RECHNER UND NETZE

UNTERRICHTSVERLAUF

Thomas Schaller – E-Mail: t.schaller@gymnasium.ettenheim.de. – Januar 2017

Bild der Kopfzeile: „Netzwerkkabel“ von Blickpixel (ownwork) via *Pixabay* [*CC0 Public Domain*] (Abgerufen: 03.2017)

Grundgedanken zu dieser Unterrichtseinheit:

Die Schülerinnen und Schüler sollen ein grundlegendes Verständnis von der Struktur des Internets bekommen, um damit beurteilen zu können, welche Chancen und Risiken sich aus dieser Struktur ergeben. Dabei werden zum einen die verschiedenen Möglichkeiten der Datenspeicherung (lokal, im eigenen Netz und in der Cloud) als auch ein internetbasierter Dienst (hier WhatsApp als ein von vielen SchülerInnen eingesetzter Messengerdienst) behandelt. Dieser verdeutlicht das Client-Server-Prinzip.

Die Datenspeicherung in der Cloud und der Versand von Daten über das (unsichere) Internet machen die Notwendigkeit einer Verschlüsselung zur Erhöhung der Datensicherheit deutlich. Die SchülerInnen sollen erste, einfache Verschlüsselungsverfahren kennenlernen und anwenden können. Sie erkennen, dass diese einfachen Verfahren noch leicht angreifbar sind und in der Praxis bessere Verfahren eingesetzt werden müssen.

Aus dem Leben der Schülerinnen und Schüler sind Smartphones nicht mehr wegzudenken. Der Umgang damit erfolgt in der Regel unreflektiert. Es sollte Schülern bewusst sein, dass durch die Nutzung der Smartphones ständig digitale Daten anfallen, die von verschiedenen Diensten gesammelt werden. Im Zusammenhang mit der Internetkommunikation müssen von den SchülerInnen außerdem eine Vielzahl von Gesetzen und Regelungen zum Datenschutz und Urheberrechten beachtet werden. Der Unterricht in Informatik soll den Schülern auch hier ein Grundverständnis vermitteln.

Es ist klar, dass in den wenigen Stunden diese ganzen Aspekte nicht erschöpfend behandelt werden können. In Klasse 7 sollen die Schüler einen ersten Einblick erhalten, der in höheren Klassen aufgegriffen und vertieft wird. Es sollten aber alle angesprochenen Aspekte im Unterricht vorkommen und altersgemäß behandelt werden.

Bemerkung:

Da die Begriffe „Datenschutz“ und „Datensicherheit“ oft falsch verwendet werden, hier eine Definition:

Datenschutz: Hier geht es nicht, um den Schutz der Daten, sondern eher des Menschen. Es geht darum, dass jeder Mensch die Kontrolle über seine Daten behalten soll.

Datensicherheit: Hier geht es darum, dass die Daten nicht verloren gehen oder manipuliert werden. Es werden beispielsweise Backups angelegt, um die Datensicherheit zu gewährleisten.

Grundstruktur des Internets

Hintergrund für den Lehrer: `02_run_hintergrund_netzwerke.odt`
Das Hintergrunddokument geht deutlich über den Inhalt der Informatik in Klasse 7 hinaus und soll dem Lehrer ein fundiertes Grundwissen vermitteln und zeigen, welche weiteren Inhalte im weiteren Verlauf des Informatikunterrichts auf die Schüler zukommen werden.

Als Aufhänger ist in den hier vorliegenden Unterrichtsmaterialien der Messengerdienst „WhatsApp“ gewählt, da dieser bei den SchülerInnen weit verbreitet ist. Andere Messengerdienste funktionieren nach dem gleichen Prinzip.

Bei den Schülern herrscht manchmal die Idee vor, dass ihr Handy die Nachrichten in Messengerdiensten direkt auf das Handy des Empfängers schicken würde. Dies ist nicht der Fall. Die Nachrichten werden zunächst zum Server des Anbieters übermittelt. Auf dem Weg dorthin werden sie zunächst per Funk (z.B. UMTS / LTE) an eine Basisstation gesendet und vom Netzbetreiber dann in das Internet eingespeist. Dort werden sie über eine ganze Reihe von **Routern** weitergegeben und an den Server des Messengerdienst-Betreibers übermittelt.

