Unterrichtsplanung – Sensibilisierung

# Lernziele:

* Die Teilnehmenden wissen, wie Hacker schwache Passwörter bei Benutzerkonten für Online Dienste ausnutzen können
* Die Teilnehmenden kennen die Satzmethode um starke Passwörter zu erstellen, die man sich einfach merken kann.
* Die Teilnehmenden wissen, wie einfach Hacker sich bei E-Mail und SMS als jemanden anderen auszugeben können.
* Die Teilnehmenden kennen zwei griffige Massnahmen um solche Meldungen zu entlarven.

# Neue Konzepte

* Brute Force Angriff
* Passwort Hashes und Angriffe auf dieses
* E-Mail und SMS Spoofing

# Anforderungen an die Teilnehmenden:

* Keine

# Voraussetzungen für die Durchführung:

* Keine

# Unterrichtsvorbereitung

Benötigtes Material:

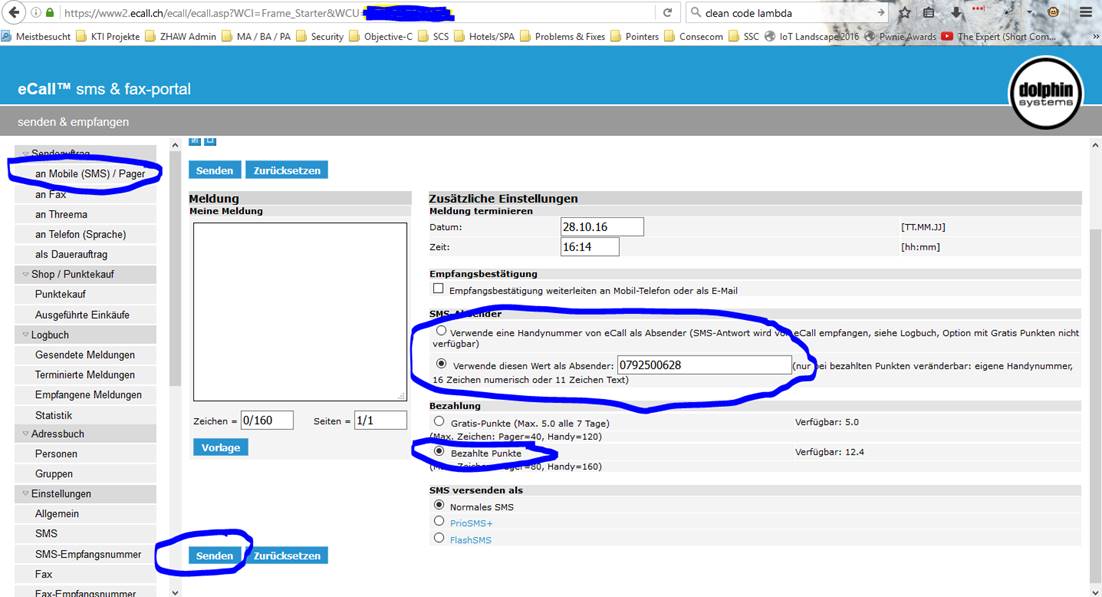
* 4 oder mehr Zettel oder Grosse Post-It pro Teilnehmenden
* Laptop mit Foliensatz und Internetzugang

Inhaltliche Vorbereitung:

Studium der Detailplanung zusammen mit den Folien und den darin enthaltenen Notizen. Insbesondere sollte die Perspektive (Hacker resp. erzählen über Hacker als Fachperson) gewählt und die Art und Weise der Einbettung in den eigenen Unterricht festgelegt werden. Die Detailplanung und die Notizen zeigen eine mögliche Storyline auf. Die Notizen enthalten jeweils einen Vorschlag, wie der Übergang zur nächsten Folie gemacht werden kann.

Vorbereitung für die Durchführung der live Demos:

* Verbindung ins Internet
* Für live Hashing und Hash-Cracking Demo folgende Webseiten im Browser öffnen:
  + <https://crackstation.net/>
  + <http://passwordsgenerator.net/sha1-hash-generator/>
* Für die **Phishing Demo** die Webseite für das Erstellen von Phishing E-Mails öffnen und gegebenenfalls mit dem zum durchzuspielenden Szenario passenden Inhalt befüllen. Tipp: Formularinhalte können auch mittels Tools wie LastPass gespeichert und per Click eingefüllt werden. Für die Demo sollte wenn möglich ein eigenes „Szenario“ entwickelt und durchgespielt werden. Ein Beispielszenario und der dazugehörende Ablauf ist auf den per Default ausgeblendeten Folien 27 bis 36 zu finden.
  + <https://emkei.cz/>
* Für die **SMS Spoofing Demo** wird ein Zugang zu einem Dienst zum Versenden von SMS mit gespooftem Absender benötigt. Eine Möglichkeit ist die Verwendung des Dienstes eCall.ch. Zum Senden einer SMS mit gefälschtem Absender sind dort Bezahlte Punkte nötig. Mit den verfügbaren Gratis Punkten funktioniert dies nicht. Die Seite für das Absetzen des SMS sollte bereits im Browser geöffnet vorliegen und der SMS Versand vorgängig mindestens einmal getestet werden.   
    
