



# A Walk on the Web's Wild Side

PROJEKTDOKUMENTATION

für die Vorlesung

**angewandtes Projektmanagement**

des Studiengangs Informatik  
Studienrichtung Angewandte Informatik

an der

Dualen Hochschule Baden-Württemberg Karlsruhe

von

**Daniel Brown**

Abgabedatum 22. Mai 2017

**Bearbeitungszeitraum**

12 Wochen

**Matrikelnummer**

3788021

**Kurs**

TINF14B2

**Betreuer der Studienarbeit**

Dr. Martin Johns

**Betreuer der Dokumentation**

Michael Vetter

# **Erklärung**

(gemäß §5(3) der „Studien- und Prüfungsordnung DHBW Technik“ vom 29.9.2015)

Ich versichere hiermit, dass ich diese Ausarbeitung selbstständig verfasst habe.

---

Karlsruhe, den 22. Mai 2017  
Ort, Datum

---

*Daniel Brown*  
Name

# Inhaltsverzeichnis

<b>Abbildungsverzeichnis</b>	<b>IV</b>
<b>Tabellenverzeichnis</b>	<b>V</b>
<b>1 Randbedingungen dieser Ausarbeitung</b>	<b>1</b>
<b>2 Projektdefinition</b>	<b>2</b>
2.1 Rahmenbedingungen . . . . .	2
2.2 Problemstellung . . . . .	2
2.3 Projektziel . . . . .	3
2.4 Anforderungen . . . . .	3
2.5 Team und Zuständigkeiten . . . . .	4
2.6 Vision . . . . .	4
<b>3 Projektplanung</b>	<b>6</b>
3.1 Terminplan . . . . .	6
3.2 Risikomanagement . . . . .	6
3.3 Arbeitsmittel . . . . .	7
<b>4 Projektdurchführung</b>	<b>9</b>
4.1 Schreiben der Studienarbeit . . . . .	9
4.2 Probleme . . . . .	10
<b>5 Qualitätssicherung</b>	<b>12</b>
5.1 Entwicklung der Anwendung . . . . .	12
5.2 Schreiben der Studienarbeit . . . . .	13
<b>6 Projektabschluss</b>	<b>15</b>
6.1 Übergabe . . . . .	15
6.2 Erkenntnisse . . . . .	16

<b>A Dokumente</b>	<b>VII</b>
A.1 Themenmitteilung zur Studienarbeit . . . . .	VIII
A.2 Vorgaben Einheit Studienarbeit . . . . .	IX
A.3 Autoren der einzelnen Kapitel . . . . .	X
<b>B E-Mails</b>	<b>XIV</b>
B.1 Terminvorschlag Mo 06.03. 12:15 Uhr (16.02. - 06.03.) . . . . .	XV
B.2 webifier-mail (16.03.) . . . . .	XVI
B.3 Analysephase gestartet & Ausarbeitung nimmt Gestalt an (30.03. - 02.04.)	XVII
B.4 Abuse Hinweis (05.04.) . . . . .	XVIII
B.5 Internes Meeting & Folgetermin (24.04. - 26.04.) . . . . .	XXII
B.6 Termine Studienarbeit (24.04. - 03.05.) . . . . .	XXIII
B.7 Erstattung Kosten des Servers für Studienarbeit (24.04. - 12.05.) . . . . .	XXIV
B.8 Verlängerung Abgabe Studienarbeit (13.05.) . . . . .	XXVI
B.9 Korrekturlesen Studienarbeit (16.05. - 17.05.) . . . . .	XXVII
B.10 Abgabe Studienarbeit (22.05.) . . . . .	XXIX
<b>C Protokolle</b>	<b>XXX</b>
C.1 Dokumentation der Meetings . . . . .	XXXI

## **Abbildungsverzeichnis**

1	<i>SecuritySquad</i> - Logo . . . . .	4
2	<i>webifier</i> - Logo . . . . .	5

## Tabellenverzeichnis

1	Terminplan . . . . .	6
2	Risiken . . . . .	7

# 1. Randbedingungen dieser Ausarbeitung

In dieser Arbeit werden alle Projektmanagement-relevanten Aspekte eines Softwareentwicklungsprojektes im Rahmen einer Studienarbeit beschrieben. Die Dokumentation wird zur Leistungsmessung der Vorlesung *angewandtes Projektmanagement* angefertigt und von Michael Vetter betreut. Da diese Vorlesung im sechsten Semester besucht wird, liegt der Fokus der Ausarbeitung auf der zweiten Hälfte des Projekts.

## 2. Projektdefinition

Dieses Kapitel beschreibt zunächst die Rahmenbedingungen des Projekts. Danach wird auf das Ziel sowie auf das Projektteam und dessen Lösungsansatz eingegangen.

### 2.1. Rahmenbedingungen

Der Name der Studienarbeit lautet *A Walk on the Web's Wild Side*. Es findet im Rahmen eines dualen Studiums an der DHBW Karlsruhe statt. Es wird über die Theoriephasen des fünften und sechsten Semesters durchgeführt, wobei dazwischen eine Praxisphase im ausbildenden Betrieb der Studenten stattfindet. Die Dauer des Projekts beträgt somit sechs Monate. Es werden offiziell für jedes Semester 150 Stunden Regelarbeitsaufwand vorgesehen. Bei dem Projekt handelt es sich um ein Softwareentwicklungsprojekt, in dem eine Webanwendung konzipiert und umgesetzt wird.

### 2.2. Problemstellung

Durchschnittliche Nutzer sind heutzutage im World Wide Web ein gefragtes Angriffsziel für webbasierte Angriffe. Häufig wird hierfür der Nutzer auf maliziöse Webseiten gelockt. Diese Webseiten nutzen dann unter anderem Sicherheitslücken im Browser des Nutzers um Schadsoftware zu verbreiten oder den Anwender auszuspähen. Die Studienarbeit beschäftigt sich mit diesen Webseiten und analysiert deren Bedrohungs-potenzial.

## 2.3. Projektziel

Ziel des Projekts ist eine systematische Untersuchung der Aktivitäten von semi-legalen Webseiten im World Wide Web. Das erwartete Ergebnis ist ein Prüfportal, auf dem jene Webseiten automatisiert analysiert und Ergebnisse präsentiert werden sollen. Nach dem Erstellen einer Übersicht von interessanten Zielen, wie z.B. One-Click-Hoster oder File-sharing Seiten sollen ausgewählte Webseiten manuell untersucht werden. Außerdem sollen verschiedene Angriffsszenarien zur weiteren Prüfung ausgewählt werden. Der Untersuchungsprozess der Webseiten soll im Verlauf der Arbeit stückweise automatisiert und in den Rahmen einer Prüfanwendung gebracht werden. Abschließend sollen eine Vielzahl von Webseiten mit der Anwendung getestet und die Ergebnisse ausgewertet und dokumentiert werden.

## 2.4. Anforderungen

Durch die Aufgabenstellung und das Erstgespräch ergeben sich folgende Anforderungen:

**Prüfung auf clientseitiger Angriffe** bestimmte Webseiten sollen auf sicherheitsrelevante Schwachstellen und clientseitige Angriffe überprüft werden können.

**Tests in gesichertem Umfeld** Die Sicherheitstests müssen abgeschottet vom Hauptsystem laufen, um vor Schadware und clientseitige Angriffe zu sein.

**Benutzerfreundliche Oberfläche** Die Anwendung muss von Durchschnittsnutzern benutzbar sein. Es sollen keine komplexen Formulare ausgefüllt und konfiguriert werden.

**Tests in gesichertem Umfeld** Die Sicherheitstests müssen abgeschottet vom Hauptsystem laufen, um vor Schadware und clientseitige Angriffe zu sein.

**Automatische Überprüfung** Die Durchführung der Sicherheitstests soll voll automatisch erfolgen.

**Darstellbarkeit der Ergebnisse** Die Ergebnisse der Analysephase sollen zur Dokumentation einsehbar sein.

## 2.5. Team und Zuständigkeiten

Das Entwicklerteam besteht aus drei Studenten der angewandten Informatik: Samuel Philipp, Daniel Brown und Jan-Eric Gaidusch. Daniel Brown ist für das Projektmanagement verantwortlich, Jan-Eric Gaidusch für die Testdurchläufe in der virtuellen Umgebung und Samuel Philipp für das Frontend. Der Verantwortliche ist nicht zwingend der Umsetzende, sondern lediglich erster Ansprechpartner. Der Name der Arbeitsgruppe ist *SecuritySquad*<sup>1</sup>. Eine genauere Beschreibung der Arbeitsgruppe kann auf der Webseite <https://www.securitysquad.de> eingesehen werden.

Abbildung 1 zeigt das Logo des Teams.



Abbildung 1.: *SecuritySquad* - Logo

Die Studienarbeit wird von Dr. Martin Johns betreut, der an der DHBW Karlsruhe die Vorlesung Datensicherheit hält. Hauptberuflich ist er Forscher eben dieses Gebietes am CEC Karlsruhe der SAP SE. 3

## 2.6. Vision

*webifier* ist eine Anwendung mit der Webseiten auf deren Seriosität und mögliche clientseitige Angriffe auf den Nutzer geprüft werden können. Sie besteht aus mehreren eigenständigen Teilanwendungen. Im Zentrum steht der Tester, welcher die einzelnen

---

<sup>1</sup> Der Name *SecuritySquad* ist angelehnt an den Titel des US-amerikanischen Actionfilms *SuicideSquad*.

