Kacper Bohaczyk 2cHIT

Cybersicherheit Kt1

Die Grundlagen der Cybersicherheit

In diesem Kapitel lernen wir die Grundlagen der Cybersicherheit kennen.

Cybersicherheit

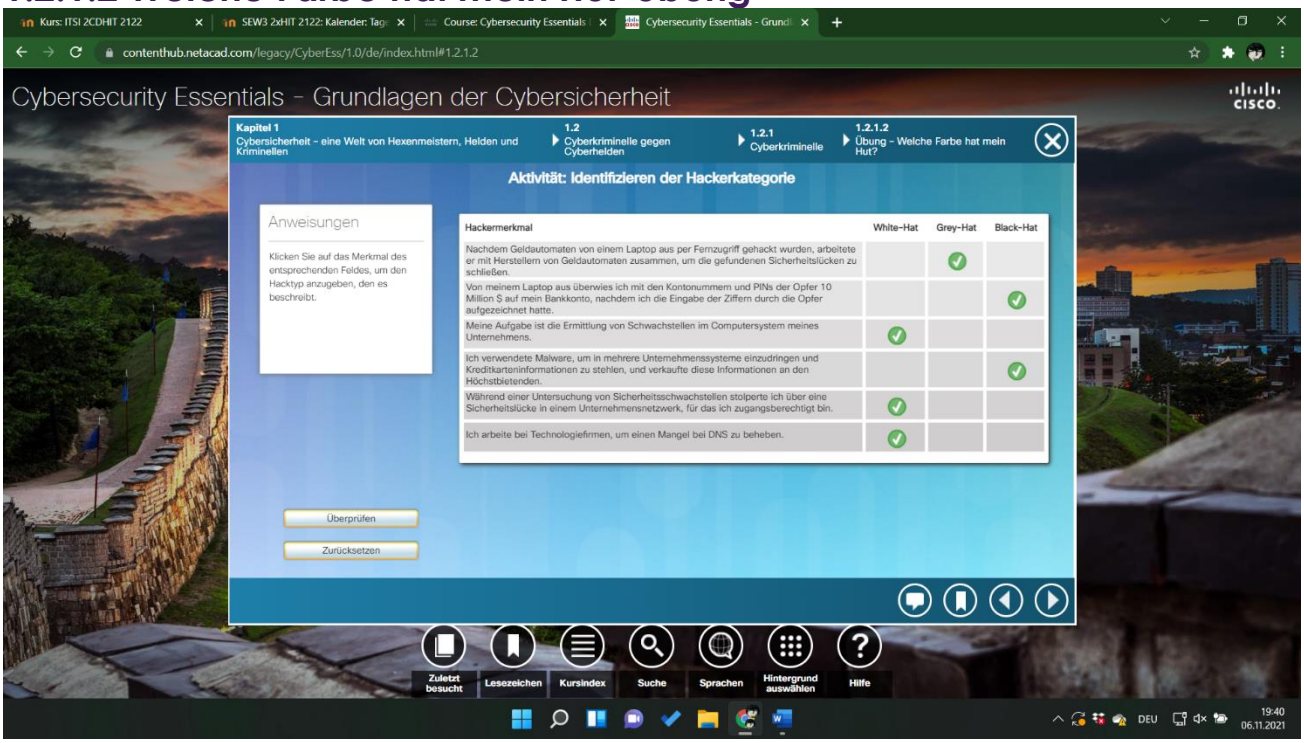
1.2.1.1 Wer sind die Cyberkriminellen

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 Stadt 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



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: Hacktivisten, Schwachstellen-Broker, Cyberkrimielle oder auch eine Gruppe die vom Staat gefordert wird.

