Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Bachelorarbeit

Stefanie Langer

Sicherheit von passwortbasierten Authentifizierungssystemen

Fakultät Technik und Informatik
Studiendepartment Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Stefanie Langer

Sicherheit von passwortbasierten Authentifizierungssystemen

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung

im Studiengang Bachelor of Science Angewandte Informatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr.-Ing. Martin Hübner
Zweitgutachter: Prof. Dr. Bettina Buth

Eingereicht am: 26. Juni 2013

Stefanie Langer

Thema der Arbeit
Sicherheit von passwortbasierten Authentifizierungssystemen

Stichworte
IT-Sicherheit, Passwortsicherheit, Single Sign-On (SSO), Authentifikation, Kerberos

Kurzzusammenfassung
Diese Arbeit hat die Untersuchung zweier Thesen zum Ziel. Es soll beleuchtet werden, ob regelmäßige/erzwungene Passwortwechsel zum einen und die Verwendung von Single Sign-On-Systemen zum anderen die Sicherheit erhöhen. Es werden zunächst Grundlagen zur Begrifflichkeit von Sicherheit sowie psychologische Grundlagen erläutert. Nachfolgend werden Konstruktion, Verwendung und Sicherheitsrisiken von Passworten erläutert, um anschliessend die erste These zu untersuchen. Im Anschluss werden passwortbasierte Authentifikationssysteme am Beispiel von Single-Sign On und unter der Verwendung von Kerberos definiert, beschrieben und deren Sicherheitsrisiken erläutert, um die zweite These zu prüfen.

Stefanie Langer

Title of the paper
Security of password-based authentification systems

Keywords
IT-security, password security, single sign-on (SSO), authentification, Kerberos

Abstract
This document targets on the investigation of two theses. It should be shown if periodical/forced password change on one hand, and the use of single sign-on systems on the other hand increases security. At first, the basics concepts of security and psychological basics were explained. Subsequently, construction, use and safety risks of passwords are explained in order to examine the first thesis. Afterwards, password-based authentication systems using the example of single sign-on and Kerberos are defined, described and their security risks were explained, followed by the examination of the second thesis.

Inhaltsverzeichnis

1. Einleitung

Heutzutage dominiert die elektronische Datenverarbeitung die Mehrheit der Arbeitsplätze. Daten, die noch vor einigen Jahrzehnten ganze Räume mit Aktenschränken füllten werden nun digital vorgehalten. Mit dieser Menge an Daten geht eine große Verantwortung einher - um den Zugriff zu regulieren und die Daten vor unberechtigtem Zugriff zu schützen findet nahezu an jedem beruflich genutzten Computer eine Authentifizierung des Benutzers mit einem Passwort statt. In einer Welt, in der das Internet auf mobilen und stationären Geräten allgegenwärtig ist, beschränkt sich die Nutzung von passwortbasierten Authentifikationssystemen nicht mehr nur auf den beruflichen Gebrauch. Soziale Netzwerke, Online-Banking, die Nutzung von Foren, E-Commerce-[1] oder auch E-Learning Plattformen erfordern stets eine Registrierung mit Benutzernamen und Passwort.

Die Sicherheit der Daten hängt bei einer passwortbasierten Authentifikation maßgeblich von der Qualität des Passworts ab. Hier trifft der Anwender die Entscheidung wie es lauten soll, abhängig von einer eventuellen Vorbildung oder Vorschrift durch das authentifizierende System. Gerade im beruflichen Umfeld hat der Benutzer Zugriff auf verschiedenste, individuell geschützte Anwendungen und Programme. Meist handelt es sich um eine Windows-Umgebung, die nach dem Einloggen weitere Programme zur individuellen Nutzung zur Verfügung stellt. Hier hat sich inzwischen die Nutzung von sogenannten Single Sign-On-Verfahren durchgesetzt die dem Benutzer erlauben, bereits nach einer initialen Authentifizierung Zugriff auf alle zu Verfügung gestellten Programme zu haben.

1.1. Motivation und Ziel

Obwohl passwortbasierte Authentifizierungen allgegenwärtig sind scheint dem durchschnittlichen Nutzer das damit verbundene Risiko, wichtige Daten durch mangelhaften Schutz offenzulegen, nicht bewusst zu sein.

Im Gegenzug zur Standard-Authentifizierung, bei der für jede Benutzung eines Systems oder Programms die Eingabe von Benutzernamen und Passwort notwendig ist sollen Single

[1] z.B. Online-Versandhäuser wie Amazon.de, Zalando.de oder Otto.de

Sign-On-Systeme die Arbeit erleichtern, indem der Workflow nicht durch wiederkehrende Authentifizierungen und den dadurch zu merkenden, verschiedenen Passworten unterbrochen wird. Doch gilt es zu klären, ob durch diese Erleichterung auch noch die notwendige Sicherheit gewährleistet werden kann - gerade dann, wenn der Anwender sein Passwort mangelhaft auswählt.

Diese Arbeit ist in zwei Schwerpunkte unterteilt: zunächst werde ich prüfen, welche Maßnahmen zur Verbesserung der Passwortsicherheit bereits existieren und deren Sinnhaftigkeit bewerten. Hierbei soll auch der psychologische Hintergrund des Benutzers betrachtet werden um zu ergründen, warum Menschen sich auf eine bestimmte Art und Weise verhalten und hierdurch zum vielbeschriebenen „Risikofaktor Mensch“ werden. Im Anschluss an die Untersuchung der Passwortsicherheit soll folgende These überprüft werden:

> Erhöhen vorgeschriebene Passwortwechsel innerhalb fester Zeiträume (z.B. monatlich, dreimonatlich) die Passwortsicherheit?

Den zweiten Schwerpunkt bildet die Untersuchung von passwortbasierten Authentifikationssystemen. Besonderes Augenmerk liegt hier auf Authentifikationssystemen, die nach dem Single Sign-On Verfahren operieren. Diese werden kategorisiert und hinsichtlich ihrer Sicherheit untersucht, um im Anschluss die zweite Kernthese zu untersuchen:

> Erhöhen Single Sign-On-Systeme die Sicherheit?

Abschließend wird der Zusammenhang beider Thesen hergestellt und überprüft, ob die Verifizierung respektive Falsifizierung der Thesen auch in einem gemeinsamen Kontext gilt: Inwieweit ist die Sicherheit von Single Sign-On-Systeme davon abhängig, ob ein Passwort in regelmäßigen Abständen zu verändern ist?

1.2. Gliederung der Arbeit

Diese Arbeit gliedert sich in 6 Kapitel auf. Kapitel 2 klärt zunächst die grundlegenden Begrifflichkeiten Sicherheit und IT-Sicherheit, wonach Kapitel 3 einen Einblick in die psychologischen Grundlagen liefert und die menschliche Handlungsweise beleuchten soll.

Im Anschluss wird in Kapitel 4 der Begriff des Passwortes sowie der verschiedenen Arten von Passworten definiert sowie erläutert, welche Sicherheitsrisiken durch menschliche Einflussnahme bestehen. Verschiedene Gegenmaßnahmen und die Untersuchung der ersten Kernthese schließen das Kapitel ab.

Nach einer Erläuterung von passwortbasierten Authentifikationssystemen im Allgemeinen und Single Sign-On-Systemen sowie deren Technologie am Beispiel von Kerberos wird die zweite Kernthese untersucht.

Den Abschluss bildet der Schluss (Kapitel 6), der eine Zusammenfassung der Arbeit geben soll. Es folgt das Fazit dieser Arbeit sowie ein Ausblick auf aktuelle und zukünftige Entwicklungen.

2. Grundlagen

Sicherheit ist ein kontextsensitiver Begriff und hat nicht nur für jeden Menschen, sondern auch in Bezug auf z.B. die Informationstechnologie (IT)[1] unterschiedliche Ausprägungen und Bedeutungen. Dieses Kapitel will Begriffe abgrenzen und definieren sowie einen Überblick über diejenigen verschaffenen, die für diese Arbeit von grundlegener Relevanz sind.

