Projekthandbuch

AI in der Security

1

Version 1.0
Projektleiter/in: Sebastian Lipp
Datum: 21.04.2020

Inhalt

Änderungsverzeichnis

Versions-nummer	Datum	Änderung	Ersteller
0.1	11.04.2020	Aktualisieren des PHB aus dem WS: Allgemeine Projektbeschreibung, Projektauftrag, Projektzieleplan, Beschreibung Vorprojekt- und Nachprojektphase, Projektmeilensteinplan, Projektrisikonanalyse Integration des Dokuments ‚MCS-SS2020-PRJ2_Projektplanung.pdf' in das PHB	Wech Maximilian
0.2	12.04.2020	Projektstrukturplan, Projektbalkenplan, Projektzeitplan	Wech Maximilian
0.3	16.04.2020	Einarbeiten des Feedbacks des Lektors: Allgemeine Projektbeschreibung, technisches Konzept, Projektbalkenplan, Projektstrukturplan, Verantwortlichkeiten	Wech Maximilian
0.4	20.04.2020	Arbeitspaketspezifikationen	Wech Maximilian

Ansprechpartner

Name	**Organisations-einheit**	**Rolle im Projekt**	**Telefon** (Büro, Mobil, Privat, …)	**e-mail**
Dipl.-Ing. Dr. Gerd Holweg	FH-Technikum Wien	Projektauftraggeber	0650 1234567	gholweg@technikum-wien.at
Bernhard Gally	FH-Technikum Wien - IT-Security	Projektteammitglied	0650 1234561	cs19m023@technikum-wien.at
Sebastian Lipp	FH-Technikum Wien - IT-Security	Projektleiter	0650 1234562	cs19m032@technikum-wien.at
Damir Marijanovic	FH-Technikum Wien - IT-Security	Projektteammitglied	0650 1234563	cs19m031@technikum-wien.at
Boris Stampf	FH-Technikum Wien - IT-Security	Projektteammitglied	0650 1234565	cs19m006@technikum-wien.at
Maximilian Wech	FH-Technikum Wien - IT-Security	Projektteammitglied	0650 1234566	cs19m020@technikum-wien.at

1 Projektpläne

1.1 Allgemeine Projektbeschreibung

Ein Thema, welches die Wissenschaft nach wie vor beschäftigt, ist die automatisierte und zeitnahe Erkennung schadhafter Angriffe auf Rechnersysteme. Um erhebliche Schäden zu vermeiden werden für diesen Zweck in Unternehmen oft Intrustion Dection Systeme (IDS) auf Basis von Anomalie-, Signaturerkennung, etc. eingesetzt. Ein relativ neuartiger Ansatz zur Erkennung von Angriffsmustern ist die Verwendung von künstlicher Intelligenz, also Machine Learning-Algorithmen. In einem Vorprojekt wurden öffentliche verfügbare Testdaten genutzt, um neuronale Netzwerke hinsichtlich der Erkennung von Anomalien zu trainieren. Dabei konnten vielversprechende Ergebnisse erzielt werden.

Ziel dieses Projekts ist es ein Dataset zu erstellen, welches für Supervised-Machine Learning zur Erkennung von bösartigem Netzwerkverkehr eingesetzt werden kann. Es sollen dabei verschiedene Angriffsarten, aber auch gutartiger Netzwerkverkehr in diesem Dataset abgebildet sein. Somit ist der Zweck des Projekts einen Beitrag zur automatisierten und verlässlichen Erkennung von schadhaften Angriffen auf Rechnersysteme zu leisten. Um dies zu erreichen, muss ein entsprechender Netzwerkverkehr simuliert, aufgezeichnet und weiterverarbeitet werden. Letztlich wird der erzeugte Datensatz mit dem neuronalen Netz aus dem Vorprojekt getestet und ein Performance-Vergleich durchgeführt.

Die Ergebnisse werden in zwei wissenschaftlichen Arbeiten dokumentiert und dienen als Basis für zukünftige Projekte.

1.2 Projektauftrag

projekthandbuch 001	PROJEKT- AUFTRAG

Projektstartereignis:	**Projektstarttermin:**
• Projekt-Kickoff	• 18.02.2020
Projektendereignis:	**Projektendtermin:**
• Abgabe der zwei wissenschaftlichen Paper und der Projektdokumentation	• 30.06.2020
Projektziele: • Erstellung eines Datensatzes, welcher für Supervised Machine Learning (neuronales Netz) zur Erkennung von bösartigem Netzwerkverkehr eingesetzt werden kann. • Verfassung von zwei wissenschaftlichen Paper zur Beschreibung der Resultate und der Vorgehensweise in diesem Projekt	**Nicht-Projektziele:** • Performance testen mit anderen Modellen/Machine Learning Algorithmen • Unsupervised Learning Ansätze für Intrusion Detection testen • Zusätzliche Paper zu dieser Thematik erstellen

Hauptaufgaben (Projektphasen):
- Detailplanung
- Aufbau der Infrastruktur
- Durchführen und Aufzeichnen von Angriffen
- Feature Extraction, Label-Vergabe
- Performance Vergleich der Datensätze mit Modell (neuronalem Netz) aus Vorjahr
- Durchführen einer Präsentation
- Erstellung wissenschaftlicher Paper

ProjektauftraggeberIn:	**ProjektleiterIn:**
• Dipl.-Ing. Dr. Gerd Holweg	• Sebastian Lipp

Projektteam:
- Bernhard Gally
- Damir Marijanovic
- Boris Stampf
- Maximilian Wech

----------	----------
Vorname Nachname, (ProjektauftraggeberIn)	*Vorname Nachname*, (ProjektleiterIn)

1.3 Projektzieleplan

projekthandbuch 001	PROJEKTZIELE- PLAN
Zielart	**Projektziele**
Ziele	• Erstellung von zwei wissenschaftlichen Paper zur Erläuterung der Ergebnisse und der Vorgehensweise, bis 30.06.2020 • Erstellung eines Proof of Concepts (Durchführung eines Angriffes, entsprechende Aufzeichnung und Weiterverarbeitung) zum Beweis, dass die Projektumsetzung wie geplant funktioniert, bis 01.05.2020 • Erstellung eines Datensatzes, welcher für Supervised-Machine Learning in Form von neuronalen Netzen zur Erkennung von bösartigem Netzwerkverkehr eingesetzt werden kann (= Durchführung, Aufzeichnung und Verarbeitung weiterer Angriffe), bis 01.06.2020 • Performance-Vergleich des neu erstellten Datensatz mit jenem des Vorjahrs unter Verwendung des erstellten Modells, bis 09.06.2020 • Erstellung einer Präsentation zur Erläuterung der Projektinhalte für die weiteren MCS-Studenten und -Lektoren, am 16.06.2020 • Erstellung einer ausführlichen Dokumentation, welche die Arbeitsdurchführung und die gewonnenen Erkenntnisse vollständig enthält (= Projekthandbuch), bis 30.06.2020
Nicht-Ziele	• Nutzung jenes Netzwerkverkehrs, welcher eine Firewall durchläuft • Performance mit anderen Machine Learning-Algorithmen testen (nur Neuronales Netz zulässig) • Verwenden eines Unsupervised Learning Ansatzes zur Intrusion Detection • Zusätzliche Paper zu dieser Thematik verfassen

1.4 Beschreibung Vorprojekt- und Nachprojektphase

projekthandbuch

001

BESCHREIBUNG VORPROJEKT- UND NACHPROJEKTPHASE

1) Beschreibung von Ergebnissen der Vorprojektphase

Das Projekt betreffende Entscheidungen/Ereignisse. Wie ist es zu dem Projekt gekommen?

