FERDINAND PORSCHE
FERN FH

Sicherheit während der Cloud-Kommunikation

Masterarbeit

eingereicht von: **Ing. Karl Hammer, BSc**
Matrikelnummer: 1510471014

im Fachhochschul-Masterstudiengang Wirtschaftsinformatik

der Ferdinand Porsche FernFH Gesellschaft zur Erhaltung und Durchführung von Fachhochschul-Studiengängen

zur Erlangung des akademischen Grades

Master of Arts in Business

Betreuung und Beurteilung: Dipl.-Ing. Dr. tech. Igor Miladinovic

Zweitgutachten: Dipl.-Ing. Thomas Györgyfalvay, B.A., MBA

Wiener Neustadt, Mai 2017

Ehrenwörtliche Erklärung

Ich versichere hiermit,

1. dass ich die vorliegende Masterarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle Inhalte, die direkt oder indirekt aus fremden Quellen entnommen sind, sind durch entsprechende Quellenangaben gekennzeichnet.

2. dass ich diese Masterarbeit bisher weder im Inland noch im Ausland in irgendeiner Form als Prüfungsarbeit zur Beurteilung vorgelegt oder veröffentlicht habe.

3. dass die vorliegende Fassung der Arbeit mit der eingereichten elektronischen Version in allen Teilen übereinstimmt.

Wien, am 30.05.2017 _____

Unterschrift

Kurzzusammenfassung: Sicherheit während der Cloud-Kommunikation

Es wurde im Rahmen dieser Arbeit auf die Frage eingegangen, unter welchen Rahmenbedingungen die Verwendung von Cloud-Services, im speziellen bei Verwendung des TLS Verschlüsselungsprotokolls, aus technischer und User-Sicht risikobehaftet ist.

Mit Hilfe theoretischer Recherche zu den Themen Cloud-Computing, sowie sicherheitstechnischer Aspekte bei der Kommunikation mit diesem Medium und eines praktischen Versuchs wurden die notwendigen Voraussetzungen für einen erfolgreichen Man-in-the-Middle Angriff auf das TLS Protokoll eruiert. Mit diesen Erkenntnissen wurde eine Online-Umfrage erstellt, welche mittels Kreuztabellen ausgewertet wurde. Es hat sich dabei herausgestellt, dass die Befragten oftmals Warnhinweise ignorieren und unsichere Verbindungen nutzen würden.

Aus technischer Sicht sind sowohl fehlerhafte Protokollimplementierungen und das im Internet eingesetzte Schlüsselmanagement risikobehaftet. Aus User-Sicht ist vor allem das fehlende Wissen in Bezug auf Zertifikate und Sicherheitsmechanismen zu nennen.

Schlagwörter:

Cloud-Computing; TLS; Informationssicherheit; Man-in-the-Middle Angriff; Kryptographie;

Abstract: Security during cloud communication

Within the scope of this thesis, the question was addressed under which conditions the use of cloud services, especially with the use of the TLS protocol, is risk-based from a technical and user perspective.

The necessary prerequisites for a successful man-in-the-middle attack on the TLS protocol were determined by theoretical research on the topics of cloud computing, as well as safety-related aspects in communication with this medium and a practical experiment. With these results, an online survey was created. The answers were evaluated with cross-tabulation tables. It turned out that the consulted people often ignores warnings and uses unsafe connections.

From a technical point of view, faulty protocol implementations and the key management used on the internet are subjects of risks. From the user's point of view, the lack of knowledge about certificates and safety mechanisms can be mentioned.

Inhaltsverzeichnis

1. Einleitung

1.1 Ausgangslage und Zielsetzung

Das Ziel der Masterarbeit ist die Evaluierung der Sicherheit bei der Verwendung von Cloud-Services und der damit verbundenen eingesetzten Verschlüsselungstechnologien, im speziellen TLS.

Im RFC 2818 (HTTP Over TLS) [1] wird unter anderem beschrieben, dass der TLS Standard keine Sicherheit gegenüber der Verbindung zu kompromittierten Websites bietet. In einigen wissenschaftlichen Arbeiten wird aufgezeigt, dass der sogenannte Man-In-The-Middle (MITM) Angriff (vergleiche hierzu Kapitel 2.5.3.3) erfolgreich durchgeführt werden kann. Ich möchte darauf eingehen und einen eigenen praktischen Versuch durchführen, welcher nicht zum Ziel hat die Möglichkeit des Angriffs zu bestätigen, sondern vielmehr die dafür notwendigen Rahmenbedingungen auszuforschen. Aus diesen Erkenntnissen wird eine Umfrage generiert, welche zeigen soll, ob Nutzerinnen und Nutzer von Cloud-Services, wie beispielsweise dem Online-Banking, auf derartige Bedrohungsszenarien sensibilisiert sind.

1.2 Forschungsfrage

Unter welchen Rahmenbedingungen ist die Verwendung von Cloud-Services, im speziellen bei Verwendung des TLS Verschlüsselungsprotokolls, aus technischer und User-Sicht risikobehaftet?

1.3 Methodisches Vorgehen

Im Zuge der Masterarbeit werden Verschlüsselungsprotokolle wie TLS und SSH in Bezug auf Cloud-Kommunikation näher analysiert indem auf die RFCs und andere Quellen eingegangen wird. Auch werden bereits bekannte Sicherheitslücken wie das „TLS Heartbleed"-Problem aufgegriffen. Hierfür wurde geeignete Literatur sowohl in Bibliotheken, als auch Online gesucht. Es wurde vor allem auf das österreichische Informationssicherheitshandbuch des Bundeskanzleramts, Büro der Informationssicherheitskommission und die IT Grundschutz Publikationen des deutschen Bundesamts für Sicherheit in der Informationstechnik eingegangen.

1.3.1 Praktischer Versuch

Anhand eines praktischen Versuches, wurde ein sogenannter „Man-in-the-Middle" Angriff während einer TLS-Kommunikation durchgeführt. Ziel dieser Aktion war es, dass man mittels Entschlüsselung und anschließender Verschlüsselung zum Klartext der Datenübertragung kommt, ohne dass der Versender der Nachricht davon etwas mitbekommt. Dieser Versuch sollte zeigen, wie leicht bzw. schwer ein derartiger Angriff Aussicht auf Erfolg hat und welche Rahmenbedingungen hierfür notwendig sind. Die Ergebnisse wurden mit Forschungsergebnissen anderer Arbeiten verglichen.

Es wurde ein praktischer Versuch unternommen, da nicht nur die Möglichkeit des Angriffs bestätigt, sondern vielmehr die Rahmenbedingungen, welche für einen derartigen Angriff notwendig sind, ausgeforscht werden sollten. Für die Definition der Rahmenbedingungen wurden beim praktischen Versuch aktuelle Browserumgebungen eingesetzt, wobei bei einer rein theoretischen Analyse, diese Rahmenbedingungen teilweise nur angenommen werden hätten können.

1.3.2 Umfrage und quantitative Auswertung

Aus den Erkenntnissen des Versuchs, wurde ein Fragebogen mit geschlossenen Fragen und vorgegebenen Antwortkategorien generiert, welcher online gestellt und sowohl im beruflichen, als auch privaten Umfeld publiziert wurde. Aus den Umfragen sollte hervorgehen, ob sich die Nutzerinnen und Nutzer von Cloud-Services im Klaren sind, welche Risiken bestehen und ob die im praktischen Versuch ermittelten Voraussetzungen für ein sicheres Arbeiten auch umgesetzt werden. Die Umfrageergebnisse wurden mittels quantitativer Methode statistisch erhoben und auf ihre Objektivität und Validität überprüft. Die Daten wurden in einer Datenmatrix gesammelt und mittels Kreuztabellen-Analyse ausgewertet. Diese Tabellen wurden durch den Chi-Quadrat-Test auf Relevanz überprüft.

2. Theoretischer Teil

2.1 Cloud Computing

Der Begriff „Cloud Computing“ ist im IT Bereich bereits seit Jahren bekannt. Sowohl Menschen im privaten Umfeld, als auch Firmen und Behörden nutzen Cloud Dienste um Arbeiten einfacher und flexibler bewältigen zu können. Wie im österreichischem Sicherheitshandbuch des Bundeskanzleramts [2, S. 603] ausgeführt wird, verbergen sich dahinter zum Teil altbekannte Architekturen und Konzepte, welche aber Dank fortschreitender technischer Entwicklungen der letzten Jahre erst markttauglich umsetzbar wurden.

Allgemein formuliert, verbirgt sich hinter Cloud Computing die Anbindung bzw. das Nutzen von bereitgestellten Ressourcen oder Diensten via Netzwerk. Dabei ist es charakteristisch, dass diese nicht dezidiert einer Kundin bzw. einem Kunden zur Verfügung stehen, sondern vielmehr dynamisch, also nach Bedarf bzw. Vertragsmodell, zugewiesen werden. Dies ermöglicht eine bedarfsgerechte und flexible Bereitstellung und auch Abrechnung. Die Kundinnen und Kunden müssen nur für die konsumierten Leistungen, nach Bedarf und Vertrag bezahlen und benötigen keine eigene teure Hardware um Leistungsspitzen abzufangen. [2, S. 603]

2.1.1 Definition

Gemäß dem National Institute of Standards and Technology (NIST) des U. S. Department of Commerce [3, S. 2], wird der Begriff des „Cloud Computing” wie folgt definiert:

“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and

released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models." (siehe [3, S. 2]*)*

Auf die in der Definition angesprochenen, notwendigen Charakteristiken, sowie auf die Service- und Deployment-Modelle wird in den nächsten Kapiteln eingegangen.

2.1.1.1 Essential Characteristics

Es gibt gemäß der NIST Definition [3, S. 2] fünf notwendige Charakteristiken für Cloud Computing. Diese sind:

- On-Demand Self-Service
- Broad Network Access
- Resource Pooling
- Rapid Elasticity
- Measured Service

Unter dem Begriff „On-Demand Self-Service" wird gemäß NIST [3, S. 2] verstanden, dass eine verbrauchende Instanz ohne Interaktion des Dienstleistungsanbieters jederzeit die benötigte Leistungen wie beispielsweise Rechenleistung oder Speicher, je nach Bedarf anfordern kann.

Broad Network Access bezeichnet den Umstand, dass Services über ein Netzwerk verfügbar sind, über welches mittels Standardmechanismen auf die jeweiligen Dienste zugegriffen werden kann. Der Einsatz von heterogenen Thin- bzw. Thick-Clientplattformen wird dadurch gefördert. [3, S. 2]

Der Begriff Resource Pooling kann mit Ressourcenzusammenlegung übersetzt werden. Von Seiten des Providers wird eine Architektur verwendet, bei welcher die Ressourcen an einer oder wenigen Stellen gebündelt werden. Es werden somit seine physischen und virtuellen Ressourcen konzentriert um sie mehreren

beziehenden Instanzen in unterschiedlicher Ausprägung, je nach Nachfrage, individuell und vor allem dynamisch zuweisen zu können. Wo sich die, der einzelnen Instanz zugewiesenen Ressourcen physisch befinden stellt sich für diese transparent dar. Auch kann in den meisten Fällen von Seiten der Kundin bzw. des Kunden keinen Einfluss darauf genommen werden. Aufgrund der Nichtnachvollziehbarkeit des Standorts der physischen Ressourcen entsteht ein Gefühl einer Standortunabhängigkeit. [3, S. 2]

Einen wesentlichen Punkt beim Thema Cloud Computing stellt die Fähigkeit dar, flexibel auf geänderte Anforderungen reagieren zu können. Diese Eigenschaft wird als Rapid Elasticity bezeichnet und bedeutet, schnell und flexibel nach Innen und Außen reagieren zu können. Für die Nutzerinnen und Nutzer stellen sich die angebotenen Services als nahezu unbegrenzt und allzeit in jeder beliebigen Menge verfügbar dar. [3, S. 2]

Mit Measured Service ist gemeint, dass Cloud-Systeme automatisch die Ressourcennutzung steuern und optimieren, indem sie eine Messkapazität auf einer gewissen Abstraktionsebene verwenden, welche der Art des Dienstes entspricht. Beispielsweise können für die Bereiche Speicherung, Verarbeitung, Bandbreite oder aktive Benutzerkonten Messgrößen definiert und aufgenommen werden. Die Ressourcennutzung wird überwacht, kontrolliert und berichtet um somit Transparenz sowohl für den Provider als auch für die Nutzerin bzw. den Nutzer des Dienstes zu schaffen. [3, S. 2]

Neben diesen fünf Charakteristiken führt das Büro der Informationssicherheitskommission (ISK) des österreichischen Bundeskanzleramts in deren Sicherheitshandbuch [2, S. 604] noch zwei weitere Charakteristiken von Cloud Computing an. Eine davon ist die Mehrmandantenfähigkeit (Multitenancy), welche aussagt, dass Ressourcen und Dienste zwischen allen Usern dynamisch aufgeteilt werden. Die andere ist die Skalierbarkeit (Massive Scalability), womit gemeint ist, dass Ressourcen je nach Anforderung im entsprechenden Umfang der Kundin bzw. dem Kunden zur Verfügung gestellt werden.

2.1.1.2 Service Models

Wie bereits angeführt werden in der Definition von NIST [3, S. 2f] drei Modelle für Cloud Services beschrieben. In der Praxis werden mittlerweile weitere Servicemodelle diskutiert, welche im Anschluss angeführt werden.

Software as a Service (SaaS)

Unter dem Modell „Software as a Service (SaaS)“, wird die Verwendung von Softwareapplikationen eines Providers verstanden, welche in einer Cloud-Infrastruktur laufen. Hierbei können die Anwenderinnen und Anwender von verschiedenen Client-Geräten entweder via Programmierschnittstelle, proprietären Applikationen, einem Webbrowser oder anderen Thin-Client-Schnittstellen auf den angebotenen Service zugreifen. Die Verwaltung und Instandhaltung der gesamten Cloud-Infrastruktur obliegt hierbei dem Provider. Eine Kundin bzw. ein Kunde hat meist nur eingeschränkte bis gar keine Konfigurationsmöglichkeiten in der Applikation. [3, S. 2]

Platform as a Service (PaaS)

Das Modell „Platform as a Service (PaaS)“ beschreibt die Bereitstellung von Cloud-Infrastruktur inklusive der notwendigen Frameworks und Entwicklungswerkzeugen, damit die Kundinnen und Kunden ihrerseits Programme und Applikationen auf der bereitgestellten Plattform entwickeln und betreiben können. Die Kundin bzw. der Kunde hat immer noch keine Kontrolle über die zugrundeliegende Cloud-Infrastruktur, jedoch auf die eingesetzten Applikationen. Gegebenenfalls hat sie bzw. er ebenfalls die Konfigurationsmöglichkeit für die Application-Hosting-Umgebung. [3, S. 2f]

Infrastructure as a Service (IaaS)

Die dritte Möglichkeit um Cloud-Services zu nutzen, stellt das Modell „Infrastructure as a Service (IaaS)“ dar. Es wird einer Kundin bzw. einem Kunden eine grundlegende Infrastruktur zur Verfügung gestellt, auf welcher individuell

Betriebssysteme und Programme laufen können. Das Management bzw. die Wartung der Infrastruktur obliegt dem Provider. Die Nutzerin bzw. der Nutzer hat aber dennoch die Kontrolle über die eingesetzten Betriebssysteme, die Speicherverwaltung und alle Anwendungen. Je nach Provider hat die Kundin bzw. der Kunde außerdem einen beschränkten Einfluss auf ausgewählte Infrastrukturkomponenten wie beispielsweise Firewalls. [3, S. 3], [2, S. 604]

Zur Darstellung der verschiedenen Elemente des Cloud Computings kann das SPI-Modell herangezogen werden, welches in Abbildung 1 gezeigt wird. Dieses stellt die drei Ebenen des Servicemodells dar, indem es sämtliche Cloud-Dienste einer von den drei Ebenen SaaS, PaaS oder IaaS zuweist. Das Akronym „SPI“ steht dabei für die drei Anfangsbuchstaben der einzelnen Ebenen. [4, S. 11]

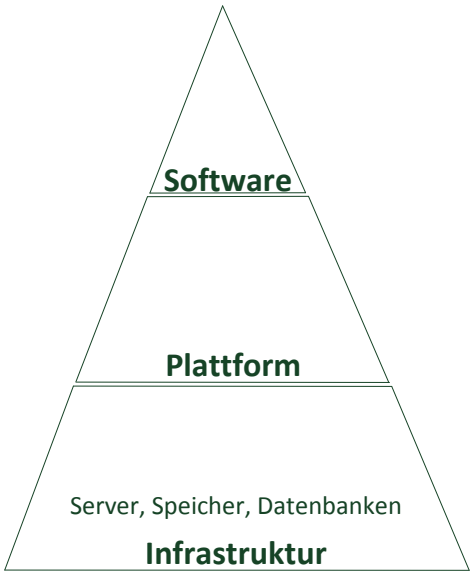


Abbildung 1: Darstellung des SPI Modells (Quelle: eigene Darstellung nach [4, S. 17])

Erweiterte Servicemodelle

Neben den drei Servicemodellen, welche durch NIST definiert wurden, werden noch weitere diskutiert: [2, S. 605]

Business Process as a Service (BPaaS)

Das „Business Process as a Service (BPaaS)“ Modell geht aus dem SaaS hervor und zeichnet sich durch eine stärkere Nähe zum Geschäftsprozess aus. Es werden somit Geschäftsprozesse in die Cloud ausgelagert. [2, S. 605]

Data as a Service (DaaS)

Bei „Data as a Service (DaaS)“ werden Daten bzw. Informationen on Demand ausgelagert und unter Umständen Anderen verfügbar gemacht.

Network as a Service (NaaS)

Mittels „Network as a Service (NaaS)“ werden Kundinnen und Kunden Netzwerkdienste zur Verfügung gestellt. NaaS bezieht die Vergabe von Ressourcen ein und behandelt das Netzwerk und die Rechner-Ressourcen als einheitliches Ganzes. Gemäß Barry [5] ist noch kein Standard definiert, weshalb die einzelnen Ausprägungen von NaaS unterschiedlich ausfallen können.

2.1.1.3 Deployment Models

Gemäß der NIST Definition [3, S. 3] kann zwischen 4 Bereitstellungsmodellen für Cloud Computing unterschieden werden. Diese Modelle werden teilweise in der Literatur erweitert, wie beispielsweise Enterprise Cloud, Exclusive Cloud oder andere, doch können diese Ausprägungen aufgrund ihrer Eigenschaften immer einer der vier Hauptmodelle untergeordnet werden. [2, S. 606]

Die angesprochenen vier Bereitstellungsmodelle sind:

- Private Cloud
- Community Cloud
- Public Cloud
- Hybrid Cloud

Anzumerken sei, dass in mehreren literarischen Werken die Community Cloud als eine Sonderform der Private Cloud angesehen wird. In dieser Arbeit wird, gemäß der NIST Definition, die Community Cloud jedoch als separates Modell betrachtet.

Eine Private Cloud stellt eine Infrastruktur dar, welche für den ausschließlichen Gebrauch durch eine einzelne Organisation bestimmt ist. Dabei können von dieser Organisation mehrere Clients gleichzeitig die Services der Cloud Infrastruktur nutzen. Die Infrastruktur kann von der Organisation oder Dritten besessen, betrieben und verwaltet werden, während die Hardware innerhalb oder außerhalb der Organisation selbst existiert. Dadurch ergeben sich einige Vorteile von Cloud Computing, ohne dabei die Nebeneffekte von Datensicherheitsbedenken, Nichteinhaltung der vorgegebenen Corporate Governance und Mangel an Zuverlässigkeit zu haben. Etwaige Skaleneffekte und Kosteneinsparungen sind erheblich reduziert, während eine stärkere Individualisierung der Dienste möglich ist. Aus Sicht der Kundinnen und Kunden nimmt die Kontrolle über die Cloud mittels dieses Bereitstellungsmodells zu. [3, S. 3], [2, S. 605], [4, S. 23]

Die Community Cloud ist eine Infrastrukturbereitstellung, welche sich durch die gemeinsame und ausschließliche Verwendung durch eine bestimmte Gemeinschaft von Verbraucherinnen und Verbrauchern kennzeichnet. Dabei kann die Infrastruktur, wie bei der Private Cloud, entweder im Besitz, in der Verwaltung und im Betrieb von einem der Nutzenden, oder bei einem Dritten liegen. Auch Kombinationsmöglichkeiten sind durchaus üblich. In diesem Modell kann die Infrastruktur sowohl bei einem der User, als auch extern verortet sein. [3, S. 3]

Aus Sicht von privaten Nutzerinnen und Nutzern, stellt das Konzept der Public Cloud die wohl am häufigsten genutzte Form von Cloud-Computing dar. Hierbei wird die Infrastruktur der Öffentlichkeit via gebräuchliche Internettechnologien zugänglich gemacht. Die Plattform selbst wird von einem Cloud-Serviceprovider betrieben, wobei die Infrastruktur auch bei diesem verortet ist. Diese Form ist normalerweise durch eine hohe Nutzeranzahl charakterisiert, wodurch sich entsprechende Skaleneffekte erzielen lassen, aber eine individuelle Anpassung an

einzelne Anwenderinnen und Anwender nicht mehr oder nur sehr eingeschränkt möglich ist. [3, S. 3], [2, S. 605]

Die Hybrid Cloud stellt eine Mischform aus zwei oder mehreren der vorangegangen Bereitstellungsmodelle dar. Dabei bleiben die unterschiedlichen Cloud-Modelle als eigenständige Entitäten erhalten, werden jedoch miteinander verbunden um eine Daten- bzw. Anwendungsportabilität sicher zu stellen. Diese Kopplung kann entweder durch standardisierte, oder proprietäre Technologien von Statten gehen. Mittels Hybrid Clouds ist es möglich, die Vorteile von mehreren Cloud-Modellen zu kombinieren und dabei die Stärken jedes einzelnen Modells zu nutzen. Mit der Nutzung dieser Vorteile geht jedoch oftmals eine kostspielige Trennung der Daten einher. [3, S. 3], [2, S. 606]

2.1.2 Vor- und Nachteile

Mittels Cloud Computing können sowohl Unternehmen als auch Privatpersonen IT-Ressourcen und Anwendungsdienste eines Service-Anbieters rund um die Uhr nutzen und zahlen in der Regel nur den tatsächlichen Verbrauch. Die für die Nutzung notwendigen IT-Ressourcen werden vom Provider ortsunabhängig, virtualisiert betrieben und als Service bereitgestellt. [6, S. 17]

Vor der Entscheidung zur Verwendung von Cloud Computing sollten sowohl die Vor-, als auch Nachteile abgewogen werden. Dies gilt sowohl für Privatpersonen, als auch Unternehmen, welche sich Gedanken machen, einen Cloud Computing Service zu nutzen.

2.1.2.1 Vorteile von Cloud Computing

Im Folgenden werden Gründe für die Verwendung von Cloud Services angeführt. Diese können je nach Anwendungsfall eine Entscheidung für die Nutzung dieser Dienste mehr oder weniger stark beeinflussen.

Mögliche Kostenersparnis

Es wird angenommen, dass durch die Verwendung von Cloud-Diensten Kosten, sowohl hinsichtlich der Kapitalinvestitionen, als auch im laufenden Betrieb eingespart werden können. Durch eine leistungsbezogene Verrechnung, werden nur jene Ressourcen in Rechnung gestellt, welche auch tatsächlich in Anspruch genommen wurden. [6, S. 17], [7]

Entlastung der eigenen IT-Abteilung

Die eigene IT-Abteilung wird durch den Outsourcing-Vorgang entlastet und die frei gewordenen Personalressourcen können für andere Aufgaben verwendet werden, welche womöglich aufgrund von Engpässen vernachlässigt wurden. Das Risiko wird von der eigenen IT in Richtung des Serviceproviders transferiert, wobei klar definierte SLAs hierbei von Nöten sind. [6, S. 17]

Elastizität und Skalierbarkeit

Die benötigten Dienstleistungen und Ressourcen können vom Serviceprovider bedarfsgerecht angefordert werden. Dies hilft vor allem kleineren Unternehmen, da diese keine eigene Infrastruktur aufbauen müssen. [6, S. 17], [7]

Verarbeitungsgeschwindigkeit

Aufgrund der Cloud-Architektur sind hohe Verarbeitungsgeschwindigkeiten möglich. [6, S. 17]

Verfügbarkeit

Die Cloud-Infrastrukturen und Dienste weisen eine sehr hohe Verfügbarkeit auf, welche eventuell höher liegen kann als bei der Verwendung eines eigenen Rechenzentrums. [6, S. 17]

Zukunftssicherheit

Bei einem Cloud-Anbieter arbeiten viele Spezialistinnen und Spezialisten in großen Rechenzentren, welche dafür sorgen, dass die Hardware und Software

immer auf dem aktuellen Stand gehalten wird. Damit regeneriert sich die Cloud selbst und die Kundin bzw. der Kunde kann, wenn gewünscht, ständig die neuste Version nutzen. [7]

Nachhaltigkeit

Der Trend „Green-IT“, welcher für ressourcen- und umweltschonende Nutzung von Informations- und Kommunikationstechnik steht, kommt auch bei Cloud-Computing zum Zug. So können wenige große Rechenzentren effizienter genutzt werden als viele kleine. Auch werden von Seiten der Cloud-Betreiber Ressourcen, welche zur Pufferung von Lastspitzen vorhanden sind, für andere Geschäftsmodelle oder eigene IT Dienstleistungen verwendet. [7]

2.1.2.2 Nachteile von Cloud Computing

Wie bereits erwähnt dürfen nicht nur die Vorteile in Betracht gezogen werden, sondern man muss sich auch bezüglich der Nachteile, welche Cloud Computing mit sich bringt, im Klaren sein.

Anbieterabhängigkeit

Wenn Prozesse in die Cloud verlagert werden, begibt sich ein Unternehmen in eine starke Abhängigkeit vom Serviceprovider. Will das Unternehmen den Service eines konkurrierenden ISP nutzen, so ergeben sich oftmals Schwierigkeiten. Dieser Umstand wird als Lock-in-Effekt bezeichnet. Aber auch wenn der Dienstleister seinen Betrieb einstellt, ergeben sich Probleme. Oftmals besteht dann keine Chance mehr auf die Daten in der Cloud zuzugreifen oder spezielle Programme weiterzuverwenden. [6, S. 17], [7]

Internetzugang

Da auf die bezogenen Dienste oder Plattformen über das Internet zugegriffen wird, entstehen aus diesem Gesichtspunkt zusätzliche Abhängigkeiten. Kommt es zu einer Unterbrechung der Verbindung, ist die Nutzung des Cloud-Dienstes nicht mehr möglich. [7]

Verlust der Kontrolle über Daten und Prozesse

Wenn man Daten in die Cloud auslagert, so weiß man oftmals nicht wo diese physikalisch gespeichert werden. Mittels vertraglicher Abkommen können zwar grundsätzliche Vereinbarungen getroffen werden, eine vollständige Kontrolle über die Daten und Prozesse kann jedoch nicht erlangt werden. [6, S. 17]

Leistungsstörungen

Es müssen alle Eventualitäten bei der Ausarbeitung des Vertrages mit dem Service-Provider berücksichtigt werden. Kommt es zu Leistungsstörungen, so muss definiert sein, wie mit diesen vorgegangen wird. Doch auch auf Seiten des Dienstbeziehers kann es zu Leistungsstörungen kommen. Erfolgen Zahlungen beispielsweise nicht zeitgerecht, so kann der ISP den Dienst einstellen, woraufhin die Kundin bzw. der Kunde womöglich seiner Geschäftstätigkeit nicht mehr nachkommen kann. [6, S. 17]

Lizenzfragen

Viele Lizenzmodelle sind nicht für die Verwendung in der Cloud konzipiert. Aus diesem Grund ist oftmals nicht einfach zu klären ob eine Software auch in der Cloud betrieben werden darf, bzw. welche Kosten durch die Verwendung entstehen. [6, S. 17]

Sicherheit

Da auf den Dienst oder die Plattform via Internet zugegriffen wird, ergeben sich auf diesem Kommunikationsweg vermehrt Risiken. Doch ist man als Nutzerin bzw. Nutzer von Cloud Services und Plattformen auch auf die Sicherheitsvorkehrungen des ISP angewiesen. Oftmals hat man als Kundin bzw. Kunde jedoch keinen Einblick in die Sicherheitsrichtlinien bzw. werden Sicherheitsvorfälle nicht bekannt gegeben. [6, S. 17], [7]

Rechtliche Aspekte

Wie im Kapitel 2.1.3 ausgeführt, ergeben sich bei der Verwendung von Cloud Services rechtliche Fragen, vor allem aber in Bezug auf den Datenschutz. Weiters ist es oftmals schwierig sein Recht durchzusetzen, wenn der Cloud-Anbieter außerhalb der EU ansässig ist. [6, S. 17]

2.1.3 Rechtliche Rahmenbedingungen

Gemäß dem österreichischem Informationssicherheitshandbuch [2, S. 606ff] sind folgende Rechtsgebiete bei der Verwendung von Cloud Computing zu beachten:

- Datenschutzrecht
- Vergaberecht
- IT-Vertragsrecht
- Haftung und Gewährleistung
- Strafprozessrecht

Des Weitern wird darauf hingewiesen, dass wie bei allen Outsourcing-Modellen bedacht auf die Unternehmensveräußerung, den Konkurs und die Liquidation, sowie den Zugriff auf die eigenen Daten im Detail rechtlich abzustimmen sind. [2, S. 606]

2.1.3.1 Datenschutzgesetz (DSG 2000)

Das österreichische Datenschutzgesetz (DSG 2000) findet Anwendung, wenn personenbezogene Daten verarbeitet werden (§ 4 Z 1 DSG 2000). Im Gegensatz zu anderen europäischen Datenschutzgesetzen kann es sich dabei nicht nur um natürliche, sondern auch juristische Personen handeln, deren Identität bestimmt oder bestimmbar ist. [6, S. 18]

Als besonders schutzwürdig sind nach § 4 Z 2 DSG 2000 Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung,

Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben eingestuft. Es muss genauestens abgeklärt werden, ob die Daten in einer Cloud verarbeitet oder gespeichert werden dürfen, da diese einem allgemeinen Verwendungsverbot unterliegen, welches nur durch die in § 9 DSG 2000 taxativ aufgezählten Ausnahmen aufgehoben wird. Abgesehen von diesen Ausnahmen ist die Verarbeitung sensibler Daten grundsätzlich nur mit einer ausdrücklichen Zustimmung der Betroffenen möglich. Somit stellt sich die Frage, ob sensible Daten gemäß dem DSG 2000 überhaupt in einer Cloud-Umgebung erfasst werden dürfen. Vor allem der Speicherort der Daten hat große Auswirkung auf die rechtliche Grundlage, da die Übertragung personenbezogener Daten in Staaten außerhalb der Europäischen Gemeinschaft äußerst problematisch ist, wie in nachstehendem Kapitel ausgeführt wird. [6, S. 18]

2.1.3.2 Speicherung sensibler Daten außerhalb von Österreich

Wenn Daten, welche unter den Begriff sensible Daten gemäß dem österreichischen Datenschutzgesetz (DSG2000) fallen, in einem Cloud-Dienst im Ausland gespeichert werden sollen, so ist zu unterscheiden, ob sich der Speicherort innerhalb oder außerhalb der Europäischen Union befindet. Dennoch gilt als Voraussetzung für die Zulässigkeit jeder Übermittlung oder Überlassung von Daten in das Ausland zunächst die Rechtmäßigkeit der Datenverwendung im Inland. [8]

Es sei anzumerken, dass das Einstellen personenbezogener Daten auf einer weltweit frei abrufbaren Internetseite, welche bei einem in der EU ansässigen Host-Provider gespeichert ist, nach Auffassung des EuGH keine Datenübermittlung in Drittstaaten darstellt. [9, S. 172]

<u>Speicherung innerhalb der EU</u>

Die Wirtschaftskammer Österreich führt auf deren Homepage aus, dass im DSG 2000 davon ausgegangen wird, dass alle EU Mitgliedsstaaten gemäß den EU-Datenschutzrichtlinien ein gleichwertiges Niveau an Datenschutz haben und somit

gemäß dem Gemeinschaftsrecht keine Beschränkungen bezüglich der Speicherung besteht. [8]

Speicherung außerhalb der EU

Es wird von Seiten der Wirtschaftskammer Österreich weiter angeführt, dass es einer Genehmigung durch die Datenschutzbehörde bedarf, wenn sensible Daten an Empfänger außerhalb der Europäischen Union übermittelt bzw. überlassen werden sollen. Von Seiten der EU wurden jedoch Ausnahmen definiert, indem Staaten gelistet wurden, welche gemäß Ansicht der Union, über ein angemessenes Maß an Datenschutz verfügen. Diese Staaten werden auf der Homepage der Wirtschaftskammer angeführt. [8]

Es wurden des Weiteren drei Abkommen zwischen der EU und Drittstaaten abgeschlossen welche ebenfalls die Übermittlung bzw. das Überlassen von Daten regeln. Eines davon ist das PNR-Abkommen zur Überlassung von Fluggastdatensätzen, welches zwischen der EU, den USA, Australien und Kanada geschlossen wurde. Ein weiteres ist das US-Data and Terrorist Finance Tracking Programme (TFTP), welches zwischen den USA und der EU zur Terrorismusbekämpfung abgeschlossen wurde. In diesem Programm wurde vereinbart, dass unter anderem die Namen von AbsenderIn und EmpfängerIn einer Überweisung, sowie die Adresse gespeichert werden, welche in oder aus der EU getätigt werden. Die dritte Vereinbarung ist das EU-US-Privacy Shield Abkommen, welches als Nachfolger von Safe Harbor beschlossen wurde. Mittels dieser Vereinbarung wurde festgestellt, dass die USA ein angemessenes Datenschutzniveau für den Datentransfer aus der EU an US-Unternehmen gewährleisten. [8]

2.2 Informationssicherheit

2.2.1 Begriffsdefinition

2.2.1.1 Sicherheit

Die Bezeichnung „Sicherheit“ steht im deutschen, im Gegensatz zum englischen Sprachgebrauch, sowohl für „safety“, als auch für „security“. Um trotzdem eine Unterscheidung zu ermöglichen, werden die beiden englischen Begriffe üblicherweise mit „Funktionssicherheit“ und „Informationssicherheit“ übersetzt. [10, S. 6]

2.2.1.2 Funktionssicherheit (Safety)

Der Begriff der Funktionssicherheit beschreibt die Tatsache, dass der Ist-Zustand eines Systems mit dem Soll-Zustand übereinstimmt und welche Bedrohungen zur Sicherheit der Funktion durch technisches Fehlverhalten entstehen können. Die Funktionssicherheit stellt die Grundlage für die Informationssicherheit dar. [10, S. 6]

2.2.1.3 Informationssicherheit (Security)

Gemäß dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) [11], wird der Begriff der Informationssicherheit wie folgt definiert:

„Informationssicherheit hat den Schutz von Informationen als Ziel.“ (Quelle: [11]*)*

Hierbei können die zu sichernden Informationen in jeder erdenklichen Art und Weise, wie zum Beispiel auf Papier, auf elektronischen Datenträgern oder in den Köpfen von Menschen gespeichert sein. [11]

Der Begriff Informationssicherheit kann seinerseits noch in die Unterbegriffe „Datenschutz“ (privacy) und „Datensicherheit“ (protection) unterteilt werden. Datenschutz bezeichnet die Kontrolle über jene Informationen, welche die kontrollierende Person auch persönlich betreffen, das bedeutet, die Person hat ein

individuelles Recht auf die informelle Selbstbestimmung. Unter Datensicherheit werden die technischen und rechtlichen Aspekte zum Umgang mit Daten verstanden um die geforderten Schutzziele zu gewährleisten. Der Begriff „Informationssicherheit“ ist umfassender zu verstehen als jener der „IT-Sicherheit“. [10, S. 6f], [11]

2.2.1.4 IT-Sicherheit

Der Begriff der IT-Sicherheit wird vom deutschen Bundesamt für Sicherheit in der Informationstechnik wie folgt definiert:

„IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind.“ (siehe [11]*)*

IT-Sicherheit ist also der Zustand, in dem die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind. Siehe hierzu auch Kapitel 2.2.3.

Nach dem Informationssicherheitshandbuch des österreichischen Bundeskanzleramts [2, S. 36] hat ein gewisser Bedeutungswandel bei den beiden Begriffen „Informationssicherheit“ und „IT-Sicherheit“ in den letzten Jahren stattgefunden. So sind die beiden Begriffe heute fast synonym zu sehen. International hat sich, ebenso wie in den Normen, der Begriff der Informationssicherheit als der umfassendere etabliert.

2.2.2 Rolle der Informationssicherheit in der Praxis

Informationen aller Art sind, gemäß dem BSI [12], ein wesentlicher Wert für Unternehmen und Behörden und müssen deshalb angemessen geschützt werden. So geht aus dem Artikel hervor, dass unzureichend geschützte Informationen

häufig ein unterschätztes Risiko darstellen und für mache Unternehmen existenzbedrohend sein können, da die Abhängigkeit von der IT immer weiter zunimmt. Mängel im Bereich der Informationssicherheit führen zu erheblichen Problemen, deren Auswirkungen sich in die Kategorien „Verlust der Verfügbarkeit“, „Verlust der Vertraulichkeit“ und „Verlust der Integrität“ einordnen lassen. Auf diese Schutzziele wird im Kapitel 2.2.3 näher eingegangen.

Die Wichtigkeit des Themas Informationssicherheit wird unter anderem dadurch unterstrichen, dass sich weltweit mehrere staatliche Einrichtungen damit beschäftigen und Handbücher für Firmen und Behörden herausbringen in welchen auf die Risiken sensibilisiert wird und Maßnahmen vorgeschlagen werden, welche die Informationssicherheit erhöhen sollen. So wird unter anderem vom österreichischen Bundeskanzleramt, genauer gesagt dem Büro der Informationssicherheitskommission (ISK), ein Handbuch mit dem Titel „Österreichisches Informationssicherheitshandbuch“ [2] herausgegeben. Das in Europa und vor allem im gesamtdeutschen Sprachraum bekanntere Gegenstück dazu stellen die Publikationen des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) dar. Darunter fallen beispielsweise die „IT-Grundschutz-Kataloge“ [11]. Ziel der publizierten Richtlinien und Vorschläge ist der angemessene Schutz von Informationen einer Behörde oder Firma. In den meisten Fällen wird hierbei ein ganzheitlicher Ansatz verfolgt, welcher durch die Kombination von organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsmaßnahmen versucht ein Sicherheitsniveau zu erreichen, welches den normalen Schutzbedürfnissen gerecht wird. [2], [12]

2.2.3 Schutzziele der IT-Sicherheit

2.2.3.1 Authentizität

Gemäß Eckert [10, S. 7], stellen Informationen, sprich Daten die zu schützenden Güter in informationssicheren bzw. datensicheren Systemen dar. Der Zugriff auf

diese ist mittels Zugriffskontrollen und –beschränkungen zu versehen, um unautorisierten Personen den Zugang zu verwehren.