2.1. Definition Sicherheit im Allgemeinen

Sicherheit bezeichnet einen Zustand des Sicherseins, Geschütztseins vor Gefahr oder Schaden bzw. das höchstmögliche Freisein von Gefährdungen[2]. Auf der Suche nach einer Definition kommen jedoch einige Aspekte zum Tragen, die eine Unterscheidung des Sicherheitsbegriffes erfordern. [Bun02] nimmt in seinem Artikel z. B. eine Unterteilung in vier Kategorien vor:

- Sicherheit bedeutet Gewissheit, Verlässlichkeit, Vermeiden von Risiken, aber auch Abwesenheit von bzw. Schutz vor Gefahren werden mit diesem Begriff assoziiert.
- Sicherheit meint aber auch Statussicherheit, Gewährleistung des erreichten Lebensniveaus und der Lebensumstände einzelner Menschen und/oder sozialer Gruppen sowie Bewahrung der gesellschaftlichen und politischen Verhältnisse, in denen Menschen leben und sich eingereichtet haben.
- Mit dem Begriff ist weiterhin ein bestimmtes institutionelles Arrangement assoziiert, das als geeignet erscheint, innere und äußere Bedrohungen einer sozialen und politischen Ordnung abzuwehren.
- Und schließlich wird Sicherheit im juristischen Sinne als Unversehrtheit von Rechtsgütern verstanden, die zu schützen und bei Verletzung wieder herzustellen Aufgabe der Rechtsordnung und des Staates ist.

Sicherheit kann auch die 100-prozentige Wahrscheinlichkeit des Zutreffens einer Aussage oder des (Nicht-)Eintreffens eines Ereignisses beschreiben (nach [BSHL12]).

[1] ebenso üblich ist die Bezeichnung Informations- und Kommunikationstechnologie (IKT).
[2] `http://www.duden.de/rechtschreibung/Sicherheit#Bedeutung1`

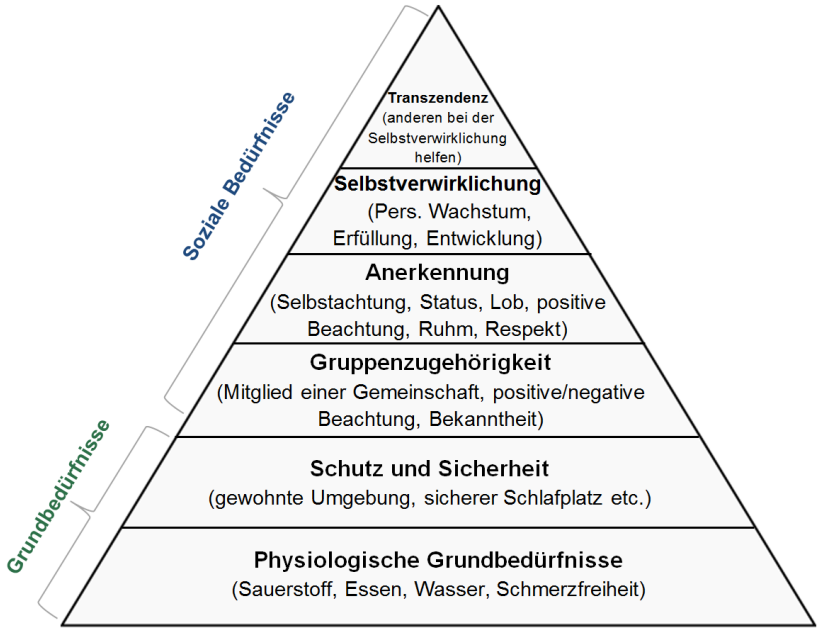

Abbildung 2.1.: Die Maslowsche Bedürfnispyramide frei nach A. H. Maslow

Abraham H. Maslow als wichtiger Vertreter der humanistischen Psychologie hat die grundlegenden menschlichen Bedürfnisse in seiner Pyramidendarstellung (siehe Abbildung 2.1 und vgl. [Ehl08]) hierarchisch angeordnet. Direkt nach den wichtigsten, den physiologischen Bedürfnissen wie Essen, Trinken, Schlaf und Schmerzfreiheit ordnet er das Bedürfnis nach Schutz und Sicherheit ein. Der Mensch strebt somit nach der Befriedigung seiner physiologischen Grundbedürfnisse nach Schutz und Sicherheit.

[GK08] unterscheidet zwischen den Risikobereichen Sicherheit und Gefahr, die durch das Grenzrisiko voneinander getrennt sind. Diese werden zwar als Gegensätze empfunden, gehören aber zum selben Maßstab: beides ist ein Schadensrisiko, das vom Grenzrisiko gleichermaßen verbunden und getrennt wird. Weder Gesetzgeber noch Technik können jedoch den Ort des Grenzrisikos effektiv festlegen, da dieser für jeden Einzelfall separat betrachtet und festgelegt werden muss. Auf diese Weise sind Sicherheit und Risiko untrennbar miteinander verbunden - die Erhöhung der Sicherheit kann nur durch Verringerung des Schadenrisikos erfolgen, wobei es keinen Zustand gibt, an dem kein Risiko besteht.

Sicherheit als Grundbedürfnis des Menschen kann es nur dann geben, wenn das Einzelfallabhängige Risiko als gering eingeschätzt wird. Sowohl gesetzliche Vorgaben als auch der Erfahrungsschatz eines Einzelnen hat maßgeblichen Einfluss auf das Empfinden einer Person.

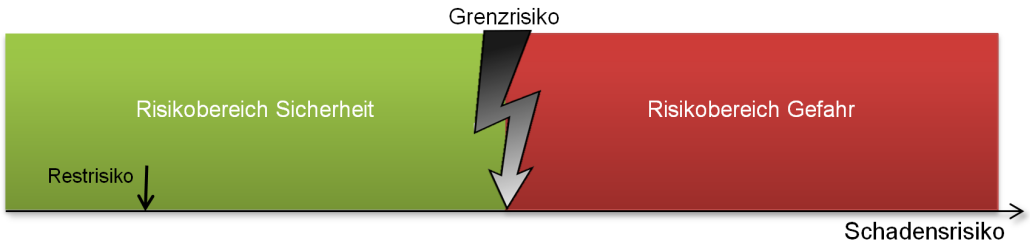

Abbildung 2.2.: Das Schadensrisiko als Maßstab von Sicherheits- und Gefahrenbereich, frei nach [GK08]

Wichtig zu berücksichtigen ist, dass sich die Risikoabschätzung und Sicherheitsempfindung durch verschiedenste Faktoren beeinflussen lässt (siehe auch: Unterkapitel 4.3.1, Social Engineering). Auch wenn ein Mensch bereits über ein eventuell eintretendes Risiko informiert ist findet die Sicherheitseinstufung individuell, und auch unter Berücksichtigung von Heuristiken (siehe auch: Kapitel 3.4, Heuristiken) statt.

Im Kontext dieser Arbeit soll daher von folgender, eigener Definition von Sicherheit ausgegangen werden:

Satz 2.1.1

Der Mensch empfindet Sicherheit genau dann, wenn er sich keines bestehenden Risikos bewusst ist.