  Für eCall sind die relevanten Felder für das Erstellen einer solchen SMS im untenstehenden Screenshot markiert. Die Eingabe eines passenden SMS Texts erfolgt live.
  + <https://www.ecall.ch/sms/ecall-sms-fax.asp>



* Für die **MS Word Malware Demo** kann das mitgelieferte Dokument im Ordner *ms-word-demo* verwendet werden. Das Dokument sollte auf den Präsentationscomputer kopiert werden.

Idealerweise wird das Dokument durch ein für das jeweilige Zielpublikum passendes Dokument ersetzt. Dazu muss das Dokument angepasst und die eingebundene ausführbare Datei durch eine eigene ersetzt werden. Der C# Code für die aktuell eingebundene Datei liegt bei und kann von entsprechend ausgebildeten Lehrpersonen einfach abgeändert und ersetzt werden. Die weiteren Angaben zur Demo sind in den Folien 44/45 zu finden.

## Anleitung für die Demos zum Unterricht

**Demo 1: Brechen von Password Hashes**

1. (Beliebiges) Passwort in einen Hash umwandeln mittels der Webseite:  
   <http://passwordsgenerator.net/sha1-hash-generator/>

Die Webseite erzeugt ungesalzene SHA-1 Hashes. Diese Art des Password Hashings entspricht nicht mehr „Best Practice“. Da es hierzu aber online Cracking Dienste gibt und man das Passwort nicht selber mittels Dictionary Angriff resp. Brute Force Angriff cracken muss, eignet es sich gut zur Demonstration. Alternativ kann man Programme wie John the Ripper verwenden um gesalzene „Best Practice“ PBKDF2 (<https://en.wikipedia.org/wiki/PBKDF2>) Passwort Hashes selber anzugreifen. Dies dauert aber zu lange für eine Demonstration, da diese nicht vorberechnet werden können und deutlich mehr Ressourcen für die Berechnung brauchen.

1. Den Password Hash auf der Webseite:  
   <https://crackstation.net/>

einfügen, das CAPTCHA lösen und auf „Crack Hashes“ klicken.

Wichtig: Wenn die CrackStation ein Passwort nicht knacken kann, ist dies nicht notwendigerweise ein starkes Passwort.

**Demo 2: Phishing Demo**

Gemäss den Angaben auf den Folien/Notizen.

**Demo 3: Malware Demo**

Gemäss den Angaben auf den Folien/Notizen.

# Unterrichtsablauf

Die Unterrichtsform ist Frontalunterricht gemischt mit interaktiven Elementen. Die Detailplanung enthält Informationen zum Ablauf sowie ergänzende Informationen zu den Folien und den darin enthaltenen Notizen.

## Detailplanung

Pausen sind nach eigenem Ermessen einzubauen. Die Zeitangaben sind Richtzeiten und können je nach Erzählweise und abgegebenen Erklärungen und Ergänzungen leicht bis stark abweichen.

