HÖHERE TECHNISCHE BUNDESLEHRANSTALT WIEN 3, RENNWEG 89B
Höhere Abteilung für Informationstechnologie

Projektnummer:	**3R IT 20 22**	Wien, im September 2019	
Antrag um Genehmigung einer Aufgabenstellung für die **DIPLOMARBEIT**			
Schuljahr:	**2019/20**	Anzahl Beiblätter:	**21**
Thema:	**Netzwerkanalyse eines Enterprise-Netzwerks (Argos)**		

Aufgabenstellung:
Mit zunehmender Größe von Netzwerken wird es für den Administrator dieser immer schwieriger den Überblick über den Datenverkehr zu behalten. Dadurch ist es für Benutzer innerhalb und außerhalb des Netzes bzw. Angreifern einfacher möglich unerlaubterweise Unternehmensrichtlinien zu umgehen bzw. dem Netzwerk zu schaden.
Das Ziel des Projektes ist es zu verstehen, wie solche Richtlinienumgehungen bzw. Angriffe für den Administrator überprüfbar gemacht und im besten Fall grafisch dargestellt werden könnten. Darunter fällt unter anderem das Zurückverfolgen einer Verbindung auf einen gewissen Benutzer oder Computer.

Kandidatinnen/Kandidaten:	Klasse	Individ. Betreuung	Unterschrift Kandidatinnen
Projektleiterin/Projektleiter **Lorenz Stechauner**	5CN	HOR	
Stellv. Projektleiterin/Projektleiter Harald Moritz	5CN	HOR	
Lukas Bandion	5CN	SDO	
Thomas Hilscher	5CN	SDO	

Betreuerinnen/Betreuer:	Unterschrift
Individuelle Betreuung (~~Hauptbetreuung~~): **Christian Schöndorfer**	
Individuelle Betreuung (~~Hauptbetreuung Stv.~~): August Hörandl	

Als Diplomarbeit zugelassen

Datum

……..
AV Gabriela Herrele

Datum

…….
Bildungsdirektion Wien

Executive Summary

Objectives

As the size of networks increases, it becomes increasingly difficult for the administrator to keep track of traffic. This makes it easier for users inside and outside the network or attackers to circumvent company policies or harm the network without permission.

The aim of the project is to understand how such policy bypasses or attacks could be made verifiable for the administrator and at best graphically displayed. This includes, among other things, tracing a connection to a certain user or computer.

Risks

Risk	Countermeasure
5th form	Since the project team also visits the 5th grade in addition to the work on the project, it can often happen that there are weeks in which little to nothing can be worked on the project.
EU-GDPR	It is a main goal of the diploma thesis to work in compliance with data protection, therefore, to save only the most important data and to anonymize data if necessary.

Milestones

Date (D.M.Y)	Milestone
23.09.2019	Initial log processing approved
14.10.2019	Query language concept approved
28.10.2019	Port mirror (deep packet inspection) approved
25.11.2019	Query language implementation approved
02.12.2019	Deep learning concept approved
16.12.2019	Visualization approved
30.12.2019	First version of diploma thesis finished
10.02.2019	Diploma thesis finished
30.03.2020	Diploma project finished and approved

Budget and Resources

Project budget	100,00 €
Costs for school	0,00 €
Total man hours	800 h

Inhaltsverzeichnis

1 Projektidee

1.1 Ausgangssituation

Mit zunehmender Größe von Netzwerken wird es für den Administrator dieser immer schwieriger den Überblick über den Datenverkehr zu behalten. Dadurch ist es für Benutzer innerhalb und außerhalb des Netzes bzw. Angreifern einfacher möglich unerlaubterweise Unternehmensrichtlinien zu umgehen bzw. dem Netzwerk zu schaden. Betreiber von Netzwerken mit hohen Sicherheitsanforderungen beanspruchen oft Dienstleistungen von diversen Security-Consulting-Unternehmen um dieser Probleme Herr zu werden. Diese sind meistens mit hohem finanziellem Aufwand verbunden.

Vor allem die HTL Rennweg sieht sich aufgrund ihres IT-Schwerpunktes massiv mit diesen Problemen konfrontiert, doch für Schulen ist der enorme finanzielle Aufwand in den meisten Fällen nicht tragbar.

