

Projekthandbuch

AI in der Security

1

Version 1.0
Projektleiter/in: Sebastian Lipp
Datum: 28.02.2020

Inhalt

| | | |
|----------|---|----------|
| 1 | Projektpläne | 5 |
| 1.1 | Allgemeine Projektbeschreibung | 5 |
| 1.2 | Projektauftrag | 6 |
| 1.3 | Projektzieleplan | 7 |
| 1.4 | Beschreibung Vorprojekt- und Nachprojektphase | 8 |
| 1.5 | Projektumwelt-Analyse..... | 9 |
| 1.6 | Projektorganigramm..... | 11 |
| 1.7 | Projektstrukturplan..... | 12 |
| 1.8 | Arbeitspaket-Spezifikationen | 13 |
| 1.9 | Projektmeilensteinplan | 22 |
| 1.10 | Projektzeitplan..... | 23 |
| 1.11 | Projektbalkenplan..... | 24 |
| 1.12 | Projektkommunikationsstrukturen..... | 25 |
| 1.13 | Projektrisikooanalyse..... | 26 |
| 1.14 | Projektdokumentation | 27 |

Änderungsverzeichnis

| Versionsnummer | Datum | Änderung | Ersteller |
|----------------|------------|--|-----------------|
| 0.1 | 14.01.2020 | Allgemeine Projektbeschreibung | Wech Maximilian |
| 0.2 | 17.01.2020 | Vorlage anpassen, Ansprechpartner, Beschreibung Vorprojekt und Nachprojektphase, Projektorganisation, Projektkommunikation, Projektdokumentation | Wech Maximilian |
| 0.3 | 23.01.2020 | Projektauftrag, Projektzieleplan, Projektumweltanalyse, Projektrisikoplan | Wech Maximilian |
| 0.4 | 30.01.2020 | Projektstrukturplan | Wech Maximilian |
| 0.5 | 14.02.2020 | Arbeitspaket-Spezifikationen | Wech Maximilian |
| 0.6 | 15.02.2020 | Projektzeitplan | Wech Maximilian |
| 0.7 | 16.02.2020 | Projektbalkenplan | Wech Maximilian |
| 1.0 | 25.02.2020 | Prüfung abgeschlossen -> Finale Version | 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 Intrusion Detection Systeme (IDS) auf Basis von Anomalie-, Signatuererkennung, 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. Im Rahmen dieses Projekts ist es nicht das Ziel einen bereits existierenden Testdatensatz zu verwenden, sondern eigenständig einen zu erzeugen. Das Projekt ist in zwei Teile aufgeteilt:

Im ersten Teil (Wintersemester 19/20) soll ein umfangreicher Überblick über die Thematik geschaffen werden. Dazu wird eine Literaturrecherche durchgeführt, um folgende Paper zu erstellen

- Paper 1: Identifizierung von Angriffsarten, Aufbau der Infrastruktur, Generierung von Netzwerkpaketen
- Paper 2: Aufzeichnung der Angriffe, Aufbereitung der Daten für Machine Learning-Algorithmen

Im zweiten Teil des Projektes (Sommersemester 20) findet die praktische Umsetzung statt. Es erfolgt der Aufbau einer geeigneten Infrastruktur und die Konzeption der weiteren Schritte. Anschließend findet die Durchführung der Angriffe statt. Dabei ist es notwendig, den Netzwerkverkehr entsprechend aufzuzeichnen. Aufbauend darauf, soll ein gelabelter Testdatensatz mit entsprechender Kategorisierung der Datenpakete erzeugt werden. Letztlich soll auf Basis dieser Daten ein neuronales Netzwerk trainiert und die Performance mit den Ergebnissen aus dem Vorprojekt verglichen werden. Die Ergebnisse, sowie die praktische Durchführung sind ebenfalls in zwei wissenschaftlichen Arbeiten zu dokumentieren.

1.2 Projektauftrag

| | | | |
|---|--|--|--|
| projekthandbuch 001 | | PROJEKT- AUFTRAG | |
| Projektstartereignis: <ul style="list-style-type: none"> Projekt-Kickoff | | Projektstarttermin: <ul style="list-style-type: none"> 03.12.2019 Projekt ist in zwei Teile aufgeteilt: Wintersemester 3.12.2019-31.01.2020 Sommersemester 18.02.2020-03.07.2020 | |
| Projektendereignis: <ul style="list-style-type: none"> Präsentation der Projektergebnisse | | Projektendtermin: <ul style="list-style-type: none"> 03.07.2020 | |
| Projektziele: <ul style="list-style-type: none"> Erstellung wissenschaftlicher Paper zum Einstieg in das Themengebiet und Beschreibung der praktischen Umsetzung Entwerfen eines gelabelten Datensatzes, der verschiedene Angriffsarten, aber auch gutartigen Netzwerktraffics enthält Aufbau einer Serverinfrastruktur | | Nicht-Projektziele: <ul style="list-style-type: none"> Performance mit anderen Machine Learning Algorithmen als Neuronales Netz testen Unsupervised Learning Ansätze für Intrusion Detection ausprobieren Zusätzliche Paper zu dieser Thematik erstellen | |
| Hauptaufgaben (Projektphasen): <ul style="list-style-type: none"> Erstellung wissenschaftlicher Paper Detailplanung Aufbau der Serverinfrastruktur Durchführen und Aufzeichnen von Angriffen Aufbereitung des Datasets (Feature Extraction) Vergleich der Ergebnisse des neuronalen Netzes (Vorjahr/aktuelles Projekt) | | | |
| ProjektauftraggeberIn: <ul style="list-style-type: none"> Dipl.-Ing. Dr. Gerd Holweg | | ProjektleiterIn: <ul style="list-style-type: none"> Sebastian Lipp | |
| Projektteam: <ul style="list-style-type: none"> Bernhard Gally Damir Marijanovic Boris Stampf Maximilian Wech | | | |
| Vorname Nachname, (ProjektauftraggeberIn) | | Vorname Nachname, (ProjektleiterIn) | |