Tests verwaltet, ausführt und anschließend die Ergebnisse auswertet. Jeder einzelne Test ist eine weitere isolierte Teilanwendung des Testers. So kann jeder Test unabhängig von allen anderen betrieben werden.



Abbildung 2.: *webifier* - Logo

*webifier* Plattform ist eine Webanwendung welche den Endnutzern eine grafische Oberfläche zur Verfügung stellt, um Webseiten zu überprüfen. Im Hintergrund nutzt die Plattform den Tester. *webifier* Mail ist ein Dienst mit dem Links aus E-Mails überprüft werden können. Anschließend erhält der Sender eine E-Mail mit den Resultaten zurück. Eine weitere Teilanwendung ist *webifier* Data. Sie stellt eine Schnittstelle für den Tester bereit, um alle Testergebnisse sammeln zu können. *webifier* Statistics ist die letzte Teilanwendung von *webifier*. Sie nutzt die vom Data-Modul gespeicherten Daten um Auswertungen aller Testergebnisse bereitzustellen.

## 3. Projektplanung

### 3.1. Terminplan

In diesem Abschnitt werden alle Phasen, Meilensteine und deren Termine tabellarisch in [Tabelle 1](#) aufgelistet.

Name	Beteiligte	Startdatum	Enddatum
Umsetzungsphase	Team	13.02.2016	26.03.2016
Startgespräch Semester 6	alle	06.03.2017	
Besprechung der schriftlichen Arbeit	alle	03.04.2017	
Analysephase	Team	27.03.2016	26.04.2016
Vorstellung der Analyseergebnisse	alle	24.04.2017	
Abschlussgespräch	alle	03.05.2017	
Fertigstellung der Studienarbeit	Team	05.05.2017	
Präsentation der Studienarbeit	Team	12.05.2017	
Gegenlesen der Studienarbeit	alle	05.05.2017	10.05.2017
Abgabe der Studienarbeit	Team		15.05.2017

Tabelle 1.: Terminplan

### 3.2. Risikomanagement

[Tabelle 2](#) listet Risiken auf. Zusätzlich gibt sie deren Auswirkungsgrad, Wahrscheinlichkeit und mögliche Maßnahmen an. Harmlose Risiken werden in **grün** dargestellt, gefährliche in **gelb** und fatale in **rot**

Risiko	Auswirkung	Wahrscheinlichkeit	Prävention & Schadensbegrenzung
Virtualisierungstechnik nicht sicher genug	hoch	gering	-
fehlendes Know-How	hoch	mittel	gutes Konzept, Betreuer fragen
Krankheit	mittel	mittel	Krankheit in Zeitplanung mit einplanen
Missverständniss mit Betreuer	mittel	hoch	regelmäßiger Austausch und Demos
Serverleistung zu gering	hoch	mittel	Upgrade oder Angebotswechsel
Zeitmangel des Teams	hoch	hoch	Prüfungsphase in Zeitplanung mit einplanen, Zusatzfeatures weglassen

Tabelle 2.: Risiken

### 3.3. Arbeitsmittel

Für die Entwicklung der Anwendung und das Schreiben der Studienarbeit wurden folgende Werkzeuge und Hilfsmittel verwendet:

**Laptop** Jedes Teammitglied besitzt einen Laptop um die Anwendung zu entwickeln und die Studienarbeit auszuarbeiten. Diese wurden privat beschafft.

**Entwicklungsumgebung** Jedes Teammitglied besitzt eine Programm auf dem Laptop, mit dem die Anwendung umgesetzt wird. Alle drei Mitglieder verwenden *IntelliJ IDEA* als Entwicklungsumgebung. Da es sich bei den Entwicklern um Studenten handelt, kann die Software kostenlos heruntergeladen und installiert werden.

**LaTeX-Editor** Die Arbeit wird in LaTeX geschrieben. Deshalb hat jedes Teammitglied ein Programm zur erleichterten Erstellung von Texten in ebendieser Sprache. Es werden die kostenlosen Tools *TeXclipse*, *Texmaker* und *TeXstudio* verwendet. Alle drei sind kostenlos nutzbar.

**einfacher Root-Server** Dieser wird von der Firma *netcup* für 12 Monate angemietet. Die Gebühren für den Server werden von der DHBW erstattet.

**leistungsstarker Root-Server** Dieser Server wird ebenfalls von der Firma *netcup* gestellt. Allerdings wird dieser nur für einen Monat gebucht, da er nur für die Analysephase gebraucht wird.

**GitHub** Für Versionskontrolle und Zusammenarbeit der Entwicklung und der wissenschaftlichen Arbeit wird die Plattform GitHub genutzt. Sie ist kostenlos und in die Entwicklungsumgebung integriert.

**Google Drive & Google Docs** Für Versionskontrolle in Dokumentation und Organisation wird der File-Sharing Dienst *Google Drive* genutzt. Um gemeinsam an einem Dokument zu arbeiten wird die Webanwendung *Google Docs* verwendet. Beide Hilfsmittel sind kostenlos, können aber in der Regel nur über einen Browser verwendet werden.

**Slack** Um miteinander zu kommunizieren wird der Chatservice *Slack* genutzt. Dieser ist ebenfalls kostenlos und bietet Integrationsmöglichkeiten für *GitHub* und *Google Drive* an.

**Google Hangouts** Meetings, die nicht persönlich abgehalten werden können, werden über *Google Hangouts* gehalten. Dabei handelt es sich um eine Webanwendung, hauptsächlich für Audio- und Videokonferenzen genutzt wird. Es bietet zusätzlich die Möglichkeit, seinen Bildschirm zu übertragen.

## 4. Projektdurchführung

Die Entwicklung der Webanwendung wird in der wissenschaftlichen Arbeit beschrieben, die im Rahmen des Projekts erstellt wurde. Diese kann im Internet auf <https://github.com/SecuritySquad/Studienarbeit/releases/download/abgabe/Studienarbeit.pdf> eingesehen werden.

### 4.1. Schreiben der Studienarbeit

Zur Anfertigung der Studienarbeit wird zunächst eine Gliederung erstellt. Jedes Teammitglied bekommt gleich viele Kapitel bzw. Abschnitte zugeteilt. Dabei wird darauf geachtet, dass die zu schreibenden Texte in Summe für alle etwa gleich lang sind und dass jeder einen etwa gleichen Anteil an Einleitung, Grundlagen, Konzept, Umsetzung, Analyse und Fazit hat.

Zu Beginn des zweiten Semesters sind lediglich einige Teile der Grundlagen fertig ausformuliert. Dies liegt daran, dass hauptsächlich an der Umsetzung der Anwendung sowie deren Zusatzfeatures gearbeitet wird. Es gibt keine festen Meilensteine für die Kapitel der Studienarbeit, sodass nicht auf eine mittelfristige Deadline hingearbeitet wird. Neben den regelmäßigen Videokonferenzen im Team und den Meetings mit dem Betreuer gibt es lediglich entwicklungsbezogene Meilensteine und Phasetermine.

Einen Monat vor Abgabe beginnt das Team deshalb konzentriert an der wissenschaftlichen Arbeit zu schreiben. Die Studienarbeit ist in sieben Kapitel unterteilt. Das erste Kapitel ist die Einleitung. Hier werden die Rahmenbedingungen für die Arbeit erläutert und es wird ein Einblick in die Hintergründe gegeben. Das nächste Kapitel, Grundlagen, behandelt Tools, die maßgeblich zur Entwicklung der Lösung verwendet werden. Weiterhin werden clientseitige Probleme bzw. Angriffspunkte fachlich aufbereitet, die in der Lösung angesprochen werden. Im dritten Kapitel werden die Ergebnisse des Entwurfsprozesses dargestellt und begründet. Dabei wird grundsätzlich zwischen der Gesamtanwendung und den Tests unterschieden. Diese Aufteilung findet sich auch im

darauffolgenden Kapitel, der Umsetzung, wieder. Dort wird hingegen auf die konkrete Implementierung des Konzepts eingegangen und bedeutende Anwendungslogik anhand von Codebeispielen erklärt. In Kapitel fünf, der Analyse, werden die Erkenntnisse der Arbeit präsentiert und danach beurteilt. Zum Abschluss der Arbeit werden in Ausblick und Fazit Ideen und Verbesserungsvorschläge für mögliche Folgeprojekte vorgetragen und die Arbeit abschließend bewertet.

## 4.2. Probleme

Jedes Mal, wenn ein Mitglied einen Abschnitt fertigstellt, veröffentlicht es seine Änderungen auf die Plattform *GitHub* über den Befehl `git push`. Dies funktioniert jedoch nicht immer, denn wenn in der Zwischenzeit ein anderer seine Änderungen veröffentlicht hat, dann müssen diese Änderungen zunächst auf die eigene Version angewandt werden. Dies geht im besten Fall über den Befehl `git pull`. Dabei werden alle reinkommenden Änderungen über einen Algorithmus eingepflegt. Schlägt der Algorithmus in einer Datei fehl, müssen die Änderungen auf die Datei manuell eingepflegt werden. Dieser Vorgang wird als *merge* bezeichnet und kann bei großen Änderungen sehr Zeitintensiv sein. Er wird über den Befehl `git merge` eingeleitet. Sind alle Änderungen übernommen, so kann die eigene Version des Projektes veröffentlicht werden.

Zudem gibt es Probleme beim kompilieren des Projektes. Nicht jeder benutzt die gleiche LaTeX-Distribution und Version, was dazu führt, dass das Projekt nicht auf jedem Entwicklerlaptop gebaut werden kann.

