

ComPete

Kompetenzaufbau Penetration Testing

| | | | |
|---------------------------------|--|------------------------|---------------|
| Programm / Ausschreibung | FoKo, Qualifizierungsseminare, Qualifizierungsseminare 7. AS | Status | abgeschlossen |
| Projektstart | 01.11.2020 | Projektende | 30.04.2021 |
| Zeitraum | 2020 - 2021 | Projektlaufzeit | 6 Monate |
| Keywords | Cyber Security, Penetration Testing | | |

Projektbeschreibung

Der steigende Vernetzungsgrad sowohl innerhalb von Unternehmen als auch zwischen kooperierenden Firmen hat eine Steigerung der Anforderungen an die IT-Sicherheit und die Robustheit gegenüber Cyber Angriffen zur Folge.

Flächendeckende, aber auch gezielte Cyber Angriffe auf Unternehmen sind seit vielen Jahren ein ernstzunehmendes Problem und richten enormen Schaden an. Aktuell zeigt sich in Trend der Verlagerung der Angriffsziele hin zu KMU's, die oft wenig geschützt sind und daher einfache Ziele darstellen.

Die Anforderungen an die IT in Unternehmen, im Speziellen KMU's, ist mit den zahlreichen Security Vorfällen gestiegen. Die IT Mitarbeiter müssen nun auch das Thema IT-Security mit abdecken, wobei die Kenntnisse in diesem Bereich nicht oder nur wenig vorhanden sind. Die zeitnahe und richtige Reaktion auf einen laufenden Security Vorfall (Incident Response) ist notwendig, um den IT-Betrieb auch im Angriffsfall am Laufen zu halten.

Das Ziel der Maßnahme ist es, Personal in der IT von KMUs das nötige Rüstzeug zu geben, um die täglichen Security Aufgaben und Vorkommnissen in Unternehmen bewerkstelligen zu können.

Nach der Absolvierung der Basis Module im Bereich Netzwerke, Betriebssysteme und WEB-Technologien werden anhand praktischer Szenarien die Penetration Testing Methoden und Tools vorgestellt. Die Teilnehmer haben die Möglichkeit, in einer simuliertem, virtuellen IT-Umgebung eines Unternehmens Schwachstellen zu identifizieren und sowohl Angriffe als auch Verteidigungsstrategien zu testen. Diese Testmöglichkeiten stehen im eigenen Unternehmen selten zur Verfügung. Die Laborinfrastruktur der FH JOANNEUM erlaubt es den Teilnehmern, Aufgabenstellungen und Konfigurationsvarianten aus dem eigenen Unternehmen mit in das Labor zu nehmen, dort zu implementieren und die entsprechenden Maßnahmen zur Absicherung zu testen. Mit dieser individuellen Möglichkeit auf Problemstellungen aus dem eigenen Unternehmen eingehen zu können, sehen wir den großen Vorteil gegenüber der am Markt angebotener Standard Security Trainings.

Die Teilnehmer sind nach Absolvierung der Qualifizierungsmaßnahme in der Lage

- Schwachstellentests im eigenen IT-System durchzuführen
- Hackerangriffe zu identifizieren
- Schutzmaßnahmen gegen Angriffe zu implementieren
- Kurzfristige Maßnahmen zur Eindämmung eines laufenden Angriffs zu treffen

Projektkoordinator

- FH JOANNEUM Gesellschaft mbH

Projektpartner

- AutForce Automations-GmbH
- Intact GmbH
- MGX Automation GmbH
- THM-IT GmbH
- RPD Rapid Product Development GmbH
- ABATON EDV - Dienstleistungs GmbH