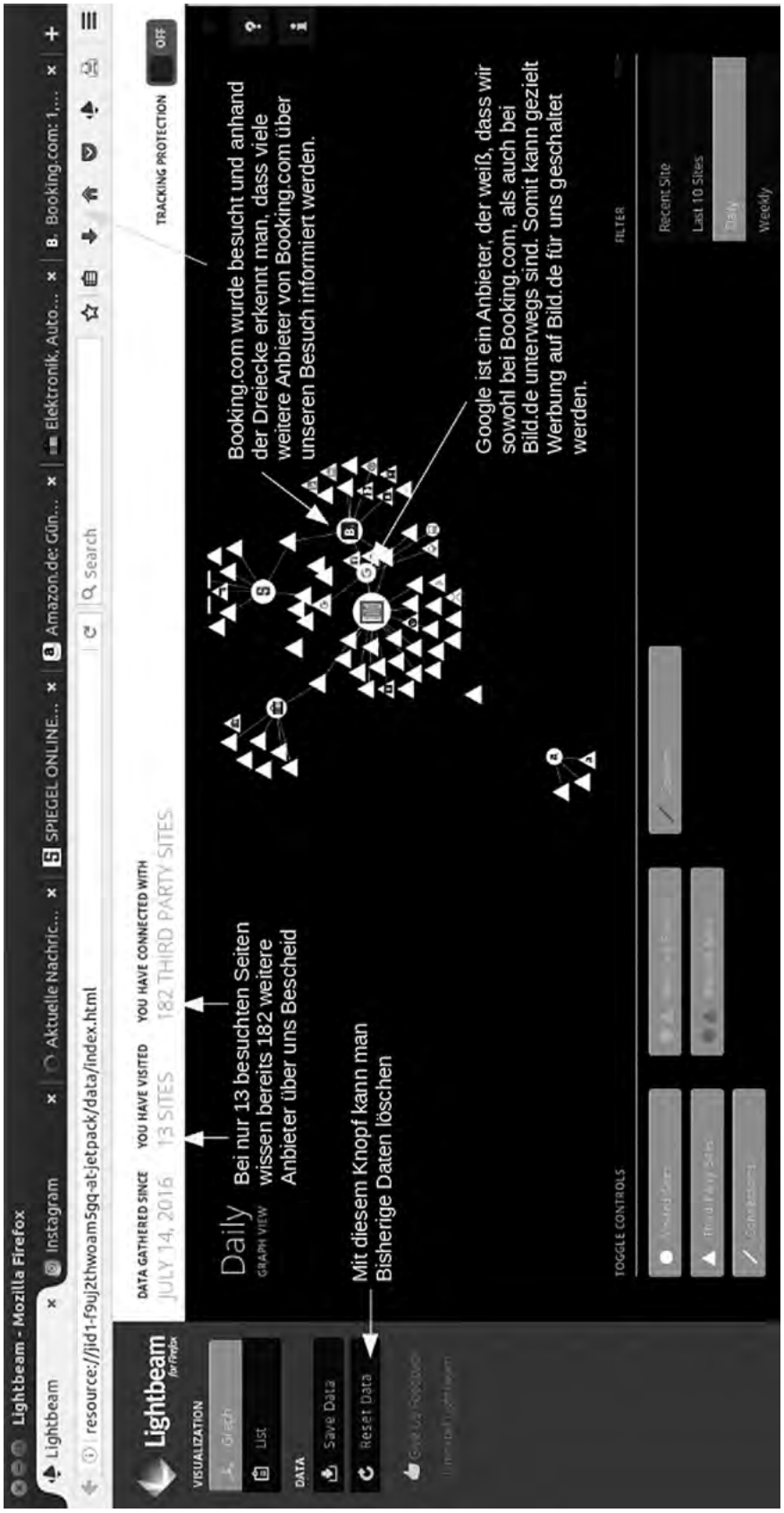
b

- Es ist sehr nützlich, wenn man als Golfspieler bei einer Suchmaschinenanfrage zum Thema „Golf“ keine Autos (VW Golf) mehr angezeigt bekommt.
- Dass Ergebnisse im Internet automatisiert personalisiert werden, birgt die Gefahr einer „Filterblase“. Menschen sehen nur noch das, was sie interessieren könnte, und übersehen so andere Dinge. Das kann auch bei der politischen Meinungsbildung negative Auswirkungen haben.
- _____
  _____
  _____
  _____
  _____
  _____
  _____
  _____
  _____
  _____

Lust auf mehr?