| Zeit | Inhalt | Diverses |
| --- | --- | --- |
| 00:00 | **Einführung – Sensibilisierung aus Sicht eines Hackers**  Je nach Hintergrund und Plausibilität eine von zwei Rollen wählen  Option 1 – Der Hacker resp. der „Techi“. Das Vorgehen und die Überlegungen der Hacker werden aus der Ich-Perspektive erzählt.  Option 2 – Informierte Fachperson die Bescheid weiss über das Vorgehen und die Überlegungen der Hacker.  Ev. kurz den persönlichen Hintergrund für das einschlägige Wissen einführen. Beim „Hacker“ den Hackernamen (z.B. *morpheuZ)* und bisherige Aktivitäten wie z.B. die Teilnehme an Hacker Wettbewerben (CTF: Capture The Flag) oder das Durchführen von Penetration Tests. | ev. Slide zum eigenen Hintergrund einfügen |
| 00:05 | **Aktivitäten + Bedrohungen im Cyber Space (Folien 2-3)**  Als Hacker ist es wichtig die Aktivitäten der potentiellen Opfer sowie die für die jeweilige Aktivität relevanten menschlichen und technischen Schwächen zu kennen. Die beiden Fragen in den Folien zielen auf diesbezügliche Informationen ab (=> Slide 2, dann 3).  Zuerst werden Aktivitäten gesammelt damit sich die Teilnehmenden Gedanken machen, was sie im Cyber Space alles nutzen. Dadurch sollte es dann etwas einfacher fallen, die Brücke zu den Gefahren zu machen.   * Teilnehmende mindestens zwei Aktivitäten und dann Gefahren auf Zettel schreiben lassen. * Teilnehmende Ihre Zettel mittels Magneten/Reiszwecken an Tafel/Pinnwand Befestigen lassen.   **Auswertung der Rückmeldungen:**  Die am häufigsten genannten Aktivitäten und Gefahren notieren und kurz zusammenfassen.  **Überleitung:**  Ein erster Schritt um sich besser vor Hacker schützen zu können, ist sich der Gefahren und geeigneter Schutzmassnahmen resp. Vorsichtsmassnahmen bewusst zu werden. Eine erste Massnahme wäre es, Hackern wie mir so wenige Informationen zu geben wie möglich… ☺  Wir werden nun folgende Gefahren und Schutzmassnahmen/Vorsichtsmassnahmen genauer beleuchten:   * Angriffe auf Benutzerkonten (DropBox, Email, WhatsApp,…) * Einschleusen von Malware   Bei grosser Abweichung der Aktivitäten und wahrgenommenen Gefahren von den obigen Themen den Fokus auf diese beiden Themen setzen und den Fokus mittels der Relevanz dieser beiden Themen für einen sicheren Schulbetrieb begründen. | Beamer  Wandtafel oder Pinnwand |
| 00:20 | **Benutzerkonten – Angriffsfläche (Attack Surface) (Folie 5 -6):**  Bevor ein Hacker mit dem Angriff auf ein Opfer startet, analysier er die Angriffsfläche seines Opfers. Da wir uns bereits auf einen Angriff auf Benutzerkonten fixiert haben, erfassen wir kurz hierfür relevante Informationen.  Durch Handheben bei der jeweiligen Option (0, <5. <10, <20, 20+) die Anzahl Benutzerkonten pro Teilnehmenden erfassen.  Durch Fragen ins Publikum (gezielt aufrufen bei keiner Meldung) eine Sammlung von verwendeten Diensten (Schulkonto, Apple Konto, DropBox, WhatsApp, Gmail, GameStop, Playstation, XBOX, …) erstellen.  Dies stellt die Angriffsfläche dar und sollte üblicherweise ganz passabel rauskommen. Alle haben meistens mind. ein paar Benutzerkonten und WhatsApp, DropBox, Microsoft, das Schulkonto und Google oder Apple sind meistens mind. dabei.  Dem Hacker bieten sich also viele Optionen für einen Angriff und es sieht nicht so aus, dass es in Zukunft weniger Konten pro Person geben wird. Aktuelle Zahlen in Studien listen 10 bis 100 Konten/Passwörter pro Person auf!!  **Überleitung:**  Als nächstes gilt es nun das Wissen über die Angriffsfläche auszunutzen und das Opfer effektiv anzugreifen. Dazu gibt es verschiedene Angriffsvektoren. | Beamer |
| 00:25 | **Angriffsvektoren (Folie 6):**  Kurze Einführung in die Grundsätzlichen Angriffspunkte gemäss dem Slide sowie den dort vorhandenen Notizen..  Bemerkung: Ein Hacker der grosses vorhat, würde zuerst die Infrastruktur, resp. den Provider auf mögliche Angriffspunkte absuchen. Da hier nicht die Teilnehmenden das Angriffsziel sind, können diese kaum was tun um solche Angriffe zu verhindern, richtig? Falsch. Zumindest können sie mit ein paar Massnahmen sicherstellen, dass der Angriff nur beschränkte Auswirkungen auf sie hat. Dies wird dann beim Thema starke Passwörter aufgegriffen. | Beamer |
