Informationssicherheit

Dieses Unterrichtspaket beinhaltet flexibel gestaltete Stundenbilder (samt zugehörigem Material), um Schüler_innen einige Konzepte der Informationssicherheit (Verschlüsselung, digitale Signaturen, Einwegfunktionen, sichere Passwörter, ...) zu lehren. Insgesamt befinden sich auf den nachfolgenden Seiten fünf Stundenbilder (5x 100 Min.). Die gesamte geplante Unterrichtszeit beläuft sich also auf 500 Minuten oder 10 Unterrichtsstunden, wobei die letzte Einheit (1x 100 Min.) überwiegend dem Wiederholen und Festigen bekannter Inhalte gewidmet ist, wobei natürlich auch Versäumnisse aufgeholt werden können bzw. bekannte Inhalte weiter vertieft werden können.

Es werden keine Informatik-Kenntnisse vorausgesetzt, jedoch sollten die Schüler_innen bis zu einem gewissen Grad vertraut mit dem Umgang mit einem PC und dem Internet sein (USB-Stick, E-Mails versenden, etc.). Als Zielgruppe wurde eine 6. Klasse AHS oder höher gewählt (15 Jahre aufwärts).

Allgemeine Ziele

- Schüler_innen lassen ihrer persönlichen Informationssicherheit einen größeren Stellenwert zukommen
- Schüler_innen können den grundlegenden Sinn und Nutzen von Informationssicherheit erklären und schildern, welche Bereiche sie persönlich besonders betreffen
- Schüler_innen können sichere Passwörter erstellen und verwenden sichere Anmeldemethoden
- Schüler_innen können zwischen den bekanntesten Virenarten und Malware unterscheiden, deren Funktionsweise erklären und Maßnahmen einrichten, wie man sich vor diesen schützt
- Schüler_innen können den Nutzen von und Unterschied zwischen symmetrischer und asymmetrischer Verschlüsselung erklären und relevante Beispiele nennen
- Schüler_innen können den Nutzen digitaler Signaturen erklären, deren Anwendungsbereiche schildern und sie in Online-Kommunikationen verwenden

Vormerkungen

Während jeder Unterrichtseinheit sollte die Lehrkraft regelmäßig die wichtigsten Begriffe, Konzepte, Erkenntnisse, etc. auf die Tafel schreiben. Schüler_innen sollen diese in einem

kollaborativ angelegten Online-Dokument (z.B. Etherpad, Google Drive, ...) zusammentragen und durch eigene Notizen ergänzen. Diese Mitschrift dient als Lernunterlage für einen Test und als ständige Wissens-Ressource während der vielen Projektarbeiten, auf die zu jeder Zeit zurückgegriffen werden kann (und soll).

Es soll zudem angemerkt werden, dass die hier vorgelegten Stundenbilder nicht in Stein gemeißelt sind. Sie zeigen lediglich eine Variante von vielen auf, wie der Unterricht gestaltet werden kann. Die Stundenbilder müssen für jede Klasse leichter oder stärker angepasst werden. Wenn eine Klasse langsamer bzw. schneller arbeitet, als geplant, können natürlich gewisse Themenbereiche nach hinten oder vorne geschoben, zusätzlich hinzugefügt oder stattdessen entfernt werden.

Stundenbilder

Einführung in Informationssicherheit

Stundenbild-ID ITSec/1

Dauer 100 Min.

Thema Grundkonzepte der Informationssicherheit

Unterrichtsziele

- Es wurde eine Mindmap über das Thema „Informationssicherheit" auf die Tafel gezeichnet
- Schüler_innen haben verschiedene Definitionen von Informationssicherheit entwickelt und diese mit im Internet verfügbaren Definitionen verglichen
- Alle Schüler_innen haben dabei mitgeholfen, eine Textpassage aus der Datei „IT-Security – Sichere Nutzung der IKT im Alltag" (siehe [1]) auszuarbeiten und zu präsentieren
- Alle Schüler_innen haben einige Begriffe der Informationssicherheit, die in der Datei „Informationssicherheit Begriffe.docx" aufgelistet sind, mit eigenen Worten und Beispielen erklärt.

Hilfsmittel Tafel, Beamer, Internet, Browser, USB-Stick

Einleitung

1. Schüler_innen bekommen 2 Minuten Zeit, alle Begriffe aufzuschreiben, die sie mit Informationssicherheit verbinden. Danach werden die Begriffe auf der Tafel gesammelt in Form einer Mindmap.

2. Schüler_innen bekommen 2 Minuten Zeit, um eine Definition von Informationssicherheit zu entwickeln. Es werden danach die verschiedenen Definitionen vorgelesen und die Schwerpunkte jeder Definition hervorgehoben. Danach wird sie mit Definitionen aus dem Internet (z.B. Wikipedia, Google Suche) verglichen werden.