1.2 Beschreibung der Idee

Das Ziel des Projektes ist es zu verstehen, wie solche Richtlinienumgehungen bzw. Angriffe für den Administrator überprüfbar gemacht und im besten Fall grafisch dargestellt werden könnten. Darunter fällt unter anderem das Zurückverfolgen einer Verbindung auf einen gewissen Benutzer oder Computer.

Hierbei gilt es natürlich die DSGVO zu beachten. Weiters ist es für Administratoren praktisch das Datenaufkommen pro Benutzer oder Raum festzustellen oder die meistbesuchte Website eines Tages einsehen zu können.

Um all dies zu bewerkstelligen benötigt man Daten, die man auswerten kann. Um an diese Daten zu kommen werden Log-Daten von diversen Intermediate-Devices (wie z.B. Firewalls, Router, WLAN-Controller, etc.) gesammelt.

2 Projektziele

2.1 Hauptziele

Ziel H1 Sammlung der Log-Daten

Es wird eine geeignete Syslog-Server-Lösung ausgewählt und aufgesetzt welche Syslog-Nachrichten von diversen Geräten sammelt und an einem zentralisierten Ort speichert.

Ziel H2 Implementierung einer Packet Capture Lösung

Ein Programm wird erstellt, welches Pakete aus einem Netzwerk (z.B. Port-Mirror auf einem Switch) mittels *Deep Packet Inspection* verarbeitet und gegebenenfalls an eine Speicherlösung weiterleitet.

Ziel H3 Aufbereitung der ASA Log-Daten

Ein Programm wird erstellt, welches bereits gesammelte Log-Daten einer Cisco ASA (Firewall) entgegennimmt und aus diesen Daten technisch nicht relevante Informationen entfernt. Dies ist notwendig, da Logs von Cisco darauf ausgelegt sind von einem Menschen gelesen zu werden, dadurch wird die Datenspeicherung und -verarbeitung erschwert.

Ziel H4 Speicherung und einfache Verarbeitung der Log-Daten

Eine für alle anfallenden Log-Daten geeignete Speicherlösung wird ausgewählt und implementiert. Die Speicherlösung muss auf Datenmengen, die in Netzen, wie z.B. einem EDV-Saal der Schule anfallen ausgelegt sein, ohne die Leistungsfähigkeit zu vermindern. Die Daten sollen in eine für möglichst simple Abfragen geeignete Form (z.B. JSON) gebracht und gespeichert werden.

Ziel H5 Query Language

Es wird ein Konzept für eine Query Language ausgearbeitet und implementiert. So soll es möglich werden mit einfachen Abfragen die gespeicherten Daten in passender Form auszugeben.

Ziel H6 Visualisierung der Daten

Daten, die mithilfe der Query Language abgerufen werden, werden in einem Webinterface grafisch dargestellt, um dem Administrator einen einfachen und schnellen Überblick über die gespeicherten Daten zu ermöglichen.

Ziel H7 Ergänzen der Daten

Ein Programm wird erstellt, welches auf Anfrage hin die Daten mit Informationen aus externen, u.a. öffentlich zugänglichen, Datenquellen (z.B. MAC-Adresse wird in Hersteller übersetzt) ergänzt.

Ziel H8 Datenschutzkonforme Behandlung von Nutzerdaten

Es werden Überlegungen zur Datenschutzkonformen Behandlung der Nutzerdaten betreffend der DSGVO getroffen, welche rechtlichen Probleme dadurch entstehen und wie diese für dieses Projekt gelöst werden könnten. Diese Lösungen werden in allen diesbezüglich relevanten Programmen umgesetzt.

Ziel H9 Vergleichen verschiedener SIEM-Lösungen

Es werden verschiedene, bereits bestehende SIEM-Systeme miteinander verglichen und evaluiert welches am besten für den Anwendungsfall dieses Projektes geeignet wäre.

Ziel H10 Evaluierung von Deep Packet Inspection auf Firewalls

Es wird überprüft, ob der Einsatz von *Deep Packet Inspection* auf Firewalls ausreichend sinnvolle Informationen liefern kann. Zusätzlich wird auch überprüft ob und wie man verschlüsselte Verbindungen (TLS, SSL, …) mitverfolgen kann.

Ziel H11 Evaluierung des Einsatzes von Deep Learning

Es wird überprüft, ob und wie der Einsatz von *Deep Learning* bzw. *Machine Learning* dabei helfen kann, aussagekräftige Voraussagen über den Netzwerkverkehr treffen kann.

