

# IT-Sicherheit im Wintersemester 2024/2025

## Übungsblatt 0

**Besprechung:** Do, 24.10.2024 um 14:00 Uhr

**Achtung:** Zur Bearbeitung einiger Übungsaufgaben ist es notwendig sich über den Vorlesungsinhalt hinaus, durch Internet- und Literaturrecherche mit dem Thema zu beschäftigen.

### Aufgabe 1: (T) Zutrittskontrolle

Die *Zutrittskontrolle* ist ein Security-Verfahren, das in der alltäglichen Welt häufig eingesetzt, jedoch selten im Detail analysiert wird.

- a. Nennen Sie verschiedene Formen und Einsatzorte der Zutrittskontrolle.  
Worin unterscheiden sich z.B.
  - “die Tür” an einem Club
  - der Einlass beim LMU Erstifest “Unser erstes Mal”
  - die Ausweiskontrolle vor der IT-Sec-Klausur und
  - das Betreten der eigenen Wohnung?
- b. Welche (Teil-)Ziele verfolgt die Zutrittskontrolle?
- c. Aus welchen Verfahrensschritten besteht sie also? Beschreiben Sie.
- d. Welche “Fehler” könnten hierbei geschehen? Wie könnte ein potentieller Angreifer die Zutrittskontrolle (ggf. mit Hilfsmitteln) unterwandern?
- e. Mit welchen technischen, baulichen oder organisatorischen Hilfsmitteln lässt sich eine Zutrittskontrolle unterstützen/verstärken?
- f. Diskutieren Sie:
  - Welche Rolle könnte ein “vertrauenswürdiger Dritter” spielen?
  - Was ist von einem Mitgliedsausweis des Sportclubs zu halten?

## Aufgabe 2: (T) Passwortqualität im Jahresverlauf

123456 ist das derzeit weltweit wohl beliebteste Passwort.

Im Internet kursieren lange Listen “beliebter” oder aus vergangenen Leaks bekannter Passworte. Anstatt alle möglichen Buchstabenkombinationen durchzuprobieren (*brute force attack*), ist es für einen Angreifer deutlich effizienter, häufig gewählte Passworte durchzutesten (*dictionary attack*), um einen Login ”zu knacken“.

Solche Listen können sich aber nicht nur Angreifer zu Nutze machen!

Die folgende Abbildung zeigt die Zahl von Studierenden-Accounts einer Ihnen bekannten Universität mit Passworten, die auf solch einer Liste stehen, im Jahresverlauf.

- Was fällt Ihnen dabei auf?
- Wie interpretieren Sie die beiden Täler (samt den ansteigenden Flanken)?
- Was kann ein IT-Dienstleister mit diesen Informationen anfangen?

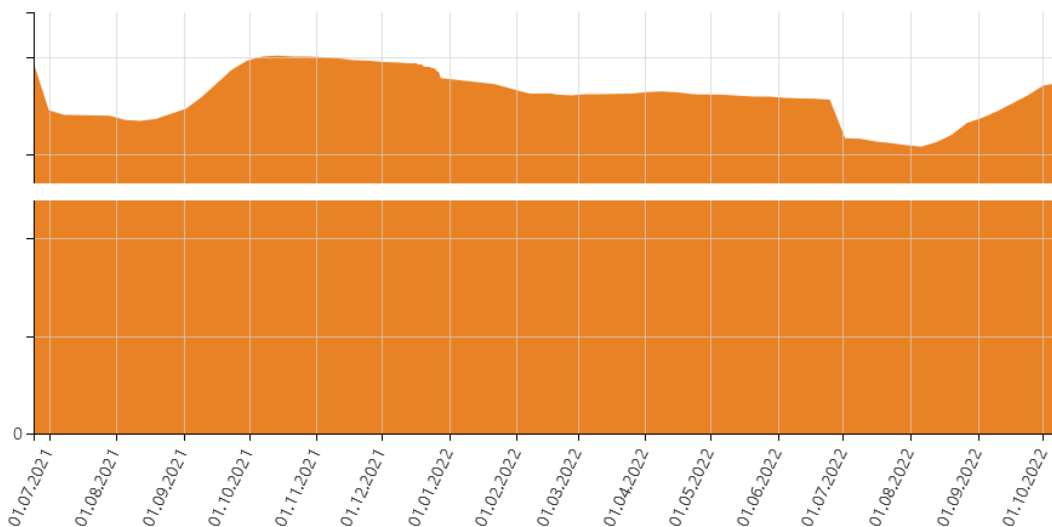


Abbildung 1: Zahl der Accounts mit Passworten aus PW-Listen im Jahresverlauf

### Aufgabe 3: (T) Cyber Security Buzzword Bingo

In Vorträgen und Berichten zur IT-Sicherheit werden häufig viele (leere?) Phrasen verwendet. Beschäftigen Sie sich mit folgenden *Buzzwords* und ordnen Sie diese grob ein!

Am Ende des Semesters werden Sie solche Vorträge fundiert einschätzen können.

Cyber	Threat	Risk	Red & Blue Team	Botnet
Ransomware	Kill Chain	NIST	Logs	Zero Trust
SIEM	C2 / C&C	<b>Buzzword Bingo!</b>	TTP	Recon
Malware	Allow- & Blocklist	Sandbox	Exploit	NGFW
Perimeter	APT	Hacker	Security Awareness	SOC