IT-Sicherheit – Sicherheit vernetzter Systeme

Vorlesung im Wintersemester 2024/2025 (LMU)

24.10.2024
WS 2024/2025

Organisation der Übung I

- Zeitpunkt:
  - Donnerstags, 14:00 – 16:00 Uhr **c.t.**
- Übungsbetrieb:
  - 24.10.2024 – 19.12.2024
  - 09.01.2025 – 30.01.2025
  - vsl. 06.02.2025 Wiederholung/Klausurvorbereitung
- (geplanter) Klausurtermin: TBA

Organisation der Übung II

- **Ca. 12** Übungsblätter mit jeweils 3 – 5 Aufgaben
- Das Übungsleiter-Team:
  - Marcel Buggele, Manfred Buchner, Daniel Weber
  - uebung-itsec@lrz.de (persönliche Fragen)
- Moodle-Kurs: *IT-Sicherheit WiSe 24/25*
  - Übungsblätter, … Forum (Fragen zum Übungsbetrieb)
  - https://moodle.lmu.de/course/view.php?id=35301
  - Einschreibeschlüssel: *password123*

Moodle-Kurs
IT-Sicherheit WiSe 24/25

Hausaufgaben, aber **kein** Notenbonus

- (T): Tutoraufgaben
  - Vorbereitung
  - Lösungsvariante in der Übung
- (H): Hausaufgaben
  - Selbstständig zu Hause
    → Wiederholung/Vertiefung der VL-Inhalte und praktische Anwendung
  - **Keine Korrektur, kein Notenbonus**
  - Meistens keine Musterlösung
  - evtl. Fragen via Moodle-Forum
  - Klausurrelevant -> Bearbeitung sinnvoll und ratsam!
- Kein Notenbonus bei Klausur!

Aufgabe 1: (T) Zutrittskontrolle

Aufgabe 1: (T) Zutrittskontrolle
(a) Worin unterscheiden sich z.B.

- (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" |
    25.10.2024 https://www.unikult.lmu.de/unser-erstes-mal/
  - die Ausweiskontrolle vor der IT-Sec-Klausur und
  - das Betreten der eigenen Wohnung?

  Hints: Überprüfte Attribute?
  Vorzulegender Nachweis?
  Durchsetzung der Kontrolle?

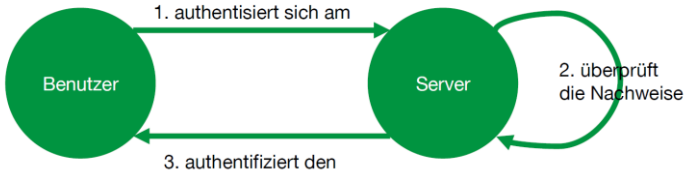
Aufgabe 1: (T) Zutrittskontrolle
(b) Welche (Teil-)Ziele verfolgt die Zutrittskontrolle?

- **Authentizität** (Echtheit von Attributen)
- **Autorisierung**
  - Nur Personen mit einem bestimmten Attribut („berechtigte" Personen) dürfen passieren
  - welche Attribute könnten dies sein?
    - Eintritt bezahlt: Eintrittskarte/Mitgliedsausweis, …
    - Identität: Personalausweis, Ü30-Party: Altersnachweis etc.

Aufgabe 1: (T) Zutrittskontrolle
(c) Aus welchen Verfahrensschritten besteht die ZuKo?

1. **Authentisierung**
   Vorlegen eines Nachweises zur Echtheit eines Attributes
   → welche Arten von Nachweisen gibt es?

2. **Authentifizierung**
   Überprüfen des vorgelegten Nachweises



3. **Autorisierung**
   Überprüfen, ob das (nachweislich echte) Attribut ausreicht, um das angefragte Recht/Zutritt unter den gegebenen Umständen (Uhrzeit etc.) zu erlangen

⚠ Spoiler: Kapitel 10

Aufgabe 1: (T) Zutrittskontrolle
(d) Fehler bzw. Angriffe auf die ZuKo? (I)

- **Authentizität brechen, z.B. durch…**
  - gefälschte Ausweise etc.
  - Ausweise von nicht-vertrauenswürdigen Quellen/Ausstellern
  - Vorgebrachte Nachweise passen nicht zum geforderten Attribut (Perso an der Theaterkasse?)
  - Vorgebrachte Nachweise werden nicht hinreichend geprüft (nur manuell-visuelle Prüfung eines QR-Codes ohne Scanner, z.B. digitale Covid-Impfzertifikate)
  - …