Ziel H12 Vergleichen verschiedener KI-Systeme

Mögliche Deep Learning Modelle (z.B. Supervised, Unsupervised) werden verglichen und es wird für das Projekt ein geeignetes Modell evaluiert.

2.2 Optionale Ziel

Ziel O1 Log-Daten aus dem Schulnetz sammeln

Die Geräte im Schulnetz werden so konfiguriert, dass sie relevante Log-Daten an einen Server weiterleiten. Dieser Server kann auch im Schulnetz aufgesetzt werden.

Ziel O2 Überprüfung der angewendeten Anonymisierung

Es werden diverse „Angriffe“ auf die eigenen Systeme ausgeführt, um zu überprüfen, wie sicher die Anonymisierung (*Ziel H9*) der personen- und nutzerbezogenen Daten tatsächlich stattgefunden hat. Falls durch eine Analyse der Metadaten trotzdem Benutzer identifizierbar sind, wird versucht dieses Problem zu beheben.

Ziel O3 Einsatz von Deep Learning

Das in *H12* ausgewählte Modell wird mit gespeicherten Daten trainiert und erste Ergebnisse werden auf ihre Aussagekraft überprüft.

Ziel O4 Packet Capture auf Switch in einem Raum durchführen

Die in H2 erstellte Lösung wird auf einen Switch in einem Raum (z.B. Raum 261) eingesetzt, um möglichst aussagekräftige Echtdaten zu erhalten. Weiters wird überprüft wie viel Datendurchsatz in Echtzeit überprüfbar ist und ob dieser für den Anwendungsfall des Projekts ausreicht.

Ziel O5 Überprüfung der Leistungsfähigkeit

Es wird überprüft, ob die Verarbeitung der anfallenden Daten einer ausreichend großen Testgruppe (z.B. EDV Saal, Raum 261) durch das gesamte System in Echtzeit möglich ist.

2.3 NICHT Ziele

Ziel N1 Wartung

Nach Abschluss und Abnahme des Projektes wird das Team die entstandene Software warten und up-to-date halten. Falls optionale Ziele bei Ende des Projektes noch offenstehen, werden diese noch vervollständigt.

Ziel N2 Änderungen am Schulnetzwerk

Das Team nimmt während des Projektes schwerwiegende Änderungen am Schulnetzwerk vor und designet dieses neu.

Ziel N3 Erstellen eines Produktes

Alle Programme und User-Interfaces werden in einem einzigen marktfähigen Produkt vereint, um das Projekt so potenziellen Kunden näher zu bringen. Die Nutzung des Produktes soll auf entgeltlicher Basis stattfinden.

2.4 Individuelle Aufgabenstellungen der Teammitglieder im Gesamtprojekt

2.4.1 Lorenz Stechauner

Themenschwerpunkt	Deterministische Verarbeitung und Speicherung der Log-Daten.
Aufgabenstellung Auflistung der einzelnen Ziele und Anforderungen	• H1 Sammlung der Log-Daten • H4 Speicherung und einfache Verarbeitung der Log-Daten • H5 Query Language • O1 Log-Daten aus dem Schulnetz sammeln • O5 Überprüfung der Leistungsfähigkeit

2.4.2 Harald Moritz

Themenschwerpunkt	Aufbereitung von Log-Daten und Einsatz von Deep Learning.
Aufgabenstellung Auflistung der einzelnen Ziele und Anforderungen	• H3 Aufbereitung der ASA Log-Daten • H11 Evaluierung des Einsatzes von Deep Learning • H12 Vergleichen verschiedener KI-Systeme • O3 Einsatz von Deep Learning