2.2. Definition Sicherheit in der Informationstechnologie

> „IT-Sicherheit hat die Aufgabe, Unternehmen und deren Werte (Know-How, Kundendaten, Personaldaten) zu schützen und wirtschaftliche Schäden [...] zu verhindern." Claudia Eckert [Eck12, S. 1]

Die Begriffe IT-Sicherheit und Informationssicherheit werden in der Literatur häufig synonym verwendet, obwohl diese bei genauer Betrachtung unterschiedliche Ziele verfolgen. [Eck12] gibt erstmals einen Gesamtüberblick über die Materie, indem sie den Begriff Sicherheit als Maßstab vorgibt und diesen in vier Bereiche unterteilt (siehe auch Abbildung 2.3):

- **Funktionssicherheit** (engl. safety): Die Übereinstimmung der realisierten Ist-Funktionalität der Komponenten eines Systems mit deren Soll-Funktionalität ohne funktional unzulässige Zustände.
- **Informationssicherheit** (engl. security): die Eigenschaft eines funktionssicheren Systems unautorisierte Informationsveränderung oder -gewinnung zu vermeiden.
- **Datensicherheit** (engl. protection): Die Eigenschaft eines funktionssicheren und informationssicheren Systems, unautorisierte Zugriffe auf Systemressourcen und Daten als auch Informationsverlust (z.B. durch fehlende Backups) zu verhindern.
- **Datenschutz** (engl. privacy): die Fähigkeit einer natürlichen Person, die Erhebung und Verwendung und Weitergabe von deren personenbezogenen Daten zu kontrollieren (siehe auch [Bun13b]).

IT-Sicherheit bezeichnet somit weniger die Sicherheit als vielmehr den Schutz von Informationen, die elektronisch als Daten gespeichert und mithilfe von Informationstechnologie (IT) verarbeitet wurden, vor Bedrohungen : dem Nutzer selbst, Malware, Hacker oder Kriminellen (vgl. [Bru06]).

Abbildung 2.3 listet sowohl englisches als auch deutsches Sicherheitsvokabular auf, um eine bessere Übersicht zu gewähren.

Englisch	Deutsch	Oberbegriff
Safety	Funktionssicherheit, Betriebssicherheit	Begriff Sicherheit
Security	Informationssicherheit	
Protection	Datensicherheit, Datensicherung	
Privacy	Datenschutz	
Authenticity	Echtheit, Glaubwürdigkeit	Sicherheitsziele
Integrity	Manipulationssicherheit	
Confidentiality	Vertraulichkeit	
Availability	Verfügbarkeit	
Non Repudiation	Verbindlichkeit, Nicht-Abstreitbarkeit	

Abbildung 2.3.: deutsches und englisches Sicherheitsvokabular nach [Kli10]

2.2.1. Definition [Sicherheits|Schutz]ziele

Authentizität

Die Authentizität eines Objekts bzw. Subjekts (engl. authenticity) bezeichnet die Echtheit und Glaubwürdigkeit des Objekts bzw. Subjekts - diese ist durch eine eindeutige Identität und charakteristischen Eigenschaften überprüfbar (vgl.[Eck12]).

Authentifikation als Beweis der Authentizität eines Subjekts (z.B. eines Benutzers) gegenüber eines Computers besteht aus zwei Schritten (vgl. [Shi07], [Eck12]):

1. **Identifikation:** der Benutzer gibt seine eindeutige Benutzerkennung (engl. *account*) an
2. **Verifikation:** der Benutzer weist nach, dass seine behauptete Identität mit den vorher festgelegten charakteristischen Eigenschaften übereinstimmt. Charakteristische Eigenschaften zum Nachweis der Identität (engl. *credentials*) sind beispielsweise Passworte, biometrische Merkmale (Fingerabdruck) oder Smartcards.[3]

Um die Authentizität von Objekten[4] über ein unsicheres Transportmedium wie z.B. das Internet nachzuweisen werden kryptographische Verfahren verwendet. Die Echtheitsprüfung der Daten beinhaltet einen Ursprungs- und Urhebernachweis, aber keine Aussagen über die Funktionalität des Objekts.

Manipulationssicherheit

Manipulationssicherheit (engl. integrity) stellt sicher, dass zu schützende Informationen nicht unautorisiert, unbemerkt und/oder unbeabsichtigt verändert werden. Als Beispiel nennt [Eck12] Lese- und Schreibberechtigungen für Dateien oder den Verfügungsrahmen eines Bankkontos, der Abbuchungen über einen bestimmten Betrag hinaus verhindert. Die Gewährleistung der Anforderungen erfolgt durch Modelle der Zugriffskontrolle, z.B. durch Role-Based Access Control (RBAC)[5]. Weiterhin muss sichergestellt werden, dass unautorisierte Manipulationen nicht unentdeckt bleiben - Datenveränderungen können z.B. mit kryptographisch sichere Hashfunktionen festgestellt werden.

[3] Aktuell etabliert sich der Personalausweis in Verbindung mit einem entsprechenden Lesegerät und einer sechsstelligen PIN zu einem Identitätsnachweis. `http://www.personalausweisportal.de/DE/Home/home_node.html`

[4] z.B. Web-Server, Access-Points oder Code

[5] spezifiert im `http://tools.ietf.org/html/rfc4949`, Internet Security Glossary, Version 2

Vertraulichkeit

Vertraulichkeit (engl. confidentiality) bedeutet, dass nur berechtigte Personen und Systeme auf Informationen Zugriff erhalten (vgl. [Bru06]). Diese lässt sich in datensicheren Systemen durch die Festlegung von Berechtigungen oder Kontrollen jeglicher Art bewirken, die sicherstellen dass kein Subjekt[6] unberechtigten Zugriff auf Informationen erhält. Um die Anforderungen an die Vertraulichkeit zu erfüllen werden kryptographische Verschlüsselungstechniken angewandt [Eck12].

Verfügbarkeit

Verfügbarkeit (engl. availability) gibt an, ob und in welcher Weise IT-Services in einem definierten Zeitraum zur Nutzung durch autorisierte Subjekte zur Verfügung stehen [Bru06]. Hier werden Ausführungsverzögerungen, die z.B. durch Prozess-Scheduling auf dem genutzten System entstehen, nicht als Verletzung der Verfügbarkeit betrachtet. Tatsächlich bezeichnet [Eck12] es als schwierig, unautorisierte Beeinträchtigungen der Verfügbarkeit zu erkennen. Um die Anforderung der Verfügbarkeit jedoch einzuhalten werden Maßnahmen zur Reglementierung von z.B. Speicher oder CPU-Zeit nach vorgegebenen Quoten empfohlen.

Verbindlichkeit

Verbindlichkeit (engl. non-repudiation) stellt sicher, dass jede Aktion nachträglich einem Subjekt zugeordnet werden kann und somit nicht abstreitbar ist. Relevanz hat diese Eigenschaft laut [Eck12] bei der Verwendung von Rechenzeit, die eine Abrechenbarkeit (engl. accountability) und Überwachung (engl. audit). Eine andere relevante Aktion ist die Sicherstellung der Rechtsverbindlichkeit getätigter Geschäfte im E-Commerce[7] - hier finden digitale Signaturen Anwendung, um die Anforderung zu erfüllen.

2.2.2. Sicherheitsmanagement

> „Sicherheit ist ein Prozess und kein Produkt." Bruce Schneier [Sch01, S. 264]

Sicherheitsmanagement bezeichnet den Prozess der Planung, Konzeption, Umsetzung und kontinuierlichen Prüfung, Steuerung und Fortentwicklung des Sicherheitsniveaus eines Unternehmens oder einer Organisationseinheit (vgl. [Mül11]).

[6] Subjekt bezeichnet in diesem Kontext einen Benutzer, kann aber durchaus auch für Prozesse oder Hardwarekomponenten stehen.

[7] für: electronic commerce, engl. für elektronische Geschäfte (z.B. Onlineshops)

Ein Sicherheitsmanagement schützt immer ein Gesamtunternehmen, was personelle, materielle und immaterielle Werte mit einschließt und diese zu Schutzobjekten macht, die anforderungsgerecht abzusichern sind. Neben den Themenfeldern Prozesse, Ressourcen und Organisation ist auch der Lebenszyklus von Prozessen, Ressourcen (Systemem), Organisation, Dienstleistung und Produkten ein wichtiger Aspekt, um einen sicheren Geschäftbetrieb, sichere Systeme und sichere Produkte zu erreichen.

