



# Projekt Nr.

**206**

Hochtaunusschule  
Berufliche Schulen des  
Hochtaunuskreises  
in Oberursel (Taunus)



<b>Projekttitle</b>	Datenschutzanalyse im Unternehmen		
<b>verantwortliche Lehrkraft</b>	Stückrath.christian	@hochtaunusschule.de	
Weitere Verantwortliche	Roy		

<b>Kurzbeschreibung des Projekts</b>	Die SuS sollen in Gruppenarbeit eine Netzwerkumgebung auf den datenschutzrelevanten Schutzziele (VIV) untersuchen (1. Tag), Maßnahmen ergreifen sich vor Angriffen zu schützen (2. Tag) und testen, ob die Maßnahmen wirkungsvoll waren [mit Pentesting] (3. Tag). Am 4. Tag werden die Ergebnisse, Probleme, Fehler und Erfolge vorgestellt. Dabei arbeiten die SuS mit realen Situationen (bspw. Clients und Server bei einem Arzt mit hochsensiblen Patientendaten oder in einer Schule in der LehrerInnen sich "analog & digital" Noten austauschen) mit virtuellen Maschinen und virtuellen Netzwerken.					
	<b>Schwerpunkt (ankreuzen)</b>	Beruflich	Sportlich	Kulturell	Allgemeinbildend	Kulturaustausch: InteA ⇔ „Deutsche“
	X					

<b>maximale Schüleranzahl</b>	25	<b>Mindestalter Schüler</b>	
<b>voraussichtliche Kosten pro Schüler</b>	7	<b>Zustimmung der Eltern erforderlich</b>	nein
<b>nötige Vorkenntnisse</b> ⇒ Schulform	IT-Berufe	<b>nötige Schüleraus-rüstung</b>	PC

## Wochenplanung des Projektes

**Bitte eintragen: KERNZEIT 9:30 - 12:30 Uhr bei Mindest - Tagesaktivität von 4,5 Zeitstunden**

Tag	Montag 18.7.22	Dienstag 19.7.22	Mittwoch 20.7.22	Donnerstag 21.7.22
<b>Uhrzeit Von / bis</b>	8:30 – 13:00 Uhr	8:30 – 13:00 Uhr	8:30 – 13:00 Uhr	8:30 – 13:00 Uhr
<b>Tätigkeit</b>	Die Gruppen analysiert die vorgegebene IT nach dem IT-Grundschutzkompendium des BSI. Dazu priorisieren sie die Schutzziele nach datenschutzrelevanten Kriterien und geben zu den einzelnen Situationen Vorschläge zur Erhöhung der Datensicherheit. (4 - 6 Schulstunden)	Alle Gruppen sollen dann mit den erstellten Analysen Maßnahmen an den virtuellen Maschinen und dem virtuellen Netzwerk ergreifen, die sensiblen Daten zu schützen. (6 Schulstunden)	In der letzten Phase erlernen die SuS Techniken, um mit frei verfügbaren Tools Pentests auszuführen. Damit soll die Sicherheit des Netzwerkes mit selbsterstellten Testabläufen überprüft, eventuelle Schwächen (bspw. nicht bestandene	<b>SCHULFEST:</b> Die SuS sollen ihre Ergebnisse Darstellen. Dabei ist es wichtig, dass sie auch über mögliche Fehlschläge, Frustrationen, Probleme, Eigen-motivationen sprechen und sich über die Wichtigkeit der Einhaltung der Schutzziele be-