2.4.3 Lukas Bandion

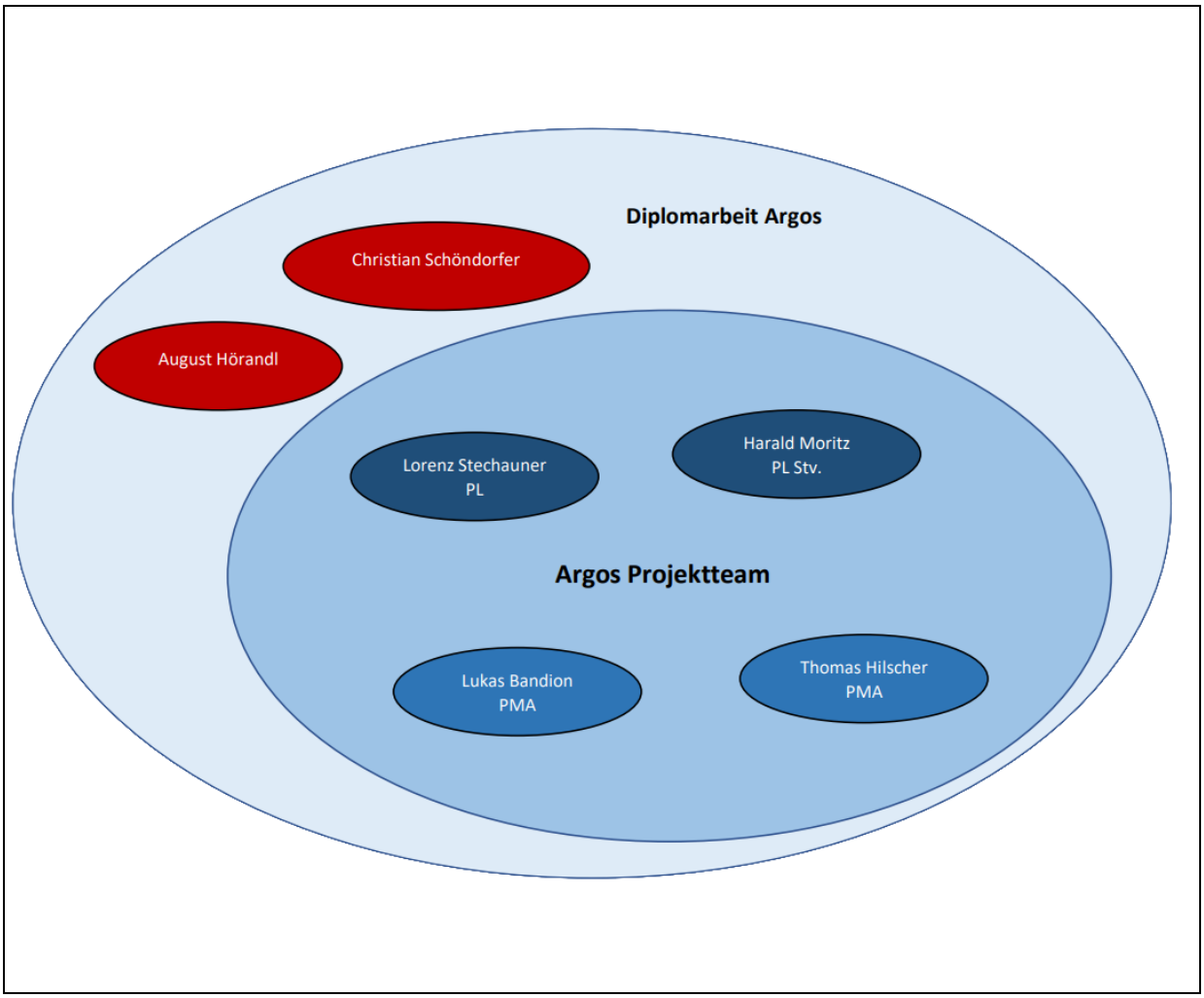
Themenschwerpunkt	Analyse von Deep Packet Inspection und externer Datenbeschaffung
Aufgabenstellung Auflistung der einzelnen Ziele und Anforderungen	• H2 Implementierung einer Packet Capture Lösung • H7 Ergänzen der Daten • H10 Evaluierung von Deep Packet Inspection auf Firewalls • O4 Packet Capture auf Switch in einem Raum durchführen

2.4.4 Thomas Hilscher

Themenschwerpunkt	Deterministische Verarbeitung der Log-Daten und Datenschutz.
Aufgabenstellung Auflistung der einzelnen Ziele und Anforderungen	• H6 Visualisierung der Daten • H8 Datenschutzkonforme Behandlung von Nutzerdaten • H9 Vergleichen verschiedener SIEM-Lösungen • O2 Überprüfung der angewendeten Anonymisierung