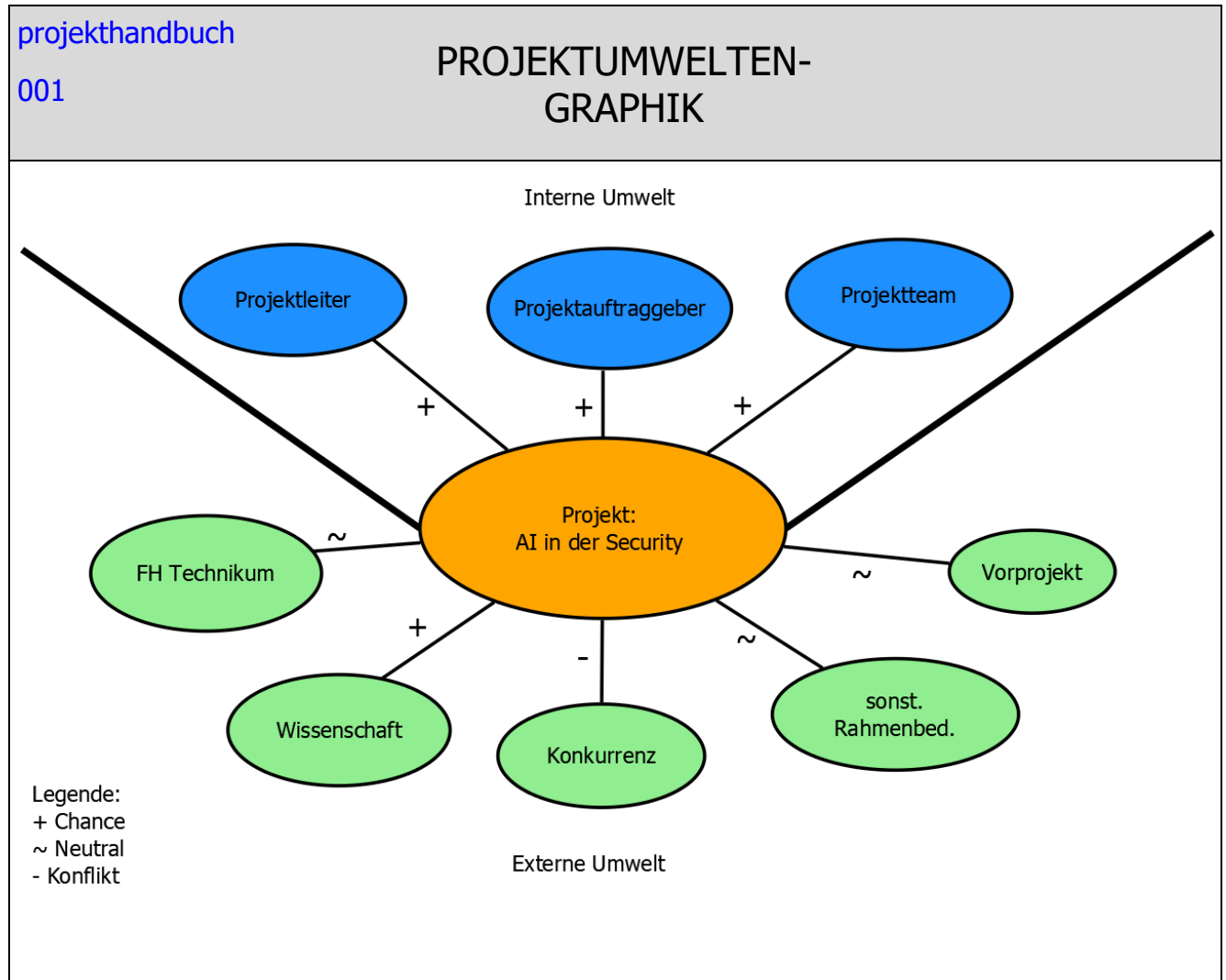
1.3 Projektzieleplan

| projekthandbuch 001 <div>PROJEKTZIELE-PLAN</div> | |
|---|---|
| Zielart | Projektziele |
| Ziele: | <ul style="list-style-type: none"> • Erstellung von zwei wissenschaftlichen Paper zur Erläuterung des Themengebiets bis 31.01.2020 • Aufbau einer geeigneten Serverinfrastruktur zur Durchführung gezielter Angriffe auf ein Zielsystem bis 21.04.2020 • Durchführung von verschiedenen Angriffsarten auf das betroffene System, samt Aufzeichnung der entsprechenden Daten, bis 19.05.2020 • Entwerfen eines gelabelten Testdatensatzes, welcher verschiedene Arten von Netzwerkangriffen, aber auch gutartigen Netzwerkverkehr abdeckt, bis zum 02.06.2020 • Performance-Vergleich des neuronalen Netzwerkes mit dem erstellten Datensatz und den Ergebnissen aus dem Vorprojekt, bis 16.06.2020 • Erstellung einer ausführlichen Dokumentation, welche die Arbeitsdurchführung und die gewonnenen Erkenntnisse vollständig enthält, bis 03.07.2020 |
| Nicht-Ziele | <ul style="list-style-type: none"> • Performance mit anderen Machine Learning-Algorithmen testen (nur Neuronales Netz) • Verwenden eines Unsupervised Learning Ansatzes zur Intrusion Detection • Zusätzliche Paper zu dieser Thematik verfassen |

1.4 Beschreibung Vorprojekt- und Nachprojektphase

| | |
|---|--|
| projekthandbuch 001 | <h1>BESCHREIBUNG VORPROJEKT- UND NACHPROJEKTPHASE</h1> |
| 1) Beschreibung von Ergebnissen der Vorprojektphase | |
| <p><i>Das Projekt betreffende Entscheidungen/Ereignisse. Wie ist es zu dem Projekt gekommen?</i></p> <ul style="list-style-type: none"> • Im Vorprojekt wurde, auf Basis eines neuronalen Netzes, ein Intrusion Detection System aufgebaut • Dabei konnte gezeigt werden, dass der Einsatz von AI-Algorithmen in diesem Kontext sinnvoll ist • Es wurde ein bereits existierender, gelabelter Datensatz verwendet | |
| <p><i>Für das Projekt relevante Dokumente (zB „Protokoll mit ...“, „Besprechung mit ...“, Inhalt der Dokumente ist hier nicht gefragt, NUR die Dokumente!)</i></p> <ul style="list-style-type: none"> • 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 | |
| <p><i>Erfahrungen aus ähnlichen Projekten</i></p> <ul style="list-style-type: none"> • 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 | |
| <p><i>Was wird nach dem Projekt passieren (Folgeaktivitäten, -projekte, etc.)?</i></p> <ul style="list-style-type: none"> • 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