Am 05.04.2017 um 10:42 Uhr trifft aus heiterem Himmel eine Hinweismail des Serverproviders *netcup* ein. Der Mailverkehr zu diesem Thema ist in [Anhang B.4](#) zu finden. Das *Bundesamt für Sicherheit in der Informationstechnik* (BSI) habe Zugriffe auf einen ihrer *Honeypots* erkannt und den Server als *gekaperten Rechner* eingestuft. Dies ist nicht verwunderlich, da es das Ziel unserer Sicherheitstest ist, maliziöse Webseiten zu untersuchen. Wenn diese Seiten vom BSI übernommen werden und diese sich dann melden, ist kann dies als Zeichen des Erfolgs gesehen werden. Auch wenn der Schock zunächst Tief sitzt, muss schnell gehandelt werden. Denn ohne eine rasche Antwort würde der Server abgeschaltet werden. Aus diesem Grund wird ein Anruf bei *netcup* getätigt und die Lage geschildert. Der Server ist enorm sicher vor Angriffen, da die Anwendung so

aufgebaut ist, dass der einzige Kontakt mit den zu testenden Webseiten nur in abgeschotteten, virtuellen Umgebungen stattfindet. Nach diesem Gespräch wird der Server wieder als *unbedenklich* eingestuft und die Analysephase kann wie geplant fortgesetzt werden.

Die Analysephase geht länger als geplant, da der leistungsstarke Server ab und zu abstürzt und das System neu aufgesetzt werden muss. Glücklicherweise ist die Datenbank separat gespeichert, sodass bereits gespeicherte Testergebnisse nicht verloren gehen. Zusätzlich beginnt im Mai die Prüfungsphase, sodass das Team sich weniger um das Projekt kümmern kann. Aufgrund dieser Gegebenheiten muss die Fertigstellung der Arbeit weiter nach hinten verschoben werden.

## 5. Qualitätssicherung

Die folgenden Abschnitte schildern Maßnahmen die zur Sicherung der Qualität geplant und durchgeführt werden. Zunächst aber werden grundsätzliche Maßnahmen aufgelistet:

**Versionskontrolle in GitHub** Der Code der Anwendung und der Studienarbeit wird auf *GitHub* gesichert, sodass nachverfolgt werden kann, zu welchem Zeitpunkt welcher Code aktuell ist. Zudem ermöglicht es ein einheitliches Zusammenarbeiten im Team.

**Dokumente in Google Drive** Dokumente, die für das Projektmanagement und andere organisatorische Aufgaben wichtig sind, werden in *Google Drive* gespeichert. Dokumente können über *Google Docs* von mehreren Benutzern gleichzeitig, online und live bearbeitet werden. Zusätzlich ermöglicht es eine beschränkte Versionskontrolle aller Dokumente.

**regelmäßige Meetings mit dem Betreuer**

### 5.1. Entwicklung der Anwendung

Zur Qualitätssicherung der Software werden folgende Maßnahmen ergriffen:

**Einheitliches Ergebnisschema** Alle Tests müssen eine Antwort liefern, die in das Schema der Hauptanwendung pass. Die Struktur ist fest vorgegeben und wird bei jedem Testdurchlauf geprüft.

**Code Reviews** Bei kritischen Codestellen werden *Code Reviews* durchgeführt. Dabei wird der Code vom jeweiligen Entwickler mindestens einem anderen Teammitglied erklärt. Das Review wird über *Google Hangouts* gemacht, wobei darüber auch der Bildschirm übertragen wird.

**Pair Programming** Bei zentralen Codestellen, oder wenn ein Entwickler Unterstützung benötigt, wird zusammen im *Pair Programming* entwickelt. Dazu holt er sich mindestens einen weiteren Entwickler zur Hilfe und startet seine Videokonferenz in *Google Hangouts*. Nun übernimmt einer die Rolle des *Schreibers*, der andere wird zum *Denker*. Der *Schreiber* überträgt seinen Bildschirm und lässt sich vom *Denker* den Code diktieren. Nach einer gewissen Zeit werden die Rollen dann getauscht.

## 5.2. Schreiben der Studienarbeit

Um die Qualität der Studienarbeit sicherzustellen, werden folgende Maßnahmen ergriffen:

**Abkürzungsverzeichnis** Um häufig vorkommende Abkürzungen einheitlich zu schreiben, wird ein Abkürzungsverzeichnis angelegt. Die darin enthaltenen Abkürzungen werden per LaTeX-Befehl `\ac{ABK}` eingebunden und beim Kompilieren überprüft. Zusätzlich gibt es die Möglichkeit für generell häufig verwendete Begriffe ein *Glossar* anzulegen. Da die meisten häufig verwendeten Begriffe jedoch im Kapitel *Grundlagen* beschrieben werden, wird kein *Glossar* verwendet.

**Vorgaben für die Arbeit** Alle selbst erdachten, in der Arbeit verwendeten Begriffe werden in einem Dokument namens *Vorgaben Einheit Studienarbeit* eingetragen. Alle Teammitglieder haben sich an die dort festgelegten Konventionen und Schreibweisen zu halten. Dies wird vor Abgabe der Arbeit manuell überprüft. Das Dokument ist in [Anhang A.2](#) im Anhang zu finden.

**Gegenlesen kritischer Abschnitte** Alle selbst erdachten, in der Arbeit verwendeten Begriffe werden in einem Dokument namens *Vorgaben Einheit Studienarbeit* eingetragen. Alle Teammitglieder haben sich an die dort festgelegten Konventionen und Schreibweisen zu halten. Dies wird vor Abgabe der Arbeit manuell überprüft. Das Dokument ist in [Anhang A.2](#) im Anhang zu finden.

**Kompilierhinweise** Beim Kompilieren der Arbeit werden Fehler- und Warnhinweise ausgegeben. Fehler müssen völlig beseitigt werden, um überhaupt eine PDF generieren zu können. Warnungen hingegen werden nur teilweise behoben, da

darunter auch irrelevante Meldungen wie z.B. Underfull \hbox (badness 10000) in paragraph oder destination with the same identifier (namepage.1) has been already used, duplicate ignored sind.

**Zuordnung zwischen Autoren und Kapiteln** Um den Überblick über die Autoren der jeweiligen Kapitel und Abschnitte zu behalten, wird eine Liste der Verantwortlichen erstellt. Diese ist in [Anhang A.3](#) abgebildet.

## 6. Projektabschluss

Dieses Kapitel beschreibt die Schlussaktivitäten und gibt eine Zusammenfassung des Projekts.

### 6.1. Übergabe

Nach Fertigstellung der Arbeit wird diese von jedem Teammitglied in Moodle hochgeladen. Die selbe Version wird per E-Mail an den Betreuer zur Bewertung eingereicht. Außerdem werden für jedes Mitglied zwei Druckfassungen erstellt, wobei eine zur Abgabe für das Sekretariat der DHBW und die andere für den persönlichen Gebrauch gedacht sind.

Die Rechte der Entwicklergruppe auf *GitHub* bleiben zunächst im Besitz des Teams. Bei Fortführung des Projekts werden die entsprechenden Studenten aufgenommen. Der Server und somit auch die online Webanwendung wird bis Ende November weiterlaufen. Bei dem Zugriff auf diese verhält es sich wie bei der Entwicklergruppe. Die Berechtigung auf *Google Drive* und *Slack* bleiben ebenfalls wie gehabt.

Ein Backup der Datenbank wird rechtzeitig gesichert und an den Betreuer weitergeleitet. Die bei der Abgabe aktuelle Version der Anwendung *webifier* wird auf *GitHub* gekennzeichnet werden. Über diese Plattform können Interessenten die Software herunterladen und installieren. Mögliche zukünftige Studienarbeiten werden die Entwicklung ab dieser Version fortsetzen.

## 6.2. Erkenntnisse

Um ein angenehmes und gleichmäßiges Arbeitstempo zu gewährleisten müssen für alle anzufertigenden Artefakte möglichst kleine Meilensteine definiert werden, die nicht länger als einen Monat entfernt liegen sollten. Dies hätte den Verzug der Abgabe der Studienarbeit wesentlich gemindert bzw. ganz verhindert.

Regelmäßige Treffen mit Stakeholdern (vor allem Auftraggebern) helfen dabei, das Projekt nicht in eine falsche Richtung laufen zu lassen. Dabei sollten die erreichten Ergebnisse nicht nur theoretisch durchgesprochen werden, sondern auch möglichst praktisch gezeigt werden. Dies lässt sich bei Software am besten durch eine Demo bewerkstelligen.