3 Projektorganisation

3.1 Grafische Darstellung (Empowered Projektorganisation)

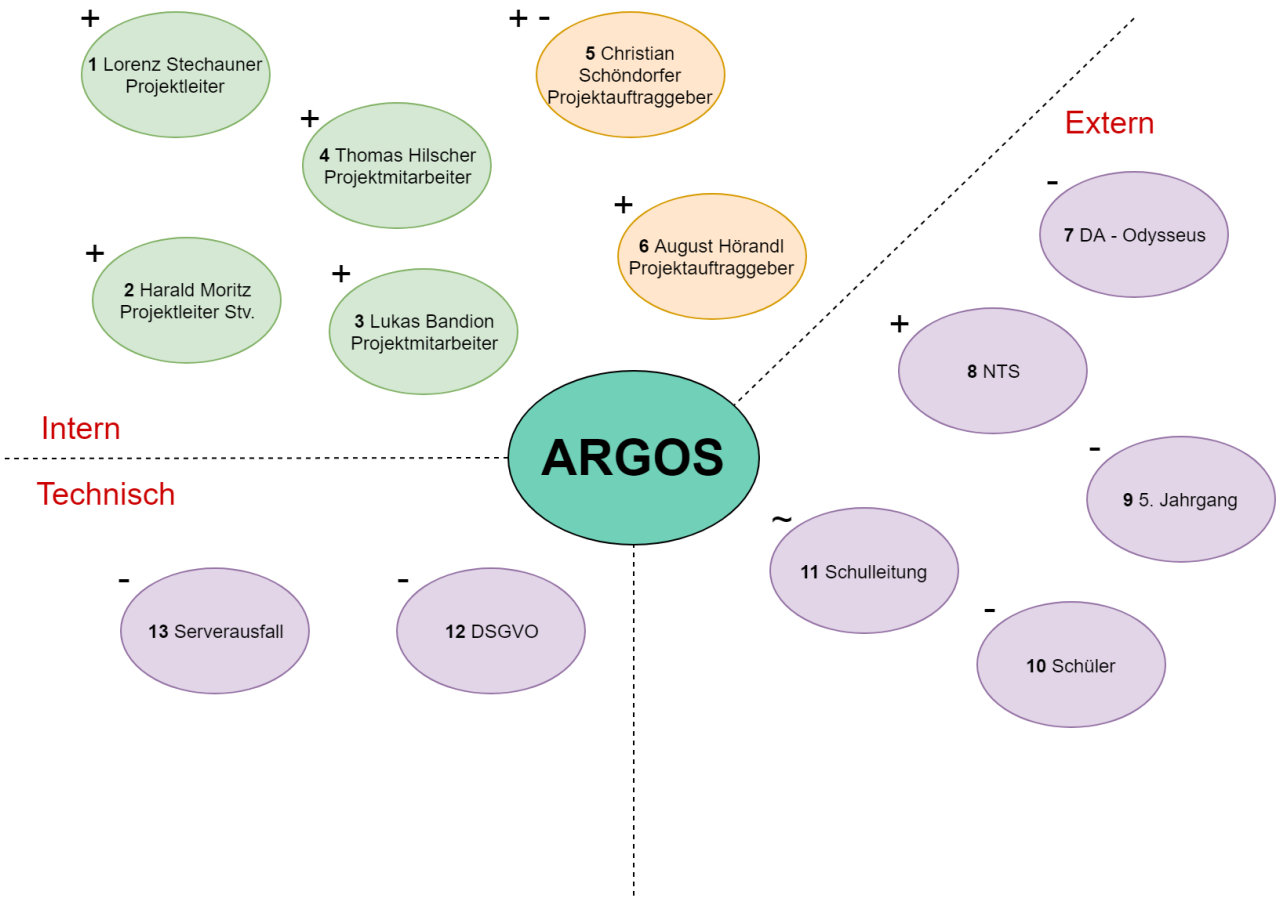


3.2 Projektteam

Funktion	Name	Kürzel	E-Mail
PL	Lorenz Stechauner	STE	lorenz.stechauner@htl.rennweg.at
PL Stv.	Harald Moritz	MOR	harald.moritz@htl.rennweg.at
PMA	Lukas Bandion	BAN	lukas.bandion@htl.rennweg.at
PMA	Thomas Hilscher	HIL	thomas.hilscher@htl.rennweg.at