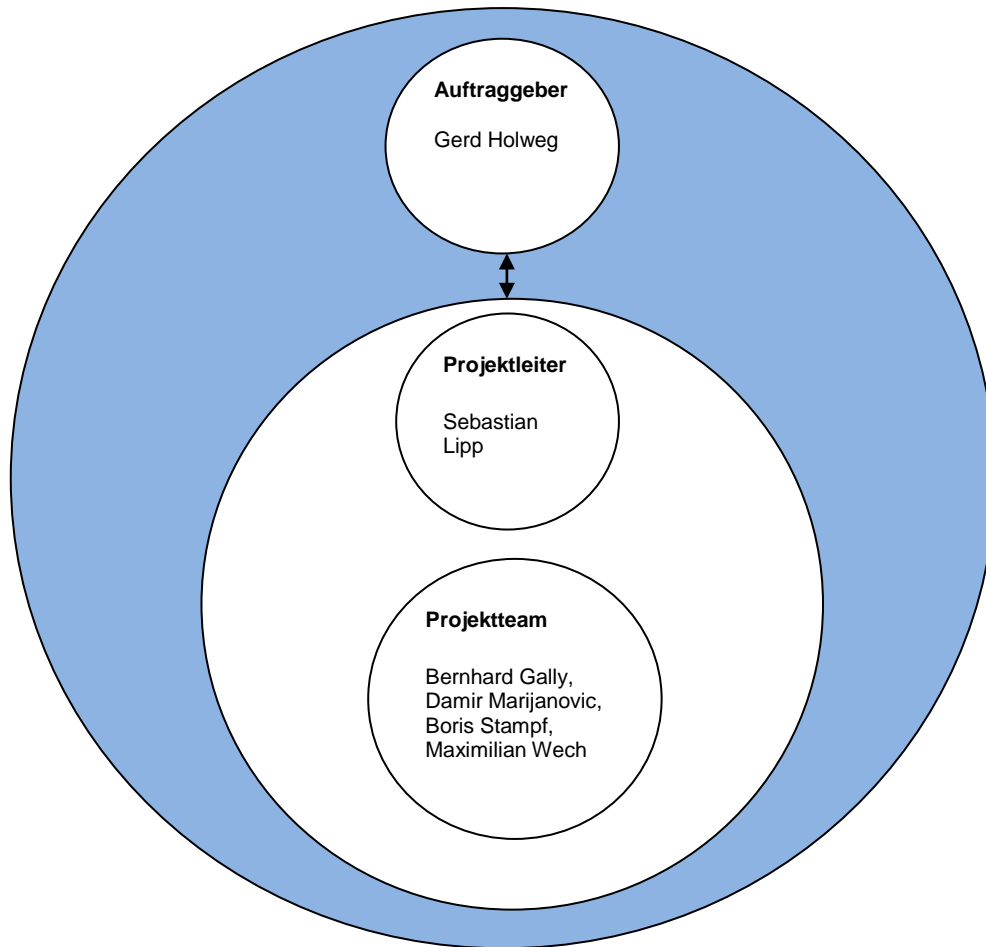
projekthandbuch
001

PROJEKTUMWELTEN-BEZIEHUNGEN

| Umwelten | Beziehung (Potential/Konflikt) | Maßnahmen | Who/When |
|---------------|--|---|------------------------------|
| Projektleiter | Potential <ul style="list-style-type: none"> gute Teamleitungsfähigkeit Spaß an der Arbeit fachliche Kompetenzen in sehr vielen Bereichen | <ul style="list-style-type: none"> Evt. Prämie am Projektende vollste Unterstützung durch Projektauftraggeber | Sebastian Lipp 03.07.2020 |