Als Einstieg in den Unterricht kann der Anfang der Präsentation `01_run_kommunikation_client-server.odp` (bis Schritt 2: Übertragung über das Internet zum Server) verwendet werden. Diese thematisiert die Frage, wie Nachrichten eines Messagerdienstes von Sender zum Empfänger übertragen werden. Da die Arbeitsweise des Internets deutlich werden soll, wird die Präsentation an dieser Stelle unterbrochen und durch ein Rollenspiel ergänzt. Die Beschreibung findet sich in der Datei `03_run_rollenspiel_netzwerk.odt`. Dieses Rollenspiel veranschaulicht die folgenden Aspekte:

Ein grundlegendes Prinzip des Internets ist es, dass es **viele Wege zu einem Ziel** gibt. Es ist nicht vorhersagbar, welchen Weg die Daten nehmen, um zum Server zu gelangen. Dies variiert von Stunde zu Stunde je nach Auslastung der Datenverbindungen. Auch der Ausfall einer Verbindung führt zu einer Veränderung der Route. Der Weg führt aber immer über viele Router. Jeder Betreiber eines Routers auf dem Weg hat eine Zugriffsmöglichkeit auf die Daten. Dies ist wichtig, um beispielsweise zu verstehen, wie die NSA große Teile des Datenverkehrs im Internet abgreifen konnte (sie brauchten nur den Zugriff auf die Router, die große Knotenpunkte des Internets darstellen).

Es sollte als Sicherung ein schematisches Bild des Aufbau des Internets festgehalten werden, das deutlich macht, dass es sich um ein vermaschtes Netz / ungerichteten Graph handelt, dessen Knoten die Router bilden und dass an jedem Router die am Internet teilnehmenden Geräte angeschlossen sind (eigentlich hängen dort jeweils lokale Netze).

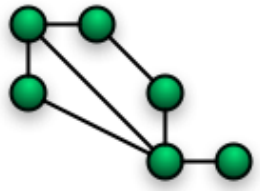

Bild: „NetworkTopologies.png“, Foobaz. URL: http://commons.wikimedia.org/wiki/File:NetworkTopologies.png (abgerufen: 4.1.2017) [gemeinfrei]

Nachdem die Schüler die Struktur des Internets verstanden haben, kann man nun mit der Präsentation fortfahren. Sie zeigt zunächst noch ein Bild eines grafischen Traceroute-Befehls, mit dem die Position der Router/Verbindungsstellen veranschaulicht werden können. Danach wird der weitere Weg der Nachricht zum Empfänger gezeigt:

Über das Internet wird die Nachricht aber nicht direkt zum Empfänger übertragen, sondern zum Server des Messengerdienstes. Der Server des Messengerdienstes ist ein Computer, der permanent läuft und auf dem ein Programm darauf wartet, dass ein Handy eine Anfrage sendet. Dies kann eine neue Nachricht sein, die versendet werden soll, es kann sein, dass es sich meldet, weil es wieder online ist, oder dass es nachfragt, ob neue Nachrichten bereitstehen. Dieses Programm zur Beantwortung von Anfragen nennt man Server (oft wird auch der Computer selbst Server bezeichnet, was aber zur Verwirrung der Schüler beiträgt. Es sollte daher nur das Programm als Server-Programm betitelt werden). Die App agiert als Client[1], der Anfragen stellt. Dies wird als **Client-Server Prinzip** bezeichnet. Die meisten der verteilten Anwendungen (z.B. WWW => Webserver – Webbrowser) arbeiten nach diesem Prinzip.

Vielen ist unklar, dass selbst wenn Sender und Empfänger in Deutschland sitzen, die Daten durchaus auf einem Server im Ausland (zwischen-)gespeichert werden können und damit nicht

1 Die Zustellung der Nachricht vom Server an die App funktioniert nicht so, dass die App streng nach dem Client-Server-Prinzip in regelmäßigen Abständen beim Server nachfragt, ob dort neue Nachrichten vorhanden sind. Tatsächlich sind dies sogenannte Push-Nachrichten, die vom Server zunächst mal an den Push-Dienst von Google, Apple oder Microsoft weitergegeben werden. Diese haben eine ständige Verbindung zum Handy (die vom Handy aufgebaut wird, sobald es online ist). Über diese Verbindung sendet der Push Dienst die Nachricht an das Handy. Dieses kann dann beim Server des Messenger-Dienstes nach weiteren Inhalten (z.B. hoch aufgelösten Bildern) nachfragen. Das läuft dann wieder nach dem Client-Server Prinzip ab. Diese Details müssen den Schülern aber nicht vermittelt werden.