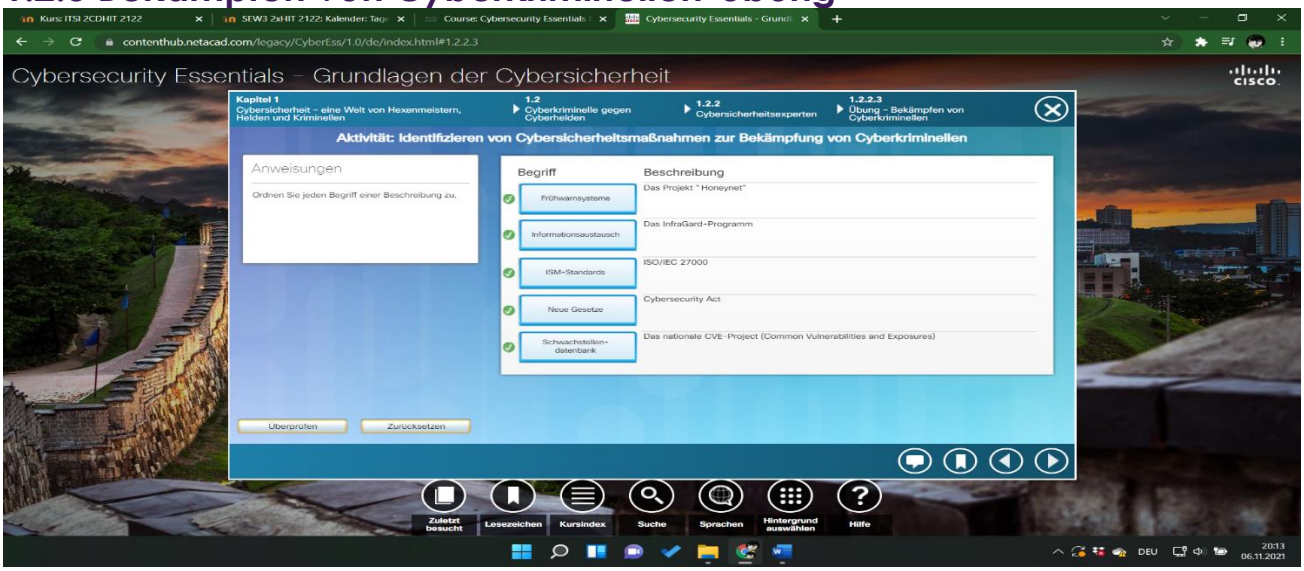
1.2.1 Warum Cybersicherheitsexperte werden

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.

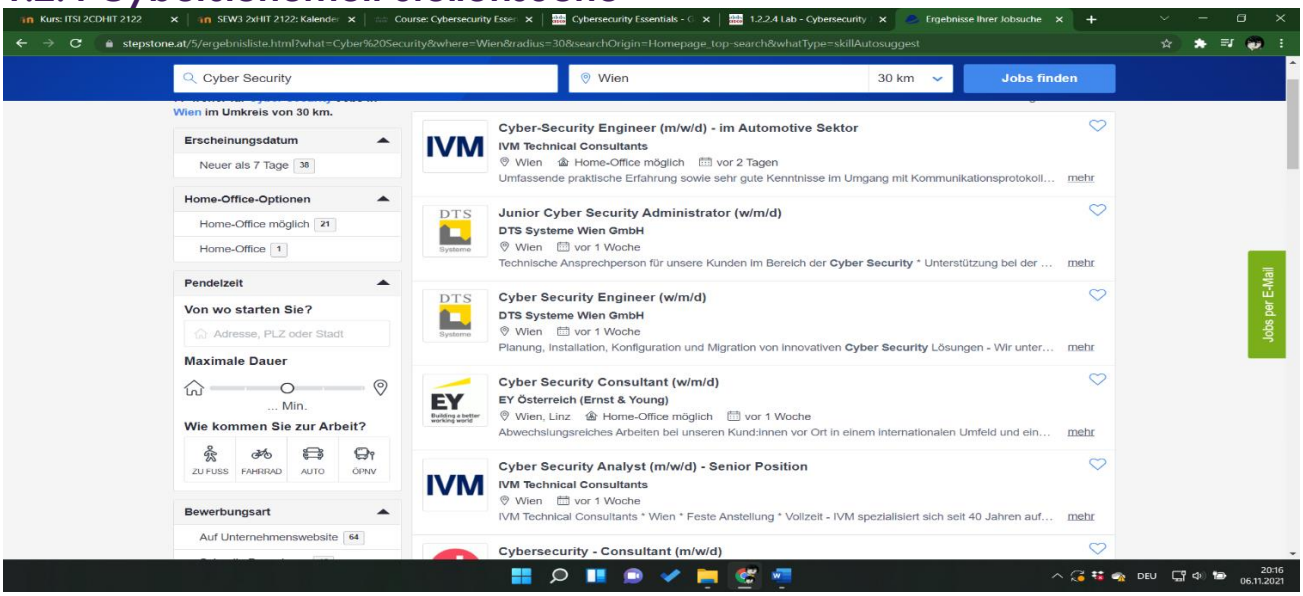
1.2.2 Bekämpfen von Cyberkriminellen

Die Bekämpfung von Cyberkriminellen ist eine sehr schwierige Aufgabe. Es wurden Datenbänke erstellt, um schon bekannte Sicherheitslücken reinzuschreiben. 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 Gesetzte erstellt wie zum Beispiel ISO 27000. Solche Gestze weißen oft hohe Geldstraffen aus.

1.2.3 Bekämpfen von Cyberkriminellen-Übung



1.2.4 Cybersicherheit Stellensuche



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 Schutzenden 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 Unternehensysteme 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