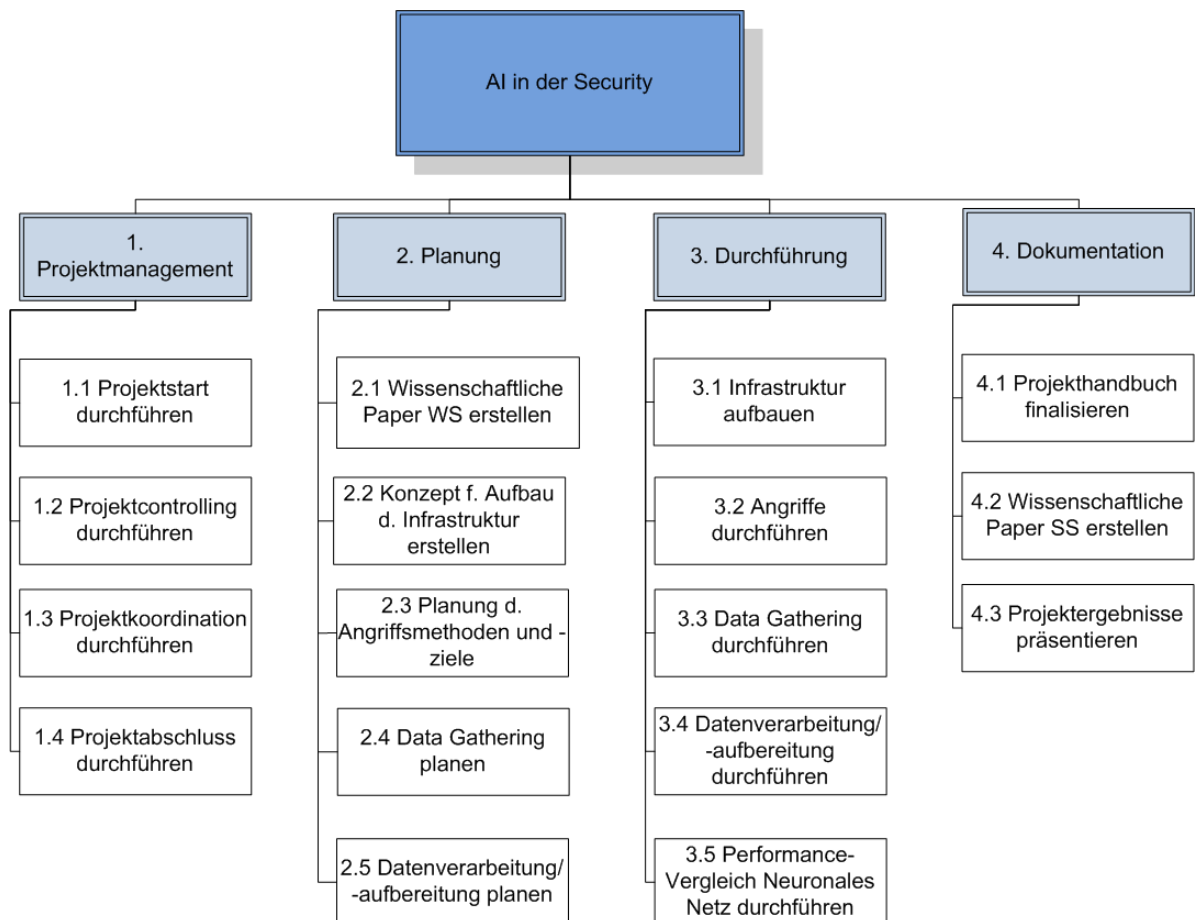
| | | | |
|---------------------|---|---|--|
| Projektteam | Potential <ul style="list-style-type: none"> • Spaß an der Arbeit • viel Projekterfahrung • gutes Konfliktmanagement | <ul style="list-style-type: none"> • Förderung in allen Belangen • Durchführung von Workshops um noch besseren Zusammenhalt zu erlangen • eventuell Zusatzleistungen | Bernhard Gally Damir Marijanovic Boris Stampf Maximilian Wech laufend |
| Projektauftraggeber | Potential <ul style="list-style-type: none"> • Hohes Interesse am Projekterfolg • Kann wichtigen Input liefern | <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • Hohes Interesse an erfolgreichen Projekten • Muss Infrastruktur bereitstellen | <ul style="list-style-type: none"> • Frühes Abklären wie Serverinfrastruktur aufgebaut werden kann (Selbsterstellung / Nutz von Bestehendem) | Sebastian Lipp Anfang März |
| Wissenschaft | Potential <ul style="list-style-type: none"> • Viele Beiträge vorhanden mit ausreichend Information für ein Projekt in diesem Kontext | <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • Rivalität zwischen den Projektteams; jedes will das beste Team sein | <ul style="list-style-type: none"> • Konsequenz und Effizienz arbeiten • Gute Planung • Viel Zeit investieren • Periodischer Vergleich des eigenen Fortschrittes mit der Konkurrenz | Sebastian Lipp laufend |
| Sonst. Rahmenbed. | Neutral <ul style="list-style-type: none"> • evtl. Ausfälle von Teammitglieder • Zeitmangel • Hohe Arbeitslast | <ul style="list-style-type: none"> • Mehrere Teams erstellen • Aufgaben gut verteilen • Detaillierte Planung | Sebastian Lipp Februar |
| Vorprojekt | Neutral <ul style="list-style-type: none"> • Viele wichtige Erkenntnisse • Diese müssen entsprechend genutzt werden • Dokumentation mangelhaft | <ul style="list-style-type: none"> • 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



| <div> <div>projekthandbuch</div> <div>001</div> <div>PROJEKT-ORGANISATION</div> </div> | | |
|--|--|--|
| 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 Projektstrukturplan



1.8 Arbeitspaket-Spezifikationen

| projekthandbuch 001 <div>ARBEITSPAKET-SPEZIFIKATIONEN</div> | |
|---|---|
| PSP-Code, AP-Bezeichnung 1.1 Projektstart durchführen | AP-Inhalt Kickoff-Meeting <ul style="list-style-type: none"> • Projektinhalt/-ziele festlegen (→ Projektauftrag) • Rahmenbedingungen ermitteln und niederschreiben • Projektvorgehensmodell auswählen • Projektorganisation und –kommunikation regeln |
| | AP-Nicht-Inhalte <ul style="list-style-type: none"> • Mit der Projektplanung beginnen • Abarbeiten von Arbeitspaketen |
| | AP-Ergebnisse <ul style="list-style-type: none"> • Klar definierte Ziele • Motivation geschaffen • Projektmitglieder werden auf denselben Informationsstand gebracht • Zusammenarbeit geregelt |
| | AP-Leistungsfortschrittsmessung <ul style="list-style-type: none"> • Kickoff-Meeting abgehalten / nicht abgehalten • Am Ende des Meetings überprüfen, ob Projektmitglieder alles verstanden haben |
| projekthandbuch 001 <div>ARBEITSPAKET-SPEZIFIKATIONEN</div> | |
| PSP-Code, AP-Bezeichnung 1.2 Projektcontrolling durchführen | AP-Inhalt <ul style="list-style-type: none"> • Sicherstellen, dass Projektziele erreicht werden • Projektfortschritt messen • Planabweichungen erkennen (z.B. Soll/Ist Vergleich) • Gegebenenfalls steuernde Maßnahmen einleiten |
| | AP-Nicht-Inhalte <ul style="list-style-type: none"> • Controllingverfahren nicht explizit festlegen • Nichtumsetzbare Vorgaben an Projektmitglieder erteilen • Datenbeschaffung vernachlässigen |
| | AP-Ergebnisse <ul style="list-style-type: none"> • Abweichungen vom Plan erkannt • Projektfortschritt ermittelt • Steuernde Maßnahmen rechtzeitig eingeleitet |
| | AP-Leistungsfortschrittsmessung <ul style="list-style-type: none"> • Soll/Ist Vergleich • Meilensteintrendanalyse • Kennzahlen |

| projekthandbuch 001 | |
|--|--|
| ARBEITSPAKET- SPEZIFIKATIONEN | |
| PSP-Code, AP-Bezeichnung 1.3 Projektkoordination durchführen | AP-Inhalt <ul style="list-style-type: none"> • Sicherung des Projektfortschrittes • Konflikte lösen • Risikomanagement durchführen • Technische und personelle Ressourcen steuern |
| | AP-Nicht-Inhalte <ul style="list-style-type: none"> • Maßnahmen mangelhaft kommunizieren • Unklare Verantwortungsbereiche definieren • Arbeitsprozesse nicht regelmäßig überprüfen |
| | AP-Ergebnisse <ul style="list-style-type: none"> • Kommunikation im Projekt festgelegt • Verantwortungsbereiche eindeutig festgelegt • Optimale Ressourcenverteilung |
| | AP-Leistungsfortschrittsmessung <ul style="list-style-type: none"> • Überprüfen, ob Deadlines eingehalten werden • Berichte |