| 00:30 | **Server-seitige Angriffe (Folien 7-11)**  Ganz grundsätzlich gibt es die Möglichkeit sich mit oder ohne Umgehung resp. Aushebeln der Sicherheitsmechanismen (=> Brute Force) sich in das System zu hacken. Diese Seite mit Umgehung resp. Aushebeln der Sicherheitsmechanismen wird nur kurz angesprochen da hier der Benutzende wenig Einfluss auf die Sicherheit hat.  Präsentation des Inhalts gemäss den Folien und den Notizen inkl. der zweiteiligen Demo 1.. | Beamer  Demo 1 |
| 00:40 | **Überleitung zum Thema starke Passwörter (Folie 13)**  Die Überleitung zum Thema erfolgt anhand einer Behauptung und einer Diskussion. Die Teilnehmenden sollen erklären, wieso starke Passwörter sowohl Brute Force Angriffe wie auch die Verwendung gestohlener Passwortdaten zumindest erschweren.  **Ziel:** Die Teilnehmenden realisieren dass beide Angriffe auf das Ausprobieren „wahrscheinlicher“ Passwörter hinauslaufen. Sind die Passwörter nicht in solchen Listen drin resp. genügend lang und „komplex“, dürfte das die Erfolgswahrscheinlichkeit gegen Null gehen lassen.  Ablauf der Diskussion:   * Die Teilnehmenden untereinander (in Zweiergruppen) ca. 3 Minuten diskutieren lassen. * Anschliessend Antworten aus dem Publikum sammeln und wo angebracht/nötig im Hinblick auf das Ziel kommentiert. | Beamer |
| 00:45 | **Starke Passwörter (Folien 14- 17)**  Präsentation des Inhalts gemäss den Folien und den Notizen. Anschliessend sollten die Teilnehmenden wissen was ein starkes Passwort ist und wie man es sich merkt.  Optional zum Abschluss von diesem Teil:   * Die Teilnehmenden Passwörter ausdenken lassen und diese dann zuerst zu hashen und dann zu knacken versuchen gemäss Demo 1. Nicht geknackt heisst nicht, dass dies ein starkes Passwort ist => zusätzliche Beurteilung durch den Unterrichtenden. Umgekehrt wird aber ein Schuh draus. ☺ * ACHTUNG: Die Teilnehmenden sollten natürlich NICHT ihre Passwörter preisgeben und diese testen….   **Überleitung:**  **Neben dem Verwenden von starken Passwörtern ist der richtige Umgang mit Passwörtern genauso wichtig.** | Beamer |
| 00:55 | **Umgang mit Passwörter [Folien 18 – 21]**  Präsentation des Inhalts gemäss der Folien und den Notizen.  **Überleitung:**  **Wenn Angriffe auf der Server Seite nicht erfolgreich sind, geht ein Hacker halt direkt auf die Benutzer los. Oder er macht das schon von Anfang an, weil ihm Angriffe auf gut geschützte Server zu mühsam oder auffällig sind. Wir werden als nächstes also Angriffe auf die Benutzenden selber anschauen.** | Beamer |
| 01:00 | **E-Mail Phishing [Folien 22 - 37]**  Einführung in die Thematik Phishing resp. E-Mail Phishing inkl. einer Phishing Demo.  Präsentation des Inhalts gemäss der Folien und den Notizen. | Beamer |
| 01:15 | **Phishing / Social Engineering im Allgemeinen [Folien 38, 39]**  Präsentation des Inhalts gemäss der Folien und den Notizen. |  |
| 01:20 | **Phishing Demo mittels SMS Spoofing**  Diese Demo kann hier optional eingebaut werden um eine weitere Möglichkeit aufzuzeigen, wie das „blinde“ Vertrauen von Personen in die Technik resp. in die Geräte missbraucht werden kann.  Ziel: Die Zielperson erhält eine SMS von einer Ihr vertrauenswürdigen |  |
| 01:28 | **Abschluss Phishing / Social Engineering [Folien 41, 42]**  Präsentation des Inhalts gemäss der Folien und den Notizen.  **Überleitung (falls noch Zeit!):**  Neben Phishing oder als Teil eines Phishing Angriffs wird oft ein Angriff mittels Malware verwendet. So kann z.B. ein Angreifer mit Hilfe der auf einem Rechner des Opfers platzierten Stück bösartiger Software (=Malware) ebenfalls deren Benutzerkontodaten aufzeichnen und abziehen (dem Angreifer zusenden). Nachfolgend zeigen wir ein Beispiel, wie man mit geschickter Manipulation des Benutzers diesen dazu bringen kann ein Stück Malware auf seinem Computer auszuführen. |  |
| 01:30  (5-8 Minuten) | **Malware Demo [Folien 44,45]**  Demo mit einem speziell präparierten MS Word Dokument.  Präsentation des Inhalts gemäss der Folien und den Notizen. |  |