Stundenkern / Ertragssicherung

3. Die Begriffe, die in der Datei „Informationssicherheit Begriffe" aufgelistet sind, werden an die Tafel geschrieben und die Schüler_innen schreiben diese ab. Alternativ kann allen Schüler_innen die Liste in digitaler Form ausgehändigt werden.

4. Die Liste zählt stichwortartig wichtige Konzepte der Informationssicherheit auf, wobei die meisten den Schüler_innen noch unbekannt sein werden. Im Laufe dieser und der nächsten Unterrichtseinheiten werden die auf der Liste genannten Konzepte näher behandelt. Schüler_innen sollen nach und nach die Liste mit eigenen Erklärungen füllen. Ziel ist, dass ganz am Ende der Unterrichtssequenz (d.h. am Ende der letzten Unterrichtseinheit dieses Unterrichtpakets) alle Schüler_innen jeden Begriff mit eigenen Worten in 3-5 Sätzen und mit mindestens 1-2 Beispielen erklärt haben. Dieses Dokument muss dann auch zur Bewertung eingereicht werden.

5. Gruppenarbeit. Schüler_innen werden in 2er oder 3er Gruppen aufgeteilt. Jede Gruppe bekommt einen Teil (einige Seiten) des IT-Security Skripts (siehe [1]) zugewiesen.

6. Jede Gruppe arbeitet die Kernaussagen und alle wichtigen Konzepte, die in ihrer Textpassage vorkommen, heraus und erstellt eine Präsentation. Zusätzlich sollen im Kontext jedes besprochenen Konzepts auch ein bis zwei konkrete Beispiele genannt werden. Diese können (sofern vorhanden) aus der Textpassage genommen werden, können online recherchiert werden oder die Schüler_innen denken sich plausible Beispiele selbst aus. Die Präsentation soll textlich wie visuell relativ simpel gehalten werden. Alle Gruppenmitglieder sollen gleichmäßig zur Präsentation beitragen. Folien dürfen nur einzelne Stichworte beinhalten und es darf kein Text abgelesen werden. Da die Vortragenden den Inhalt ihrer jeweiligen Textpassage auch tatsächlich verstehen müssen, um die Informationen akkurat weitergeben zu können, muss ihnen auch genügend Vorbereitungszeit und Präsentationszeit zur Verfügung gestellt werden. Es kann auch betont werden, dass bei der Präsentation weniger der formale Grad im

Vordergrund steht, sondern die akkurate Wissensvermittlung. Das Internet darf für zusätzliche Recherche verwendet werden.

7. Schüler_innen arbeiten ihre Präsentationen aus während die Lehrkraft als Hilfskraft bei Fragen zur Seite steht
8. Jede Gruppe präsentiert den Inhalt ihrer Textpassage. Es sollte darauf hingewiesen werden, dass Schüler_innen aufmerksam zuhören, Notizen mitschreiben und bei Unklarheiten Fragen stellen sollen. Viele der Begriffe, die sich in der Datei „Informationssicherheit Begriffe.docx" befinden, werden bei den Gruppenpräsentationen bereits Erwähnung finden. Allerdings wird hier Schüler_innen eher ein Überblick geboten. In zukünftigen Unterrichtseinheiten werden zahlreiche Begriffe nochmals (genauer) behandelt.

Hausübung

9. keine

Digitale Signaturen

Stundenbild-ID ITSec/2

Dauer 100 Min.

Thema Den Nutzen und die Funktionsweise von digitalen Signaturen verstehen

Unterrichtsziele

- Das Spiel/Die Demonstration, wie eine Nachricht abgefangen und geändert werden kann, wurde durchgearbeitet
- Alle Schüler_innen haben selbständig oder in kleinen Gruppen die Aufgabenstellungen des Arbeitsauftrags über digitale Signaturen gemacht und am Ende (evtl. mithilfe der Lehrkraft) alle Fragen richtig beantwortet
- Die Lehrkraft hat für mehrere bekannte Nachrichtendienste (z.B. Webmail, Webchat…) demonstriert, wie man bei diesen eine digitale Signatur erstellt
- Alle Schüler_innen haben weiter an der Datei „Informationssicherheit Begriffe.docx" gearbeitet und einige neue Begriffe mit eigenen Worten und Beispielen erklärt

Hilfsmittel Tafel, Beamer, Internet, Browser, USB-Stick, evtl. Outlook, Thunderbird, o.Ä.