| projekthandbuch 001 | |
|--|--|
| ARBEITSPAKET- SPEZIFIKATIONEN | |
| PSP-Code, AP-Bezeichnung 1.4 Projektabschluss durchführen | AP-Inhalt <ul style="list-style-type: none"> • Überprüfen, ob alle Ziele erreicht wurden • Wissen und Erfahrungen dokumentieren • Feedbackgespräche • Abschlussbericht erstellen • Projektabschlussfeier |
| | AP-Nicht-Inhalte <ul style="list-style-type: none"> • Auf Abschlussbericht verzichten • Verbesserungspotentiale nicht definieren |
| | AP-Ergebnisse <ul style="list-style-type: none"> • Projektnachbereitung durchgeführt • Lessons Learned dokumentiert • Projektdokumentation vervollständigt |
| | AP-Leistungsfortschrittsmessung Ermitteln, ob <ul style="list-style-type: none"> • Dokumentation vervollständigt ist • alle Ziele erreicht sind |

| projekthandbuch 001 | |
|---|---|
| ARBEITSPAKET-SPEZIFIKATIONEN | |
| PSP-Code, AP-Bezeichnung 2.1 Wissenschaftliche Paper WS erstellen | AP-Inhalt <ul style="list-style-type: none"> Literaturrecherche durchführen zur Erstellung einer Grobkonzeption Überblick über das Themengebiet schaffen Basis für die Feinkonzeption im SS20 erstellen |
| | AP-Nicht-Inhalte <ul style="list-style-type: none"> Detailplanung des Sommersemesters Zusätzliche Paper weit über das Themengebiet hinaus erstellen |
| | AP-Ergebnisse <ul style="list-style-type: none"> Wissenschaftliche Paper zum Einstieg in das Themengebiet fertiggestellt Auf Basis der Paper kann mit Detailplanung begonnen werden |
| | AP-Leistungsfortschrittsmessung <ul style="list-style-type: none"> Laufendes Reporting des aktuellen Stands an den Projektleiter Überprüfung: Paper fertig / nicht fertig; fristgerechte Einhaltung der Deadline |

| projekthandbuch 001 | |
|---|--|
| ARBEITSPAKET-SPEZIFIKATIONEN | |
| PSP-Code, AP-Bezeichnung 2.2 Konzept f. Aufbau d. Infrastruktur erstellen | AP-Inhalt <ul style="list-style-type: none"> Bedarfsermittlung: welche (Server-)Infrastruktur wird gebraucht (zur Durchführung der Angriffe) Planen, wie die notwendigen Komponenten beschafft werden können (FH Technikum?) Skizzieren des Aufbaues Literaturrecherche |
| | AP-Nicht-Inhalte <ul style="list-style-type: none"> Bereits mit dem praktischen Aufbau beginnen Über Planungsschritte hinausarbeiten |
| | AP-Ergebnisse <ul style="list-style-type: none"> Genau definierter Plan, welche Komponenten benötigt werden, wie diese beschafft werden und wie diese aufgebaut wird |
| | AP-Leistungsfortschrittsmessung <ul style="list-style-type: none"> Laufendes Reporting des aktuellen (Planungs-)Stands an den Projektleiter Überprüfung: Konzept fertig / nicht fertig; fristgerechte Einhaltung der Deadline |

ARBEITSPAKET- SPEZIFIKATIONEN

| | |
|---|---|
| PSP-Code, AP-Bezeichnung 2.3 Planung d. Angriffsmethoden und -ziele | AP-Inhalt <ul style="list-style-type: none"> • Festlegen, welche Tools eingesetzt werden (zum Durchführen der Angriffe) • Definieren, welche Arten von Angriffen ausgeführt werden (DOS, SQL-Injection, etc...) • Angriffsziele festlegen (was soll angegriffen werden) • Literaturrecherche |
| | AP-Nicht-Inhalte <ul style="list-style-type: none"> • Praktische Ausführung der Angriffe • Alles, was über die Planung hinausgeht |
| | AP-Ergebnisse Vollständiges Konzept mit <ul style="list-style-type: none"> • Auflistung der auszuführenden Angriffe • Auflistung der zu verwendenden Tools • Beschreibung, worauf die Angriffe abzielen |
| | AP-Leistungsfortschrittsmessung <ul style="list-style-type: none"> • Laufendes Reporting an den Projektleiter (samt Erläuterung: was wurde bereits getan / fehlt noch, etc.) • Planung abgeschlossen / nicht abgeschlossen, Deadline eingehalten / nicht eingehalten |

ARBEITSPAKET- SPEZIFIKATIONEN

| | |
|---|---|
| PSP-Code, AP-Bezeichnung 2.4 Data Gathering planen | AP-Inhalt <ul style="list-style-type: none"> • Spezifizieren, wie ausgeführte Angriffe bzw. gutartiger Traffic aufgezeichnet werden sollen • Festlegen, welche Tools für diesen Zweck eingesetzt werden sollen • Definieren, wo und wie die aufgezeichneten Informationen abgespeichert werden sollen • Literaturrecherche |
| | AP-Nicht-Inhalte <ul style="list-style-type: none"> • Über die Planungsphase hinausgehen • Feature Extraction planen |
| | AP-Ergebnisse <ul style="list-style-type: none"> • Konzept, wie das Mitschneiden des Netzwerktraffics erfolgt • Spezifizieren von einzusetzenden Tools / Speicherort |
| | AP-Leistungsfortschrittsmessung <ul style="list-style-type: none"> • Laufendes Reporting an den Projektleiter • Data Gathering Konzept fertig / nicht fertig, Deadline eingehalten / nicht eingehalten |

| projekthandbuch 001 | |
|--|--|
| ARBEITSPAKET-SPEZIFIKATIONEN | |
| PSP-Code, AP-Bezeichnung 2.5 Datenverarbeitung/-aufbereitung planen | AP-Inhalt <ul style="list-style-type: none"> • Festlegen, welche Features aus dem Datensatz relevant für Machine Learning sind • Festlegen, nach welchen Kriterien klassifiziert werden soll (z.B. DOS, gutartiges Datenpaket, etc.) • Planen wie Daten für das neuronale Netz aufbereitet und verarbeitet werden sollen • Literaturrecherche |
| | AP-Nicht-Inhalte <ul style="list-style-type: none"> • Schritte, welche über die Planung hinausgehen • Praktische Durchführung der Datenverarbeitung /-aufbereitung |
| | AP-Ergebnisse <ul style="list-style-type: none"> • Vollständiges Konzept, wie die Daten aufbereitet und verarbeitet werden sollen (Feature Extraction, Kriterien, etc.) • Abschluss der Planungsphase |
| | AP-Leistungsfortschrittsmessung <ul style="list-style-type: none"> • Reporting an den Projektleiter; bei Fertigstellung dem Projektauftraggeber mitteilen, dass Planungsphase beendet ist • Überprüfen, ob Deadline eingehalten wurde |