Smokesignal-Blog: Wie funktionieren Push Nachrichten? (2015)
URL: *https://smokesignal.ch/de/blog/wie-funktionieren-push-nachrichten*

mehr dem europäischen Recht unterliegen. Die **Nutzung dieser Daten** ist die Geschäftsgrundlage der Anbieter von „kostenlosen“ Apps. Das muss den Schülern klar sein. Wir sind nicht die Kunden der Firmen, unsere Daten sind die Waren dieser Firmen. Die Werbetreibenden sind die Kunden der Firmen. Das muss nicht bedeuten, dass man diese Dienste deswegen nicht nutzen darf/sollte. Aber im Rahmen der **informationellen Selbstbestimmung** sollten die SchülerInnen diese Entscheidung selbst treffen und sich der Konsequenzen bewusst sein.

Wenn noch Zeit ist, kann noch auf die Problematik der Erstellung von Nutzerprofilen hingewiesen werden. Den Schülern muss klargemacht werden, dass sie im Internet nicht so anonym und unbeobachtet sind, wie sie vielleicht denken. Zum einen ist immer nachvollziehbar, welcher Nutzer welche Webseiten besucht und was er dort tut. Im Fall einer Strafanzeige oder Schadensersatzklage werden diese Informationen verwendet. Zum anderen gibt es eine Vielzahl von Firmen wie z.B. die Google-Tochterfirma DoubleClick, die das Surfverhalten von Nutzern beobachten und auswerten („Tracker“), um daraus Profile für die Werbewirtschaft zu erstellen.

Um die Verbindungen zwischen Webseiten und Trackern zu visualisieren, kann z.B. die Firefox-Erweiterung „Lightbeam“ verwendet werden. Als alltagstaugliche Hilfe sollte den Schülern gezeigt werden, wie man den eigenen Browser so einstellt, dass Cookies automatisch beim Schließen gelöscht werden.

Manche Smartphone-Apps sind zudem sehr neugierig und erfordern einen Zugriff auf die Standortdaten (GPS) des Geräts. Bei solchen Apps sollte man vorsichtig sein, da diese Positionsdaten oft an den Server des Betreibers übermittelt werden. Wenn Standortdaten für die Funktion der App nötig sind (z.B. Routenplaner), kann der Zugriff erlaubt werden, andernfalls sollte man sich gut überlegen, ob die App unbedingt nötig ist. Aus den Bewegungsdaten eines Nutzers können mehr Schlussfolgerungen gezogen werden, als man denkt.

Verschiedene Speicherorte

Hintergrund für den Lehrer: `04_run_hintergrund_cloud.odt`

Begleitende Präsentation: `02_run_dateispeicherung.odp`

Als Aufhänger wird hier die Frage verwendet, wie man große Datenmengen an andere Personen weitergeben kann. Die Schüler werden vor die Frage gestellt, wie sie eine 1 GB große Videodatei, die sie z.B. auf dem Handy oder einem USB-Stick dabei haben, an einen Freund schicken wollen. Dabei wird zwischen drei Situationen unterschieden: Der Freund befindet sich gerade auch im Computerraum; der Freund ist auch Schüler der Schule, kann aber nicht direkt getroffen werden; der Freund befindet sich im Ausland. Um im letzteren Fall Lösungen der Art „per Post oder Kurier schicken“ auszuschließen, wird die Zusatzbedingung gestellt, dass die Datei bis zum Abend beim Empfänger sein soll.

Bei kleinen Dateien (< 20 MB) ist es meist möglich, E-Mail oder Messenger-Dienste als Medium zu verwenden. Bei größeren Dateianhängen blockiert der Anbieter (von Sender oder Empfänger) allerdings den Versand. Die Datei im vorgestellten Szenario ist allerdings bei weitem zu groß, also sind andere Wege notwendig, die jeweils verschiedene Vor- und Nachteile haben.

Wenn der Empfänger sich im gleichen Raum befindet, kann die Datei „direkt“ kopiert werden. Entweder verwendet man einen Computer, um die Datei von USB-Stick zu USB-Stick zu kopieren oder man verschickt sie per Bluetooth-Verbindung über das Handy. Vorteile sind die hohe Geschwindigkeit (USB je nach Version zwischen 20 und 100 MB/s, Bluetooth in der neuesten Version bis zu 12 MB/s) und dass kein Dritter Zugriff auf die Daten hat.