Einleitung

1. Spiel/Demonstration.
    a. Die Lehrkraft wählt (ohne Schüler_innen zu informieren) zwei Personen im Raum aus, die weit voneinander entfernt sitzen. Danach holt sie drei Schüler_innen, die zwischen diesen beiden Personen sitzen, zu sich nach vorne, sodass, egal welchen Pfad eine Nachricht von Person A nach B nimmt, dieser über mindestens eine der drei Schüler_innen geht. Die drei Schüler_innen bekommen den Auftrag, jede Nachricht, die an ihnen vorbeigeschickt wird, zu verfälschen, indem sie die Bankdaten der Originalnachricht durch andere Bankdaten (sehr offensichtlich) ersetzen (z.B. „`Konto 999999, BLZ 33033`").
    b. Danach wird noch Person A geholt und angewiesen, die folgende Nachricht an Person B zu senden:

```
To: <Name von Person B>
From: <Name von Person A>
Message: Überweisen Sie bitte 110 Euro an die RAIKA,
Konto 202020, BLZ 12345. Danke! LG <Person A>
```

    c. Person A schreibt diesen Text auf einen Zettel und reicht ihn einer Person, die neben ihr sitzt. Alle Schüler_innen werden nun durch die Lehrkraft darauf hingewiesen, dass sie, sofern sie die Nachricht erhalten, jeweils auf einen neuen Zettel kopieren müssen. Dabei müssen sie eine identische Kopie vom Original anfertigen. Dann reichen sie die Nachricht an eine andere Person weiter, die neben ihnen sitzt. Das Kopieren ist zwar langwierig, spiegelt aber einerseits die Funktionsweise von Netzwerken wider und erlaubt den drei Personen, die die Nachricht verfälschen sollen, unentdeckt zu bleiben.
    d. Dieser Vorgang wird wiederholt, bis die Nachricht am Ziel angekommen ist.
    e. Person B liest dann die Nachricht laut vor. Es sollte bei allen, die die ursprüngliche Nachricht gesehen haben, Verwirrung stiften.
    f. Die Lehrkraft deckt den „Betrug" auf und weist auf die möglichen Konsequenzen hin. Die Nachricht wurde irgendwo auf dem Weg verfälscht und in diesem besonderen Fall hätte es sein können, dass Geld auf das falsche Konto überwiesen worden wäre.
2. Schüler_innen bekommen einige Minuten Zeit.

3. Die Schüler_innen werden dann gebeten, Lösungsvorschläge zu machen. Wie hätte man die Nachricht sicher über ein ungeschütztes/unsicheres Netzwerk schicken können?

Stundenkern / Ertragssicherung

4. Arbeitsauftrag. Schüler_innen bekommen einen Ausdruck oder die digitale Version der Datei „Arbeitsauftrag Digitale Signatur.docx" und arbeiten entweder selbständig oder in 2er-Gruppen an den Aufgabenstellungen. Ihnen muss genügend Zeit gegeben werden, um die Internetrecherchen durchzuführen.

5. Während die Schüler_innen arbeiten, steht die Lehrkraft als Hilfskraft zur Verfügung. Sollten einige Schüler_innen viel schneller die Aufgabenstellungen erfüllt haben als die anderen, können die Antworten inspiziert und auf eventuelle Fehler oder Ungereimtheiten hingewiesen werden oder detailliertere Antworten eingefordert werden. Zusätzlich und/oder alternativ können diese Schüler_innen den anderen beim Ausarbeiten helfen oder sich in der Zwischenzeit der Ausarbeitung der Datei „Informationssicherheit Begriffe.docx" widmen.

6. Die erste Seite der Datei „Arbeitsauftrag Digitale Signatur.docx" kann währenddessen auf die Wand projiziert werden, und für die Online-Recherche nützliche Tipps und Links sowie die Uhrzeit, zu der die Arbeit abgeschlossen sein muss, anzuzeigen.

7. Im Anschluss werden die Ergebnisse kontrolliert, indem verschiedene Schüler_innen/Gruppen ihre Antworten vorlesen. Die Lehrkraft stellt sicher, dass alle Fragen richtig beantwortet wurden und etwaige Fehler/Missverständnisse beseitigt werden. Es kann darauf hingewiesen werden, dass diese Ausarbeitung Teil der Prüfungsunterlagen darstellt und auch für die „Informationssicherheit Begriffe.docx"-Mitschrift wichtig ist.

8. Schüler_innen können nun befragt werden, welche Software sie verwenden, um Nachrichten zu senden. Für einige der Software-Applikationen können dann von der Lehrkraft vorgezeigt werden, wie man digitale Signaturen anlegt.

    a. Desktop-Clients: OpenPGP oder EnigmaGPG für Programme wie Outlook oder Thunderbird

    b. Für Web-Applikationen wie Gmail kann beispielsweise EnigmaGPG als Browser-Erweiterung hergezeigt werden

    c. Mobilgeräte wie z.B. WhatsApp, Telegram, TextSecure/Signal

d. Bürgerkarte / Handy-Signatur besprechen
https://www.digitales.oesterreich.gv.at/site/cob__52135/7918/default.aspx
sowie mögliche Einsatzbereiche:
https://www.digitales.oesterreich.gv.at/site/6476/default.aspx

Hausübung

9. Die Lehrkraft gibt den Schüler_innen ihre E-Mail-Adresse bekannt. Als Hausübung sollen alle Schüler_innen bis zu einer festgelegten Frist eine Nachricht mit gültiger Signatur an diese Adresse senden.