Aufgabe 1: (T) Zutrittskontrolle
(d) Fehler bzw. Angriffe auf die ZuKo? (II)

- **Autorisierung brechen, z.B. durch…**
  - sich selbst in die Liste der Berechtigten eintragen
  - mehr als eine Person passiert gleichzeitig (Drehkreuze)
  - Person darf zwar passieren, nimmt jedoch unerlaubt Material mit (Diebstahl auf dem Rückweg)
  - Person darf zwar prinzipiell passieren, jedoch nur zu bestimmten Zeiten, die nicht eingehalten wurden
  - …

Aufgabe 1: (T) Zutrittskontrolle
(d) Fehler bzw. Angriffe auf die ZuKo? (III)

- **Zutrittskontrolle komplett umgehen, z.B. durch…**
  - außen vorbei vorbeilaufen
  - Tailgating
  - technischen Defekt herbeiführen und hoffen, dass die ZuKo in der Fehlersitutation leichter zu umgehen ist
  - …

Aufgabe 1: (T) Zutrittskontrolle
(d) Fehler bzw. Angriffe auf die ZuKo? (IV)

Wo und wie würden Sie folgende Angriffsarten einordnen:

1. Lockpicking
2. Eine Haustür eintreten
3. Einen digitalen Transponder klonen

Aufgabe 1: (T) Zutrittskontrolle
(e) Hilfsmittel zur Stärkung der ZuKo?

Mit welchen technischen, baulichen oder organisatorischen Hilfsmitteln lässt sich eine Zutrittskontrolle unterstützen/verstärken?

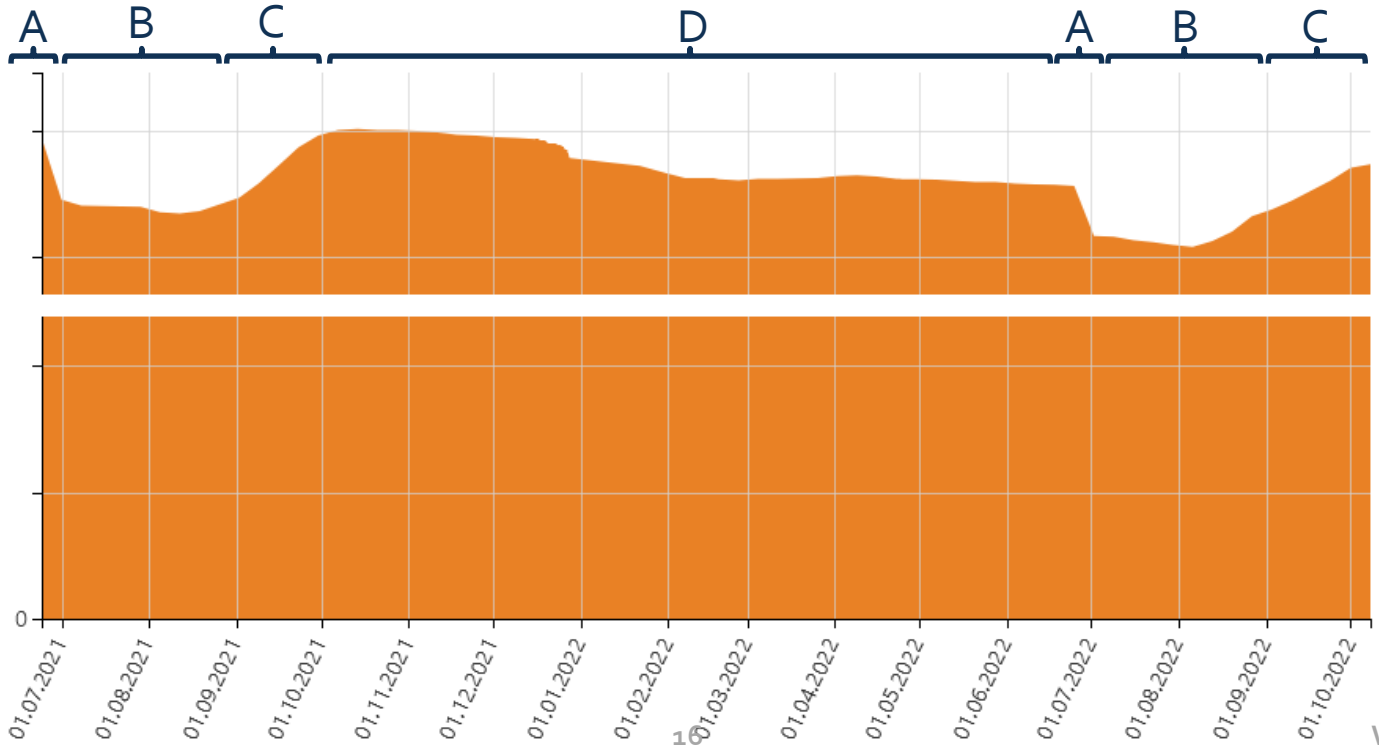
- Personenvereinzelung
- Pforte an prägnanter Stelle / nicht außen herum laufen können
- Mitarbeiterlose Pforten (Türschloss)?
- Verlässlicher Abgleich mit Berechtigungsmatrix / Autorisierungstabelle
- Fälschungs„sichere" Nachweise fordern
- Lesegeräte für Ausweise
- Technische Zutrittskontrollsysteme: Türschlösser mit mechanischen Schlüsseln (Nachteile?) Digitalen Transpondern etc.
- …