Wenn eine Person auf die Daten zugreifen will, muss diese zuerst eindeutig identifiziert und dann ihre Identität verifiziert werden. Unter dem Begriff der Identifikation versteht man die Bekanntgabe der jeweiligen Person, während man unter Authentifizierung den Beweis der Identität versteht. Unter der Authentizität versteht man somit die Echtheit und Glaubwürdigkeit eines Subjektes. In der Praxis kann die Authentizität beispielsweise durch die Identifikation mittels Usernamen und Authentifizierung durch das entsprechende Passwort ermittelt werden. Doch nicht nur Wissen, wie zum Beispiel ein Passwort, sondern auch biometrische Merkmale wie ein Fingerabdruck können für eine Authentifizierung verwendet werden. Weiters kann auch der Besitz von Dingen wie beispielsweise einer RFID Karte oder eines Zertifikates zum Ausweisen einer Person herangezogen werden. [10, S. 7f]

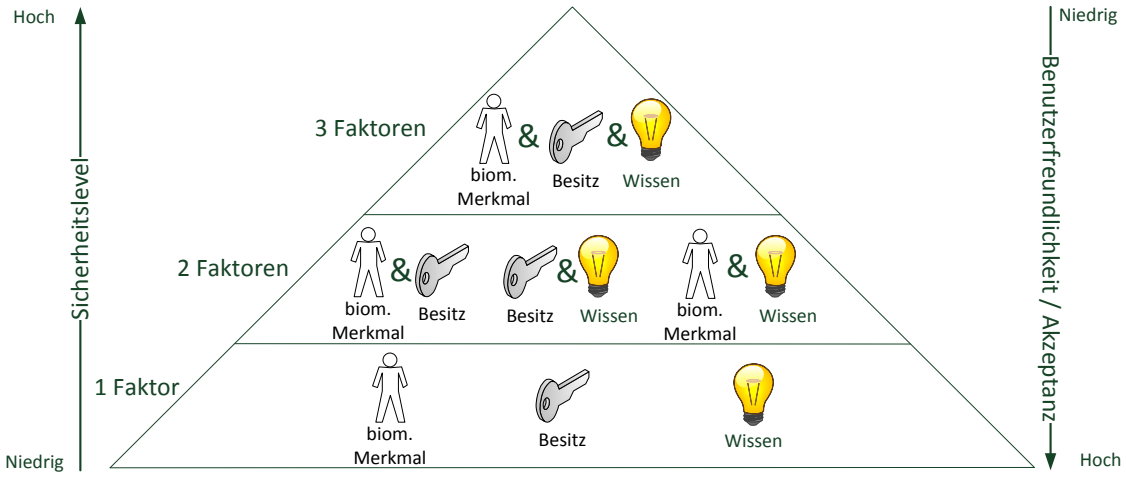


Abbildung 2: Authentifizierung durch einen oder mehrere Faktoren (Quelle: modifiziert übernommen aus [13, S. 319])

Wie in Abbildung 2 dargestellt, können je nach Sicherheitsanspruch ein oder mehrere Faktoren für die Authentifizierung einer Person gefordert werden. So können entweder zwei Faktoren, wie beispielsweise biometrisches Merkmal und

Wissen oder auch alle drei, also das Wissen, der Besitz eines Gegenstandes und ein biometrisches Merkmal erforderlich sein um Zugriff auf das System zu bekommen. Je mehr Faktoren für das Ausweisen einer Person notwendig sind, desto höher ist die Systemsicherheit, allerdings umso niedriger dessen Benutzerfreundlichkeit bzw. die Akzeptanz der Nutzerinnen und Nutzer.

2.2.3.2 Datenintegrität

Die Datenintegrität beschreibt den Umstand, dass es in einem System nicht möglich ist, Daten unautorisiert und unbemerkt zu verändern. Diese Eigenschaft fordert die Festlegung von Rechten für die Nutzung von Daten. Bekannte Beispiele hierfür sind Schreib- und Leserechte in IT Systemen. Es dürfen die Rechte von Subjekten nicht nur eingeschränkt werden, so müssen bestimmte Personen auch weitergehende Privilegien haben um ihren Tätigkeiten nachgehen zu können. Die Festlegung der Zugriffsrechte hat einen großen Einfluss darauf, in welcher Qualität die Datenintegrität im System vorhanden ist. So können Zugriffsbeschränkungen einfach oder komplex gestaltet sein. Einfach heißt in diesem Zusammenhang, dass das Subjekt für den Zugriff nur das entsprechende Zugriffsrecht besitzen muss. Im Gegensatz dazu, kann bei komplexen Zugriffsbeschränkungen der Zugriff auch von weiteren Bedingungen abhängen. Klassische Betriebssysteme realisieren in der Regel ein Referenzmonitorkonzept, womit nur einfache Zugriffsbeschränkungen erfasst werden können. Für komplexe Beschränkungen müssen diese in den Anwendungsprogrammen implementiert werden und auf das Operating System abgestimmt werden. [10, S. 9], [10, S. 257f]

Neben den Zugriffskontrollen müssen außerdem unautorisierte Manipulationen aufgedeckt werden. Es gilt zwar vorrangig unautorisierte Manipulationen zu unterbinden, doch sollte eine derartige Aktion nicht verhindert worden sein, so muss diese mittels geeigneten Maßnahmen erkennbar gemacht werden. Auf diese Weise wird der Schaden begrenzt und manipulierte Daten werden nicht weitergegeben oder weiterverarbeitet. Zur Erkennung von durchgeführten

Veränderungen an den Daten werden kryptographisch sichere Hashfunktionen eingesetzt, auf welche in Kapitel 2.3.7 eingegangen wird. [10, S. 9]

2.2.3.3 Informationsvertraulichkeit

Ein System erfüllt das Schutzziel der Informationsvertraulichkeit, wenn es gewährleistet, dass keine unautorisierte Informationsgewinnung stattfinden kann. [10, S. 10]

Dies wird in datensicheren Systemen durch das Festlegen von Berechtigungen und Kontrollen realisiert. Es muss sichergestellt werden, dass Subjekte nicht unautorisiert Kenntnis über Informationen erlangen. [10, S. 10]

In informationssicheren Systemen sind Maßnahmen zur Festlegung und Kontrolle zulässiger Informationsschlüsse zwischen den Subjekten des Systems erforderlich. Es muss ausgeschlossen werden, dass Informationen zwischen den Subjekten unautorisiert bzw. ungewollt verteilt werden. Dieses Problem wird als Confinement-Problem bezeichnet. Abhilfe schafft die Festlegung zur Kontrolle der Informationsflüsse, in welcher spezifiziert wird, welche Person Kenntnis von welchen Informationen erlangen darf. [10, S. 10]

Anforderungen an die Informationsvertraulichkeit im weiteren Sinn werden laut Eckert [10, S. 10f] unter anderem durch Verschlüsselungsverfahren erfüllt. Mittels dieser Methoden ist es möglich, dass Daten geeignet übertragen werden, ohne dass unautorisierte Dritte in der Lage sind, sie sinnvoll zu interpretieren. Nur mit dem entsprechenden Entschlüsselungsschlüssel ist eine Decodierung der Nachricht in der Regel möglich. Neben den kryptographischen Verfahren werden auch Labeling-Techniken eingesetzt um Datenobjekten eine spezielle Sicherheitseinstufung zuzuordnen. Dadurch kann sichergestellt werden, dass Informationen nicht in unautorisierte Hände gelangen.

2.2.3.4 Verfügbarkeit

Gemäß Bedner und Ackermann [14, S. 326] betrifft die Verfügbarkeit sowohl die informationstechnischen Systeme als auch die darin enthaltenen Daten. Verfügbarkeit bedeutet, dass die Systeme jederzeit betriebsbereit sind und auf die darin enthaltenen Daten auch ständig zugegriffen werden kann.

Ein System erfüllt die Eigenschaft der Verfügbarkeit, wenn autorisierte und authentifizierte Subjekte in der Wahrnehmung ihrer Berechtigungen nicht unautorisiert beeinträchtigt werden können. Zur Gewährung der Verfügbarkeit sind Maßnahmen zu treffen, welche die Nutzung von Systemressourcen reglementieren. Unter Ressourcen können in diesem Zusammenhang Rechnerressourcen wie Speicher, CPU-Zeit aber auch Netzwerkauslastung oder andere Systemparameter verstanden werden. Eine entsprechende Detektion eines unautorisierten Ressourcenbedarfs ist oftmals nur schwer möglich. Beispielsweise kann eine hohe Netzwerklast auf normalen Datenverkehr oder aber auf einen Angriff mittels synthetisch erzeugten Nachrichten zurückzuführen sein. [10, S. 12]

Im Geschäftsleben wird die Verfügbarkeit pro System oder Dienst angegeben und stellt das Verhältnis zwischen der tatsächlich verfügbaren zu der gesamten Zeit in einem definierten Zeitraum dar. Die Verfügbarkeit wird in Prozent angegeben und liegt im Idealfall bei 100 Prozent, was bedeutet, dass das System oder der Dienst ständig zur Verfügung steht. Der Zeitraum ohne Verfügbarkeit wird als Ausfallszeit bezeichnet. [14, S. 326]

2.2.3.5 Verbindlichkeit

Das Schutzziel der Verbindlichkeit beschreibt die Nichtabtreitbarkeit von Aktionen, welche durch ein Subjekt erfolgt sind. Diese Eigenschaft wird auch als Zuordenbarkeit bezeichnet, da Aktionen einer bestimmten Person zugeordnet werden. [10, S. 12]

Solche Verbindlichkeiten sind unter anderem beim elektronischen Handel von Bedeutung um rechtsverbindliche Transaktionen zu gewährleisten. Aber auch bei der Nutzung von Systemressourcen im Multiuser-Betrieb ist das Schutzziel der Verbindlichkeit unabdingbar. Im Bereich des Cloud-Computing ist mit der Nichtabstreitbarkeit auch die Forderung nach Abrechenbarkeit von verbrauchten Systemressourcen verbunden. Technisch werden diese Anforderungen durch den Einsatz von digitalen Signaturen erfüllt, welche in Kapitel 2.3.8 näher beschrieben werden. Weiters sind Maßnahmen zur Überwachung und Protokollierung einzelner Aktivitäten erforderlich. [10, S. 12f]

2.2.3.6 Anonymisierung und Pseudomisierung

Unter dem Begriff Anonymisierung versteht man die Veränderung personenbezogener Daten, so dass diese keine Rückschlüsse mehr auf die eigentliche Person zulassen. Es müssen dabei alle Einzelangaben über persönliche oder sachliche Verhältnisse berücksichtigt und in den Prozess mit einbezogen werden. [10, S. 13]

Die schwächere Form der Anonymisierung stellt jene der Pseudomisierung dar. Dabei werden personenbezogene Daten durch Zuordnungsvorschriften, wie beispielsweise durch die Verwendung von Pseudonymen, verändert. Es lassen sich danach keine Rückschlüsse zur natürlichen Person ableiten, ohne von den Vorschriften Kenntnis zu haben. [10, S. 13]

Das Thema Privatsphäre gewinnt immer mehr an Bedeutung, wenn man bedenkt, dass neben herkömmlichen Internetzugriffen auch durch die Verwendung von Smartphones oder anderen ubiquitären Computern immer mehr Daten von einzelnen Personen gesammelt werden. Oftmals sind sich die Nutzerinnen und Nutzer solcher Geräte dessen nicht bewusst, oder haben keinen Einfluss darauf. In Österreich und Europa wurde bereits in den 90er Jahren das Recht der informellen Selbstbestimmung gesetzeswirksam. Später wurde mit dem österreichischem Datenschutzgesetz (DSG 2000) beschlossen, dass Daten anonymisiert oder gelöscht

werden müssen, sobald sie nicht länger dem Zweck, für den sie erhoben wurden dienen. [10, S. 14], [15], [16]

2.2.3.7 Zusammenfassende Darstellung der IT Schutzziele

In Tabelle 1 werden die bereits beschriebenen Schutzziele übersichtlich zusammengefasst.

Schutzziel	Kurzbeschreibung
Authentizität	Die Echtheit und Glaubwürdigkeit eines Subjektes ist überprüfbar.
Datenintegrität	Die Daten können nicht unautorisiert manipuliert werden bzw. wird eine derartige Manipulation erkannt.
Informationsvertraulichkeit	Es ist keine unautorisierte Informationsgewinnung möglich.
Verfügbarkeit	Autorisierte und authentifizierte Subjekte sind in der Wahrnehmung ihrer Berechtigungen nicht unautorisiert beeinträchtigt.
Verbindlichkeit	Ein Subjekt kann die Durchführung einer Aktion im Nachhinein nicht abstreiten.
Anonymisierung und Pseudomisierung	Personenbezogene Daten werden derart verändert, dass sensible bzw. schützenswerte Angaben nicht mehr replizierbar sind.

Tabelle 1: Zusammenfassende Darstellung der IT Schutzziele

Abschließend sei erwähnt, dass die im Anschluss diskutierten Protokolle TLS und SSH auf die Schutzziele Authentizität, Integrität und Vertraulichkeit abzielen.

2.2.4 Verwundbarkeit, Bedrohung, Risiko und Angriff

2.2.4.1 Verwundbarkeit und Schwachstelle

Unter dem Begriff Verwundbarkeit wird gemäß Eckert [10, S. 16] eine Schwachstelle eines Systems oder Teilsystems verstanden, an welchem die Sicherheitsdienste umgangen, getäuscht oder unautorisiert modifiziert werden können und das System somit beeinträchtigt werden kann. Eckert definiert

Schwachstellen als Schwäche eines Systems oder einen Punkt an dem das System verwundbar ist. Ein IT System kann mehrere Schwachstellen aufweisen. Gelingt es einem angreifenden Subjekt eine dieser Schwachstellen zu identifizieren und auszunutzen, so kann dies zu einer Beeinträchtigung der Schutzziele Datenintegrität, Informationsvertraulichkeit oder auch Verfügbarkeit führen.

2.2.4.2 Bedrohung

Nahezu jedes IT-System ist vielfältigen Bedrohungen ausgesetzt, welche das System gefährden. Diese Bedrohungen zielen darauf ab, Schwachstellen und Verwundbarkeiten des Systems auszunutzen und die Schutzziele zu gefährden. Die Gewichtung der Bedrohung hängt von der Funktionalität und Einsatzumgebung des Systems ab. Um die tatsächliche Gefährdungslage des Systems zu bestimmen, muss zuerst das Risiko bestimmt werden, welches mit den potentiellen Bedrohungen verknüpft ist. [10, S. 16f]

2.2.4.3 Risiko

Um ein potentielles Risiko zu bestimmen, müssen die zu schützenden Güter bewertet und ein Schadenspotential, welches bei Eintritt eines Schadens entsteht, bestimmt werden. Ebenso ist die Schadenseintrittswahrscheinlichkeit abzuschätzen. Unter dem Begriff Risiko zu einer Bedrohung sind somit die Wahrscheinlichkeit eines Schadenseintritts und die damit verbundene Höhe des potentiellen Schadens zu verstehen. [10, S. 17f]

2.2.4.4 Angriff

Bedrohungen ergeben sich gemäß Eckert [10, S. 19] aus passiven und aktiven Angriffen auf das System. Die Angriffe zielen auf den nicht autorisierten Zugriff auf das System, wobei passive Angriffe auf die unautorisierte Informationsgewinnung und somit auf den Verlust der Vertraulichkeit abzielen und sich aktive Angriffe gegen die unautorisierte Modifikation von Datenobjekten richten, was die Datenintegrität und Verfügbarkeit des Systems gefährdet.

2.2.4.5 Zusammenhänge und Abhängigkeiten

In Abbildung 3 werden die einzelnen Begriffe miteinander in Zusammenhang gebracht und deren Abhängigkeiten veranschaulicht. So wird gezeigt, dass Schutzziele durch Schutzkonzepte erfüllt werden, welche wiederum gegen Bedrohungen und Angriffe schützen. Angriffe nutzen Schwachstellen eines Systems aus und bedrohen somit die schützenswerten Güter, welche sich in der IT meist als Informationen oder Verfügbarkeiten des Systems darstellen. Die Werte, welche die schützenswerten Güter aufweisen, können nach erfolgreichen Angriffen an Wertigkeit verlieren, weshalb Schwachstellen somit das Risiko erhöhen und diese Werte bedrohen. Ebenso erhöhen vermehrte Angriffsversuche oder unzureichende Schutzkonzepte das Risiko. Auf der anderen Seite können die Risiken durch geeignete Maßnahmen auch minimiert werden. Die Risiken induzieren die Schutzziele und Sicherheitspolicy in einem System, was wiederum die Definition der Schutzkonzepte beeinflusst.

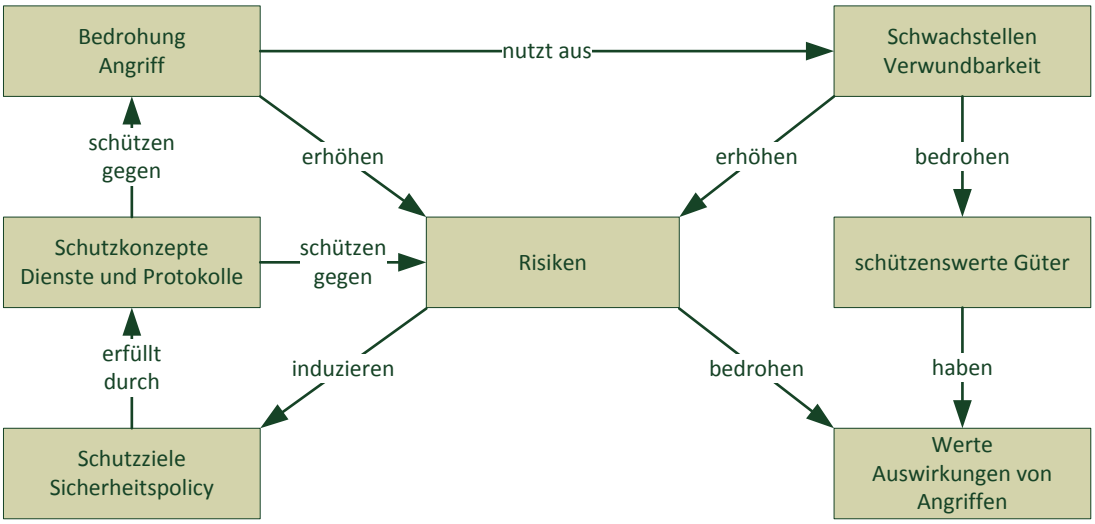


Abbildung 3: Zusammenhänge und Abhängigkeiten (Quelle: modifiziert übernommen aus [10, S. 38])

2.3 Kryptographische Grundlagen

In diesem Kapitel wird auf die Grundlagen der Kryptographie eingegangen, welche für das Verständnis der nachfolgend beschriebenen Cloud-Kommunikations-Protokolle notwendig sind.

2.3.1 Definition Kryptographie, Kryptoanalyse und Kryptologie

Unter dem Begriff Kryptographie wird nach Eckert [10, S. 295] die Lehre von den Methoden zur Ver- und Entschlüsselung von Nachrichten zum Zweck der Geheimhaltung von Informationen gegenüber Dritten verstanden. Mittels der Kryptographie können Daten somit für Dritte nicht einsehbar gemacht werden, während die berechtigt Nutzenden weiterhin darauf Zugriff haben. Dem gegenüber steht die Kryptoanalyse, welche die Wissenschaft von den Methoden zur Entschlüsselung von Nachrichten ist, ohne dabei Zugriff auf den verwendeten Schlüssel zu haben. In der Praxis sind die beiden Wissenschaftsgebiete Kryptographie und Kryptoanalyse eng miteinander verbunden und werden unter dem Oberbegriff Kryptologie zusammengefasst. Beispielsweise wird zur Entwicklung sicherer kryptographischer Verfahren auch stets die Beurteilung mittels der Kryptoanalyse notwendig sein. Anzumerken sei, dass die Kryptologie nicht die Existenz der Nachricht verbergen, sondern diese für Dritte nicht einsehbar machen soll. Mit der Verbergung der Nachricht beschäftigt sich das Fachgebiet der Steganographie. [10, S. 295]

2.3.2 Kerckhoffs-Prinzip

Das Kerckhoffs-Prinzip besagt, dass die Sicherheit eines kryptographischen Verfahrens allein vom verwendeten Schlüssel abhängen darf. Die Geheimhaltung des kryptographischen Verfahrens an sich, stellt keinen Sicherheitsaspekt dar. Um

dies zu gewährleisten, benötigt man einen sehr großen Auswahlbereich von Schlüsseln. Ansonsten könnte ein Angreifer den geheimen Schlüssel durch einfaches Ausprobieren herausfinden. [10, S. 296]

2.3.3 Grundlagen kryptographischer Systeme

Gemäß Eckert [10, S. 301] legt ein kryptographisches System, auch Kryptosystem genannt, fest wie Klartexte zu verschlüsselten Nachrichten, den sogenannten Kryptotexten, transformiert und wieder zurück in den ursprünglichen Klartext entschlüsselt werden. Das Ziel dieser Aktionen ist die Geheimhaltung der in den Nachrichten codierten Informationen gegenüber Dritten.

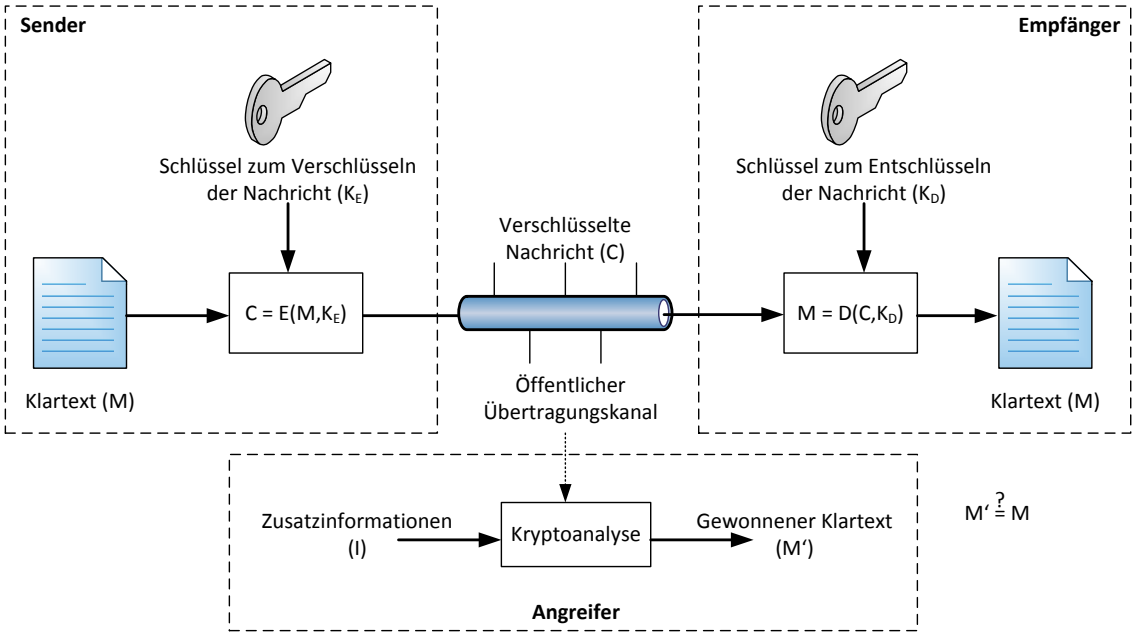


Abbildung 4: Darstellung eines Kryptosystems (Quelle: modifiziert übernommen aus [10, S. 303])

Die einzelnen Komponenten eines Kryptosystems werden in Abbildung 4 dargestellt. Ein Klartext M bestehend aus einem endlichen Zeichensatz soll vom Sender mittels dessen privaten Schlüssels K_E in einen Chiffretext C transformiert werden um über einen öffentlichen Kanal sicher übertragen werden zu können.

Dabei können die Alphabete von M und C auf unterschiedlichen endlichen Zeichensätzen basieren, was jedoch in der Praxis meist nicht vorkommt. Nach Eingang der Nachricht, entschlüsselt der Empfänger den Chiffretext C mit dem passenden Schlüssel K_D und erhält die ursprüngliche Nachricht M. Um sowohl die Methoden der Ver- und Entschlüsselung als auch die Geheimhaltung zu gewährleisten, kann die mit dem Verschlüsselungsschlüssel codierte Nachricht ausschließlich vom dazu passenden Entschlüsselungsschlüssel decodiert werden. [10, S. 302]

In Abbildung 4 werden die Ver- und Entschlüsselungsalgorithmen mittels Blöcke auf Seiten des Senders bzw. des Empfängers dargestellt. Der linke Block stellt den Verschlüsselungsalgorithmus E dar. E generiert mittels des Schlüssels des Senders K_E und dem Klartext M die verschlüsselte Nachricht C. Der Empfänger entschlüsselt diese mit dem Entschlüsselungsalgorithmus D unter Zuhilfenahme des Entschlüsselungsschlüssels K_D. Wird die Nachricht während der Übermittelung von einem Angreifer abgefangen, so kann dieser unter Anwendung von kryptoanalytischen Methoden versuchen die Nachricht zu entschlüsseln. Der Angreifer erhält die encodierte Nachricht M‘. Diese stimmt jedoch nur bei einer korrekten Entschlüsselung mit der ursprünglichen Nachricht M überein. Die Entschlüsselung kann für den Angreifer erleichtert werden, wenn diesem, weitere Zusatzinformationen I zur Verfügung stehen. Solche Zusatzinformationen können beispielsweise die Information über die verwendete Sprache, oder die Information über bestimmte immer wiederkehrende Muster sein. [10, S. 302f]

2.3.3.1 Einsatzbereiche von Kryptographischen Systemen

Es werden kryptographische Verfahren in den unterschiedlichsten sicherheitsrelevanten Bereichen angewandt. So werden für die Identifikation und Authentifikation beispielsweise Verschlüsselungsverfahren eingesetzt um Passwörter sicher abzulegen. Um die Datenintegrität zu gewährleisten werden kryptographische Algorithmen verwendet, welche einen digitalen Fingerabdruck der Daten erstellen. Auch Signaturen werden mit Hilfe von kryptographischen

Methoden erzeugt, um die Verbindlichkeit von Aktion sicherzustellen. Allgemein formuliert, werden kryptographische Methoden verwendet um die Schutzziele der Informationstechnik zu gewährleisten, auf welche bereits im Kapitel 2.2.3 eingegangen wurde. [10, S. 297]

2.3.4 Symmetrische Verfahren

Kennzeichnend für symmetrische Verschlüsselungsverfahren ist, dass sie für die Ver- und Entschlüsselung des Klartextes denselben Schlüssel verwenden, d.h. dass K_E und K_D in Abbildung 4 gleich sind. Dieser Schlüssel muss geheim gehalten werden, da auf diesem die gesamte Sicherheit des eingesetzten Systems beruht. Es ergibt sich daraus das Problem des sicheren Schlüsselaustausches, auf welches in Kapitel 2.3.6 näher eingegangen wird. Für symmetrische Verfahren gibt es zwei Realisierungsvarianten, entweder als Blockchiffren oder als Stromchiffren. Symmetrische Verschlüsselungen sind für die Praxis von großer Relevanz, da diese in der Regel auf einfachen Operationen wie beispielswiese Shifts oder XOR-Verknüpfungen beruhen, welche effizient in Hard- und Software implementierbar sind. [10, S. 316]

2.3.4.1 Blockchiffren

Die Blockchiffren zerteilen einen Klartext in vordefinierte Blöcke bevor die eigentliche Verschlüsselung stattfindet. Die Größe dieser Blöcke wird durch den Algorithmus vorgegeben und stellt das eigentliche Sicherheitskriterium neben dem verwendeten geheimen Schlüssel dar. Für den Einsatz von Blockchiffren muss der Klartext gänzlich vorliegen. Sollte der letzte Block mit dem Klartext nicht vollständig aufgefüllt werden können, so wird dieser mittels „Padding“, also dem Erweitern mittels vordefinierten Zeichen, vervollständigt. Die verschlüsselten Blöcke werden an den Empfänger versendet und von diesem entschlüsselt und anschließend wieder zu einem vollständigen Klartext zusammengefügt. [17, S. 796ff]

Da eine Nachricht, welche öfters mit demselben Verfahren verschlüsselt wird, auch immer wieder dieselbe Nachricht ergeben würde, wurden sogenannte Betriebsmodi (Cipher Modes) eingeführt. Ohne diese könnte mittels kryptoanalytischen Maßnahmen, sogenannten Reply-Attacken (siehe auch Kapitel 2.5.3.6), auf den Klartext geschlossen werden. Alle von Seiten des BSI (siehe hierzu Kapitel 2.3.4.3) empfohlenen Modi verwenden einen sogenannten Initialisierungsvektor. Dieser wird in der Regel zufällig gewählt und mit dem symmetrischen Schlüssel mit übertragen, damit der Empfänger die Nachricht auch wieder entschlüsseln kann. [17, S. 805ff]

Moderne Blockchiffren sind verschachtelt aufgebaut, so dass mehrere Runden durchlaufen werden. Durch diese Rundendurchläufe werden die Grundprinzipien der Diffusion und Konfusion gewährleistet. Unter Diffusion versteht man die Verteilung der im Klartext enthaltenen Information auf möglichst große Bereiche des Geheimtextes. Im Gegensatz dazu beschreibt die Konfusion die Verschleierung des Zusammenhangs zwischen Klar- und Geheimtext. [18, S. 118]

2.3.4.2 Stromchiffren

Stromchiffren verarbeiten Folgen von kleinen Klartexteinheiten mittels sequentiellen Chiffren. Diese Einheiten werden separat verschlüsselt und an den Empfänger übermittelt. In Abgrenzung zu den größeren Einheiten der Blockchiffren, bezeichnet man die kleinen Klartexteinheiten bei den Stromchiffren als Zeichen. Dabei sind gängige Zeichengrößen 1 Bit oder 1 Byte. Im Gegensatz zu den Blockchiffren muss der Klartext allerdings nicht bereits zu Beginn der Verschlüsselung vollständig vorliegen. [10, S. 320f]

$$C_1 \text{ XOR } C_2 = (M_1 \text{ XOR Key}) \text{ XOR } (M_2 \text{ XOR Key}) = M_1 \text{ XOR } M_2$$

Code 1: Known Plaintext Angriff auf eine Stromchiffre (Quelle: [10, S. 322])

Ein Stromalgorithmus generiert im Gegensatz zum Blockalgorithmus eine pseudozufällige Folge von Bits, welche mit den Klartextdaten XOR-addiert wird. Diese Folge wird als Schlüsselstrom bezeichnet, da sie nur durch die Kenntnis des

geheimen Schlüssels generiert werden kann. Wie bei den vielen Blockchiffren verwenden Stromchiffren einen Initialisierungsvektor, welcher zusammen mit dem geheimen Schlüssel ausgetauscht werden muss. Das Problem welches sich hieraus ergibt ist, dass ein Angreifer alleine durch das Abhören zweier Geheimtexte die XOR verknüpften Klartexte bekommt, wie in Code 1 gezeigt wird. Kann der Angreifer nun einen eigenen Klartext (M_2) mittels Algorithmus verschlüsseln lassen (C_2), also dem Opfer gezielt unterschieben, so kann er aus diesen Informationen alle weiteren Nachrichten welche mit dem Schlüsselstrom codiert wurden entschlüsseln. Diese Angriffsmethode wird Known Plaintext Angriff bezeichnet und in Kapitel 2.5.3.2 näher beschrieben. [10, S. 321f]

2.3.4.3 Empfehlungen des BSI zu symmetrischen Verschlüsselungsverfahren

Das deutsche Bundesamt für Sicherheit in der Informationstechnik empfiehlt die Verwendung des AES Verschlüsselungsverfahrens, welches ein symmetrisches Blockchiffren-Verfahren ist. Gemäß der BSI-Empfehlung, sollen nur Blockchiffren mit einer Blockgröße von mindestens 128 Bit zum Einsatz kommen. Weiters sind viele verschiedene Arten von Betriebsmodi definiert und stehen den Anwenderinnen und Anwender zur Verfügung. Von Seiten des BSI werden jedoch lediglich die Betriebsarten „Galois/Counter-Mode“ (GCM), „Cipher-Block Chaining“ (CBC) und „Counter Mode“ (CTR) empfohlen. [19, S. 23f]

Das BSI gibt außerdem an, dass momentan keine Stromchiffre empfohlen wird. Sollte dennoch eine Stromchiffre eingesetzt werden, so ist die Integrität der übertragenen Informationen durch separate kryptographische Mechanismen zu schützen. Ein angreifendes Subjekt könnte in Abwesenheit solcher Mechanismen bitgenaue Änderungen am Klartext vornehmen. [19, S. 26]

2.3.5 Asymmetrische Verfahren

Asymmetrische Verschlüsselungsverfahren werden auch als Public-Key Verfahren bezeichnet, da bei dieser Art der Verschlüsselung mit einem privaten, also geheimen und einem öffentlichen Schlüssel gearbeitet wird. Diese beiden Schlüssel werden als Schlüsselpaar bezeichnet. Für die asymmetrischen Verfahren gelten gemäß Eckert [10, S. 345] die folgende Bedingungen:

- Die Schlüsselpaare K_E und K_D müssen leicht und effizient zu erzeugen sein, wobei der Schlüssel K_E auch öffentlich gemacht werden kann.
- Weiters gilt, dass K_D eine mittels K_E encodierte Nachricht wieder entschlüsseln kann.
- Sowohl die Verschlüsselungsfunktion E, als auch die Entschlüsselungsfunktion D müssen effizient zu berechnen sein.
- Der Schlüssel K_D darf aus der Kenntnis von K_E nicht mit vertretbarem Aufwand berechenbar sein.
- Treffen die Bedingungen zu, dass eine mittels K_D encodierte Nachricht auch mit dem Schlüssel K_E decodiert werden kann und die Mengen an möglichen Klar- bzw. Chiffretexten gleich groß sind, so kann das Verfahren auch zur Signierung eingesetzt werden, auf welche in Kapitel 2.3.8 näher eingegangen wird.

Aus den angeführten Anforderungen lässt sich erkennen, dass eine Funktion gesucht werden muss, welche auch mit der Kenntnis des öffentlichen Schlüssels nicht zulässt, dass der private Schlüssel effizient berechnet werden kann. Derartige Funktionen werden als Einweg-Funktionen bezeichnet. Da aber eine solche Funktion auch für jene mit dem passenden Decodierungsschlüssel eine fast unüberwindbare Hürde darstellen würde, muss eine zusätzliche Anforderung an die Funktion gestellt werden. Es muss mittels eines Geheimnisses möglich sein, die Einweg-Funktion effizient umzukehren. Dieses Geheimnis stellt der private Schlüssel dar. Eine derartige Funktion wird als Einweg-Funktion mit Falltür bezeichnet. [10, S. 346f]

2.3.5.1 Empfehlungen des BSI zu asymmetrischen Verschlüsselungsverfahren

Da die asymmetrischen Verfahren für den Austausch der symmetrischen Schlüssel verwendet werden, sollen diese gemäß BSI [19] auch über einen stärkeren Schlüssel verfügen. Dies wird dadurch begründet, dass mit dem asymmetrischen Verfahren vor einem Schlüsselwechsel in der Regel viele Schlüssel für ein symmetrisches Verfahren verschlüsselt und übermittelt werden.

In der aktuellen technischen Richtlinie für empfohlene kryptographische Verfahren und Schlüssellängen [19] gibt das BSI die in Tabelle 2 angegebenen Werte bekannt. Von Seiten des BSI wird weiters angemerkt, dass die Schlüssellänge von RSA und DLIES für einen Verwendungszeitraum über das Jahr 2022 hinaus auf 3000 Bit angehoben werden sollte. [19, S. 29]

Verfahren	ECIS	DLIES	RSA
Schlüssellänge in Bit	250	2000	2000

Tabelle 2: Übersicht der vom BSI empfohlenen asynchronen Verfahren und Schlüssellängen (Quelle: [19, S. 29])

2.3.6 Hybride Verfahren

Es werden die beiden bereits beschriebenen Klassen der symmetrischen und asymmetrischen Verfahren in heutigen IT Systemen häufig in Kombination gesetzt. Man spricht in diesem Zusammenhang von hybriden Systemen. [10, S. 304]

Gemäß dem deutschen Bundesamt für Sicherheit in der Informationstechnik [20] sollen aus Performancegründen in der Praxis für die meisten Anwendungen keine reinen asymmetrischen Implementierungen eingesetzt werden. Das Problem an asymmetrischen Verfahren liegt in der Verarbeitungsgeschwindigkeit. Durch die beispielsweise in RSA verwendeten Operationen, sowie die großen Zahlen, welche den Klartext repräsentieren, ist eine Ver- und Entschlüsselung wesentlich

langsamer als mit einem symmetrischen Verfahren. Aus diesem Grund werden asymmetrische Verfahren in der Praxis oftmals nicht für die Verschlüsselung, sondern für den Austausch des symmetrischen Schlüssels verwendet. [10, S. 354]

2.3.7 Hashfunktionen

Hashfunktionen erstellen sogenannte digitale Fingerabdrücke von Datenobjekten, mittels welchen die Integrität des Objektes überprüft und etwaige unautorisierte Manipulationen aufgedeckt werden können. Neben der Überprüfung der Integrität ist es unter Zuhilfenahme eines Schlüssels auch möglich die Authentizität des Datenursprungs zu überprüfen, wie in Kapitel 2.3.7.2 beschrieben wird. [10, S. 379f]

Eine Hashfunktion ist eine nicht injektive Abbildung, welche ein jedes Objekt beliebiger Länge auf eine Hashadresse mit fester Länge abbildet. Da die Funktionen jedoch nicht injektiv sind und der abzubildende Adressbereich meist sehr viel größer als der Zielbereich ist, können sogenannte Kollisionen auftreten. Von einer Kollision spricht man, wenn zwei unterschiedliche Objekte auf denselben Hashwert abgebildet werden. Im Bereich der Kryptographie bereitet dieser Umstand erhebliche Probleme, da eine Nachricht über den Hashwert charakterisiert und deren Integrität überprüft wird. Durch eine hinreichende große Länge des Hashwerts kann die Wahrscheinlichkeit einer Kollision signifikant reduziert werden. Außerdem spielt die Tatsache eine Rolle, ob es sich um eine schwach oder stark kollisionsresistente Hashfunktion handelt. [10, S. 380ff]

Von einer schwach kollisionsresistenten Hashfunktion spricht man, wenn diese gemäß Eckert [10, S. 381] die folgenden Anforderungen erfüllt:

- Die Hashfunktion hat die Eigenschaft einer Einweg-Funktion, mittels welcher der Hashwert leicht zu berechnen ist. Weiters darf es nicht effizient möglich sein, den ursprünglichen Wert zu berechnen.
- Es ist bei gegebenen Hashwert nicht effizient möglich eine dazu passende Nachricht zu bestimmen, welche denselben Hashwert liefert.