Verschlüsselungsverfahren

Stundenbild-ID ITSec/3

Dauer 100 Min.

Thema Die Funktionsweise von modernen oft genutzten Verschlüsselungsverfahren

Unterrichtsziele

- Die Lehrkraft hat zu Beginn der Unterrichtseinheit die Funktionsweise der ROT1 und ROT13/Caesar-Verschlüsselung demonstriert
- Das Spiel/die Demonstration wurde mindestens einmal für jeweils symmetrische, asymmetrische und hybride Verschlüsselung durchgearbeitet
- Alle Schüler_innen haben selbständig oder in kleinen Gruppen die Aufgabenstellungen des Arbeitsauftrags über Verschlüsselung gemacht und am Ende (evtl. mithilfe der Lehrkraft) alle Fragen richtig beantwortet
- Die Funktionsweise der symmetrischen, asymmetrischen und hybriden Verschlüsselung wurde am Ende der Stunde noch einmal in grafischer Form (z.B. Zeichnung auf Tafel) wiederholt
- Alle Schüler_innen haben weiter an der Datei „Informationssicherheit Begriffe.docx" gearbeitet und einige neue Begriffe mit eigenen Worten und Beispielen erklärt

Hilfsmittel Beamer, Internet, Browser, USB-Stick, abschließbare Box/Schachtel, vier Schlösser und vier Schlüssel, wobei zwei Schlüssel und Schlösser identisch sein müssen (d.h. zwei Schlüssel müssen dasselbe Schloss aufsperren

können!)

Einleitung/Stundenkern

1. Anmerkung: Diese Unterrichtseinheit profitiert davon, dass sie im Anschluss zur Unterrichtseinheit über digitale Signaturen (IPSec/2) stattfindet.

2. Als Einstieg kann der Klasse über dem Beamer demonstriert werden, wie ROT1 und ROT13/Caesar-Verschlüsselung funktionieren. Dazu kann entweder die Tafel verwendet werden, um zu demonstrieren, wie man mit diesem Verfahren kurze Texte schnell verschlüsseln kann. Es kann auch das Programm „caesar" vorgezeigt werden (siehe auch „caesar.c).

3. Für den Rest der Stunde werden zeitgerechtere Verschlüsselungsalgorithmen AES (für symmetrische Verschlüsselung) und RSA (für asymmetrische Verschlüsselung) betrachtet.

4. Die Lehrkraft bereitet die Schlösser und Schlüssel vor der Unterrichtseinheit vor. Um symmetrische Verschlüsselung vorzuzeigen, wird am besten ein Schloss und zwei Schlüssel verwendet, wobei beide Schlüssel dieses Schloss aufsperren können. Um asymmetrische Verschlüsselung zu demonstrieren, werden zwei andere Schloss-Schlüssel-Paare benötigt. Es wird empfohlen, die jeweiligen Schlösser und Schlüssel richtig zu kennzeichnen (z.B. „symmetrisch", „asymmetrisch", „public", „private"), um ihren jeweiligen Verwendungszweck zu verdeutlichen und jegliche Verwechslungsgefahr zu vermeiden.

5. Spiel/Demonstration

    a. Die Lehrkraft demonstriert im Folgenden auf rudimentäre Art und Weise, mithilfe einer abschließbaren Box/Schachtel und mehreren Schlössern und Schlüsseln, wie symmetrische und asymmetrische Verschlüsselung funktioniert.

    b. Symmetrische Verschlüsselung: Die Lehrkraft wählt zwei Schüler_innen aus, die im Raum weit voneinander entfernt sitzen. Beide bekommen von der Lehrkraft ein Schloss und einen Schlüssel gereicht. Diese sind jeweils z.B. mit „symmetrisch" gekennzeichnet. Person A soll Person B nun eine vertrauliche Nachricht über ein unsicheres Netzwerk schicken (z.B. das Internet). Dazu schreibt sie ihre Nachricht (z.B. „Ich bin verschlüsselt") und „verschlüsselt" im Anschluss diese, indem sie die vertrauliche Nachricht in die Box legt und diese mit ihrem Schloss absperrt. Dann reicht sie die Box an eine Nachbarperson. Die Box wird solange von jeder Person an eine Nachbarperson weitergereicht, bis

sie bei der Zielperson B angekommen ist. Diese öffnet mit ihrem Schlüssel die Box und liest die Nachricht vor.

c. Dasselbe Szenario kann bei Bedarf ein zweites Mal mit zwei anderen Schüler_innen durchgeführt werden.