Das weiß das Internet über dich! – Selbstexperiment
Ein Selbstexperiment zum Thema Tracking von YouTuber Felix Michels aka Tomatolix findest du hier:
https://tinyurl.com/wn8cmdx

AB 2: Anhang 1 – Screenshot „Wer trackt mich eigentlich?“

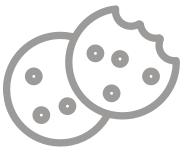


Leider ist die Software „Lightbeam“ veraltet und wird von Firefox nicht mehr unterstützt. Trotzdem ist der Screenshot sehr aufschlussreich.

AB 2: Anhang 2 – Tipps, wie man Tracking einschränken kann

1. Eine Maßnahme ist, die Cookies für Drittanbieter im Browser zu sperren. Das geht auch auf mobilen Geräten.
   Hinweis: Leider gibt es zahlreiche andere Tracking-Methoden, sodass sich Tracking dadurch nicht ganz verhindern lässt.

2. Bei Firmen wie Apple, Microsoft oder Google gibt es an den Mail-Account gebundene Verläufe, in denen Browser-Eingaben gespeichert werden, bspw. https://myactivity.google.com. Man sollte regelmäßig überprüfen, welche Informationen dort liegen und diese ggf. löschen.



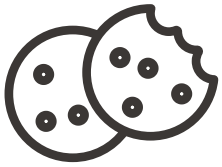
3. In Firefox und Chrome kann man folgendes Add-on installieren: https://addons.mozilla.org/de/firefox/addon/privacy-badger17

4. Man kann bewusste Produkt- und Kaufentscheidungen treffen, indem man auf Firmen ausweicht, die auf das Auswerten ihrer Kundendaten verzichten bzw. diese nicht an Dritte weitergeben.
   Beispiel: Es gibt datensparsame und werbefreie Mail-Anbieter wie posteo.de oder mailbox.org. (Achtung: Das ist keine Produktempfehlung! In der Vergangenheit haben sich diese beiden Anbieter jedoch positiv hervorgetan.)

5. Es empfiehlt sich, auf seinen Geräten nicht zu viele Apps und Add-ons zu installieren bzw. vorher zu prüfen, welche Berechtigungen diese verlangen.
   Hinweis: Ein regelmäßiger „Frühjahrsputz“ der eigenen Geräte ist sinnvoll!

6. Für private Suchen (Krankheiten, sexuelle Vorlieben etc.) sollte man eine Proxy-Suchmaschine wie Startpage (https://startpage.com) oder den Tor-Browser (https://ogy.de/qdib) verwenden, wobei dieser Browser erst verwendet werden sollte, wenn man sich damit auskennt.

AB 2: Tracking und personalisierte Werbung



Aufgaben:

1. Wie funktioniert Tracking mit Cookies?
   Ein Rollenspiel für vier Personen.

Du: Hey Browser, ich will mal wieder in den Urlaub. Kannst du mir bitte mal booking.com aufrufen?

Dein Browser: Ja klar, das mache ich sofort! Hey booking.com, mein Meister will Inhalte von dir. Gib mir deine Startseite!

booking.com: Klar, hier hast du die gewünschten Inhalte. Ich binde übrigens externe Inhalte mit ein, bspw. von Google. Kennst du „Google Analytics“? Das ist voll praktisch für meinen Betreiber!