IKT- bzw. Informationssicherheitsmanagement als integrativer Teilbereich eines Sicherheitsmanagement erstreckt sich über den Bereich der Informations- und Kommunikationstechnologie und somit über alle IT-Prozesse, die Phasen des Lebenszyklus von Computersystemen und über alle Ressourcen (z.B. Hardware, Software, Middleware, Betriebssysteme, Knowledgeware (Wissen) und Paperware (Unterlagen und Dokumente).

Um einen gleichbleibenden Standard zu bieten sind Normen, Standards und Best Practice-Ansätze einem kontinuierlichen Verbesserungsprozess unterzogen und sollen nachfolgend und in Kürze aufgezeigt werden.

Sicherheitsstandards und ITIL

Sowohl nationale als auch internationale Standards beschäftigen sich mit IT-Sicherheit. An dieser Stelle soll ein kurzer Überblick hierüber gegeben werden ohne explizit auf Details (wie deren Anwendungsbereiche oder Auswahl) einzugehen (vgl. [Bru06], [Mül11]).

TCSEC (Orange Book) 1985 veröffentlichte das Department of Defense (DoD) der USA einen ersten umfassenden Maßnahmenkatalog zur Messung der erreichten IT-Sicherheit, das „Trusted Computer System Evaluation Criteria“ (TCSEC), aufgrund der Umschlagfarbe Orange Book genannt. Die Sicherheitseinstufung erfolgt in vier Stufen von A bis D, wobei A für beweisbaren Schutz (engl. verified protection), D für minimalen Schutz (engl. minimal protection) steht. 1987 erfolgte eine Adaption für vernetzte Systeme (Trusted Network Interpretation of the TCSEC, auch: Red Book).

ISO/IEC 27000 Dieser Standard ist eine Reihe von Dokumenten, die von der International Standards Organization (ISO) und der International Electrotechnical Commission (IEC) zur Festlegung einheitlicher Terminologien und Definitionen, das *Informationssicherheitsmanagement* (ISMS) betreffend, veröffentlicht wurden.

BSI Grundschutzhandbuch Analog zum ISO/IEC 27000 Standard bietet auch das Grundschutzhandbuch des Bundesinstituts für Sicherheit in der Informationstechnik einen Best Practice Ansatz zur Modellierung eines ISMS.

Die Basis des Grundschutzhandbuchs wird durch ein modulares Bausteinsystem abgebildet, indem übergeordnete Prozesse und Verfahren (z.B. Organisation, Notfallplanung, Sicherheitsmanagement) als eigene Bausteine definiert sind. Komplettiert wird das Grundschutzhandbuch durch einen ausführlichen Gefährdungs- und Maßnahmenkatalog.

Ziel des Grundschutzhandbuchs ist es, durch Standards für personelle, technische und organisatorische Schutzmaßnahmen ein angemessenes Sicherheitniveau für IT-Systeme zu erreichen.

Common Criteria Die Common Criteria for Information Technology Security Evaluation (Common Criteria,CC) existiert seit 1996 und ist ein Standard zur Bewertung und Zertifizierung der Sicherheit von Computersystemen. Federführend sind sowohl Australien, Kanada, Frankreich, Deutschland, Italien, Japan, Malaysia, die Niederlande, Neuseeland, Norwegen, Südkorea, Spanien, Schweden, Türkei, Großbritannien und die USA beteiligt. Der Maßnahmenkatalog gliedert sich in drei Teile:

1. Einführung und allgemeines Modell / Introduction and General Model
2. Funktionale Sicherheitsanforderungen / Functional Requirements
3. Anforderungen an die Vertrauenswürdigkeit / Assurance Requirements

Ziel der CC ist es, die Sicherheitsfunktionalität und erfolgte Zusicherungen voneinander zu trennen (nach [Wit06]).

Information Technology Infrastructure Library (ITIL) ITIL beschreibt von IT-Dienstleistern zu implementierende Prozesse, um IT-Services erfolgreich zu betreiben. Fünf Kerndokumente bilden ein umfassende Dokumentensammlung, die weltweit Anwendung findet.

3. Psychologische Grundlagen

Nachdem die Grundlagen zur Sicherheit im Allgemeinen und in Bezug auf IT-Sicherheit betrachtet wurden will dieses Kapitel zeigen, wie und warum Menschen in Bezug auf Sicherheit handeln. So kann ein Übergang zur Passwortsicherheit geschaffen werden, die maßgeblich von der Handlung und den Fehlern des Menschen abhängig ist. Der Ansatz hierbei ist eklektisch, das heisst es wird kein umfassender Überblick geboten sondern die Bereiche betrachtet, die nach Einschätzung der Autorin für diese Arbeit von Relevanz sind.

3.1. Definition Kommunikation

> „Man kann nicht *nicht* kommunizieren, denn jede Kommunikation (nicht nur mit Worten) ist Verhalten und genauso wie man sich nicht nicht verhalten kann, kann man nicht nicht kommunizieren." Paul Watzlawick [Ben12]

Kommunikation ist ein Synonym für den zwischenmenschlichen Informationsaustausch mittels Worten, Gesten und Mimik. Bezogen auf die Informationstechnologie wird der Begriff analog verwendet - kommunizieren zwei Entitäten (z.B. Client, Server, Peripheriegeräte, Prozesse) miteinander findet eine Kommunikation im Sinne eines Informationsaustausches statt.

> „Kommunikation ist der Prozess, Informationen von einer Instanz zu einer anderen zu transferieren. Kommunikation zieht Interaktion zwischen zumindest zwei Beteiligten nach sich und kann als gegenseitiger Prozess betrachtet werden, bei dem es einen Austausch von Informationen gibt und eine Entwicklung oder Abfolge von Gedanken, Gefühlen oder Ideen bezogen auf ein gegenseitig akzeptiertes Ziel oder eine (Handlungs-)Richtung." Christopher Hadnagy [Had11, S. 69]

Relevant für diese Arbeit ist die Wahrnehmung, dass Kommunikation für die Sicherheit im allgemeinen und die IT-Sicherheit entscheidend ist. Ohne Kommunikation von Komponenten kann kein System funktionieren - dies ist einem Informatiker bekannt und würde nie in Frage gestellt. Doch auch die zwischenmenschliche Kommunikation ist von Bedeutung, denn ein

Mensch kann ohne Information, was Sicherheit ist und wie er sich verhalten soll, kein sicheres Verhalten anwenden (vgl. [BSHL12]).

Kommunikation birgt jedoch auch Schwachstellen - neben Mißverständnissen und Fehlinterpretationen können auch simple Botschaften dazu führen, dass neben der reinen Sachinformation auch Botschaften übertragen werden, die auf diese Weise nicht beabsichtigt waren.

Abbildung 3.1 zeigt das wohl bekannteste Kommunikationsmodell, das „Kommunikationsquadrat“ nach Friedemann Schulz von Thun (vgl. [Sch13]). Diese zeigt die vier Ebenen einer Kommunikation: die Sachinformation („das Fenster ist offen“), die Selbstkundgabe („mir ist kalt“), einen Beziehungshinweis („ich möchte,dass Du etwas für mich tust“) und einen Apell („mach das Fenster zu“).

Abbildung 3.1.: Das Kommunikationsquadrat nach [Sch13]

Die Qualität der Kommunikation hängt nach [Sch13] ausschliesslich von Sender und Empfänger der Nachricht ab. Relevant für die Sicherheit ist, dass sowohl Sender als auch Empfänger einer Nachricht nach korrekter Einschätzung des Gegenübers in der Lage sind, den anderen zu beinflussen und sogar zu manipulieren. Diese Art der Beeinflussung ist besonders häufig im Konfliktmanagement zu finden, kann aber auch im Social Engineering (siehe Kapitel 4.3.1) Anwendung finden.