d. Im Anschluss wird Schüler_innen 2-3 Minuten Zeit gegeben, um mindestens zwei Vorteile und zwei Einschränkungen/Nachteile dieser Methode zu identifizieren. Die Antworten werden laut vorgetragen und kurz diskutiert. Die Lehrkraft schreibt die wichtigsten Punkte *stichwortartig* auf der Tafel mit.

e. Asymmetrische Verschlüsselung: Die Lehrkraft wählt zwei andere Schüler_innen aus, die im Raum weit voneinander entfernt sitzen. Person A erhält den Schlüssel „private A" und das Schloss „public A", während Person B den Schlüssel „private B" und das Schloss „public B" erhält. Danach erstellt Person A wieder eine vertrauliche Nachricht und legt sie in eine Box. Allerdings benötigt sie zum Abschließen das Schloss „public B" von Person B. Deshalb sendet in einem nächsten Schritt Person B ihr Schloss an Person A. Sobald angekommen, „verschlüsselt" Person A die Box, indem sie diese mit dem Schloss von Person B absperrt. Danach sendet sie die Box zurück zu Person A. Diese kann ihr eigenes Schloss mit ihrem Schlüssel öffnen und die Nachricht vorlesen.

f. Im Anschluss wird Schüler_innen 2-3 Minuten Zeit gegeben, um mindestens zwei Vorteile und zwei Einschränkungen/Nachteile dieser Methode zu identifizieren. Die Antworten werden laut vorgetragen und kurz diskutiert. Die Lehrkraft schreibt die wichtigsten Punkte wieder *stichwortartig* auf der Tafel mit.

g. Es sollte auch auf die Bedeutung von „symmetrisch" und „asymmetrisch" in diesem Zusammenhang eingegangen werden. Zusätzlich kann eine Eselsbrücke für Schüler_innen angeboten werden, um öffentliche (*public*) und private (*private*) Schlüssel den jeweiligen Personen einfach zuordnen zu können: Private Schlüssel dürfen immer nur genau einer einzigen Person bekannt sein, während öffentliche Schlüssel (= Schlösser) an eine beliebige Menge an Personen weitergereicht werden können.

h. Hybride Verschlüsselung: Diese Art der Verschlüsselung könnte nach demselben Prinzip durchgespielt und besprochen werden, wie symmetrische und asymmetrische Verschlüsselung. Alternativ können Schüler_innen auch fünf- bis

zehnminütiges Zeitfenster erhalten, in dem sie selbständig die Funktionsweise der hybriden Verschlüsselung recherchieren.

6. Arbeitsauftrag. Schüler_innen bekommen einen Ausdruck oder die digitale Version der Datei „Arbeitsauftrag Verschlüsselung.docx" und arbeiten entweder selbständig oder in 2er-Gruppen an den Aufgabenstellungen. Ihnen muss genügend Zeit gegeben werden, um die Internetrecherchen durchzuführen.
7. Während die Schüler_innen arbeiten, steht die Lehrkraft als Hilfskraft zur Verfügung. Sollten einige Schüler_innen viel schneller die Aufgabenstellungen erfüllt haben als die anderen, können die Antworten inspiziert und auf eventuelle Fehler oder Ungereimtheiten hingewiesen werden oder detailliertere Antworten eingefordert werden. Zusätzlich und/oder alternativ können diese Schüler_innen den anderen beim Ausarbeiten helfen oder sich in der Zwischenzeit der Ausarbeitung der Datei „Informationssicherheit Begriffe.docx" widmen.
8. Die erste Seite der Datei „Arbeitsauftrag Verschlüsselung.docx" kann währenddessen auf die Wand projiziert werden, und für die Online-Recherche nützliche Tipps und Links sowie die Uhrzeit, zu der die Arbeit abgeschlossen sein muss, anzuzeigen.
9. Im Anschluss werden die Ergebnisse kontrolliert, indem verschiedene Schüler_innen/Gruppen ihre Antworten vorlesen. Die Lehrkraft stellt sicher, dass alle Fragen richtig beantwortet wurden und etwaige Fehler/Missverständnisse beseitigt werden. Die richtigen Antworten können auch stichwortartig auf die Tafel geschrieben werden. Es kann darauf hingewiesen werden, dass diese Ausarbeitung Teil der Prüfungsunterlagen darstellt und auch für die „Informationssicherheit Begriffe.docx"-Mitschrift wichtig ist.

Ertragssicherung

10. Wichtige Aspekte sollten von der Lehrkraft nochmal im Detail durchgegangen werden. Um die verschiedenen Verschlüsselungsarten nochmals zu besprechen, können rudimentäre Zeichnung auf der Tafel als Denkhilfe hergenommen werden. Vor allem für den Verschlüsselungsprozess bietet es sich an, diesen nochmals auf der Tafel Schritt-für-Schritt zu visualisieren.