Um eine Datei an einen Mitschüler zu schicken, den man nicht direkt treffen kann, kann man sie auf ein Tausch-Laufwerk im Schulnetz kopieren und dem Freund den Dateipfad (z.B. per Mail

oder Messenger) mitteilen. Dort kann dieser sie dann später auf sein Gerät kopieren. Dieses Vorgehen ist immer noch sehr schnell (Schulnetz zwischen 10 und 100 MB/s je nach Ausstattung). Der Nachteil ist, dass unter Umständen jeder Schüler und Lehrer der Schule die Datei ebenfalls abrufen kann.

Wenn beides nicht möglich ist, kommt ein Cloudspeicher zum Einsatz. Hier muss vermutlich erst allen Schülern erklärt werden, was ein Cloudspeicher überhaupt ist. Es bietet sich an, bei einem verbreiteten Anbieter zu demonstrieren, wie eine Datei hoch- und heruntergeladen sowie geteilt wird. Die Lösung für das Szenario ist also, die Datei beim Cloudspeicher der Wahl hochzuladen und die Datei mit dem Freund zu teilen. Der Vorteil des Cloudspeichers ist die weltweite Erreichbarkeit. Nachteile sind die (zusätzliche) Abhängigkeit von einem funktionierenden Internetzugang, die niedrige Geschwindigkeit (der Flaschenhals[2] ist hier der Internetzugang z.B. über DSL) und der mögliche Zugriff auf die Daten durch Dritte (Hacker oder Anbieter des Clouddienstes).

Es sollte dann besprochen werden, wo sich die Dateien eigentlich physisch befinden. Den Schülern muss klargestellt werden, dass Dateien sich grundsätzlich auf Datenträgern wie z.B. Festplatten befinden. Die Frage ist nur, wo sich jeweils die Festplatte befindet. Bei einer lokalen Speicherung befinden sich die Dateien auf der Festplatte, die direkt im Computer am Arbeitsplatz eingebaut ist – es bietet sich an, eine als Anschauungsobjekt mitzubringen. Eine Speicherung im Netzwerk bedeutet, dass die Dateien auf der Festplatte im Schulserver liegen. Hier bietet es sich – sofern möglich und praktikabel – an, den Schulserver mit der Klasse anzuschauen. Die Schüler sind oft erstaunt, dass der Server relativ unspektakulär aussieht. Wichtig ist aber, zu zeigen, dass auch der Server kein abstraktes Gebilde, sondern ein konkreter Computer in einem Zimmer ist.

Hinweis zur Präsentation: Auf Folie 3 wird die Struktur des Schulnetzes mit Windows-Clients skizziert. Hier gibt es für die Clients jeweils eine lokale Festplatte (C:). Dazu kommt das Laufwerk H:, das den „Eigenen Dateien“ („Home“) entspricht, auf die nur der Nutzer selbst Zugriff hat, sowie ein Laufwerk T: („Tausch“), auf das unter Umständen alle Nutzer des Schulnetzes Zugriff haben. Es gibt Netzwerkinstallationen, bei denen es ein solches Laufwerk nicht gibt, stattdessen gibt es z.B. Klassen-Tauschordner und Projekt-Tauschordner. Die Lehrkraft muss die Präsentation den örtlichen Gegebenheiten anpassen.

Die Speicherung in einer Cloud ist da etwas komplizierter. Die riesigen Datenmengen, die ein Cloudanbieter verwaltet, können nicht auf einem einzelnen Computer gespeichert werden. Stattdessen betreibt er eine oder mehrere Serverfarmen, also Gebäude, in denen hunderte oder tausende Server betrieben werden. Wo genau die Daten dann tatsächlich liegen, ist für den Endbenutzer nicht nachvollziehbar. Diese „Unfassbarkeit“ ist der Hintergrund des Begriffs „Cloud“. Es reicht, wenn die Schüler erkannt haben, dass ihre Daten irgendwo auf einem Server liegen, der unter Kontrolle des Cloudanbieters liegt. Wer sonst noch Zugriff auf die Daten hat, ist offen[3]. Man geht davon aus, dass die Daten vertraulich behandelt werden und vor Fremdzugriff gesichert sind, kann es aber nicht mit Sicherheit wissen.