- Im Vorprojekt wurde auf Basis eines neuronalen Netzes und einem bereits existierenden Datensatz ein Intrusion Detection System aufgebaut
- Dabei konnte gezeigt werden, dass der Einsatz von AI-Algorithmen in diesem Kontext sinnvoll ist
- Im WS19/20 wurde ein Überblick über verschiedene Angriffsarten, Tools, Infrastruktur, Aufzeichnung und Verarbeitung des Netzwerkverkehrs gegeben

Für das Projekt relevante Dokumente (zB „Protokoll mit ...", „Besprechung mit …", Inhalt der Dokumente ist hier nicht gefragt, NUR die Dokumente!)

- SS19: Setup & Infrastructure: A Neural-Network Approach for an Intrusion Detection System
- SS19: A Neural-Network Approach for an Intrusion Detection System
- WS18/19: Introduction to data gathering methods in an AI-supported IDS context
- WS18/19: Survey on recent neural network research and approaches for intrusion detection
- WS19/20: Network packet generation for Artificial Intelligence
- WS19/20: Network Data Collection for Artifical Intelligence

Erfahrungen aus ähnlichen Projekten

- Im Vorprojekt wurden acht verschiedene Angriffsarten und gutartiger Traffic vom neuronalen Netz mit einer Genauigkeit von mindestens 99,85% erreicht.
- Es ist eine hohe Rechenleistung notwendig, um ein neuronales Netz zu betreiben
- Der Netzwerkverkehr wurde mit tcpdump aufgezeichnet, für die Feature Extraction wurde CIC Flow Meter verwendet.

2) Beschreibung von Ergebnissen der Nachprojektphase

Was wird nach dem Projekt passieren (Folgeaktivitäten, -projekte, etc.)?

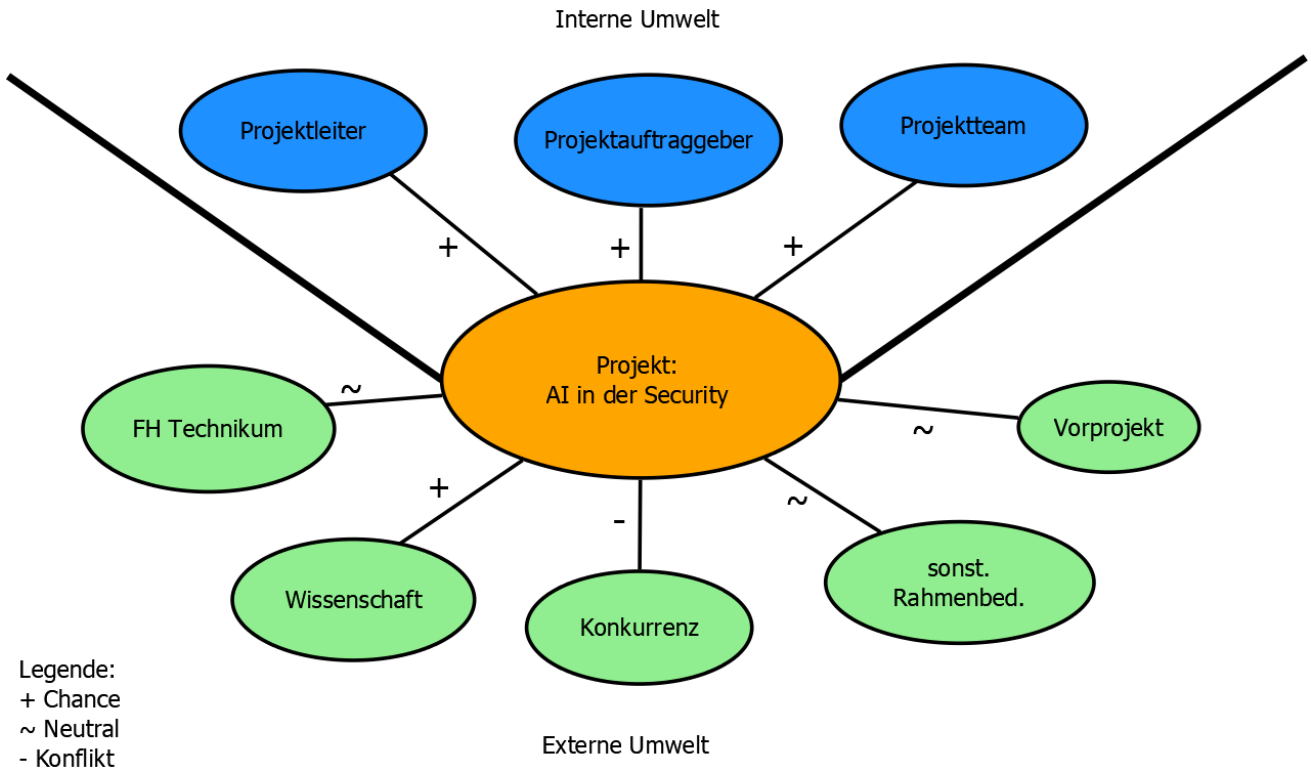
- Einbeziehen weiterer Angriffsarten
- Erweiterung des Datasets, um zusätzliche relevante Features
- Verwendung eines anderen Machine Learning Algorithmus und Durchführen eines Performance Vergleichs

