Stoffverteilungsplan

Schulform	Gymnasium
Klassenstufe	11/12
Lernbereich Nr.	3
Lernbereich Name	Sicherheit von Informationen
Autor	Alexander Luther; Dominic Dietze, Marvin Dropp
Bemerkungen	

Abkürzungen:

Anf.	Anforderungen
Asym.Vsvf.	Asymmetrisches Verschlüsselungsverfahren
Bsp.	Beispiel(e)
CCC	ChaosComputerClub
Def.	Definition
entschl.	Entschlüsseln
FP	Fingerabdruck (engl. Fingerprint)
Komplx.	Komplexität
Id.	Identität
ISS	Informationssicherheitssystem
IÜ	Informationsübertragung
LB	Lernbereich
LK	Lehrkraft
Öff.SL	öffentlicher Schlüssel
Priv.SL	privater Schlüssel
SL	Schlüssel
SP	Smartphone
SvI	Sicherheit von Informationen
SuS	Schüler und Schülerinnen
Sym.Vsvf.	symmetrisches Verschlüsselungsverfahren
SZ	Schutzziel(e)
TN	Teilnehmer*innen
Ustd.	Unterrichtsstunde
verschl.	Verschlüsseln
ZS	Zeichensatz
Vsvf.	Verschlüsselungsverfahren
Wdh.	Wiederholung

St.	Stundenthema	Lernziele	Inhalt	Fachbegriffe	Materialien/Ideen
1	Einführung in die SvI	SuS begreifen die Relevanz der SvI im Alltag, indem sie Anhand von Bsp. neg. Auswirkungen fehlender SvI finden	• Finden von notwendigen Alltagssituationen mit Notwendigkeit für SvI (Hohe kreativität der SuS triggern, um Begriffsklärung nachhaltig zu setzen) • Begriffsklärung: Sicherheit (von Informationen)	Datenschutz, Datensicherung, IT-Sicherheit Bekannt: Netzwerke und Dienste (LB 10.3), Kommunikation in Netzen (LB 12.1)	• Einleitung: Rollenspiel der LK als Hacker (Hoodie) + https://hackertyper.net/ ◦ ggf. SP eines SuS entsperren lassen und Bildschirm.SL merken + anschl. eigenhändiges Entsperren ◦ Vllt. auf die Hacker-Ethik des CCC verweisen *(könnte cool wirken)* https://www.ccc.de/de/hackerethik (White- / Gray- / Blackhat Hacksen) • Begriffsnetz von SvI erarbeiten (Brainstorm), um Def. zu bilden (Ideal: Fächerverbind. GRW / Ethik) (Ggf. kollabotarives Online-Tool zum Zusammentragen der Ideen) ◦ Verlust von Priv.Daten (GRW: DSGVO) Bsp. Strafzahlungen Datenverlust ◦ Abhörigen von Information (globalisierte Kommunikation) (Ethik) ▪ Bsp. „Zoom-roullett“ während der Corona-Zeit ◦ Nachweisbarkeit von Verträgen (GRW) ◦ Zugangsberechtigungen (GRW) ◦ **Ideen für nächste Ustd. festhalten** • Begriffsklärung: Gültige und Verständliche Def. Sicherheit (von Informationen) muss noch ausgearbeitet werden.

St.	Stundenthema	Lernziele	Inhalt	Fachbegriffe	Materialien/Ideen
2	Schutzziele (auch als Doppelstunde mit 1 Ustd. umsetzbar)	Kennen von allen 4 Anf. an die SvI, indem Alltagssituationen zugeordnet wreden können und SZ gennant werden können	• Vorstellung der SZ (siehe Begriffe) • Einordnen der Alltagssituationen (vorherige Ustd.) zu den verletzten SZ	Schutzziele: Vertraulichkeit, Integrität, Authentizität, Verbindlichkeit	• Arbeitsblätter zu Schutzzielen zur Verfügung stellen (muss noch erstellt werden) und mittels Stamm-Expert*innen-Gruppen erarbeiten und in den Gruppen vorstellen lassen • Zuordnen der Alltagssituationen zu den jeweilgien SZ ◦ evtl. noch weitere neue kreative Situationen finden
3	Einführung in die Kryptographie	SuS verstehen die Notwendigkeit von VS kennen Missbrauchszenarien indem sie Bsp. nennen	• Wiederholung SZ • Wofür benötigen wir SvI? (mgl. Angriffe) • einfache Verschl. machen • Bedeutung SL.länge	Trojaner, Brute-Force-Methode, Caesar-Vsvf. Vigenère-Vsvf., SL	• Aktuell bekannt gewordene Sicherheitslücken besprechen, Auswirkungen diskutieren (verletzte SZ, Angriffsmotive …) • Selbst ausgedachte Nachrichten verschl.
4	Kryptographie	SuS sind in der Lage einfache Vsvf. selbst anzuwenden und können mit Hilfe des SL. Nachrichten entschl.	• Klartext – Chiffre – SL. Identifizieren • nichtkryptographische Verfahren • Wandel der Vsvf. im Laufe der Zeit		• Die SuS versuchen lassen gegenseitig ihre verschl. Nachrichten ohne SL zu entschl. • Brainstorm zu nichtkryptographischen Vsvf.