Wenn die Schüler sehen, welchen Aufwand ein Cloudanbieter betreiben muss (Anschaffung, Betrieb und Wartung von hunderten Servern), ist ihnen leicht klarzumachen, dass dies mit immensen Kosten verbunden ist. Diese Kosten müssen wieder eingenommen werden – die

2 Als „Flaschenhals“ bezeichnet man in der Informatik aber auch der Logistik das langsamste Glied einer Kette von aufeinanderfolgenden Verarbeitungsschritten. Zum Beispiel wird auch eine schnelle Festplatte ausgebremst, wenn sie über eine langsame Schnittstelle ausgelesen wird – das System kann nicht schneller arbeiten als der langsamste Teilnehmer. Die Metapher kommt daher, dass beim Ausleeren einer Flasche der Durchmesser der schmalsten Stelle (der Hals) maßgeblich für die Geschwindigkeit ist.

3 Die Übertragung zum Cloudspeicher ist üblicherweise unproblematisch, da sie HTTPS-verschlüsselt sind. Fraglich ist nur, was mit den Daten passiert, wenn sie unverschlüsselt auf dem Server liegen.

Frage ist, wie? Den Schülern muss klargemacht werden, dass kein Angebot im Internet tatsächlich kostenlos ist. Es gibt immer jemanden, der dafür bezahlt und der hat knallharte geschäftliche Interessen. Wie offen diese gezeigt werden, ist unterschiedlich. Google bietet beispielsweise die Möglichkeit unter *http://myactivity.google.com* die gespeicherten Daten zu einem Google-Account einzusehen. Da bei der Nutzung eines Android-Smartphones ein Google-Account notwendig ist, sollten die meisten Schüler einen Account besitzen. Hat der Nutzer in den Datenschutzeinstellungen das Sammeln der Daten nicht explizit verboten, können hier Standortdaten, Youtube-Aufrufe uvm. des Nutzer über mehrere Jahre hinweg eingesehen werden.

Danach sollte die Problematik der Datensicherheit angesprochen werden: Wer kümmert sich darum, dass die Daten nicht verloren gehen? Beim Computer zuhause ist der Nutzer selbst dafür verantwortlich, ein Backup durchzuführen. Das Schulnetz wird von einem Administrator betreut, der (hoffentlich) ebenfalls ein regelmäßiges Backup durchführt. Bei Cloudspeichern wird vom Anbieter für ein Backup gesorgt, indem z.B. die Daten zwischen den einzelnen Serverfarmen hin und her kopiert werden. Hier stellt sich aber das Problem, dass für den Zugriff auf Clouddaten nicht nur der eigene Computer funktionieren muss, sondern dass auch der Internetzugang nutzbar sein muss und die Verbindung zum Cloudspeicher nicht getrennt sein darf. Was im Falle einer Insolvenz des Cloudanbieters mit den Daten passiert, ist zudem völlig unklar.

Zusammenfassend sollte den Schülern eingeschärft werden, dass (unverschlüsselte) sensible Daten nichts in der Cloud zu suchen haben und dass von wichtigen Daten immer eine Kopie im eigenen Computer existieren sollte.

Um die Inhalte zu festigen, kann das Quizspiel (`6_Software\1_quiz\Quiz.jar`) verwendet werden. Für die Ausführung des Programms ist Java 8 erforderlich. Das Programm kann den Schülern im Tauschlaufwerk bereit gestellt werden und von den SchülerInnen dort gestartet werden.

Sobald das Programm gestartet wurde, wählen die Schüler die Spieleranzahl (2-4). Die Schüler können der Reihe nach eine Frage aussuchen. Beantwortet der Spieler die Frage richtig, bekommt er die Punkte. Ist sie falsch, darf der nächste Spieler die Frage beantworten. Sie wird so lange weitergegeben, bis sie richtig beantwortet wurde. Unabhängig davon, wer die Frage richtig beantwortet hat, sucht danach der nächste Schüler eine Frage aus und darf sie als erster beantworten.

Die Fragen ergeben sich überwiegend aus den in der Präsentation angesprochenen Aspekten. Sie gehen aber auch darüber hinaus (z.B. historische Fragen, Anzahl Hosts im Internet). Dort dürfen die Schüler raten. Wenn Sie als Lehrer die Fragen auch verändern möchten, können Sie die Datei `questions.xml` bearbeiten, die alle Fragen enthält.

Rechte im Internet

Die Einleitung zur Stunde kann eine einfache Frage des L sein:

„Wir haben vor einer Weile besprochen, wie WhatsApp funktioniert. Seid ihr euch sicher, dass die Nachricht per WhatsApp tatsächlich nur beim gewünschten Empfänger gelesen werden kann? Und darf man eigentlich alles versenden, was man will?“

Nähere Informationen zur Durchführung des Unterrichtvorschlags und zu rechtlichen Hintergründen finden Sie unter `05_run_hintergrund_fallbeispiele.odt`.

