

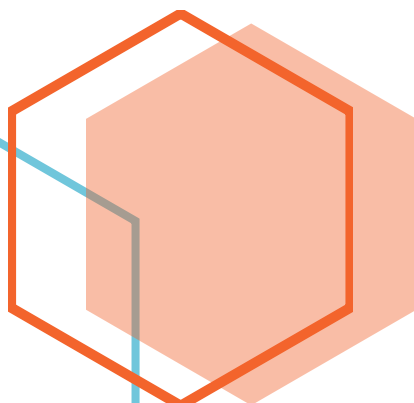
# Cybersicherheit Kt1



---

## Die Grundlagen der Cybersicherheit

In diesem Kapitel lernen wir die Grundlagen der Cybersicherheit kennen.



## Cybersicherheit

1.2.1.1 Wer sind die Cyberkriminellen .....	1
1.2.1.2 Welche Farbe hat mein Hut-Übung.....	2
1.2.1.3 Motive der Cyberkriminellen .....	2
1.2.1 Warum Cybersicherheitsexperte werden .....	2
1.2.2 Bekämpfen von Cyberkriminellen.....	2
1.2.3 Bekämpfen von Cyberkriminellen-Übung .....	3
1.2.4 Cybersicherheit Stellensuche .....	3
1.3.1.2 Arten von persönlichen Daten .....	3
1.4.1.1 Interne und Externe Bedrohung .....	3
1.4.1.3 Der Siegeszug des Internet of Things.....	4
1.4.1.4 Die Auswirkungen von Big Data .....	4
1.5.1.2 Sieben Kategorien von Cybersicherheitsexperten .....	4
1.5.1.3 Identifizieren der Nist-Übung.....	4

### 1.2.1.1 Wer sind die Cyberkriminellen

**White Hat-Hacker:** Hacken für das Gute. Ihr Job ist es eine Lücke in der Website zu finden und diese melden. Damit verbessern sie die Sicherheit der Website.

**Gray Hat-Hacker:** Können sowohl gut, als auch Böse sein. Sie können die Lücken melden oder sie öffentlich posten, damit sich ein Black Hat leichter reinhacken kann

**Black Hat-Hacker:** Das sind Kriminelle. Sie Hacken um Kreditkarten, Informationen, Bilder oder vieles mehr rausbekommen. Sie können auch von der Regierung angestellt sein.

**Organisierte Angreifer:** Können für den Staat eine Terroristengruppe oder einen Politiker arbeiten

**Amateure:** Auch Skript-Kiddies genannt. Haben keine, oder eine sehr geringe Programmierfertigkeiten. Benützen meist vorhandene Tools oder Anleitungen aus dem Internet. Sind meist nur neugierig oder wollen ihre Fähigkeiten unter Beweis stellen. Können auch gefährlich werden

### 1.2.1.2 Welche Farbe hat mein Hut-Übung

The screenshot shows the Cisco Cybersecurity Essentials interface. The main window displays an exercise titled 'Aktivität: Identifizieren der Hackerkategorie'. On the left, there are instructions: 'Anweisungen: Klicken Sie auf das Merkmal des entsprechenden Feldes, um den Hacktyp anzugeben, den es beschreibt.' Below the instructions are buttons for 'Überprüfen' and 'Zurücksetzen'. The main area contains a table with hacker characteristics and their corresponding hat colors.

Hackermerkmal	White-Hat	Grey-Hat	Black-Hat
Nachdem Geldautomaten von einem Laptop aus per Fernzugriff gehackt wurden, arbeitete er mit Herstellern von Geldautomaten zusammen, um die gefundenen Sicherheitslücken zu schließen.		✓	
Von meinem Laptop aus überwies ich mit den Kontonummern und PINs der Opfer 10 Millionen \$ auf mein Bankkonto, nachdem ich die Eingabe der Ziffern durch die Opfer aufgezeichnet hatte.			✓
Meine Aufgabe ist die Ermittlung von Schwachstellen im Computersystem meines Unternehmens.	✓		
Ich verwendete Malware, um in mehrere Unternehmenssysteme einzudringen und Kreditkarteninformationen zu stehlen, und verkaufte diese Informationen an den Höchstbietenden.			✓
Während einer Untersuchung von Sicherheitschwachstellen stolperte ich über eine Sicherheitslücke in einem Unternehmensnetzwerk, für das ich zugangsberechtigt bin.	✓		
Ich arbeite bei Technologiefirmen, um einen Mangel bei DNS zu beheben.	✓		

At the bottom of the interface, there are navigation icons: 'Zuletzt besucht', 'Lesezeichen', 'Kursindex', 'Suche', 'Sprachen', 'Hintergrund auswählen', and 'Hilfe'. The bottom status bar shows the date '06.11.2021' and time '19:40'.