3.2. Definition Verhalten - Handlung

Verhalten wird an dieser Stelle als Gesamtheit der möglichen Lebensäußerungen von Menschen definiert (vgl. [BSHL12]). Diese Arbeit beschäftigt sich mit dem Verhalten gesunder, erwachsener Menschen und deren Wunsch, Ziele mittels gerichteter und möglichst rationell ausgerichteter Tätigkeiten zu erreichen.

Sobald das Verhalten einer Person planvoll, zielgerichtet und weitgehend bewusst kontrolliert abläuft wird in der Psychologie von einer Handlung gesprochen (vgl. [Ase12]).Handlungen sind aber auch relativ selbstständige Abschnitte zielgerichteter Tätigkeiten, die Teilziele realisieren.

Einflussfaktoren auf Handlungen Die klassische Psychoanalyse geht davon aus, dass Bedürfnisse (siehe auch Abbildung 2.1, die Bedürfnispyramide nach Maslow) sich direkt auf die Verhaltensrichtung auswirken, da ein physiologisch vorgegebener Soll-Wert permanent mit dem Ist-Wert verglichen wird und erreicht werden will.

Ein weiterer Einflussfaktor ist die Motivation. Nach der Erwartungs-Wert-Theorie (Heckhausen und Heckhausen 2006, siehe [Ase12]) ist die Motivation das Produkt aus dem Nutzen bzw. Wert, den eine Sache oder ein Zustand für uns hat, und unserer subjektiven Einschätzung der Wahrscheinlichkeit, ob wir diese Sache oder diesen Zustand erreichen können (= Erwartung).

Erwartung x Wert = Motivation

Die beste Motivation erfolgt dann, wenn ein Ziel in Aussicht gestellt wird, das die aktuelle Bedürfnislage möglichst genau trifft.

Die Feldtheorie (Lewin, 1946) hingegen ist ein Motivationskonzept (vgl. [Kie08]) welches besagt, dass jede Person stets in einem Feld verschiedener Kräfte situiert ist, welche auf ihn einwirken. Die Kräfte entstammen der Umwelt oder der Person selbst und wirken auf diese ein, ähnlich magnetischer Felder in der Physik. Eine Person bewegt sich immer auf Ziele zu, die sie positiv anziehen (positive Valenz) und von Dingen weg, die sie abstoßen (negative Valenz). Als Beispiel lässt sich ein Mitarbeiter in einem Büro von einem zu ordnenden Aktenberg abstossen, von einer frischen Tasse Kaffee anziehen. Übertragen auf die Fragestellung, warum Menschen Sicherheitsaspekte häufig außer Acht lassen lässt sich nur vermuten, dass diese mit einer negativen Valenz behaftet sind, wogegen die schnelle Erledigung eines Anliegens eine positive Valenz ausübt. Der resultierende Zielkonflikt „positiv-negativ“ geht (nach Lewin) stets zugunsten der positiven Valenz aus[1].

Kompetenz als subjektive Wahrnehmung, ob eine Person sich die Bewältigung eines Problems zutraut, steht im Gegensatz zum landläufigen Begriffsverständnis (Sachverstand oder die Befähigung innerhalb eines spezifischen Fachbereiches). Die Ausprägung dieser Wahrnehmung beeinflusst die Handlungsfähigkeit unmittelbar: sobald die Kompetenz gering erscheint wird die entsprechende Person eine Handlung eher unterlassen.

Zusammenfassend ist der Mensch nur schwer vorhersehbar - es variiert, abhängig von den Bedürfnissen sowie der Motivation eines Menschen, ob er sich (spontan und unvorhergesehen)

[1] weitere Zielkonflikte sind nach Lewin positiv-positiv und negativ-negativ, sollen an dieser Stelle aber nicht weiter betrachtet werden.

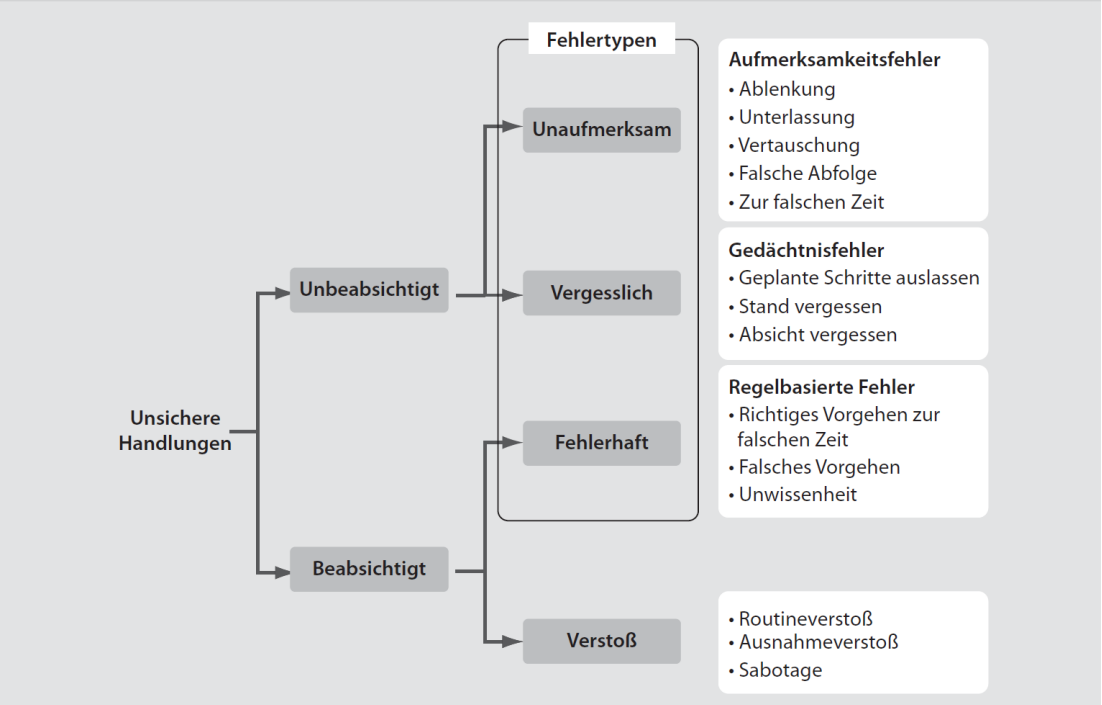

Abbildung 3.2.: Fehlerklassifikation nach Reason (1990) siehe [BSHL12]

verhält oder (bewusst und zielgerichtet) *handelt*. Um herauszufinden warum Menschen sich auf eine bestimmte Weise verhalten/handeln muss nicht die Gesamtheit, sondern das Individuum betrachtet werden.

3.3. Definition Fehler

Ein Fehler liegt genau dann vor, wenn eine beabsichtigte Handlung, zu der es eine Alternative gab, nicht das beabsichtigte Ergebnis erbrachte. Ob ein Fehler vorliegt wird vom Zielkriterium bestimmt. Die klassische Fehlerforschung untersucht die Klassifikation von Fehlern, im Anschluss werden möglich Ursachen betrachtet (vgl. [BSHL12]).

Die bekannteste Klassifikation erfolgte durch Reason (1990, vgl. [BSHL12]), welcher Formen „unsicherer Handlungen“ untersucht und diese danach klassifiziert, auf welcher Ebene der Handlungskontrolle sie vorkommen (Fehler in der Ausführung oder in der Planung) und ob diese auf Absicht beruhen oder nicht (Regelverstöße vs. Fehler), siehe Abbildung 3.2.