4 Projektumfeldanalyse

4.1 Grafische Darstellung



Beschreibung der wichtigsten Umfelder

#	Bezeichnung	Beschreibung	Bewertung
1	Lorenz Stechauner	Lorenz Stechauner ist durch die Erfahrungen, die er in einem vorherigen Projekt namens Inginious gewonnen hat, der perfekte Projektleiter für unser Team.	+
2	Harald Moritz	Schon in jungen Jahren ist Harald Moritz durch seine Programmierkenntnisse hervorgestochen, was ihn zum perfekten Mann zur ASA-Logverarbeitung macht.	+
3	Lukas Bandion	Durch sein starkes Interesse im Bereich der Deep Packet Inspection, hat sich Lukas Bandion als der perfekte Kandidat herausgestellt, die Diplomarbeitsziele in diesem Bereich zu übernehmen.	+
4	Thomas Hilscher	Thomas Hilscher hat durch sein Interesse an der Europäischen Datenschutzgrundverordnung, die Aufgabe übernommen sich über diese zu informieren und darauf zu achten, dass das Diplomarbeitsprojekt im Einklang mit dem Recht steht.	+
5	Christian Schöndorfer	Christian Schöndorfers umfangreiches Wissen im Bereich der Netzwerktechnik erleichtert dieses Projekt ungemein. Jedoch ist Christian Schöndorfer durch seine wichtige Rolle an der Schule und der Tatsache, dass er sehr viele Diplomarbeitsprojekte betreut, oftmals schwer zu erreichen.	+-
6	August Hörandl	Ist durch seine Open-Source Affinität ein Experte auf den Gebieten Linux und Git. Weiters ist August Hörandl durch seine vielen Jahre Erfahrung hinsichtlich Softwareentwicklung, der perfekte Ansprechpartner bei Programmierfragen.	+
7	DA-Odysseus	Das Diplomarbeitsteam Odysseus hat durch die Umstrukturierung der Authentifizierungsmethode des WLANs der Schule es erheblich schwerer gemacht unsere Anwendung mit Echtdaten zu befüllen.	-
8	NTS	Steht dem Team bei Fragen zur Verfügung und setzt sich sehr für das Gelingen unserer Diplomarbeit ein.	+
9	5. Jahrgang	Da das Projektteam neben den Arbeiten am Projekt auch noch die 5. Klasse besucht, kann es öfters vorkommen, dass es Wochen gibt, in denen wenig bis nichts am Projekt gearbeitet werden kann.	-

10	Schüler	Schüler der HTL Rennweg haben mehr oder weniger freien Zugang zum Serverraum, in welchem wir unsere Spielwiese und unserem Server stehen haben und könnten Kabel ab-/umstecken oder Geräte abdrehen.	-
11	Schulleitung	Die Schulleitung könnte durch kurzfristige Änderungen der Anforderungen an die Diplomarbeit Chaos in das Projekt bringen.	~
12	DSGVO	Wir fallen mit den Zielen unseres Projekts genau in die Zuständigkeit der Datenschutzgrundverordnung. Diese beinhaltet sehr strenge Richtlinien bezüglich des Speicherns von Nutzerdaten.	-
13	Serverausfall	Es kann aufgrund von technischen Störungen zu einem Ausfall des Servers, auf dem unsere Software läuft, kommen und dadurch das Arbeiten sehr einschränken.	-

