# Lern- und Arbeitsauftrag *LA\_183\_04\_Grundbegriffe.docx*

Ein Bild, das Text, Schrift, Zahl, Typografie enthält.

Automatisch generierte Beschreibung

Bild von paulracko auf Pixabay

|  |  |
| --- | --- |
| Titel | Grundbegriffe |
| Modul | 183 Informatiker/in EFZ |
| Autor / Version | Michael Schneider / V1.0  Birgit Rieder / V2.0 |
| Hilfsmittel: | PR\_183\_Grundbegriffe.pptx |
| Nachweis |  |
| Sozialform | Einzelarbeit / Partnerarbeit |
| Leistungsziele | 1.1, 1.2 |

## 

### Aufgabe 1: Schutzziele

Beurteilen Sie bei den folgenden Szenarien, wie hoch die Schutzziele betroffen sind: 0 bedeutet «gar nicht», 1 bedeutet «teilweise» und 2 bedeutet «erheblich».

1. Durch eine DDOS[[1]](#footnote-1)-Attacke wird die Applikation mit Anfragen überflutet und lahmgelegt.
2. Durch Phishing wird das Passwort eines Mitarbeiters gestohlen.
3. Ein Angreifer platziert ein Gerät im Firmennetzwerk, das den Netzwerkverkehr protokolliert.
4. Ein Angreifer erhält Zugriff auf die Artikel-Datenbank und passt Werte für die Applikation an.
5. Über eine XSS-Attacke wird eine Session eines Mitarbeiters gestohlen.

|  |  |  |  |
| --- | --- | --- | --- |
| Aufgabe | Vertraulichkeit | Integrität | Verfügbarkeit |
| a) | 0 | 0 | 2 |
| b) | 2 | 2 | 0 |
| c) | 2 | 0 | 0 |
| d) | 2 | 2 | 1 |
| e) | 2 | 2 | 0 |

### Aufgabe 2: Risiko

Sie besitzen ein günstiges und ein teures Fahrrad und haben jeweils in einem Stadtteil mit niedriger und einem mit hoher Kriminalitätsrate zu tun. Sie haben Angst, dass die Fahrräder gestohlen werden könnten.

1. Ordnen Sie die Fahrrad-Stadtteil Kombinationen nach dem Risiko von hoch nach tief:

Kombinationen  
Nach höchstem Risiko geordnet

1. Teures Fahrrad – hohe Kriminalitätsrate
2. Günstiges Fahrrad – hohe Kriminalitätsrate
3. Teures Fahrrad – tiefe Kriminalitätsrate
4. Günstiges Fahrrad – tiefe Kriminalitätsrate
5. Zeichnen Sie die Fahrrad-Stadtteil Kombinationen in folgendem Diagramm ein:

T Fahrrad Hohe Kriminalitätsrate

G Fahrrad  
Hohe Kriminalitätsrate T

Eintrittswahrscheinlichkeit  
(Likelihood)

Niedrig Hoch

T Fahrrad Niedrige Kriminalitätsrate

G Fahrrad Niedrige Kriminalitätsrate

Niedrig Hoch

Schaden (Impact)

1. Wie könnten Sie mit dem Risiko umgehen?
2. Tf +Hk   
   vermeiden mit dem Fahrrad in diesem Stadteil zu fahren
3. Gf + Hk

Gute Deponieren, Fahrradschloss und wenn möglich ebenso, den Stadtteil vermeiden um auf ganz sicher zu gehen

1. Tf + Tk

Fahradschloss nicht unbeaufsichtigt lassen, an gut bewachten Ort deponieren

1. Gf + tk

Braucht nicht viele Vorsichtsmassnahmen, aber wenn man auf ganz sicher gehen will optional ein Schloss

### Aufgabe 2: OWASP

Folgen Sie dem auch in der Präsentation erwähnten Link zu [OWASP](https://owasp.org/). Versuchen Sie, folgende Fragen zu beantworten:

1. Was bedeutet OWASP?

«Open Web Application Security Project» steht für eine Online Community, welche verschiedenen Tools, Technologien usw. für die Sicherheit von Webanwendungen erstellt.

1. Welche Informationen finden Sie auf der Website?

Informationen, wie man die Sicherheit einer Webanwendung verbessern kann.

1. Wer ist verantwortlich für den Inhalt?

Es ist eine unabhängige Organisation, welche nicht von einem Einzelnen oder eine, Anbieter verbunden ist.

1. Was bedeutet «Top Ten»?

Dies ist eine bekannte aktualisierte Liste mit den Top Ten Sicherheitsrisiken für Webanwendungen.

1. Was sind Cheat Sheets?

Anleitungen zur Sicherung von Webanwendungen.

1. Und was um Himmels Willen sind CWE?

«Common Weakness Enumeration» eine liste der Community, über häufige Schwachstellen in Software und Hardware.

## Gütekriterien

Der Lern- und Arbeitsauftrag ist erfüllt, wenn …

* Sie die Szenarien bezüglich der Schutzziele bewertet haben.
* Sie alle Fahrrad-Stadtteil-Kombinationen nach Risiko geordnet haben.
* Sie alle Fahrrad-Stadtteil-Kombinationen im Risikodiagramm eingezeichnet haben.
* Sie für alle Fahrrad-Stadtteil-Kombinationen eine Empfehlung abgegeben haben, wie damit umzugehen ist.
* .

## Zusätzliche Angaben zum Auftrag

-

## Mögliche Erweiterungsaufträge

**Erweiterungsauftrag 1: Vertrauen**

Libraries in der BBB InsecureApp

1. Welchen Libraries und Komponenten wird auf Programmebene (ohne .NET, Betriebssystem, …) in der BBB InsecureApp vertraut, in welchen Versionen sind diese eingebunden und welches wäre die neuste Version der kompatiblen Reihe?

|  |  |  |
| --- | --- | --- |
| Komponente | Verwendete Version | Neuste Version |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. Wenn Sie selber oder im Lehrbetrieb eine Applikation erstellen, gibt es Vorkehrungen wie Sie über Sicherheitslücken in 3th-Party Libraries informiert werden bzw. wie Sie damit umgehen?

1. DDoS: Distributed Denial of Service. Siehe https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/massnahmen-schutz-ddos.html. [↑](#footnote-ref-1)