Der Unterschied zwischen unbeabsichtigten und beabsichtigten Fehlern ist der, dass unbeabsichtigte im Nachhinein vom Auslösenden auch als Fehler wahrgenommen werden. Verstöße

gegen Sicherheitsaspekte, wie zum Beispiel das manuelle Deaktivieren einer Firewall um eine (für den Nutzer) wichtige Email mit sicherheitskritischem Anhang zu versenden, fällt unter der Klassifikation von Reason in die Kategorie Verstoß - Ausnahmeverstoß. Die Begründung solcher Verstöße liegt darin, dass diese dem Ausübenden als sinnvoll für die Erreichung seiner Ziele erscheinen. Sie sind entweder persönlicher Art (Schlafbedürfnis, Kompetenzstreben, Statussicherung) oder aus arbeitsbezogenen Zielen (Zeitersparnis, Ressourcenersparnis, Optimierung von Arbeitsabläufen) entstanden.

Die Ursachen für Fehler zeigen laut [BSHL12] kein eindeutiges Ergebnis, können aber in Fehlerursachen innerhalb (*endogenous error*) oder außerhalb (*exogenous error*) der Person liegen:

- **Fehlerursachen außerhalb der handelnden Person:** Organisationsfaktoren (Sicherheitskultur, Zielprioritäten), Arbeitsumgebung (Lärm, Arbeitszeiten, Geräteausstattung), Merkmale der Arbeitsaufgabe (Komplexität, Strukturiertheit), Team (Kommunikationsregeln, Erfahrung)
- **Fehlerursachen innerhalb der handelnden Person:** Physiologische und biologische Faktoren (Müdigkeit, Ablenkung durch Lärm, krankheitsbedingte Aufmerksamkeitsstörung), individuelles Wissen, Fertigkeiten und Fähigkeiten (individuell unterschiedlich und personenabhängig), Mechanismen der menschlichen Informationsverarbeitung und Motivationsregulation.

Zu den letztgenannten Mechanismen gehören nach [BSHL12] u.a. folgende:

Ressourcenschonung Begrenzte kognitive Ressourcen, die an sich verändernde Informationsverarbeitungsprozesse angepasst werden müssen, können zu Fehlern führen. Die sparsame Verwendung bewussten Denkens zeigt sich besonders darin, dass Handlungsroutinen und Automatismen gebildet werden, um die Komplexität zu verringern. Wahrnehmungsinhalte werden nach Ähnlichkeit zu vorherigen Situationen (Schemata) erkannt; von mehreren möglichen Schemata wird das bisher am häufigsten aufgetretene gewählt. Erst, wenn vorhandene Muster und damit verbundene (Verhaltens-)Regeln nicht anwendbar sind werden neue Lösungen erdacht.

> „Menschen bevorzugen das sparsame fertigkeits- und regelbasierte Handeln vor dem wissensbasierten Handeln und problemlösenden Denken." Petra Badke-Schaub et al. [BSHL12, S. 56]

Aktives Gedächtnis Das Prinzip der Bahnung sagt aus, dass oft aufgerufene Gedächtnisinhalte am leichtesten zugänglich sind. So kommt es dazu, dass die assoziativ miteinander verknüpften Inhalte abhängig von der persönlichen Relevanz schneller verfügbar sind. Ambivalent ist diese Tatsache, da die persönliche Relevanz bei der Auswahl von Gedächtnisinhalten nicht mit sachlicher Relevanz einhergehen muss, und die Wiederholung bereits stattgefundener Denkprozesse dazu führen kann, konservativ an neue Aufgaben und Probleme heranzugehen.

Überwertigkeit des aktuellen Motivs Bereits in Kapitel 3.2, Definition Handlung - Verhalten, hat sich die Motivation als wesentlicher Aspekt des Handelns erwiesen. Als mögliche Fehlerursache kommt sie ebenfalls genau dann vor, wenn das aktuelle Motiv überbewertet wird und andere in den Hintergrund rücken. Dies erleichtert zwar ein zielgerichtetes, unabgelenktes Handeln einerseits, langfristige Aspekte werden aber eventuell außer Acht gelassen.

Kompetenzschutz und soziale Motive Das Gefühl von Kompetenz wird also benötigt um eine Handlung auszuführen und wird intuitiv geschützt, um die Handlungsfähigkeit aufrecht zu erhalten. Hierdurch entstehen z.B. Bestätigungsfehler (confirmation bias) - ein Bestätigungsfehler bezeichnet die Neigung, Informationen, die die eigene Erwartung widerlegen könnten, zu ignorieren, was zu einer Selbsttäuschung führt.

Da Menschen weiterhin die Nähe und Akzeptanz anderer Menschen benötigen, wird eventuell nicht auf Fehler anderer hingewiesen, um die Akzeptanz und den Status innerhalb einer Gruppe nicht zu gefährden.

3.4. Heuristiken

Jeder Mensch trifft individuelle Entscheidungen, insbesondere als Benutzer eines Computersystems und in Bezug auf Sicherheit. Diese Entscheidungen fallen oft nicht spontan, sondern aufgrund von unbewusst eingeübte Handlungs- oder Denkroutine, die zum gewünschten Ziel führen soll. Diese Routinen und Automatismen werden als Heuristiken bezeichnet und in zwei Kategorien aufgeteilt.

> "Menschen können in der Regel nicht jede Situation komplett durchdenken, um zu einer Handlungsentscheidung zu gelangen." Bettina Weßelmann [Weß08, S. 601]

3.4.1. kognitive Heuristiken

[Weß08] unterscheidet in ihrem Artikel zwischen kognitiven und sozialen Heuristiken. Der Unterschied liegt darin, dass kognitive Heuristiken ohne Einflussnahme Dritter Anwendung finden, während soziale Heuristiken erst dadurch benötigt werden. Ausführliche Informationen zu diesen Heuristiken bietet [Sch08b].

Sure-Gain-Heuristik

Bereits in der Urzeit bedeutete ein schneller, aber geringerer Erfolg bei der Jagd einen höheren Gewinn (engl. „gain“) als eine lange, risikoreiche Jagd, die bei Mißerfolg zum Verhungern führen konnte. Aus diesem Grund greifen Menschen bei einer Entscheidung zwischen einem sicheren, aber kleinen Gewinn oder einem weniger sichereren, langfristigeren Gewinn eher zu ersterem.

Übertragen in die IT-Sicherheit bedeutet dies, dass ein Benutzer z.B. zum Abschluss einer für ihn wichtigen Arbeit eine dabei behindernde Sicherheitsmaßnahme eher abschaltet, anstatt deren Ursache zu ergründen. Als Beispiel kann das Absenden einer wichtigen Email genannt werden, die durch eine Firewall behindert wird. Das Risiko, dass hierdurch eine Sicherheitslücke entsteht ist dem Nutzer zwar bewusst, die persönliche Risikoeinschätzung der Bedrohung ist jedoch gering.

Optimismus

Eine subjektive Gefahreneinstufung ist generell niedriger als würde der Benutzer dieselbe Situation für einen anderen bewerten. Diese „optimistische“ Grundeinstellung - „das passiert nur den anderen“ - findet sich häufig im IT-Bereich, da die Mitarbeiter hier über ein besonders hochwertiges Wissen rund um die Sicherheit verfügen und davon ausgehen, dass sie gerade dadurch besonders geschützt sind und fehlerfrei(er) arbeiten.

Heuristik der Kontrolle

Kurioserweise schätzen Menschen Gefahren geringer ein, wenn Sie das Gefühl haben die Situation aktiv zu kontrollieren. Als Beispiel lässt sich nennen, dass Menschen die Gefahr eines Unfalls als Fahrer eines PKW gering einschätzen, die Gefahr/das Risiko mit einem Flugzeug abzustürzen, das statistisch sehr viel geringer ist, jedoch höher.

Affekt-Heuristik

Diese Heuristik sagt aus, dass Menschen sich abhängig von der aktuellen Gefühlslage unterschiedlich verhalten und hierdurch beeinflusst werden. Eine positive Grundstimmung kann also beispielsweise zu einer höheren Risikobereitschaft führen.