1.5 Projektumwelt-Analyse

projekthandbuch

001

PROJEKTUMWELTEN-GRAPHIK



projekthandbuch

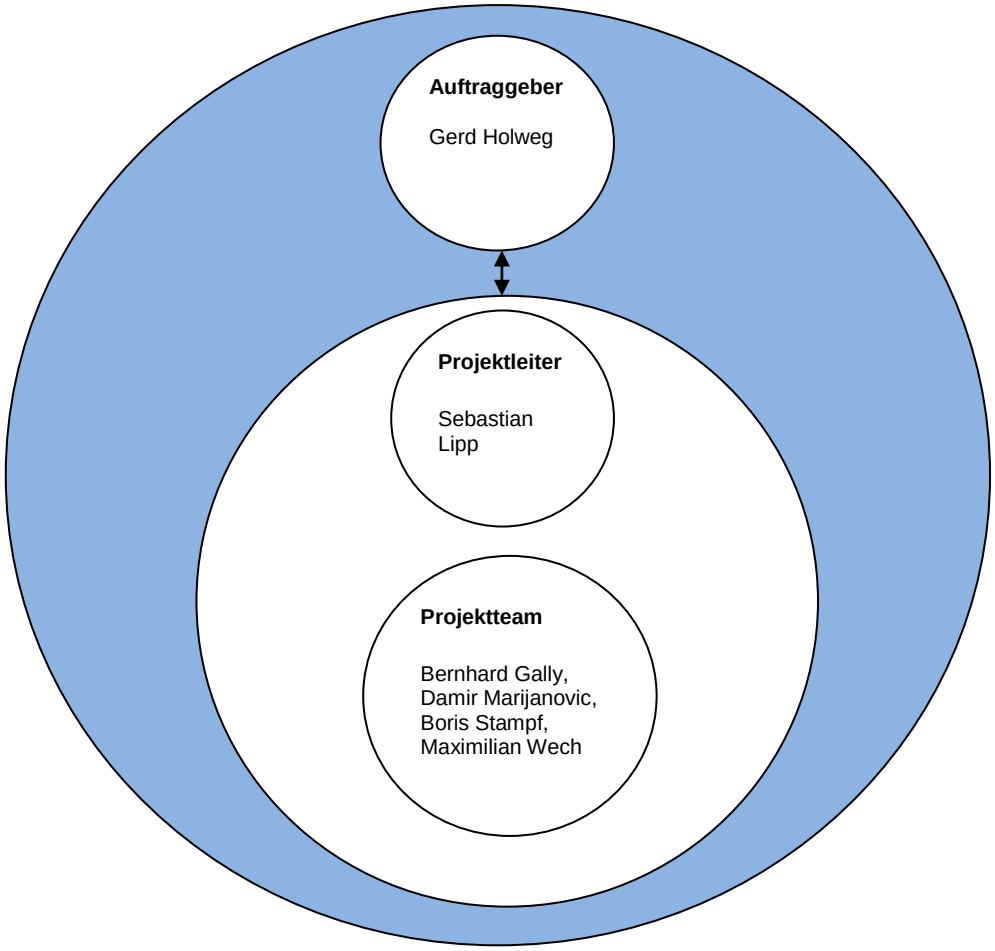
001

PROJEKTUMWELTEN-BEZIEHUNGEN

Umwelten	**Beziehung** (Potential/Konflikt)	**Maßnahmen**	**Who/When**
Projektleiter	Potential • gute Teamleitungsfähigkeit • Spaß an der Arbeit • fachliche Kompetenzen in sehr vielen Bereichen	• Evt. Prämie am Projektende • vollste Unterstützung durch Projektauftraggeber	Sebastian Lipp 03.07.2020

Projektteam	Potential ● Spaß an der Arbeit ● viel Projekterfahrung ● gutes Konfliktmanagement	● Förderung in allen Belangen ● Durchführung von Workshops um noch besseren Zusammenhalt zu erlangen ● eventuell Zusatzleistungen	Bernhard Gally Damir Marijanovic Boris Stampf Maximilian Wech laufend
Projektauftraggeber	Potential ● Hohes Interesse am Projekterfolg ● Kann wichtigen Input liefern	● Laufendes Reporting und Projektcontrolling ● Informieren über Erfolge und Hemmnisse ● Eskalation von Problemen vermeiden ● Miteinbeziehen bei wichtigen Entscheidungen	Dipl.-Ing. Dr. Gerd Holweg laufend
FH Technikum	Neutral ● Hohes Interesse an erfolgreichen Projekten ● Muss Infrastruktur bereitstellen	● Frühes Abklären wie Serverinfrastruktur aufgebaut werden kann (Selbsterstellung / Nutz von Bestehendem)	Sebastian Lipp Anfang März
Wissenschaft	Potential ● Viele Beiträge vorhanden mit ausreichend Information für ein Projekt in diesem Kontext	● Detaillierte Recherche um das benötigte Know-how zu erlangen ● Vergleich unterschiedlicher Literatur und Sammeln der Relevantesten	Bernhard Gally Damir Marijanovic Boris Stampf Maximilian Wech Sebastian Lipp Februar bis März
Konkurrenz	Konflikt ● Rivalität zwischen den Projektteams; jedes will das beste Team sein	● Konsequent und Effizient Arbeiten ● Gute Planung ● Viel Zeit investieren ● Periodischer Vergleich des eigenen Fortschrittes mit der Konkurrenz	Sebastian Lipp laufend
Sonst. Rahmenbed.	Neutral ● evtl. Ausfälle von Teammitglieder ● Zeitmangel ● Hohe Arbeitslast	● Mehrere Teams erstellen ● Aufgaben gut verteilen ● Detaillierte Planung	Sebastian Lipp Februar
Vorprojekt	Neutral ● Viele wichtige Erkenntnisse ● Diese müssen entsprechend genützt werden ● Dokumentation mangelhaft	● Nachvollziehen was im Vorprojekt genau geleistet wurde ● Die Erfahrungen nutzen ● Auf dieser Basis aufbauen	Bernhard Gally Damir Marijanovic Boris Stampf Maximilian Wech Sebastian Lipp laufend

1.6 Projektorganigramm



projekthandbuch

001

PROJEKT-ORGANISATION

Projektrolle	Aufgabenbereiche/Skills	Name
ProjektauftraggeberIn	Gibt die Rahmenbedingungen vor, Nimmt Projekt ab	Dipl.-Ing. Dr. Gerd Holweg
ProjektleiterIn	Koordination, Leitung der Meetings	Sebastian Lipp
Projektteam-mitgliederInnen	Teilnahme an Meetings, Erfüllung der Arbeitspakete	Bernhard Gally, Damir Marijanovic, Boris Stampf, Maximilian Wech