Gesetzestexte sind von Natur aus von Juristen für Juristen formuliert und dem Normalbürger nicht immer sofort zugänglich, jüngeren Schülern schon gar nicht. Dies gilt natürlich auch für die Bestimmungen zum Datenschutz aus Bundes- und Landes-Datenschutzgesetz,

Kunsturheberrechtsgesetz und Strafgesetzbuch. Daher ist es schwer, diese in der Schule zu vermitteln. Lehrer sind außerdem keine Juristen. Wir können daher keine rechtsverbindlichen Aussagen machen und sollten dies auch nicht tun! Trotzdem stehen wir in der Verantwortung, rechtliche Regelungen mit den Schülerinnen und Schülern zu besprechen.

Daher sollen (fiktive) Fallbeispiele aus dem Bereich der Schule wesentliche Elemente der Gesetzeslage deutlich machen und zur Diskussion anregen. Die Fallbeispiele können dabei nicht alle rechtlichen Aspekte berücksichtigen, mit denen SchülerInnen in ihrem Alltagsleben konfrontiert werden. Für die Klasse 7 sehen die Bildungsstandards vor, dass die Schülerinnen und Schüler „in Grundzügen alltagsrelevante gesetzliche Regelungen zum Umgang mit (digitalen) Daten (Recht am eigenen Bild, Urheberrecht, informationelle Selbstbestimmung) nennen“ können. Daher wurden hier zwei Beispiele ausgewählt, die sich mit der Anfertigung und Verbreitung von Bildern im schulischen Umfeld beschäftigen. Häufig haben sich dabei Verfahren eingebürgert, die rechtlich nicht zulässig sind. Mindestens einer dieser Fälle sollte besprochen werden. Für andere Aspekte der Rechte im Internet sei auf die Materialien von Klicksafe.de verwiesen, die einen deutlich größeren Bereich abdecken.

Sicherheit bei mobilen Geräten

Hintergrund: `06_run_hintergrund_sicherheit.odt`

Wenn ein Smartphone verloren geht, ist der Verlust inzwischen nicht mehr nur auf den Wert des Geräts beschränkt. Ein Smartphone enthält inzwischen eine Menge persönlicher Informationen, die von einem Dieb ausgenutzt werden können. Das sind zum einen Zugangsdaten zu verschiedenen Online-Diensten und zum anderen enthalten App Stores z.B. Zahlungsinformationen, über die ein Dieb auf Kosten des Eigentümers digitale Waren einkaufen kann.

Zur Vorbereitung auf die Stunde sollte die Hausaufgabe aus `01_run_ab_handyverlust.odt` gestellt werden. Die Aufgabe in der Stunde selbst bearbeiten zu lassen, ist weniger sinnvoll, da das Schreiben einer brauchbaren Geschichte länger dauert und somit wenig Unterrichtszeit zur Besprechung übrig bleibt.

Idealerweise gehen die Schüler in ihren Geschichten auf Aspekte wie dem Missbrauch persönlicher Daten, Identitätsdiebstahl in sozialen Netzwerken und Betrug durch das Bezahlen über den App Store ein.

Im Unterricht sollte dann besprochen werden, wie die Probleme vermieden werden können. Gemeinsam werden die verschiedenen Verhaltensmaßnahmen (Bildschirmsperre, IMEI-Nummer aufschreiben usw.) besprochen und es sollte auf Vor- und Nachteile hingewiesen werden. Dazu sollte zur Datensparsamkeit angehalten werden: Was gar nicht erst auf dem Smartphone ist, kann nicht damit gestohlen werden.

Als Ergebnissicherung könnten eine Reihe von Sicherheitshinweisen erstellt werden, die einerseits im Vorfeld ergriffen werden und die andererseits im Fall des Diebstahls notwendig sind.

Datensicherheit und Verschlüsselungsverfahren

Hintergrunddokument: `07_run_hintergrund_kryptografie.odt`
Dieses Dokument geht deutlich über die in Klasse 7 verlangten Inhalte hinaus. Es dient dem Lehrer zur fachlichen Vorbereitung und zeigt, welche Inhalte im Bereich der Kryptologie in den darauffolgenden Jahren von den SchülerInnen gelernt werden sollen.