## **A. Dokumente**

## A.1. Themenmitteilung zur Studienarbeit



Informatik

### Themenmitteilung zur Studienarbeit

Studiengang Informatik, DHBW Karlsruhe  
Erzbergerstr. 121, 76133 Karlsruhe

#### Modul T2\_3201, Theorie 5. + 6. Semester)

Studierende/r	Daniel Brown	Betreuer	Martin Johns
Kurs	TIN14B2	E-Mail	martin.johns@sap.com
Zusammen mit	Samuel Philipp Jan-Eric Gaidusch		

Titel der Arbeit	A walk on the Web's wild side
Typ der Arbeit	Softwareentwicklung
Problemstellung, Erwartetes Ergebnis	Anbieter von zwielichtigen Web-Angeboten greifen ihre User mit diversen Client-seitigen Methoden an.  Ziel der Arbeit ist eine systematische Untersuchung der Aktivitäten von semi-legalen Webseiten im WWW. Das erwartete Ergebnis ist ein Prüfportal, auf dem jene Webseiten automatisiert analysiert werden und Ergebnisse präsentiert werden.
Geplantes Vorgehen	<ul style="list-style-type: none"> <li>• Ermittlung einer Übersicht von interessanten Zielen, wie z.B. One-Click-Hoster oder File-sharing Sites.</li> <li>• Manuelles untersuchen der ausgewählten Webseiten.</li> <li>• Auswahl von zu beobachtenden maliziösen Aktionen, wie beispielsweise Malware Downloads, Phishing, JavaScript Intranet Angriffe, oder Browser Exploits.</li> <li>• Konzeption einer Evaluierungsplattform, basierend beispielsweise auf einem automatisch angesteuerten Web Browser in einer virtuellen Maschine.</li> <li>• Erforschung und Auswertung der verschiedenen Methoden und Dokumentation der Ergebnisse.</li> </ul>
Entwicklungsumgebung	IntelliJ IDEA, Java, Docker, YouTrack, GitHub
Literaturliste	c't Security 2016, EAN: 4018837009932 Primer on Client-Side Web Security, ISBN: 978-331-91222-6-7 Web security   MDN, <a href="https://developer.mozilla.org/en-US/docs/Web/Security">https://developer.mozilla.org/en-US/docs/Web/Security</a> The Honeynet Project, <a href="https://www.honeynet.org">https://www.honeynet.org</a>

## A.2. Vorgaben Einheit Studienarbeit

### Vorgaben Einheit Studienarbeit

SecuritySquad

Bilder: Abbildung

Listings: Listing/Codelisting/Codebeispiel

Kein \autoref sondern nur die Zahl als Link

Teilanwendungen/Teilkomponenten:

*webifier*

*webifier Statistics*

*webifier Mail*

*webifier Plattform*

*webifier Data*

*webifier Tester*

*webifier Tests*

---

Tests/Testarten:

*Virenscan der Webseite*

*Vergleich in verschiedenen Browsern*

*Überprüfung der Port-Nutzung*

*Überprüfung der IP-Nutzung*

*Prüfung aller verlinkten Seiten*

*Google Safe Browsing*

*Überprüfung des SSL-Zertifikats*

*Erkennung von Phishing*

*Screenshot der Seite*

---

Ergebnistypen/Ergebnis:

*CLEAN / unbedenklich*

*MALICIOUS / bedrohlich*

*SUSPICIOUS / verdächtig*

*UNDEFINED / unbekannt*

Auswertungen / Analysen / Grafiken

Gesamtauswertungen

Einzelanalysen

Direktzitate

Text,Tabelle oder Listing: Zitat Autor (Jahr) S. x Tabelle/Listing y

Bild: Siehe Autor (Jahr) S. x Abbildung y

## A.3. Autoren der einzelnen Kapitel

Auf den folgenden Seiten werden die Kapitel in den Farben der Autoren markiert. Dabei steht die Farbe gelb für Samuel Philipp, blau für Daniel Brown und grün für Jan-Eric Gaidusch.

---

Abstract

1 Einleitung

1.1 Aufbau der Arbeit

1.2 Aufgabenstellung

1.3 Team

1.4 webifier

2 Grundlagen

2.1 Frontend Technologien und Framework

- HTML
- CSS
- JavaScript
- jQuery
- Bootstrap

2.2 Backend Technologien und Frameworks

- Java
- Spring
- MongoDB
- Gradle
- Rest

- Docker
- R

## 2.3 Technologien und Frameworks der Tests

- - Python
- - PhantomJS
- - Bro
- - HTtrack
- - Resemble.js

## 2.4 Angriffstypen

### 2.4.1 Malware

### 2.4.2 Request Header Investigation

### 2.4.3 JavaScript Port & IP Scanning

### 2.4.4 Phishing

## 3 Konzept

### 3.1 Gesamtkonzept

#### 3.1.1 webifier Tests

#### 3.1.2 webifier Tester

#### 3.1.3 webifier Plattform

#### 3.1.4 webifier Mail

#### 3.1.5 webifier Data

#### 3.1.6 webifier Statistics

## 3.2 Testarten

### 3.2.1 Virenscan der Webseite

### 3.2.2 Vergleich in verschiedenen Browsern

3.2.3 Überprüfung der Port-Nutzung

3.2.4 Überprüfung der IP-Nutzung

3.2.5 Prüfung aller verlinkten Seiten

3.2.6 Google Safe Browsing

3.2.7 Überprüfung des SSL-Zertifikats

3.2.8 Erkennung von Phishing

3.2.9 Screenshot der Seite

## 4 Umsetzung

4.1 Gesamtsystem

4.1.1 webifier Tests

4.1.2 webifier Tester

4.1.3 webifier Plattform

4.1.4 webifier Mail

4.1.5 webifier Data

4.1.6 webifier Statistics

## 4.2 Tests

4.2.1 Virenscan der Webseite

4.2.2 Vergleich in verschiedenen Browsern

4.2.3 Überprüfung der Port-Nutzung

4.2.4 Überprüfung der IP-Nutzung

4.2.5 Prüfung aller verlinkten Seiten

4.2.6 Google Safe Browsing

4.2.7 Überprüfung des SSL-Zertifikats

4.2.8 Erkennung von Phishing

**4.2.9 Screenshot der Seite**

**5 Analyse**

**5.1 Gesamtauswertungen**

**5.2 Einzelauswertungen**

**5.2.1 Virenscan der Webseite**

**5.2.2 Vergleich in verschiedenen Browsern**

**5.2.3 Überprüfung der Port-Nutzung**

**5.2.4 Überprüfung der Port-Nutzung**

**5.2.5 Prüfung aller verlinkten Seiten**

**5.2.6 Google Safe Browsing**

**5.2.7 Überprüfung des SSL-Zertifikats**

**5.2.8 Erkennung von Phishing**

**5.3 Bewertung der Ergebnisse**

**6 Ausblick**

**7 Fazit**

## **B. E-Mails**

## B.1. Terminvorschlag Mo 06.03. 12:15 Uhr (16.02. -

**Subject:** Re: Terminvorschlag Mo 06.03. 12:15 Uhr

**From:** "Johns, Martin" <martin.johns@sap.com>

**Date:** 2017-02-16 15:01

**To:** Daniel Brown <dhw@djbrown.de>

**CC:** "team@securitysquad.de" <team@securitysquad.de>

Hallo,

Sorry, die andere Mail ist mir durchgerutscht. 6.3. ist gut. Habe ich mir eingetragen.

Viele Grüße  
Martin

---

**From:** Daniel Brown <dhw@djbrown.de>

**Date:** Thursday, February 23, 2017 at 4:00 PM

**To:** "Johns, Martin" <martin.johns@sap.com>

**Cc:** "team@securitysquad.de" <team@securitysquad.de>

**Subject:** Fwd: Terminvorschlag Mo 06.03. 12:15 Uhr

Hallo Martin,

hier nochmal unser Vorschlag als Reminder.

Viele Grüße

Daniel

----- Forwarded Message -----

**Subject:** Terminvorschlag Mo 06.03. 12:15 Uhr

**Date:** Thu, 16 Feb 2017 10:59:12 +0100

**From:** Daniel Brown <[dhw@djbrown.de](mailto:dhw@djbrown.de)>

**To:** Johns, Martin <[martin.johns@sap.com](mailto:martin.johns@sap.com)>

**CC:** [team@securitysquad.de](mailto:team@securitysquad.de) <[team@securitysquad.de](mailto:team@securitysquad.de)>

Hallo Martin,

am 27.02. sind wir nicht an der DH.

Bist du an einem anderen Wochentag noch an der DH?

Ansonsten würden wir Montag, den 06.03. 12:15 Uhr vorschlagen.

Viele Grüße  
Daniel

On 16.02.2017 10:40, Johns, Martin wrote:

> Hallo,  
>  
> Ich bin am kommenden Montag leider nicht in der DH. Wie sieht es bei Euch mit dem 27.02. aus?  
>  
> Gruß  
> Martin  
>  
> On 2/16/17, 8:55 AM, "Daniel Brown" <[dhw@djbrown.de](mailto:dhw@djbrown.de)> wrote:  
>  
> Hallo Martin,  
>  
> wir würden uns gerne mit dir treffen um unseren aktuellen Stand sowie  
> unser geplantes weiteres Vorgehen zu besprechen.  
>  
> Passt dir kommender Montag, den 20.02.2017 um 12:15?  
>  
> Viele Grüße  
>  
> Daniel  
>

## B.2 webifier-mail (16.03.)

**From:** Samuel Philipp <samuel@securityquad.de>

**Date:** 16.03.2017 10:24

**To:** "Johns, Martin" <martin.johns@sap.com>

**CC:** team@securitysquad.de

Hallo Martin,

gestern ist unser Mail-Service online gegangen. Gerne kannst du ihn  
testen: [check@webifier.de](mailto:check@webifier.de). Es werden bis zu 5 Links pro Mail getestet.  
Das Testen eines Links kann allerdings bis zu 5 Minuten dauern. Deshalb  
nicht wundern wenn es eine Weile dauert.

Viele Grüße,  
Samuel

## B.3. Analysephase gestartet & Ausarbeitung nimmt Gestalt an

Subject: Re: Analysephase gestartet | Ausarbeitung nimmt Gestalt an

From: "Johns, Martin" <martin.johns@sap.com>

Date: 03.03.2017 12:21

To: Daniel Brown <securitysquad@djbrown.de>

CC: "team@securitysquad.de" <team@securitysquad.de>

Alles klar. Dann bin ich mal gespannt. Bis morgen,  
Martin

On 3/30/17, 3:21 PM, "Daniel Brown" <[securitysquad@djbrown.de](mailto:securitysquad@djbrown.de)> wrote:

Hallo Martin,

seit Dienstag arbeitet unsere Anwendung auf Hochtouren daran die Blacklists durchzugehen.

