FH | JOANNEUM
University of Applied Sciences

Konzept einer qualitativ hochwertigen Hochschullehre mit Fokus auf berufsbegleitende, technische Studiengänge

Förderung von High Potentials

September 2017

INHALTSVERZEICHNIS

EINLEITUNG

Ein berufsbegleitendes Studium unterscheidet sich merklich von einem Vollzeitstudium. Studierende stehen meist voll und ganz im Berufsleben und absolvieren das Studium zusätzlich zu einer 40 Stundenwoche. Die außerordentliche Belastung durch Unterricht am Abend bzw. am Wochenende ist auch in der Gestaltung von Lehrveranstaltungen zu berücksichtigen. Die Zeit zum Verarbeiten von neuen Inhalten, Bearbeitung von Hausübungen und Erarbeitung von Seminarthemen ist sehr begrenzt.

Studierende sind sowohl in Präsenzphasen als auch im Online-Unterricht meist weniger aufnahmefähig da bereits zuvor ein normaler Arbeitstag absolviert wurde. Andererseits bringen berufsbegleitende Studierende oft große Erfahrung und Wissen in spezifischen Bereichen mit. Lehrende sollten darauf Rücksicht nehmen und dieses Wissen auch in der Lehrveranstaltung nutzen.

Online-Unterricht und im speziellen synchroner[1] Online-Unterricht fordert sowohl Lehrende als auch Studierende. Trotz moderner technischer Lösungen bietet der synchrone Online-Unterricht nur stark reduzierte Kommunikationsmöglichkeiten. Aktivierende Werkzeuge von Vortragendenden sowie Gestik und Mimik können nur eingeschränkt transportiert werden. Auch diese Tatsache ist bei der Gestaltung von Lehrveranstaltungen zu berücksichtigen. Aus Feedbackgesprächen mit Studierenden geht hervor, dass Online-Einheiten sowohl für Lehrende als auch für Studierende sehr anstrengend sind. Die Aufmerksamkeitsphasen können durch Ablenkung im privaten Umfeld und fehlender Abwechslung im Vortrag stark eingeschränkt werden.

Das vorliegende Konzept zeigt unter Berücksichtigung der oben angesprochenen Problematik die Gestaltung einer integrierten Lehrveranstaltung aus dem Bereich der IT-Sicherheit.

ZIEL DER LEHRVERANSTALTUNG

Die Lehrveranstaltung soll neben technischen Fertigkeiten auch außergewöhnlich kreative Lösungskompetenzen vermitteln. Studierende kennen nach erfolgreicher Absolvierung die gängigsten Angriffsmethoden von Hackern, können diese nachvollziehen und auch anwenden und sind mit dem erworbenen Wissen in der Lage, bestehende IT-Systeme entsprechend abzusichern und gegen Angriffe zu verteidigen. Ein weiteres Ziel besteht in der Förderung von High Potentials ohne gleichzeitig andere Studierende zu überfordern.

[1] Studierende und Vortragende kommunizieren während der Online-Einheit mittels elektronischer Kommunikationsmittel. D.h., die Online-Vorlesung findet live statt.

Strukturierung und Organisation der Lehrveranstaltung

Um den zeitlichen Aufwand der Studierenden außerhalb der Lehrveranstaltung zu minimieren, muss die Festigung des neu erlernten Wissens bereits im Rahmen des Unterrichts erfolgen. Dabei kommen Ketten aus Kombinationen von Vorstellung neuer Methoden und Werkzeugen und deren sofortiger praktischer Umsetzung im Labor zum Einsatz.

Als Feedback über den Lernfortschritt für Studierende und Vortragende erfolgt regelmäßig eine schriftliche Kurzwiederholung zu Beginn der darauffolgenden Einheit. Das kurze Feedback wird einerseits als Teil der Beurteilung genutzt und andererseits kann durch die Reflexion der vorhergehenden Inhalte sofort nahtlos auf das Stoffgebiet der letzten Einheit aufgebaut werden. Der Vortragende kann bei Verständnisproblemen zeitnah reagieren und Unklarheiten der Thematik vor der Behandlung eines neuen Stoffgebietes aufklären.

Die stark reduzierte Anwesenheit von berufsbegleitenden Studierenden erfordert, dass diese Vorgehensweise auch außerhalb der FH Räumlichkeiten in den Online-Einheiten fortgesetzt wird.