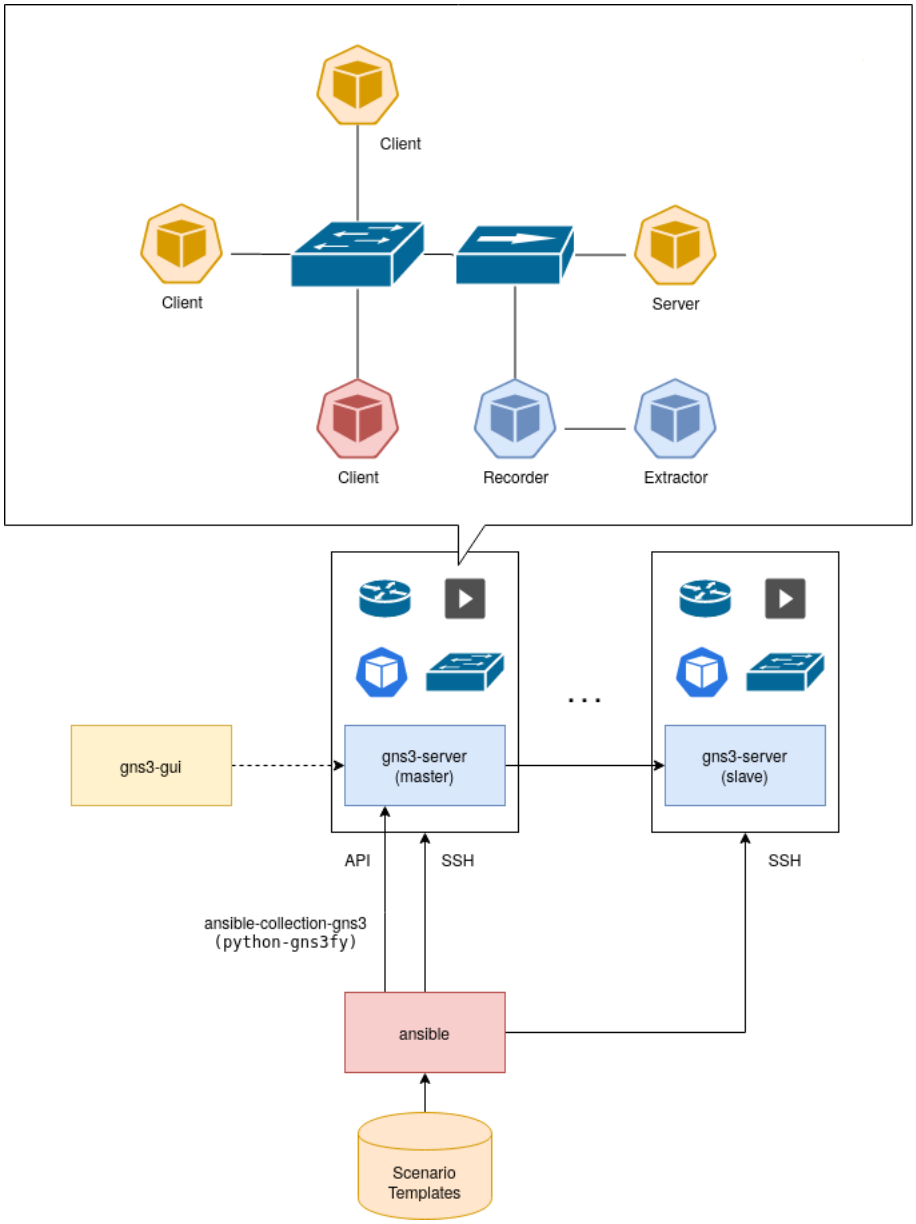
1.7 Technisches Konzept

Um den Netzwerkverkehr zu erzeugen wird der Netzwerksimulator GNS3 verwendet. Dieser verfügt über eine API, mit welcher es möglich ist Netzwerktopologien (für Angriffe und normalen Netzwerkverkehr) zu erstellen. Darüber hinaus können Container und virtuelle Maschinen in die Simulation integriert werden, wodurch die Weiterleitung des Netzwerkverkehrs an einen Recorder (zum Aufzeichnen des Verkehrs) und einen Extractor (zum Extrahieren relevanter Features) bewerkstelligt werden kann. Um den Netzwerksimulator in einer virtuellen und skalierbaren Umgebung zu betreiben wird Vagrant verwendet. Für das Deployment kommen Ansible Playbooks zum Einsatz, welche zum Definieren des Host-Setups und der verschiedenen Netzwerktopologien dienen. Der Simulations-Workflow beginnt somit bei der Eingabe des gewünschten Netzwerkszenarios. Daraufhin erfolgt das Deployment (von Host-System, Netzwerktopologie, Extractor, Recorder).

Konkret wird Folgendes durchgeführt:

- Aufbau mehrerer GNS3 Server mittels Ansible Playbooks
- Bereitstellung von GNS3 Netzwerken mittels dem gns3fy Ansible Modul über die GNS3 API. Ein GNS3 Netzwerk beinhaltet eine Netzwerktopologie (Angriff und normaler Netzwerkverkehr), sowie Recorder und Extractor.
- Verschiedene Szenarien können bereitgestellt und getestet werden mittels Ansible Playbooks (samt Parameter zum Extrahieren von Features).

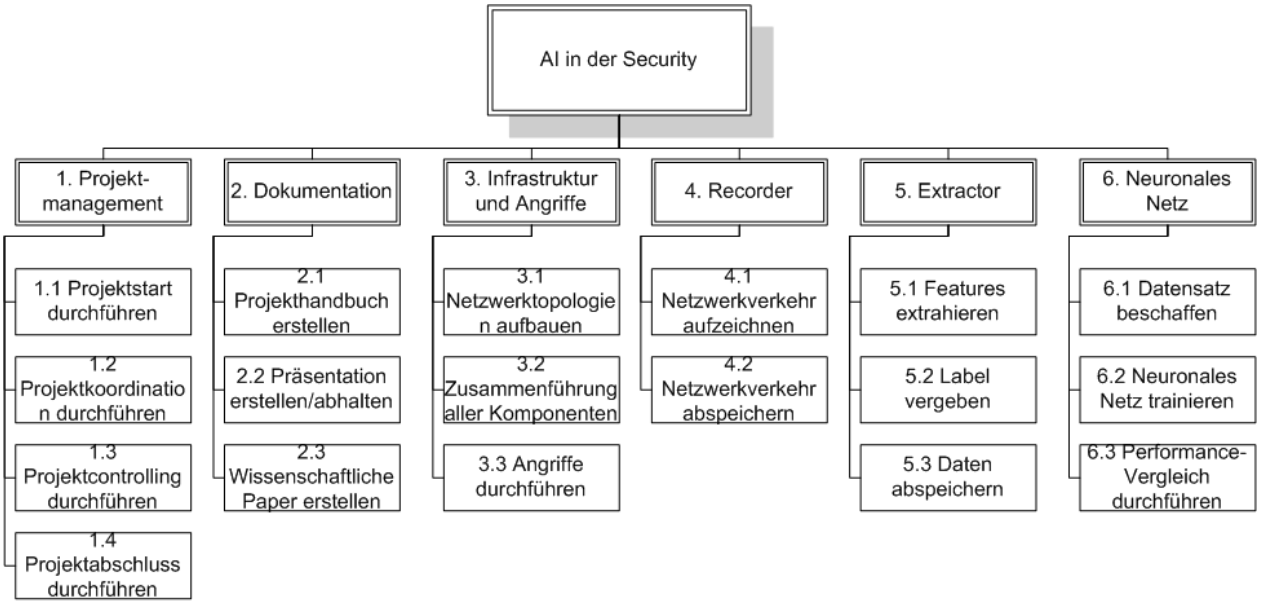
Die folgende Abbildung zeigt eine grafische Darstellung des technischen Konzepts:



Beschreibung:

Ziel ist es eine erweiterbare Umgebung zu schaffen, die mittels Konfigurationsskripts möglichst automatisiert gestartet und verwaltet werden kann. Kernelemente sind die GNS3-Server. Diese simulieren jeweils ein GNS3-Netzwerk, welches aus einer Netzwerktopologie (Angriff und gutartiger Netzwerkverkehr über Client, Server, Router, Hub, etc.), sowie Recorder und Extractor (zum Aufzeichnen und Extrahieren der Daten) besteht. Skalierbarkeit wird dadurch erreicht, dass mehrere GNS3-Server zum Einsatz kommen und somit verschiedene Szenarien simuliert werden. Der Aufbau der GNS-3 Server erfolgt über Ansible-Playbooks, die Bereitstellung von GNS3-Netzwerken mittels dem gns3fy Ansible Modul.