### 1.2.1.3 Motive der Cyberkriminellen

Hacker haben viele Motive, jedoch ist das häufigste Geld. Dennoch gibt es Motive wie Politische Meinung oder auch Lust seine Fähigkeiten auszutesten oder anerkannt zu werden. Durch die Jahre haben sich viele Gruppen gebildet wie zum Beispiel: Haktivisten, Schwachstellen-Broker, Cyberkriminelle oder auch eine Gruppe die vom Staat gefordert wird.

### 1.2.1 Warum Cybersicherheitsexperte werden

Als Cybersicherheitsexperte hat man gute Verdienstmöglichkeiten. Die Nachfrage für Cybersicherheitsexperte ist stark gestiegen, da die Technologie selbst nicht jede Lücke finden kann und ständig neue Technologien erfunden werden. Dazu ist die Anzahl von gut Ausgebildeten Cybersicherheitsexperten relativ gering. Man kann praktisch überall einen Job finden und ein Cybersicherheitsexperte ist eine Unverzichtbare Person bei einer großen Organisation.

### 1.2.2 Bekämpfen von Cyberkriminellen

Die Bekämpfung von Cyberkriminellen ist eine sehr schwierige Aufgabe. Es wurden Datenbanken erstellt, um schon bekannte Sicherheitslücken reinschreiben. Diese werden zwischen Organisationen weltweit geteilt. Implementierung von Frühwarnsensoren und Warnnetzwerken. Das heißt es werden Netzwerke überwacht. Natürlich nicht alle sonst würde das Milliarden kosten, es werden nur High value Netzwerke überwacht. Die Unternehmen tauschen außerdem wichtige Informationen aus. Es werden auch Normen und Gesetze erstellt wie zum Beispiel ISO 27000. Solche Gesetze weisen oft hohe Geldstrafen aus.

## 1.2.3 Bekämpfen von Cyberkriminellen-Übung

**Aktivität: Identifizieren von Cybersicherheitsmaßnahmen zur Bekämpfung von Cyberkriminellen**

Anweisungen: Ordnen Sie jeden Begriff einer Beschreibung zu.

Begriff	Beschreibung
Frühwarnsysteme	Das Projekt "HoneyNet"
Informationsaustausch	Das InfraGard-Programm
ISM-Standards	ISO/IEC 27000
Neue Gesetze	Cybersecurity Act
Schwachstellen-datenbank	Das nationale CVE-Projekt (Common Vulnerabilities and Exposures)

Buttons: Überprüfen, Zurücksetzen

Navigation: Zuletzt besucht, Lesezeichen, Kursindex, Suche, Sprechen, Hintergrund auswählen, Hilfe

## 1.2.4 Cybersicherheit Stellensuche

Suche: Cyber Security, Wien, 30 km, Jobs finden

Wien im Umkreis von 30 km.

Filter: Erscheinungsdatum (Neuer als 7 Tage: 38), Home-Office-Optionen (Home-Office möglich: 21), Pendelzeit, Von wo starten Sie? (Adresse, PLZ oder Stadt), Maximale Dauer, Wie kommen Sie zur Arbeit? (ZU FUSS, FAHRAD, AUTO, ÖPNV), Bewerbungsart (Auf Unternehmenswebsite: 64).

Jobs:

- IVM** Cyber-Security Engineer (m/w/d) - im Automotive Sektor
- DTS** Junior Cyber Security Administrator (w/m/d)
- DTS** Cyber Security Engineer (w/m/d)
- EY** Cyber Security Consultant (w/m/d)
- IVM** Cyber Security Analyst (m/w/d) - Senior Position
- Cybersecurity - Consultant (m/w/d)**

### 1.3.1.2 Arten von persönlichen Daten

Es gibt viele Arten von persönlichen Daten und sie reichen von Medizinischen Daten bis zu Finanzdaten. Beispielsweise werden nach jedem Arztbesuch Daten über deinen körperlichen Zustand gesammelt. Auch medizinische Geräte wie ein Fitnesband sammeln deine Daten. Auch Informationen über deine Bildung gespeichert und über deine Arbeitgeber oder Finanzdaten.