Monitor: <https://monitor.webifier.de/>

Analysen: <https://statistics.webifier.de/>

Wir haben unsere Gliederung verfeinert und begonnen an der Ausarbeitung zu schreiben.

Gliederung:

[https://docs.google.com/document/d/1r5DZqAXD77c0aEAnJmmZ6ST\\_G04J1bgMrobC3ek5nZ0](https://docs.google.com/document/d/1r5DZqAXD77c0aEAnJmmZ6ST_G04J1bgMrobC3ek5nZ0)

Studienarbeit:

<https://github.com/SecuritySquad/Studienarbeit/blob/master/Studienarbeit.pdf>

Wir würden unsere Ergebnisse und das weitere Vorgehen gerne mit dir besprechen. Dazu möchten wir uns mit dir am kommenden Montag, den 03.04. um 12:00 Uhr mit dir treffen. Passt dir das?

Viele Grüße

Daniel

## B.4. Abuse Hinweis (05.04.)

Subject: Fwd: Abuse Hinweis zu v22016114014940435 - RS 1000 SAS G7 SE 12M

From: Samuel Philipp <samuel.philipp@t-online.de>

Date: 05.04.2017 10:59

To: "Johns, Martin" <martin.johns@sap.com>

CC: team@securitysquad.de

Hallo Martin,

ich hab gerade die angehängte Abuse-Mail von netcup bekommen und wollte dich jetzt mal nach deiner Meinung fragen. Ich hab unsere Blacklists mal geprüft und wir haben die aufgeführte Domain in unseren Blacklists, also ist es sehr wahrscheinlich, dass wir diese tatsächlich aufgerufen haben.

Soll ich dem Support einfach eine Antwort schreiben, in der ich unsere Studienarbeit und das Projekt erkläre, oder was würdest du tun?

Viele Grüße,  
Samuel

----- Weitergeleitete Nachricht -----

Betreff: Abuse Hinweis zu v22016114014940435 - RS 1000 SAS G7 SE 12M

Datum: Wed, 05 Apr 2017 10:42:01 +0200

Von: [abuse@netcup.de](mailto:abuse@netcup.de)

An: [samuel.philipp@t-online.de](mailto:samuel.philipp@t-online.de)

Guten Tag Samuel Philipp,

wir haben heute eine Abusemeldung betreffend Ihres Produkt v22016114014940435 - RS 1000 SAS G7 SE 12M erhalten. Einzelheiten dazu finden Sie am Ende dieser E-Mail.

Bitte prüfen Sie den geschilderten Sachverhalt und teilen Sie uns innerhalb von 14 Tagen mit, was die Ursache der Meldung ist. Sollten Sie uns nicht antworten oder weitere Abusemeldungen eintreffen, werden wir Ihr Produkt deaktivieren, um weiteren Schaden zu vermeiden.

Bitte beachten Sie, dass wir zur Sicherheit jeder Abusemeldung nachgehen müssen. Sollte der Grund für die Meldung nicht nachvollziehbar oder Sie nicht der Verursacher sein, benötigen wir dennoch eine Rückmeldung von Ihnen.

Abusemeldung:

[English version below]

Sehr geehrte Damen und Herren,

mit dieser E-Mail informieren wir Sie über Schadprogramm-Infektionen in Ihrem Netzbereich.

Strafverfolgungsbehörden haben international koordinierte Maßnahmen zur Deaktivierung der Botnetz-Infrastruktur 'Avalanche' durchgeführt. Die Infrastruktur wurde von Cyberkriminellen für die Steuerung zahlreicher Botnetze verwendet. Weitere Informationen hierzu finden Sie unter:

<<https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2016/>>

[Botnetz\\_Avalanche\\_01122016.html](#)

Im Zuge der durchgeführten Maßnahmen wurden Domänennamen, welche von Schadprogrammen in Bezug auf diese Botnetze zur Kontaktaufnahme mit einem Kontrollserver der Täter verwendet werden, auf so genannte 'Sinkholes' umgeleitet. Weitere Informationen zum Sinkhole-Verfahren finden Sie unter:

[<https://reports.cert-bund.de/schadprogramme>](https://reports.cert-bund.de/schadprogramme)

Ein Zugriff auf diese Sinkholes ist ein gutes Indiz, dass sich unter der Quell-IP-Adresse mit hoher Wahrscheinlichkeit ein System befindet, welches mit einem entsprechenden Schadprogramm infiziert ist. CERT-Bund erhält Protokolldaten dieser Sinkholes, um die zuständigen Netzbetreiber entsprechend informieren zu können.

Nachfolgend senden wir Ihnen eine Liste protokollierter Zugriffe auf die Sinkholes aus Ihrem Netzbereich. Neben IP-Adresse, Zeitstempel und Bezeichnung der Schadprogramm-Familie sind jeweils (soweit uns diese Daten vorliegen) Quell-Port, Ziel-IP-Adresse, Ziel-Port und Ziel-Hostname zu den einzelnen Verbindungen angegeben.

Eine Angabe der Schadprogramm-Familie "generic" bedeutet:

- a) Das betroffene System hat sich zu einem Domänenamen verbunden, welcher zur Avalanche-Botnetzinfrastruktur gehört, aber noch nicht eindeutig einer Schadprogramm-Familie zugeordnet werden konnte.  
oder
- b) Der HTTP-Request des betroffenen Systems enthielt keine Angabe eines Domänenamens. Daher kann auf der Sinkhole nicht ermittelt werden, welchen Domänenamen das System vorher aufgelöst hat, um sich zu der entsprechenden IP-Adresse zu verbinden.

Die meisten der hier gemeldeten Schadprogramme verfügen über Funktionen zum Identitätsdiebstahl (Ausspähen von Benutzernamen und Passwörtern) und/oder zur Manipulation der Kommunikation beim Online-Banking. Informationen zu den einzelnen Schadprogrammen sowie weitere Hilfe finden Betroffene unter:

[<https://www.bsi-fuer-buerger.de/avalanche>](https://www.bsi-fuer-buerger.de/avalanche)

Wir möchten Sie bitten, den Sachverhalt zu prüfen und entsprechende Maßnahmen zur Bereinigung der Systeme einzuleiten bzw. Ihre Kunden zu informieren.

Diese E-Mail ist mittels PGP digital signiert.

Informationen zu dem verwendeten Schlüssel finden Sie unter:

[<https://reports.cert-bund.de>](https://reports.cert-bund.de)

Bitte beachten Sie:

Dies ist eine automatisch generierte Nachricht. Antworten an die Absenderadresse [<reports@reports.cert-bund.de>](mailto:reports@reports.cert-bund.de) werden NICHT gelesen und automatisch verworfen. Bei Rückfragen wenden Sie sich bitte unter Beibehaltung der Ticketnummer [CB-Report#...] in der Betreffzeile an [<certbund@bsi.bund.de>](mailto:certbund@bsi.bund.de).

=====

Dear Sir or Madam,

this is a notification on systems on your network most likely infected with malware.

With an internationally coordinated operation, law enforcement agencies took down the 'Avalanche' botnet infrastructure. The infrastructure was used by cybercriminals for controlling various botnets. Additional information is available at:

[<https://www.europol.europa.eu/newsroom>](https://www.europol.europa.eu/newsroom)

In the course of this operation, domain names used by malware related to those botnets for contacting command-and-control servers operated by the criminals have been redirected to so called 'sinkholes'. Additional information on this technique is available at:

[<https://reports.cert-bund.de/en/malware>](https://reports.cert-bund.de/en/malware)

Any connection to a sinkhole is usually a good indicator for the host sending the request being infected with an associated malware. CERT-Bund receives log data from the sinkholes for notification of the responsible network operators.

Please find below a list of logged requests to the sinkholes from your networks. Each record includes the IP address, a timestamp and the name of the corresponding malware family. If available, the record also includes the source port, target IP, target port and target hostname for each connection.

A value of 'generic' for the malware family means:

- a) The affected system connected to a domain name related to the Avalanche botnet infrastructure which could not be mapped to a particular malware family yet.  
or
- b) The HTTP request sent by the affected system did not include a domain name. Thus, on the sinkhole it could not be decided which domain name the affected system resolved to connect to the respective IP address.

Most of the malware families reported here include functions for identity theft (harvesting of usernames and passwords) and/or online-banking fraud. Further information on the different malware families as well as additional help is available at:

[<https://www.bsi-fuer-buerger.de/EN/avalanche>](https://www.bsi-fuer-buerger.de/EN/avalanche)

We would like to ask you to check the issues reported and to take appropriate action to get the infected hosts cleaned up or notify your customers accordingly.

This message is digitally signed using PGP. Information on the signature key is available at:

[\(<https://reports.cert-bund.de/en/>\)](https://reports.cert-bund.de/en/)

Please note:

This is an automatically generated message. Replies to the sender address [<reports@reports.cert-bund.de>](mailto:reports@reports.cert-bund.de) will NOT be read but silently be discarded. In case of questions, please contact [<certbund@bsi.bund.de>](mailto:certbund@bsi.bund.de) and keep the ticket number [CB-Report#...] of this message in the subject line.