1.8 Projektstrukturplan



Der Projektmanagementblock trägt insgesamt dazu bei, einen zeitgerechten und erfolgreichen Projektabschluss zu bewerkstelligen. Es soll der laufend der Fortschritt gemessen und bei Bedarf steuernd eingegriffen werden.

Die Dokumentation besteht aus mehreren Komponenten. Es soll ein ausführliches und vollständiges Projekthandbuch erstellt werden, welches eine detaillierte Projektplanung enthält. Die Ergebnisse des Projekts werden im Rahmen einer Präsentation vorgeführt und in zwei wissenschaftlichen Papers erläutert.

Der Infrastruktur- und Angriffsteil wird mit einem Netzwerksimulator simuliert und beinhaltet den Aufbau einer entsprechenden Netzwerktopologie, bei welcher mehrere Komponenten (wie Clients, Server, etc.) zusammengeschalten werden. Dabei erfolgt eine Durchführung verschiedener Angriffsarten (z.B. SSH Brute Force).

Die nächsten zwei Bereiche beschäftigen sich mit dem Aufzeichnen des Netzwerkverkehrs (mittels tcpdump), der Extrahierung relevanter Features (mittels CIC-Flowmeter) und der Vergabe von Labels.

Der letzte Teil inkludiert die Thematik des neuronalen Netzes. Dabei soll ein Performance-Vergleich mit dem im Vorprojekt erzeugten Modell durchgeführt und die Eignung unterschiedlicher Datensätze geprüft werden.

1.9 Arbeitspaket-Spezifikationen

projekthandbuch 001	ARBEITSPAKET-SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 1.1 Projektstart durchführen	**AP-Inhalt** Kickoff-Meeting • Projektinhalt/-ziele festlegen (→ Projektauftrag) • Rahmenbedingungen ermitteln und niederschreiben • Projektvorgehensmodell auswählen • Projektorganisation und –kommunikation regeln
	AP-Nicht-Inhalte • Mit der Projektplanung beginnen • Abarbeiten von Arbeitspaketen
	AP-Ergebnisse • Klar definierte Ziele • Motivation geschaffen • Projektmitglieder werden auf denselben Informationsstand gebracht • Zusammenarbeit geregelt
	AP-Leistungsfortschrittsmessung • Kickoff-Meeting abgehalten / nicht abgehalten • Am Ende des Meetings überprüfen, ob Projektmitglieder alles verstanden haben

projekthandbuch 001	ARBEITSPAKET-SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 1.2 Projektcontrolling durchführen	**AP-Inhalt** • Sicherstellen, dass Projektziele erreicht werden • Projektfortschritt messen • Planabweichungen erkennen (z.B. Soll/Ist Vergleich) • Gegebenenfalls steuernde Maßnahmen einleiten
	AP-Nicht-Inhalte • Controllingverfahren nicht explizit festlegen • Nichtumsetzbare Vorgaben an Projektmitglieder erteilen • Datenbeschaffung vernachlässigen
	AP-Ergebnisse • Abweichungen vom Plan erkannt • Projektfortschritt ermittelt • Steuernde Maßnahmen rechtzeitig eingeleitet
	AP-Leistungsfortschrittsmessung • Soll/Ist Vergleich • Meilensteintrendanalyse • Kennzahlen

projekthandbuch 001	ARBEITSPAKET-SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 1.3 Projektkoordination durchführen	**AP-Inhalt** • Sicherung des Projektfortschrittes • Konflikte lösen • Risikomanagement durchführen • Technische und personelle Ressourcen steuern
	AP-Nicht-Inhalte • Maßnahmen mangelhaft kommunizieren • Unklare Verantwortungsbereiche definieren • Arbeitsprozesse nicht regelmäßig überprüfen
	AP-Ergebnisse • Kommunikation im Projekt festgelegt • Verantwortungsbereiche eindeutig festgelegt • Optimale Ressourcenverteilung
	AP-Leistungsfortschrittsmessung • Überprüfen, ob Deadlines eingehalten werden • Berichte

projekthandbuch 001	ARBEITSPAKET-SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 1.4 Projektabschluss durchführen	**AP-Inhalt** • Überprüfen, ob alle Ziele erreicht wurden • Wissen und Erfahrungen dokumentieren • Feedbackgespräche • Abschlussbericht erstellen • Projektabschlussfeier
	AP-Nicht-Inhalte • Auf Abschlussbericht verzichten • Verbesserungspotentiale nicht definieren
	AP-Ergebnisse • Projektnachbereitung durchgeführt • Lessons Learned dokumentiert • Projektdokumentation vervollständigt
	AP-Leistungsfortschrittsmessung Ermitteln, ob • Dokumentation vervollständigt ist • alle Ziele erreicht sind

projekthandbuch 001	ARBEITSPAKET- SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 2.1 Projekthandbuch erstellen	**AP-Inhalt** • Aktualisieren der Inhalte aus dem WS1920 • Projektplanung SS20 erstellen • Dokumentation der Projektstruktur und des Projektfortschrittes • Management
	AP-Nicht-Inhalte • Überschneidungen mit den wissenschaftlichen Paper erzeugen
	AP-Ergebnisse • PDF-Dokument, welches die genannten Inhalte vollständig abdeckt und zeitgerecht abgegeben wird
	AP-Leistungsfortschrittsmessung • Laufende Überprüfung, wie viele Kapitel mit ansprechender Qualität fertiggestellt wurden

projekthandbuch 001	ARBEITSPAKET- SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 2.2 Präsentation erstellen / abhalten	**AP-Inhalt** • Kontext des Projekts, sowie Ergebnisse und die Vorgangsweise dokumentieren • Erstellen einer PowerPoint-Präsentation, welche die genannten Aspekte beinhaltet • Präsentation vor den MCS-Studenten (2.Semester) und den Lektoren abhalten
	AP-Nicht-Inhalte • Zu sehr ins Detail geraten • Eine Live-Demo praktizieren
	AP-Ergebnisse • Erfolgreich abgehaltene Präsentation, welche die im Projekt geleistete Arbeit gut wiedergegeben hat
	AP-Leistungsfortschrittsmessung • Laufende Überprüfung, wie viele Slides bereits erstellt wurden

