

# Übung – Identifikation von Sicherheitsrisiken

## Zielsetzung

Analysieren Sie, welche Sicherheitsfunktionen Organisationen zum Schutz ihrer Daten nutzen.

**Teil 1: Analyse der Bedrohung durch Cyber-Angriffe**

**Teil 2: CIA-Dreieck**

## Hintergrund/Szenario

Die Bedrohungen in der Cyberwelt sind sehr real. Sie können in computerbasierten Umgebungen erheblichen Schaden anrichten. Es ist wichtig, diese Bedrohungen zu verstehen und zu bekämpfen. Dazu werden engagierte Personen benötigt, die Bedrohungen erkennen und Cyberkriminellen das Handwerk legen können. Aus diesem Grund haben Organisationen wie CompTIA, Cisco Systems und ISC2 Programme zur Schulung und Zertifizierung von Cybersicherheitsexperten entwickelt.

## Erforderliche Ressourcen

- PC oder Mobilgerät mit Internetzugang

## Teil 1: Analyse der Bedrohung durch Cyber-Angriffe

Cyber-Angriffe gehören zu den größten Bedrohungen weltweit. Bei Bedrohungen der nationalen oder internationalen Sicherheit denken die meisten Menschen an physische Angriffe oder Massenvernichtungswaffen. Tatsache ist jedoch, dass Cyberbedrohungen in mehr als zwanzig Ländern weltweit zu den größten Bedrohungen gehören. Dass Cyber-Angriffe jetzt auf Platz 1 liegen, zeigt, wie sehr sich unsere Gesellschaft verändert hat. Computer und Computer-Netzwerke beeinflussen die Art und Weise, wie wir lernen, einkaufen, kommunizieren, reisen und leben. Computersysteme kontrollieren beinahe jeden Aspekt unseres Lebens. Daher kann die Störung von Computersystemen und -Netzwerken verheerende Auswirkungen auf unser modernes Leben haben. Stromerzeugungs- und -versorgungssysteme, Wasseraufbereitungs- und -versorgungssysteme, Transportwesen sowie Finanzsysteme sind die Ziele von Cyber-Angriffen. Jedes dieser Systeme wurde bereits von Cyberkriminellen angegriffen. Sehen Sie sich das nachfolgende Video an. Bilden Sie Gruppen aus 3 bis 4 Personen. Nachdem Sie sich das Video angesehen haben, beantworten Sie die nachfolgenden Fragen.

### Schritt 1: Informieren Sie sich über Bedrohungen.

In Schritt 1 sollen Sie sich über Bedrohungen informieren.

- a. Klicken Sie [hier](#), um sich das Video anzusehen. Welche ist laut diesem Video die gefährlichste Waffe der Welt? Warum? Stimmen Sie dem zu?

---

---

- b. Geben Sie fünf Möglichkeiten an, wie Cyberkriminelle mithilfe von Computern gegen das Gesetz verstoßen können. Könnte eine dieser Straftaten Sie persönlich treffen? Waren Sie selbst oder Ihre Familienangehörige schon Opfer einer dieser Straftaten?

---

---

- c. Wurde eine der im Video beschriebenen potenziellen Bedrohungen bereits in die Tat umgesetzt? Klicken Sie [hier](#), um mehr über diese Angriffe zu erfahren.

---

---

**Schritt 2: Analysieren Sie kürzlich erfolgte Angriffe.**

- a. Viele Unternehmen und Regierungsbehörden sind wegen der Auswirkungen und dem Ausmaß der letzten Cyber-Angriffe besorgt. Klicken Sie [hier](#), um sich die zehn verheerendsten Cyber-Angriffe aus dem Jahr 2015 anzusehen.

Wie viele Personen waren von der Datensicherheitsverletzung im US Office of Personnel Management betroffen?

---

---

- b. Beschreiben Sie den Angriff auf TalkTalk im Jahr 2015. Wer war verantwortlich und was haben die Cyberkriminellen gestohlen?

---

---

**Teil 2: CIA-Dreieck**

Vertraulichkeit, Integrität und Verfügbarkeit sind die drei grundlegenden Prinzipien der Cybersicherheit. Aus diesen drei Prinzipien besteht das CIA-Dreieck. Die Elemente des Dreiecks sind die drei wichtigsten Komponenten im Bereich Sicherheit. Alle Experten im Bereich Cybersicherheit sollten diese drei Grundprinzipien kennen.

**Schritt 1: Analysieren Sie das CIA-Dreieck.**

- a. Klicken Sie [hier](#), um sich das Video anzusehen. Was bedeutet Datensicherheit? Warum ist Datensicherheit für Einzelpersonen und Organisationen so wichtig?

---

---

- b. Was bedeutet Datenintegrität? Geben Sie drei Möglichkeiten an, bei denen die Datenintegrität oder Vertrauenswürdigkeit beeinträchtigt wird.

---

---

- c. Was bedeutet Systemverfügbarkeit? Welche Folgen kann es haben, wenn ein wichtiges Computersystem nicht mehr verfügbar ist?

---

---

**Schritt 2: Analysieren Sie Cyber-Angriffe.**

Klicken Sie [hier](#), um sich ein Video anzusehen. Wie lautete der Plan der Cyberkriminellen? Zu welcher Tageszeit wurde der Angriff ausgeführt? Ist die Wahrscheinlichkeit, dass Netzwerkangriffe nach Geschäftsschluss ausgeführt werden, groß? Warum?

---

---