| projekthandbuch 001 | |
|---|--|
| ARBEITSPAKET-SPEZIFIKATIONEN | |
| PSP-Code, AP-Bezeichnung 3.1 Infrastruktur aufbauen | AP-Inhalt <ul style="list-style-type: none"> • Gemäß der in 2.2 erstellten Planung soll nun die Infrastruktur beschaffen und aufgebaut werden • Zusammenstellen der Komponenten zum Aufbau der Infrastruktur |
| | AP-Nicht-Inhalte <ul style="list-style-type: none"> • Bereits Angriffe auf Knoten des Systems durchführen • Nicht an die in 2.2 erstellte Planung halten |
| | AP-Ergebnisse <ul style="list-style-type: none"> • Vollständig aufgebaute Infrastruktur • Bereit für das Durchführen der Angriffe auf Knoten des Systems |
| | AP-Leistungsfortschrittsmessung <ul style="list-style-type: none"> • Reporting an den Projektleiter (was ist bereits erledigt, was nicht) • Infrastruktur erfolgreich aufgebaut / nicht erfolgreich aufgebaut |

projekthandbuch
001

ARBEITSPAKET- SPEZIFIKATIONEN

| | |
|---|--|
| PSP-Code, AP-Bezeichnung 3.2 Angriffe durchführen | AP-Inhalt <ul style="list-style-type: none"> Anhand der in 2.3 erstellten Planung, sollen nun die Angriffe auf Knoten des Systems durchgeführt werden (ggf. unter Verwendung von Tools) Dabei sollen verschiedene Arten von Angriffen ausgeführt werden Unterschiedliche Angriffsziele angreifen bzw. Schwachstellen ausnützen |
| | AP-Nicht-Inhalte <ul style="list-style-type: none"> Nicht geplante Angriffsarten ausführen Andere Angriffsziele, als jene die geplant sind, angreifen |
| | AP-Ergebnisse <ul style="list-style-type: none"> Es wurden gezielt Angriffe auf Knoten des Systems mit der Serverinfrastruktur ausgeführt Auch legitimer Traffic findet statt |
| | AP-Leistungsfortschrittsmessung <ul style="list-style-type: none"> Reporting an den Projektleiter (was fehlt noch, was ist erledigt..) Anzahl Angriffe durchgeführt durch Anzahl aller Angriffe Angriffe durchgeführt / nicht durchgeführt |

projekthandbuch
001

ARBEITSPAKET- SPEZIFIKATIONEN

| | |
|---|---|
| PSP-Code, AP-Bezeichnung 3.3 Data Gathering durchführen | AP-Inhalt <ul style="list-style-type: none"> Gemäß der in 2.4 erstellten Planung: Aufzeichnen des Netzwerktraffics Angriffe (und Angriffsarten) entsprechend kennzeichnen Einsatz von Tools |
| | AP-Nicht-Inhalte <ul style="list-style-type: none"> Nur bestimmte Features aufzeichnen (Feature Extraction erfolgt später) Nicht plangemäß vorgehen |
| | AP-Ergebnisse <ul style="list-style-type: none"> Traffic erfolgreich mitgeschnitten Datenpakete entsprechend gekennzeichnet |
| | AP-Leistungsfortschrittsmessung <ul style="list-style-type: none"> Reporting des aktuellen Status an den Projektleiter Data Gathering fertiggestellt / nicht fertiggestellt; an Deadline halten |

| projekthandbuch 001 | |
|--|---|
| ARBEITSPAKET-SPEZIFIKATIONEN | |
| PSP-Code, AP-Bezeichnung 3.4 Datenverarbeitung / -aufbereitung durchführen | AP-Inhalt <ul style="list-style-type: none"> • Reduzierung der aufgezeichneten Daten auf relevante Features (→Feature Extraction) gemäß der Planung aus 2.5 • Verarbeitung und Aufbereitung der Daten für das neuronale Netz |
| | AP-Nicht-Inhalte <ul style="list-style-type: none"> • Nicht an die Planung halten • Daten mangelhaft aufbereiten / verarbeiten |
| | AP-Ergebnisse <ul style="list-style-type: none"> • Aufbereitete Daten, anhand denen ein neuronales Netz trainiert werden kann • Bereitstellung der Daten |
| | AP-Leistungsfortschrittsmessung <ul style="list-style-type: none"> • Reporting an den Projektleiter • Datenverarbeitung -aufbereitung fertig / nicht fertig |

| projekthandbuch 001 | |
|--|--|
| ARBEITSPAKET-SPEZIFIKATIONEN | |
| PSP-Code, AP-Bezeichnung 3.5 Performance-Vergleich Neuronales Netz durchführen | AP-Inhalt <ul style="list-style-type: none"> • Es soll ein Performance-Vergleich (unter Verwendung neuronaler Netze) der öffentlich verfügbaren Testdaten aus dem Vorprojekt, mit dem in diesem Projekt erstellten Datensatz durchgeführt werden. • Ergebnisse entsprechend dokumentieren |
| | AP-Nicht-Inhalte <ul style="list-style-type: none"> • Weitere Datensätze testen • Andere Machine Learning Algorithmen für diese Thematik ausprobieren |
| | AP-Ergebnisse <ul style="list-style-type: none"> • Ergebnis, welche Klassifizierungsgenauigkeit mit dem erstellten Datensatz und neuronalen Netzen möglich ist • Erkenntnis welcher Datensatz besser für diese Thematik geeignet ist |
| | AP-Leistungsfortschrittsmessung <ul style="list-style-type: none"> • Reporting an den Projektleiter • Performance-Vergleich durchgeführt / nicht durchgeführt |