Dein Browser: Nee, kenn ich nicht, und ist mir auch egal. Ich möchte nur das, was mein Meister mir befiehlt. Sag einfach, was ich laden soll, er wird ungeduldig.

booking.com: Ja ja, hier sind deine Inhalte. Ach, übrigens, damit ich dich später wiedererkenne, gebe ich dir diese kleine Textdatei, ein Cookie. Wenn du noch was von mir willst, zeig mir den. So erinnere ich mich an dich, und du musst Formulardaten nicht neu eingeben, oder ich habe vielleicht gerade ein Sonderangebot für deinen Meister, das ihm gefällt.

Dein Browser: Das klingt praktisch, den speichere ich mir ab. Jetzt kann ich meinem Nutzer schneller Inhalte von dir ausliefern, das macht ihn sicher glücklich.

booking.com: Ach, hier sind übrigens noch ein paar Cookies von Anbietern, mit denen ich zusammenarbeite. Sie schalten manchmal Sonderangebote auf anderen Seiten. Damit sie dich ebenfalls wiedererkennen können, habe ich auch von denen Cookies, die ich dir gerne geben würde.

Dein Browser: Klingt sinnvoll, die nehme ich auch, danke. Meister, hier sind die von dir gewünschten Inhalte von booking.com! Was wünschst du jetzt?

Du: Danke, Browser. Jetzt hätte ich gerne, dass du mir die neuesten Nachrichten von dieser „Bild-Zeitung“ anzeigst. Die habe ich bisher noch nie angeschaut.

Dein Browser: Wird sofort erledigt! He, bild.de, zeig mal, was es Neues gibt!

bild.de: Klar, gerne doch. Ich binde dir aber Werbung ein, denn damit verdiene ich mein Geld. So kann ich deinem Meister meine Inhalte kostenlos anbieten!

Dein Browser: Das klingt nur fair. Hoffentlich interessiert sich mein Meister für diese Werbung …

bild.de: Aber sicher doch! Kennen wir uns denn schon? Denn dann kann ich dir definitiv passende Werbung einblenden.

Dein Browser: Ich schau mal in meinen Cookies nach … keiner von bild.de. Ich war noch nie bei dir.

bild.de: Wir kennen uns noch nicht, aber ich arbeite unter anderem mit Google zusammen. Die schalten auch Werbung für uns. Vielleicht kennt Google dich? Ah, da ist ein Google-Cookie. Sei unbesorgt: Die Werbung, die dein Meister zu sehen bekommt, wird ihm gefallen. Google kennt ihn bereits (woher auch immer, das weiß ich nicht, und ist mir auch egal) und kann für ihn gezielt Werbung einblenden.

Du: Wow, wie geht das denn? Ich bin noch nie auf bild.de gewesen mit dem Browser, aber trotzdem kommt da jetzt Werbung von booking.com? Echt krass!

2. Sammelt zunächst in Einzelarbeit,
   dann gemeinsam an der Tafel,
   was man gegen Tracking tun kann:

Methodisch-didaktische Hinweise zu AB 3: Selbstdatenschutz durch Verschlüsselung (ab 14 Jahren)