Häufigkeit und Erinnerung

Je leichter man sich an ein bestimmtes Ereignis erinnern kann, desto höher ist die individuelle Wahrscheinlichkeitsempfindung, dass dieses erneut eintreten kann. Einen wesentlichen Einfluss haben hier die Medien (z.B. in Bezug auf Internetkriminialität oder Terrorismus) sowie das persönliche Umfeld. So kann es dazu kommen, dass sich Personen mit mehreren Antivirenscannern „bewaffnen“, jedoch keine Maßnahmen zur Datensicherung treffen, weil sie noch nichts darüber gehört haben.

Bestärkungs-Heuristik

Möchte ein Mensch eine Entscheidung treffen ist er eher gewogen, Informationen zu vertrauen die seine vorgefasste Meinung bestätigen.

3.4.2. soziale Heuristiken

[Weß08] zitiert insbesondere Robert Cialdini („Die Psychologie des Überzeugens“) für die Betrachtung von soziale Heuristiken, die in Bezug auf die Einflussnahme von Social Engineering (siehe Kapitel 4.3.1) wertvolle Erkenntnisse liefern.

Reziprozität

Über kulturelle Grenzen hinweg findet Reziprozität Anwendung. Der Ablauf ist - ausgenommen sind laut Gouldner lediglich Kinder, Kranke und Behinderte - kaum zu durchbrechen. Das Wertbehaftete, das weggeben wird muss für den Empfänger einen Wert haben, es muss sich jedoch nicht um eine Sache handeln. Es kann auch ein Dienst, eine Hilfestellung oder Information sein. Die Schuld, die der Empfänger durch den Erhalt unbewusst aufbaut hängt vom Wert der Sache sowie dem Grad der Überraschung ab; es wird ein Gefühl der Verpflichtung erzeugt, eine Gegenleistung zu erbringen.

Mittels Reziprozität - der inhärenten Erwartung gut behandelt zu werden, wenn man dies ebenfalls tut - bietet sich die Möglichkeit, durch eine Tat oder Hilfestellung einen Gefallen herbeizuführen oder zu erzwingen. Die „Norm der Reziprozität“, die eine grundlegende transkulturelle Dimension sittlichen Verhaltens darstellen soll, sagt aus:

> „ 1. Man soll denen helfen, die einem helfen.
> 2. Man soll jene nicht verletzen, die einem geholfen haben.“

Alvin W. Goudler [AM05, S. 109]

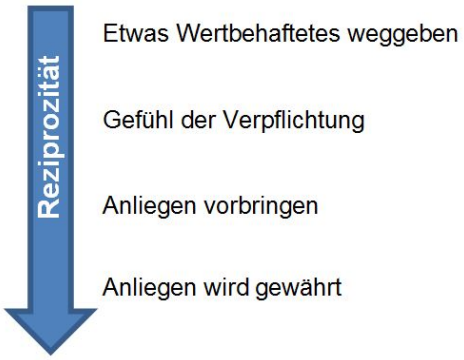

Abbildung 3.3.: Ablauf der Reziprozität

Commitment und Konsistenz

Menschen möchten sich konsistent verhalten und orientieren sich hierbei anhand früherer Verhaltensweisen und getroffener Entscheidungen. Jegliche Art von Verpflichtung (engl. *commitment*), z.B. ein zu vermittelnder Eindruck oder ein Versprechen) gegenüber Dritten ist ein Motivator, diese Verpflichtung auch einzuhalten. Ringt z.B. ein Social Engineer dem Gesprächspartner ein erstes Commitment ab, z.B. der Bitte auf etwas kurz zu achten, wird sich dieser verpflichtet fühlen, dies auch zu erfüllen.

Soziale Bewährtheit

In die selbe Richtung wie Commitment und Konsistenz wirkt auch der soziale Bewährtheit (engl. *social proof*), die Tatsache dass Menschen sich in unsicheren Situationen an ihrem sozialen Umfeld orientieren und eine Handlungsweise ableiten. Beispiel hierfür ist z.B. das Experiment, eine Person an einem belebten Ort in den Himmel sehen zu lassen. Bereits nach kurzer Zeit folgen Passanten diesem Beispiel.

Sympathie

Menschen vertrauen anderen eher, wenn sie diese mögen bzw. sympathisch finden. Empfundene, körperliche Attraktivität führt zu unbewusster Sympathie und zur Verknüpfung mit anderen Erfolgsqualitäten, die nicht zwangsläufig zutreffen müssen[2]. Auch die Einschätzung

[2] dieses Phänomen ist auch als *Halo-Effekt* bekannt.

des Gegenübers, dass einem ehrliche Unterstützung oder Hilfestellung zuteil wird, kann zu Sympathie führen.

Autorität

Autorität ist eine weitere wichtige Einflussgröße in der Psychologie. Egal ob es sich um die legale Autorität (Regierung und Gesetz, vertreten durch Polizei und Behördenvertreter), organisatorische Autorität (der Unternehmenshierarchie, vertreten durch Vorgesetzte) oder die soziale Autorität(dem Eindruck, Anführer einer Gruppe zu sein) handelt - die meisten Menschen unterwerfen sich gedankenlos jeglicher Autorität ohne diese aktiv zu hinterfragen (vgl. [Had11]). Hierbei wird jedoch meist nicht die Autorität selbst respektiert (die Persönlichkeit mit maßgeblichem Einfluss und hohem Ansehen[3]), sondern deren Symbole in Form von Titel, Kleidung oder Fahrzeugen, gegebenenfalls auch der Ausdrucksweise (beispielsweise „militärisch-zackig“).

Knappheit

Informationen, Gegenstände oder Gelegenheiten wirken anziehender auf Menschen, wenn diese für knapp, selten oder schwer zu kriegen gehalten werden. Je seltener eine Ressource ist, desto höher ist der für das Objekt wahrgenommene Wert. Die Anwendung findet sich am häufigsten in der Werbung wieder („Begrenztes Angebot“ etc.), lässt sich aber auch auf die zwischenmenschliche Kommunikation übertragen - in einem Prozess der Entscheidungsfindung kann durch Verknappung als Werkzeug Druck aufgebaut werden. Die Anwendung von Knappheit wird wirksamer, wenn man sie mit weiteren sozialen Heuristiken mischt.

3.5. Bewertung von Heuristiken

[Sch08b] betont in seinem Artikel, dass Sicherheit stets ein Kompromiss ist, die Menschen jedoch dazu tendieren, wesentliche Aspekte außer Acht zu lassen:

- Die Schwere (engl. severity) des Risikos,
- Die Wahrscheinlichkeit des Risikos,
- Das Ausmaß der Kosten,
- Wie effektiv eine Gegenmaßnahme das Risiko senkt,
- Wie gut Risiken und Kosten gegeneinander aufgewogen werden können.

[3] `http://www.duden.de/rechtschreibung/Autoritaet`

Je stärker die subjektive Wahrnehmung von der Realität abweicht, desto weniger wird der erwogene Kompromiss vom benötigten abweichen. Die Ursache sieht Schneier darin, dass der Mensch sich auf unwesentliche Dinge stärker konzentriert als auf wesentliche, weil diese seit Millionen von Jahren in unserem Unterbewusstsein verankert sind.

Die Risikoeinschätzung erfolgt, analog zu Tieren, in der Amygdala, einem der „ältesten“ Bestandteile des Gehirns. Hier ist eine schnelle Reaktion das Maß aller Dinge, da das evolutionäre Überleben (und somit erfolgreiche Fortplanzen) im Vordergrund steht.

Die Analyse und Vorhersage eine Risikos erfolgt jedoch durch den Neocortex, den nur Säugetiere besitzen und der langsamer als die Amygdala arbeitet, was zu einem Zielkonflikt führt, da beide parallel arbeiten.