projekthandbuch 001	ARBEITSPAKET- SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 2.3 Wissenschaftliche Paper erstellen	**AP-Inhalt** • Dokumentation der Projektergebnisse • Beschreibung wie die Ergebnisse erreicht werden konnten (was wurde konkret getan) • Diskussion der Arbeit • Ausblick auf zukünftige Arbeiten/Projekte geben
	AP-Nicht-Inhalte • Beschreibung des Projektmanagements
	AP-Ergebnisse • Zwei PDF-Dokumente, welche die angeführten Inhalte abdecken
	AP-Leistungsfortschrittsmessung • Laufende Überprüfung der Seitenanzahl

projekthandbuch 001	ARBEITSPAKET- SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 3.1 Netzwerktopologien aufbauen	**AP-Inhalt** • Verschiedene Netzerktopologien planen und aufbauen, welche zur Simulation von Angriffen und gutartigem Netzwerkverkehr dienen • Konkret: GNS3-Netzwerke bestehend aus Clients, Server, Router, Hubs, etc. aufbauen • Angriffstools zur Durchführung von Angriffen einsetzen
	AP-Nicht-Inhalte • Netzwerktopologien in anderen Simulatoren außer GNS3 aufbauen
	AP-Ergebnisse • Fertige Ansible-Konfigurationsskripts mit welchen die jeweiligen Netzwerktopologien automatisiert aufgebaut werden können
	AP-Leistungsfortschrittsmessung • Laufende Überprüfung der Anzahl bereits fertiggestellter Netzwerktopologien

projekthandbuch 001	ARBEITSPAKET- SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 3.2 Zusammenführung aller Komponenten	**AP-Inhalt** • Zusammenführung von Netzwerktopologie, Extractor und Recorder • Erstellung notwendiger Konfigurationsskripts für diesen Zweck
	AP-Nicht-Inhalte • Durchführung von Angriffen
	AP-Ergebnisse • Netzwerkverkehr findet nicht nur innerhalb der Topologie statt, sondern wird auch an Recorder und Extractor weitergeleitet • Fertige Konfigurationsskripts, welche die Komponenten zusammenführen
	AP-Leistungsfortschrittsmessung • Laufende Überprüfung, wie viele Netzwerktopologien bereits mit Recorder und Extractor zusammengeschalten sind

projekthandbuch 001	ARBEITSPAKET- SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 3.3 Angriffe durchführen	**AP-Inhalt** • Durchführung von Angriffen (jeweils einzeln) durch den Einsatz entsprechender Tools • Erzeugung von Skripts zur automatisierten Durchführung
	AP-Nicht-Inhalte • Angriffe durchführen oder Angriffstools verwenden, welche nicht vorher nicht entsprechend geprüft und geplant wurden
	AP-Ergebnisse • Vollständige Durchführung aller geplanten Angriffe gelungen
	AP-Leistungsfortschrittsmessung • Anzahl erfolgreich durchgeführter Angriffe

projekthandbuch 001	ARBEITSPAKET- SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 4.1 Netzwerkverkehr aufzeichnen	**AP-Inhalt** • Aufbau eines Docker Images • Netzwerkverkehr wird an Recorder weitergeleitet und aufgezeichnet • Einsatz einer entsprechenden Tools (tcpdump)
	AP-Nicht-Inhalte • Einen anderes Recordertool als tcpdump zum Aufzeichnen des Netzwerkverkehrs verwenden • Bereits mit der Extrahierung von Features beginnen
	AP-Ergebnisse • Dockerfile, welches alle notwendigen Schritte zur Erstellung des Recorders beinhaltet
	AP-Leistungsfortschrittsmessung • Anzahl der erfolgreich stattgefunden Aufzeichnungsvorgänge

projekthandbuch 001	ARBEITSPAKET- SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 4.2 Netzwerkverkehr abspeichern	**AP-Inhalt** • Tatsächliche Abspeicherung des aufgezeichneten Netzwerkverkehrs in PCAP Files • Jeder Aufzeichnungsvorgang wird einzeln in ein PCAP File abgespeichert
	AP-Nicht-Inhalte • Mehrere PCAP-Files pro Aufzeichnungsvorgang erstellen
	AP-Ergebnisse • PCAP-Files, welche den aufgezeichneten Netzwerkverkehr abbilden
	AP-Leistungsfortschrittsmessung • Anzahl fertiggestellter PCAP-Files

projekthandbuch 001	ARBEITSPAKET- SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 5.1 Features extrahieren	**AP-Inhalt** • Es wird ein Docker Image für den Extractor erstellt • Die zuvor erstellten PCAP-Files werden in den CIC-Flowmeter geladen • Definierte Features werden aus dem Datensatz extrahiert
	AP-Nicht-Inhalte • Zusätzliche Features extrahieren
	AP-Ergebnisse • Fertig extrahierte Features, welche für das Trainieren des Modells verwendet werden
	AP-Leistungsfortschrittsmessung • Anzahl erfolgreich durchgeführter Feature-Extraktionsvorgänge

projekthandbuch 001	ARBEITSPAKET- SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 5.2 Label vergeben	**AP-Inhalt** • Es wird pro Datenpaket ein Label vergeben, ob es sich beim betrachteten Datenpaket um gutartigen oder bösartigen Netzwerkverkehr (wenn bösartig, welche Angriffsart) handelt
	AP-Nicht-Inhalte • Nicht vorab definierte Labels vergeben • Unkorrekte Vergabe von Label
	AP-Ergebnisse • Gelabelter Datensatz als Basis für Supervised-Machine Learning
	AP-Leistungsfortschrittsmessung • Laufende Überprüfung, wie viel des Datensatzes bereits erfolgreich gelabelt wurde

projekthandbuch 001	ARBEITSPAKET- SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 5.3 Daten abspeichern	**AP-Inhalt** • Erzeugung eines finalen Datensatzes für Supervised-Machine Learning • Zusammenführung von Features und Labels
	AP-Nicht-Inhalte • Daten in einer Datenbank abspeichern
	AP-Ergebnisse • CSV-File, welches den gesamten Netzwerkverkehr abbildet (nur extrahierte Features und entsprechende Labels)
	AP-Leistungsfortschrittsmessung • CSV-File fertig / nicht fertig

projekthandbuch 001	ARBEITSPAKET- SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 6.1 Datensatz beschaffen	**AP-Inhalt** • Es wird das csv-File in eine passende Entwicklungsumgebung geladen
	AP-Nicht-Inhalte • Text
	AP-Ergebnisse • Text
	AP-Leistungsfortschrittsmessung • Text