Titel	**Selbstdatenschutz durch Verschlüsselung**
Ziele	**Die SuS erarbeiten sich die Notwendigkeit von Selbstdatenschutz und erlernen Verfahren, wie man Daten verschlüsselt.**
Unterrichtsstunden à 45 min.	1–2
Methoden und Material	Video, Gespräch, Bild Fahrrad (Analogie), Live-Demonstration: Verschlüsselung Word-Dokument, VeraCrypt (https://veracrypt.fr), optional: Zip-Ordner-Verschlüsselung
Zugang Internet/PC	ja
Hinweise für die Durchführung	• Bestenfalls bringen die SuS eigene Rechner mit, um die Software direkt installieren und testen zu können (Einverständniserklärung für Software-Installation auf SuS-Geräten von Eltern via Elternbrief einholen). • Alternativ können die SuS an den Schulrechnern ihre mitgebrachten USB-Sticks verschlüsseln. Hierzu muss VeraCrypt vorinstalliert sein. • Sollten die beiden obigen Varianten nicht möglich sein, wird die Unterrichtseinheit zentral mit einem Präsentationsgerät durchgeführt. Davon wird im Folgenden ausgegangen. · Die SuS sollten jedoch dazu ermuntert werden, alles Zuhause auf den eigenen Geräten zu wiederholen. · **Wichtig:** Die hier verwendeten Tutorials sind sehr wahrscheinlich nicht ganz auf Ihr System übertragbar. Testen Sie vorher alles.
Einstieg	• Sehen Sie sich mit den SuS auf der Website https://haveibeenpwned.com die Liste der PwnedWebsites[1] an. Diskutieren Sie mit ihren SuS am Beispiel der betroffenen Dienste Dropbox und Snapchat, was es für die Nutzer bedeutet, wenn ihre privaten Daten an die Öffentlichkeit gelangen. • Sie können als alternativen Einstieg aktuelle Nachrichten über Hacks[2] zeigen und dabei darauf eingehen, dass solche Daten gerne im Darknet[3] gehandelt werden. *Wer von euch fühlt sich online sicher?* • Holen Sie ein kleines Meinungsbild ein.
Erarbeitung	*Offensichtlich gibt es Probleme mit der „Datensicherheit" in der IT. Was meinen wir eigentlich mit dem Begriff „Datensicherheit"?* • Lassen Sie die SuS Aufgabe 1 des Arbeitsblatts bearbeiten und lassen Sie sich Lösungen einiger SuS nennen. Datensicherheit hat vor allem das technische Ziel, Daten aller Art in ausreichendem Maße gegen Manipulationen, Verlust und andere Bedrohungen abzusichern. *Nähern wir uns dem Begriff „Datensicherheit" mit einer Analogie: Was seht ihr auf diesem Bild?* • Zeigen Sie direkt das Fahrrad-Bild aus Anhang 1. • Ein Fahrrad, sein Hinterrad ist abgeschlossen. *Wieso ist es abgeschlossen? Fahrraddiebstahl ist doch per Gesetz verboten.* • Weil es Leute gibt, die dennoch Fahrräder stehlen. Daher trifft man eigene Schutzvorkehrungen → Selbstdatenschutz. **„Hacker-Paragraf"** Es gibt auch für Diebstahl im Digitalen Gesetze, die uns als Bürger schützen. Neben den Datenschutzgesetzen gibt es den „Hacker-Paragrafen" (§ 202 c)[4] im Strafgesetzbuch, der das Vorbereiten des Ausspähens und Abfangens von Daten sowie ihre Beschaffung und Weitergabe unter Strafe stellt. *Genauso wie im Analogen gibt es im Digitalen Kriminelle. Trefft ihr im Digitalen wie mit dem Fahrradschloss ähnliche Vorkehrungen?* **Hinweis:** Eine passwortgeschützte Verschlüsselung entspricht dem Fahrradschloss im Analogen. • Die SuS bearbeiten Aufgabe 2. Kurz im Plenum vergleichen. • Die SuS bearbeiten Aufgabe 3 auf dem Arbeitsblatt. Lassen Sie eine Lösung vorlesen und die Gruppe beurteilen, ob die Analogien gut formuliert wurden.

1 https://haveibeenpwned.com/PwnedWebsites
2 https://ogy.de/bcta
3 https://ogy.de/bfrf
4 https://dejure.org/gesetze/StGB/202c.html