Das Internet stellt ein Medium für den Datentransport zur Verfügung. Viele verschiedene Anbieter stellen Dienste zur Datenspeicherung, zur Kommunikation, für Bankgeschäfte usw. zur Verfügung. Diese Dienste sind praktisch und werden zunehmend mehr genutzt. Auf der anderen

Seite wird von Kriminellen (z.B. Phishing, Diebstahl von Zugangsdaten oder Kreditkartendaten) oder auch staatlichen Behörden (z.B. NSA-Skandal) versucht, die Daten auszuspähen oder Server anzugreifen. Jedem, der das Internet nutzt, sollte bewusst sein, wie sicher oder unsicher die Nutzung des Internets ist.

Grundsätzlich spielten bei der Konzeption des Internet Fragen der Datensicherheit keine große Rolle. Bei der Datenübertragung wird lediglich sicher gestellt, dass die Daten vollständig und ohne Übertragungsfehler ankommen. Gegen Mitlesen oder bewusster Veränderung der Daten sind keine Maßnahmen ergriffen worden. Erst durch den Einsatz von Verschlüsselungsverfahren (z.B. https statt http als Übertragungsprotokoll beim WWW) werden die Vertraulichkeiten und Datenintegrität gewährleistet. Ohne diese Maßnahmen ist das Internet vergleichbar mit dem Versenden von Postkarten. Jeder Postbote (entspricht den Routern im Internet) kann die Postkarte lesen, wegwerfen, verändern, austauschen usw.

WhatsApp hat erst im Jahr 2016 eine Verschlüsselung der Nachrichten eingeführt. Davor wurden die Nachrichten unverschlüsselt übertragen. Nun sind die Daten Ende-zu-Ende verschlüsselt. Dies wird den Nutzern bei jedem neuen Kontakt einmal mitgeteilt. Die SchülerInnen kennen diese Meldung, wissen aber in der Regel nicht, was sie bedeutet. Daher bietet sich dies als Einstieg in diese Thematik an. Aber auch bei der Nutzung von Cloud-Datenspeichern kann man sich überlegen, dass der Administrator ohne Verschlüsselung Zugriff auf die gespeicherten Daten hat. Dies ist bei sensiblen Daten sicher nicht erwünscht.

WhatsApp tauscht am Beginn des Chats mit einem asymmetrischen Verschlüsselungsverfahren die Schlüssel für ein symmetrisches Verfahren aus. Danach wird dieses symmetrische Verfahren für die Verschlüsselung der Nachrichten verwendet. Das asymmetrische Verfahren ist notwendig, da die Apps der Kommunikationspartner ohne ein Zutun der Nutzer einen Schlüsselaustausch durchführen sollen. Auch die Firmenzentrale/Server von WhatsApp besitzen die Schlüssel zum Entschlüsseln der Nachrichten (auch der Bilder) nicht. Diese asymmetrischen Verfahren sind leider recht schwer zu verstehen und daher für Klasse 7 noch nicht geeignet. In Klasse 7 sollen anhand von einfachen symmetrischen Verfahren einige grundlegende Begriffe (Klartext, Kryptotext, Schlüssel, Verschlüsselungsverfahren, Verschlüsseln, Entschlüsseln) eingeführt und eingeübt werden. Mögliche Angriffe (Brute Force und Häufigkeitsanalyse) auf diese Verfahren zeigen, dass sie noch nicht sicher genug sind. Sichere, in der Praxis verwendete Verfahren (z.B. AES – Advanced Encryption Standard) sind aber deutlich komplizierter und können in der Schule im Detail nicht besprochen werden. Bei der Verwendung eines symmetrischen Verfahrens zum Austausch geheimer Nachrichten innerhalb der Klasse wird auch die Problematik des Schlüsseltauschs deutlich. Dieser kann nicht ebenfalls auf einem Zettel durch die Klasse geschickt werden, sondern muss im Vorfeld in geheimer Absprache festgelegt werden (ein sicherer Kanal ist notwendig).

Der Einstieg in die Thematik erfolgt wieder über eine Präsentation: `03_run_sicherheit_im_internet.odp`. Dabei wird wieder ausgehend von Ende-zu-Ende-Verschlüsselung von WhatsApp und Speicherung von Daten in der Cloud deutlich gemacht, wer Zugriff auf unverschlüsselte Daten hätte. Die grundlegenden Fachbegriffe der Kryptologie sollten anhand dieser Präsentation eingeführt werden. Es muss darauf geachtet werden, für die Ver-/Entschlüsselung nicht das Wort Codierung zu benutzen, da ein Code im Allgemeinen keinen geheimen Schlüssel verwendet (z.B. ASCII-Code). Ein Synonym zu Verschlüsselung wäre Chiffrierung.