St.	Stundenthema	Lernziele	Inhalt	Fachbegriffe	Materialien/Ideen
5/6	Verfahren zur Gewährleistung der Vertraulichkeit	SuS kennen den Unterschied zw. Öff.- u. Priv.SL, können Sym.- u. Asym.Vsvf. Voneinander abgrenzen.	• Vsvf. mit geheimen SL.: DES, AES • RSA • Komplx. der Vsvf vgl. u. deren Sicherheit abschätzen • Sensibilität v. Daten (Was sollte wie gut geschützt werden?)	Öff.SL, Priv.SL, Sym.verschl. Asym.verschl	• Ablauf der IÜ bei den verschiedenen Vsvf. graphisch darstellen • Vorstellung von Vsvf. in den TN unterschiedliche SL benutzen (bsp. Facebook) • Online-Tool zur Verschl. Verschiedener Nachrichten mit verschiedenen Vsvf. verwenden
7/8	Kryptoanalyse	SuS kennen unterschiedliche Angreiferrollen (Eve, Mallory etc.) und können ihnen bedrohte SZ zuordnen. SuS können zu jeder Rolle eine mögliche Angriffsmethode wiedergeben	• Wie unterscheiden sich TN (gewünscht oder unerwünscht) eines ISS im Bezug auf ihre Rechte / Möglichkeiten • Wann gewinnt eine Angreiferin • Ressourcen: Verschl.-Entschl. - Perfekte Sicherheit?	Kerkhoffs‘ Prinzip, Timing Attach, Brute-Force, One-Time-Pad	• Alice-Bob-Szenario, Bsp. Timing-Attack (WLAN) • Bruteforce: Rechenbsp. bei Änderung der Wortlänge o. Erweiterung des ZS • Diskussion Anwendbarkeit von OTP‘s • Server-Angreifer-Rollenspiel: Chosen-Plaintext verarbeiten lassen → Angreifer soll SL erraten

St.	Stundenthema	Lernziele	Inhalt	Fachbegriffe	Materialien/Ideen
9/10	Datensicherheit	SuS können existierende Sicherheitsvorkehrungen in ihren Alltag integrieren, indem Sie konkerte Implementierungen (E-Mailverschl., FP-Abgleich) anwenden	• SuS sollen in der Doppelstunde konkrete Anwendungen zur Verbesserung der Sicherheit ihrer Informationen ausprobieren	E-Mailverschlüsselung (PGP), SL-FP, Festplattenverschlüssel, Passwortmanager	• Einführung bzgl. Verlust von Daten, mittels Passwort-Leak-DBs (https://haveibeenpwned.com/, https://sec.hpi.de) → Alltagsrelevants wieder hervorrufen • Anwendung v. Sicherheitsvorkehrungen (vorherige kurze Umfrage, was SuS für Kommunikationsmittel nutzen) ◦ Tools zusammentragen: ▪ E-Mailverschl.Enigmail@Thundbird, Whatsapp, Signal: FP – Abgleich, TrueCrypt: Geräteverschl., Passwortmanager: KeePass ◦ Aufkurzanleitungen (müssen noch zusammen getragen werden)
11	Übung / Puffer + Klausurvorbereitung	SuS können die im LB erarbeiteten Vsvf. anwenden, die Bedeutung von Fachwörtern kann mit eigenen Worten wiedergegeben werden	• SZ wiedergeben, wodurch könnte konkretes SZ gefährdet weredn • Klartext-SL-Vsvf. Identifizieren • Anwendungsbereiche von Vsvf. • Mgl. Entschl.methoden • Unterschied: Sym.-Asym.Vsvf. • Durchführung von Vsvf.	Wdh.	• Fragerunde zur Klausur vorbereiten • Diskussion: Wie kann man vertrauliche Informationen am besten Schützen? • Wo liegt die Grenzen von Svl.?
12	KLAUSUR				