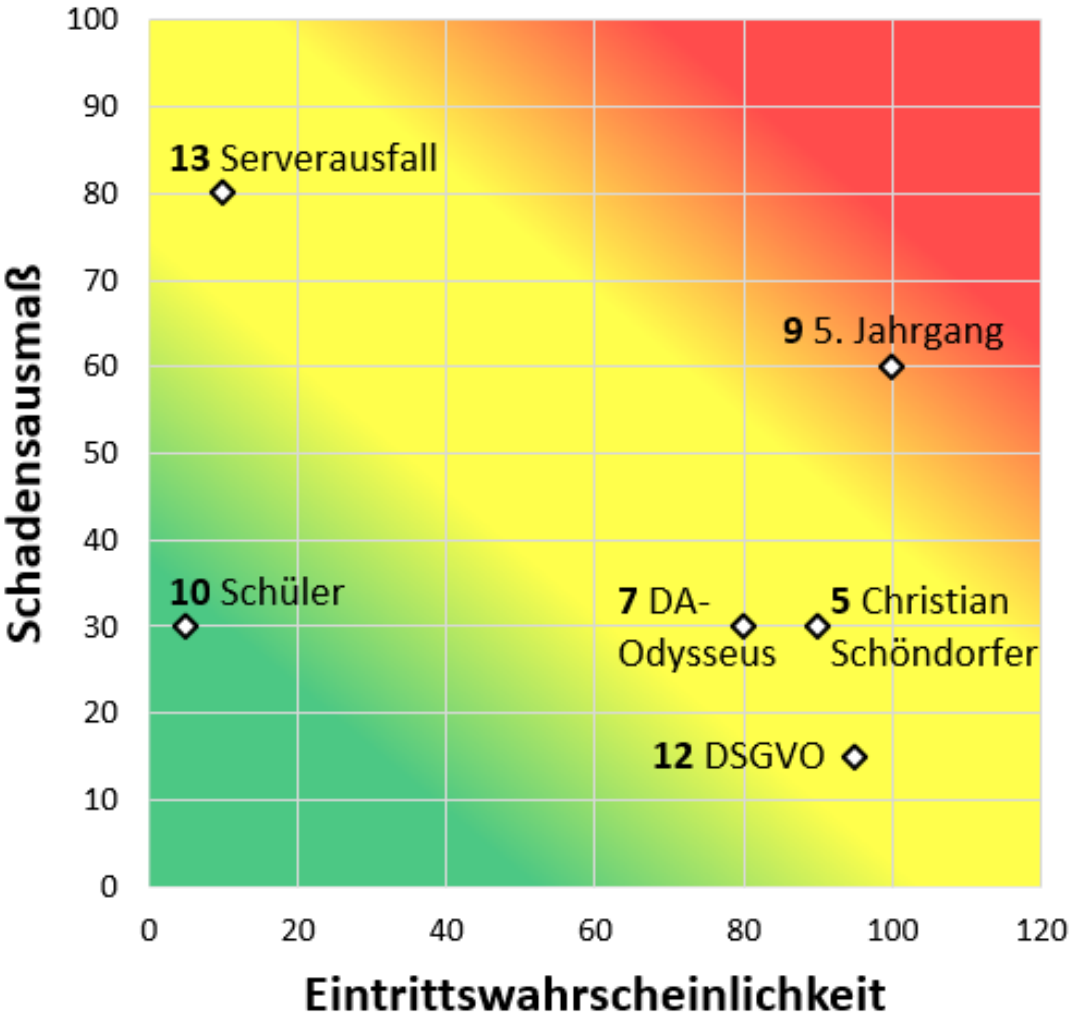
5 Risikoanalyse

5.1 Beschreibung der wichtigsten Risiken

#	Bezeichnung	Beschreibung des Risikos	P	A	RF
5	Christian Schöndorfer	Durch Christian Schöndorfers wichtige Rolle an der Schule und der Tatsache, dass er sehr viele Diplomarbeitsprojekte betreut, kann es immer wieder zu Zeitproblemen kommen.	90	30	2700
7	DA-Odysseus	Das Diplomarbeitsteam Odysseus hat durch die Umstrukturierung der Authentifizierungsmethode des WLANs der Schule es erheblich schwerer gemacht unsere Anwendung mit Echtdaten zu befüllen.	80	30	2400
9	5. Jahrgang	Da das Projektteam neben den Arbeiten am Projekt auch noch die 5. Klasse besucht, kann es öfters vorkommen, dass es Wochen gibt, in denen wenig bis nichts am Projekt gearbeitet werden kann.	100	60	6000
10	Schüler	Schüler der HTL Rennweg haben mehr oder weniger freien Zugang zum Serverraum, in welchem wir unsere Spielwiese und unserem Server stehen haben und könnten Kabel ab-/umstecken oder Geräte abdrehen.	5	30	150
12	DSGVO	Wir fallen mit den Zielen unseres Projekts genau in die Zuständigkeit der Datenschutzgrundverordnung. Diese beinhaltet sehr strenge Richtlinien bezüglich des Speicherns von Nutzerdaten.	95	15	1425
13	Serverausfall	Es kann auf Grund von technischen Störungen zu einem Ausfall des Servers, auf dem unsere Software läuft, kommen und dadurch das Arbeiten sehr einschränken.	10	80	800

P...Eintrittswahrscheinlichkeit des Risikos
A...Schadensausmaß bei Eintritt des Risikos
RF...berechneter Risikofaktor

