



Unterrichtsbeispiel: „Datenschutz“

Klasse: E1AT
Erstes Lehrjahr „Elektroniker/in für Automatisierungstechnik“
Fach: Lernfeld 4: „Informationstechnische Systeme bereitstellen“
Verfasser: Thomas Frietsch
Zeitumfang: 180 min

Hinweise:

- Der Unterricht findet in zwei 90-Minuten-Blöcken statt.
- In den Stunden zuvor wurden Bedrohungen auf IT-Systeme erarbeitet. Dabei ging es unter anderem um die Themen:
 - Viren, Trojaner
 - Botnetze
 - Social Engineering
- Die nachfolgende Unterrichtseinheit widmet sich dem Thema Backups.

Lernziele:

- Die Schülerinnen und Schüler (SuS) können die drei Schutzziele der Informationssicherheit benennen und an einem konkreten Beispiel anwenden.
 - Die SuS können E-Mails mittels S/MIME-Zertifikaten signieren.
 - Die SuS wenden Laufwerks- und Dateiverschlüsselungen an.
 - Die SuS erkennen sichere Websites im Internet (SSL) können asynchrone und synchrone Verschlüsselungsverfahren beschreiben
 - Die SuS wenden Methoden zur Passwortsicherheit an.
 - Die SuS kennen Regeln für die IT-Sicherheit in Unternehmen

Ablauf:

Block 1: (90 min)

Zeit	Inhalt	Medien	Sozialform
20 min	Schutzziele der Informationssicherheit erarbeiten	Digitales AB 1 (Video)	Einzelarbeit
10 min	Besprechung und Diskussion der Einzelergebnisse	Digitale Tafel	Plenum
5 min	Gruppeneinteilung und Erklärung der Aufgabenstellung	LearningApp zur Gruppeneinteilung Digitales AB 2	Lehrervortrag
50 min	Arbeiten in den Expertenrunden	Digitale AB 3a-3d	Gruppenarbeit
5 min	Abschluss: Wer ist wie weit gekommen?	-	Schüler-Lehrer-Gespräch

Hausaufgabe nach Block 1: Eigenes Expertenarbeitsblatt fertig machen, falls dies im bereits geschehen ist.





Block 2: (90 min)

Zeit	Inhalt	Medien	Sozialform
10 min	Arbeiten in den Expertenrunden Ziel: Alle Experten sind auf dem gleichen Stand	Digitale AB 3a-3d	Gruppenarbeit
60 min	Arbeiten in den Stammgruppen Ziel: Alle Schüler können alle Technologien anwenden	Digitale AB 3a-3d	Gruppenarbeit
20 min	Anwendung: Jeder sendet eine signierte E-Mail, die eine verschlüsselte Datei einhält (einheitliches Passwort / Inhalt: Textdatei mit Schülernamen) an Lehrkraft	E-Mail-Klient mit selbst zertifizierter SMIME-Signatur VeraCrypt	Einzelarbeit

Materialien:

Hinweis: Es handelt sich um Digitale Arbeitsblätter, die für die Anwendung OneNote entwickelt wurden. Diese sind nur bedingt auf einem gedruckten Dokument darstellbar.

Arbeitsblatt 1:

Schutzziele der Informationssicherheit

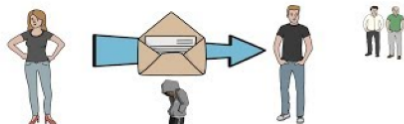
Aufgabe:

Schaue Dir das folgende Video an und beantworte die unten gestellten Fragen:

https://www.youtube.com/watch?v=H4f_Olfh4P0

SCHUTZZIELE DER INFORMATIONSSICHERHEIT

IN 3 EINFACHEN PUNKTEN ERKLÄRT!



Fragen:

- Was sind die Schutzziele von Datensicherheit und wie lauten die englischen Fachbegriffe hierzu?
- Du hast eine Datei in deinem OneDrive-Ordner gespeichert. Überlege Dir bzw. recherchiere, in wie fern diese Datei gemäß der drei Schutzziele sicher ist.





Arbeitsblatt 2:

Praktische Übung: Gruppenpuzzle

Stammgruppen:

Gruppeneinteilung erfolgt mit einer individuellen App aus Learningapp.com die hier aus Datenschutzgründen nicht dargestellt wird, da Sie Schülernamen enthält. (Ähnlich: <https://learningapps.org/75643>)

Aufgaben:

- Jede der fünf Stammgruppe entsendet ein oder zwei Gruppenmitglieder zur Expertenrunde (5 Minuten)
- Folgende Expertenrunden gibt es:
 - Signieren von E-Mails
 - Verschlüsseln von Laufwerken und Dateien
 - Sicher im Netz surfen
 - IT-Sicherheit am Arbeitsplatz / Umgang mit Passwörtern
- Die Expertengruppen haben 45 Minuten Zeit Ihre Aufgabe zu erledigen und Experte für Ihr Gebiet zu werden.
 - Kommen sie spätestens 5 Minuten vor Unterrichtsende wieder ins Klassenzimmer zurück.
 - Inhalte, die nicht geklärt werden konnten sind zu Hause nachzuarbeiten.
- In der nächsten Stunde gehen die Experten anschließend in ihre Stammgruppe zurück und erklären und zeigen Ihren Gruppenmitgliedern, was Sie in der Expertenrunde erarbeitet haben