Weist die Funktion des Weiteren noch die Eigenschaft auf, dass es nicht effizient möglich ist, dass zwei verschiedene Werte gefunden werden, welche den selben Hashwert ergeben, so spricht man nicht mehr von einer schwachen, sondern starken kollisionsresistenten Hashfunktion. [10, S. 383]

2.3.7.1 Empfehlungen des BSI zu Hashfunktionen

Von Seiten des deutschen Bundesamts für Sicherheit in der Informationstechnik werden nur stark kollisionsresistente Hashfunktion empfohlen. Im Detail werden die Funktionen SHA-256, SHA-512/256, SHA-384, SHA-512, SHA3-256, SHA3-384 und SHA3-512 angeführt. [19, S. 40f]

2.3.7.2 Message Authentication Code

Der Message Authentication Code (MAC) stellt eine Spezialform der Hashfunktionen dar, da bei dieser Ausprägung mittels Zuhilfenahme eines Schlüssels auch Aussagen über die Authentizität der erzeugenden Instanz gemacht werden können. Es muss angemerkt werden, dass es sich hierbei allerdings um eine sehr schwache Ausprägung des in Kapitel 2.2.3.1 definierten Begriffs handelt, da über die Daten selbst keine Authentizitätsaussagen möglich sind. [10, S. 391f]

Bei der Verwendung des Verfahrens wird ein gemeinsamer geheimer Schlüssel vereinbart, welcher zur Generierung eines MAC-Werts verwendet wird. Dieser Wert wird mit dem Originaldokument mitversandt. Die Empfangsstelle überprüft den Code indem er die MAC-Funktion ebenfalls über das Dokument ausführt. Bei Wertegleichheit ist das Dokument authentisch. [10, S. 392]

2.3.8 Elektronische Signaturen

Wie bereits beschrieben, kann durch den Einsatz von Hashfunktionen oder MACs die Urheberschaft einer Nachricht nicht zweifelsfrei bestimmt werden. Um digitale Dokumente einer Person zuordnen zu können, werden Signaturen eingesetzt, welche als digitales Gegenstück zur handschriftlichen Unterschrift gesehen werden können. Daraus lassen sich die Anforderungen an eine Signatur ableiten. So muss diese die Identität des Signaturgebers zweifelsfrei bestätigen, nicht wiederverwendbar und nur in Zusammenhang mit dem Originaldokument gültig sein. Außerdem darf ein signiertes Dokument nicht verändert werden können, oder muss eine nachträgliche Änderung erkennbar sein. Weiters darf die unterzeichnende Person die Signierung im Nachhinein nicht abstreiten können. Da die Signatur vom jeweiligen Dokument abhängig ist, besteht eine Relation zwischen der Integrität der signierten Nachricht und der Authentizität des Signierenden. Da Signaturen überprüfbar und nachzuweisen sind, sind sie auch rechtsgültig beweisbar. [10, S. 293f]

Grundsätzlich können für Signaturen auch symmetrische Verfahren eingesetzt werden. Da gemäß der BSI Empfehlungen [19, S. 44f] jedoch nur asymmetrische Verfahren eingesetzt werden sollen, wird nur auf diese näher eingegangen. Die Anforderungen an solche Verfahren wurden bereits in Kapitel 2.3.5 behandelt.

Die Daten werden in Signaturalgorithmen zunächst mittels Hashfunktionen auf eine fixe Länge gebracht. Danach wird aus diesem Hashwert die Signatur mit Hilfe des geheimen Schlüssels des Signaturausstellers berechnet. Will eine andere Person die Signatur verifizieren, so braucht es lediglich den öffentlichen Schlüssel des Ausstellers um auf den Hashwert des Dokuments zu kommen, welcher leicht überprüfbar ist. Zur Verteilung der Schlüssel wird meist ein Public-Key Verfahren eingesetzt, welches in Kapitel 2.3.9.2 beschrieben wird. [19, S. 44f]

2.3.8.1 Empfehlungen des BSI zu elektronischen Signaturen

Gemäß der BSI Empfehlung, sollen lediglich asymmetrische Verfahren eingesetzt werden, da ein gesicherter Schlüsselaustausch gegeben sein muss. Es gelten hierbei unter anderem die Empfehlungen an asymmetrische Verfahren, an die Hashfunktionen, an das Schlüsselmanagement, welches in Kapitel 2.3.9 beschrieben wird und an die Signatur selbst. Es werden konkret das RSA-Verfahren, das DSA-Verfahren, mehrere DSA-Varianten auf elliptischen Kurven (ECDSA, ECKDSA und ECGDSA), sowie Merkle-Signaturen empfohlen. [19, S. 45]

2.3.9 Schlüsselmanagement

Gemäß dem in Kapitel 2.3.2 angeführten Kerckhoffschen Prinzip ist die Sicherheit eines kryptographischen Systems vom verwendeten Schlüssel abhängig. Die Hauptaufgaben des Schlüsselmanagements bestehen nach Eckert [10, S. 415] aus der sicheren Erzeugung, Verteilung, Zertifizierung, Speicherung beziehungsweise Archivierung, sowie der Vernichtung von Schlüsseln.

2.3.9.1 Zertifikate

Mittels eines Zertifikats erfolgt die digitale Zuordnung einer natürlichen oder juristischen Person zu einem öffentlichen Signierschlüssel. Dabei kann das Zertifikat naturgemäß keine Aussage über den Inhalt eines signierten Dokumentes bzw. über die Vertrauenswürdigkeit der signierenden Person machen. Erst durch die Verwendung von Zertifikaten, können im Nachrichtenverkehr die Schutzziele Authentizität, Vertraulichkeit und Integrität von Daten gewährleistet werden. [10, S. 415]

<u>Der X.509 Standard</u>

Der Aufbau und die Struktur von in der Praxis üblichen Zertifikaten, werden durch den X.509 Standard festgelegt. Dieser Standard wurde im Mai 2017 zuletzt

von der International Organization for Standardization (ISO) überarbeitet und als ISO/IEC 9594-8 [21] herausgegeben. Grob teilt sich ein X.509-Zertifikat in einen Zertifikats- und einen Signaturabschnitt. Ein Beispielzertifikat findet sich im Anhang A, wobei der Zertifikatsteil schwarz und der Signaturabschnitt grün gekennzeichnet ist. Eine ausführliche Beschreibung findet sich im RFC 3280 [22]. Gemäß dem Standard muss ein Zertifikat mindestens die Inhalte aufweisen, welche in Tabelle 3 angeführt sind.

Inhalt	**Erklärung**
version	Beschreibt das verwendete Zertifikatsformat
serialNumber	Eindeutiger Identifikator des Zertifikats
signature	Verwendete Algorithmen und Parameter
issuer	Name der ausstellenden Instanz (CA)
validity	Angabe eines Zeitintervalls wie lange das Zertifikat gültig ist
subject	Eindeutiger Name eines Users
subjectPublicKeyInfo	Schlüssel des Users und die eingesetzten Algorithmen
issuerUniqueID	Eindeutige ID der ausstellenden Instanz (optional ab Version v2)
subjectUniqueID	Eindeutige ID des Inhabers bzw. der Inhaberin (optional ab Version v2)
extensions	Erweiterungen

Tabelle 3: Struktur eines X.509 Zertifikates (Quelle: [22, S. 15f], [10, S. 416])

Mittels der Versionsnummer können Änderungen der Formatfestlegung nachvollzogen werden. Dies ist wichtig, da momentan bereits die Version 3 im Einsatz ist und mittels dieses Verfahrens eine Abwärtskompatibilität ermöglicht wird. Die ausstellende Instanz muss sicherstellen, dass keine Zertifikate mit gleichen Seriennummern vergeben werden, da über diese Nummern Zertifikate zurückgerufen, also ungültig gemacht werden können. Weiters ist ein Zertifikat ungültig wenn die Gültigkeitsdauer abgelaufen ist. Diese wird im Zertifikat mit angegeben um vom Empfänger rasch überprüft werden zu können. Möchte eine Person mehr als ein Zertifikat verwenden, so ist dies möglich, da im Feld „subject“ eine Person zwar eindeutig angegeben werden muss, aber mehrere Zertifikate

derselben Person zugeordnet werden können. Damit ein Zertifikat verifiziert werden kann, werden die Informationen bezüglich der verwendeten Verfahren, sowie der öffentliche Schlüssel der Zertifizierungsstelle benötigt. Diese werden im Zertifikat, ebenso wie der eindeutige Name der ausstellenden Instanz mit angegeben. [10, S. 416f]

2.3.9.2 Public Key Infrastructure

Um die Erzeugung und Verwaltung von Zertifikaten zu ermöglichen, werden spezielle Infrastrukturen eingesetzt. Diese werden im Bereich der asymmetrischen Kryptosysteme, Public Key Infrastructure (PKI) genannt. Diese PKI bestehen aus den Certification Authorities (CA), den Registration Authorities (RA) und dem Verzeichnisdienst, dem sogenannten Repository. [10, S. 421f]

Die Zertifikate werden von unabhängigen Stellen, den sogenannten Certification Authorities oder Zertifizierungsstellen, ausgegeben. Zuvor muss jedoch die Identität der Person in der Registration Authority überprüft und dieser ein eindeutiger Name zugewiesen werden. Die RA bürgt für die Verbindung zwischen dem öffentlichen Schlüssel und der Identität einer Person. Danach kann ein bestehendes oder neu generiertes Schlüsselpaar zusammen mit den Personendaten von Seiten der CA für ein Zertifikat verwendet werden. Bei der Erstellung von Zertifikaten wird dieses mit dem privaten Schlüssel der CA signiert. Damit das Zertifikat von Extern über den öffentlichen Schlüssel der CA überprüft werden kann, wird es im Repository verwaltet und zur Verfügung gestellt. Die Komponenten CA und RA werden häufig in einem sogenannten Trust Center zusammengefasst. [10, S. 417ff]

Die Zertifizierungsstelle ist neben der Erstellung auch für das Zurückziehen, also für die Erstellung eines Sperrvermerkes von Zertifikaten verantwortlich. Soll ein Zertifikat ungültig werden, so listet die CA, welche das betreffende Zertifikat ausgestellt hat, dieses in der sogenannten Certificate Revocation List (CRL). Die CRL wird ebenso wie die Zertifikate im Repository veröffentlicht. [10, S. 422ff]

Damit nicht eine Zertifizierungsstelle weltweit alle Zertifikate ausgeben muss, wurde eine hierarchische Ordnung eingeführt, welche eine flexible und skalierbare Verwaltung zulässt und in Abbildung 5 dargestellt wird. Da eine einzelne zentrale Instanz wohl auch nicht akzeptiert werden würde, können mehrere sogenannte Root-CAs eine eigene PKI Struktur aufbauen. Diese signieren die Zertifikate der darunterliegenden regionalen Authorities welche wiederum die darunterliegenden CAs signieren. Dieser Prozess kann je nach Anwendungsfall in beliebig vielen Stufen unterteilt werden. Die Kette an Zertifikaten wird als Chain of Trust bezeichnet. Es ergibt sich jedoch das Problem, dass keine übergeordnete Stelle das Zertifikat der Root-CA signieren kann. Aus diesem Grund erfolgt die Signierung durch den privaten Schlüssel der Root selbst. Das Zertifikat der Root wird auch als Stammzertifikat bezeichnet. [17, S. 828ff], [10, S. 423f]

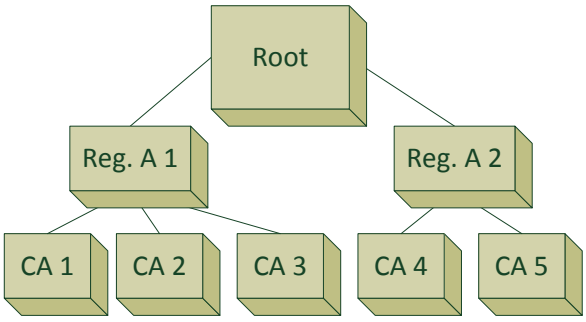


Abbildung 5: Hierarchische Struktur einer PKI (Quelle: eigene Darstellung nach [17, S. 829])

2.4 Spezielle Protokolle während der Cloud-Kommunikation

Von Seiten des BSI Deutschland, wird im IT Grundschutz unter Kapitel „M 5.174 Absicherung der Kommunikation zum Cloud-Zugriff“ [23] auf das Thema der sicheren Übertragung während der Nutzung von Cloud-Diensten eingegangen. Hierbei müssen gemäß dem BSI, sowohl sichere Schnittstellen, als auch Protokolle genutzt werden, welche eine verschlüsselte Kommunikation zwischen Cloud-

Provider und Cloud-Benutzerinnen und -Benutzer ermöglichen. Es wird auf die Verwendung des Hypertext Transfer Protocol Secure „HTTPS“ Protokolls anstatt des Hypertext Transfer Protocol „HTTP“ hingewiesen, welches auf SSL bzw. TLS basiert.

In den folgenden Kapiteln, wird auf die beiden Protokolle TLS und SSH näher eingegangen.

2.4.1 TLS

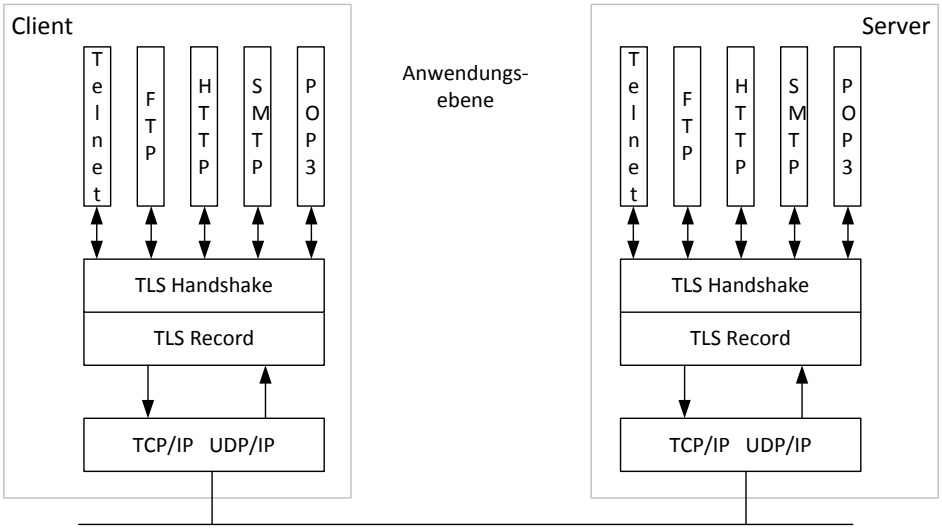


Abbildung 6: Schichteneinordnung des SSL/TLS Protokolls (Quelle: modifizierte Darstellung nach [10, S. 811])

Das Transport Layer Security (TLS) Protokoll, welches ursprünglich als Secure Socket Layer (SSL) Protokoll entwickelt wurde, setzt gemäß dem Open Systems Interconnection (OSI) Model auf der Transportschicht auf. Es besteht aus den beiden Teilschichten TLS Record Layer und dem darauf aufsetzenden TLS Handshake Layer, wie in Abbildung 6 gezeigt wird. Die Einordnung ins OSI Modell verdeutlicht, dass TLS Aufgaben der Sitzungs- und Präsentationsschicht übernimmt, was den Vorteil birgt, dass Zustandsinformationen über einen längeren Zeitraum und verschiedene Einzelverbindungen hinweg gespeichert und für die Verwaltung genutzt werden können. Im Beispiel des HTTP Protokolls

bedeutet das, dass mehrere Verbindungen zu einer Sitzung gebündelt und somit effizienter verwaltet werden können. Mit TLS hat sich mittlerweile ein de facto Standard für sichere HTTP Verbindungen etabliert, der von allen gängigen Browsern unterstützt wird, wie in Kapitel 2.4.1.5 beschrieben wird. [10, S. 809ff]

Das TLS Protokoll soll die Schutzziele der Authentizität, der Integrität und der Vertraulichkeit gewährleisten. Die Authentifizierung erfolgt in TLS mittels asymmetrischen Verschlüsselungsverfahren und Zertifikaten, während die Vertraulichkeit mittels End-to-End Datenverschlüsselung unter Nutzung eines gemeinsamen symmetrischen Sitzungsschlüssels sichergestellt wird. Für die bidirektionale Verbindung zwischen Server und Client werden zwei unterschiedliche Sitzungsschlüssel verwendet. Die Integrität der transportierten Nachricht wird mittels Message Authentication Codes garantiert. Die für die kryptographische Sicherheit verwendeten Verfahren werden für jede Verbindung bzw. für jede Sitzung welche mehrere Verbindungen umfassen kann, neu abgestimmt. [10, S. 810f]

2.4.1.1 TLS Handshake Protokoll

Das TLS Protokoll ist zustandsbehaftet, wodurch Sitzungen zwischen Kommunikationspartnern etabliert werden können. Ein Client kann dabei mehrere solcher Sitzungen zu einem oder mehreren Servern gleichzeitig unterhalten. Mittels des Handshake Protokolls werden diese Sitzungsinformationen koordiniert und konsistent gehalten. In Abbildung 7 wird der Ablauf des TLS Handshakes veranschaulicht. [10, S. 813]

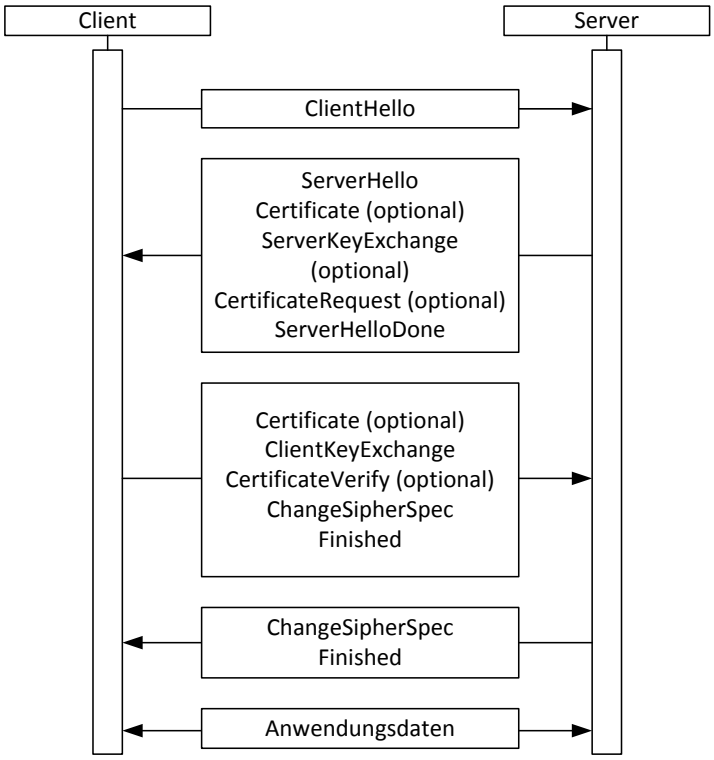


Abbildung 7: TLS Handshake Protokoll (Quelle: eigene Darstellung nach [10, S. 814])

Mittels einer ClientHello Nachricht des Clients wird eine Verbindung zum Server initiiert. Diese Nachricht enthält bereits Informationen welche später zur Berechnung des gemeinsamen Schlüssels erforderlich sind. Die wichtigsten sind eine Datenstruktur mit einem Zeitstempel und Zufallszahl, einer Sitzungs-ID und einer Cipher Suite der vom Client unterstützten Verfahren. Der Server antwortet auf die Anfrage des Client mit einer Hello-Nachricht, welche ebenso eine Datenstruktur aus Zeitstempel, Zufallszahl und Verfahren aufweist. Die Algorithmen, welche der Server an den Client übermittelt, entsprechen jenen, welche vom Server bevorzugt und von beiden Systemen verstanden werden. Soll der Server authentifiziert werden, so muss er dem Client sein Zertifikat zukommen lassen, welches dem im Client-Hello geforderten Format zu entsprechen hat. Falls der Server ebenfalls ein Zertifikat vom Client fordert, so erfolgt der Vorgang vice-versa. In der optionalen CertificateRequest Nachricht gibt der Server X.500 Namen von denjenigen CAs an, denen er vertraut und teilt dem Client weiters mit, welche

Verfahren er beherrscht. Wird kein Zertifikat versendet, so übermittelt der Server dem Client einen temporären öffentlichen RSA Schlüssel. Nach Erhalt der Daten vom Server kontrolliert der Client zunächst die Gültigkeit des übermittelten Zertifikates. Weiters prüft er ob die vom Server übermittelten Verfahren tatsächlich denen im ClientHello angebotenen entsprechen. Ist dies der Fall, so sendet der Client mittels ClientKeyExchange das 48 Byte Pre-Master-Secret verschlüsselt an den Server. Hierbei wird das abgestimmte Verschlüsselungsverfahren eingesetzt. Das Pre-Master-Secret wird sowohl vom Client als auch vom Server, zusammen mit den beiden Zufallszahlen verwendet um die geheimen Schlüssel zu errechnen. Falls vom Server ein Client-Zertifikat verlangt wurde, sendet dieser die CertificateVerify Nachricht zur Überprüfung an den Server. Mit der ChangeCipherSpec Meldung zeigen beide Teilnehmer an, dass sie ab diesem Zeitpunkt die ausgehandelten kryptographischen Verfahren verwenden. Als Abschluss signalisieren beide die erfolgreiche Beendigung der Datenvereinbarung mittels eines Finish-Telegramms. [10, S. 813ff]

2.4.1.2 TLS Record Protokoll

Die TLS Record Schicht hat die Aufgabe, Datenpakete in TLS-Records mit einer vorgegebenen maximalen Größe von 2^{14} Byte zu fragmentieren und optional zu komprimieren. Anschließend wird mittels MAC-Verfahren ein Hash gebildet und an den Record angehängt. Dieses Paket wird verschlüsselt und mit einem Record-Header versehen. Dieser enthält unter anderem Informationen über die verwendete TLS-Version, den Content-Type, der angibt, welches TLS-Protokoll zu verwenden ist, sowie die Länge der Bytes des Klartextfragments. Dieser Vorgang wird in Abbildung 8 dargestellt. Das TLS Record Protokoll verwendet das vom Handshake Protokoll vereinbarte Master Secret und leitet daraus die für die konkrete Verbindung benötigten Schlüssel ab. Wie einleitend beschrieben, wird in TLS zwischen Sitzung und Verbindung unterschieden, wobei eine Sitzung mehrere Verbindungen umfassen kann. Die verwendeten Schlüssel gelten jeweils für eine Verbindung, während für alle Verbindungen einer Sitzung dieselben Verfahren

verwendet werden. Aus diesem Grund kann bei einer erneuten Verbindung auf das Aushandeln der Verfahren im Handshake verzichtet werden. [10, S. 817ff]

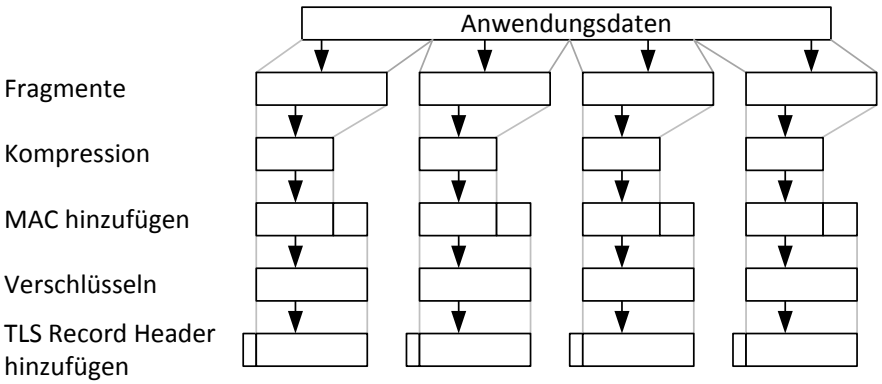


Abbildung 8: Aufgaben des TLS Record Protokolls (Quelle: eigene Darstellung nach [10, S. 817]

2.4.1.3 Zusammenarbeit zwischen SSL und TLS

Die Unterschiede zwischen TLS 1.0 und SSL 3.0 sind nicht dramatisch, aber groß genug, dass die beiden Protokolle nicht zusammenarbeiten, wie im RFC 2246 [24] des TLS Protokolls beschrieben wird. Die Internet Engineering Task Force (IETF) hat zuerst im Jahr 2011 (siehe RFC 6176 [25]) das SSL 2.0 Protokoll und dann im Jahr 2015 ebenso die Version SSL 3.0 (siehe hierzu RFC 7568 [26]) als unsicher eingestuft, als immer wieder Sicherheitslücken aufgedeckt wurden. [27]

2.4.1.4 Reservierte Ports

Bezeichnung	Portadresse	Bedeutung
https	443	TLS-basiertes HTTP
ssmtp	465	TLS-basiertes SMTP
snntp	563	TLS-basiertes NNTP
telnet	992	TLS-basiertes Telnet
ftps	990	TLS-basiertes FTP (Kontrollnachrichten)
ftp-data	889	TLS-basiertes FTP (Daten)

Tabelle 4: Auszug reservierter TLS-Portadressen (Quelle: eigene Darstellung nach [10, S. 813])

Damit nicht in jedem Protokoll, welches mit TLS gekapselt werden soll, eine Adaptierung zur Aushandlung des TLS Vorgangs erfolgen muss, wurden von der

IANA spezielle Portadressen reserviert. Wird ein derartiger Port angesprochen, so kann davon ausgegangen werden, dass der betreffende Dienst TLS-basiert ausgeführt werden soll. Eine Übersicht der wichtigsten Portadressen findet sich in Tabelle 4. [10, S. 812f]

2.4.1.5 Fallstudie Hypertext Transfer Protocol Secure (HTTPS)

Das HTTPS Protokoll stellt eine Erweiterung des HTTP Protokolls dar, indem es eine zusätzliche Schicht zwischen HTTP und TCP einzieht, wie in Abbildung 6 gezeigt wird. Das TLS Verfahren kapselt die Daten des HTTP Protokolls um die Schutzziele Authentizität, Integrität und Vertraulichkeit sicherzustellen. Ohne der TLS Erweiterung könnte keine Authentifizierung oder Verschlüsselung einer HTTP-Verbindung stattfinden und die Kommunikation würde ungeschützt von statten gehen. Die Aushandlung der TLS Parameter erfolgt gemäß Abbildung 7, wobei als Anwendungsdaten die HTTP-Datenpakete zu verstehen sind. Um eine verschlüsselte Verbindung in einem Browser zu initiieren, gibt man statt des „http://“ ein „https://“ in das Schema der aufzurufenden URL ein. Der Browser öffnet daraufhin eine Verbindung auf das Port 443 des Servers anstatt auf das sonst in HTTP üblichen Port 80. [28]

2.4.1.6 Sicherheitslücken und bekannte sicherheitsrelevante Probleme in TLS

Es sind seit September 2011 mehrere Sicherheitslücken im TLS Protokoll bekannt geworden, welche in Tabelle 5 angeführt werden.

Datum	**Name**	**Sicherheitslücke**	**Gegenmaßnahme**
Sep. 2011	Beast	TLS 1.0 und ältere Protokolle führen zu Sicherheitslücken auf der Client Seite	Nur AES-GCM Suiten verwenden, die nur in TLS 1.2 unterstützt werden.
Aug. 2012	Breach	Lässt Klartextdaten durchsickern	HTTP-Komprimierung deaktivieren
Feb. 2013	Lucky13	Alle TLS- und DTLS-Cypher Suites, die	OpenSSL, NSS und zugehörige

		Verschlüsselung im CBC-Modus enthalten, sind potenziell anfällig	Verschlüsselungsbibliotheken updaten
Jun. 2013	Crime	Angreifer können Daten nutzen, die durch Komprimierung durchgesickert sind, um Klartext teilweise zu gewinnen	TLS/SPDY-Komprimierung deaktivieren
Apr. 2014	Heartbleed	OpenSSL-Bug, der ausgenutzt werden konnte, um die privaten SSL-Schlüssel abzugreifen und somit die Sicherheit der Benutzerdaten zu kompromittieren	OpenSSL updaten; SSL-Zertifikate widerrufen und neu ausstellen; Benutzer ihre Passwörter ändern lassen
Okt. 2014	Poodle	Angreifer können Server dazu bringen, wieder auf SSLv3 zurückzugreifen	SSLv3 deaktivieren oder TLS_FALLBACK_SCSV implementieren, wenn Sie ältere Browser unterstützen müssen
Mär. 2015	Bar Mitzvah Angriff	Nutzt veraltete RC4-Verschlüsselung aus	RC4 deaktivieren
Mär. 2015	Freak	Clients können von starker RSA auf Export-RSA heruntergestuft werden, wenn sowohl Browser und Server anfällig sind	Export-Verschlüsselung in Serverkonfigurationen deaktivieren; OpenSSL patchen; User sollten Browser upgraden
Mai 2015	Logjam	Server, die Duffie-Hellman-Schlüsselaustausch verwenden, sind dafür anfällig, dass ihre Sitzungen auf extrem schwaches 512-Bit-Schlüsselmaterial heruntergestuft werden	DHE_EXPORT-Verschlüsselung deaktivieren; Kundinnen und Kunden sollten ihre Browser upgraden
Mär. 2016	Drown	Sites, die SSLv2 und EXPORT-Cypher Suites unterstützen	SSLv2 deaktivieren und/oder OpenSSL updaten

Tabelle 5: SSL/TLS Sicherheitslücken und Gegenmaßnahmen (Quelle: eigene Darstellung nach [29])

Fallbeispiel Heartbleed-Exploit

Beispielhaft wird auf den Heartbleed-Exploit eingegangen, welcher eine Sicherheitslücke darstellt, die in den letzten Jahren nicht nur in IT Foren, sondern auch im Fernsehen und Radio thematisiert wurde.

Die sogenannte Heartbeat Funktionalität wurde in TLS eingebaut, um eine bestehende Client-Server Verbindung aufrecht zu erhalten. Hierzu wird von einem Kommunikationspartner eine Payload mit beliebigem Inhalt an den anderen Teilnehmer gesendet. Dieser empfängt die Daten und sendet daraufhin exakt dieselben Daten wieder zurück. Dadurch wird bestätigt, dass die Verbindung in Ordnung ist. Siehe hierzu auch [30]. In der praktischen Umsetzung der TLS Heartbeat Funktion in OpenSSL wurde jedoch nicht überprüft, wie lange die empfangene Payload tatsächlich ist. Es wurde angenommen, dass der Eintrag „payload_length“ im Header des Payload Pakets der tatsächlichen Länge entspricht. Hat ein Angreifer jedoch einen geringeren Wert, als die tatsächliche Payload Länge eingetragen, so sendet der Empfänger die Payload inklusive der nachstehenden Speicherstellen an den Angreifer zurück. Der Angreifer kann somit den Arbeitsspeicher des Opfers auslesen. [31]

Gemäß den Daten von Netcraft [32] war zum Zeitpunkt des Bekanntwerdens des Implementierungsfehlers, auf rund 17 Prozent aller Webserver welche TLS verwenden, auch die Heartbeat Funktion im Einsatz. Bei einer Überprüfung der laut Alexa [33] Top 10.000 Sites, erlaubten 628 Server den Zugriff auf den Arbeitsspeicher über diese Sicherheitslücke. Siehe hierzu auch [31].

Der Heartbleed Bug, welcher in CVE-2014-0160 [34] offiziell reportet wird, resultierte nicht aus einem fehlerhaften Design des TLS Protokolls, sondern aus dessen fehlerhaften Implementierung. [35]

2.4.1.7 Empfehlungen von Seiten des BSI zu TLS

Wie bereits einleitend beschrieben, werden von Seiten der IETF die SSH Protokolle als unsicher eingestuft und sollten somit nicht mehr verwendet werden. Von Seiten des BSI wird weiters angemerkt, dass weder TLS 1.0, noch TLS in der Version 1.1 zum Einsatz kommen sollen. Lediglich TLS Version 1.2 wird von Seiten des BSI als sicher eingestuft und empfohlen. In der Publikation des BSI werden Empfehlungen zu Cipher-Suiten getroffen, wobei darauf aufmerksam gemacht wird, dass jene mit Perfect Forward Secrecy zu bevorzugen sind. Unter dem Begriff Perfect Forward Secrecy wird die Eigenschaft des Protokolls verstanden, dass eine Verbindung auch bei Kenntnis der Langzeitschlüssel der Kommunikationspartner nicht nachträglich entschlüsselt werden kann. Es wird weiters auf einige in Kapitel 2.4.1.6 angeführten Sicherheitslücken eingegangen und erörtert, wie mit diesen umgegangen werden soll. Auch wird angeführt, dass eine Authentifizierung zumindest auf Serverseite gegeben sein muss, sowie auf die mindestens zu verwendenden Schlüssellängen. [36]

2.4.2 SSH

Das SSH Protokoll wurde im Jahr 1995 von Tatu Ylönen an der technischen Universität von Helsinki entwickelt und sollte eine sichere Alternative zur unsicheren „r Familie“ (rsh, rlogin, rcp, rdist) sowie telnet darstellen. [37] Momentan ist SSH in der Version 2 verfügbar, wobei diese wesentlich sicherer und flexibler als seine Vorgängerrelease SSHv1 ist. Im Gegensatz zum Vorgänger handelt es sich bei SSHv2 nicht mehr um ein einzelnes großes Protokoll, sondern gliedert sich in mehrere Teilspezifikationen. SSHv2 setzt sich im Kern aus drei Teilkomponenten zusammen. Dem Verbindungsprotokoll (RFC 4254 [38]), dessen Aufgabe in einer flexiblen Handhabung der sicheren Verbindungen liegt, dem Authentifizierungsprotokoll (RFC 4252 [39]), das beschreibt, wie sich Clients gegenüber einem SSH-Server authentifizieren müssen und dem Transportprotokoll

(RFC 4253 [40]), das zuständig für den anfänglichen Verbindungsaufbau, der Server-Authentifizierung und der Verschlüsselung ist. Die SSH Protocol Architecture gibt einen Überblick über die SSHv2 Protokollsammlung und ist somit kein echtes Teilprotokoll von SSH. In ihr ist in zusammenfassender Weise der Sinn und Zweck der Secure Shell dargelegt. Als wesentliche Bausteine werden das Transport-, das Authentifizierungs- und das Verbindungsprotokoll identifiziert. Das SSH Protocol Architecture ist in RFC 4251 [41] verabschiedet. [42, S. 145f]

In SSH können neben den Basisprotokollen noch weitere Spezifikationen verwendet werden. Ein Subsystem ist beispielsweise das SSH File Transfer Protokoll welches das Standardprotokoll zur Datenübertragung mittels SSH ist. [42, S. 148]

2.4.2.1 Transportprotokoll

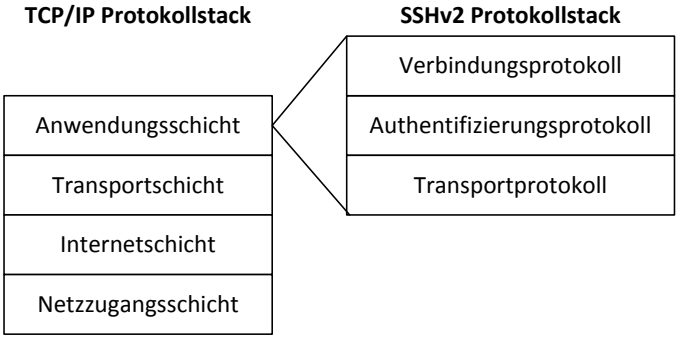


Abbildung 9: Einordnung der SSHv2 Protokolle in das TCP/IP Referenzmodell (Quelle: modifizierte Darstellung nach [42, S. 146])

Das Transportprotokoll ist für die sichere Übertragung der SSH Pakete innerhalb des Protokolls zuständig. Das SSH Protokoll setzt gemäß dem TCP/IP Model auf der Anwendungsschicht auf wie in Abbildung 9 veranschaulicht wird. Das Protokoll gewährleistet eine kryptographisch sichere Verbindung durch die Vereinbarung der Algorithmen, durch die Serverauthentifizierung, durch die Vereinbarung des Sitzungsschlüssels, durch die Verschlüsselung des Klartextes,

durch die Sicherstellung der Integrität mittels HMAC und durch eine optionale Kompression des Klartextes. Da die Server-Authentifikation nur hostbasierend ist, erfolgt in diesem Protokoll keine Userauthentifizierung. Basis für eine ordnungsgemäße Funktion des Transportprotokolls ist eine zuverlässige Netzwerkverbindung. Basiert diese auf TCP/IP, so hört der SSH-Server standardmäßig auf Port 22, da dieses von der Internet Assigned Numbers Authority (IANA) zugewiesen wurde. [42, S. 146ff]

Es kann ein erneuter Schlüsselaustausch für den symmetrischen Schlüssel angestoßen werden. Gemäß der Protokollspezifikation sollte dies nach der Übertragung von 1Gigabyte an Daten oder nach Ablauf einer Stunde erfolgen. [42, S. 176f]

2.4.2.2 Authentifizierungsprotokoll

Das Authentifizierungsprotokoll ist zwischen dem Transportprotokoll und dem Verbindungsprotokoll angesiedelt und ist auf das Vorhandensein von Vertraulichkeit und Integrität angewiesen, welche durch die Transportschicht geleistet werden. Weiters übernimmt es vom Transportprotokoll die Sitzungs-ID zu Signaturzwecken. Es dient der Benutzerauthentifizierung und bietet für diesen Zweck eine Reihe an Mechanismen, wie Passwörter, hostbasierter Login und Public-Key Techniken. Es stellt dem Verbindungsprotokoll einen authentifizierten Übertragungsweg bereit. [42, S. 186]

2.4.2.3 Verbindungsprotokoll

Das Verbindungsprotokoll ist das oberste der drei Teilprotokolle und basiert auf der Funktionalität der darunterliegenden Teile. Das Protokoll bietet interaktive Login-Sitzungen, entfernte Befehlsausführungen, Weiterleitung von TCP/IP- und X11-Verbindungen sowie Zugriff auf sichere Subsysteme auf dem Server Host. Jeder dieser Dienste wird über eine eigene Verbindung, einem sogenannten Kanal

abgewickelt. Alle Kanäle werden zusammengeführt und über eine einzige verschlüsselte und authentifizierte Verbindung abgewickelt. [42, S. 204f]