Erarbeitung

Ransomware – Verschlüsselungstrojaner legen Rechner lahm
Wenn man die Zeit hat oder falls die Lerngruppe etwas älter ist, kann man mit dem Fahrrad-Vergleich außerdem den Begriff „Ransomware“ erläutern. Eine solche Ransomware-Attacke ist z. B. WannaCry, die Mitte Mai 2017 Zehntausende Rechner weltweit infizierte.
Es gibt zwei Sprechrollen – „das Digitale“ und „die analoge Welt“, die von je einer Schülerin oder einem Schüler vorgelesen werden.
Die analoge Welt: Du kommst nach der Schule zu deinem Fahrrad und siehst, dass der Vorderreifen mit einem fremden Schloss abgeschlossen ist. Hast du keinen Bolzenschneider, hast du ein Problem.
In der IT-Welt gibt es einen solchen Angriff ebenfalls: „Ransomware“.
Das Digitale: Deine Daten werden dabei von einem Verschlüsselungstrojaner unbrauchbar gemacht, und ein Erpresser fordert Lösegeld für den richtigen Schlüssel, damit du sie wieder „aufschließen“ und so weiterverwenden kannst.
Die analoge Welt: In der realen Welt ohne Bolzenschneider baue ich das angeschlossene Vorderrad aus. Habe ich ein Ersatzrad zur Hand, kann ich ohne großen Aufwand weiterfahren.
Das Digitale: In der IT löscht man die unbrauchbar gemachten Daten einfach. Das Ersatzrad heißt hier „Sicherheitskopie“ (oder „Back-up“). Ist sie vorhanden, spielt man sie auf den Rechner auf und arbeitet normal weiter.

Welche Dateiverschlüsselungsverfahren kennt ihr?

- In-File-Verschlüsselung, bspw. eines Office-Dokuments (MS Word etc.)
- Verschlüsselung eines Zip-Ordners (nur optional besprechen)
- Verschlüsselungsprogramme wie „VeraCrypt“ (es gibt viele Alternativen)

Live-Demonstration 1:
Schauen wir uns zuerst die Verschlüsselung eines Dokuments in Microsoft Office an.

- **Hinweis:** MS Word wurde hierfür gewählt, da die meisten Office-Installationen auf das Konto von Microsoft gehen. Alternativen wie Libre Office bieten diese Art der Verschlüsselung ebenfalls an. Anleitungen dazu finden Sie sehr leicht im Internet. Es lohnt sich ggf., LibreOffice vorzustellen, da dieses auf allen Plattformen kostenlos installiert werden kann.
- Zeigen Sie, wie man eine Datei mit einem Passwort abspeichert, bspw. mit dieser Anleitung von Microsoft: https://ogy.de/z003

Erarbeitung

Je nach Version ergibt sich ein der folgenden Abbildung ähnliches Bild:

Optional: **Verschlüsseln eines Zip-Ordners**
Zeigen Sie, wie man einen Zip-Ordner mit einem Passwort versehen kann, z. B. zum Versenden von Bildern oder mehreren Dateien per E-Mail. Sie können dazu diese Anleitung verwenden: www.bitdefender.de/support/erstellen-eines-passwort-geschuetzten-zip-archives-363.html

Vielleicht möchtet ihr andere Dateitypen als Office-Dokumente versenden oder in einem Online-speicherdienst wie GoogleDrive ablegen. Dafür gibt es nützliche Programme wie VeraCrypt.

- Schauen Sie gemeinsam das Video „Daten verschlüsseln“[4], auch zu finden auf https://klicksafe.de/klicksafetogo.
- Direkt danach öffnen Sie über einen Präsentationsrechner oder in der Gruppe VeraCrypt. Die Installation können Sie, falls möglich, den SuS zeigen und dazu die Anleitung[5] aus der Lehrerfortbildung BaWü nutzen.
- Gehen Sie mit den SuS Schritt für Schritt die Installationsanleitung durch, und erzeugen Sie einen Container mit einem Passwort. Spätestens an dieser Stelle wird man auf die Problematik von sicheren Passwörtern und deren Verwaltung aufmerksam. Dies wird in der nächsten Stunde genauer beleuchtet.

Alternativen zu VeraCrypt
Es gibt viele andere Angebote neben VeraCrypt, wie etwa DiskCryptor oder BoxCryptor. VeraCrypt hat sich in seiner (noch relativ jungen) Vergangenheit als zuverlässig erwiesen und ist „Open Source“, d. h., man kann den Quellcode sehen, wodurch Sicherheitslücken transparent werden. Es ist zudem kostenlos und plattformübergreifend nutzbar.

Sicherung

Die SuS bearbeiten Aufgabe 4 und fassen damit zusammen, welche Verschlüsselungsverfahren sie kennengelernt haben.