Arbeitsblatt 3a:

Signieren von E-Mails

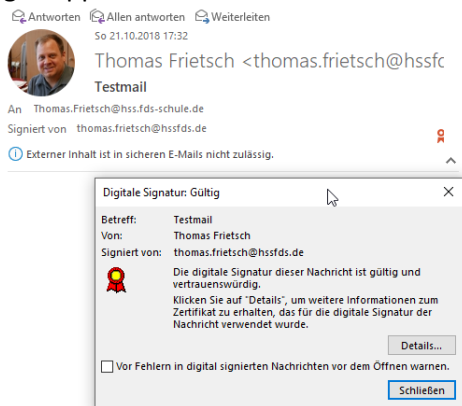
Ziel deiner Gruppe ist es, nur noch digital unterschriebene E-Mails zu versenden. Dazu ist es notwendig, euch von einer Zertifizierungsstelle eure "Unterschrift" bestätigen zu lassen. Wie das alles geht ist in einer Anleitung beschreiben. Jedoch der Reihe nach...

- Aufgabe vorab:
Richte den lokalen Outlook-Client auf Deinem Tablet ein. Eine Anleitung findest Du hier: <https://www.youtube.com/watch?v=lmRna2C3tsk>
- Versucht zunächst gemeinsam an einem eurer Tablets die Signierung einzurichten. Eine Schritt-für-Schritt-Anleitung gibt's hier (Relevant sind die Seiten 1-9): https://lehrerfortbildung-bw.de/st_recht/daten/2014/smime-vortragmaterial-grupp/Uebung-03c-Outlook-mit-SMIME-Verschlueselung_v140922.pdf





- Versendet hinterher als Test eine signierte Nachricht an ein Gruppenmitglied. Wenn alles geklappt hat müsste eine Mail ankommen, die so wie unten abgebildet aussieht.



- War die Einrichtung erfolgreich so führt diese an allen euren Tablets durch und beantwortet die Fragen.

Fragen:

- Welches der drei Schutzziele wird mit der digitalen Signatur erreicht?
- Ist die Nachricht verschlüsselt?
- Wie lange ist das Zertifikat gültig?

Legt zum Abschluss jeweils ein Backup eures Zertifikats im persönlichen OneDrive ab, falls euer Tablet neu aufgesetzt werden muss (s. letzte Seite der Anleitung)

Arbeitsblatt 3b:

Verschlüsseln von Dateien und Datenträgern

Eure Gruppe untersucht drei Methoden zur Verschlüsselung von Dateien:

- Gesamtes Laufwerk verschlüsseln mittels Bitlocker
- Einen Bereich verschlüsseln mittels VeraCrypt (Container)
- Eine einzelne Datei verschlüsseln

1. Eure Gruppe hat einen USB-Stick. Dieser soll mittels Bitlocker verschlüsselt werden. Notiert in Stichworten und Screenshots wie dabei vorgegangen werden muss. Probiert den verschlüsselten Stick an einem anderen Tablet aus. Funktioniert die Verschlüsselung bzw. Entschlüsselung.

Fragen dazu:

- Welchen Verschlüsselungsalgorithmus verwendet Bitlocker? Wie sicher ist dieser?
- Wäre eine Datei auf dem USB-Stick noch verschlüsselt, wenn ich diese per Mail versenden würde?

2. Schaut Euch als nächstes das folgende Video an:

<https://www.youtube.com/watch?v=6UfiuKb9-3o>

Ladet also VeraCrypt aus dem Internet herunter und erstellt einen Container von 5 MB.

Fragen dazu:

- Welchen Vorteil hat dieser Container im Vergleich zu der Laufwerksverschlüsselung mittels Bitlocker?
- Was passiert, wenn der Container voll ist?





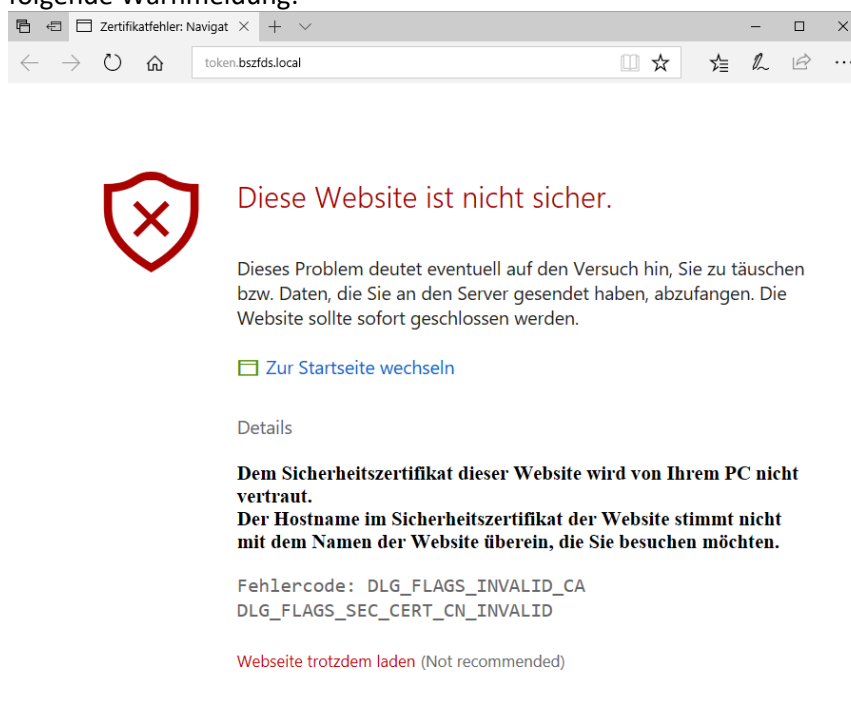
3. Die letzte Möglichkeit, wenn man nur eine Office-Datei versenden will, ist in jedem MS Office-Programm eingebaut. Erstelle eine Word-Datei und verschlüsselt diese. Wie muss man vorgehen? Dokumentiert dies mit Hilfe von Stichworten.