| projekthandbuch 001 | | ARBEITSPAKET- SPEZIFIKATIONEN |
|--|---|----------------------------------|
| PSP-Code, AP-Bezeichnung 4.1 Projekthandbuch finalisieren | AP-Inhalt <ul style="list-style-type: none">• Vervollständigen der Projektdokumentation• Aktualisieren von veralteten Inhalten• Zusammenfassen der Projektergebnisse | |
| | AP-Nicht-Inhalte <ul style="list-style-type: none">• Andere Tätigkeiten außer dem Dokumentieren | |
| | AP-Ergebnisse <ul style="list-style-type: none">• Vollständig ausgefülltes Projekthandbuch• Wesentliche Projektergebnisse und Erkenntnisse dokumentiert | |
| | AP-Leistungsfortschrittsmessung <ul style="list-style-type: none">• Überprüfen, wie weit das Projekthandbuch ausgefüllt ist• Reporting an den Projektleiter• Projekthandbuch vollständig / nicht vollständig | |

| projekthandbuch 001 | | ARBEITSPAKET- SPEZIFIKATIONEN |
|--|---|----------------------------------|
| PSP-Code, AP-Bezeichnung 4.2 Wissenschaftliche Paper SS erstellen | AP-Inhalt <ul style="list-style-type: none">• Zwei wissenschaftliche Paper erstellen, um einen Überblick über die Thematik zu erhalten (WS 19/20)• Zwei wissenschaftliche Paper erstellen, um die wesentlichen Ergebnisse und Erkenntnisse der Projektausführung zu dokumentieren (SS 20) | |
| | AP-Nicht-Inhalte <ul style="list-style-type: none">• Zusätzliche Paper zu dieser Thematik erstellen• Plagiate aus bereits existierenden Arbeiten | |
| | AP-Ergebnisse <ul style="list-style-type: none">• Vollständige wissenschaftliche Paper die das Themengebiet und die praktische Durchführung abdecken | |
| | AP-Leistungsfortschrittsmessung <ul style="list-style-type: none">• Laufende Überprüfung des Status der Vollständigkeit• Deadlines eingehalten / nicht eingehalten | |

ARBEITSPAKET- SPEZIFIKATIONEN

| | |
|--|--|
| PSP-Code, AP-Bezeichnung 4.3 Projektergebnisse präsentieren | AP-Inhalt <ul style="list-style-type: none"> • Schreiben des Projektabschlussberichtes • Präsentieren der wesentlichen Ergebnisse • Erkenntnisse und Erfahrungen für zukünftige Projekte weitergeben |
| | AP-Nicht-Inhalte <ul style="list-style-type: none"> • Bereits zukünftige Projekte zu dieser Thematik vorstellen |
| | AP-Ergebnisse <ul style="list-style-type: none"> • Projektauftraggeber und relevante Stakeholder wurden im Rahmen der Abschlusspräsentation über die wesentlichen Ergebnisse und Erkenntnisse der Projektausführung informiert |
| | AP-Leistungsfortschrittsmessung <ul style="list-style-type: none"> • Status Abschlussbericht überprüfen • Abschlusspräsentation zeitgerecht abgehalten / nicht abgehalten |

1.9 Projektmeilensteinplan

| <div> <div>projekthandbuch</div> <div>001</div> <div>PROJEKT- MEILENSTEINPLAN</div> </div> | | | |
|--|-------------------|-------------------------|----------------|
| Meilenstein | Basis- termine | Aktuelle Plantermine | Ist Termine |
| Projektauftrag erhalten | 03.12.2019 | 03.12.2019 | 03.12.2019 |
| WS-Paper verfasst | 31.01.2020 | 28.02.2020 | |
| Konzeption erstellt | 24.03.2020 | 24.03.2020 | |
| Serverinfrastruktur aufgebaut | 21.04.2020 | 21.04.2020 | |
| Angriffe erfolgreich durchgeführt und aufgezeichnet | 19.05.2020 | 19.05.2020 | |
| Feature Extraction und Aufbereitung des Datasets fertiggestellt | 02.06.2020 | 02.06.2020 | |
| Vergleich der Performance mit Ergebnissen aus Vorprojekt durchgeführt | 16.06.2020 | 16.06.2020 | |
| Projektabschluss durchgeführt | 03.07.2020 | 03.07.2020 | |

1.10 Projektzeitplan

Grundlegende Informationen:

| Semester | ECTS | ECTS in h | FH-Präsenzzeit in h | Anzahl Mitglieder | Gesamtaufwand aller Mitglieder in h |
|----------|------|-----------|---------------------|-------------------|-------------------------------------|
| WS 19/20 | 1,5 | 37,5 | 7,5 | 5 | 187,5 |
| SS 20 | 4,5 | 112,5 | 22,5 | 5 | 562,5 |

Geplante Zeitaufteilung im WS 19/20:

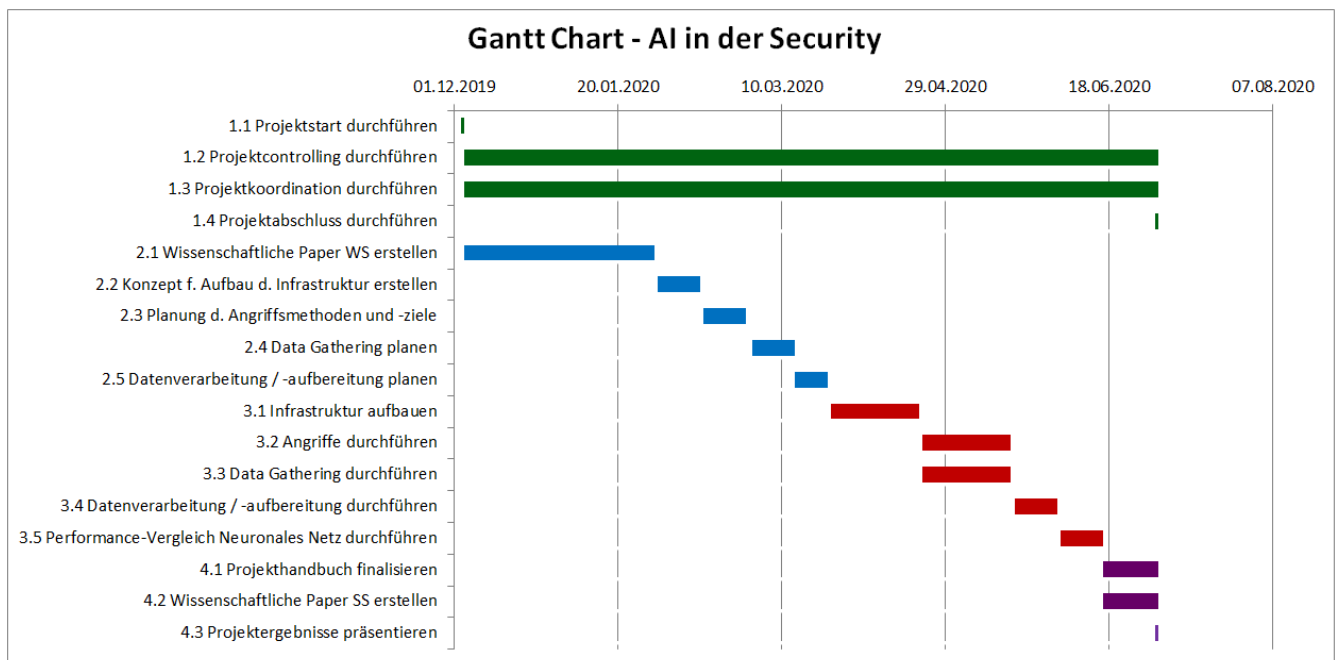
| Aufgabe | Zeitdauer in h pro Person |
|---|---------------------------|
| Einarbeitung in das Themengebiet | 5 |
| Literaturrecherche | 15 |
| Ausarbeitung der wissenschaftlichen Paper | 12,5 |
| Projektmanagement und Koordination | 5 |