Hausübung

11. Schüler_innen sollen an der Datei „Informationssicherheit Begriffe.docx" weiterarbeiten.

Passwörter und Anmeldemethoden

Stundenbild-ID ITSec/4

Dauer 100 Min.

Thema Den Sinn von Passwörtern verstehen und sichere Passwörter erstellen und verwalten

Unterrichtsziele

- Es wurde diskutiert, wofür man Passwörter eigentlich benötigt, und alle Schüler_innen waren an der Diskussion beteiligt
- Es wurden verschiedene Aspekte des Umgangs der Schüler_innen mit Passwörtern diskutiert und alle Schüler_innen waren an der Diskussion beteiligt
- Die Lehrkraft hat erfolgreich vorgezeigt, wie einfach es sein kann, Passwörter in geleakten Datenbank-Dumps zu knacken
- Die Lehrkraft hat den Schüler_innen eine kurze Einführung/Erklärung bezüglich Hashes/Einwegfunktionen gegeben
- Alle Schüler_innen haben selbständig oder in kleinen Gruppen die Aufgabenstellungen des Arbeitsauftrags über Passwörter gemacht und am Ende (evtl. mithilfe der Lehrkraft) alle Fragen richtig beantwortet
- Alle Schüler_innen haben weiter an der Datei „Informationssicherheit Begriffe.docx" gearbeitet und einige neue Begriffe mit eigenen Worten und Beispielen erklärtWebseite-Hacks
- Alle Schüler_innen haben demonstriert, dass sie ein sicheres Master-Passwort für ihren Passwort-Manager anlegen können
- Alle Schüler_innen haben einen Test-Account angelegt (z.B. mit Wegwerf-E-Mail), und zwar mit einem im Passwort-Manager generiertem und dort abgespeicherten Passwort
-

Hilfsmittel Tafel, Beamer, Internet, Browser, USB-Stick, Passwort-Manager, Handy

Einleitung

1. Diskussion. Wofür braucht man Passwörter? Schüler_innen bekommen einige Minuten Zeit, um mindestens drei Gründe zu finden. Die wichtigsten Gründe werden auf der Tafel von der Lehrkraft stichwortartig zusammengetragen. Folgende Haltungen gegenüber Passwörtern sollten auf jeden Fall besprochen werden:
    a. Was sind sensible Daten? Erwartete Antworten: Gesundheit, Sexualleben, religiöse Überzeugung, philosophische Überzeugung, politische Meinung, rassische/ethnische Herkunft, Gewerkschaftszugehörigkeit …
    b. Schüler_innen, die als Antwort „sie haben nichts zu verstecken" geben, höflich bitten, ob sie der Lehrkraft ihr Handy samt Passwort reichen (natürlich nicht annehmen). Den Schüler_innen soll verdeutlicht werden, dass „nichts zu verstecken" bedeuten würde, dass es ihnen nichts ausmachen würde, alle Facebook-Nachrichten, WhatsApp-Konversationen, Fotos, persönliche Informationen, E-Mails, usw. öffentlich zu machen. Wenn sich die Schüler_innen weigern, der Aufforderung nachzukommen, können sie darauf hingewiesen werden, dass diese Haltung bedeutet, sie haben doch etwas zu verstecken.
    c. Zusätzlich kann argumentiert werden, dass man heutzutage mit vielen Menschen vernetzt ist und sensible Informationen über andere besitzt, von denen sie nicht möchten, dass diese weitererzählt werden. Hat man nichts zu verbergen, so würden auch diese Informationen preisgegeben werden, ohne Rücksicht auf die Wünsche anderer Personen. Dieses ethische Dilemma sollte auch angesprochen werden.

Stundenkern / Ertragssicherung

2. Diskussion und Umfrage. Die Lehrkraft fragt die Schüler_innen, wie sie mit ihren Passwörtern umgehen. Sie werden gebeten, jede gestellte Frage auf einem Zettel zu beantworten und dass sie das folgende Format beim Niederschreiben verwenden: <Fragenummer> | <Antwort auf Frage> | <eigene Einschätzung, wie „sicher" ihr momentanes Verhalten ist, wobei 1 für sehr gut/absolut ausreichend steht und 5 für nicht genügend>
    a. Wie viele verschiedene Passwörter verwendest du?
    b. Änderst du in regelmäßigen Abständen deine Passwörter?
    c. Aus wie vielen Zeichen bestehen deine Passwörter durchschnittlich?
    d. Welche Zeichen verwendest du in deinen Passwörtern (Großbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen…)?

e. Wo/Wie hast du deine Passwörter „abgespeichert" (Kopf, Zettel, Textdatei...)?

f. Welchen Grad an Sicherheit/Privatsphäre, glaubst du, bietet dein Passwort?