2.4.2.4 Hostschlüssel

Die Verwendung von Hostschlüssel zur Serveridentifikation ist ein zentraler Bestandteil der SSH-Sicherheitsarchitektur. Gemäß der Protokollspezifikation darf ein Host sowohl mehrere Schlüssel mit unterschiedlichen Algorithmen besitzen, aber genauso ist es möglich, dass sich mehrere Hosts einen gemeinsamen Schlüssel teilen. Der Client kann den Host-Schlüssel mit Daten aus einer lokalen Datenbank oder einer Certification Authority vergleichen und somit sicherstellen, dass es sich bei der Gegenstelle um den gewünschten Server handelt. Um eine größere Verbreitung zu erreichen, wurde in das Protokoll die Option eingebaut, dass die Kommunikation auch ohne Host-Schlüssel aufgebaut werden kann. Diese Vorgehensweise ist jedoch sehr unsicher da sie gegenüber MITM Angriffe (siehe hierzu Kapitel 2.5.3.3) anfällig ist. Wurde erstmalig eine Verbindung zum Server aufgebaut, so wird dieser in die „known host“ Datei eingetragen und bei allen folgenden Verbindungen gegen diesen Eintrag geprüft. Um diese Sicherheitsschwachstelle abzumildern wurde in SSH vorgesehen, dass alle Implementierungen zusätzliche Maßnahmen, wie die Bestimmung des Hashwertes vom öffentlichen Schlüssel, ergreifen können. [42, S. 159ff]

2.4.2.5 Verbindungsaufbau und Zusammenspiel der einzelnen Protokolle

Beim Verbindungsaufbau arbeiten die einzelnen Teilprotokolle von SSH zusammen, um der nutzenden Person einen Dienst zur Verfügung zu stellen. Dieser Prozess wird in Abbildung 10 dargestellt. Der Client startet eine Verbindungsanfrage an den Server und einigt sich mit diesem auf die zu verwendende SSH Version. In den nächsten Schritten werden Abstimmungen bezüglich der zu verwendenden Verschlüsselung, zur Kompression und anderer Verfahren getroffen. Teil dieser Schritte ist die Authentifizierung des Servers-Hosts und der Schlüsselaustausch. Sowohl der Client, als auch der Server sind

nach Abschluss dieser Phase in Besitz des symmetrischen Sitzungsschlüssels, weshalb ab diesem Zeitpunkt die Kommunikation nur noch verschlüsselt stattfindet. Danach sind die Aufgaben des Transportprotokolls, was den Verbindungsaufbau betrifft, abgeschlossen und das Authentifizierungsprotokoll kann die Authentifizierung des Nutzers vornehmen. Hierbei können verschiedene Verfahren zum Einsatz kommen. Zum Abschluss kommt das Verbindungsprotokoll zum Einsatz, welches zwischen den beiden Kommunikationspartnern einen Kanal öffnet. Dieser ist typgebunden, das heißt, dass er von der gewünschten Verwendung abhängig ist. [42, S. 161ff]

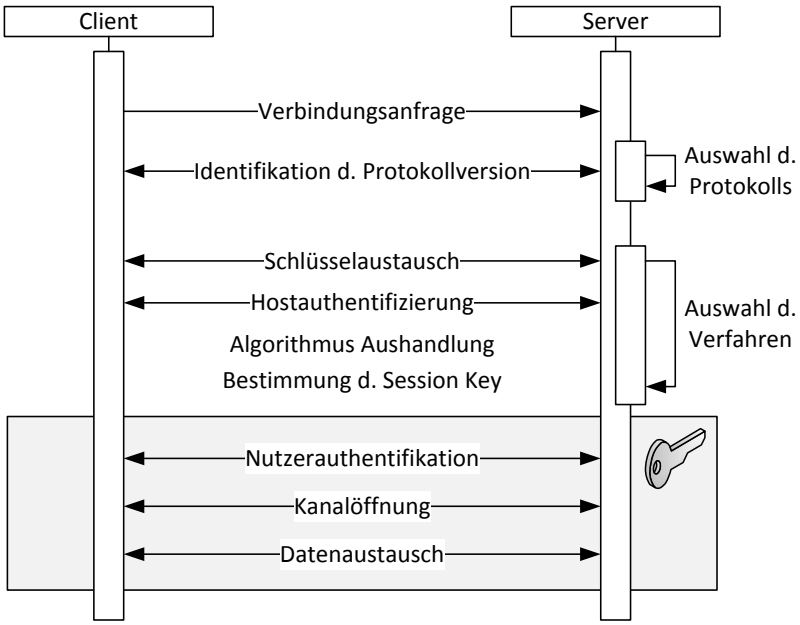


Abbildung 10: Aufbau einer SSHv2 Verbindung (Quelle: eigene Darstellung nach [42, S. 162])

2.4.2.6 Empfehlungen von Seiten des BSI zu SSH

Da die ursprüngliche SSH-1 Version kryptographische Schwächen aufweist, wird von Seiten des BSI [43] nur die Verwendung von SSH-2 empfohlen. Weiters wird darauf aufmerksam gemacht, dass nur bestimmte Schlüsselaustauschmethoden empfohlen werden. Während des Key Exchange Verfahrens einigen sich Client und Server auf einen Verschlüsselungsalgorithmus sowie einen gemeinsamen

Sitzungsschlüssel, welcher gemäß BSI nach einer bestimmten Zeit bzw. verbrauchten Datenvolumen erneuert werden soll. Dies kann sowohl von Seiten des Clients, als auch vom Server getriggert werden. Als Verschlüsselungsalgorithmus sollen gemäß BSI Richtlinie ebenfalls wie bei der MAC-Sicherung und der Server- bzw. Clientauthentifizierung nur bestimmte Algorithmen verwendet werden. Eine Aufstellung findet sich in der Publikation des BSI [43].

2.5 Sicherheitsrelevante Probleme und Angriffe

Da im Zuge dieser Arbeit auf die Protokolle TLS und SSH eingegangen wurde, sind die im Folgenden beschriebenen sicherheitsrelevanten Probleme und Angriffe speziell auf diese angelehnt. Es existieren im Internet noch weitaus mehr Protokolle mit unterschiedlichen Sicherheitslücken und anzuwendende Angriffsszenarien, auf welche allerdings nicht eingegangen wird, da dies über den Rahmen dieser Arbeit hinausgehen würde.

2.5.1 Sicherheitsrelevante Probleme durch Zertifizierungsstellen

2.5.1.1 Unzulängliche Prüfungen durch Zertifizierungsstellen

Die Electronic Frontier Foundation (EFF) [44] hatte 2010 TLS-Zertifikate und Zertifizierungsstellen auf deren Verhalten und mögliche Probleme untersucht. Mittels dem EFF SSL Observatory [45], einem Add-on zum Überprüfen des Zertifikates einer Webseite bei deren Aufruf, wurde ein Test im WWW durchgeführt. Es kann mittels diesem Add-on überprüft werden, ob es sich bei dem gelieferten Zertifikat um die richtige Website oder um eine „Fälschung“ und somit um einen MITM Angriff handelt.

Es wurde bei diesem Versuch festgestellt, dass zum Zeitpunkt des Tests im Jahr 2010 rund 16,2 Millionen IP Adressen auf den Port 443 hörten und davon 11,3

anfingen einen Handshake zu initialisieren. Weiters wurde festgestellt, dass fast 1.500 Zertifizierungsstellen aus 52 Ländern von Microsoft und Mozilla als „vertrauenswürdig“ eingestuft wurden. [44]

In einem weiteren Bericht von EFF [46] wird beanstandet, dass CAs augenscheinlich Zertifikate ohne ausreichende Prüfung ausgeben. So werden zumeist unqualifizierte Domainnamen wie „mail“ anstatt von Fully-Qualified Domain Names (FQDN), also einer eindeutigen Adresse, verwendet. Bei der Untersuchung wurde festgestellt, dass alleine für „localhost“, also dem eigenen Rechner, über 2.200 Zertifikate ausgestellt wurden. Weiters wurden von einigen CAs mehrere Zertifikate für eben diese Adresse vergeben. Nicht nur, dass solche Zertifikate sinnlos sind, es zeigt laut EFF im gleichen Maße, dass die CAs neben der nicht erfolgten Validierung, noch nicht einmal aufzeichnen, für welche Domains sie Zertifikate ausstellen. [46], [47]

Mit einem mittels unqualifizierten Domainnamen versehenen Zertifikat ist ein potentieller Angreifer in der Lage, einen MITM Angriff erfolgreich durchzuführen. Von Seiten EFF wird aus diesem Grund vor der Nutzung von unqualifizierten Domainnamen gewarnt und vorgeschlagen, dass Browser unterbinden sollten, Zertifikate mit eben diesen unqualifizierten Domainnamen austauschen. [44]

Obwohl die Probleme des CA-Systems bekannt sind, sind momentan keine Alternativen verfügbar. Es wird diskutiert DNSSEC zu verwenden um die Zertifikate zu überprüfen. Eine entsprechende TLS Implementierung namens DANE [48] gibt es bereits. [49]

2.5.1.2 Nachladen von Zertifizierungsstellen in Windows

Für die Betriebssysteme Windows 8.1 und Windows Server 2012 R2 hat Microsoft die Konfiguration der vertrauenswürdigen Stämme und unzulässiger Zertifikate adaptiert und für die Administratorinnen und Administratoren konfigurierbar gemacht. [50]

Hierbei gibt es laut der Fachzeitschrift c't [51], aus dem Jahr 2013 eine Sicherheitslücke, welche von Seiten Microsoft, oder anderen ausgenutzt werden kann um Sicherheitszertifikate als scheinbar sicher zu deklarieren. Mittels der CryptoAPI von Windows können die Stammzertifikate des Betriebssystems dynamisch aktualisiert werden, wenn das gerade benötigte Zertifikat nicht auf dem System vorgefunden wurde. Von Seiten Microsoft wird dieses Verfahren „Automatic Root Certificates Update" genannt und ist standardmäßig bei allen Windows-Versionen aktiviert.

Da sowohl der Internet Explorer, als auch die Browser Chrome und Safari die Krypto-Infrastruktur des Betriebssystems verwenden, können Zertifikate, welche das Betriebssystem als „sicher" einstuft, für den jeweiligen Nutzer nicht als potentiell bedrohlich angezeigt werden. Lediglich der Firefox Browser von Mozilla pflegt seine eigenen Krypto-Bibliotheken. [51]

Findet der entsprechende Browser eine Webseite, deren Zertifikat von einer unbekannten Stelle signiert wurde, wird automatisch im Hintergrund online eine Liste von weiteren Zertifizierungsstellen nachgeladen. [49] Nach dem Bericht von c't [51] kann ein Systemuser somit ohne besondere Privilegien im Betriebssystem durch den Aufruf einer URL eine neue Root-CA im System verankern. Somit wäre die TLS/SSL-Verschlüsselung einfach auszuhebeln und sogenannte „Man-In-The-Middle" Attacken zu erlauben. Neben diesem Problem, wäre es ebenso denkbar, dass von Seiten Microsoft eine Art von Zensur ermöglicht wird, indem es Personen in unterschiedlichen Ländern unterschiedliche Listen präsentiert.

Von Seiten c't [51] wird weiters angemerkt, dass angesichts der im Rahmen von PRISM bereits dokumentierten Zusammenarbeit zwischen Microsoft und der NSA anzunehmen ist, dass solche Hintertüren in Verschlüsselungsfunktionen für das Sammeln von Informationen genutzt werden.

2.5.2 Erkenntnisse aus dem NSA Skandal in Bezug auf TLS

Im Jahr 2013 hat sich im Zuge der NSA Affäre gezeigt, dass Geheimdienste daran interessiert sind, dass Datenverschlüsselungen durch sie einsehbar werden. Mittels des Patriot-Act, welcher im Jahr 2001 in den USA beschlossen wurde, ist eine Rechtsgrundlage aufrecht, mittels welcher die NSA Zugriff auf den privaten Schlüssel eines Dienstanbieters erlangen kann. Dieser Schlüssel wird zur Übermittelung des Session Keys verwendet, weshalb durch dessen Kenntnis faktisch alle Nachrichten abgehört werden können, welche über den betreffenden Server verlaufen. Zahlreiche Zertifizierungsdienstanbieter, die Zertifikate für die öffentlichen TLS-Schlüssel eines Service-Providers ausstellen, erzeugen die geheimen und öffentlichen Schlüssel gleich mit und bieten die Aufbewahrung des Schlüsselpaars als Recovery-Service für den Fall eines Schlüsselverlusts an. Da die ausstellende Instanz im Zertifikat angeführt wird, ist es für den Nachrichtendienst ein leichtes diese ausfindig zu machen und zur Zusammenarbeit aufzufordern. Mit dem Zugriff auf einen oder mehrere Zertifizierungsdienste ergab sich für die NSA noch eine weitere Möglichkeit TLS-Verbindungen zu kompromittieren. So konnten mittels gefälschten Zertifikaten Man-in-the-Middle Angriffe durchgeführt werden, ohne dass die Betroffenen davon Kenntnis erlangt hätten. Aus Sicht der NSA stellt dieses Vorgehen jedoch einen hohen Aufwand dar und ist für die Massenüberwachung ungeeignet. [52, S. 78ff]

Im Bericht von Fox [52, S. 82] wird des Weiteren angedeutet, dass von Seiten der Geheimdienste immer wieder versucht wird, mittels Hintertüren in der Implementierung oder durch Vorgabe bestimmter Standards, Einfluss auf die Sicherheit von kryptographischen Protokollen zu gewinnen.

2.5.3 Mögliche Angriffe auf TLS und SSH

Die Sicherheit von Rechnernetzwerken wird nicht nur durch Viren, Trojanern oder DoS-Angriffe bedroht, sondern es steht dem potentiellen Angreifer ein schier

unerschöpfliches Reservoir an Möglichkeiten zur Auswahl. Allgemein unterscheidet man zwischen passiven und aktiven Angriffen. Bei den passiven Angriffen beschränkt sich der Angreifer auf die Beobachtung, während bei aktiven Angriffen auch Daten manipuliert oder gelöscht werden. Da bei passiven Angriffen keine Datenänderungen vorgenommen werden, sind sie in der Regel schwerer zu detektieren. Im Folgenden werden mögliche Angriffsszenarien auf das TLS bzw. das SSH Protokoll beschrieben. [42, S. 93f]

2.5.3.1 Brute Force Angriff

Der Brute Force Angriff stellt eine sehr zeit- und rechenintensive Angriffsmethode dar, bei welcher der gesamte Schlüsselraum nach dem eingesetzten geheimen bzw. privaten Schlüssel durchsucht wird. Einen wirksamen Schutz bieten große Schlüssellängen, wie bereits im Kapitel 2.3.4.3 für symmetrische bzw. im Kapitel 2.3.5.1 für asymmetrische Verfahren beschrieben wurde. [53]

2.5.3.2 Known Plaintext Angriff

Diese Angriffsmethode nutzt den Umstand aus, dass Teile des übertragenen Geheimtextes bekannt sind und so der geheime Schlüssel leichter gefunden werden kann. TLS und SSH begegnen den Known Plaintext Angriff mit einem entsprechend langen Schlüssel, was diese Art von Angriff nicht praktikabel macht. [53]

2.5.3.3 Man in the Middle Angriff

Das Ziel eines sogenannten Man-in-the-Middle Angriffs ist es, die Datenkommunikation zwischen zwei Teilnehmern zu kontrollieren, wobei sich dieser Vorgang für die beiden Kommunikationspartner vollständig transparent darstellt und sie somit von diesem Vorgang nichts mitbekommen. Hierzu schaltet sich der Angreifer zwischen die beiden Parteien und gibt diesen vor, dass sie miteinander kommunizieren. Ein MITM Angriff kann unterbunden werden, indem sich die beiden Teilnehmer untereinander authentifizieren, die Datenverbindung

verschlüsselt ist und alle Protokollpakete signiert und mit Sequenznummern bzw. Zeitstempel versehen sind. In TLS basiert die Authentifizierung auf der Verwendung von X.509 Zertifikaten und in SSH durch die Nutzer-Authentifikation. [42, S. 95f]

2.5.3.4 Spoofing

Unter Spoofing wird die Verschleierung bzw. Verfälschung von eigenen Daten verstanden. Beispiele hierfür sind das IP Spoofing, das ARP Spoofing oder das DNS Spoofing. Mittels dieser Angriffstypen werden in der Regel zwei Ziele verfolgt. Einerseits die Schaffung von unbefugtem Zutritt oder die Verschleierung der eigenen Identität. [42, S. 97]

IP Spoofing

IP Spoofing kann einerseits verwendet werden um die Absenderadresse von IP Paketen zu manipulieren und so das Paket vom Server an eine andere Adresse weiterleiten zu lassen. Auf der anderen Seite kann mittels dieser Angriffsmethode aber auch vorgegeben werden, dass der Absende-Host ein anderer Rechner ist, d.h. eine andere IP Adresse hat, als tatsächlich vorhanden. Dies ermöglicht dem Angreifer das Empfangen von Datenpaketen, welche eigentlich an einen anderen Empfänger gerichtet gewesen wären. Dieser Angriff hat jedoch nur Aussicht auf Erfolg, wenn der tatsächliche Zielhost nicht auf die Datenpakete antworten kann, wie beispielsweise wenn er durch einen anderen Angriff außer Gefecht gesetzt ist. Diese Art von Angriff kann mittels Grenz-Router, Egress-Filterung oder Ingress-Filterung verhindert werden. [42, S. 96ff]

ARP Spoofing

Beim ARP-Spoofing Angriff werden gefälschte ARP Pakete versendet um die ARP-Tabellen, d.h. die IP- zu MAC-Adressen Zuordnung auf einer Netzwerkkomponente wie beispielsweise einem Rechner oder Switch, derart zu verändern, dass das betroffene Gerät seine Datenpakete nicht an den eigentlich bestimmten Host,

sondern an den des Angreifers sendet. Diese Methode ist jener des IP Spoofings sehr ähnlich und stellt eine sehr gute Basis für eine Man-in-the-Middle Attacke dar. [54]

DNS Spoofing

Beim DNS Spoofing werden einem DNS Server falsche Daten übermittelt, welche dieser für weitere Abfragen verwendet. Um DNS Spoofing zu erschweren, kann das sogenannte Reverse-Lookup verwendet werden. Hierbei wird nicht zu einem Namen die IP Adresse, sondern umgekehrt zur IP der entsprechende Name gesucht. Mittels dieser zusätzlichen Prüfung wird ein DNS Spoofing Angriff erschwert, vor allem wenn die beiden Tabellen für das DNS-Lookup und das Reverse-Lookup auf unterschiedlichen Rechnern liegen. [42, S. 100ff]

2.5.3.5 IP Hijacking

Bei dieser Angriffsmethode versucht der Angreifer eine bestehende IP Verbindung zu übernehmen. Grundsätzlich ähnelt diese Angriffsmethode jener des IP Spoofing, da der Angreifer eine falsche IP vortäuschen muss. Dieser Angriff wird von TLS bzw. SSH verhindert, da zu Beginn der Sitzung die Verschlüsselungsparameter ausgehandelt werden. [55]

2.5.3.6 Replay Angriff

Bei einem Replay Angriff sammelt der Angreifer alte Nachrichten seines Opfers um diese später wieder an den betreffenden Server zu senden. Da beim TLS Protokoll im Zuge des Handshakes Zufallszahlen verwendet werden, hat dieser Angriff keine Aussicht auf Erfolg. Im Gegensatz zu den vorher genannten Angriffsmöglichkeiten, kann mittels des Replay Angriffs somit der zu übertragende Content nicht eingesehen bzw. eine erneute Übermittelung von Daten nicht ausgelöst werden. Dennoch kann der Replay Angriff gegen eine besehende TLS Verbindung eingesetzt werden, da durch dessen Einsatz ein Verbindungsaufbau zwischen zwei Kommunikationspartnern unterbunden werden kann. [55]

2.5.3.7 SYN Flooding

Wie bereits bei der Replay Attacke, ist auch beim Einsatz des sogenannten SYN Flooding nicht das Ziel, die Datenverbindung zu kompromittieren, sondern eben diese Verbindung zu unterbinden. Die SYN-Nachricht wird beim TCP Handshake zur Etablierung einer TCP Verbindung vom einen Kommunikationsteilnehmer an den zweiten gesendet. Der Partner sendet eine SYN-ACK Nachricht zurück um den Verbindungsaufbau zu bestätigen. Im Regelfall sollte der erste Teilnehmer nun eine ACK Nachricht an den Sender des SYN-ACK Telegramms senden um den sogenannten Three-Way-Handshake zur Etablierung der Datenverbindung abzuschließen. Bleibt diese Bestätigung jedoch aus, so wartet die Gegenstelle einige Zeit bis sie die Verbindung fallen lässt. Kommen viele der Anfragen, so werden die Ressourcen des betreffenden Rechners gebunden und dieser kann auf keine weiteren Anfragen reagieren. TLS bzw. SSH bieten keinen Schutz vor diesen Angriffen, da die Protokolle oberhalb der TCP-Ebene operieren. [55]

2.5.3.8 Abschließende Bemerkung zu den Angriffsmethoden

In einem Netzwerk sind alle Schwachstellen Angriffspunkte, welche durch Angreifer ausgenutzt werden können. Es gibt eine Vielzahl an verschiedenen Angriffsmethoden, wobei durch Kombination deren Anzahl noch steigt. In der Praxis werden viele Methoden kombiniert oder nacheinander eingesetzt. Oftmals werden mittels des ersten Angriffs Informationen gesammelt um dann die nächsten Angriffe effizienter gestalten zu können. In der Praxis gibt es kein Allheilmittel gegenüber allen Angriffsmöglichkeiten. Es können jedoch Gegenmaßnahmen ergriffen werden, welche es einem potentiellen Angreifer soweit erschweren, dass dieser vom Angriff absieht. Der grundlegende Schritt zum Erreichen von erhöhter Sicherheit ist die Gewährleistung der Schutzziele gemäß Kapitel 2.2.3, was in Abbildung 3 verdeutlicht wird. [42, S. 103]

3. Praktischer Teil

3.1 Praktischer Versuch

3.1.1 Ausgangslage und Zielsetzung

Wie bereits eingangs erörtert, soll im Zuge von praktischen Versuchen eruiert werden, welche Rahmenbedingungen für einen erfolgreichen MITM Angriff auf eine HTTPS Verbindung, welche als Verschlüsselung das TLS Protokoll verwendet, notwendig sind.

Um die Aussagekraft der einzelnen Tests zu erhöhen, beziehungsweise um eine von Betriebssystemen und Web-Browser unabhängige Aussage zu erzielen, wird jeder Versuch sowohl mittels Android Smartphone, im Folgenden mit Opfer 1 bezeichnet und mit einem Windows Laptop, im Folgenden mit Opfer 2 bezeichnet, durchgeführt. Auf einen Test mit einem iOS Gerät wurde bewusst verzichtet, da dies den Rahmen dieser Arbeit gesprengt hätte.

3.1.2 Beschreibung des Versuchsaufbaus

Für den Versuch einer Man-in-the-Middle Attacke auf eine HTTPS Verbindung, wurde das Programm mitmproxy [56] verwendet. Dieses ist im Internet frei zugänglich und kann auf Github unter „https://github.com/mitmproxy/mitmproxy/releases“ downgeloadet werden. Es wird als TLS-Proxy verwendet um Daten, welche eigentlich an einen Server im Internet gesendet werden sollen, abzufangen und weiterzugeben. Unter einem Proxy versteht man eine Kommunikationsschnittstelle, welche auf Protokollebene als Vermittler zwischen zwei oder mehreren Netzwerken, bzw. Teilnetzen dient. Der Versuchsaufbau wird in Abbildung 11 skizziert.

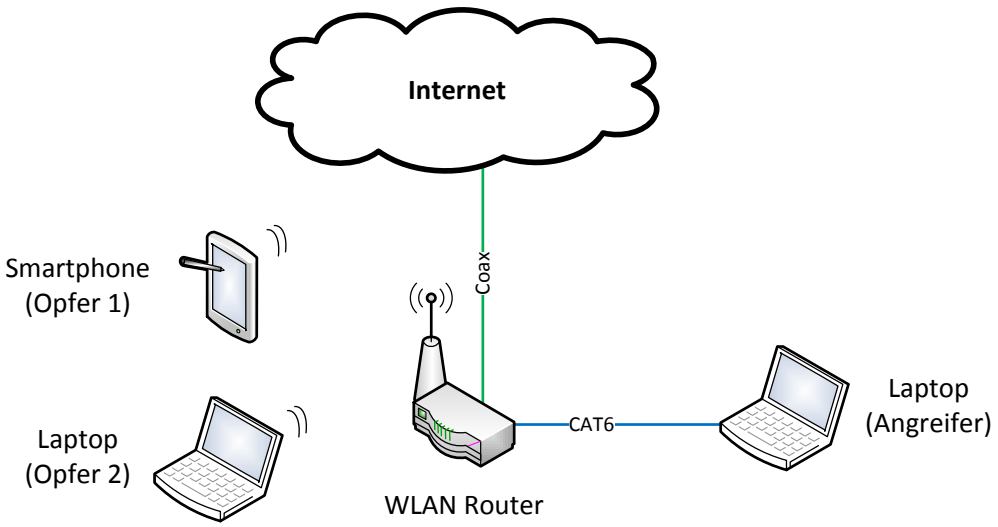


Abbildung 11: Schematische Darstellung des Testaufbaus

Den zentralen Punkt des Testnetzwerks stellt ein WLAN Router dar, welcher ebenfalls als Layer 2 Switching-Device fungiert. Über den Router wurde ein lokales Layer 2 Netzwerk aufgezogen, in welchem mehrere Geräte angebunden sein können. Der Einfachheit halber wurde im Testaufbau lediglich der Angreifer-Rechner platziert. Der Router dient neben der Verwaltung des lokalen Netzes auch als Firewall und Gateway ins Internet.

Wählt sich nun ein potentielles Opfer in das WLAN ein, so wird ihm vom Router via DHCP automatisch eine IP-Adresse aus dem lokalen Netzwerk zugewiesen wodurch sich der neue User im selben Netzwerk wie der Angreifer befindet. Dieses Vorgehen stellt eine gängige Praxis bei der Verwendung von WLAN dar. Anzumerken sei, dass es für den Versuch unerheblich ist, ob sowohl der Angreifer, als auch das Opfer mittels WLAN Zugang oder LAN Verbindung mit dem Netzwerk kommunizieren.

Im Test wurde das potentielle Opfer einmal mit einem Smartphone und ein zweites Mal mit einem Laptop ausgestattet. Dadurch sollte ermittelt werden, ob die einzelnen Betriebssysteme auf einen derartigen Angriff unterschiedlich reagieren und diesen eventuell sogar erkennen.

3.1.3 Eckdaten der verwendeten Komponenten

Bei den Testversuchen stellt der Router die zentrale Netzwerkkomponente dar. Die Eckdaten zu diesem finden sich in Tabelle 6.

Firma	Technicolor
Modell	TC7200.U
Verwendetes Netz	2,4 GHz
SW-Version	STD6.02.41
HW-Version	2.0.

Tabelle 6: Gerätedaten des WLAN-Routers

Als Angriffs-Device wurde ein Laptop gewählt welcher gemäß Tabelle 7 folgende Spezifikationen aufweist.

Firma	Dell
Modell	Latitude E5570
Betriebssystem	Windows 7 Enterprise Service Pack 1
Betriebssystemtype	64 Bit Betriebssystem
Prozessor	Intel Core i5-6200U
CPU Taktung	2,30GHz / 2,40 GHz
Arbeitsspeicher	16 GB

Tabelle 7: Gerätedaten des Angreifer-Rechners

Das Smartphone von Opfer 1 weist die folgenden Gerätedaten auf, welche in Tabelle 8 zusammengefasst wurden.

Modellnummer	SM-G900F
Android-Version	6.0.1
Basisbandversion	G900FXXS1CQA3
Kernel-Version	3.4.0-4493471 dpi@SWDD6603 #1
Buildnummer	MMB29M.G900FXXS1CQAV
SE for Android	Enforcing SEPF_SECMOBILE_6.0.1_0030
Sicherheitssoftware Version	MDF v1.1 Release 6 VPN v1.4 Release 6.0 ASKS v1.2_161011

Tabelle 8: Gerätedaten des Smartphones von Opfer 1

In Tabelle 9 finden sich die Eckdaten des Opfers-Notebooks, welcher in Abbildung 11 mit „Opfer 2“ bezeichnet wird.

Firma	Sony
Modell	Vaio VPCEB2M1E
Betriebssystem	Windows 10 Home
Betriebssystemtype	64 Bit Betriebssystem
Prozessor	Intel Core i3 350M
CPU Taktung	2,27 GHz / 2,27 GHz
Arbeitsspeicher	4 GB

Tabelle 9: Gerätedaten des Rechners von Opfer 2

3.1.4 Funktionsweise der Software mitmproxy

Ein für Internetanwendungen gebräuchlicher Proxy kann in der Regel nicht auf die verschlüsselten Daten des via HTTPS zu übertragenden Inhaltes zugreifen. Wie in [57] beschrieben, öffnet ein Standardproxy lediglich einen Übertragungstunnel zwischen Server und Client und fungiert somit nur als Übermittler der Datenpakete weiterleitet, ohne deren Inhalt zu kennen. Die Verbindung ist für den Proxy somit weder auf Daten-, noch auf Protokollebene einsehbar.

Das Programm mitmproxy platziert sich wie ein gewöhnlicher Proxy in der Mitte der Verbindung, gibt aber, wie es bei Man-in-the-Middle Attacken üblich ist, für den Server als Client und vice versa für den Client als Server aus. Das Problem an diesem Vorgang ist, dass die Verwendung von X.509 Zertifikaten genau solche Angriffe aufdecken soll, indem eine Zertifizierungsstelle überprüft, ob ein Zertifikat auch wirklich vom betreffenden Sender stammt und gültig ist. Stimmt beim empfangenen Zertifikat die Signatur nicht, oder ist sonst ein Problem mit dessen Gültigkeit detektiert worden, so wird der Client gewarnt und die Verbindung nicht akzeptiert. Das Programm mitmproxy umgeht dieses Problem, indem es sich selbst als vertrauenswürdige Zertifizierungsstelle ausgibt. Zu diesem Zweck beinhaltet es eine vollständige CA, welche Zertifikate „on the fly“ ausstellen kann. Es bleibt nur noch das Problem, dass mitmproxy als vertrauenswürdige CA am Client eingetragen werden muss. [57]

Damit der MITM Angriff Erfolg hat, muss die im Zertifikat anzugebende Domäne bekannt sein. Wäre diese nicht bekannt, so könnte der mitmproxy diese nicht an den Client senden und dieser würde die Verbindung abbrechen. Zu diesem Zweck wird die Connect-Anfrage des Clients analysiert. Steht in dieser die benötigte Domäne, so wird diese vom Proxy gespeichert und im eigenen, kreierten Dummy-Zertifikat eingetragen. Ist in der Connect-Anfrage nur eine IP Adresse verfügbar, so genügt diese Information zumindest um einen Übertragungstunnel zur gewünschten Site einzurichten. Hierzu wird die Verbindung zum Opfer kurzzeitig pausiert und der TLS-Handshake mit der angeforderten Seite abgeschlossen um das Zertifikat der Seite zu analysieren. Der Common-Name des Zertifikates wird zur Erstellung eines Dummy-Zertifikates für den Client verwendet, um damit die Verbindung zum Client etablieren zu können. Da jedoch der Common Name nicht immer der tatsächliche Hostname ist, mit welchem sich der Client zu verbinden versucht, wird der bzw. die Subject Alternative Name(s) (SAN) vom empfangenen Zertifikat extrahiert und in das Dummy-Zertifikat eingefügt. Empfängt nun das Opfer dieses Dummy-Zertifikat, so wird es die Verbindung etablieren, auch wenn die Domäne nicht mit dem Zertifikat übereinstimmt. [57]

Eine der größten Limitationen von TLS ist, dass jedes Zertifikat eine eigene IP Adresse benötigt. Um nicht eine schier unendliche Anzahl an Zertifikaten übermitteln zu müssen, wurde die Servernamen-Identifikation (Server Name Indication SNI) zum TLS Protokoll hinzugefügt. Diese Erweiterung des Protokolls erlaubt es den Clients zu Beginn des TLS-Handshakes den Namen des angewählten Servers bekannt zu geben, damit der Server das benötigte Zertifikat auswählen kann. Diese SNI Erweiterung wird auch im Programm mitmproxy zunutze gemacht, da ohne diese nur ein Standardzertifikat ausgestellt und der Client nicht das erwartete Server-Zertifikat bekommen würde. Beim Verbindungsaufbau des Clients mit dem Proxy wird der TLS Handshake kurz nach der Übergabe des SNI-Werts pausiert um die benötigten Werte vom Server zu bekommen, indem der Verbindungsaufbau mit dem Server vollzogen wird. Der Server schickt im Zuge dieses Kommunikationsaufbaus das benötigte Upstream-

Zertifikat in welchem die vom Client erwarteten CN und SANs beinhaltet sind. Erst dann wird der Verbindungsaufbau mit dem Client abgeschlossen. Dieser Vorgang ist in Abbildung 12 dargestellt. [57]

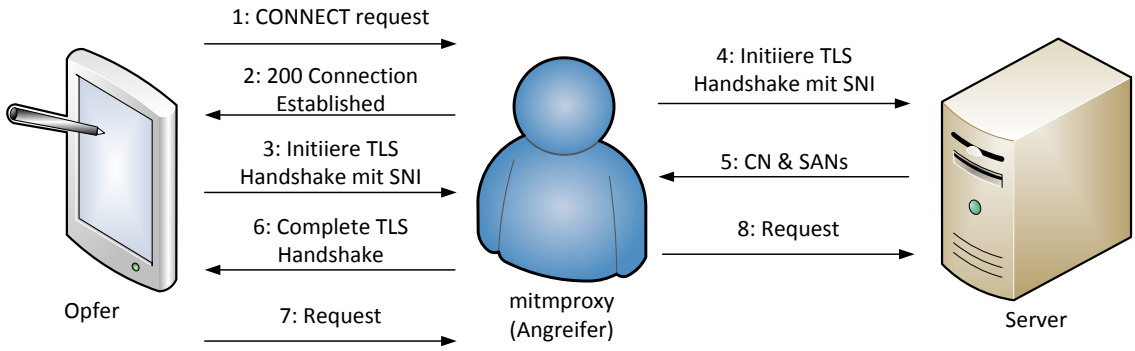


Abbildung 12: Verbindungsaufbau einer HTTPS Session über mitmproxy (Quelle: modifiziert übernommen aus [57])

In Abbildung 12 ist der Verbindungsaufbau einer HTTPS Session dargestellt, welcher gemäß [57] wie folgt zusammengefasst werden kann:

1. Der Client verbindet sich zum mitmproxy und initiiert einen CONNECT request.
2. Der mitmproxy reagiert und antwortet mit einer 200 Connection Established Meldung, als wenn er eine CONNECT Pipe geöffnet hätte.
3. Der Client glaubt er würde mit dem angewählten Server kommunizieren und initiiert den TLS-Handshake. Weiters verwendet dieser SNI zur Identifikation des Hostnamens.
4. Mitmproxy verbindet sich zum Server und initiiert seinerseits eine TLS Verbindung mittels der SNI Hostname Identifikation des Clients.
5. Der Server antwortet mit dem entsprechenden Zertifikat in welchem die CN und SAN Werte eingetragen sind.
6. Mitmproxy generiert ein eigenes Dummy-Zertifikat, in welches die Werte vom Server eingetragen werden und komplettiert den TLS Handshake mit dem Client, welcher nach Step 3 pausiert wurde.

7. Nach der erfolgreichen Etablierung der TLS Session, sendet der Client entsprechende Requests über die Verbindung.
8. Mitmproxy protokolliert, bzw. ändert die Daten vom Client und schickt sie über die zweite TLS Verbindung zum Server weiter.

3.1.5 Potentielle Angriffsmöglichkeiten

Während der Recherche, aber auch dann während des praktischen Versuchs selbst, hat sich herausgestellt, dass mehrere Angriffsszenarien auf die Verbindung des Opfers möglich sind. Dabei ist vor allem die Ausgangssituation auf Seiten der betroffenen Person ausschlaggebend dafür, welcher Angriff gewählt werden muss.

Wie in [58] beschrieben, hängt der jeweilige Angriffsmodus davon ab, ob auf Seiten des Opfers bereits ein Proxy für die Internetverbindung verwendet wird, bzw. ob einer über ein Drittprogramm konfiguriert werden kann. Ist bereits ein Proxy in Verwendung, so kann versucht werden, einen zweiten Proxy in Serie zum ersten zu schalten. Diese Möglichkeiten werden in nachstehendem Flussdiagramm Abbildung 13 veranschaulicht.

Es wird in Abbildung 13 auch gezeigt, dass im Falle von mitmproxy zwischen 3 Client-Angriffsverfahren unterschieden werden kann. Der Vollständigkeit halber wird darauf verwiesen, dass auch ein Angriffsmodus für die Serverseite zur Verfügung steht. Da in dieser Arbeit jedoch ausschließlich die Angriffspotentiale auf den Client eruiert werden sollen, ist dieser Modus für die zu untersuchenden Szenarien nicht von Bedeutung.