Arbeitsblatt 3c:

Safer Surfen

Beantworte folgende Fragen:

- Woran erkennt man ob eine Website verschlüsselt übertragen wird?
- Was ist ein Zertifikat und wer stellt dies aus? Schau dir das folgende Video an: <https://www.youtube.com/watch?v=ANqhinZkkZ8>
- Im lokalen Intranet der Schule steht ein Webserver. Auf den Webseiten dieses Server werden vertrauliche Informationen gespeichert. Beim Start der Website kommt immer die folgende Warnmeldung:



Sind die Informationen trotzdem sicher? Begründe deine Antwort.

Aufgabe:

Webseiten werden asymmetrisch verschlüsselt. In dem folgenden Rätsel geht es prinzipiell genau darum. <http://www.spiegel.de/wissenschaft/mensch/raetsel-der-woche-was-tun-gegen-diebe-beim-paketdienst-a-1027722.html>

Überlegt euch in der Expertenrunde eine Lösung bevor ihr die Lösung auf der Website anschaut. Im Internet passiert dies wie unter der Lösung in Kommentar Nr. 4 dargestellt.

Das Verfahren ist auch nochmals hier erklärt (ab 3:48): <https://youtu.be/OP5kpVlKoRk?t=227>

Stelle den Vorgang der Ver- und Entschlüsselung und der Schlüsselpaare grafisch dar.





Arbeitsblatt 3d:

IT-Sicherheit am Arbeitsplatz und Passwörter

Aufgabe:

Auf der folgenden Website sind drei Lernspiele hinterlegt:

<https://www.sichere-identitaet-bb.de/sicheriminternet>

Spiele alle drei Episoden durch und beantworte die folgenden Fragen?

- Was macht ein gutes Passwort aus?
- Wo sollten Passwörter aufbewahrt werden?

Übungen:

- Schau die folgende Seite an: <https://www.sicher-im-netz.de/dsin-passwortkarte>
Wie funktioniert die Passwortkarte? Was hältst Du persönlich davon?
- Lade Dir das Programm KeePass 2 herunter und installiere es:
<https://sourceforge.net/projects/keepass/files/KeePass%202.x/2.40/KeePass-2.40-Setup.exe/download>
 - Schau dir die beiden Videos an und teste KeePass 2 selbst an einer Website aus (z. B. bei deinem privaten Mail-Account).
 - <https://youtu.be/A8U78sEXpNc>
 - <https://youtu.be/VqK0PMmifLQ>
 - Diskutiert in der Gruppe die Vor- und Nachteile dieser Software
 - Was wäre ein sinnvoller Ort für die Passwortdatenbank, wenn du mehrere PCs / Smartphones / Tablets hast?

Fragen:

- Was versteht man unter Phishing?
- Nenne Merkmale, woran man eine Phishing-Mail erkennt
- Welche weiteren Regeln sollten Unternehmen bezüglich ihrer IT-Sicherheit aufstellen?

Arbeitsauftrag zur Wissenssicherung:

Block 2 wurde in einer Vertretungsstunde durchgeführt ohne Anwesenheit des Fachlehrers: Durch die Kommunikationsplattform „Teams“ wurde der Auftrag übermittelt.

Suchen oder Befehl eingeben

EAT_21_LBT_Fh > Allgemein ...

Unterhaltungen Dateien Kursnotizbuch Aufgaben +

← Antworten

25. Oktober 2018

Thomas Frietsch 25.10.18 20:11

Hallo zusammen,
Ich habe mit Herrn [redacted] abgemacht, dass ihr die Gruppenarbeit in den Stammgruppen (1-5) in der 3./4. h fertig machen könnt. Ich möchte als „Beweis“ von jedem von euch eine Signierte E-Mail mit einem verschlüsselten Veracrypt-Container (1MB). In den Container soll eine Textdatei liegen mit eurem Namen. Das Passwort zum Verschlüsseln soll E1ATsinddiebesten lauten.
Grüße

Weniger anzeigen

← Antworten