=====

Betroffene Systeme in Ihrem Netzbereich:  
Affected systems on your network:

Format: ASN,IP,Last seen (UTC),Malware,Source Port,Destination IP,Destination Port,Destination Hostname

"197540","188.68.39.59","2017-04-04  
23:42:06","ranbyus","55351","216.218.185.162","80","vrfkllxhaimrhrqpo.tw"

Mit freundlichen Grüßen / Kind regards  
Team CERT-Bund

Bundesamt für Sicherheit in der Informationstechnik (BSI)  
Referat CK22 - CERT-Bund  
Godesberger Allee 185-189  
D-53175 Bonn

Mit freundlichen Grüßen / best regards

Ihr netcup Team

---

netcup GmbH  
Daimlerstr. 25  
D-76185 Karlsruhe

Telefon: +49 721 / 7540755 - 0  
Telefax: +49 721 / 7540755 - 9

Kunden- und Interessenten-Hotline: 08000 netcup  
(Kostenlos aus dem Festnetz der Deutschen Telekom)

Web: [www.netcup.de](http://www.netcup.de)  
E-Mail: [mail@netcup.de](mailto:mail@netcup.de)

Handelsregister: HRB 705547, Amtsgericht Mannheim

Geschäftsführer (Executive directors):

- Dipl.-Ing. (BA) Felix Preuß
- Dipl.-Ing. (BA) Oliver Werner

USt.-IdNr. (VAT Reg. No.): DE262851304

---

## B.5. Internes Meeting & Folgetermin (24.04. - 26.04.)

Subject: Re: Meeting heute | Folgetermin  
**From:** Daniel Brown <[securitysquad@djbrown.de](mailto:securitysquad@djbrown.de)>  
**Date:** 26.04.2017 14:01  
**To:** "Johns, Martin" <[martin.johns@sap.com](mailto:martin.johns@sap.com)>, "team@securitysquad.de"  
<[team@securitysquad.de](mailto:team@securitysquad.de)>

Hallo Martin,

nächsten Mittwoch 12:00 Uhr passt 😊

Viele Grüße

Daniel

On 26.04.2017 10:54, Johns, Martin wrote:

Hallo Daniel,

Sorry, der Termin ist mir völlig aus der Aufmerksamkeit gerutscht. Ich bin kommende Woche Mittwoch an der DH und hätte um 12:00 Zeit.

Passt das bei Euch?

Viele Grüße  
Martin

On 4/24/17, 12:39 PM, "Daniel Brown" <[securitysquad@djbrown.de](mailto:securitysquad@djbrown.de)> wrote:

Hallo Martin,  
wir wollten uns ja heute um 12 Uhr mit dir treffen.  
Leider bist Du nicht da, deshalb haben wir die Zeit für ein Meeting unter uns genutzt.  
Wir möchten den Termin mit dir gerne nachholen.  
Nächste Woche Montag ist Feiertag.  
Wann würde es Dir passen?  
Viele Grüße  
Daniel

## B.6. Termine Studienarbeit (24.04. - 03.05.)

Subject: Termine Studienarbeit

**From:** Daniel Brown <securitysquad@djbrown.de>

**Date:** 03.05.2017 11:38

**To:** Martin Johns <martin.johns@sap.com>

**CC:** "team@securitysquad.de" <team@securitysquad.de>

Hallo Martin,

folgende Termine sind für die Studienarbeit festgelegt:

Angabe der Studienarbeit: Montag, den 15.05.2017

Angabe der Bewertung: Montag, den 29.05.2017

Viele Grüße

Daniel

## B.7. Erstattung Kosten des Servers für Studienarbeit

**(24.04.-12.05.)**

Hallo Herr Braun,  
es geht um die zweite Teilnahme am Wettbewerb „Gewinn eine tolle Reise“.  
Übrigens erhielt ich bis jetzt keine Reaktion von Ihnen, ob Sie eine Reise gewonnen haben.  
Falls bei der Nachfrage nach dem Gewinner eine Fehlermeldung erscheint, bitte Sie mich an.  
Fürstlich der Zusammenhang besteht, Seien Sie sicher, dass die E-Mail-Personen erreicht ist, falls das Problem weiterhin besteht, werden Sie sich an mich wenden.  
Viele Grüße  
Erico Hünberg

Von: Braun, Prof. Dr. Heinrich  
Gesendet: Freitag, 12. Mai 2017 13:52  
An: [team@securityquad.de](mailto:team@securityquad.de)  
Betreff: WIC: Kosten des Servers für Studienarbeit

Hallo Herr Hünberg,  
die Rechnung habe ich bereits erhalten.  
Sie haben meine eingeprägte, dass die Abrechnung mit der Verwaltung über Sie läuft.  
Viele Grüße  
Heinrich Braun

Von: Servat Philipp [team@securityquad.de](mailto:team@securityquad.de)  
Gesendet: Freitag, 12. Mai 2017 13:52  
An: [team@securityquad.de](mailto:team@securityquad.de)  
Betreff: Erstattung Kosten des Servers für Studienarbeit

Hallo Herr Braun,  
ich kann Ihnen schon mal meine Kontrakte, damit Sie den Betrag der Rechnung an mich überweisen können, sobald Sie diese erhalten haben.  
Bank Sparkasse Kielstrasse 4 2000 0115 22  
HIC: GENOGENSIEG  
Die Rechnung habe ich auch angehängt.  
Vielen Dank noch im Voraus.

Viele Grüße  
Samuel Philipp

----- Nachricht -----  
Betreff: WIC: Server für Studienarbeit - Rechnung  
Datum: Tue, 4 Apr 2017 07:42:45 +0000  
Von: Servat Philipp [team@securityquad.de](mailto:team@securityquad.de)  
An: Servat Philipp [team@securityquad.de](mailto:team@securityquad.de)  
Kopie (C): Braun, Prof. Dr. Heinrich [team@securityquad.de](mailto:team@securityquad.de)

Hallo Herr Philipp,  
Ihre Verzählung sollte die Erstattung des gesamten Betrags mit Begründung möglich sein, informiert sind sie schon mal. Kommen jetzt noch weitere Kosten oder kann das Projekt endgültig abgeschlossen werden? Die Erstattung wurde an Herrn Braun gehebt, der Ihnen nach Erhalt des Gelds auszahlt. Eine Erstattung direkt an Sie ist leider nicht möglich.

Viele Grüße  
Erico Hünberg

Von: Samuel Philipp [team@securityquad.de](mailto:team@securityquad.de)  
Gesendet: Montag, 2. April 2017 09:45  
An: Servat Philipp [team@securityquad.de](mailto:team@securityquad.de)  
Betreff: WIC: Server für Studienarbeit - Rechnung

Hallo Herr Philipp,  
Vielen Dank für Ihre Antwort. Zum Beipackzettel unserer letzten Mail an Prof. Dr. Braun aufgrund Ihrer Rechnung war der Server gerade im Angebot für knapp 44,99 €. Als wir Ihnen Ende März geschrieben und den Server bestellt haben war dieser leider nicht mehr im Angebot, weshalb der höhere Preis rückläufig kommt.  
Wäre es dennoch möglich den vollen Preis erstattet zu bekommen?  
Viele Grüße,  
Samuel Philipp  
Am 1. April 2017 08:15:15 MEZ schrieb [Erico.Huenberg@uni-kiel.de](mailto:Erico.Huenberg@uni-kiel.de):  
Hallo Herr Philipp,  
  
Sie hatten lediglich einen Betrag von 44,99 € vermerkt lassen, rechnen nun aber 54,99 € ab. Sicht es dafür eine Erklärung?  
  
Viele Grüße  
Erico Hünberg

Von: Samuel Philipp [team@securityquad.de](mailto:team@securityquad.de)  
Gesendet: Montag, 2. April 2017 09:45  
An: Servat Philipp [team@securityquad.de](mailto:team@securityquad.de)  
Cc: Braun, Prof. Dr. Heinrich [team@securityquad.de](mailto:team@securityquad.de)  
Betreff: WIC: Server für Studienarbeit - Rechnung

Hallo Herr Hünberg,  
Vielen Dank für die Bemerkung des Servers. Anbei habe ich die Rechnung zur Erstattung der Kosten.  
Vielen Dank schon mal im Voraus für Ihre Mühe.  
  
Viele Grüße,  
Samuel Philipp  
Am 23.03.2017 um 15:08 schrieb Hünberg, Erico:  
Hallo Herr Braun,  
  
Ich habe gerade mit der Verwaltung telefoniert. Der Betrag ist vorgenommen, die können den Server für einen Monat annehmen. Beachten Sie bitte, dass die Erstattung bis zu drei Monate dauern kann. Diese erfolgt über Ihren Prof. Dr. Braun. Bitte vergessen Sie die fristgerechte Kündigung nicht. Die Verrennung ist nur für einen Monat genehmigt!  
  
Viele Grüße und viel Erfolg  
Erico Hünberg

Von: Samuel Philipp [team@securityquad.de](mailto:team@securityquad.de)  
Gesendet: Dienstag, 3. April 2017 09:45  
An: Servat Philipp [team@securityquad.de](mailto:team@securityquad.de)  
Cc: Braun, Prof. Dr. Heinrich [team@securityquad.de](mailto:team@securityquad.de)  
Betreff: server für Studienarbeit

Hallo Herr Hünberg,  
für unsere Studienarbeit möchten wir nun den unten genannten Server benötigen.  
Soll der Server über die DEWIP oder direkt über uns (eine kleine Zeile mal) bezahlt werden?  
  