4 https://ogy.de/9tuf
5 https://ogy.de/hfpf

AB 3: Anhang: Fahrradsicherheit vs. Datensicherheit

Quelle: https://pixabay.com/en/bike-wheel-stadtrad-bike-lock-780049 (Pixabay-Lizenz: https://pixabay.com/de/service/license)

AB 3: Selbstdatenschutz durch Verschlüsselung

Aufgaben

1. Was bedeutet für dich der Begriff „Datensicherheit"?

2. Was tust du dafür, dass deine Daten online sicher sind?

3. Notiere mit eigenen Worten die Analogie zwischen einem Fahrrad(schloss) und dem Absichern der eigenen Daten.

4. Welche Möglichkeiten hast du kennengelernt, um deine Daten zu verschlüsseln?

Hausaufgabe

Falls du es nicht bereits im Unterricht installiert hast, installiere VeraCrypt zu Hause und berichte in der Klasse von deinen Erfahrungen. Folge diesem Tutorial: https://lehrerfortbildung-bw.de/werkstatt/sicherheit/stickcrypt/vc.
Es gibt aber auch zahlreiche andere Tutorials, bspw. auf YouTube. Achte darauf, woher du die Installationsdatei beziehst. Du solltest immer auf die Herstellerseite gehen, auch wenn Tutorials auf andere Quellen verweisen.

Methodisch-didaktische Hinweise zu AB 4: Passwort-Management und Back-ups (ab 14 Jahren)

Titel	**Passwort-Management und Back-ups**
Ziele	**Die SuS erarbeiten sich die Notwendigkeit von Selbstdatenschutz und erlernen Grundlagen zu Back-up-Lösungen und Passwort-Management.**
Unterrichtsstunden à 45 min.	1–2
Methoden und Material	Video, Gespräch, Live-Demonstration: KeePass (https://keepassx.org bzw. https://keepass.info)
Zugang Internet/PC	ja
Hinweise für die Durchführung	• Bestenfalls bringen die SuS eigene Rechner mit, um die Software Keepass direkt installieren und testen zu können (Einverständniserklärung für Software-Installation auf SuS-Geräten von Eltern via Elternbrief einholen). • Sollte die obige Variante nicht möglich sein, wird die Unterrichtseinheit zentral mit einem Präsentationsgerät durchgeführt. Davon wird im Folgenden ausgegangen. · Die SuS sollten jedoch dazu ermuntert werden, alles Zuhause auf den eigenen Geräten zu wiederholen. · **Wichtig:** Die hier verwendeten Tutorials sind wahrscheinlich nicht genauso auf Ihr System übertragbar. Testen Sie vorher alles.
Einstieg	Schauen Sie das Video „Passwörter einfach erklärt“ von Alexander Lehmann[1], welches auch auf https://klicksafe.de/klicksafetogo verlinkt ist. Die SuS sollen sich dazu bei Aufgabe 1 auf dem Arbeitsblatt bereits Notizen machen. *Welche Tipps gibt es im Video zu Passwörtern?* • Passwörter sollten lang sein (mind. 13 Zeichen). • Sie sollen Sonderzeichen, Zahlen, Groß- und Kleinbuchstaben enthalten. • Passsätze (auch Passphrasen genannt) sind oft leicht zu merken und lang → hohe Sicherheit. • Verwende nie ein bestimmtes Passwort für verschiedene Dienste (auch kein Single-Sign-in verwenden, z. B. über Facebook für einen anderen Dienst anmelden). • Ändere ein Passwort sofort, wenn es in falsche Hände gelangt ist. Dies kann zum Beispiel durch einen Website-Hack passieren oder weil man selbst das Passwort nicht ausreichend geschützt hat. • Verschicke deine Passwörter nie per Mail, denn unverschlüsselte E-Mails sind wie Postkarten – von Unbekannten lesbar. Wenn man wichtige Passwörter übermitteln muss, kann man sie bspw. zerteilen und auf verschiedenen, verschlüsselten Kommunikationskanälen verschicken. Generell sollte man seine Passwörter natürlich gar nicht preisgeben. **Passwörter werden oft Beute von Hackern** Zeigen Sie auf der Seite https://haveibeenpwned.com, dass in vielen Fällen bereits eigene Passwörter und Accounts gestohlen wurden und online gehandelt werden. Der Screenshot zeigt einen solchen Fall mit einer Mail-Adresse des Autors. Wenn eine Ihrer Mail-Adressen betroffen ist, sollten Sie diesen Fall zeigen. Alternativ probieren Sie einige Mail-Adressen von SuS durch.  Listete die Seite im Mai 2017 noch 2,6 Milliarden gehackte Zugangsdaten, waren es im November 2019 schon über 8,6 Millarden Zugangsdaten von insgesamt 412 Webseiten. *Quelle: https://haveibeenpwned.com (abgerufen am 10. 5. 2017)* Als optionale Überleitung zum nächsten Block (Passwortmanager) eignet sich ein kurzes Gespräch zwischen Edward Snowden und einem Reporter. Snowden diskutiert über sichere Passwörter. Doch am Ende sagt der Reporter, keine sicheren Passwörter verwenden zu wollen, weil ihm der Umgang damit zu kompliziert sei. https://tinyurl.com/txfqysb (leider nur auf englisch verfügbar)