3. Danach können die Ergebnisse besprochen werden. Schüler_innen geben ihre Antworten auf die erste Frage bekannt sowie ihre Selbsteinschätzung. Danach folgt eine kurze Erklärung durch die Lehrkraft, wie idealerweise vorgegangen wird (z.B. bei Frage 1, dass jedem Login ein einzigartiges Passwort zugeteilt wird). So wird jede Frage einzeln durchbesprochen.

   a. Was sind Daten, die Firmen oder große Organisationen über euch speichern und wie/durch welche Dienste kommen sie zu diesen Daten?

      i. z.B. Suchanfragen, angemeldet surfen über User-Account, Surfverhalten, Online-Chat, Online-Profile, Kalender, installierte Apps am Handy, Kaufverhalten, App-Bewertungen, Location-/Ortungsdaten, Likes, Freundeskreis in sozialen Netzwerken, ...

   b. Wie gefährlich sind sensible Daten in den Händen von Personen aus dem näheren Umfeld (und die einen vielleicht nicht so mögen)?

   c. Wie gefährlich sind sensible Daten, auf die Firmen, Geheimdienste,

   d. Wenn wir über Google, Datenkrake Google, sprechen, welche „Daten" sammelt Google denn überhaupt? Irgendwelche Ideen?

4. Als nächstes soll gezeigt werden, dass man sich nicht auf die Sicherheitsmaßnahmen der Webseiten verlassen darf, sondern, sofern es in der eigenen Macht steht (und das tut es bei Passwörtern), selber Sicherheitsmaßnahmen anwenden. Da jährlich viele Dumps von Datenbank-Leaks ins Internet gestellt werden, würde es sich anbieten, wenn die Lehrkraft beispielsweise einen DB-Dump mit unslated MD5-Hashes herunterlädt, diesen anonymisiert und dann mithilfe Hashcrackern wie oclHashcat (siehe cudaHashcat-1.36.7z) vorzeigt, wie einfach es ist, kurze Passwörter zu entschlüsseln.

5. Es sollten auch Einwegfunktion bzw. Hashes und deren Einsatzbereiche noch kurz erwähnt werden. Allerdings sollten Informationen diesbezüglich noch eher seicht gehalten werden, da sich Schüler_innen sollen selbständig mit diesem Begriff im folgenden Arbeitsauftrag auseinandersetzen sollten.

6. Arbeitsauftrag. Schüler_innen bekommen einen Ausdruck oder die digitale Version der Datei „Arbeitsauftrag Passwörter.docx" und arbeiten entweder selbständig oder in 2er-

Gruppen an den Aufgabenstellungen. Ihnen muss genügend Zeit gegeben werden, um die Internetrecherchen durchzuführen.

7. Während die Schüler_innen arbeiten, steht die Lehrkraft als Hilfskraft zur Verfügung. Sollten einige Schüler_innen viel schneller die Aufgabenstellungen erfüllt haben als die anderen, können die Antworten inspiziert und auf eventuelle Fehler oder Ungereimtheiten hingewiesen werden oder detailliertere Antworten eingefordert werden. Zusätzlich und/oder alternativ können diese Schüler_innen den anderen beim Ausarbeiten helfen oder sich in der Zwischenzeit der Ausarbeitung der Datei „Informationssicherheit Begriffe.docx" widmen.
8. Die erste Seite der Datei „Arbeitsauftrag Passwörter.docx" kann währenddessen auf die Wand projiziert werden, und für die Online-Recherche nützliche Tipps und Links sowie die Uhrzeit, zu der die Arbeit abgeschlossen sein muss, anzuzeigen.
9. Im Anschluss werden die Ergebnisse kontrolliert, indem verschiedene Schüler_innen/Gruppen ihre Antworten vorlesen. Die Lehrkraft stellt sicher, dass alle Fragen richtig beantwortet wurden und etwaige Fehler/Missverständnisse beseitigt werden. Die richtigen Antworten können auch stichwortartig auf die Tafel geschrieben werden. Es kann darauf hingewiesen werden, dass diese Ausarbeitung Teil der Prüfungsunterlagen darstellt und auch für die „Informationssicherheit Begriffe.docx"-Mitschrift wichtig ist.
10. (optional) Kleinen Gruppen von Schüler_innen werden Themenbereiche zugeteilt, die in den letzten Unterrichtseinheiten durchgenommen wurden (z.B. asymmetrische Verschlüsselung,
11. In den letzten 25-30 Minuten der Unterrichtseinheit wird von der Lehrkraft demonstriert, wie ein Passwortmanager funktioniert und wie man ihn verwendet (z.B. anhand von Keepass demonstrieren). Schüler_innen sollen danach testweise selbständig ein sicheres Master-Passwort anlegen (welches sie der Lehrkraft bekanntgeben, um überprüfen zu können, ob das Passwort tatsächlich sicher ist) sowie ein Passwort generieren und auf einer beliebigen Seite austesten (z.B. neuen Benutzer mit Wegwerf-E-Mail und Test-Passwort anlegen).
12. Im Anschluss wird auch demonstriert, wie man Passwörter, die in einem Passwort-Manager gespeichert sind, auch am Handy verwenden kann (z.B. Keepass2Android https://play.google.com/store/apps/details?id=keepass2android.keepass2android_nonet (Android) und MiniKeePass https://itunes.apple.com/at/app/minikeepass-secure-password/id451661808?mt=8 (iOS))