Viele Grüße  
Samuel Philipp  
----- Fazit/Ende Message -----  
Subject: WIC: Server für Studienarbeit  
X-Mailer: MailScanner (version 1.5.2)  
Date: Tue, 3 Apr 2017 13:58:59 +0000  
From: Servat Philipp [team@securityquad.de](mailto:team@securityquad.de)  
To: Daniel Braun [team@securityquad.de](mailto:team@securityquad.de)  
Cc: Jolana, Martin [team@securityquad.de](mailto:team@securityquad.de)  
Johanna, Martin [team@securityquad.de](mailto:team@securityquad.de)  
Braun, Prof. Dr. Heinrich [team@securityquad.de](mailto:team@securityquad.de)  
  
Hello Prof. Dr. Braun,  
  
Mit der Werte des Servers bin ich einverstanden.  
Bitte senden Sie sich wegen der Kostentabrechnung an unseren Lehrungsleiter, Herrn Müller.  
  
Viele Grüße  
Sehrlich Ihr  
  
Von: Jolana, Martin [team@securityquad.de](mailto:team@securityquad.de)  
Gesendet: Montag, 4. März 2017 09:45  
An: Servat Philipp [team@securityquad.de](mailto:team@securityquad.de)  
Cc: Daniel Braun [team@securityquad.de](mailto:team@securityquad.de)  
Braun, Prof. Dr. Heinrich [team@securityquad.de](mailto:team@securityquad.de)  
Betreff: WIC: Kosten des Servers für Studienarbeit

Hallo Prof. Dr. Braun,  
  
ich möchte hinzufügen, in meiner Funktion als Rektor der (noch vielversprechenden) Studienarbeit, diese Aufgabe unterstützen.  
  
Viele Grüße  
Martin  
  
From: Daniel Braun [team@securityquad.de](mailto:team@securityquad.de)  
Datum: Montag, 4. März 2017 09:45  
Uhrzeit: 09:45  
Von: Servat Philipp [team@securityquad.de](mailto:team@securityquad.de)  
Cc: "Jolana, Martin" [team@securityquad.de](mailto:team@securityquad.de)  
Braun, Prof. Dr. Heinrich [team@securityquad.de](mailto:team@securityquad.de)  
Betreff: WIC: Kosten des Servers für Studienarbeit

sehr geehrte Herr Prof. Dr. Braun,  
  
Ihre beiden unserer Studienarbeiten "WIC: Wiss' wie's geht" profitieren wir eine große Anzahl an Webseiten auf Angriffe. Da wir jedoch keine Möglichkeit haben, die Angriffe auf unsere Seiten zu erkennen, müssen wir diese Seiten weiterlassen, Leistungsgestarteten Mail-server liefern, da der bisherige Server nicht für unsere Analyse ausreicht.  
Daten zum Server:  
  
Address:  
saturn.ubm  
Website:  
<http://www.ubm.de>  
Name:  
RS 6000 07 BE  
Art:

# AW: Erstattung Kosten des Servers für Studienarbeit

Root-Server  
RAM:  
48 GB DDR4 RAM (ECC)  
Prozessor:  
Intel Xeon E5-2680V4, 12 Kerne, jeweils 2,4 GHz  
Festplatte:  
240 GB SSD  
Produktesite:  
<https://www.intel.com/de/bestellen/productinfo.php?product=153>  
Kosten:  
46,99 €  
Ist es möglich die Kosten von 46,99 € für den zusätzlichen Server von der DHHW erstattet zu bekommen, oder einen Server mit entsprechender Leistung gestellt zu bekommen?  
Viele Grüße  
Daniel Brown

--  
Diese Nachricht wurde von meinem Android-Mobiltelefon mit K-9 Mail gesendet.

## B.8. Verlängerung Abgabe Studienarbeit (13.05.)

Subject: AW: Verlängerung Abgabe Studienarbeit  
**From:** "Braun, Prof. Dr. Heinrich" <braun@dhwkarlsruhe.de>  
**Date:** 13.05.2017 23:05  
**To:** Samuel Philipp <samuel.philipp@t-online.de>  
**CC:** "team@securitysquad.de" <team@securitysquad.de>, "Johns, Martin" <martin.johns@sap.com>, Böcker, Nicole <boecker@dhwkarlsruhe.de>

Hallo Herr Philipp.

mit der Abgabe bis spätestens 22.05.17 bin ich einverstanden.

Viele Grüße  
Heinrich Braun

---

Von: Samuel Philipp [[samuel.philipp@t-online.de](mailto:samuel.philipp@t-online.de)]  
Gesendet: Samstag, 13. Mai 2017 18:49  
An: Braun, Prof. Dr. Heinrich  
Cc: [team@securitysquad.de](mailto:team@securitysquad.de); Johns, Martin  
Betreff: Verlängerung Abgabe Studienarbeit

Hallo Herr Braun,

wir (Jan-Eric Gaidusch, Daniel Brown und Samuel Philipp) würden gerne den Abgabetermin unserer Studienarbeit auf Montag, den 22. Mai 2017 verlängern, da wir in zeitliche Schwierigkeiten gekommen sind, weil die Analyse mehr Zeit in Anspruch genommen hat als geplant.

Vielen Dank schon mal im Voraus für Ihr Verständnis.

Viele Grüße,  
Samuel Philipp

## B.9. Korrekturlesen Studienarbeit (16.05. - 17.05.)

**Subject:** Re: Korrekturlesen Studienarbeit [\*]  
**From:** "Johns, Martin" <martin.johns@sap.com>  
**Date:** 17.05.2017 11:51  
**To:** "Samuel.Philipp@fiduciagad.de" <Samuel.Philipp@fiduciagad.de>  
**CC:** "team@securitysquad.de" <team@securitysquad.de>

Hallo,

Feedback:

Kapitel 1:

- 1.1 Umbenennen in "Struktur der Arbeit" oder so ähnlich
- Den Satz „Anbieter von zwielichtigen Web-Angeboten greifen ihre User mit diversen Client- seitigen Methoden an. Beispiele für solche Angriffe sind Malware Downloads, Phising, JavaScript Intranet Angriffe, oder Browser Exploits.“ aus 1.2 würde ich nach oben in die Motivation vor 1.1 nehmen, da passt er besser und macht die Motivation verständlicher.
- SAP AG gibt es nicht mehr, ist jetzt SAP SE ;)
- 1.4 ist gut

Kapitel 2.4

- Eventuell erst das Angreifermodell einführen. Also Attacker betreibt Web Site, User besucht diese, Angreifercode wird aus dem Netz auf den Rechner des Users geladen und von dessen Browser interpretiert, mögliche Angriffe erfolgen auf dem Rechner des Users (!) und in dessen internen Netz hinter der Firewall (!)
- 2.4.1 ist gut
- 2.4.2 ist kein Angriff an sich sondern ermöglicht nur eventuelle Angriffe. Ist also nicht auf der selben Ebene wie „Malware“ oder „Port Scanning“
- 2.4.3 Dieser Satz ist technisch falsch: „Beispielsweise kann dieser in Image- Tags versteckt werden, welche dann beim Laden der Seite aufgerufen werden.“ Außerdem wäre es hier relevant, wenn ihr beschreibt, wie das IP/Portscanning über JavaScript funktioniert
- 2.4.4 ist gut

Kapitel 5.3: Ist ok so. Kann man natürlich immer noch mehr schreiben. Da ich Euren Hauptbeitrag allerdings bei der grundsätzlichen Konzeption und Implementierung des Basis-Frameworks sehe, braucht es keine tiefere Analyse der Daten.

Kapitel 6 & 7: Sind gut.

Viele Grüße  
Martin

---

**From:** "Samuel.Philipp@fiduciagad.de" <Samuel.Philipp@fiduciagad.de>  
**Date:** Tuesday, May 16, 2017 at 10:59 AM  
**To:** "Johns, Martin" <martin.johns@sap.com>  
**Cc:** "team@securitysquad.de" <team@securitysquad.de>  
**Subject:** Korrekturlesen Studienarbeit [\*]

Hallo Martin,

wie du wahrscheinlich bereits weißt haben wir den Abgabetermin leider nicht einhalten können und werden dir die Endgültige Version am Montag zur Bewertung zuschicken. Vorab hier schon mal der fast fertig Entwurf. Gerne

würden wir noch auf dein Angebot zurückkommen Feedback für einzelne Teile der Arbeit zu erhalten. Uns wären hierfür die Kapitel 1 (Einleitung), 2.4 (Angriffstypen), 5.3 (Bewertung der Ergebnisse), 6 (Ausblick) und 7 (Fazit).

Wir würden uns freuen, wenn du uns dein Feedback, bzw. Verbesserungsvorschläge im Laufe dieser Wochen zukommen lassen könntest.

Viele Grüße,  
Samuel

(Siehe angehängte Datei: Studienarbeit.pdf)

Fiducia & GAD IT AG | [www.fiduciagad.de](http://www.fiduciagad.de)

AG Frankfurt a. M. HRB 102381 | Sitz der Gesellschaft: Hahnstr. 48, 60528 Frankfurt a. M. | USt-IdNr. DE 143582320

Vorstand: Klaus-Peter Bruns (Vorsitzender), Claus-Dieter Toben (stv. Vorsitzender),

Jens-Olaf Bartels, Martin Beyer, Jörg Dreinhöfer, Carsten Pfläging, Jörg Staff

Vorsitzender des Aufsichtsrats: Jürgen Brinkmann

## B.10. Abgabe Studienarbeit (22.2.05.)

Subject: Abgabe Studienarbeit [\*]  
**From:** Samuel.Philipp@fiduciagad.de  
**Date:** 22.05.2017 11:02  
**To:** "Johns, Martin" <martin.johns@sap.com>  
**CC:** team@securitysquad.de

Hallo Martin,

im Anhang befindet sich die finale Version unserer Studienarbeit, mit der Bitte um Korrektur. Dafür ist auch der Beurteilungsbogen, den wir bis zum 5. Juni in dreifacher Ausfertigung im Sekretariat abgeben müssen.