1 https://ogy.de/kg2p

Erarbeitung

Im Video kam ein sogenannter Passwort-Tresor vor. Wir schauen uns einen solchen an, er heißt „KeePass“.

Führen Sie die Installation selbst zentral einmal durch. Alternativ schauen Sie sich zusammen dieses Beispiel-Tutorial an: https://youtube.com/watch?v=tX-Izo7o4a4

Die SuS installieren KeePass auf ihren mitgebrachten Laptops oder installieren die Software als Hausaufgabe.

Diskutieren Sie die Problematik, wenn man sein Master-Passwort (für den Tresor) vergisst oder falls es in falsche Hände gelangt oder eine solche Software Schwachstellen hat.

- Wie immer gilt: Bequemlichkeit und Sicherheit schließen sich gegenseitig aus. Manche Sicherheitsexperten lehnen daher Passwort-Manager grundsätzlich ab.
- Jeder soll eine eigene Risikobewertung durchführen und eine eigene Entscheidung treffen. (Anmerkung: Der Autor verwendet aktuell den Passwort-Manager KeePassX)
- Man muss dort nicht alle Passwörter ablegen; die hochsensitiven sind meistens wenige, und die kann man sich ggf. anders merken.

Alternativen zu KeePass
Es gibt viele Angebote neben KeePass, z. B. LastPass. KeePass hat sich in der Vergangenheit als zuverlässig erwiesen, ist kostenlos und plattformübergreifend. Der Quellcode ist für jedermann einsehbar. Wer trotzdem nach Alternativen sucht, kann hier weiterrecherchieren: https://ogy.de/yk7u.

Sind Daten verschlüsselt, ist der Zugriff für Unbefugte unterbunden. Sollen die Daten für einen selbst zugänglich bleiben, ist es wichtig, Sicherungskopien anzulegen. Denn es reicht nicht, sich ein Passwort zu merken, da Unbefugte auch ohne dieses in der Lage sind, die Daten unbrauchbar zu machen. Außerdem kann Technik ausfallen oder verloren gehen. Auch hiervor schützt ein Back-up. Gleichzeitig ist es wichtig, dass Benutzer sich benötigte Passwörter wie das Master-Passwort merken. Vergisst man beispielsweise das Passwort für den eigenen Passworttresor, hat man als Ersteller keinen Zugriff mehr auf die gespeicherten Daten.

Um Daten vor Unbefugten zu schützen, kann man sie verschlüsseln und mit einem sicheren Passwort versehen. Um uns vor ihrem Verlust zu schützen, sollten wir sie zudem regelmäßig mit einem Back-up sichern.

Was man beim Erstellen von Back-ups beachten sollte, lernen die SuS mit Aufgabe 2. Diese ist neben der auf dem Arbeitsblatt vermerkten 3-2-1-Regel die Sicherung.