Geplante Zeitaufteilung im SS 20:

| Aufgabe | Zeitdauer in h pro Person |
|---|---------------------------|
| Detailplanung (Konzeption) | 20 |
| Praktische Durchführung | |
| • Aufbau der Infrastruktur | 18 |
| • Durchführung und Aufzeichnung der Angriffe | 18 |
| • Feature Extraction und Aubereitung des Datasets | 10 |
| • Performance Vergleich | 10 |
| Literaturrecherche (für Erstellung d. Paper) | 10 |
| Ausarbeitung der wissenschaftlichen Paper | 8,5 |
| Abschlusspräsentation (+Vorbereitung) | 6 |
| Projektmanagement und Koordination | 12 |

1.11 Projektbalkenplan

| Arbeitspaket-Name | Start | Ende | Dauer (Tage) |
|---|------------|------------|--------------|
| 1.1 Projektstart durchführen | 03.12.2019 | 04.12.2019 | 1 |
| 1.2 Projektcontrolling durchführen | 04.12.2019 | 03.07.2020 | 212 |
| 1.3 Projektkoordination durchführen | 04.12.2019 | 03.07.2020 | 212 |
| 1.4 Projektabschluss durchführen | 02.07.2020 | 03.07.2020 | 1 |
| 2.1 Wissenschaftliche Paper WS erstellen | 04.12.2019 | 31.01.2020 | 58 |
| 2.2 Konzept f. Aufbau d. Infrastruktur erstellen | 01.02.2020 | 14.02.2020 | 13 |
| 2.3 Planung d. Angriffsmethoden und -ziele | 15.02.2020 | 28.02.2020 | 13 |
| 2.4 Data Gathering planen | 01.03.2020 | 14.03.2020 | 13 |
| 2.5 Datenverarbeitung / -aufbereitung planen | 14.03.2020 | 24.03.2020 | 10 |
| 3.1 Infrastruktur aufbauen | 25.03.2020 | 21.04.2020 | 27 |
| 3.2 Angriffe durchführen | 22.04.2020 | 19.05.2020 | 27 |
| 3.3 Data Gathering durchführen | 22.04.2020 | 19.05.2020 | 27 |
| 3.4 Datenverarbeitung / -aufbereitung durchführen | 20.05.2020 | 02.06.2020 | 13 |
| 3.5 Performance-Vergleich Neuronales Netz durchführen | 03.06.2020 | 16.06.2020 | 13 |
| 4.1 Projekthandbuch finalisieren | 16.06.2020 | 03.07.2020 | 17 |
| 4.2 Wissenschaftliche Paper SS erstellen | 16.06.2020 | 03.07.2020 | 17 |
| 4.3 Projektergebnisse präsentieren | 02.07.2020 | 03.07.2020 | 1 |



1.12 Projektkommunikationsstrukturen

| <div> <div>projekthandbuch 001</div> <div>PROJEKT-KOMMUNIKATION</div> </div> | | | | |
|--|---|--|-------------------------------|---|
| Bezeichnung | Ziele, Inhalte | Teilnehmer | Termine | Ort |
| Management-Sitzung | <ul style="list-style-type: none"> • Diskussion Projektstatus, Abweichungen im Projekt • Entscheidungsfindung auf Basis der Projektcontrolling-Sitzung • Freigabe Projektfortschrittsbericht | Projektauftraggeber, Projektleiter | Monatlich, am ersten Dienstag | FH Technikum Wien |
| Projektcontrolling-Sitzung | <ul style="list-style-type: none"> • Projektstatus • Controlling Leistungsfortschritt, Termine und Ressourcen • Controlling der Umweltbeziehungen • Soziales Projektcontrolling • Diskussion übergeordneter Problemstellungen • Entscheidungsaufbereitung für Projektauftraggeber-Sitzung | ProjektleiterIn, Projektteam, Projektcoach | Wöchentlich am Montag | FH Technikum Wien, beziehungsweise über Skype |

1.13 Projektrisikooanalyse

| 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) |
| Mitarbeiter- ausfall | m | / | 40 | / | 2 | Arbeit gut aufteilen und rechtzeitig reagieren | / |
| Problem beim Aufbau der Infrastruktur | m | / | 20 | / | 2 | Gut planen und rechtzeitig beginnen / Abhängigkeiten mit FH Technikum früh klären | / |
| 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 | / |
| Unvorhersehba- rer Schaden an der Serverinfrastrukt- ur entsteht | l | / | 5 | / | 2 | Kontrolle der Durchführung, Ausreichend Planen | / |
| Projektteil im WS kann nicht rechtzeitig fertiggestellt werden | m | / | 35 | / | 2 | Frühzeitig mit der Erstellung der Paper beginnen, Aufgaben gut verteilen | / |
| Finden aussagekräftige r 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 | / |

1.14 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. |