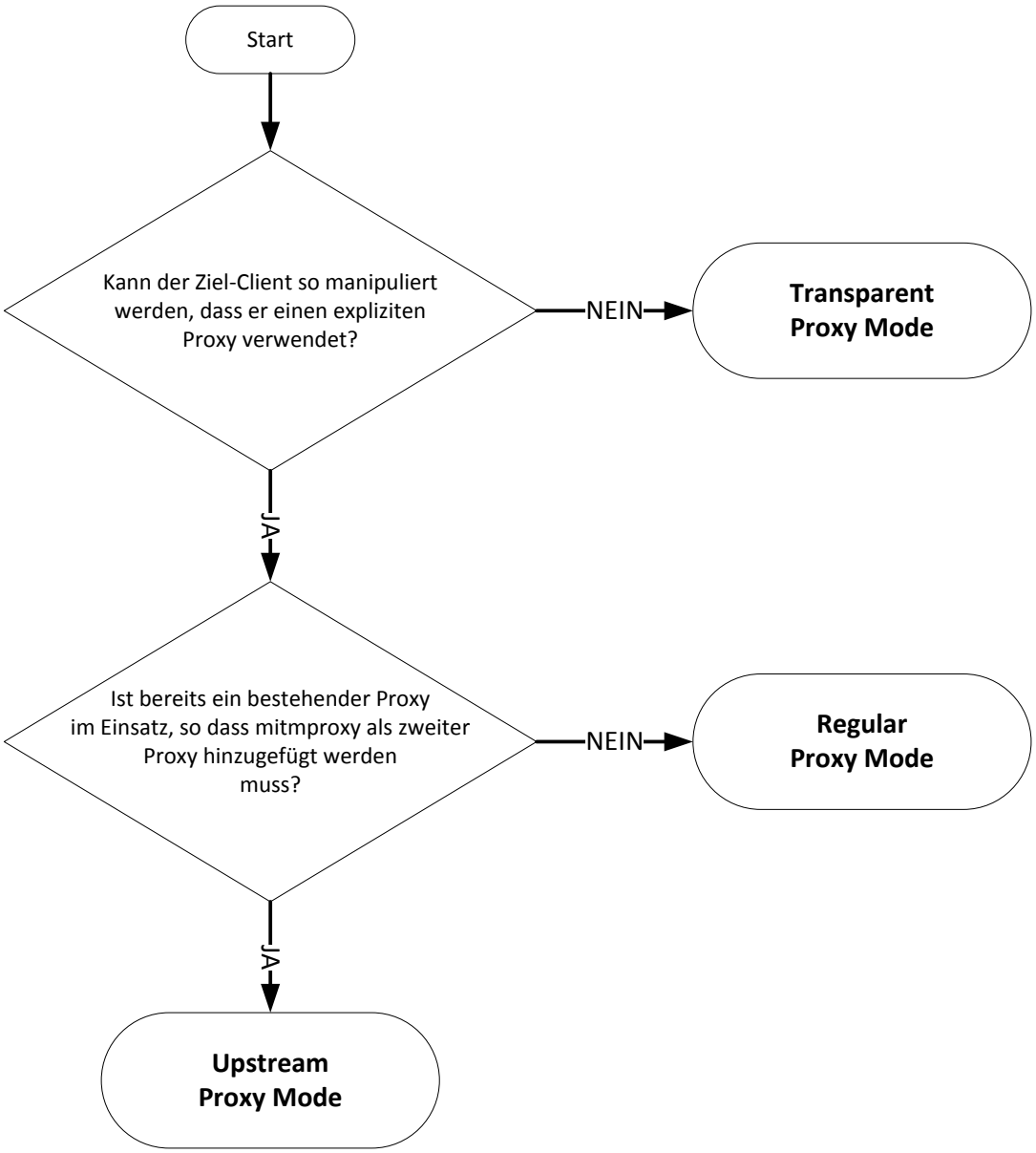


Abbildung 13: Auswahl des richtigen Angriffsmodus im Falle des Programms „mitmproxy“ (Quelle: eigene Darstellung nach [58])

3.1.5.1 Regular Proxy Mode

Bei dieser Variante wird die Software mitmproxy, welche am Rechner des Angreifers läuft, als Proxy in der Internetverbindung des Opfers eingetragen. Das

bedeutet, dass alle Anfragen, welche in das Netzwerk gesendet werden sollen, an den Proxy zur weiteren Übermittlung übertragen werden. [58]

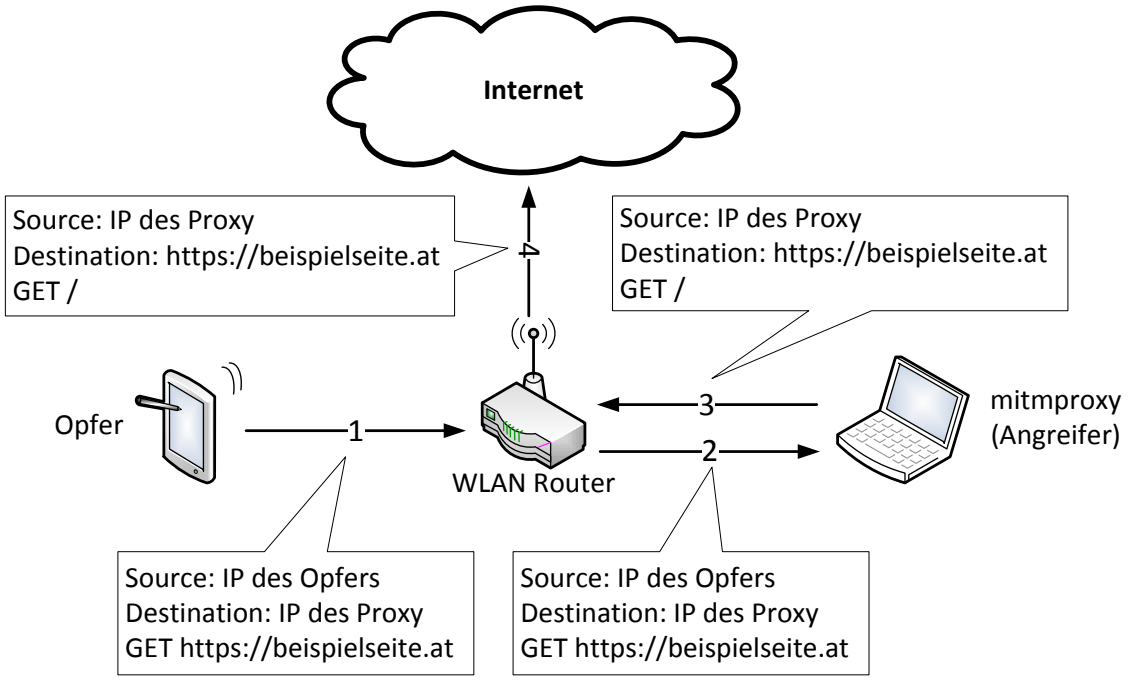


Abbildung 14: Schematische Darstellung der Funktion des Regular Proxy (Quelle: eigene Darstellung nach [58])

Wie in Abbildung 14 dargestellt, sendet das Opfer eine Anfrage für die Webseite „https://beispielseite.at“ an den Proxy des Angreifers. Diese Nachricht wird über den Router an den Rechner des Angreifers weitergeleitet. Das Programm mitmproxy, welches als Übermittler fungiert, nimmt die Anfrage des Opfers entgegen und schickt diese weiter an die betreffende Webseite, nachdem die Daten des Opfers mitgeloggt wurden. Der Request an die Website wird wiederum über den Router ins Internet weitergeleitet.

3.1.5.2 Upstream Proxy Mode

Sollen mehrere Proxys hintereinander geschaltet werden, da bereits ein bestehender Proxy im Netzwerk vorhanden ist, so kommt der Upstream Proxy Mode zum Einsatz. Die Software mitmproxy wird dabei zwischengeschaltet um die

Datenverbindung zu korrumpieren und den Datenaustausch zwischen Opfer und Proxy einzusehen. Die Funktionsweise ist in Abbildung 15 skizziert. [58]

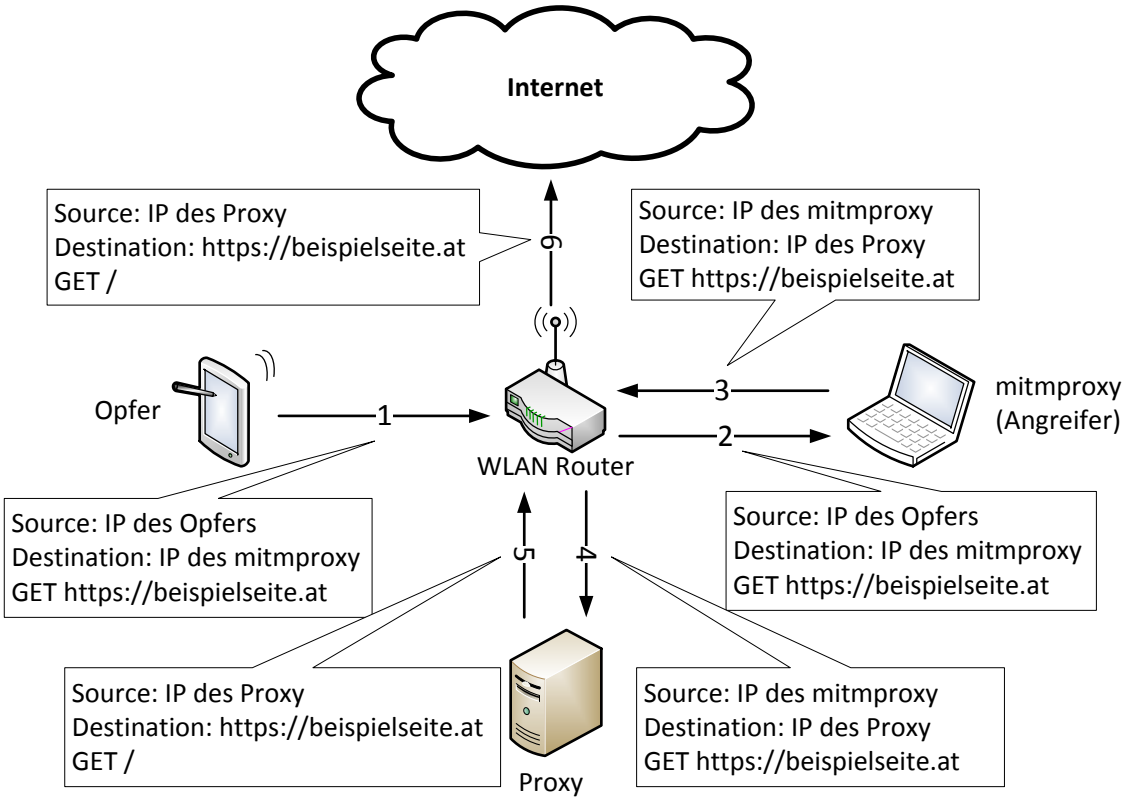


Abbildung 15: Schematische Darstellung der Funktion des Upstream Proxy (Quelle: eigene Darstellung nach [58])

Beim Upstream Proxy Mode wird aus Sicht des Opfers, wie bereits beschrieben, der Proxy des Angreifers vor dem eigentlichen Proxy platziert. Im Prinzip entspricht der Upstream Mode jenen des Regular Proxy Modes, mit der Ausnahme, dass der mitmproxy die GET Anforderung nicht direkt an die entsprechende Webseite, sondern an den eigentlichen Proxy sendet, was in Abbildung 15 in den Kommunikationswegen 3 und 4 dargestellt wird. Der Proxy sendet dann die GET Anforderung des Clients über den Router an das Internet. Mittels des mitmproxys des Angreifers kann die Datenübertragung, analog dem Regular Proxy Verfahrens, eingesehen werden.

3.1.5.3 Transparent Proxy Mode

Kann dem potentiellen Opfer die Verwendung eines Proxys nicht aufgezwungen werden, so kommt der Transparent Proxy Mode zum Einsatz. Der Datenverkehr wird wieder über den mitmproxy geleitet, diesmal jedoch ohne dass auf Seiten des Clients eine Konfiguration erforderlich ist. In der Regel kann der transparente Proxy über zwei verschiedene Netzwerkadaptierungen zum Einsatz kommen. So kann der Standard-Gateway des Opfers manipuliert oder auf Seiten des Netzwerk selbst das Routing entsprechend adaptiert werden, dass die Nachrichtenpakete über den Transparent Proxy umgeleitet werden. Im Folgenden wird auf die am häufigsten angewandten Verfahren näher eingegangen. [58]

Transparent Proxy via Custom Gateway

Bei diesem Angriffsmodus wird der Standard-Gateway (Default-Gateway) des Opferrechners so konfiguriert, dass dieser die IP Adresse des Angreiferrechners beinhaltet. In der Regel kann dies über die automatisierte IP Vergabe via DHCP in einem Netzwerk erfolgen. Der Angreifer muss hierbei die Hoheit über den bestehenden DHCP Server bekommen, oder falls kein derartiger Server im Netzwerk vorhanden ist, einen eigenen DHCP Dienst installieren. Ist dies nicht möglich, so kann die Opfer-Verbindung auch mittels ARP-Spoofing Angriff kompromittiert werden.

Wie in Abbildung 16 ersichtlich, verläuft der Datenverkehr in diesem Szenario über den Rechner des Angreifers und dann in das Internet. Auf den ersten Blick könnte man annehmen, dass dieser Angriff jenen des Regular Proxy Modes entspricht, da die Abbildungen sehr ähnlich aussehen. Allerdings stellt sich die Situation auf Seiten des Netzwerks sehr different dar. So sendet das Opfer seine Daten zwar ebenfalls an den Proxy, doch ist sich die bzw. der Betroffene dessen nicht bewusst. Während beim Regular Proxy Mode die bzw. der Geschädigte noch vom Proxy Services gewusst hatte, bzw. von dessen Existenz Kenntnis gewinnen konnte, ist dies bei dieser Variante des Angriffs nicht der Fall. Somit wird auch

keine GET Nachricht über das Netzwerk gesendet, sondern die jeweilige Website als Destination im Netzwerkprotokoll angegeben.

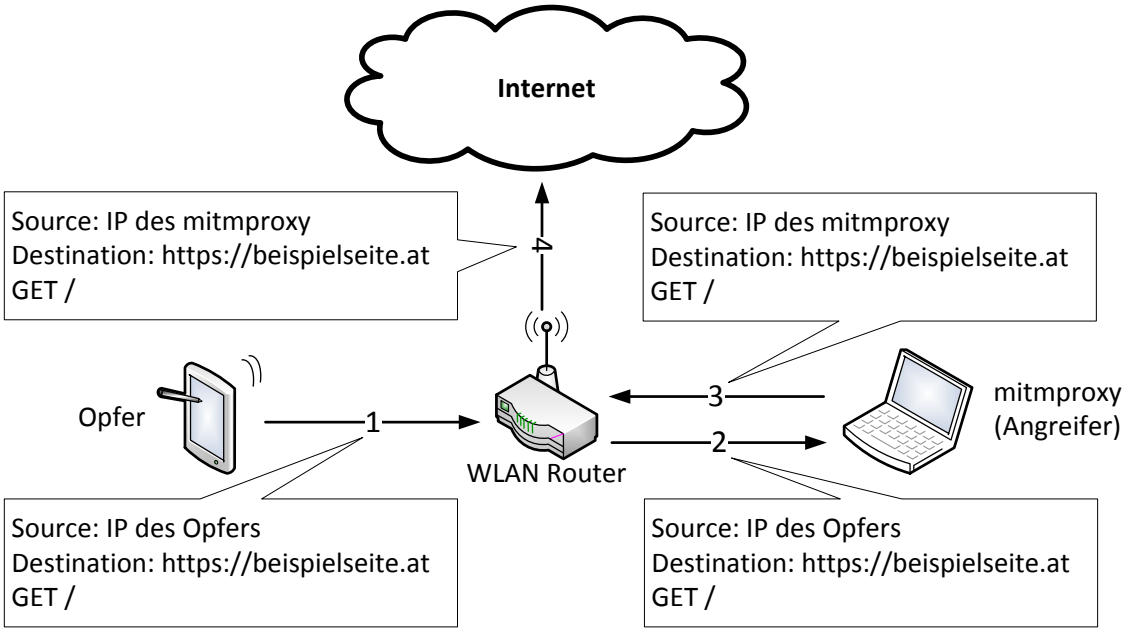


Abbildung 16: Schematische Darstellung der Funktion des Transparent Proxy (Quelle: eigene Darstellung nach [58])

Transparent Proxy via Custom Routing

Kann der Standard-Gateway des Opfers nicht geändert werden, bzw. ist kein Zugriff auf den DHCP Server möglich, so kann neben dem ARP-Spoofing auch die Einstellung des Routers im Netzwerk angepasst werden. Hierbei kann die Routerkonfiguration über Paketfilter oder individuellem Routing für bestimmte Adressen, derart adaptiert werden, dass der Datenverkehr des Opfers über den mitmproxy des Angreifers umgeleitet wird. [58]

Der Angriff stellt sich nahezu ident mit jenen des Transparent Proxys mit angepasstem Standard Gateways dar, wie in Abbildung 16 gezeigt wird. Es wird lediglich die Datenumleitung über den Router geführt. Das heißt, der Opferrechner sendet seine Daten wie vom User erwartet an den Router, doch dieser leitet diese an den Angreifer anstatt zum Internet Service Provider weiter.

3.1.6 Testablauf

Es wurden mehrere Versuche unternommen um die Rahmenbedingungen, unter welchen ein MITM Angriff Erfolg hat, auszuloten.

3.1.6.1 Testfall 1 mit dem „Regular Proxy“

Es wurde das Programm mitmproxy für den ersten Test im „Regular Proxy Mode“ betrieben. Hierzu wird am Smartphone des Opfers 1 ein Proxy eingetragen, welcher auf das Notebook des Angreifers verweist. Dieser Vorgang wird in Abbildung 17 gezeigt.

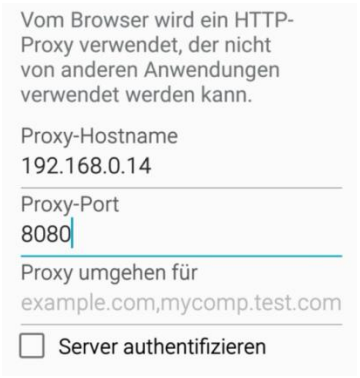


Abbildung 17: Darstellung der Proxyeinstellungen am Smartphone des Opfers 1

Hierbei hat sich herausgestellt, dass ohne ein gültiges Zertifikat, die in Abbildung 18 dargestellte Fehlermeldung am Smartphone des Opfers 1 erscheint. Wie im Screenshot ersichtlich, sollte die Webseite von Google aufgerufen werden. Da das Android Betriebssystem bzw. der Webbrowser jedoch aufgrund des fehlenden Zertifikates keine gesicherte Verbindung aufbauen konnte, wurde die dargestellte Fehlermeldung ausgegeben. Wird diese Warnung ignoriert und die Webseite dennoch aufgerufen, so stellt sich diese wie in Abbildung 19 ersichtlich dar.

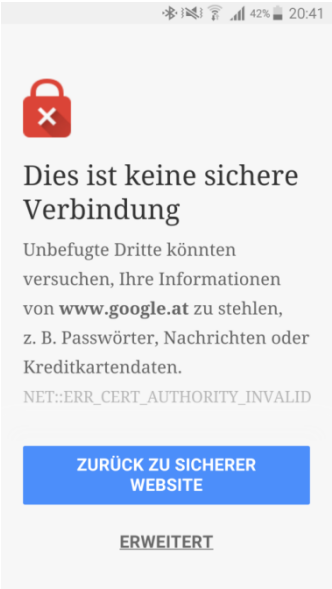


Abbildung 18: Screenshot des Warnhinweises zum fehlenden Zertifikat am Smartphone des Opfers 1

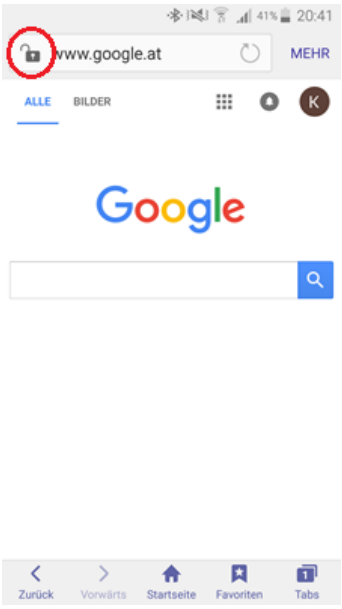


Abbildung 19: Screenshot der aufgerufenen Webseite via Smartphone von Opfer 1

Zu beachten ist das rot eingerahmte Symbol neben der angewählten URL in Abbildung 19. Dieses bedeutet, dass das Zertifikat der Webseite nicht überprüft werden konnte. Im Standardfall sollte das Symbol wie in der Abbildung 20 gezeigt,

dargestellt werden. Wird das Symbol neben der URL von Seiten des Users ignoriert, so kann mittels des MITM Angriffs die Datenverbindung durch den Angreifer eingesehen werden.

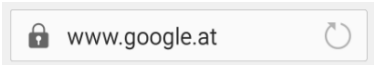
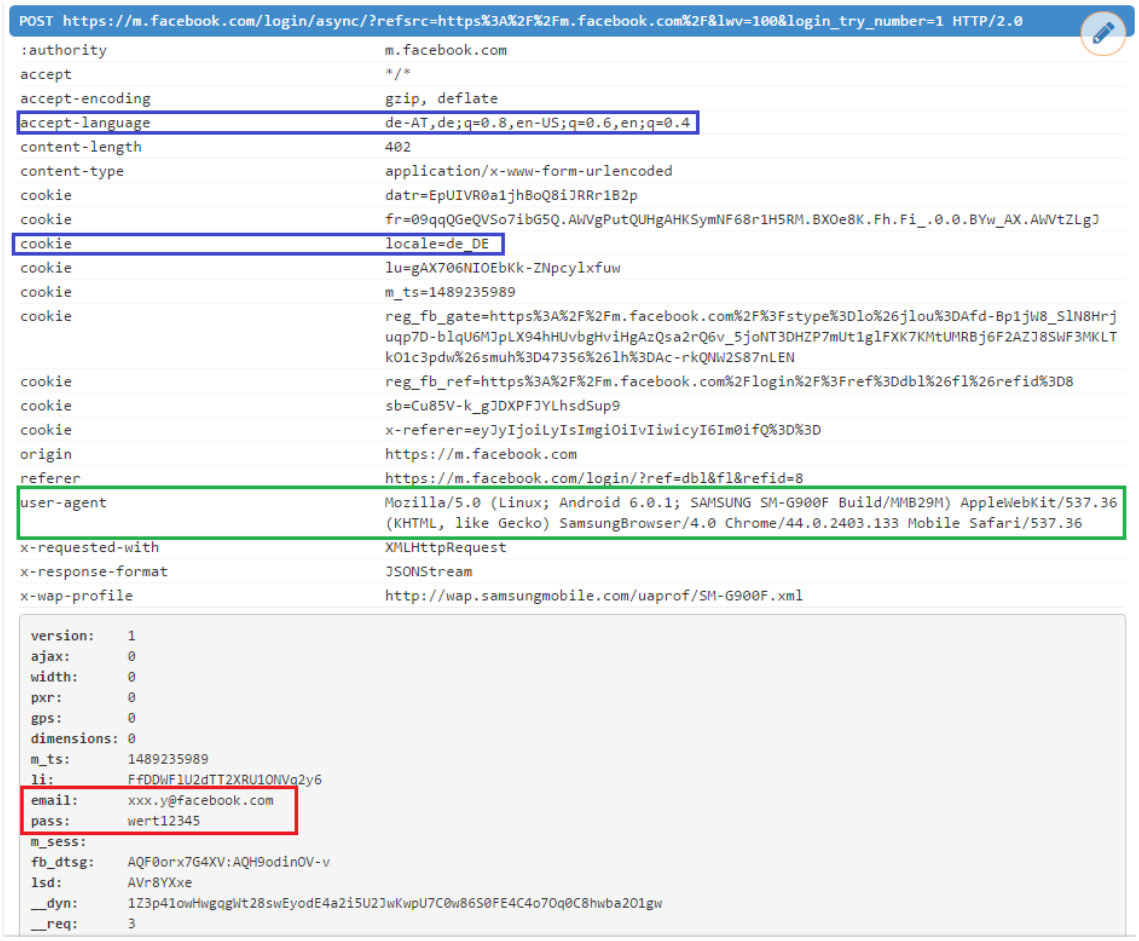


Abbildung 20: Ausschnitt eines Screenshots einer überprüften zertifizierten Website

Nach der Installation des fehlenden Zertifikates konnte die Website ohne einen Hinweis wie in Abbildung 18 und einer scheinbar sicheren URL wie in Abbildung 20 gezeigt, aufgerufen werden. Für den User ist somit nicht ersichtlich, dass mittels eines MITM Angriffs die Datenverbindung eingesehen wird.



POST https://m.facebook.com/login/async/?refsrc=https%3A%2F%2Fm.facebook.com%2F&lwv=100&login_try_number=1 HTTP/2.0

:authority	m.facebook.com
accept	*/*
accept-encoding	gzip, deflate
accept-language	de-AT,de;q=0.8,en-US;q=0.6,en;q=0.4
content-length	402
content-type	application/x-www-form-urlencoded
cookie	datr=EpUIVR0a1jhBoQ8iJRRr1B2p
cookie	fr=09qqQGeQVSo7ibG5Q.AWVgPutQUHgAHKSymNF68r1H5RM.BXOe8K.Fh.Fi_.0.0.BYw_AX.AWVtZLgJ
cookie	locale=de_DE
cookie	lu=gAX706NIOEbKk-ZNpcylxfuw
cookie	m_ts=1489235989
cookie	reg_fb_gate=https%3A%2F%2Fm.facebook.com%2F%3Fstype%3Dlo%26jlou%3DAfd-Bp1jW8_SlN8Hrjuqp7D-blqU6MJpLX94hHUvbgHviHgAzQsa2rQ6v_5joNT3DHZP7mUt1glFXK7KMtUMRBj6F2AZJ8SWF3MKLTkO1c3pdw%26smuh%3D47356%26lh%3DAc-rkQNW2S87nLEN
cookie	reg_fb_ref=https%3A%2F%2Fm.facebook.com%2Flogin%2F%3Fref%3Ddbl%26fl%26refid%3D8
cookie	sb=Cu85V-k_gJDXPFJYLhsdSup9
cookie	x-referer=eyJyIjoiLyIsImgiOiIvIiwicyI6Im0ifQ%3D%3D
origin	https://m.facebook.com
referer	https://m.facebook.com/login/?ref=dbl&fl&refid=8
user-agent	Mozilla/5.0 (Linux; Android 6.0.1; SAMSUNG SM-G900F Build/MMB29M) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/4.0 Chrome/44.0.2403.133 Mobile Safari/537.36
x-requested-with	XMLHttpRequest
x-response-format	JSONStream
x-wap-profile	http://wap.samsungmobile.com/uaprof/SM-G900F.xml

version:	1
ajax:	0
width:	0
pxr:	0
gps:	0
dimensions:	0
m_ts:	1489235989
li:	FfDDWF1U2dTT2XRU1ONVq2y6
email:	xxx.y@facebook.com
pass:	wert12345
m_sess:	
fb_dtsg:	AQF0orx7G4XV:AQH9odinOV-v
lsd:	AVr8YXxe
__dyn:	1Z3p41owHwgqgWt28swEyodE4a2i5U2JwKwpU7C0w86S0FE4C4o7Oq0C8hwba2O1gw
__req:	3

Abbildung 21: Ausschrift von mitmproxy beim Login auf Facebook durch Opfer 1

Für den Testfall wählt sich das Opfer mittels seines Smartphones auf der Website von Facebook ein. Dieser Vorgang wird vom Programm mitmproxy erfasst und mitprotokolliert. Es ergibt sich im Webinterface des Programms jene Ausschrift, welche in Abbildung 21 dargestellt wird. Bei der Anforderung des Logins wurden unter anderem die E-Mail Adresse, also der Login und das Passwort übertragen. Diese werden in Abbildung 21 rot gekennzeichnet. Weiters werden Daten wie die gewählte Spracheinstellung und Landesaufenthalt blau markiert, sowie Informationen über den Browser bzw. von welchem Betriebssystem die Seite aufgerufen wurde mittels grüner Markierung kenntlich gemacht.

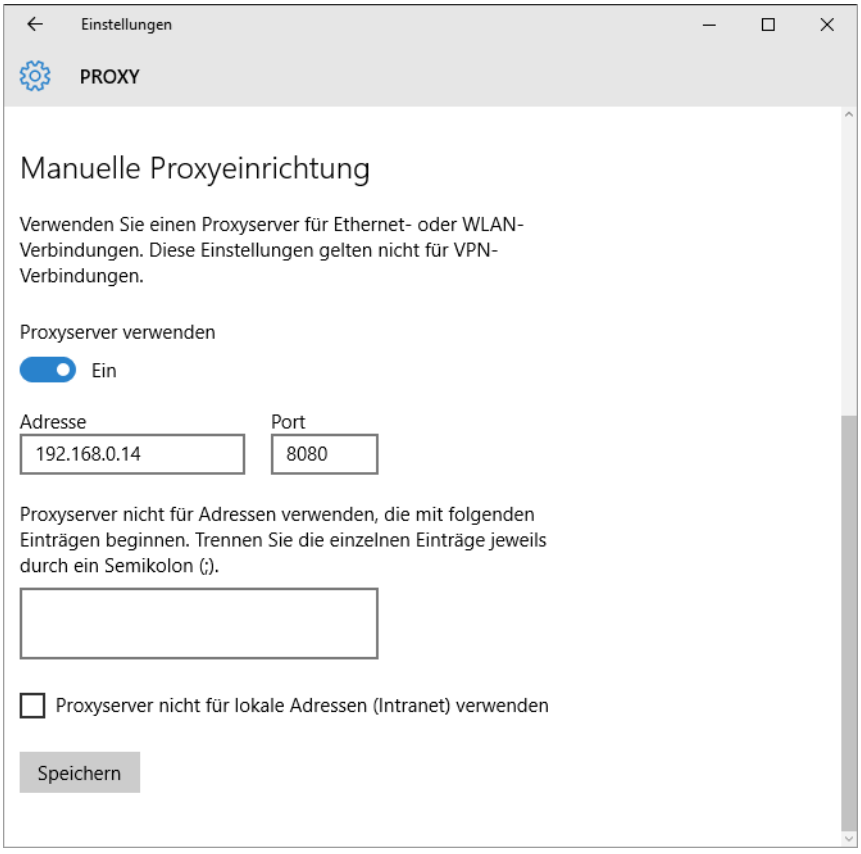


Abbildung 22: Einrichten des Proxys am Rechner von Opfer 2

Wie in Abbildung 11 dargestellt, wird mittels des Programms mitmproxy auch auf die Datenverbindung von Opfer 2 zugegriffen, welcher sich mittels Windows 10 Laptop auf eine Website verbindet. Hierzu wird, wie in Abbildung 22 gezeigt,

analog zum Smartphone, der Rechner des Angreifers als Proxy eingetragen. Wird das benötigte Zertifikat nicht installiert, so erscheint ebenso wie am Smartphone ein Warnhinweis, dass die Verbindung eingesehen werden kann. Ein Screenshot dieses Hinweises wird in Abbildung 23 gezeigt.

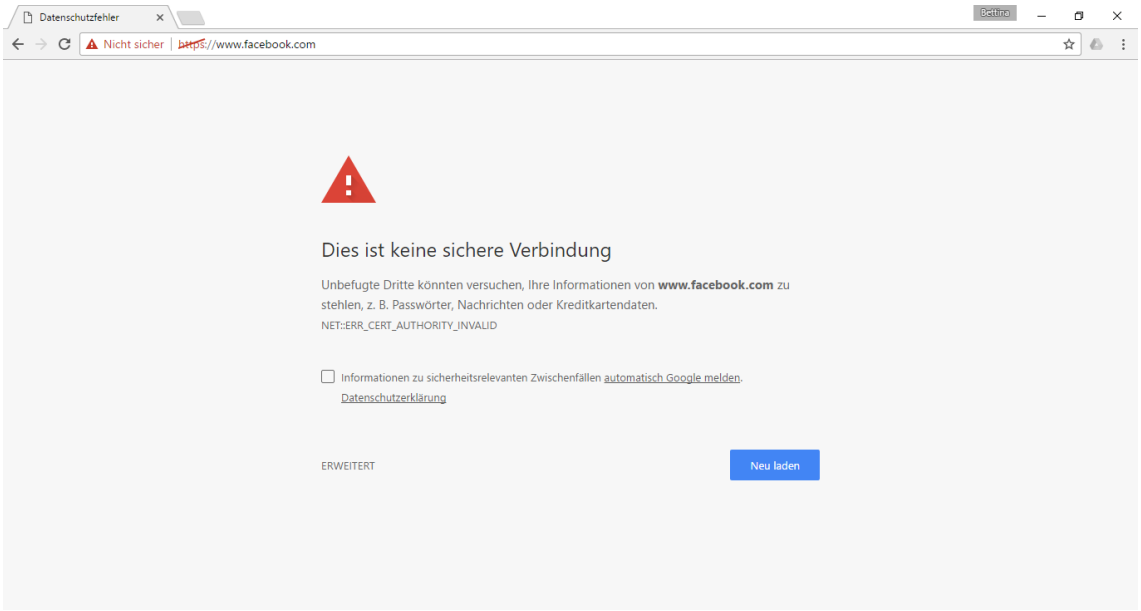


Abbildung 23: Warnhinweis im Browser von Opfer 2

Durch einen Klick auf das rote Warnsymbol neben der URL erscheint, wie in Abbildung 24 dargestellt, die Detailinformation zum ausgegebenen Datenschutzfehler.

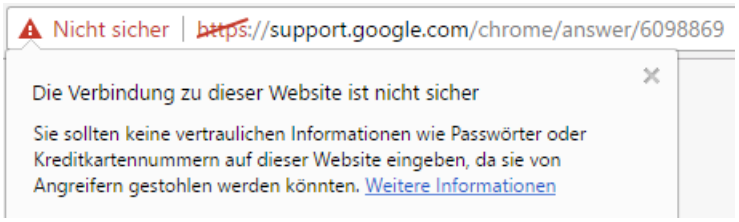


Abbildung 24: Bildausschnitt der Detaildarstellung zum Datenschutzfehler im Browser von Opfer 2

Wie bereits am Smartphone wird dieser Hinweis nach der Installation des Zertifikates nicht mehr angezeigt, wie in Abbildung 25 ersichtlich ist. Wenn man

einen Blick auf das Zertifikat der Webseite wirft, so stellt man fest, dass dieses vom Programm mitmproxy ausgestellt wurde. Ein entsprechender Screenshot findet sich in Abbildung 26.

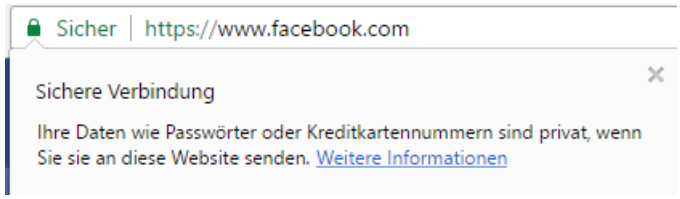


Abbildung 25: Scheinbar sicherer Webseitenaufruf am Rechner des Opfers 2

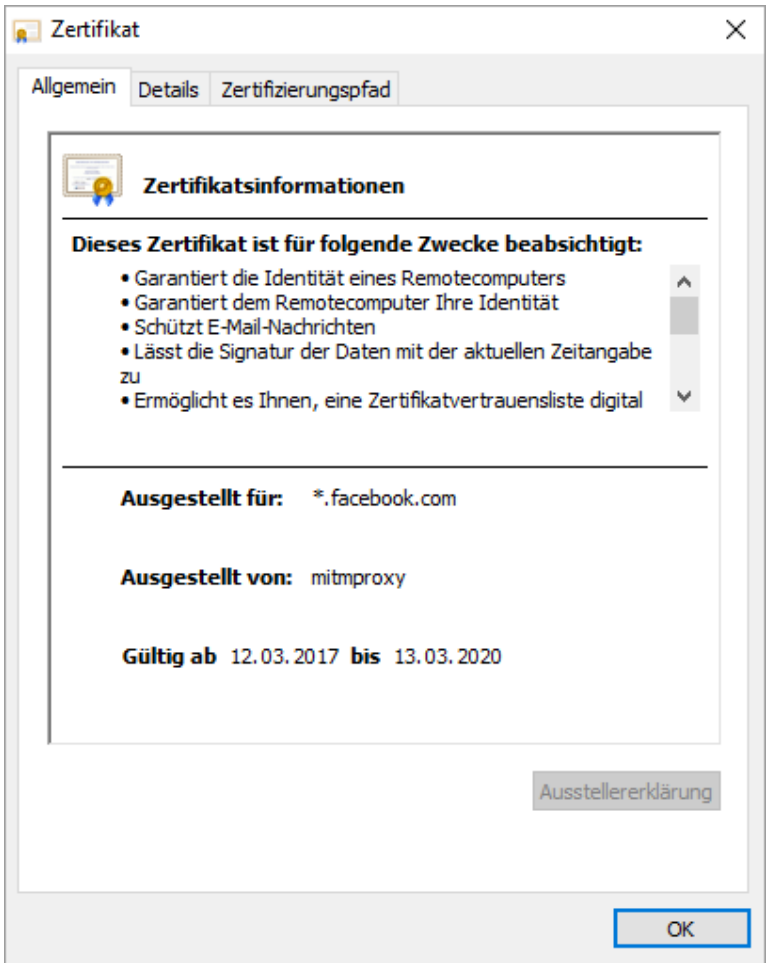
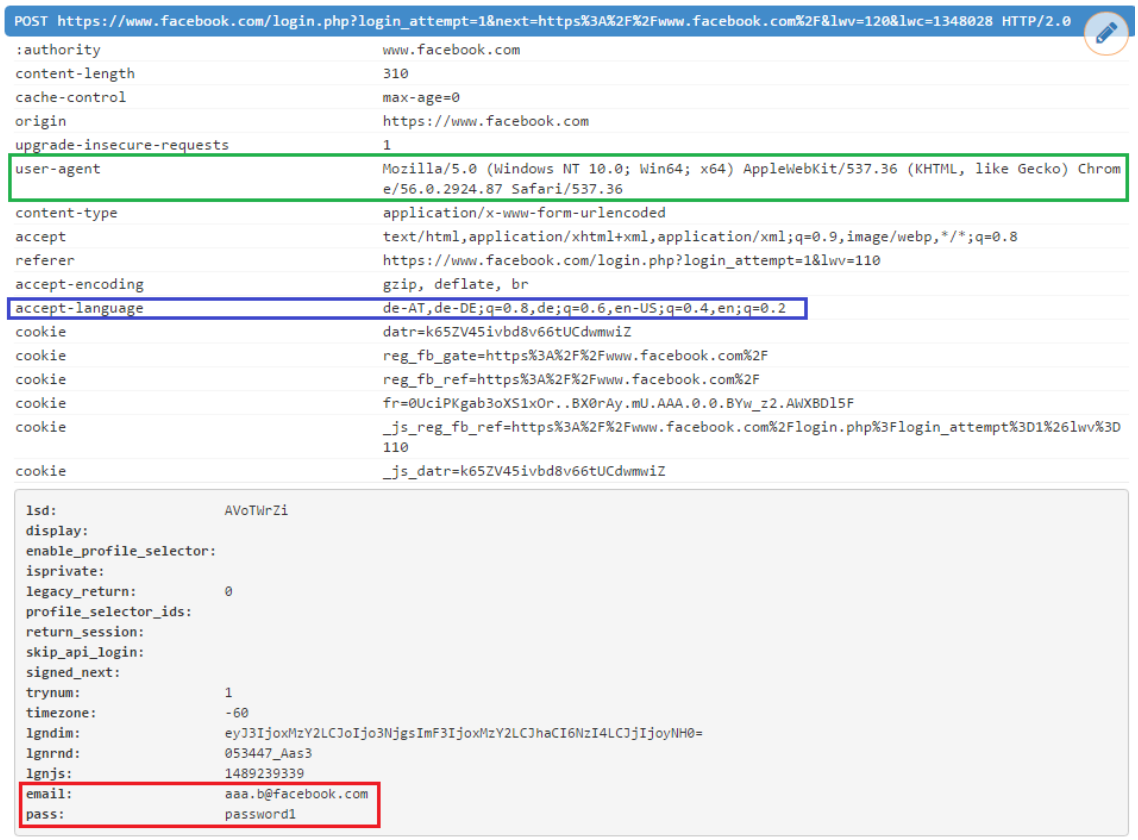


Abbildung 26: Zertifikat der Webseite, ausgestellt von mitmproxy

Im Testfall mit dem Opfer 2, welches mittels Windows Notebook den Proxy für die Internetverbindung nutzt, hat sich gezeigt, dass auch für diesen User keine Möglichkeit besteht einen MITM Angriff zu erkennen, sobald der Proxy eingetragen und das Zertifikat installiert wurde.



