Höhere Technische Bundeslehranstalt Wien 3
Rennweg 89b, A -1030 Wien, www.htl.rennweg.at

Ansuchen um Zulassung zur Diplomarbeit

Maturajahrgang:	2020	Projektnummer:	

Projektthema (Arbeitstitel):

Netzwerkanalyse eines Enterprise-Netzwerks (Argos)

Projektteam:

Schülerin/Schüler	Klasse	Individuelle/r Betreuer/in	Unterschrift Schüle-rin/Schüler
Projektleiterin/Projektleiter **Lorenz Stechauner**	4CN	HOR	
Stellv. Projektleiterin/Projektleiter Harald Moritz	4CN	HOR	
Lukas Bandion	4CN	SDO	
Thomas Hilscher	4CN	SDO	

Projektbetreuung:	Unterschrift Betreuung
Individuelle Betreuung ~~(Hauptbetreuung)~~ **Christian Schöndorfer**	
Individuelle Betreuung ~~(Hauptbetreuung Stv.)~~ August Hörandl	
Individuelle Betreuung:	
Individuelle Betreuung:	

Projektvergabe (durch AV):

Hauptbetreuung:	
HB Stellvertretung:	
Indiv. Betreuungen:	

Bewilligt (Unterschrift AV):

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: 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 H3: Speicherung der Log-Daten

Eine für alle anfallenden Log-Daten geeignete Speicherlösung wird ausgewählt und implementiert. Die Speicherlösung muss auf Datenmengen, die in größeren Netzen (z.B. Schulnetz) anfallen ausgelegt sein, ohne die Leistungsfähigkeit zu vermindern.

Ziel H4: „Website-of-the-Day“

Die am meisten aufgerufene Website im Netzwerk eines gewissen Zeitraums (z.B. Tag) wird mit einem Programm aus den gespeicherten Log-Daten ermittelt. Verwendet werden könnten DNS-Abfragen oder noch unverschlüsselte Daten aus dem TLS Header.

Ziel H5: Ermittlung von TCP/UDP Sessions

Aus den gespeicherten Log-Daten wird mittels eines Programms eine Liste der TCP und UDP Sessions mit wichtigen Kenngrößen (z.B. Dauer, Datenvolumen, etc.) erstellt. Diese Liste ist für weitere Verarbeitungszwecke nötig.

Ziel H6: Zuordnung von Sessions zu Benutzern

Es wird ein Programm erstellt, welches Sessions und Benutzer/Räume einander zuordnen kann. Dies soll mittels angegeben Parameter (z.B. Benutzer, Session Id, Raum, Zeitraum, etc.) geschehen.

Ziel H7: 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 H8: Evaluierung des Einsatzes von Deep Packet Inspection

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 H9: Evaluierung des Einsatzes von Deep Learning

Es wird überprüft, ob und wie der Einsatz von *Deep Learning* bzw. *Machine Learning* dabei helfen kann Anomalien im Netzwerk bzw. Angriffe auf das Netzwerk zu erkennen.

Ziel H10: Vergleichen verschiedener KI-Systeme

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

2.2 Optionale Ziele

Ziel O1: Erstellung eines Webinterfaces

Ein einfaches Webinterface, mit dem der Administrator einen grundlegenden Überblick über den aktuellen Status des Netzwerks einsehen kann, wird erstellt. Das Interface stellt alle im Projekt ermittelten Nennwerte grafisch aufbereitet dar.

Ziel O2: Aufsetzen eines Deep Learning Clusters

Mögliche Cluster Technologien werden verglichen um eine möglichst geeignete Lösung für die Anforderungen des Projektes zu finden. Mit den EDV-Rechnern wird ein Cluster erstellt, welcher für das Trainieren von Deep Learning Modellen verwendet wird.

Ziel O3: Überprüfung der angewendeten Anonymisierung

Es werden diverse „Angriffe“ auf die eigenen Systeme ausgeführt um zu überprüfen, wie sicher die Anonymisierung (*Ziel H7*) der personen- und nutzerbezogenen Daten tatsächlich stattgefunden hat. Falls durch eine Analyse der Metadaten trotzdem Benutzer identifizierbar sind, wird versucht dieses Problem zu beheben.

2.3 NICHT Ziele

Ziel N1: Wartung

Nach Abschluss und Abnahme des Projektes wird das gesamte Team alle Teile der entstehenden 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 potentiellen Kunden näher zu bringen. Die Nutzung des Produktes soll auf entgeltlicher Basis stattfinden.

Individuelle Aufgabenstellungen der Teammitglieder im Gesamtprojekt

2.3.1 Lorenz Stechauner

Themenschwerpunkt	Deterministische Verarbeitung der Log-Daten und Speicherung der Log-Daten.
Aufgabenstellung Auflistung der einzelnen Ziele und Anforderungen	• Ziel H1 Sammlung der Log-Daten • Ziel H3 Speicherung der Log-Daten • Ziel H5 Ermittlung von TCP/UDP Sessions • Ziel O1 Erstellung eines Webinterfaces

2.3.2 Harald Moritz

Themenschwerpunkt	Aufbereitung von Log-Daten und Einsatz von Deep Learning.
Aufgabenstellung Auflistung der einzelnen Ziele und Anforderungen	• Ziel H2 Aufbereitung der ASA Log-Daten • Ziel H9 Evaluierung des Einsatzes von Deep Learning • Ziel O2 Aufsetzen eines Deep Learning Clusters • Ziel N1 Wartung