projekthandbuch 001	ARBEITSPAKET-SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 6.2 Neuronales Netz trainieren	**AP-Inhalt** • Das neuronale Netz (fertiges Modell) aus dem Vorprojekt muss beschaffen werden • Trainieren des Modells mit dem in diesem Projekt erstellten Datensatz
	AP-Nicht-Inhalte • Andere Modelle oder Machine Learning Algorithmen verwenden
	AP-Ergebnisse • Fertig trainiertes Modell
	AP-Leistungsfortschrittsmessung • Modell fertig trainiert / nicht fertig trainiert

projekthandbuch 001	ARBEITSPAKET-SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 6.3 Performance-Vergleich durchführen	**AP-Inhalt** • Es wird ein Performance-Vergleich auf Basis der Accuracy durchgeführt • Vergleich Ergebnis Vorprojekt / aktuelles Projekt • Analyse des Ergebnisses
	AP-Nicht-Inhalte • Ergebnis durch Boosting zu verbessern
	AP-Ergebnisse • Erkenntnis, welcher Datensatz besser für diesen Einsatzzweck geeignet ist
	AP-Leistungsfortschrittsmessung • Analyse abgeschlossen / nicht abgeschlossen

1.10 Verantwortlichkeiten

Folgende Tabelle zeigt eine vorübergehende Einteilung der Arbeitspakete. Es ist an dieser Stelle festzuhalten, dass es sich hier nicht um eine finale Version handelt; es kann daher durchaus noch zu Änderungen kommen.

PSP-Überbereich	**PSP-Unterbereich**	**Verantwortliche Person(en)**
1. Projektmanagement		
	1.1 Projektstart durchführen	Gally, Lipp, Marijanovic, Stampf, Wech
	1.2 Projektcontrolling durchführen	Lipp, Wech
	1.3 Projektkoordination durchführen	Lipp, Wech
	1.4 Projektabschluss durchführen	Gally, Lipp, Marijanovic, Stampf, Wech
2. Dokumentation		
	2.1 Projekthandbuch erstellen	Wech
	2.2 Präsentation erstellen / abhalten	Gally, Lipp, Marijanovic, Stampf, Wech
	2.3 Wissenschaftliche Paper erstellen	Gally, Lipp, Marijanovic, Stampf, Wech
3. Infrastruktur und Angriffe		
	3.1 Netzwerktopologien aufbauen	Gally, Lipp, tbd
	3.2 Zusammenführung aller Komponenten	Lipp, tbd
	3.3 Angriffe durchführen	Gally, Lipp, tbd
4. Recorder		
	4.1 Netzwerkverkehr aufzeichnen	Marijanovic
	4.2 Netzwerkverkehr abspeichern	Marijanovic
5. Extractor		
	5.1 Features extrahieren	Stampf
	5.2 Label vergeben	Stampf
	5.3 Daten abspeichern	Stampf
6. Neuronales Netz		
	6.1 Datensatz beschaffen	Wech
	6.2 Neuronales Netz trainieren	Wech, tbd
	6.3 Performance-Vergleich durchführen	Wech, tbd

1.11 Projektmeilensteinplan

projekthandbuch 001	PROJEKT- MEILENSTEINPLAN		
Meilenstein	**Basis-termine**	**Aktuelle Plantermine**	**Ist Termine**
Projektkickoff durchgeführt	18.02.2020	18.02.2020	18.02.2020
Projektplanung erstellt	03.04.2020	03.04.2020	03.04.2020
Proof of Concept erstellt • Erste Netzwerktoplogie umgesetzt • Eine Angriffsart wurde durchgeführt • Anfallender Netzwerkverkehr aufgezeichnet • Entsprechende Features extrahiert • Labels vergeben	01.05.2020	01.05.2020	
Datensatz fertiggestellt • Wie bei Proof Of Concept; weitere Szenarien durchgeführt	01.06.2020	01.06.2020	
Neuronales Netz – Performance Vergleich durchgeführt • Erzeugter Datensatz wird mit den neuronalen Netz aus dem Vorprojekt getestet • Vergleich der Performance	09.06.2020	09.06.2020	
Projektpräsentation durchgeführt • Präsentation wesentlicher Projektergebnisse und der Vorgangsweise durchgeführt	16.06.2020	16.06.2020	
Projektabnahme durchgeführt • Wissenschaftliche Paper erstellt • Wesentliche Projektmaterialien (Source Code, Datensatz, etc.) und Projekthandbuch an den Projektauftraggeber übergeben	30.06.2020	30.06.2020	

1.12 Projektzeitplan

Grundlegende Information:

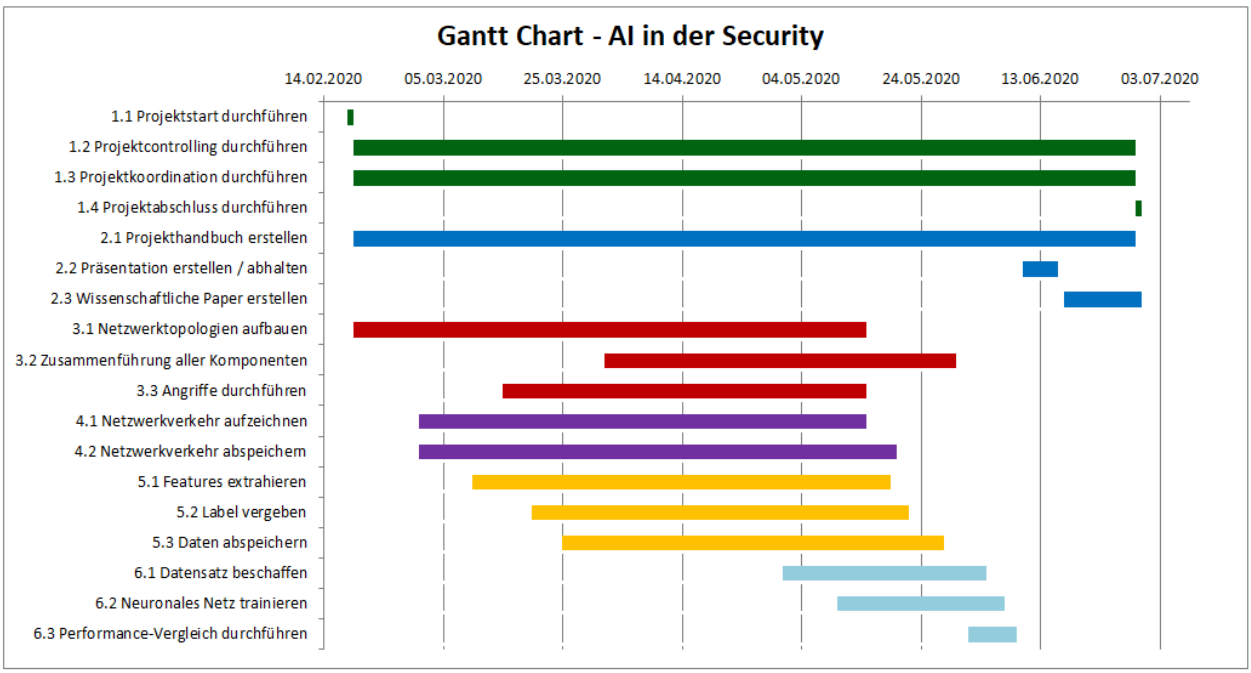
Semester	ECTS	ECTS in h	FH-Präsenzzeit in h	Anzahl Mitglieder	Gesamtaufwand aller Mitglieder in h
SS 20	4,5	112,5	22,5	5	562,5