POST https://www.facebook.com/login.php?login_attempt=1&next=https%3A%2F%2Fwww.facebook.com%2F&lwv=120&lwc=1348028 HTTP/2.0

:authority	www.facebook.com
content-length	310
cache-control	max-age=0
origin	https://www.facebook.com
upgrade-insecure-requests	1
user-agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
content-type	application/x-www-form-urlencoded
accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
referer	https://www.facebook.com/login.php?login_attempt=1&lwv=110
accept-encoding	gzip, deflate, br
accept-language	de-AT,de-DE;q=0.8,de;q=0.6,en-US;q=0.4,en;q=0.2
cookie	datr=k65ZV45ivbd8v66tUCdwmwiZ
cookie	reg_fb_gate=https%3A%2F%2Fwww.facebook.com%2F
cookie	reg_fb_ref=https%3A%2F%2Fwww.facebook.com%2F
cookie	fr=0UciPKgab3oXS1xOr..BX0rAy.mU.AAA.0.0.BYw_z2.AWXBDl5F
cookie	_js_reg_fb_ref=https%3A%2F%2Fwww.facebook.com%2Flogin.php%3Flogin_attempt%3D1%26lwv%3D110
cookie	_js_datr=k65ZV45ivbd8v66tUCdwmwiZ

lsd:	AVoTWrZi
display:	
enable_profile_selector:	
isprivate:	
legacy_return:	0
profile_selector_ids:	
return_session:	
skip_api_login:	
signed_next:	
trynum:	1
timezone:	-60
lgndim:	eyJ3IjoxMzY2LCJoIjo3NjgsImF3IjoxMzY2LCJhaCI6NzI4LCJjIjoyNH0=
lgnrnd:	053447_Aas3
lgnjs:	1489239339
email:	aaa.b@facebook.com
pass:	password1

Abbildung 27: Ausschrift von mitmproxy beim Login auf Facebook durch Opfer 2

In obiger Abbildung 27 ist ersichtlich, dass auch die Verbindung via Windows Notebook mittels MITM Angriff eingesehen werden kann. In der Abbildung wurden die einzelnen Detailinformationen wieder mit den Farben Rot, Grün und Blau gekennzeichnet, wobei Rot die Login- und Passwortdaten, Grün die Browser- und Betriebssystemdaten und Blau die Landes- und Sprachinformationen hervorheben.

Erkenntnisse aus Test 1

Zusammenfassend kann zum ersten Testfall gesagt werden, dass ein Angriff auf eine HTTPS Verbindung ohne Probleme erfolgen kann, solange es der Angreifer schafft, seinen Rechner als Proxy auf Seiten des Opfers zu platzieren, sowie ein gefälschtes Zertifikat am Rechner des Opfers zu installieren. Dies kann einerseits durch eine Schadsoftware erfolgen, oder durch die Vorgabe eines Proxys in einem freien WLAN. In zweitem Fall würde ein Warnhinweis gemäß Abbildung 18 bzw. Abbildung 19 am Gerät des Opfers aufscheinen. Ignoriert das Opfer diesen, so könnte der Angreifer die Verbindung kompromittieren und Zugriff auf die Verkehrs- und Übertragungsdaten erlangen.

Nicht nur für den privaten Bereich stellt dies ein Problem dar. In Firmennetzwerken werden Proxys von Seiten der Administratorinnen und Administratoren eingerichtet um die Netzwerksicherheit zu erhöhen. Kann ein Angreifer jedoch seinen eigenen Proxy platzieren, so würde der Datenfluss über diesen geleitet werden und die Netzwerksicherheit wäre nicht mehr gegeben.

3.1.6.2 Testfall 2 mit dem „Transparent Proxy“

Der transparente Proxy wird dann eingesetzt, wenn von Seiten des Angreifers die Clienteinstellungen nicht geändert werden können, beziehungsweise das Opfer nicht dazu gebracht werden kann dies selbst zu erledigen. Solche Ausgangssituationen machen diese Art von Proxy für Anwendungen interessant, bei welchen von Seiten der Opfer keine Interaktion, wie beispielsweise das Ändern von Netzwerkeinstellungen oder das Ignorieren von Warnhinweisen, vorausgesetzt werden kann.

Hierzu wurde der Transparent Proxy Mode am Rechner des Angreifers aktiviert und dessen IP als Standardgateway der beiden Opfer eingetragen. Optional wäre es auch möglich gewesen, dass der Angreifer mittels ARP-Spoofing Angriff die Datenverbindung auf seinen Proxy umgelenkt, oder die Netzwerkeinstellung am

Router geändert hätte, so dass der Datenverkehr vom Router an den Proxy umgeleitet worden wäre. Hierzu muss jedoch angemerkt werden, dass die Konfigurationsmöglichkeiten auf Seiten des WLAN Routers sehr begrenzt sind. Aus Sicht der Opfer ändert die Tatsache des eingetragenen Gateways allerdings nichts an der Aussagekraft des Tests.

Es wurde versucht, das Programm mitmproxy über den Web-Dienst zu starten, doch hat sich gezeigt, dass dieser am Windows-OS nicht im Transparent Mode betrieben werden kann. Generell ist zu sagen, dass das Programm mitmproxy eher für den Einsatz auf Linux oder MacOS Betriebssystemen konzipiert ist. So wurde mitmproxy über die „mitmdump.exe“ Anwendung gestartet. Mittels dieses kommandozeilenbasierten Programms war es möglich, die Verbindung der Opfer einzusehen. Weiters musste festgestellt werden, dass das Windows Betriebssystem erst Pakete weiterleitet wenn der entsprechende Registry Wert gesetzt wurde. Der DWORD Eintrag „IPEnableRouter“ muss unter „HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\ Parameters” auf den Wert “1” gesetzt werden. Ab dem Zeitpunkt der erfolgreichen Konfiguration erfolgt der Zugriff des Opfers auf das Internet über den Rechner des Angreifers.

Es hat sich im Zuge des Tests analog zum ersten Versuch gezeigt, dass ohne die Installation des benötigten Zertifikates eine Verbindung zwar möglich ist, der Client jedoch eine entsprechende Fehlermeldung wie im ersten Versuch (siehe hierzu Abbildung 18 und Abbildung 19) erhält.

Nach der Installation des Zertifikates kann der Client nicht mehr ohne weiteres erkennen, dass die Verbindung mittels MITM Angriffs eingesehen wird. Es wurde beispielhaft ein Login-Versuch am Onlinecampus der Ferdinand Porsche Fern FH mitgeloggt. Aufgrund der Verwendung des mitmdump Programms, welches mit dem Befehl „mitmdump.exe -T -d -v 7-w LogFile.txt“ aufgerufen wurde, erfolgt die Ausgabe nicht in einer grafischen Darstellung, sondern Commandline-basierend,

bzw. in einem Textfile (LogFile.txt). Ein Auszug des Logfiles wird in Code 2 gezeigt.

Host,25:onlinecampus.fernfh.ac.at,]28:10:Connection,10:keep-alive,]23:14:Content-Length,2:71,]29:13:Cache-Control,9:max-age=0,]87:6:Accept,74:text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,/*;q=0.8,]46:6:Origin,33:https://onlinecampus.fernfh.ac.at,]33:25:Upgrade-Insecure-Requests,1:1,]184:10:User-Agent,165:Mozilla/5.0 (Linux; Android 6.0.1; SAMSUNG SM-G900F Build/MMB29M) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/4.0 Chrome/44.0.2403.133 Mobile Safari/537.36,]53:12:Content-Type,33:application/x-www-form-urlencoded,]63:7:Referer,49:https://onlinecampus.fernfh.ac.at/login/index.php,]36:15:Accept-Encoding,13:gzip, deflate,]58:15:Accept-Language,35:de-AT,de;q=0.8,en-US;q=0.6,en;q=0.4,]130:6:Cookie,116:__utma=171381175.774064284.1426713732.1473488772.1473508800.10; MoodleSessiononlinecampus=u4mkhufibiu5fh4mkbsca88ge2,]69:13:x-wap-profile,48:http://wap.samsungmobile.com/uaprof/SM-G900F.xml,]]7:content;71:username=Karl.hammer%40mail.fernfh.ac.at&password=dasisteintest&anchor=,12:http_version;8:HTTP/1.1,4:path;16:/login/index.php,15:timestamp_start;18:1489571018.5779145^4:port;3:443#9:is_replay;5:false!6:scheme;5:https,6:method;4:POST,}8:metadata;0:}2:id;36:948e4ca1-73a0-481b-a5e5-bbaa07435b37;8*

Code 2: Auszug aus dem Logfile des Programms mitmdump.exe

Es wurden die entsprechenden Passagen analog zum Testfall 1, mittels der Farben Rot (User und Passwort), Grün (Gerätedaten) und Blau (Sprach- und Landeseinstellungen) markiert.

Ein Test mit dem Windows Rechner des Opfers 2 zeigte dasselbe Bild. Auch hierbei wurde nach der Installation des Zertifikats der Netzwerk-Traffic mitgetraced, ohne dass ein entsprechender Warnhinweis am Client aufgeschienen ist.

Erkenntnisse aus Test 2

In diesem Testfall hat sich gezeigt, dass ein Angreifer mittels ARP-Spoofing, bzw. der Kontrolle über das Netzwerk auch ohne „Mithilfe“ des Opfers einen Man-in-the-Middle Angriff, auf die scheinbar sichere HTTPS Verbindung des Opfers, erfolgreich durchführen kann. Wie bereits im Testfall 1, war es auch in diesem Versuch notwendig, dass der Client das entsprechende Serverzertifikat des Proxys installiert und als sicher beglaubigt.

Bei der Verwendung eines freien WLANs hat der Angreifer möglicherweise sowohl das Netzwerk, als auch alle sonstigen benötigten Ressourcen zur Verfügung um einen Angriff durchzuführen. Gibt der Angreifer bei der Verwendung seines WLANs noch die Installation eines Zertifikates vor, welches von Usern ohne entsprechende Kenntnisse und ohne den notwendigen Bedacht auf die Sicherheit der Datenverbindung installiert wird, so stellt es ein leichtes Unterfangen dar den Netzwerk-Traffic zu kompromittieren.

3.1.6.3 Testfall 3 mit dem „Upstream Proxy“

Auf einen dritten Test mit dem „Upstream Proxy“ wurde bewusst verzichtet, da aus diesem keine neuen Erkenntnisse gewonnen werden könnten. Die Ergebnisse aus den beiden erfolgten Testfällen würden gemäß Recherche bestätigt werden, allerdings hätte sich aus Sicht der Opfer keine neue Situation ergeben. Die beiden Testfälle mit dem Regular und dem Transparent Proxy wurden bewusst gewählt, weil diese den häufigsten Angriffsmodi entsprechen, da in der Regel ein Standarduser keinen Proxy im Einsatz hat.

3.1.7 Gewonnene Erkenntnisse

In der Praxis bedeuten die Ergebnisse aus den Versuchen, dass bei der Verwendung von TLS Proxys stets das Risiko besteht, dass die vermeintlich

sichere Verbindung kompromittiert wird. Beispielsweise verwenden Virenschutz- und Kinderschutzprogramme eigene TLS Proxys, welche gemäß einer Studie [59] nicht immer sicher sind. In besagter Studie wurden 14 Antivirus- und Kinderschutzprodukte unterschiedlicher Hersteller untersucht und dabei festgestellt, dass keines davon als sicher eingestuft werden kann. Die vorgefundenen Probleme reichten von einfach akzeptierten aber gefälschten Zertifikaten bis hin zu reduziertem Schutz gegen aktuelle Angriffe.

Auf Seiten der Smartphones wiegt dieses Problem mindestens genauso stark, da in den einzelnen App-Stores viele unterschiedliche Apps zum Download angeboten werden, welche mitunter Schadsoftware beinhalten. In vielen Stores werden die angebotenen Programme nicht bzw. nur sehr oberflächlich getestet, wodurch nie die Sicherheit gegeben ist, dass man durch eine Installation nicht doch einem Angreifer ausgeliefert ist.

Doch nicht nur bei installierten Programmen oder Apps können Sicherheitslücken entstehen, welche vom User gar nicht erst erkannt werden können, sondern auch bei der Verwendung von öffentlichen WLANs, wenn beispielsweise bei der Verwendung eben dieser WLANs Proxys oder eigene Zugangsprogramme vorgeschrieben werden. Ebenso könnte die Installation eines Zertifikats verlangt werden um mittels eines transparenten Proxys an die Kommunikationsdaten zu gelangen.

Generell muss gesagt werden, dass in frei zugänglichen Netzwerken die Übermittlung von sensiblen oder geheimen Daten nicht ohne Restrisiken möglich ist, wie im Test auch gezeigt wurde. Bei Cloud-Services wie dem Online-Banking sollte deshalb ein anderer Kommunikationskanal, beispielsweise über den Telefonprovider gewählt werden. Es ist anzumerken, dass von der Installation nicht bekannter und nicht vertrauenswürdiger Zertifikate Abstand zu halten ist. Diese können zu einem sehr hohen Sicherheitsrisiko führen, welches für die User weder abschätzbar, noch erkennbar ist. Im Testfall hat sich gezeigt, dass ohne die

Installation des entsprechenden Zertifikates ein Warnhinweis gekommen und ein potentielles Opfer somit gewarnt worden wäre.

3.2 Umfrage

3.2.1 Ausgangslage und Ziel der Befragung

Im Zuge der praktischen Versuche wurde evaluiert, dass eine HTTPS Verbindung mittels MITM Angriff erfolgreich abgehört werden kann. Diesbezüglich braucht es nur die Installation des entsprechenden Zertifikates, beziehungsweise eines entsprechenden Programmes welches dieses Zertifikat mitführt, oder die Leichtgläubigkeit und Unvernunft der Anwenderinnen und Anwender, welche auf Warnhinweise oder Symbole im Webbrowser nicht entsprechend reagieren.

In einer Online-Umfrage (siehe Anhang B) soll eruiert werden, ob sich die Umfrageteilnehmerinnen und -teilnehmer der Gefahr, welche vor allem bei der Verwendung von öffentlichen Netzwerken bestehen, bewusst sind. Ebenfalls soll hervorgehen, ob die Nutzerinnen und Nutzer von Cloud-Services die im praktischen Versuch ermittelten Voraussetzungen für ein sicheres Arbeiten auch einhalten.

3.2.2 Methodisches Vorgehen

Es wurde eine quantitative Umfrage erarbeitet und der entsprechende Fragebogen online gestellt, welcher geschlossene Fragen mit vorgegebenen Antwortkategorien beinhaltete. Die damit ermittelten Daten wurden mittels Kreuztabellen in Relation gestellt, ausgewertet und mit dem Chi-Quadrat-Test auf Relevanz überprüft. Die Daten in den Kreuztabellen sind sowohl in absoluten Häufigkeiten und prozentuiert nach Gesamthäufigkeit oder in zeilenweiser prozentueller Darstellung angegeben. Einzig in den beiden Kreuztabellen zu den persönlichen Angaben sind

die Umfragewerte zwecks Übersichtlichkeit nur in absoluten Häufigkeiten angegeben. Es wurde statistisch erhoben, ob Personen unterschiedlicher Altersgruppen auf die Gefahren sensibilisiert sind, welche bei der Verwendung von Cloud-Services und speziell in der Kommunikation mit diesen Diensten, bestehen.

3.2.3 Planung und Durchführung der Umfrage

3.2.3.1 Definition der Zielgruppe

Als Zielgruppe wurden Menschen aller Altersklassen definiert, welche Onlineaktivitäten nachgehen. Es ist dabei unerheblich, über welches Gerät bzw. über welchen Zugang die einzelnen Personen online kommunizieren.

3.2.3.2 Durchführung der Umfrage

Um einen möglichst großen Personenkreis ansprechen zu können, wurde eine Online-Umfrage erstellt. Diese wurde zuerst an 5 Pre-TesterInnen versendet, welche ein Feedback zur Verständlichkeit der Fragen gaben um Fehlern vorzubeugen. Es wurde mittels mitgeführten Tools des Frameworks der SoSci Survey GmbH die durchschnittliche Durchlaufzeit erhoben. Auch wenn die Fragen geschlossen und die Antwortkategorien vorgegebenen sind, so gestattet es das Framework dennoch, die Fragen in Abhängigkeit voneinander zu stellen, um so die Nutzerakzeptanz zu erhöhen und in weiterer Folge mehrere vollständige Datensätze zu erhalten.

Der Pre-Test wurde durch das Einarbeiten der Feedbacks abgeschlossen und die Online-Umfrage sowohl im privaten, als auch beruflichem Umfeld publiziert. Hierzu wurden Mails mit dem Link versendet, sowie die Umfrage im Onlinecampus der FernFH, auf Facebook und auf Xing gepostet.

Der Fragebogen findet sich in Anhang B und ist gemäß den Kapiteln für dessen Auswertung gegliedert.

3.2.4 Datenaufbereitung und –analyse

Die Daten wurden aus der Onlineumfrage als CSV-File exportiert und in die Auswerteprogramme importiert. Für die statistische Auswertung wurden die freie Software R, welche unter „https://www.r-project.org/“ verfügbar ist, sowie das Tabellenkalkulationsprogramm Microsoft Excel verwendet. Mittels dieser beiden Softwareprodukte können statistische Berechnungen durchgeführt und Grafiken erstellt werden.

Die Online-Umfrage wurde insgesamt 567-mal aufgerufen, wobei jedoch nur 163 Personen den Fragebogen vollständig ausgefüllt haben. Für die weitere Analyse wurden nur jene Befragungsdaten berücksichtigt, bei welchen ein vollständig ausgefüllter Umfragebogen vorlag. Der statistische Rücklauf der Umfrageergebnisse wird in Tabelle 10 dargestellt. Es lässt sich leicht erkennen, dass sehr viele Personen, den Fragebogen zwar aufgerufen, jedoch nicht begonnen haben diesen zu beantworten. Von jenen, welche mit der Beantwortung der Fragen begonnen haben, ist der Fragebogen auch großteils abgeschlossen worden.

Aufgerufene Fragebögen	567
Begonnene Fragebögen	175
Beendete Fragebögen	163
Durchschnittliche Bearbeitungszeit [in Sekunden]	215

Tabelle 10: Darstellung des Rücklaufs der Onlinefragebögen

3.2.4.1 Evaluierung der Persönlichen Daten

Von den insgesamt 163 Personen, sind rund 37% weiblich und 63% männlich. Gemäß dem Umfrageergebnis arbeiten davon 31% in der IT-Branche, 68% in einem andern beruflichen Umfeld und der Rest hat dazu keine Angabe gemacht. Die persönlichen Daten der Umfrageteilnehmerinnen und Teilnehmer finden sich in nachstehender Tabelle 11 und der berufliche Tätigkeitsbereich in Relation zum Alter in Tabelle 12. Zum Beruf der Umfrageteilnehmerinnen und Teilnehmer ist anzumerken, dass im Fragebogen nur nach einer Tätigkeit im IT Bereich gefragt

wurde, da eine Unterscheidung in andere Berufsgruppen für die Umfrage keine Relevanz hat.

	unter 14	14 bis 18	19 bis 25	26 bis 29	30 bis 39	40 bis 49	50 bis 59	60 und darüber	Summe
Weiblich	0	2	6	15	19	12	6	1	61
Männlich	0	1	11	19	40	22	7	2	102
Summe	0	3	17	34	59	34	13	3	163

Tabelle 11: Kreuztabelle Geschlecht und Alter der Umfrageteilnehmerinnen und Teilnehmer

	unter 14	14 bis 18	19 bis 25	26 bis 29	30 bis 39	40 bis 49	50 bis 59	60 und darüber	Summe
Im IT-Bereich	0	1	6	13	22	6	3	0	51
Anderer Bereich	0	2	11	21	36	28	10	3	111
Keine Angabe	0	0	0	0	1	0	0	0	1
Summe	0	3	17	34	59	34	13	3	163

Tabelle 12: Kreuztabelle berufliches Tätigkeitsfeld und Alter der Befragten

3.2.4.2 Einstellung der Befragten in Bezug auf Cloud-Services

Verwendung	Anzahl d. Befragten	Prozent-satz
Cloudspeicher (z.B. Dropbox, Google Drive, ...)	113	70%
Social Media Services (z.B. Facebook, Instagram, ...)	137	85%
Serviceportale für Finanzen (z.B. Onlinebanking, Bank-Webportal, ...)	142	88%
Serviceportale für Einkauf (z.B. E-Bay, Amazon, ...)	141	87%
Virtualisierungsplattformen (Amazon, Microsoft, ...)	60	37%
Officeanwendungen im Web (z.B. Office 365, Google Docs, ...)	86	53%
Mail und organisatorische Webservices (z.B. GMX, Google Kalender, ...)	142	88%
Enterprise-Resource-Planning (ERP) Online-Cloud-Dienste (z.B. Scopevisio, SAP, ...)	18	11%
Weitere Cloud-Services	15	9%

Tabelle 13: Verwendung von Cloud-Services gemäß Umfrageergebnis (Mehrfachnennungen möglich)

Von den befragten Personen verwenden alle bis auf eine Cloud-Services, was einem Prozentsatz von über 99% ausmacht. Die Antworten auf die Frage welche Cloud-Services in Anspruch genommen werden würden, sind in Tabelle 13 zusammengefasst. Hierbei hat sich herausgestellt, dass die Befragten vor allem Dienste in Anspruch nehmen, bei welchen sensible oder vertrauliche Daten ausgetauscht werden. Auffallend ist auch, dass der Prozentsatz von Services bei welchen Finanztransaktionen getätigt werden sehr hoch ist.

Von den Personen, welche Cloud-Services in Anspruch nehmen, haben 46% angegeben, dass sie diese nur privat und 49% sowohl privat als auch im beruflichen Umfeld verwenden. Insgesamt ergibt sich somit, dass 95% der Teilnehmerinnen und Teilnehmer Cloud-Services im privaten Rahmen verwenden, wie in Tabelle 14 gezeigt wird.

	Nicht beantwortet	Verw. nur privat	Verw. nur beruflich	Verw. privat u. beruflich	Summe
Im IT- Bereich	0 (0%)	13 (8%)	4 (2%)	34 (21%)	51 (31%)
Anderer Bereich	3 (2%)	60 (37%)	1 (1%)	46 (28%)	110 (68%)
Keine Angabe	0 (0%)	1 (1%)	0 (0%)	0 (0%)	1 (1%)
Summe	3 (2%)	74 (46%)	5 (3%)	80 (49%)	162 (100%)

Tabelle 14: Kreuztabelle berufliches Tätigkeitsumfeld und Verwendung von Cloud-Services prozentuiert nach Gesamthäufigkeit

Mittels des Chi-Quadrat-Tests kann das Ergebnis auf Signifikanz überprüft werden, indem ausgewertet wird, ob Zusammenhänge zwischen dem beruflichen Tätigkeitsfeld und den Einsatzbereichen von Cloud-Services mehr als nur zufällig sind. Da der ermittelte p-Wert für die asymptotische Signifikanz bei 0.004477 und somit weit unter dem Wert von 0,01 liegt, kann das Ergebnis als hoch signifikant angesehen werden. Es besteht somit ein nachgewiesener Zusammenhang zwischen dem Beruf in der IT und der Verwendung von Cloud-Services im privaten und beruflichen Umfeld. Dieser Zusammenhang ist sowohl in Tabelle 14, als auch in Abbildung 28 ersichtlich, da die Teilnehmerinnen und Teilnehmer, welche im IT Bereich tätig sind, vorwiegend Cloud-Services sowohl privat als auch beruflich verwenden, während bei Menschen in anderen Berufen dies gemäß Umfrage nicht

derart ausgeprägt der Fall ist. Von diesen nehmen mehr als die Hälfte die Dienste nur privat in Anspruch. In Abbildung 28 werden Personen, welche im IT-Bereich tätig sind dunkel dargestellt, während jene aus anderen Berufszweigen den grauen Bereichen der Balken entsprechen. Der helle Bereich an der Spitze der Säule „privat“ entspricht dem nicht angegebenen Tätigkeitsbereich.

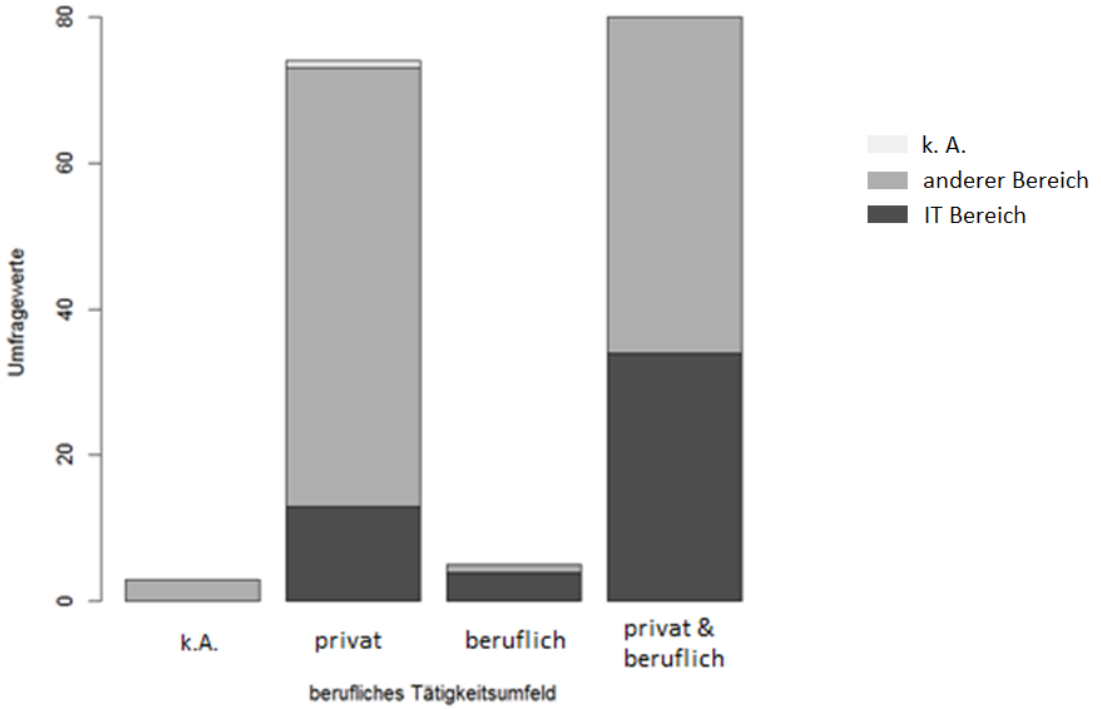


Abbildung 28: Gruppiertes Balkendiagramm der Kreuztabelle berufliches Tätigkeitsumfeld und Verwendung von Cloud-Services

3.2.4.3 Verwendung von öffentlichen WLAN-Zugängen

In der Umfrage haben 74% der Befragten angegeben, dass sie öffentliche WLAN-Zugänge nutzen. Setzt man die WLAN-Verwendung mit dem beruflichen Umfeld in Relation, ergibt sich jene Kreuztabelle, welche in Tabelle 15 dargestellt wird. Es ist zu betonen, dass diese jedoch gemäß Chi-Quadrat-Test (p-Wert von 0.1788) keine Relevanz aufweist und somit kein Zusammenhang zwischen dem beruflichen Umfeld und der WLAN-Nutzung nachgewiesen werden kann. Es kann somit nicht gesagt werden, dass Menschen welche im IT Bereich arbeiten, öffentliche WLAN Zugänge öfter oder weniger oft verwenden als andere.

	Verwendung öffentlicher WLAN Zugänge	Keine Verwendung öffentlicher WLAN Zugänge	Summe
Im IT- Bereich	40 (25%)	11 (7%)	51 (31%)
Anderer Bereich	81 (50%)	30 (18%)	111 (68%)
Keine Angabe	0 (0%)	1 (1%)	1 (1%)
Summe	121 (74%)	42 (26%)	163 (100%)

Tabelle 15: Kreuztabelle Verwendung von öffentlichen WLAN-Zugängen und berufliche Tätigkeit prozentuiert nach Gesamthäufigkeit

Es wurde in der Umfrage darauf eingegangen, ob sich die Befragten, welche öffentliche WLAN Netze nutzen, sich in einem solchen sicher fühlen und ob sie dabei persönliche bzw. auch Bank-Daten übertragen. Die Ergebnisse werden in den beiden folgenden Kreuztabellen Tabelle 16 und Tabelle 17 veranschaulicht. Es ist in Tabelle 16 zu erkennen, dass der Austausch von persönlichen Daten sowohl für Menschen, welche sich in öffentlichen WLAN-Netzen sicher fühlen, als auch von jenen, welche dieses Gefühl nicht haben, keine Bedenken hervorruft. Auch wenn von den Personen, welche sich im öffentlichen WLAN nicht sicher fühlen prozentuell mehrere von ihnen keine dieser Daten übertragen würden, so stellen diese immer noch eine Minderheit dar. Insgesamt würden rund 80% aller Befragten persönliche Daten über ein öffentliches Netz übertragen. Der Zusammenhang, welcher in Tabelle 16 angenommen wurde, kann als Signifikat angesehen werden, da eine Überprüfung mittels Chi-Quadrat-Test einen p-Wert von 0.02007 ergeben hat.

	persönliche Daten übertragen	keine persönliche Daten übertragen	Summe
Sicher	54 (45%)	7 (6%)	61 (50%)
Nicht Sicher	43 (36%)	17 (14%)	60 (50%)
Summe	97 (80%)	24 (20%)	121 (100%)

Tabelle 16: Kreuztabelle Sicherheitsgefühl bei der Verwendung von WLAN und Übertragung von persönlichen Daten prozentuiert nach Gesamthäufigkeit

Handelt es sich bei den betreffenden Daten jedoch um Bankdaten, so würden gemäß der Umfrage nur noch insgesamt 21% das öffentliche WLAN verwenden, wie aus Tabelle 17 hervorgeht. Auch dieser Zusammenhang konnte mittels Chi-Quadrat-Test nachgewiesen werden (p-Wert von 0.03032). Das bedeutet, dass

Menschen, welche sich in öffentlichen Netzwerken nicht sicher fühlen, diese auch weniger häufig zur Übertragung von Bankdaten nutzen als andere.

	Bankdaten übertragen	keine Bankdaten übertragen	Summe
Sicher	18 (15%)	43 (36%)	61 (50%)
Nicht Sicher	8 (7%)	52 (43%)	60 (50%)
Summe	26 (21%)	95 (79%)	121 (100%)

Tabelle 17: Kreuztabelle Sicherheitsgefühl bei der Verwendung von WLAN und Übertragung von Bankdaten prozentuiert nach Gesamthäufigkeit

3.2.4.4 Sicherheitsaspekte während der Cloud-Kommunikation

Im nächsten Abschnitt des Fragebogens wurde auf die Sicherheitsaspekte bei Onlineaktivitäten eingegangen. Hierbei wurden Fragen ausgewählt, welche die Risiken, die im Rahmen des praktischen Versuchs eruiert wurden, ausforschen. Als erstes wurde hinterfragt, ob die Teilnehmerinnen und Teilnehmer verschlüsselte Verbindungen, im speziellen das HTTPS Protokoll präferieren, oder ob es ihnen gleichgültig ist, wie diese abgehandelt werden.

		Nutzung unsicherer Verbindungen bei Warnhinweisen in Browser				
Achtsamkeit in Bezug auf gesicherte Verbindungen		Ja Immer	Nur wenn ich die aufgerufene Webseite kenne	Gele-gentlich	Nie	Summe
	Immer	14 (9%)	18 (11%)	3 (2%)	1 (1%)	36 (22%)
	Oft	8 (5%)	39 (24%)	10 (6%)	1 (1%)	58 (36%)
	Selten	8 (5%)	21 (13%)	7 (4%)	2 (1%)	38 (23%)
	Nie	4 (2%)	21 (13%)	6 (4%)	0 (0%)	31 (19%)
	Summe	34 (21%)	99 (61%)	26 (16%)	4 (2%)	163 (100%)

Tabelle 18: Kreuztabelle Aufmerksamkeit auf gesicherte Verbindungen und Nutzung trotz Warnhinweis prozentuiert nach Gesamthäufigkeit

Wie aus Tabelle 18 hervorgeht, hat sich hierbei ergeben, dass lediglich 22% der befragten Personen immer darauf achten, dass eine gesicherte Verbindung besteht, während 19% hingegen nie darauf achtgeben. Dennoch ist zu erwähnen, dass insgesamt 58% angegeben haben, dass sie „Immer“ bzw. „Oft“ darauf achten. Würde bei der Onlineaktivität ein entsprechender Warnhinweis erscheinen, wie in

Abbildung 29 gezeigt wird, so hätten die Befragten gemäß dem Umfrageergebnis eher Skrupel davor, die Seite aufzurufen. Über 61% geben an, dass sie die entsprechende Webseite nur aufrufen, wenn sie diese kennen würden. Dennoch haben 37% angegeben, dass sie trotz eines Warnhinweises immer oder zumindest gelegentlich eine solche Internetadresse aufrufen würden.

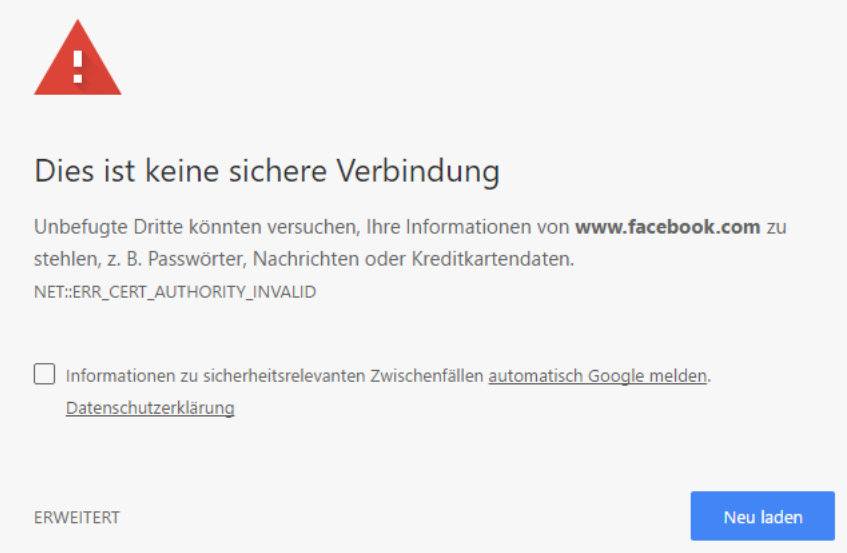


Abbildung 29: Warnhinweis zu unsicherer Verbindung

Setzt man diese beiden Fragen in Abhängigkeit voneinander, so ergibt sich Tabelle 18, sowie deren grafische Darstellung Abbildung 30. In der Abbildung wird die Aufmerksamkeit auf gesicherte Verbindungen in Graustufen der Balken abgebildet. Es geht hervor, dass die entsprechende Webseite von einer Mehrheit von 98% aufgerufen wird, sofern sie bekannt ist. Ob ein entsprechendes Zertifikat der Webseite vorhanden ist, spielt dabei gemäß Umfrage für einen Großteil der Teilnehmerinnen und Teilnehmer keine Rolle. Anzumerken sei in diesem Zusammenhang, dass gemäß dem Chi-Quadrat-Test (p-Wert von 0.1482) das Ergebnis als nicht signifikant angesehen werden muss. Dies bedeutet, dass gemäß diesem Test kein Zusammenhang zwischen der Aufmerksamkeit zu gesicherten Verbindungen und der Nutzung von Webseiten trotz eines Warnhinweises besteht. Es kann somit nicht angenommen werden, dass Personen, welche auf die Symbole

und Warnhinweise im Webbrowser achten, diese Warnungen auch berücksichtigen würden.

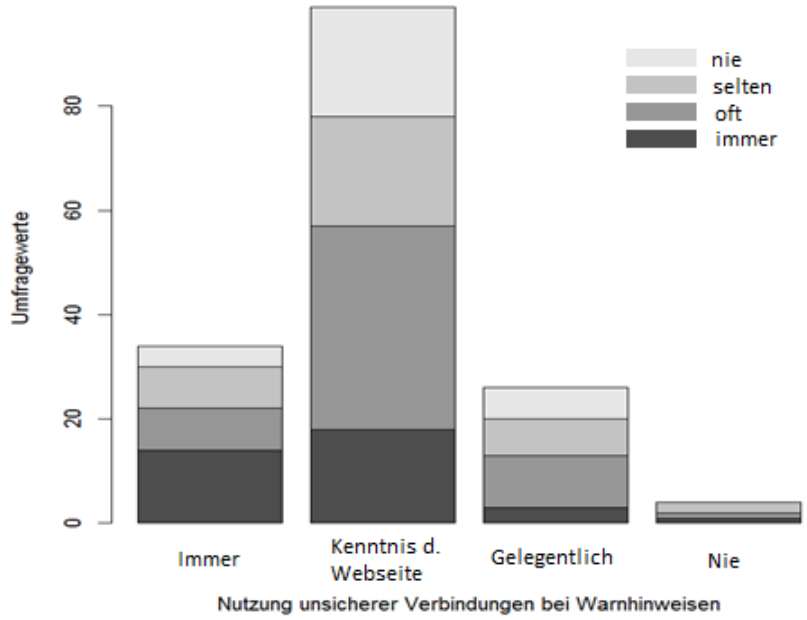


Abbildung 30: Gruppiertes Balkendiagramm der Kreuztabelle Aufmerksamkeit auf gesicherte Verbindungen und Nutzung trotz Warnhinweis

		Nutzung unsicherer Verbindungen bei Warnhinweisen in Browser				
		Ja Immer	Nur wenn ich die aufgerufene Webseite kenne	Gele-gentlich	Nie	Summe
Berufliches Tätigkeitsfeld	Im IT-Bereich	6 (12%)	36 (71%)	6 (12%)	3 (6%)	51 (100%)
	Anderer Bereich	28 (25%)	63 (57%)	19 (17%)	1 (1%)	111 (100%)
	Keine Angabe	0 (0%)	0 (0%)	1 (100%)	0 (0%)	1 (100%)
	Summe	34 (21%)	99 (61%)	26 (16%)	4 (2%)	163 (100%)

Tabelle 19: Kreuztabelle berufliches Tätigkeitsfeld und Nutzung trotz Warnhinweis in zeilenweiser prozentueller Darstellung

Die Nutzung unsicherer Verbindungen wurde in Abhängigkeit zum beruflichen Tätigkeitsbereich gestellt, wie Tabelle 19 zeigt. Zur leichteren Lesbarkeit wird diese in zeilenweiser prozentueller Darstellung angegeben. Die Kreuztabelle wird in Abbildung 31 mittels gruppierten Balkendiagramms dargestellt. Es lässt sich

daraus ablesen, dass eine Tätigkeit im IT Bereich einen Einfluss auf die Nutzung unsicherer Webseiten hat. Dies wird durch den Chi-Quadrat-Test (p-Wert von 0.03445) bestätigt. Es sind allerdings immer noch 12% der IT-Beschäftigten, welche angeben, immer eine unsichere Webseite aufzurufen.