2.3.3 Lukas Bandion

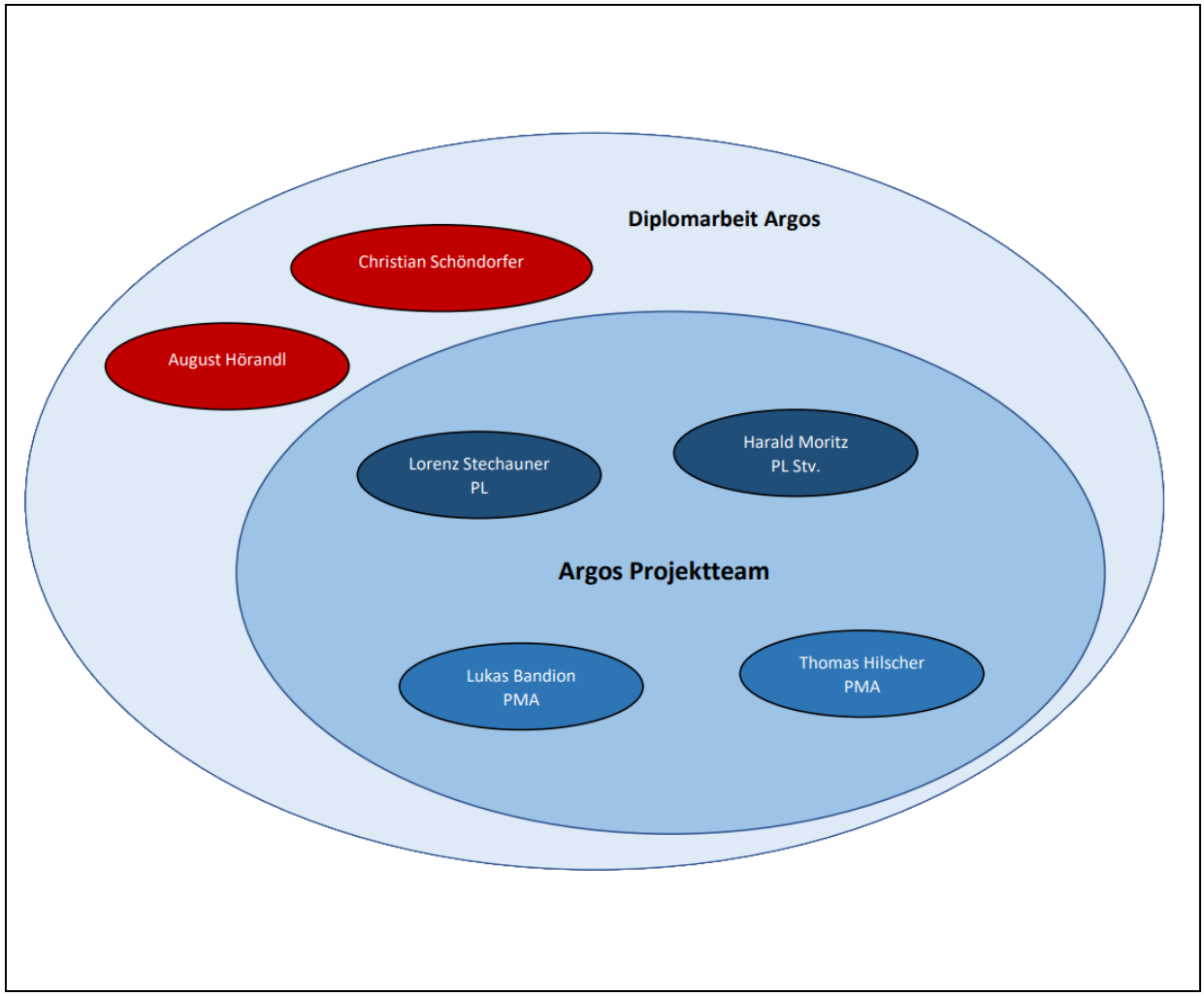
Themenschwerpunkt	Analyse von Deep Packet Inspection und Deep Learning.
Aufgabenstellung Auflistung der einzelnen Ziele und Anforderungen	• Ziel H8 Evaluierung des Einsatzes von Deep Packet Inspection • Ziel H10 Vergleichen verschiedener KI-Systeme • Ziel O3 Überprüfung der angewendeten Anonymisierung • Ziel N2 Änderungen am Schulnetzwerk

2.3.4 Thomas Hilscher

Themenschwerpunkt	Deterministische Verarbeitung der Log-Daten und Datenschutz.
Aufgabenstellung Auflistung der einzelnen Ziele und Anforderungen	• Ziel H4 „Website-of-the-Day“ • Ziel H6 Zuordnung von Sessions zu Benutzern • Ziel H7 Datenschutzkonforme Behandlung von Nutzerdaten • Ziel N3 Erstellen eines Produktes

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 Budget

4.1 Auflistung der Aufwände für die Durchführung der Diplomarbeit

Pos.	Bezeichnung des Aufwands	Bemerkung	Kosten
1	Domain-Only-Kosten für DA-Website	1-2 Jahre	30,00 €
2	„Argos“ Visitenkarten	200 Stk.	40,00 €
Gesamtkosten			**70,00 €**

4.2 Kostendeckung

Die Gesamtkosten für das Projekt werden vorübergehend vom Projektteam übernommen.

5 Geplante externe Kooperationspartner

Es ist im Moment nicht geplant mit externen Kooperationspartnern zusammen zu arbeiten.

6 Geplante Verwertung der Ergebnisse

Das Team wird das Projekt zur eigenen Weiterbildung verwenden, es ist nicht angedacht die diversen Programme zu veröffentlichen bzw. als Produkt zu verkaufen. Bei Nachfrage könne die Programme auch nachfolgenden Diplomarbeiten bzw. Lehrpersonen zur Verfügung gestellt werden.