Geplante Zeitaufteilung im SS20:

Aufgabe	Zeitdauer in h
LV-Anwesenheit	21 * 5 = 105
Planung	8 * 5 = 40
Einarbeiten in GNS3/notwendige SW	4 * 5 = 20
Netzwerktopologie(n) inkl. Angriffe aufbauen	50
Recorder erstellen	40
Extraktor erstellen	40
Zusammenführung der Komponenten	50
Performance-Vergleich NN	27,5
Abschlusspräsentation (+Vorbereitung)	6 * 5 = 30
Projektdokumentation und -management	60
Erstellen der wissenschaftlichen Paper	20 * 5 = 100

1.13 Projektbalkenplan

Arbeitspaket-Name	Start	Ende	Dauer (Tage)
1.1 Projektstart durchführen	18.02.2020	19.02.2020	1
1.2 Projektcontrolling durchführen	19.02.2020	29.06.2020	131
1.3 Projektkoordination durchführen	19.02.2020	29.06.2020	131
1.4 Projektabschluss durchführen	29.06.2020	30.06.2020	1
2.1 Projekthandbuch erstellen	19.02.2020	29.06.2020	131
2.2 Präsentation erstellen / abhalten	10.06.2020	16.06.2020	6
2.3 Wissenschaftliche Paper erstellen	17.06.2020	29.06.2020	13
3.1 Netzwerktopologien aufbauen	19.02.2020	15.05.2020	86
3.2 Zusammenführung aller Komponenten	01.04.2020	30.05.2020	59
3.3 Angriffe durchführen	15.03.2020	15.05.2020	61
4.1 Netzwerkverkehr aufzeichnen	01.03.2020	15.05.2020	75
4.2 Netzwerkverkehr abspeichern	01.03.2020	20.05.2020	80
5.1 Features extrahieren	10.03.2020	20.05.2020	70
5.2 Label vergeben	20.03.2020	22.05.2020	63
5.3 Daten abspeichern	25.03.2020	28.05.2020	64
6.1 Datensatz beschaffen	01.05.2020	04.06.2020	34
6.2 Neuronales Netz trainieren	10.05.2020	07.06.2020	28
6.3 Performance-Vergleich durchführen	01.06.2020	09.06.2020	8



1.14 Projektkommunikationsstrukturen

projekthandbuch 001	PROJEKT- KOMMUNIKATION			
Bezeichnung	**Ziele, Inhalte**	**Teilnehmer**	**Termine**	**Ort**
Management-Sitzung	• Diskussion Projektstatus, Abweichungen im Projekt • Entscheidungsfindung auf Basis der Projektcontrolling-Sitzung • Freigabe Projektfortschrittsbericht	Projektauftraggeber, Projektleiter	Monatlich, am ersten Mittwoch	Microsoft Teams
Projektcontrolling-Sitzung	• Projektstatus • Controlling Leistungsfortschritt, Termine und Ressourcen • Controlling der Umweltbeziehungen • Soziales Projektcontrolling • Diskussion übergeordneter Problemstellungen • Entscheidungsaufbereitung für Projektauftraggeber-Sitzung	ProjektleiterIn, Projektteam, Projektcoach	Wöchentlich, am Dienstag	Microsoft Teams
Projektteambesprechung	• Besprechung aktueller Probleme • Besprechung weitere Vorgehensweise • Aufgabeneinteilung • Konfliktlösung	Projektleiter, Projektteam	Wöchentlich, am Montag	Microsoft Teams

1.15 Projektrisikoanalyse

PROJEKT-RISIKOANALYSE							
Risiko-beschreibung, Ursache	Priorität	Risiko-kosten	Eintritts-wahrschein-lichkeit	Risiko-budget	Ver-zögerung	Präventive und korrektive Maßnahmen	Risiko-minimierungs-kosten
(Text)	*(Auswahl)*	*(Euro)*	*(Prozent)*	*(Euro)*	*(Wochen)*	*(Text)*	*(Euro)*
Ausfall eines Teammitgliedes	m	/	40	/	2	Arbeit gut aufteilen und rechtzeitig reagieren	/
Netzwerksimulator stellt sich als ungeeignet dar	m	/	10	/	2	Rechtzeitig ausprobieren und versuche Proof of Concept umzusetzen	/
Schwierigkeiten beim Aufzeichnen des Traffics	l-m	/	15	/	1	Anderes Tool verwenden, Frühzeitig Testen	/
Tools zum Durchführen der Angriffe ungeeignet	m	/	25	/	3	Weitere Tools recherchieren und ausprobieren	/
Probleme beim Zusammenführen von Recorder, Extraktor, Topologie entstehen	m	/	15	/	2	Kontrolle der Durchführung, Zeitpolster einplanen	/
Zu komplizierte Netzwerktopologien geplant	m	/	25	/	2	Review durch andere Kollegen, Schnelle Reaktion	/
Finden aussagekräftiger Features schwierig	l	/	15	/	1	Ausprobieren und Testen weiterer Features	/
Source Code aus dem Vorprojekt nicht lauffähig	l	/	10	/	1	Debuggen und versuchen das Problem rechtzeitig zu lösen	/
Anforderungen verändern sich erheblich	h	/	3	/	5	Regelmäßiges Feedback des Projektauftraggebers einholen	/
Meilensteine können nicht eingehalten werden	l-m	/	20	/	2-3	Regelmäßige Fortschrittskontrolle	/

1.16 Projektdokumentation

Bereich	Beschreibung
Ablage	Die im Zuge des Projekts erstellten Dokumente müssen am Projektserver der FH Technikum Wien abgespeichert werden. Zusätzlich erfolgt eine Versionsverwaltung mittels git.
Zugriffs-berechtigung	Auf die entstehenden Dateien dürfen nur der Projektauftraggeber, der Projektleiter, sowie die Projektteammitglieder Lese- und Schreibzugriff haben.
Namenskonvention	Die Benennung der im Laufe des Projekts entstehenden Dateien muss klar und eindeutig erfolgen. Anhand des Dateinamen soll der Ersteller bzw. der Titel (z.B. Projekthandbuch) des Dokuments, ersichtlich sein.
Spielregeln	Die durchgeführten Arbeiten beziehungsweise die gewonnen Erkenntnisse müssen zeitnah und verständlich dokumentiert werden.