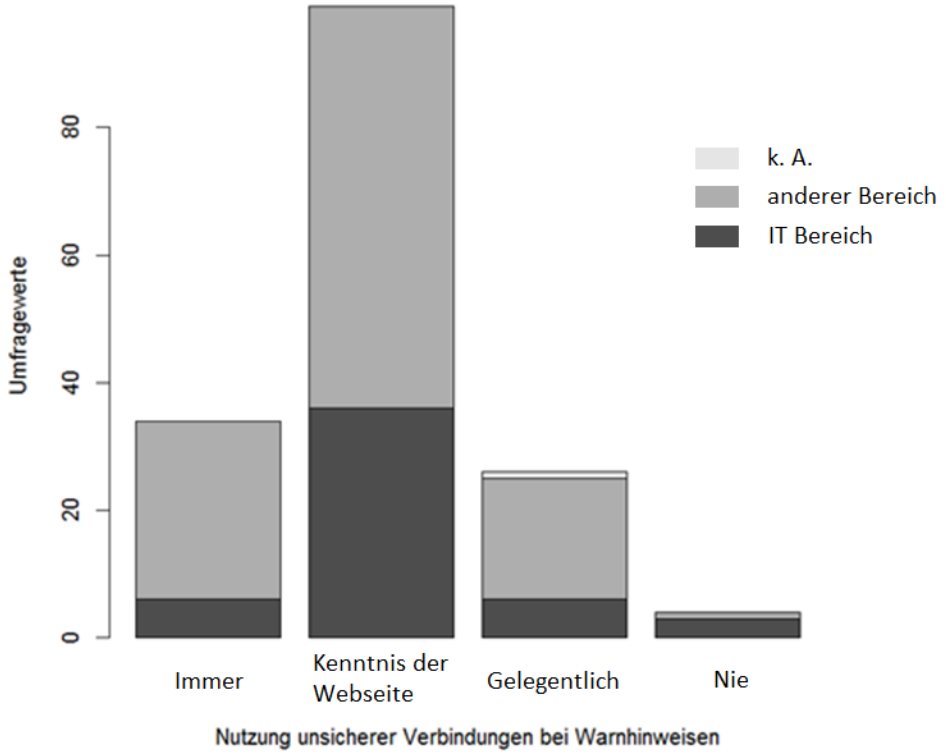


Abbildung 31: Gruppiertes Balkendiagramm der Kreuztabelle berufliches Tätigkeitsfeld und Nutzung trotz Warnhinweis

		Installation eines SSL/TLS Zertifikats					
		Keine Angabe	Ja immer	Nur wenn ich dem Aussteller des Zertifikates vertraue	Nur wenn ich die Seite bzw. die App unbedingt nutzen will	Nein nie	Summe
Kenntnis über SSL/TLS Zertifikat	Ja	0 (0%)	6 (9%)	49 (70%)	10 (14%)	5 (7%)	70 (100%)
	Nein	1 (1%)	3 (3%)	49 (53%)	31 (33%)	9 (10%)	93 (100%)
	Summe	1 (1%)	9 (6%)	98 (60%)	41 (25%)	14 (9%)	163 (100%)

Tabelle 20: Kreuztabelle Kenntnis über SSL/TLS Zertifikat und Installation eines SSL/TLS Zertifikats in zeilenweiser prozentueller Darstellung

Es wurde hinterfragt, ob die Befragten wissen was ein SSL/TLS Sicherheitszertifikat ist, beziehungsweise ob sie ein derartiges Zertifikat installieren würden wenn sie auf einer Website beziehungsweise in einer App darauf hingewiesen werden. Die Ergebnisse dieser beiden Fragen werden in Tabelle 20 mittels Kreuztabellendarstellung zusammengefasst und in Abbildung 32 visualisiert.

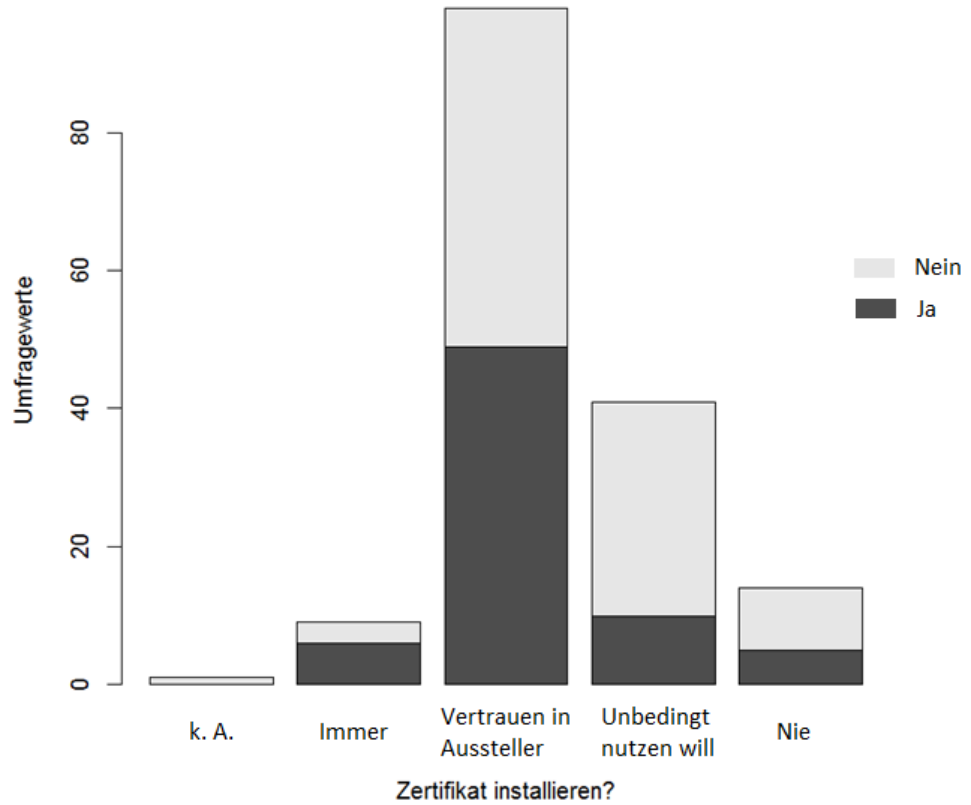


Abbildung 32: Gruppiertes Balkendiagramm der Kreuztabelle Kenntnis über SSL/TLS Zertifikat und Installation eines SSL/TLS Zertifikats

Die Umfrageteilnehmerinnen und -Teilnehmer haben angegeben, dass 43% von ihnen wissen, um was es sich bei einem Zertifikat handelt. Es wurde ermittelt, dass 60% von ihnen ein solches installieren, wenn sie dem Aussteller vertrauen. Hierbei ist es für den Großteil der Befragten unerheblich, ob ihnen der Begriff Zertifikat bekannt ist oder nicht. 25% geben an, dass sie ein Zertifikat installieren, wenn sie eine Seite bzw. eine App unbedingt nutzen wollen. Hierbei ist vor allem die Zahl jener Personen sehr hoch, welchen Zertifikate kein Begriff sind. Bei der

Auswertung mittels Chi-Quadrat-Tests (p-Wert von 0.02806) zeigt sich, dass ein Zusammenhang zwischen dem Wissen über ein Zertifikat und dessen Installation besteht. Man erkennt diesen Zusammenhang sehr gut, da Menschen welche wissen was ein Zertifikat ist, gemäß Umfrageergebnis vorsichtiger beim Installieren sind.

Die Frage nach dem Kenntnisstand eines SSL/TLS Zertifikats relativiert sich mit der Frage, ob die Befragten auf das Symbol neben der URL im Browser achten würden, welches beispielhaft in Abbildung 33 in mehreren Varianten dargestellt wird. Bei Beachtung dieses Symboles könnte erkannt werden, ob eine Webseite über ein gültiges Zertifikat verfügt oder nicht. In Hinblick auf die Fragen nach einer möglichen Zertifikatsinstallation hat dies keinen Einfluss, da nach einer erfolgten Installation eines gefälschten Zertifikates kein Warnhinweis mehr erscheinen würde. Die Umfrageergebnisse hierzu finden sich in Tabelle 21. Es ist ersichtlich, dass lediglich 28% immer auf eine gesicherte Verbindung achten, während dies bei ebenfalls 28% nie der Fall ist.

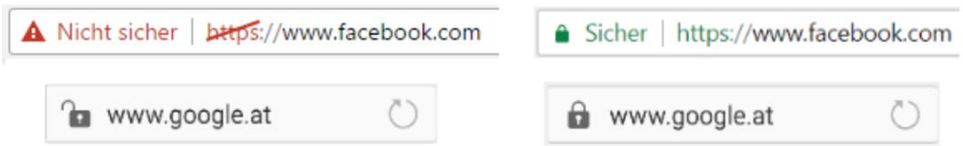


Abbildung 33: Beispiele für die Darstellung des Sicherheitsstatus im Browser

Achten Sie auf das Symbol im Browser neben der Website-URL?	Anzahl d. Befragten	Prozentsatz
Ja immer	45	28%
Gelegentlich	62	38%
Nur wenn es farblich auffällt	10	6%
Nie	46	28%
Summe	163	100%

Tabelle 21: Beachtung von Browsersymbolen und Warnhinweisen gemäß Umfrageergebnis

3.2.4.5 Verwendung von Proxys

Da beim praktischen Versuch eruiert wurde, dass auch bei der Verwendung von einem Netzwerkproxy Sicherheitsbedenken bestehen können, wurde im Zuge der Umfrage erhoben, ob die Befragten solche Proxys im Einsatz haben. Das Ergebnis findet sich in Tabelle 22. Es ist ersichtlich, dass nicht alle Teilnehmerinnen und

Teilnehmer eine Art Proxy im Einsatz haben. Der Virenscanner stellt dabei erwartungsgemäß die am häufigsten eingesetzte Variante dar. Zu beachten ist, dass Mehrfachnennungen im Zuge der Erhebung möglich waren. So haben manche Personen verschiedene Anwendungen mit einem integrierten Proxy im Einsatz.

Art des Proxys	Anzahl der Nennungen
Kinderschutzprodukte	16
Virenscanner	141
Webserver mit TLS Proxy	22
Andere Art von TLS Proxy	7
Keine Proxyanwendung	20

Tabelle 22: Einsatz von Proxyanwendungen bei den befragten Personen (Mehrfachnennungen möglich)

Da 20 Personen (12%) keine Proxyanwendung im Einsatz haben, sind diese für die weiteren Fragen zum Thema Proxy nicht relevant. Die restlichen Umfrageteilnehmerinnen und -teilnehmer wurden bezüglich der gefühlten Sicherheit bei der Verwendung der Proxys und zu der Tatsache, dass gemäß einer Studie, viele Virenscanner und Kinderschutzprogramme nicht sicher sind (siehe hierzu Kapitel 3.1.7), befragt. Die Ergebnisse wurden in Tabelle 23 zusammengefasst, aus welcher erwartungsgemäß hervorgeht, dass Personen, welche von der Studie Kenntnis hatten diese Proxys als eher unsicher einstuften und vice versa.

Kenntnis der Proxy-Studie bzw. von dessen Ergebnis	Fühlen Sie sich bei der Verwendung der Produkte sicher?		
	Ja	Nein	Summe
Ja	35 (24%)	16 (11%)	51 (36%)
Nein	86 (60%)	6 (4%)	92 (64%)
Summe	121 (85%)	22 (15%)	143 (100%)

Tabelle 23: Kreuztabelle Kenntnis der Proxy-Studie bzw. von dessen Ergebnis und Sicherheitsgefühl bei der Verwendung von Proxy-Anwendungen prozentuiert nach Gesamthäufigkeit

Die Erkenntnis aus Tabelle 23 lässt sich ebenfalls leicht aus Abbildung 34 ableiten, in welcher die Personen, welche Kenntnis von der Studie hatten dunkel und jene

welche keine Kenntnis hatten hell dargestellt werden. Auffallend ist, dass die Mehrheit der Befragten, welche eigentlich Kenntnis hatten, die Produkte trotzdem als sicher empfinden. Der Zusammenhang zwischen der Kenntnis der Studie und dem Sicherheitsempfinden gegenüber den Anwendungen lässt ich mittels Chi-Quadrat-Test (p-Wert von $7{,}969*10^{-5}$) bestätigen und kann als hoch signifikant angenommen werden.

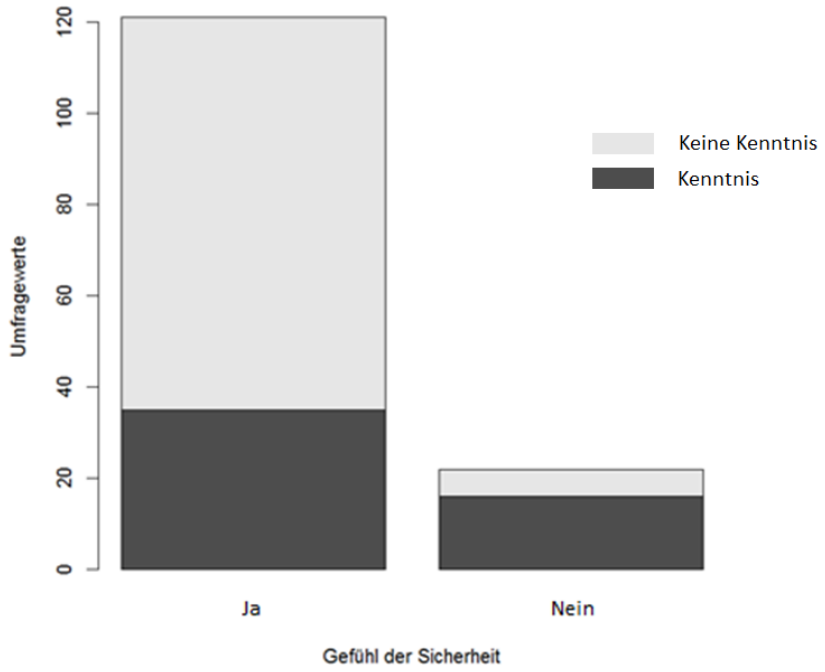


Abbildung 34: Gruppiertes Balkendiagramm der Kreuztabelle Kenntnis der Proxy-Studie bzw. von dessen Ergebnis und Sicherheitsgefühl bei der Verwendung von Proxy-Anwendungen

3.2.4.6 Negative Erfahrungen der Umfrageteilnehmer in Bezug auf Onlinesicherheit

Um die negativen Erfahrungen der Teilnehmerinnen und Teilnehmer auszuwerten wurde zuerst die Frage gestellt, ob diese in der Vergangenheit schon mal bemerkt hätten, dass ihre Internetverbindung „abgehört“ worden wäre, bzw. ob sie mittels einer Sicherheitswarnung davon in Kenntnis gesetzt wurden. Wenn sie eine entsprechende Meldung bekommen hätten, so sollte diese in die vorgegebenen

Kategorien eingetragen werden, wobei Mehrfachmeldungen möglich sind. Die entsprechenden Antworten sind in Tabelle 24 zusammengefasst.

Antwortmöglichkeiten	Anzahl der Nennungen
Ich wurde vom Browser mittels Meldung oder Symbol darauf aufmerksam gemacht.	18
Ich wurde vom Betriebssystem darauf aufmerksam gemacht.	5
Ich wurde über eine andere Software darüber in Kenntnis gesetzt.	8
Ich hatte selbst das Gefühl „abgehört“ zu werden.	6
Ich habe diesbezüglich noch keine negativen Erfahrungen gemacht.	141

Tabelle 24: Negative Erfahrungen der befragten Personen zu MITM Angriffen (Mehrfachnennungen möglich)

Falls die Umfrageteilnehmerinnen und -Teilnehmer noch weitere negative Erfahrungen bezüglich Security-Mängel im Internet gemacht hätten, so wurden sie gebeten diese bekannt zu geben indem die entsprechenden Antwortmöglichkeiten anzuwählen waren. Auch bei dieser Frage waren wieder Mehrfachnennungen möglich. Die Antworten sind in Tabelle 25 dargestellt.

Antwortmöglichkeiten	Anzahl der Nennungen	Prozentsatz
Probleme mit nicht vertrauenswürdigen Zertifikaten	40	25%
Rechner bzw. Dienste wurden gehackt	15	9%
Benutzerkonten und/oder Passwörter wurden gehackt	29	18%
Viren oder Trojaner auf einem Gerät	71	44%
Vortäuschen einer falschen Identität	31	19%
Entlocken von Daten mittels gefälschten E-Mails oder Webseiten (Phishing)	63	39%
Andere Art von negativer Erfahrung	17	10%
Keine Nennung	37	23%

Tabelle 25: Negative Erfahrungen der befragten Personen zu anderen Security-Mängel im Internet (Mehrfachnennungen möglich)

Es zeigt sich, dass sicherheitstechnische Bedenken beim Umgang mit Online-Diensten durchaus angebracht sind. Dies wird vor allem dadurch deutlich, dass

von den insgesamt 163 befragten Personen 40 bereits Probleme mit nicht vertrauenswürdigen Zertifikaten hatten, was einen Schnitt von rund 25% ausmacht. Erwartungsgemäß liegt der Anteil der Negativerfahrungen mit Viren oder Trojanern sogar noch weitaus höher und ist mit rund 44% angegeben worden. Des Weiteren wurde bei rund 39% der Befragten versucht Daten mittels gefälschten E-Mails oder Webseiten zu entlocken. Es ist anzumerken, dass lediglich 37 Personen keine Nennung bei dieser Frage getätigt haben, was einem Prozentsatz von 23% ausmacht.

3.2.5 Gewonnene Erkenntnisse

Durch die Verbreitung von mobilen und ubiquitären Geräten, hat sich auch das Verhalten der User geändert. Während früher der Internetzugriff auf das eigene Heim, den Arbeitsplatz oder sogenannte Internetcafés beschränkt war, kann man sich heute nahezu überall ins WWW einwählen. Es wurde im Zuge der Umfrage eruiert, dass 74% der befragten Personen öffentliche Internetzugänge nutzen und dabei persönliche Daten mit der Cloud austauschen. Lediglich bei der Übertragung von Bankdaten sind die Befragten vorsichtiger. Anzumerken ist hierbei, dass gemäß der statistischen Auswertung zwar ein Zusammenhang zwischen dem Beruf in der IT und der Nutzung von Cloud-Diensten, aber keiner zur Inanspruchnahme von öffentlichen WLAN-Zugängen besteht. Es ist daher anzunehmen, dass Menschen mit IT Hintergrund genauso öffentliche Internetzugänge verwenden wie andere. 21% der Befragten geben an, dass sie eine Internetseite auch dann anwählen würden, wenn im Browser ein Hinweis erscheint, dass die Verbindung nicht sicher ist. Auch kann gemäß der Umfragedaten nicht angenommen werden, dass Personen, welche auf die Symbole und Warnungen im Webbrowser achten, diese auch berücksichtigen. Wie bereits im praktischen Versuch beschrieben, können in solch einem Fall sogenannte MITM Angriffe nicht ausgeschlossen werden. Lediglich 2% geben an, dass sie im Falle eines Warnhinweises die Seite niemals aufrufen. Stellt man die Nutzung unsicherer Verbindungen bei

Warnhinweisen in Browser und die berufliche Tätigkeit in Relation, so erkennt man, dass Menschen, welche in der IT Branche tätig sind, eher auf die möglichen Gefahren sensibilisiert sind. Doch ist der Prozentsatz von jenen IT Mitarbeiterinnen und Mitarbeiter, welche immer eine potentiell gefährliche Webseite aufrufen, bzw. auch von jenen welche eine solche Seite aufrufen sobald sie diese unbedingt nutzen wollen, sehr hoch.

Wird wie im technischen Teil beschrieben, ein Zertifikat des Angreifers installiert, so würde kein entsprechender Warnhinweis erscheinen. Auf die Frage nach der Installation solcher Zertifikate wurde angegeben, dass 60% diese nur installieren wenn sie der ausstellenden Instanz vertrauen, aber auch 25% dieses installieren, wenn sie die Webseite oder die App nutzen wollten. Positiv anzumerken ist, dass die Befragung ergeben hat, dass wenn Menschen Kenntnis vom Zertifikat und dessen Nutzen haben, sie diese auch nicht leichtfertig installieren. Risiken sehen die Befragten bei der Verwendung von Proxys wie beispielsweise bei Virenscannern großteils nicht. Doch hat sich auch hier gezeigt, dass diejenigen welche die Studie oder zumindest das Ergebnis der Studie zur Untersuchung der Proxy-Programme kannten, diese auch eher kritischer betrachteten. Die Wichtigkeit des Themas wurde nochmals durch die statistische Erhebung der negativen Erfahrungen der einzelnen Umfrageteilnehmerinnen und -teilnehmer bestätigt.

3.3 Future Work

Mittels des verwendeten Programms „mitmproxy“ lassen sich HTTPS Verbindungen hervorragend kompromittieren und werden somit für Dritte einsichtig. Andere, mitunter auch TLS basierende Protokolle, wie beispielsweise FTPS oder SMTPS könnten im Zuge weiterführender Arbeiten ebenfalls auf mögliche Attacken untersucht werden. Da die Verschlüsselung dieser Protokolle auf dem TLS Protokoll basiert, ist anzunehmen, dass sich ein ähnliches Bild wie im

beschriebenen Versuch darstellt. Da es neben dem TLS Protokoll noch weitere, während der Cloud Kommunikation verwendete Protokolle gibt, können in weiterführenden Arbeiten diese ebenfalls auf mögliche Angriffsszenarien hin untersucht werden. Beispielhaft sei hierbei das in diesem Dokument beschriebene SSH Protokoll angeführt.

Der im Zuge dieser Arbeit beschriebene praktische Versuch kann auf andere Betriebssysteme, wie beispielsweise iOS angewandt werden. Die Ergebnisse können mit den Erkenntnissen dieser Arbeit verglichen werden.

Es können in zukünftigen Arbeiten Sicherheitskriterien erarbeitet und definiert werden, mittels welchen sich derartige Angriffe unterbinden lassen und somit eine sichere Kommunikation mit Cloud Services ermöglichen.

Sowohl für Unternehmen und Privatpersonen können Verhaltensrichtlinien, welche zum Schutz vor Cyberangriffen definiert wurden, evaluiert und mit den Ergebnissen dieser Studie verglichen werden. Als Ankerpunkt können hierzu die Publikationen des österreichischen Bundeskanzleramts und jene des deutschen Bundesamts für Sicherheit in der Informationstechnik dienen.

3.4 Diskussion und Schlussfolgerung

3.4.1 Beantwortung der Forschungsfrage

Zunächst wird auf die Forschungsfrage eingegangen und beantwortet.

Unter welchen Rahmenbedingungen ist die Verwendung von Cloud-Services, im speziellen bei Verwendung des TLS Verschlüsselungsprotokolls, aus technischer und User-Sicht risikobehaftet?

Die Frage teilt sich in einen technischen und einen Anwendungs-Bereich. Der technische Part wurde mittels Recherche und dem praktischen Versuch eruiert, während auf den zweiten Teil mittels der Umfrage eingegangen wurde.

3.4.1.1 Technische Risiken

Aus technischer Sicht ist vor allem das im Internet umgesetzte Konzept des Schlüsselmanagements problematisch, da es in der Praxis immer wieder vorkommt, dass Zertifikate ausgestellt werden, welche nicht oder nur unzureichend überprüft wurden (siehe Kapitel 2.5.1.1). Weiters sind viele Anwendungen wie beispielsweise Virenscanner anfällig auf gefälschte Zertifikate wie eine Studie [59] ergeben hat. Im praktischen Versuch konnte gezeigt werden, dass die Sicherheit des TLS Protokolls mit der Installation eines eigenen Zertifikates nicht mehr gegeben ist. Es hat sich weiters herausgestellt, dass es in der Praxis irrelevant ist, ob man sich in einem Netzwerk mittels vermeintlichen Proxy-Schutzes oder direkt auf eine Internetseite verbindet. Wenn es ein Angreifer schafft, sich in dasselbe Netzwerk einzuschleusen, so kann er auch auf die Daten mittels Man-in-the-Middle Angriff zugreifen, sofern die User die Warnhinweise des Browsers ignorieren oder das entsprechende Zertifikat installiert wurde. Dass ein potentieller Angreifer in dasselbe Netzwerk gelangt, ist vor allem bei öffentlichen WLAN Zugängen oftmals keine Herausforderung.

Auch wenn das TLS Protokoll in der aktuellen Version als sicher eingestuft wird, kommt es immer wieder vor, dass aktuelle Implementierungen Fehler aufweisen. Beispielhaft wurde auf die Heartbleed Sicherheitslücke in der OpenSSL Variante eingegangen. Diese war kein Fehler im Protokoll an sich, sondern resultierte aus dessen fehlerhafter Umsetzung. Wichtig ist, dass die Nutzerinnen und Nutzer solcher Technologien sofort nach Bekanntwerden eines Implementierungsfehlers einen entsprechenden Patch einspielen um das Problem zu beheben.

3.4.1.2 Risiken aus User-Sicht

Aus Sicht der User bestehen Sicherheitsbedenken bei der Verwendung öffentlicher Netzwerke, wie aus der Umfrage hervor geht. So verwenden zwar 74% der Befragten öffentliche WLAN Zugänge, allerdings fühlen sich nur rund 50% in solchen Netzen auch sicher. Trotz der Bedenken tauschen 80% der befragten WLAN User auch sensible Daten über dieses Medium aus. Fast ein Viertel aller befragten Teilnehmerinnen und Teilnehmer haben angegeben, dass sie trotz Warnhinweisen dennoch unsichere Verbindungen nutzen würden. Der Anteil an Menschen, welche in der IT Branche arbeiten lag prozentuell wesentlich darunter. Es konnte mit wissenschaftlichen Methoden nachgewiesen werden, dass ein Zusammenhang zwischen der beruflichen Tätigkeit und der Sensibilisierung auf einen behutsamen Umgang mit unsicheren Verbindungen besteht. Das Wissen vor unvorsichtigem Hantieren mit Datenverbindungen bzw. Programmen schützen kann, wurde auch in der Fragestellung zu den Proxy-Anwendungen bestätigt. Auch hierbei konnte ein statistischer Zusammenhang festgestellt werden. Ein solcher Zusammenhang ist ebenfalls in der Frage zu den SSL/TLS Zertifikaten erhoben worden. Hierbei haben 70% der Personen, welche über diese Zertifikate Bescheid gewusst haben angegeben, dass sie diese nur installieren würden wenn sie dem Herausgeber des Zertifikates vertrauen würden. Von jenen Teilnehmerinnen und Teilnehmer der Umfrage, welche keine Kenntnis von Zertifikaten gehabt haben waren dies nur 53%. Möglicherweise kommt dies daher, dass 87% der Befragten noch keine negativen Erfahrungen mit Man-in-the-Middle Angriffen bzw. anderen derartigen Angriffsmethoden machen mussten und sich somit noch nicht mit diesem Thema beschäftigt haben. In anderen Bereichen der Cyberkriminalität sind Menschen gemäß der Umfrage vermehrt Angriffen ausgesetzt. So haben bereit 44% Probleme mit Viren oder Trojanern gehabt. Lediglich 23% haben angegeben noch nie mit irgendeiner Art von Angriffen in Berührung gekommen zu sein.

3.4.1.3 Zusammenfassung der Beantwortung der Forschungsfrage

Zusammenfassend kann gesagt werden, dass die Verwendung von Cloud-Services, im speziellen bei Verwendung des TLS Verschlüsselungsprotokolls aus technischer Sicht vor allem in der aktuellen Handhabung des Schlüsselmanagements und in einigen fehlerhaften Implementierungen liegt, sofern die Empfehlungen der Behörden in Bezug auf Schlüssellängen und kryptographische Verfahren berücksichtigt werden. Aus User-Sicht ist die Verwendung von Cloud-Services unter Einsatz von TLS vor allem durch die mangelnde Kenntnis der eingesetzten Technologien risikobehaftet. So ignorieren viele die Sicherheitswarnungen, bzw. können ohne entsprechende Kenntnis nicht richtig darauf reagieren. Auch werden Zertifikate installiert ohne zu wissen, was diese eigentlich bewirken.

3.4.2 Empfehlungen für die Praxis

Für die Praxis bedeuten die Ergebnisse dieser Arbeit, dass nach Bekanntwerden einer Sicherheitslücke schnellstmöglich der entsprechende Patch eingespielt werden muss um Sicherheitsmängel zu beseitigen. Doch hat sich im Zuge des praktischen Versuchs und der Umfrage gezeigt, dass ein sehr großes Sicherheitsproblem durch den Faktor Mensch gegeben ist. Oftmals werden bestehende Sicherheitsmechanismen ignoriert um Webseiten aufzurufen oder Programme zu nutzen, womit neue Angriffsmöglichkeiten geschaffen werden. Es hat sich aber auch gezeigt, dass Personen, welche mit dem Nutzen von Zertifikaten und potentiellen Schwachstellen vertraut sind, vorsichtiger in der Nutzung von Online-Diensten sind. Aus diesem Grund sollten die Menschen im beruflichen und privaten Umfeld auf die bestehenden Gefahren sensibilisiert werden, welche im Zuge dieser Arbeit aufgezeigt werden.

Neben diesem Aspekt sollte vor allem in Unternehmen und staatlichen Einrichtungen über die Sicherstellung der Verwendung von ausschließlich

vertrauenswürdigen Zertifikaten Überlegungen angestellt werden. In sensiblen Bereichen kann unter Umständen eine eigene Certification Authority installiert werden um das Problem zu umgehen. Für den Großteil der Infrastruktur stellt dies jedoch keine adäquate Lösung dar.

Literaturverzeichnis

[1] E. Rescorla, „HTTP Over TLS“, *RFC2818*, Mai-2000. [Online]. Verfügbar unter: https://tools.ietf.org/html/rfc2818. [Zugegriffen: 18-Feb-2017].

[2] Bundeskanzleramt, Büro der Informationssicherheitskommission (ISK), „Österreichisches Informationssicherheitshandbuch, Version 4.0.1“. Jän-2016.

[3] P. Mell und T. Grance, „The NIST definition of cloud computing“, *Spec. Publ. 800-145*, 2011.

[4] T. Mather, S. Kumaraswamy, und S. Latif, *Cloud security and privacy: [an enterprise perspective on risks and compliance]*, 1. ed. Sebastopol, Calif.: O'Reilly, 2009.

[5] D. K. Barry, „Network as a Service (NaaS)“, *Service Architecture*, o. J. [Online]. Verfügbar unter: http://www.service-architecture.com/articles/cloud-computing/network_as_a_service_naas.html. [Zugegriffen: 08-März-2017].

[6] Wirtschaftskammer Österreich, „IT Sicherheitshandbuch, Datensicherheit schafft Vorsprung, 6. Auflage“. Feb-2014.

[7] T. Scheible, „Teil 4: Vor- und Nachteile der Cloud“, *Vor- und Nachteile der Cloud*, 2017. [Online]. Verfügbar unter: https://scheible.it/teil-4-artikelserie_vor-und-nachteile-von-cloud-computing/. [Zugegriffen: 06-Mai-2017].

[8] Wirtschaftskammer Österreich, „Datenverkehr mit dem Ausland“, *wko.at*, 20-Okt-2016. [Online]. Verfügbar unter: https://www.wko.at/Content.Node/Service/Wirtschaftsrecht-und-Gewerberecht/Verwaltungs--und-Verfassungsrecht/Datenschutz/Datenverkehr_mit_dem_Ausland.html. [Zugegriffen: 09-März-2017].

[9] S. Hetmank, *Internetrecht*. Wiesbaden: Springer Fachmedien Wiesbaden, 2016.

[10] C. Eckert, *IT-Sicherheit*, Bd. 9. Auflage. Oldenbourg: Oldenbourg Wissenschaftsverlag GmbH; De Gruyter Oldenbourg, 2014.

[11] Bundesamt für Sicherheit in der Informationstechnik - BSI, „IT-Grundschutz - Glossar und Begriffsdefinitionen“, 2013. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html. [Zugegriffen: 13-Feb-2017].

[12] Bundesamt für Sicherheit in der Informationstechnik - BSI, „BSI - IT-Grundschutz - Basis für Informationssicherheit - IT-Grundschutz-Kataloge - 1 IT-Grundschutz - Basis für Informationssicherheit“, *IT-Grundschutz*, o. J. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/allgemein/einstieg/01001.html. [Zugegriffen: 21-Feb-2017].

[13] Siemens AG Österreich, „Portfolio Zutrittskontrolle“. Siemens AG Österreich, Building Technologies, 2017.

[14] M. Bedner und T. Ackermann, „Schutzziele der IT-sicherheit“, *Datenschutz Datensicherheit-DuD*, Bd. 34, Nr. 5, S. 323–328, 2010.

[15] LEXandTAX, „Einführung in das österreichische Datenschutzrecht“, 25-Mai-2001. [Online]. Verfügbar unter: http://www.lexandtax.at/index.php?option=com_content&view=article&id=11776:8&catid=53:4131&Itemid=64. [Zugegriffen: 02-Mai-2017].

[16] o.V., „Datenschutzgesetz (DSG)“, *Rechtsinfo.com*, 2010. [Online]. Verfügbar unter: http://www.rechtsinfo.com/datenschutzgesetz.html. [Zugegriffen: 02-Mai-2017].

[17] A. S. Tanenbaum und D. J. Wetherall, *Computer Networks*, Fifth Edition. Pearson, 2010.

[18] R. Wobst, *Abenteuer Kryptologie: Methoden, Risiken und Nutzen der Datenverschlüsselung*, 3. Auflage. Addison-Wesley, 2001.

[19] Bundesamt für Sicherheit in der Informationstechnik - BSI, „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“, 08-Feb-2017. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile. [Zugegriffen: 30-Apr-2017].

[20] Bundesamt für Sicherheit in der Informationstechnik - BSI, „BSI - M 2 Maßnahmenkatalog Organisation - IT-Grundschutz-Kataloge - M 2.164 Auswahl eines geeigneten kryptographischen Verfahrens“, *IT-Grundschutz*, 2016. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02164.html. [Zugegriffen: 30-Apr-2017].

[21] International Organization for Standardization, „ISO/IEC 9594-8:2017“, *International Organization for Standardization - ISO/IEC 9594-8:2017*, 2017. [Online]. Verfügbar unter: https://www.iso.org/standard/72557.html. [Zugegriffen: 07-Mai-2017].

[22] D. Solo, R. Housley, W. Ford, und W. Polk, „RFC3280; Internet X.509 Public Key Infrastructure“, *Certificate and Certificate Revocation List (CRL) Profile*, Apr-2002. [Online]. Verfügbar unter: https://tools.ietf.org/html/rfc3280. [Zugegriffen: 07-Mai-2017].

[23] Bundesamt für Sicherheit in der Informationstechnik - BSI, „BSI - M 5 Maßnahmenkatalog Kommunikation - IT-Grundschutz-Kataloge - M 5.174 Absicherung der Kommunikation zum Cloud-Zugriff“, *IT-Grundschutz*, 2014. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05174.html. [Zugegriffen: 18-Feb-2017].

[24] T. Dierks und C. Allen, „The TLS Protocol Version 1.0“, *RFC2246*, Jän-1999. [Online]. Verfügbar unter: https://tools.ietf.org/html/rfc2246. [Zugegriffen: 13-Feb-2017].

[25] S. Turner und T. Polk, „Prohibiting Secure Sockets Layer (SSL) Version 2.0“, *RFC6176*, 2011. [Online]. Verfügbar unter: https://tools.ietf.org/html/rfc6176. [Zugegriffen: 10-Mai-2017].

[26] A. Langley, A. Pironti, R. Barnes, und M. Thomson, „Deprecating Secure Sockets Layer Version 3.0“, *RFC7568*, 2015. [Online]. Verfügbar unter: https://tools.ietf.org/html/rfc7568. [Zugegriffen: 10-Mai-2017].

[27] L. Toms, „SSL vs. TLS – Worin bestehen die Unterschiede?“, *GlobalSign Blog*, 21-Juli-2016. [Online]. Verfügbar unter: https://www.globalsign.com/de-de/blog/ssl-vs-tls-unterschiede/. [Zugegriffen: 10-Mai-2017].

[28] Elektronik Kompendium, „HTTPS / HTTP Secure“, *HTTP + SSL/TLS*, o.J. [Online]. Verfügbar unter: http://www.elektronik-kompendium.de/sites/net/1811281.htm. [Zugegriffen: 12-Mai-2017].

[29] D. Beattie, „Die DROWN-Angriff Sicherheitslücke“, 17-März-2016. [Online]. Verfügbar unter: https://www.globalsign.com/de-de/blog/drown-angriff/. [Zugegriffen: 14-Feb-2017].

[30] M. Tuexen, R. Seggelmann, und M. Williams, „Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) Heartbeat Extension“, *RFC6520*, Feb-2012. [Online]. Verfügbar unter: https://tools.ietf.org/html/rfc6520. [Zugegriffen: 14-Feb-2017].