Aufgabe 1: (T) Zutrittskontrolle
(f) Diskussion

- Welche Rolle könnte ein „vertrauenswürdiger Dritter“ spielen?
- Was ist von einem Mitgliedsausweis des Sportclubs zu halten?

Aufgabe 2: (T) Passwortqualität im Jahresverlauf

Aufgabe 2: (T) Passwortqualität im Jahresverlauf
a) & b) Interpretation?



Aufgabe 2: (T) Passwortqualität im Jahresverlauf
c) Was kann ein IT-Dienstleister mit diesen Informationen anfangen?

- Sein Sicherheitsrisiko und Exposition fundierter einschätzen
- Betroffene Nutzerkonten zum PW-Wechsel auffordern / sperren
- Vorteil gegenüber statischen PW-Qualitätsvorgaben (8-12 Zeichen, [a-zA-z0-9] etc.)?
  - Ist „`Passwort123`“ ein „gutes“ Passwort?
  - Dynamische Reaktion auf neu auftretende Leaks

BSI-Basisschutz: Sichere Passwörter (I)

Grundsätzlich können Sie zwei Strategien anwenden, um ein sicheres Passwort zu erstellen:

Weitere Informationen:
https://www.bsi.bund.de/dok/6596574

Sicheres Passwort

Kurzes, dafür komplexes Passwort

- Ist acht bis zwölf Zeichen lang.
- Besteht aus vier verschiedenen Zeichenarten.
- Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen werden willkürlich aneinandergereiht.

Langes, dafür weniger komplexes Passwort

- Ist mindestens 25 Zeichen lang.
- Besteht aus zwei Zeichenarten.
- Kann zum Beispiel aus sechs aufeinanderfolgenden Wörtern bestehen, die jeweils durch ein Zeichen voneinander getrennt sind.

BSI-Basisschutz: Sichere Passwörter (II)

Um ihre Accounts und Daten zu schützen, sollten Sie außerdem folgende Tipps beherzigen:

Generell gilt

- ✓ Ein individuelles Passwort pro Account!
- ✓ Eine Mehr-Faktor-Authentisierung (ergänzend zum Passwort durch bspw. eine Gesichtserkennung, eine App-Bestätigung, E-Mail oder einer PIN auf einem anderen Gerät) ist empfehlenswert.
- ✓ Alle verfügbaren Zeichen nutzen inklusive Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen (Leerzeichen, ?!%+...).
- ✓ Das vollständige Passwort sollte nicht im Wörterbuch vorkommen.

Zu vermeiden

- ✗ Namen von Familienmitgliedern, Haustieren, Geburtsdaten etc.
- ✗ Einfache oder bekannte Wiederholungs- bzw. Tastaturmuster wie „asdfgh“ oder „1234abcd“
- ✗ Ziffern oder Sonderzeichen an den Anfang oder ans Ende eines ansonsten einfachen Passwortes.
- ✗ Dasselbe Passwort bei mehr als einem Account.

Aufgabe 3: (T) Buzzword Bingo!

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