Sicherung

Lösung:

Die folgenden Teile von Aufgabe 2 sind korrekt, die anderen sind zu streichen:

- Mache von den Daten, die dir wichtig sind, regelmäßig ein Back-up, indem du sie bspw. auf ein externes Laufwerk kopierst. Du kannst dieses jetzt sogar verschlüsseln, und das solltest du auch, wenn die Daten privat sind.
- Das externe Speichermedium sollte nie unnötig mit dem Rechner verbunden sein, damit es nicht von Viren befallen werden kann.
- Viele Betriebssysteme bieten eigene Back-up-Lösungen an, die man kennen und nach Bedarf auch nutzen sollte.
  Bemerkung: Dies kann als Hausaufgabe gestellt werden.
- Nachdem du ein Back-up gemacht hast, teste es. Sonst kannst du dir nicht sicher sein, dass es funktioniert, wenn du es brauchst.

klicksafe TO GO

1234567 abc123abc Hasi_007

AB 4: Passwort-Management und Back-ups

Aufgaben:

1. Das will ich mir zu Passwörtern merken:

Hausaufgabe:

Falls du es nicht bereits im Unterricht installiert hast, probiere den Passwortmanager KeePass Zu Hause aus und berichte in der Klasse von deinen Erfahrungen. Nutze dazu ein YouTube-Tutorial, wie z. B. „Passwörter verwalten mit KeePass 2" von PC Welt: www.youtube.com/watch?v=tX-lzo7o4a4

2. Nachdem du weißt, wie man Daten verschlüsselt und die dafür nötigen Passwörter verwalten kannst, lies den folgenden Text zu Back-ups. In diesen Text haben sich Fehler eingeschlichen. Streiche die aus deiner Sicht falschen Tipps durch!

- Mache von den Daten, die dir wichtig sind, regelmäßig ein Back-up, indem du sie bspw. auf ein externes Laufwerk kopierst. Du kannst dieses jetzt sogar verschlüsseln, und das solltest du auch, wenn die Daten privat sind.
- Ein Back-up soll nie verschlüsselt sein, damit man im Notfall sicher drankommt.
- Das externe Speichermedium sollte nie unnötig am Rechner hängen, damit es nicht von Viren befallen werden kann.
- Private Daten sollte man immer unverschlüsselt in der Cloud, also bei Onlinespeicherdiensten, ablegen. Da sind sie sicher.
- Viele Betriebssysteme bieten eigene Back-up-Lösungen an, die man kennen und nach Bedarf auch nutzen sollte.
- Nachdem du ein Back-up gemacht hast, teste es. Sonst kannst du dir nicht sicher sein, dass es funktioniert, wenn du es brauchst.
- Das Back-up (bspw. ein Stick) und die eigentlichen Daten (z. B. in deinem Laptop) sollten immer nebeneinanderliegen, damit man schnell auf das Back-up zugreifen kann.

Für Profis gibt es die 3-2-1-Regel

- Daten immer in **dreifacher** Kopie aufbewahren.
- Daten mit **zwei** verschiedenen Technologien sichern. Das können Festplatte, USB-Stick, CD, NAS, Cloud usw. sein.
- Immer **eine** Datensicherung außer Haus aufbewahren, bspw. im Banksafe oder bei den Eltern, nachdem man ausgezogen ist. Achte auf Verschlüsselung!

klicksafe wird kofinanziert
von der Europäischen Union.

Herausgeber:

klicksafe ist das deutsche Awareness Centre im CEF Telecom Programm der Europäischen Union.

klicksafe sind:

LMK – medienanstalt rlp –
www.medienanstalt-rlp.de

Landesanstalt für Medien NRW –
www.lfm-nrw.de

Bezugsadresse:
klicksafe
c/o LMK – medienanstalt rlp
Turmstraße 10
D-67059 Ludwigshafen
E-Mail: info@klicksafe.de
Web: www.klicksafe.de

klicksafe
TO GO