Hausübung

13. (nur wenn Punkt 10 durchgeführt wird) Schüler_innen sollen für ihr zugewiesenes Thema eine fünf- bis zehnminütige Präsentation bis zur nächsten Unterrichtseinheit erstellen und diese vor dem Rest der Klasse präsentieren.

Rückstand aufholen und Wiederholung

Stundenbild-ID ITSec/5

Dauer 100 Min.

Thema Grundkonzepte der Programmierung

Unterrichtsziele
- Alle Schüler_innen haben die jeweiligen von der Lehrkraft geplanten Aktivitäten erfolgreich erfüllt bzw. ihr Wissen jeweils ausreichend demonstriert
- Alle Schüler_innen haben die Datei „Informationssicherheit Begriffe.docx" zur Benotung eingereicht.

Hilfsmittel Tafel, Beamer, Internet, Browser, USB-Stick

Anmerkung

1. Diese Unterrichtseinheit ist so konzipiert, dass Bereiche, die z.B. aus Zeitgründen zuvor nicht ausführlich besprochen werden konnten oder übersprungen werden mussten, jetzt besprochen werden können. Zusätzlich dient diese Stunde dazu, Fragen der Schüler_innen zu beantworten, die Datei „Informationssicherheit Begriffe.docx" fertig auszufüllen und wichtige Konzepte (z.B. Passwörter und Passwort-Manager) zu wiederholen. Im Folgenden werden einige Aktivitäten vorgeschlagen, die im Unterricht eingesetzt werden können.

Stundenkern

2. Wiederholung: Schüler_innen präsentieren in einer fünf- bis zehnminütigen
3. Wiederholung: Schüler_innen sollen je drei sicher Passwörter mit zwei verschiedenen Methoden erstellen (z.B. Aneinanderreihung von vier unzusammenhängenden Wörtern, komplexes Passwort dient als Basis und wird um z.B. Monatsnamen am Ende erweitert, um jedes Passwort einzigartig zu machen)
4. Wiederholung: Schüler_innen sollen einen Passwortmanager einrichten und eines der sicheren Passwörter als Master-Passwort verwenden. Danach sollen sie sich auf einer

Testseite mit z.B. einer Wegwerf-E-Mail und einem vom Passwort-Manager generierten Passwort anmelden und dies der Lehrkraft demonstrieren.

5. Wiederholung: Schüler_innen sollen die grundlegende Funktionsweise der in einer vorigen Unterrichtseinheit durchgenommenen Verschlüsselungsverfahren (symmetrische, asymmetrische, hybride Verschlüsselung) visualisieren. Diese Übung/Wiederholung ist kombinierbar mit anderen Unterrichtsinhalten, die bereits durchgenommen wurden. Beispielsweise können ein Bildbearbeitungsprogramm wie Adobe Photoshop, ein Videoschnittprogramm wie Adobe Premiere oder eine Programmier- oder Animationsumgebung wie Scratch oder Adobe Flash verwendet werden, um die Verschlüsselungsverfahren zu visualisieren. Alternativ kann natürlich auch per Hand gezeichnet werden.
6. Alle relevanten Themen und Punkte, die bisher nicht aufgegriffen wurden (oder werden konnten), können in dieser Einheit Erwähnung finden. Bereits besprochene Inhalte können weiter vertieft werden.
7. Schüler_innen können die Online-Quiz durcharbeiten: http://www.easy4me.info/microsoft-office-20072010/modul-8/
8. Schüler_innen verbringen den Rest der Unterrichtseinheit damit, an der Datei „Informationssicherheit Begriffe.docx" weiterzuarbeiten.

Hausübung

9. Sofern noch nicht in der Stunde eingereicht, sollen Schüler_innen an der Datei „Informationssicherheit Begriffe.docx" weiterarbeiten und diese bis zu einer im Vorhinein festgelegten Frist per E-Mail an die Lehrkraft senden.

Quellenangabe

1. easy4me.info (2015). „IT-Security – Sichere Nutzung der IKT im Alltag" http://www.easy4me.info/downloads/locked/it-sec_skriptum.pdf [29. Dezember 2015]
2. lct-dp (2012). lct-innovation-LPI-Fig-110-3_1.png. https://en.wikibooks.org/wiki/Ict-innovation/LPI/110.3#/media/File:Ict-innovation-LPI-Fig-110-3_1.png [29. Dezember 2015]