5.2 Risikoportfolio



5.3 Risiko Gegenmaßnahmen

#	Bezeichnung	Gegenmaßnahme
5	Christian Schöndorfer	Es muss darauf geachtet werden, anstehende Meetings möglichst früh anzukündigen und dafür eine E-Mail mit einem Outlook-Termin zu versenden.
7	DA-Odysseus	Es sollte in regelmäßigen Abständen nachgefragt werden wie es momentan vorangeht, um einerseits den Ist-Stand zu erfahren aber andererseits auch anklingen zu lassen, dass wir daran interessiert wären, dass die Authentifizierungsmethode geändert wird.
9	5. Jahrgang	Es sollte bereits in den ersten Schulwochen möglichst viel Zeit in die Diplomarbeit investiert werden
10	Schüler	Es muss darauf geachtet, dass keine Kabel zu einladend aus dem Serverrack hängen, damit andere Schüler nicht zu sehr dazu verleitet werden sie abzustecken. Der Serverschrank sollte verschlossen bleiben.
12	DSGVO	Es ist ein Hauptziel der Diplomarbeit, datenschutzkonform zu arbeiten, daher nur die notwendigsten Daten zu speichern und wenn nötig Daten zu pseudonymisieren.
13	Serverausfall	Es sollte darauf geachtet werden, dass ein Ausfall möglichst früh erkannt wird und dadurch das schlimmste verhindert werden kann.

6 Meilensteinliste

Darstellung der Meilensteine mit geschätzten Terminen

Datum	Meilenstein
23.09.2019	Initiale Verarbeitung der Logs abgenommen
14.10.2019	Konzept für Query Language abgenommen
28.10.2019	Port Mirror (Deep Packet Inspection) abgenommen
25.11.2019	Implementierung der Query Language abgenommen
02.12.2019	Deep Learning Konzept abgenommen
16.12.2019	Visualisierung abgenommen
30.12.2019	Erste Version Diplomarbeitsbuch fertiggestellt
10.02.2019	Diplomarbeitsbuch fertiggestellt
30.03.2020	Diplomarbeit abgenommen

7 Projektressourcen

7.1 Projektressourcen: Soll-Ist-Vergleich

SOLL Bereich	IST
Know-how im Bereich Datenbanken	Teilweise vorhanden
Know-how im Bereich Deep Learning	Nicht ausreichend
Know-how im Bereich Packet Capture	Nicht ausreichend
Know-how im Bereich Python	Vorhanden
Know-how im Bereich Visualisierung	Teilweise vorhanden
Software (Entwicklungsumgebungen)	Vorhanden
Hardware (Server)	Vorhanden

7.2 Personelle Ressourcen

#	Teammitglied	Personenstunden
1	Lorenz Stechauner	200
2	Harald Moritz	200
3	Lukas Bandion	200
4	Thomas Hilscher	200
SUMME		800

7.3 Budget

7.3.1 Auflistung der Aufwände für die Durchführung der Diplomarbeit

Pos.	Bezeichnung des Aufwands	Kosten
1	Domain-Only-Kosten für DA-Website	13,90€
2	Krawatten in Teamfarbe	37,90€
-	Gesamtkosten	51,80€

7.3.2 Kostendeckung

Die Gesamtkosten für das Projekt werden vom Projektteam übernommen.

8 Geplante externe Kooperationspartner

Zwischen der „NTS Netzwerk Telekom Service AG“, kurz NTS und dem Projektteam besteht eine unverbindliche Kooperation. Die NTS unterstützt das Team mit technischem Know-how sowie mit Lizenzen und Hardware, falls etwas davon benötigt wird. Als beiderseitiges Ziel für die Zusammenarbeit wird das Knüpfen von Kontakten gesehen.

9 Geplante Verwertung der Ergebnisse

Der Auftragnehmer räumt dem Kunden das unwiderrufliche sowie zeitlich, örtlich und sachlich unbeschränkte Nutzungsrecht an dem für den Kunden geschaffenen Werk ein ("Werknutzungsrecht").

Das Werknutzungsrecht berechtigt den Kunden, das geschaffene Werk auf jede bekannte oder zukünftig bekannt werdende Art zu nutzen, insbesondere das geschaffene Werk im Rahmen der Nutzung zu vervielfältigen, zu verbreiten, drahtlos oder drahtgebunden zu senden und aufzuführen sowie zur Verfügung zu stellen (§18a UrhG).

Der Kunde ist berechtigt, das geschaffene Werk selbst oder durch Dritte zu bearbeiten und diese Bearbeitung im selben Umfang zu nutzen (“Werkbearbeitungsrecht”).
Die Urheberrechte am Quellcode verbleiben beim Urheber.