Danach sollen die SchülerInnen zwei einfache Verfahren (Cäsar-Verschlüsselung und monoalphabetische Verschlüsselung) kennenlernen. Sie lernen zunächst jeweils das Verfahren kennen, verschicken Nachrichten in der Klasse und versuchen dann, den Code zu brechen. Dazu benötigen sie beim Cäsar das Arbeitsblatt `05_run_ab_caesar.odt` und die Bastelmaterialien `05_run_caesar-rad.pdf` und dazu je eine Musterbeutelklammer. Einige

ergänzende Fragen runden das Aufgabenblatt ab. Die Lösungen befinden sich im Unterordner Lösungen. Den Angriff auf die Verschlüsselung kann man auch zeitgleich mit der ganzen Klasse durchführen und jedem Schüler eine Verschiebung zuordnen. Das beschleunigt das Brute-Force-Verfahren.

Verschlüsselungsverfahren (Teil 2)

In der darauffolgenden Stunde lernen sie die monoalphabetische Verschlüsselung analog zur Cäsar-Verschlüsselung kennen. Zunächst wird das Cäsar-Verfahren kurz wiederholt. Dazu kann das Scratch-Projekt `5_praesentationen\04_run_caesar-chiffre.sb2` eingesetzt werden. Dies stellt die Verbindung zur Scratch-Einheit her und zeigt, dass in Scratch auch völlig andere Algorithmen als Spiele implementiert werden können. Danach wird das Cäsar-Verfahren erweitert: Die Cäsar-Scheibe wird für die monoalphabetische Verschlüsselung wiederverwendet und mit einer willkürlichen Buchstabenfolge versehen. Man kann die Scheibe dann immer noch drehen und hat mit der willkürlichen Buchstabenkombination 26 Varianten. Den Schülern muss aber klar werden, dass es jetzt nicht nur 26 Möglichkeiten gibt, sondern dadurch dass man am Anfang die Buchstaben willkürlich verteilt hat, sind es 26! ≈ 4 * 10^{26} = 400 Quadrillionen Möglichkeiten.

Trotzdem kann man den Kryptotext mit etwas Aufwand durch eine Häufigkeitsanalyse brechen. Allerdings klappt das nur bei nicht zu kurzen Texten. Diese von Hand auszuzählen ist sehr mühselig. Daher sollen die Schüler das Programm `6_software\2_breakmono\BreakMono.jar` verwenden (Java 8 muss installiert sein, dann kann das Programm einfach im Tauschlaufwerk zur Verfügung gestellt werden). Dazu fügen die SuS den Kryptotext in das obere Textfeld ein. Mit Hilfe der 10 häufigsten Buchstaben, Bigramme und Doppelbuchstaben lassen sich die 8-10 ersten Buchstaben ermitteln: Das E ist der häufigste Buchstabe, aus den Bigrammen ER und EN kann das R und das N erschlossen werden. C und H sind auch eindeutig, da das Bigramm CH sehr häufig auftaucht, die Buchstabenhäufigkeiten von C und H einzeln aber gering sind und daher nicht in der Liste der Einzelhäufigkeiten auftauchen. Bei den Doppelbuchstaben sticht vor allem die häufigste Kombination (SS) hervor. Damit hat man schon E, N, R, C, H, S. T und I als recht häufige Buchstaben können auch noch geraten werden. Danach schaut man sich den entschlüsselten Text und sucht nach Wörtern, die man raten kann. Die neuen Buchstaben trägt man ein. Trägt man aus Versehen zweimal den gleichen Buchstaben ein, zeigt das Programm dies rot an.

Der Text ist so gemacht, dass die Häufigkeiten ziemlich gut mit den normalen Häufigkeiten im Deutschen übereinstimmen. Wenn Sie einen anderen Text verwenden wollen, achten Sie darauf, da das Brechen des Codes sonst deutlich schwieriger wird. Längere Texte entsprechen automatisch der üblichen Verteilung. Um auf einfache Weise Texte mit der monoalphabetischen Verschlüsselung zu verschlüsseln, können Sie das Programm `6_software\4_monoalphabetische_substitution\MonoalphabetischeSubstitution.exe` verwenden.