Schriftliche Kurzwiederholungen sind im synchronen Online-Unterricht sehr gut über elektronische Fragebögen durchführbar. Durch rasche Beantwortung einer hohen Anzahl von Ja/Nein Fragen innerhalb kurzer Zeit ist einerseits sehr schnell ein Bild über das Verständnis der Studierenden über das Stoffgebiet vorhanden, andererseits ist damit auch die Möglichkeit einer Abstimmung der Studierenden untereinander eingeschränkt. Ist die Gefahr von Gruppenarbeiten im Online-Betrieb zu groß, so kann die Befragung auch anonym gestaltet werden. Der Lehrende erhält trotzdem rasch Feedback über den Lernerfolg. Ein Beitrag zur Beurteilung ist dann allerdings nur bei Präsenzterminen möglich.

Online Laborübungen

Praktische Laborübungen im Online-Betrieb sind durchaus möglich und dienen zur Aktivierung der Studierenden, im Vergleich zu Präsenz Laborübungen sind allerdings folgende Punkte zusätzlich zu beachten:

Zugriff auf das Laborsystem aus dem Internet: Mittlerweile existieren zahlreiche Möglichkeiten, virtuelle Systeme bei Cloud-Anbietern zu hosten und den Studierenden zugänglich zu machen. Da die Unterstützung durch die Lehrenden bei verteilten Laborübungen eingeschränkt ist (Einfaches über die Schultern blicken funktioniert nicht), muss ein Laborsystem einfache Rücksetzmechanismen in den Ausgangszustand anbieten.

Offline Bereitstellung von Labor Aufgaben: Virtualisierte Systeme können den Studierenden auch vorab zur Verfügung gestellt werden. Bei dieser Form der Laborvorbereitung besteht allerdings die Gefahr, dass es durch unterschiedliche Systemumgebungen der Studierenden zu Installationsproblemen kommen kann. Eine Ferndiagnose durch den Vortragenden im Rahmen der Lehrveranstaltung ist meist nur eingeschränkt möglich.

Für eine einheitliche Laborumgebung ist die erste Variante zu bevorzugen. Der Lehrende kann die Infrastruktur vorab bereitstellen und testen. Der spätere Zugriff im Rahmen der Lehrveranstaltung erfolgt auf ein einziges, homogenes System.

Hilfestellung durch den Lehrenden: Die Unterstützung durch den Vortragenden während der Laborübung kann durch Screen Sharing mit den Studierenden erleichtert werden. So bietet beispielsweise Skype for Business [2]die Möglichkeit, Präsentationsrechte an Studierende zu übergeben und damit den Lehrenden Zugriff auf Studierenden Desktop zu erlauben. Eine weitere Möglichkeit ist die Nutzung von Remote Access Tools wie z.B. TeamViewer[3] zur „vor Ort" Hilfe durch den Lehrenden.

Mehrere Einstiegspunkte in Laborübungen: Bei Online-Laborübungen ist die Gefahr groß, dass Studierende, trotz Unterstützung durch den Vortragenden, den Anschluss verlieren. Ohne weitere Maßnahmen könnten die betroffenen Studierenden für die restliche Zeit an der Laborübung nicht mehr teilnehmen bzw. dem Übungsfortschritt folgen. Der Vortragende kann Teillösungen im Bedarfsfall bereitstellen bzw. freischalten um den Wiedereinstieg bei z.B. 25%, 50% oder 75% der Laborübung zu ermöglichen. Damit wird zwar ein Teil der Übung übersprungen, der Rest kann aber normal fortgesetzt werden.

INHALTLICHER GESTALTUNG

Der inhaltliche Aufbau der Lehrveranstaltung gliedert sich in drei Bereiche, wobei die Komplexität von Bereich zu Bereich zunimmt.

Methoden und Werkzeuge: Der erste Bereich behandelt die Basismechanismen, Methoden und Werkzeuge die sowohl für einen erfolgreichen Angriff als auch für eine effektive Verteidigung eines IT-Systems notwendig sind. Die praktische Festigung des Wissens erfolgt durch Anwendung auf isolierte, vordefinierte Übungssysteme.

Angriff auf komplexe Systeme: Die zweite Phase der Festigung des im ersten Bereichs erworbenen Wissens erfolgt durch Anwendung auf komplexe Laborsysteme mit umfangreicher Funktionalität. Die Übungssysteme beinhalten nun alle Bestandteile, die im ersten Bereich einzeln geübt wurden.