Vielen Dank schonmal und viele Grüße,  
Samuel

(Siehe angehängte Datei: Studienarbeit-Final.pdf)(Siehe angehängte Datei:  
Bewertung\_DH\_032009.xls)

Fiducia & GAD IT AG | www.fiduciagad.de  
AG Frankfurt a. M. HRB 102381 | Sitz der Gesellschaft: Hahnstr. 48, 60528 Frankfurt a. M. | USt-IdNr. DE  
143582320  
Vorstand: Klaus-Peter Bruns (Vorsitzender), Claus-Dieter Toben (stv. Vorsitzender),  
Jens-Olaf Bartels, Martin Beyer, Jörg Dreinhöfer, Carsten Pfläging, Jörg Staff  
Vorsitzender des Aufsichtsrats: Jürgen Brinkmann

—Attachments:————

Studienarbeit-Final.pdf	3,5 MB
Bewertung_DH_032009.xls	430 KB

## **C. Protokolle**

## C.1. Dokumentation der Meetings

### Dokumentation der Meetings

#### Intern 06.11.2016

- Dokument "Angriffe" mit Inhalten aus dem [Paper](#) updaten
- Angriffe besprechen und aufteilen
- Test Konzept entwerfen
- Kapitel für Studienarbeit vorschreiben (Rohtext)
- ? Ergebnisse verlinkter Seiten anzeigen
- ? Verlinkte Seiten ohne Ergebnisse zur Prüfung vorschlagen
- ? [Saucelabs](#) als Frontend testing suite
- [clamav](#) als CLI File-Virusscanner (<https://www.virustotal.com/>)
- [SAD](#) erstellt
- [Metasploit](#) für Anwendungs-Tests

#### Extern 07.11.2016

- Erwartungen bis Weihnachten (Anwendung, Dokumentation)
- Angriffe besprechen
- Weitere Ideen von ihm
- Vorstellung Konzept (SAD)
- Metasploit, VirensScanner (clamav, virustotal)

#### Intern 09.11.2016

- Schnittstelle definieren

#### Intern 17.11.2016

- Multi-Header-Check (Browser-Integrity-Check) nur als Warnung
- Virusscan fertig, noch kein Code-Review
- Virusscan wird über offiziell anerkannte *infizierte* Datei geprüft
- Tester haben einen optionalen Parameter **-i** für die Mitgabe einer ID
- URL-resolving über `java.net.HttpURLConnection`: werden hier maliziöse Daten heruntergeladen?
- Server kaufen
- Gliederung der Studienarbeit verfeinert

## Intern 24.11.2016

- Daniel
  - header inspection test fertig implementiert, ohne Docker
  - E-Mail Martin
    - Link zum Server (webifier.de)
    - Link zur Gliederung
  - E-Mail Herr Freudenmann wegen Förderung
- Samuel:
  - Server setup
  - Recherche Resolving URL / Reachable check
- Jan-Eric
  - Test fertig
- Datenbankmodell planen

## Intern 01.12.2016

- Daniel
  - Team Kapitel Rohaufschrieb
  - URL-Parameter akzeptieren
  - ID-Parameter akzeptieren
  - Output-Format definieren (Tester)
  - Java-Klasse in webifier-tester erstellen ([Beispiel](#))
- Samuel
  - Einleitung
  - URL Resolving “PreTest”
- Jan-Eric
  - Test fertig
- Fördergelder

## Intern 08.12.2016

- Daniel
  - Team Kapitel Rohaufschrieb
  - Java-Klasse in webifier-tester erstellen ([Beispiel](#))
  - 3€ für Domains an Samuel
- Samuel
  - Einleitung schreiben
- Jan-Eric
  - 3€ für Domains an Samuel
- Stand Studienarbeit

## Intern 15.12.2016

- Daniel
  - schreiben
  - Result-Klasse in webifier-tester schreiben (nicht ergänzend zur Info-Klasse)
  - 3€ für Domains an Samuel
- Samuel
  - schreiben
- Jan-Eric
  - schreiben
  - Test in webifier-tester integrieren
  - 3€ für Domains an Samuel

## Extern 19.12.2016

- HtmlUnit als reiner Java-Browser, mit dem sich Standardverhalten (z.B. über Links navigieren) einstellen lässt
- #neuer Test: IP-Scan Test
- neuer Test: auftretende Links testen
  - Externe Blacklist
  - Interne Datenbank
- #neuer Test: JS-Analyse
  - Ice Shield ([Paper](#)) zur statischen JS-Code-Analyse
- Idee: Phishing, schwer umsetzbar, ggf. wenn Zeit ist Testkonzept erstellen
- Idee: Live-Übertragung der Tests (Screencast) oder einfacher Screenshot der Seite
- Idee: Crawler, "Google für maliziöse Seiten"
- Idee: Browser Plugin
- Priorisierung: [Sheet](#)

## Intern 22.12.2016

- Daniel
  - <http://www.reliably.org/tools/requestheaders.php>
- Samuel
- Jan-Eric
- gemeinsam
  - Definition Test Ergebnis (Gewichtung)
  - malicious-Boolean durch Enum ersetzen
- 2017
  - Daniel

- Samuel
  - Performance für Test optimieren, parallelisieren, multithreading bzw. -processing
- Jan-Eric
- Treffen im nächsten Jahr für Retro und Planung der Weiterarbeit während der Praxisarbeit
- welche Aufgaben, nur Kleinigkeiten? Schreiben?

## Intern 04.01.2017

### 6. Semester:

- Code-Review am Anfang
- Rechnung von netcup an Hüneborg → Genehmigung → Fördermittel über Braun an Samuel
- Analyse
  - Datenbankmodell für Platform
  - Blacklist durchlaufen lassen

## Projektmeeting mit Martin 06.03.2017 12:15 in der Kantine

- Vorstellung der aktuellen webanwendung
- bisher
  - viele tests hinzugefügt
  - batch-verarbeitung (100.000 Einträge reduziert -> sonst zu viel Last)
  - datenbank nimmt erste daten an
  - einzelne neue tests besprochen
- nächste Schritte
  - analyse der daten
  - auswertung visualisieren
- Vorschläge von Martin
  - google-service/open-dns `isMalicious("URL")` einbinden, auch Phishing-Dienste
  - optional: e-mail analyse: alle urls der email checken und ergebnis zurückliefern (ggf. auch Screenshot)
- nächster Termin: in 4 Wochen
  - alle Features implementiert
- Aufgaben
  - E-Mail an Heinrich Braun bzgl. Server
  - ice-shield fertigstellen (bei Fragen gerne über Martin)

# Projektmeeting mit Martin 03.04.2017 12:00 Uhr in der Kantine (alle sind da)

Vorstellung der ergebnisse:

- analyse läuft seit letzten Dienstag
- Statistiken:
  - pro Test
  - Gesamt
- E-Mail
  - läuft noch nicht so rund (Keine Rückmeldung über Ergebnisse)

Gliederung Studienarbeit:

- Aufteilung ist schon ziemlich fix
  - Fazit wird wahrscheinlich zusammen geschrieben
  - Ausblick nicht zum Schluss, besser vorher, für positives Ende
  - Nicht mehrere Lösungsansätze (Architekturen) beschreiben
  - eher weniger bei Standardtechnologien (nicht mehr als notwendig)
  - wichtiger: Angriffstypen beschreiben
  - Optische Entscheidungen (Visualisierung),
  - Analyse braucht mehr Struktur! noch keine Unterpunkte
- 
- Vorschläge: chron-job um schlechte Seiten regelmäßig zu überprüfen (haben sie sich verändert)
  - Martin wird nicht die gesamte Arbeit Probelesen können
  - Draft schreiben
  - unsichere Kapitel zur Prüfung bei Martin einreichen

Folgetermin: 24.04.2017 12:00 Uhr

# Internes Meeting 24.04.2017 12:00 Uhr in der Kantine

Martin ist nicht da, ohne Abmeldung

- todo
  - testspezifische auswertungen
  - ergebnisse nach domain [prozentual]
  - Daniel
    - erkenntnisse
  - Anzahl der Tests pro Tag hängt stark von Webseitengröße ab
- Inhalte

- Analyse: woher kommen die Listen
  - Screenshots
  - GitHub und Slack im Team-Kapitel
- Rechnerinfrastruktur erläutern
- Überleitung Diagramme
  - Daten in MongoDB
- Fragen
  - Wie steht Martin zu Wikipedia als Quelle?
  - Hat Martin Literaturvorschläge
    - Phishing
- **Deadline: 05.05.2017**

## Meeting 03.05.2017 11:00 Uhr

- Ausblick: Länderkarte → IP Geodaten Auswertung
- Übergabe der Test- und Auswertungsdaten, am besten in Drive hochladen
- Wikipedia nur ungern als Quelle, vlt. bei Historien, nicht bei technischen Daten
  - lieber dort verwendete Primärquellen
- Literatur über Phishing → wurde per Mail verschickt
- Analyse
  - nicht nur Datenquellen und Ergebnisse, sondern auch Diskussion also was können wir aus den Ergebnissen lernen, Zusammenhänge
  - Zusammenhänge zwischen den Tests
  - Schwellwerte
- Umsetzung
  - Statistics: wieso wurden die Ergebnisse so umgesetzt
  - Generell können wir viel über Implementierung schreiben
- Für Definitionen lieber Bücher oder noch besser wissenschaftliche Paper