[31] heise Security, „So funktioniert der Heartbleed-Exploit“, *Security*, 04-Okt-2014. [Online]. Verfügbar unter: http://www.heise.de/security/artikel/So-funktioniert-der-Heartbleed-Exploit-2168010.html. [Zugegriffen: 13-Feb-2017].

[32] Netcraft, „Half a million widely trusted websites vulnerable to Heartbleed bug“, Apr-2014. [Online]. Verfügbar unter: https://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html. [Zugegriffen: 13-Feb-2017].

[33] Alexa Internet Inc., „Alexa Top 500 Global Sites“, 2017. [Online]. Verfügbar unter: http://www.alexa.com/topsites. [Zugegriffen: 13-Feb-2017].

[34] The MITRE Corporation, „Common Vulnerabilities and Exposures, CVE-2014-0160“, 2014. [Online]. Verfügbar unter: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-0160. [Zugegriffen: 13-Feb-2017].

[35] o.V., „Heartbleed Bug“, 29-Apr-2014. [Online]. Verfügbar unter: https://heartbleed.com/. [Zugegriffen: 13-Feb-2017].

[36] Bundesamt für Sicherheit in der Informationstechnik - BSI, „Kryptographische Verfahren: Empfehlungen und Schlüssellängen; Teil 2 – Verwendung von Transport Layer Security (TLS)“, Jän-2017. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=4#. [Zugegriffen: 10-Mai-2017].

[37] T. Ylönen, „SSH — Secure Login Connections over the Internet“, *Sixth USENIX Security Symposium*, 10-Jän-2003. [Online]. Verfügbar unter: https://www.usenix.org/legacy/publications/library/proceedings/sec96/full_papers/ylonen/. [Zugegriffen: 10-Mai-2017].

[38] T. Ylönen und C. Lonvick, „The Secure Shell (SSH) Connection Protocol“, *RFC4254*, Jänner-2006. [Online]. Verfügbar unter: https://www.ietf.org/rfc/rfc4254.txt. [Zugegriffen: 11-Mai-2017].

[39] T. Ylönen und C. Lonvick, „The Secure Shell (SSH) Authentication Protocol“, *RFC4252*, Jänner-2006. [Online]. Verfügbar unter: https://www.ietf.org/rfc/rfc4252.txt. [Zugegriffen: 11-Mai-2017].

[40] T. Ylönen und C. Lonvick, „The Secure Shell (SSH) Transport Layer Protocol“, *RFC4253*, Jänner-2006. [Online]. Verfügbar unter: https://www.ietf.org/rfc/rfc4253.txt. [Zugegriffen: 11-Mai-2017].

[41] T. Ylönen und C. Lonvick, „The Secure Shell (SSH) Protocol Architecture“, *RFC4251*, Jänner-2006. [Online]. Verfügbar unter: https://www.ietf.org/rfc/rfc4251.txt. [Zugegriffen: 11-Mai-2017].

[42] T. Dotzauer und T. Lütticke, *Das SSH-Buch; Leitfaden für den sicheren Einsatz von OpenSSH*, Auflage: 1. Nicolaus Millin Verlag, 2006.

[43] Bundesamt für Sicherheit in der Informationstechnik - BSI, „Kryptographische Verfahren: Empfehlungen und Schlüssellängen; Teil 4 – Verwendung von Secure Shell (SSH)“, Jän-2017. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-4.pdf?__blob=publicationFile&v=4. [Zugegriffen: 10-Mai-2017].

[44] P. Eckersley und J. Burns, „Is the SSLiverse a safe place“, in *Chaos Communication Congress*, 2010.

[45] Electronic Frontier Foundation, „The EFF SSL Observatory“, *Electronic Frontier Foundation*, 03-Aug-2010. [Online]. Verfügbar unter: https://www.eff.org/de/observatory. [Zugegriffen: 13-Feb-2017].

[46] C. Palmer, „Unqualified Names in the SSL Observatory“, *Electronic Frontier Foundation*, 05-Apr-2011. [Online]. Verfügbar unter: https://www.eff.org/deeplinks/2011/04/unqualified-names-ssl-observatory. [Zugegriffen: 13-Feb-2017].

[47] J. Ihlenfeld, „SSL-Zertifikate: Unzulängliche Prüfungen durch CAs bringen Nutzer in Gefahr - Golem.de“, 06-Apr-2011. [Online]. Verfügbar unter: https://www.golem.de/1104/82573.html. [Zugegriffen: 13-Feb-2017].

[48] J. Schlyter und P. Hoffman, „The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA“, *RFC6698*, Aug-2012. [Online]. Verfügbar unter: https://tools.ietf.org/html/rfc6698. [Zugegriffen: 13-Feb-2017].

[49] H. Böck, „SSL/TLS: Problematisches Nachladen von Zertifizierungsstellen“, 29-Juli-2013. [Online]. Verfügbar unter: https://www.golem.de/news/ssl-tls-problematisches-nachladen-von-zertifizierungsstellen-1307-100667.html. [Zugegriffen: 13-Feb-2017].

[50] Microsoft Corp., „Konfigurieren vertrauenswürdiger Stämme und unzulässiger Zertifikate“, o. J. [Online]. Verfügbar unter: https://msdn.microsoft.com/de-de/library/dn265983(v=ws.11).aspx. [Zugegriffen: 13-Feb-2017].

[51] J. Schmidt und M. Borrmann, „Zweifelhafte Updates gefährden SSL-Verschlüsselung“, *c't*, 27-Juli-2013. [Online]. Verfügbar unter: https://www.heise.de/ct/ausgabe/2013-17-Zweifelhafte-Updates-gefaehrden-SSL-Verschluesselung-2317589.html. [Zugegriffen: 13-Feb-2017].

[52] D. Fox, „TLS, das Vertrauen und die NSA“, *Datenschutz Datensicherheit-DuD*, Nr. 2, S. 78–84, 2015.

[53] M. Repges, „Kryptographische Angriffe“, *SSL Angriffe*, o. J. [Online]. Verfügbar unter: http://www.repges.net/SSL/Angriffe_SSL/Kryptographische_Angriffe_SSL/kryptographische_angriffe_ssl.html. [Zugegriffen: 02-Mai-2017].

[54] Bundesamt für Sicherheit in der Informationstechnik - BSI, „G5.112 Manipulation von ARP-Tabellen“, *IT-Grundschutz-Kataloge*, 2006. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05112.html. [Zugegriffen: 12-Mai-2017].

[55] M. Repges, „Internetspezifische Angriffe“, *SSL Angriffe*, o. J. [Online]. Verfügbar unter: http://www.repges.net/SSL/Angriffe_SSL/Internetspezifische_Angriffe_S/internetspezifische_angriffe_s.html. [Zugegriffen: 02-Mai-2017].

[56] The mitmproxy project, „mitmproxy — mitmproxy 3.0.0.dev documentation“, *mitmproxy*, 2016. [Online]. Verfügbar unter: http://docs.mitmproxy.org/en/latest/mitmproxy.html. [Zugegriffen: 07-März-2017].

[57] The mitmproxy project, „How mitmproxy works — mitmproxy 3.0.0 documentation“, *How mitmproxy works*, 2016. [Online]. Verfügbar unter: http://docs.mitmproxy.org/en/latest/howmitmproxy.html. [Zugegriffen: 18-Apr-2017].

[58] The mitmproxy project, „Modes of Operation — mitmproxy 3.0.0 documentation“, *Modes of Operation*, 2016. [Online]. Verfügbar unter: http://docs.mitmproxy.org/en/latest/modes.html. [Zugegriffen: 18-Apr-2017].

[59] X. de C. de Carnavalet und M. Mannan, „Killed by Proxy: Analyzing Client-end TLS Interception Software“, in *Network and Distributed System Security Symposium (NDSS 2016), San Diego, CA, USA*, 2016.

Abbildungsverzeichnis

Tabellenverzeichnis

Codeverzeichnis

Abkürzungsverzeichnis

ARP	Address Resolution Protocol
BSI	Bundesamt für Informationssicherheit (Deutschland)
CA	Certification Authority (Zertifizierungsstelle)
CRL	Certificate Revocation List
DANE	DNS-Based Authentication of Named Entities
DLIES	Discrete Logarithm Integrated Encryption Scheme
DNSSEC	Domain Name System Security Extensions
DoS	Denial of Service
ECIES	Elliptic Curve Integrated Encryption Scheme
EFF	Electronic Frontier Foundation
FQDN	Fully-Qualified Domain Names
FTP	File Transfer Protocol
FTPS	FTP over TLS
IaaS	Infrastructure as a Service
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ISP	Internet-Serviceprovider
IT	Informationstechnik
ITU	International Telecommunication Union (Internationale Fernmeldeunion)

MAC	Message Authentication Code
MITM	Man-In-The-Middle
NIST	National Institute of Standards and Technology (USA)
PaaS	Platform as a Service
PKI	Public Key Infrastructure
RA	Registration Authorities
RFC	Request for Comments
RFID	Radio-Frequency Identification
RSA	Rivest, Shamir und Adleman (asymmetrisches Kryptoverfahren)
SaaS	Software as a Service
SAN	Subject Alternative Name
SFTP	SSH File Transfer Protocol
SLA	Service Level Agreement
SMTPS	Simple Mail Transfer Protocol Secure
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator
WLAN	Wireless Local Area Network

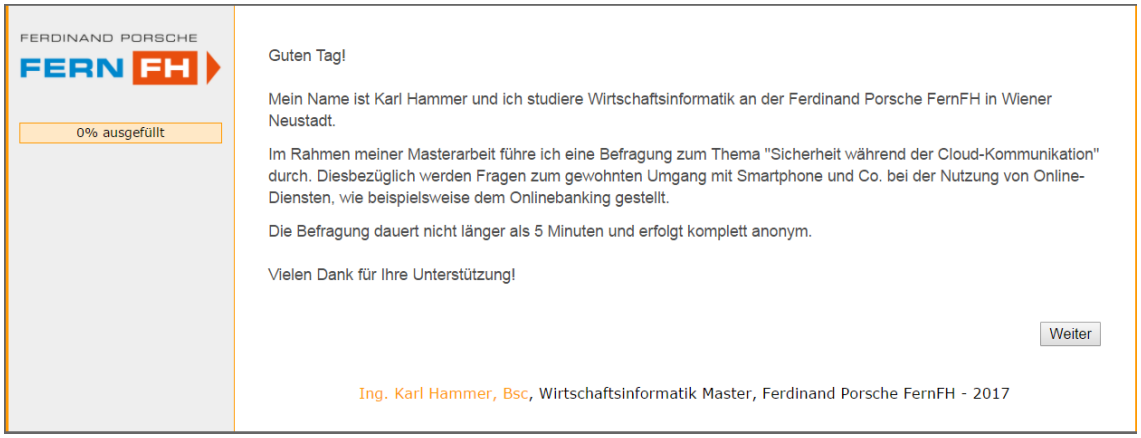
Anhang A: Beispiel eines OpenSSL Zertifikates

```
Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number:
         81:bf:d1:36:35:7f:1e:bc
   Signature Algorithm: sha256WithRSAEncryption
      Issuer: C = AT, ST = Vienna, L = Vienna, O = Hammer, OU = Karl, CN =
HammerKarl, emailAddress = karl.hammer@mail.fernfh.ac.at
      Validity
         Not Before: May  7 14:47:16 2017 GMT
         Not After : May  1 14:47:16 2042 GMT
      Subject: C = AT, ST = Vienna, L = Vienna, O = Hammer, OU = Karl, CN =
HammerKarl, emailAddress = karl.hammer@mail.fernfh.ac.at
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
               00:d4:df:f5:ae:a6:3b:0a:b4:05:9c:83:57:6d:5c:
               a9:44:95:ed:65:d6:c9:fe:0b:a9:12:db:3d:52:fc:
               2a:ca:b3:d4:17:a7:61:6f:49:28:59:60:c0:cf:df:
               9c:89:da:85:2a:38:c0:a1:14:60:f5:93:32:f9:59:
               01:30:4b:6a:82:5b:e4:2d:d8:80:b9:b2:12:f6:97:
               eb:44:bc:bd:bc:a9:a2:b2:6d:99:93:e2:6a:3e:73:
               a8:ff:ad:44:a4:35:e2:bf:80:40:68:9a:dc:87:df:
               05:93:19:b3:e8:33:fa:ce:bb:f7:92:f4:09:57:89:
               e9:9a:82:e3:88:7a:4e:50:2b:70:1c:b8:0c:c2:87:
               47:c5:ac:97:2d:6b:76:85:fd:d7:6a:db:da:15:f3:
               67:fc:22:a0:9c:35:94:88:cc:2f:a9:70:98:a5:38:
               46:9d:2f:a1:ec:8a:ae:62:d3:3d:8b:59:b9:e2:41:
               c1:aa:42:b4:09:50:17:27:fc:f3:50:ff:b2:8e:88:
               5a:a7:9f:8b:f3:52:b1:86:f8:0b:df:d4:f8:f7:35:
               87:72:83:ae:a6:b4:92:21:f1:63:72:dc:ff:37:7d:
               f4:00:55:64:86:68:a8:0e:02:3d:42:bb:ed:31:39:
               46:3b:bc:55:05:1b:e7:a1:d4:b5:34:64:13:50:60:
               88:61
            Exponent: 65537 (0x10001)
      X509v3 extensions:
         X509v3 Subject Key Identifier:
            0C:4C:76:4A:0D:43:08:6B:B6:DF:D2:DD:78:11:15:E4:0E:17:D7:06
         X509v3 Authority Key Identifier:
            keyid:0C:4C:76:4A:0D:43:08:6B:B6:DF:D2:DD:78:11:15:E4:0E:17:D7:06
```

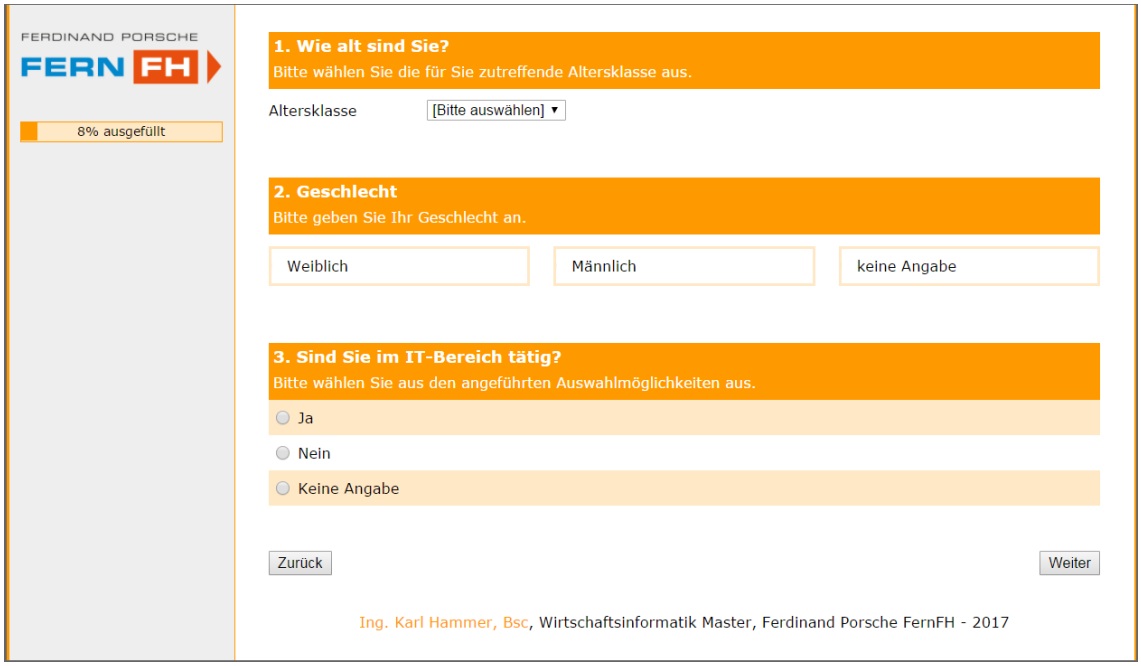
```
        X509v3 Basic Constraints: critical
            CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
        36:92:b4:b3:55:f7:6e:e0:70:7c:b1:96:50:7a:90:f6:c7:a8:
        c1:9f:b0:74:cc:7f:fb:65:4f:e3:91:43:21:a0:bf:92:5e:5e:
        dd:6e:1d:67:bd:19:1b:44:de:da:76:ed:c7:d7:32:28:7b:00:
        50:b4:49:0f:fb:7e:04:ed:d3:a2:e9:c2:55:56:4d:92:cf:9b:
        6b:66:c2:dc:4c:b0:93:42:3d:9e:77:a0:bc:66:32:63:5a:ce:
        db:4a:f4:4c:06:15:2b:eb:5b:c3:19:da:33:46:a2:68:01:57:
        f6:81:20:97:33:6b:54:d7:cb:21:77:75:48:b5:c9:b9:90:15:
        d8:48:a6:59:f7:88:1f:3c:ae:98:83:6b:03:1d:1b:9f:71:87:
        85:06:f7:ac:ec:77:f1:c1:8b:00:2e:a2:93:ee:05:a7:3e:ca:
        8c:0b:35:5e:a3:5c:e4:cc:18:59:b6:de:4b:e9:8e:b5:1d:77:
        59:c7:3e:9c:08:b4:7c:2b:ca:6b:22:a0:cb:80:82:ee:eb:32:
        f1:dc:1a:05:75:cd:8b:b1:48:c4:e6:5e:f3:a7:f1:76:fb:0f:
        ef:05:38:67:4d:0c:74:d8:d1:1c:9e:ae:eb:49:ec:93:94:b8:
        e6:4c:e7:26:c3:e0:a0:6c:bd:bd:20:7c:0e:90:81:30:70:34:
        67:02:19:19
```

Anhang B: Fragebogen der Onlineumfrage

B1: Begrüßung und Einleitung

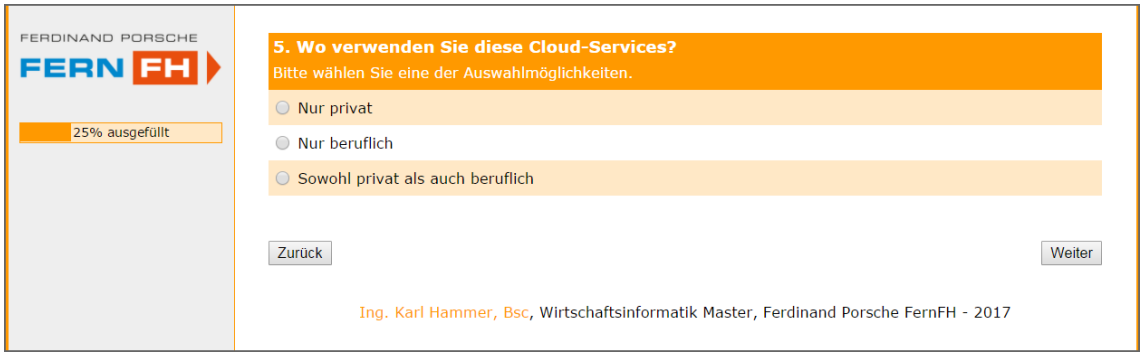


B2: Evaluierung der persönlichen Daten (Fragen 1 - 3)

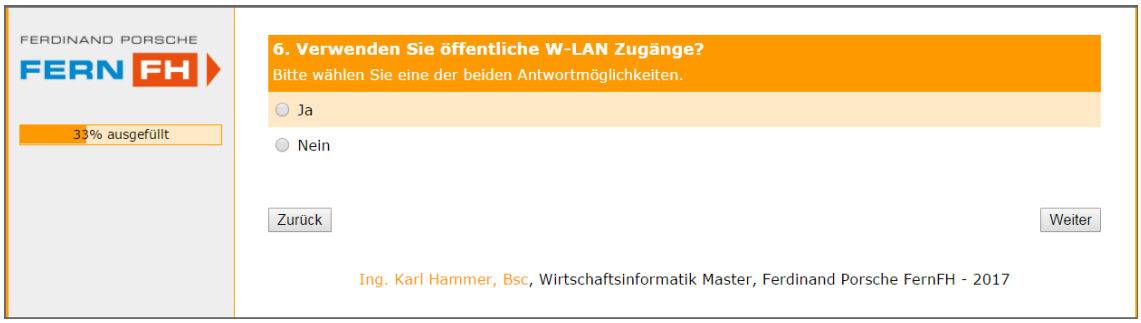


B3.1: Einstellung der Befragten in Bezug auf Cloud-Services (Frage 4)

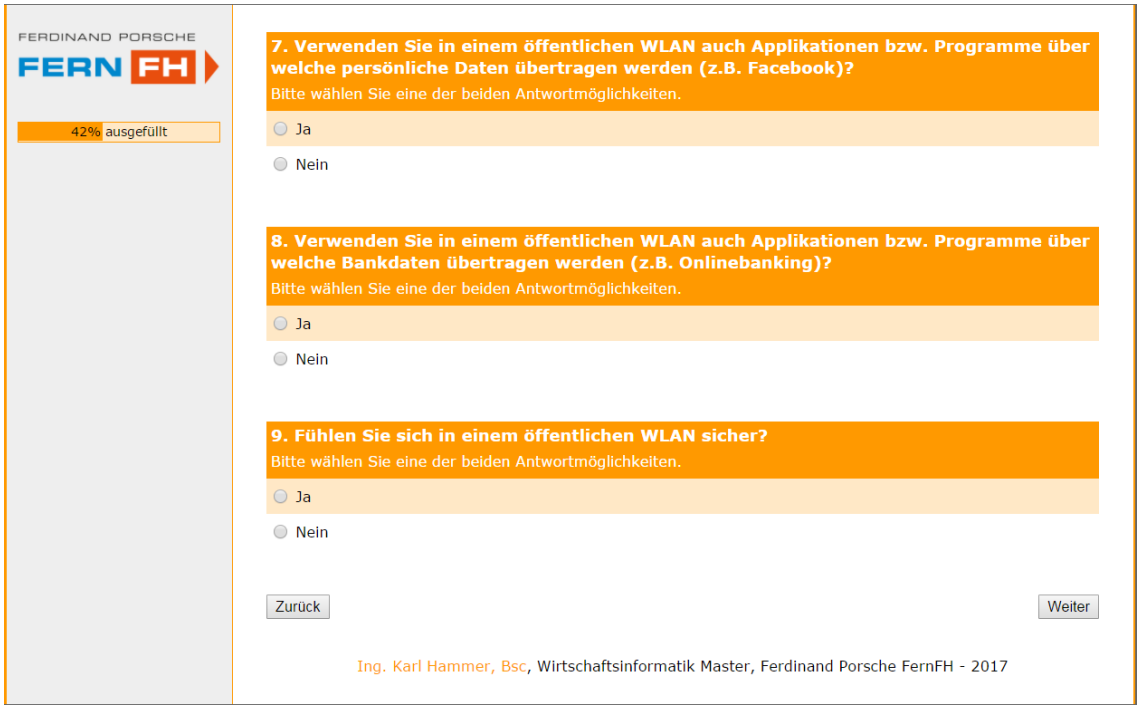
B3.2: Einstellung der Befragten in Bezug auf Cloud-Services (Frage 5)



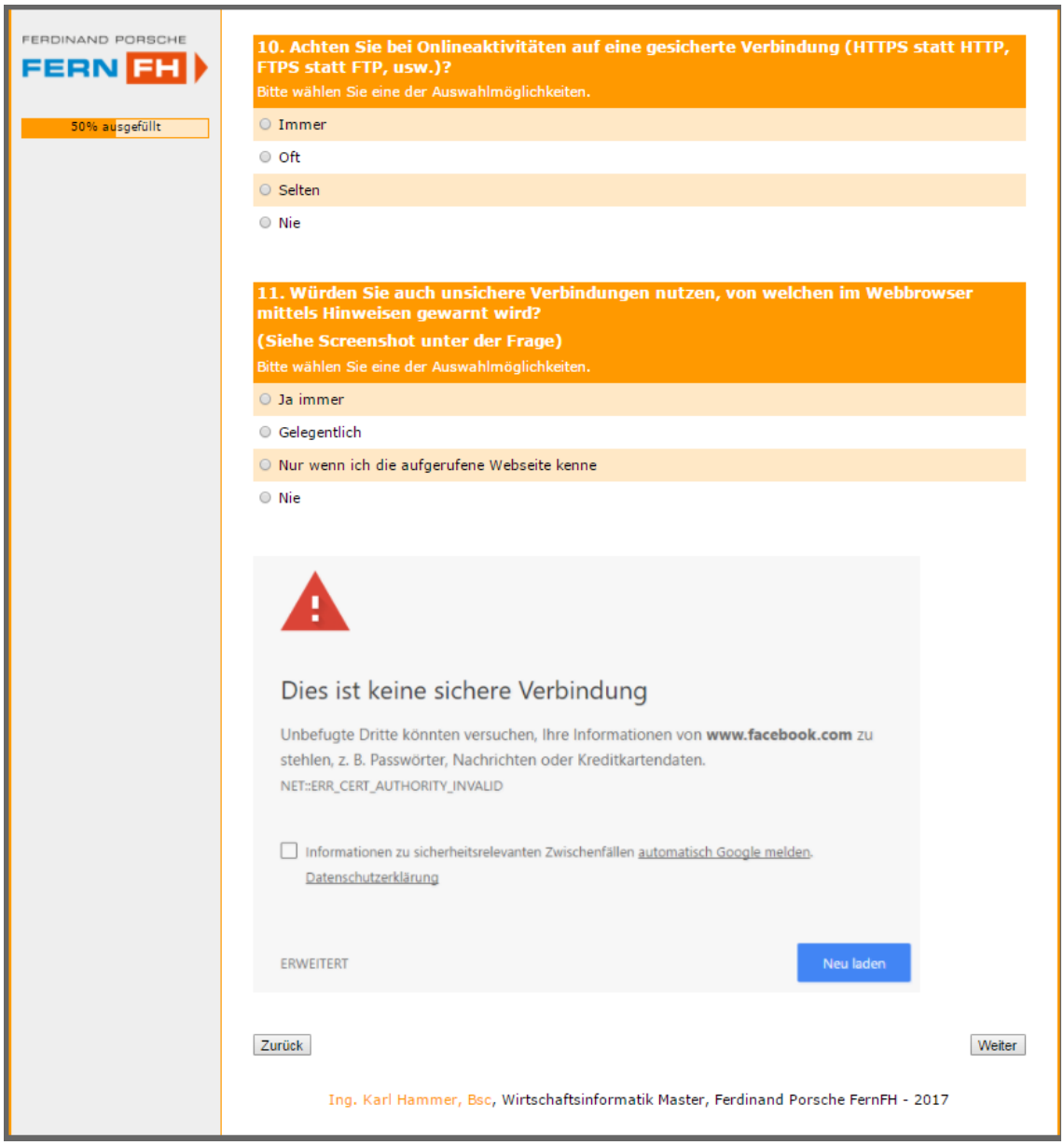
B4.1: Verwendung von öffentlichen WLAN Zugängen (Frage 6)



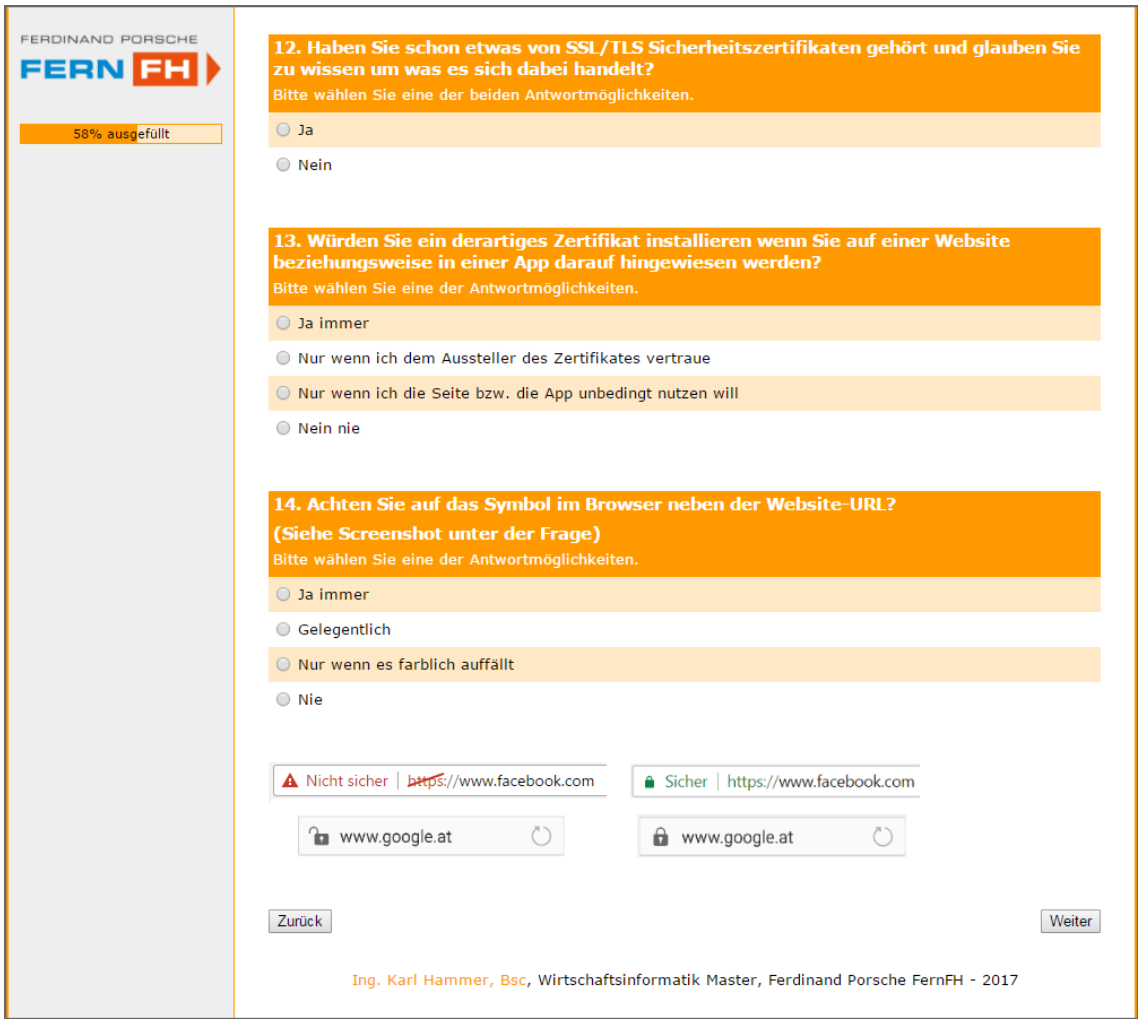
B4.2: Verwendung von öffentlichen WLAN Zugängen (Fragen 7 - 9)



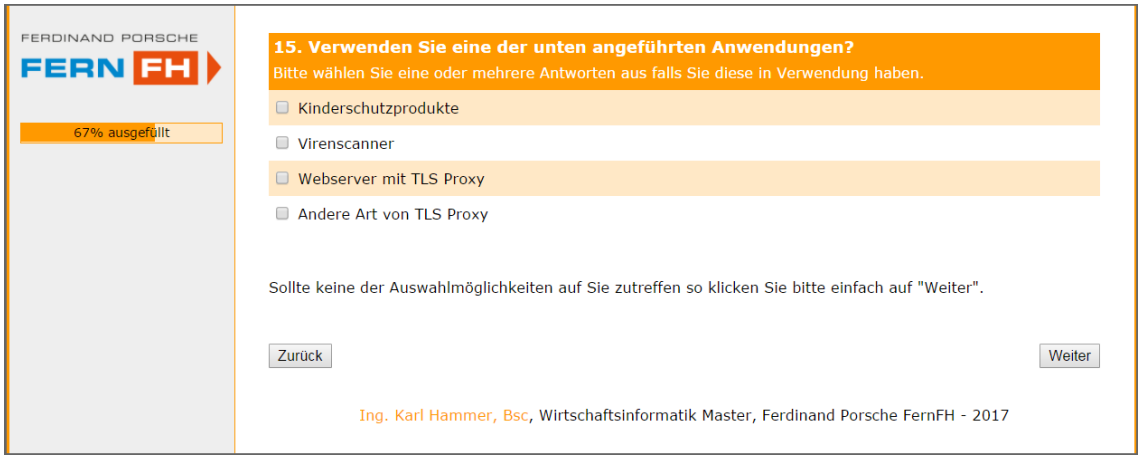
B5.1: Sicherheitsaspekte während der Cloud-Kommunikation (Fragen 10 und 11)



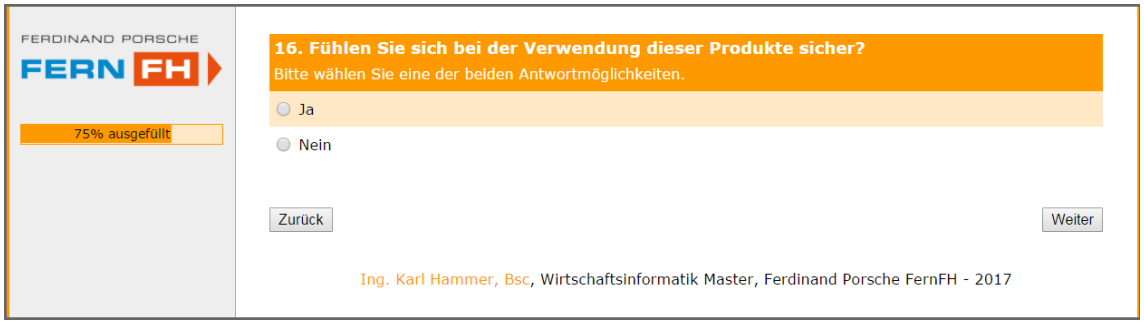
B5.2: Sicherheitsaspekte während der Cloud-Kommunikation (Fragen 12 - 14)



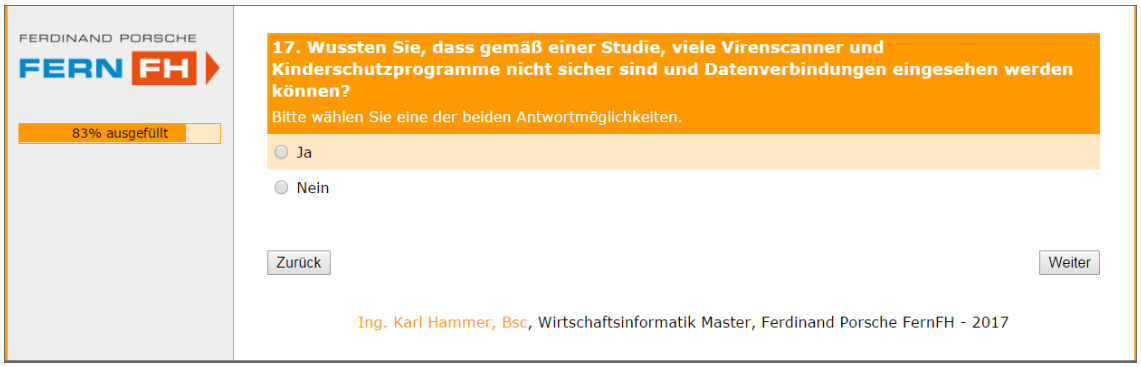
B6.1: Verwendung von Proxys (Frage 15)



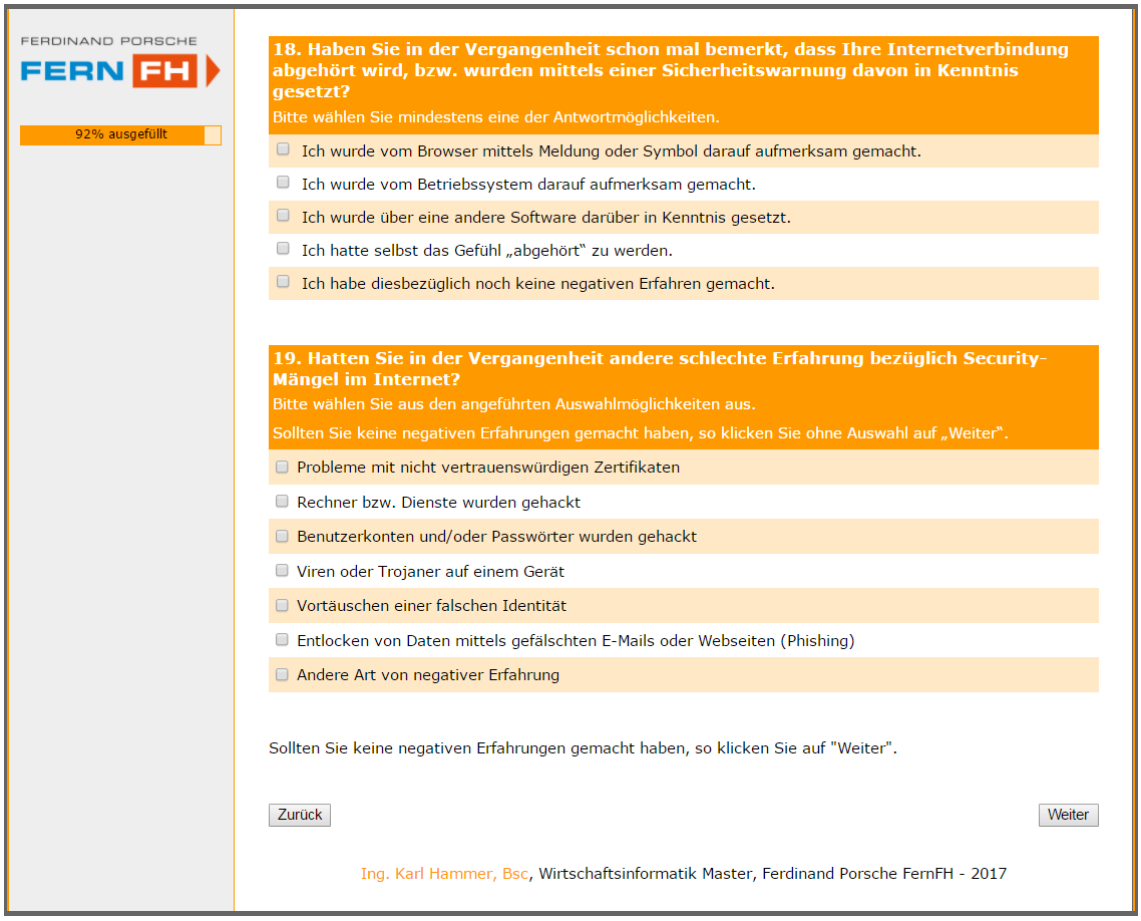
B6.2: Verwendung von Proxys (Frage 16)



B6.3: Verwendung von Proxys (Frage 17)



B7: Negative Erfahrungen der Umfrageteilnehmer in Bezug auf Onlinesicherheit (Fragen 18 und 19)



B8: Abschluss der Befragung