Verteidigung komplexer Systeme: Die ersten beiden Bereiche stellen die Sicht, Motivation und Möglichkeiten von Angreifern (Hacker) dar. Im dritten Bereich wechseln die Studierenden nun die Seite und haben die Aufgabe ein komplexes IT-System im Labor gegen klassische Angriffe abzusichern.

Nach dem Motto „Kenne deinen Feind"[4] wurde die Absicherung/Verteidigung von IT-Systemen durch Kenntnis der Angriffsmöglichkeiten erarbeitet.

---

[2] https://products.office.com/en-us/skype-for-business/online-meetings
[3] https://www.teamviewer.com/de/
[4] Sun Tzu, Die Kunst des Krieges

Den Abschluss der Lehrveranstaltung bildet eine Hacking-Challenge auf Basis „Capture The Flag“. Zwei Teams treten gegeneinander an. Beide Teams erhalten zwei exakt ident konfigurierte IT-Systeme. Die Teams haben nun die Aufgabe sog. Flags[5] vom gegnerischen System zu sammeln und das eigene System entsprechend abzusichern. Dabei wird die Fähigkeit gefördert, kreative Lösungswege unter Zeitdruck zu finden.

Um High Potentials bzw. Studierenden mit einschlägiger Berufserfahrung in der Thematik die Möglichkeit einer Wissenserweiterung zu geben besteht die Möglichkeit an einer Österreich weiten Qualifikation[6] für Nachwuchstalente in der IT-Security teilzunehmen. Dazu stellt der in der Lehrveranstaltung vermittelte Inhalt die Basis dar. Eine erfolgreiche Qualifikation erfordert eine wesentlich weitere Vertiefung. Dazu besteht parallel zur Lehrveranstaltung die Möglichkeit an einer öffentlichen Trainingsplattform zahlreiche Security Aufgaben mit unterschiedlichem Schwierigkeitsgrad zu absolvieren. Der Austausch mit anderen Studierenden und Lehrenden ist erlaubt und auch erwünscht.

BEURTEILUNG

Die Beurteilung der Lehrveranstaltung erfolgt einerseits durch Bewertung der Kurzwiederholungen während des Semesters (20%), der Mitarbeit bei Laborübungen (20%) und einer praktischen Abschlussarbeit (60%).

Der praktische Abschlussteil besteht aus ausgewählten Aufgaben ein IT-Service abzusichern oder anzugreifen. Dabei kann aus eine Reihe von unterschiedlich komplexen Aufgaben und Punkten gewählt werden. (EASY: 10, MODERATE: 20, CHALLENGING: 30 und INSANE: 40)

Es müssen nicht alle Aufgaben gelöst werden. Die Aufgabenstellung ist zu 100% erfüllt, wenn 40 Punkte erreicht wurden. Bei derartigen Aufgabenstellungen kann es durchaus vorkommen, dass sich Studierende in einem Lösungsansatz verlaufen. Es können während der Prüfung je Aufgabe drei Lösungshinweise mit jeweils 10% Punkteabzug genutzt werden.

Für Studierende die sich im Rahmen der Qualifikation der Cyber Security Challenge Austria vorbereiten und auf der Trainingsplattform eine Reihung unter den Top 100 erreichen bzw. sich für das Österreich Finale qualifizieren, entfällt die Absolvierung der Abschlussarbeit. Der Aufwand ist hier allerdings wesentlich höher als sich für die Prüfung vorzubereiten, auf der Trainingsplattform sind etwa 50.000 Benutzer registriert – wobei ca. 2000 ernsthaft Aufgaben lösen. Pro Jahrgang entscheiden sich etwa 5% bis 10% der Studierenden für diesen Weg mit dem Erfolg, dass es heuer einer der Teilnehmer unter die Top 10 der österreichischen Studierenden und damit in das Finale geschafft hat.

Das Beispiel zeigt eindrucksvoll, dass durch entsprechende Motivation und Schaffung von Rahmenbedingungen Höchstleistungen von Studierenden möglich sind und auch die Bereitschaft von weit über den Umfang einer Lehrveranstaltung hinausgehenden Aufwänden gegeben ist.

---

[5] Flag = Geheimer Code der nur nach Kompromittierung eines Systems auslesbar ist

[6] Cyber Security Challenge Austria http://www.verbotengut.at/