### 1.4.1.1 Interne und Externe Bedrohung

Es gibt interne und externe Sicherheitsbedrohungen. Die internen haben ein größeres Bedrohungsgrad, da der Angreifer einen direkten Zugang hat. Diese können unabsichtlich oder auch absichtlich geführt werden. Ein Mitarbeiter kann ein USB-Stick mit malware einstecken oder Passwörter leaken. Bei externen Angriffen werden Sicherheitslücken benutzt oder Social Engineering Skills benutzt. Es wird oft auf herkömmliche Daten gezielt. Diese sind Beispielsweise Patente, Markenzeichen und Pläne für neue Produkte Personaldaten, Bewerbungsunterlagen, Gehaltslisten, Angebotsschreiben, Mitarbeitervereinbarungen sowie alle relevanten Informationen für Einstellungsentscheidungen.



### 1.4.1.3 Der Siegeszug des Internet of Things

Das Internet of Things ermöglicht verschiedene Geräte an das Internet zu verbinden. Die verändert unsere Umgebung sowohl im privaten als auch im geschäftlichen Leben. Wegen der Technologie nimmt die Menge der zu schützenden Daten rasant zu. Wegen der Technologie wurde ein eigener Geschäftsbereich hinzugefügt, der heißt „Big Data“.

### 1.4.1.4 Die Auswirkungen von Big Data

Big Data sind große und komplexe Datensätze. Daraus ergeben sich Herausforderungen in drei Dimensionen: Datenvolumen bzw. Datenmenge, Datengeschwindigkeit, Auswahl an Datentypen und Datenquellen. Angriffe auf Großunternehmen durch die Nachrichten. Angriffe auf Firmen wie Target, Home Depot und PayPal finden große Beachtung in der Öffentlichkeit. Deshalb müssen Unternehmenssysteme ihr Design ändern.

### 1.5.1.2 Sieben Kategorien von Cybersicherheitsexperten

Das Workforce Framework ordnet Aufgaben im Bereich der Cybersicherheit in sieben Kategorien ein. Diese sind: Betrieb und Wartung (Operate and Maintain), Schutz und Verteidigung (Protect and Defend), Untersuchung (Investigate), Erfassung und Abwehr (Collect and Operate), Analyse (Analyze), Überwachung und Entwicklung (Oversight and Development), Sichere Bereitstellung (Securely Provision). Jede Kategorie ist in mehrere Spezialgebiete unterteilt.

### 1.5.1.3 Identifizieren der Nist-Übung

The screenshot shows a web-based interface for the Cisco Cybersecurity Essentials course. The main window displays the exercise 'Identifizieren der NIST/NICE-Cybersicherheits-Spezialgebiete'. The interface includes a sidebar with navigation links and a main content area with instructions and a table of specialties.

**Anweisungen:**  
Wählen Sie die passenden Cybersicherheits-Spezialgebiete für die jeweiligen Beschreibungen aus.

Spezialgebiete Cybersicherheit	Beschreibungen
Überwachung und Entwicklung (Oversight and Development)	Bereitstellen von Führung, Management, Direktion und/oder Entwicklung
Betrieb und Wartung (Operate and Maintain)	Bereitstellen von Support, Administration und Wartung
Erfassung und Betrieb (Collect and Operate)	Spezielle Verweigerungs- und Täuschungsoperationen
Sichere Bereitstellung (Securely Provision)	Konzepterstellung, Entwicklung und Aufbau sicherer IT-Systeme
Schutz und Verteidigung (Protect and Defend)	Identifizierung, Analyse und Abwehr von Bedrohungen
Analyse	Prüfung und Bewertung eingehender Cybersicherheitsinformationen
Untersuchen	Überprüfung von Cyberereignisse und/oder Straftaten in IT-Systemen

Buttons: Überprüfen, Zurücksetzen

Navigation: Zuletzt besucht, Lesezeichen, Kursindex, Suche, Sprachen, Hintergrund auswählen, Hilfe

Footer: 22:09 06.11.2021