Obwohl Heuristiken durchaus nützlich sind können sie aufgrund des evolutionären Hintergrunds heutzutage auch fehlschlagen. In genau diesen Fällen stimmt die subjektive Sicherheitseinstufung nicht mehr mit der Realität überein, wodurch die situative Sicherheit gefährdet wird. Hier sieht [Sch08b] auch die Lösung des Zielkonflikts - das Gefühl und die Realität von Sicherheit müssen übereingebracht werden. Sicherheitsmaßnahmen, die ein Gefühl von Sicherheit vermitteln können dazu verwendet werden, das Sicherheitsbewusstsein der Menschen mit dem aktuellen Risikolevel überein zu bringen.

4. Passwortsicherheit

Nach der Klärung grundlegender Begrifflichkeiten in den bisherigen Kapiteln wird sich dieses Kapitel mit Passworten und deren Sicherheitsrisiken und Maßnahmen zur Verbesserung ebendieser beschäftigen. Der Schwerpunkt liegt hier jedoch auf der menschlichen Komponente.

Die Überprüfung der Authentizität (siehe Kapitel 2.2.1) von Subjekten ist notwendig, um die bereits erläuterten Schutzziele (Kapitel 2.2.1) zu erreichen und zu erhalten (vgl.[Eck12]). Es gibt mehrere Möglichkeiten der Authentifikation, wobei die Authentifizierung per Passwort und Benutzername seit den 1960er Jahren verwendet wird[1] und sich trotz neuerer und vermeintlich sicherer Technologien gleichbleibender Beliebtheit erfreut.

4.1. Definition Passwort

Die Herkunft des Wortes Passwort liegt laut dem Duden sowohl im Englischen (engl. *password*, aus „pass“ = Ausweis, Passierschein, Zugang) als auch dem Französischen („passe“, von „passer“ = passieren). So soll einem bestimmten Personenkreis mittels eines Geheimnisses Zugang zum Gebrauch einer Sache gewährt werden, um dessen Mißbrauch durch Außenstehende zu verhindern.

War ein Passwort bereits vor Jahrhunderten ein Schlagwort oder eine Parole, handelt es sich im heutigen Zeitalter der elektronischen Datenverarbeitung um eine aus Buchstaben, Ziffern, Sonderzeichen oder deren Kombinationen bestehende Zeichenkette. Diese wird in Kombination mit einem Benutzernamen (Usernamen), der meist aus dem Nachnamen, dem Vornamen oder einer Kombination aus beidem besteht, oder Pseudonym/E-Mail-Adresse zur passwortbasierten Zugangskontrolle verwendet. Der Austausch des Passwortes sollte immer über einen vertrauenswürdigen, also vor Abhören (engl. *eavesdropping*) und unberechtigter Modifikation geschützten Kanal stattfinden - klassisch ist dies beispielsweise die Briefpost oder der persönliche Kontakt.

[1] Das erste, bekannte Passwort für einen Computer wurde vermutlich in den 1960er Jahren für ein Compatible Time Sharing System (CTSS), einem der ersten Multi-Client-Systeme, am Massachusetts Institute of Technology vergeben um die unterschiedlichen Daten der Terminalnutzer zu schützen [IEE11].

Man unterscheidet die Verwendung von Verfahren mit einem Dauer-Passwort, das immer wieder verwendet wird, und andere mit Einmal-Passwörtern, die nach jeder Benutzung gewechselt werden - an dieser Stelle werden nur Dauer-Passworte betrachtet, eine kurze Übersicht zu Einmal-Passwörtern ist jedoch im Anhang A, Einmal-Passworte zu finden.

Ein (Dauer-)Passwort wird entweder von vorherein vom Benutzer ausgewählt oder vom zu benutzenden System vorgegeben. Wählt der Benutzer es selbst stehen ihm alle Zeichen des Alphabets, Ziffern und Sonderzeichen zur Verfügung. Diese kombiniert er nach seinen persönlichen Vorlieben und in einer Länge seiner Wahl, allerdings abhängig von eventuellen Passwortrichtlinien.

Systemgenerierte Passworte sind zufällig erzeugte Zeichenfolgen, die durch Ihre willkürliche Zeichenwahl in der Regel schlecht erinnert werden können (vgl. [Eck12], [ZH99]). Diese können entweder durch ein Anwendungssystem vorgegeben (beispielsweise als Initialpasswort), oder aber auf Wunsch des Benutzers selbst erdacht oder durch Webseiten[2] oder Tools[3] generiert worden sein (siehe auch: Kapitel 4.4,Maßnahmen zur Erhöhung der Sicherheit von Passworten).

> „An ideal password is something that you know, something a computer can verify that you know, and something nobody else can guess - even with access to unlimited computating resources. [...] in practice it's difficult to even come close to this ideal." Mark Stamp [Sta06, S. 231]

Zur besseren Abgrenzung verwende ich im weiteren Verlauf dieser Arbeit die Begrifflichkeit „herkömmlich" um benutzergewählte und systemgenerierte Passworte zusammenzufassen.

4.2. Klassische Sicherheitsrisiken

> „Passwords are the most often used form of authentication today, but this is primarily because passwords are free and definitely not because they are secure." Mark Stamp [S. 231][Sta06]

Die häufigsten Angriffe auf Passworte sind neben *Wörterbuch-Angriffen* (engl.: dictionary attack), die Passworte mittels vorgegebener Begriffe, deren Permutationen sowie sprachspezifischen Worthäufigkeiten „erraten" (engl. *guessing*) Brute Force-Attacken, die alle möglichen Permutationen einer Länge mit ca. 1000 Wörtern pro Sekunde abarbeiten. Hinzu kommt das klassische „Über-die-Schulter-Schauen" (engl. *shoulder surfing*), wobei der Angreifer in

[2] vgl. [Vle12], http://www.passwort-generator.com usw.
[3] z.B. `http://www.heise.de/download/passwort-generator.html`

unmittelbarer Nähe des Benutzers Einblick in die Tastatureingabe hat, verschiedende Arten des Social Engineering (siehe auch Kapitel 4.3.1) als geschicktes Erfragen von Informationen im persönlichen oder fernmündlichen Gespräch, sowie Phishing von Informationen durch gefälschte Webseiten. Weiterhin werden Passworte durch Viren, Würmer, Trojaner, Keylogger und verschiedenste Mal- und Spyware erschlichen, welche als technische Hilfsmittel zur Datenspionage hier zwar genannt, jedoch nicht näher erläutert werden.

Unabhängig von den Angriffsmöglichkeiten durch Dritte darf der Benutzer selbst nicht außer Acht gelassen werden. Risiken wie das Vergessen, Notieren oder Bekanntmachen von Passworten sind nicht unwesentlicher als die vorgenannten, jedoch schwerer zu beseitigen.

> „The number of such SPs with which a typical user routinely interacts has grown beyond the point at which most users can memorize the required credentials. The most common solution is for users to use the same password with every SP with which they register /a tradeoff between security and usability in favour of the latter." Andreas Pashalidis, Chris J. Mitchell [PM03, S. 1]

Nur durch Angriffe auf bestehende Systeme und dadurch offengelegte Passwortdaten lassen sich Aussagen darüber treffen, welche Passworte tatsächlich von Nutzern verwendet werden und welche Voraussetzungen diese erfüllen - oder auch nicht. Die Firma Splashdata, ein großer Hersteller von Sicherheitslösungen in den USA, gibt zum Zweck der Sensibilisierung von Benutzern einmal jährlich eine Liste der schlechtesten Passworte heraus (siehe Abbildung 4.1). [Bon12] hingegen konnte in seiner 2012 durchgeführten Studie auf 70 Millionen (anonymisierte) Passworte zugreifen, die u.a. aus einem Sicherheitsvorfall bei Yahoo stammten. Hieraus ergaben sich beispielsweise, dass 6,5 Prozent der deutschsprachigen Benutzer-Passworte innerhalb von 1000 Versuchen mit einem deutschsprachigen Dictionary-Angriff erraten werden konnten. Weiterhin ergab die Studie, dass 8,4 Prozent der Passworte von Jugendlichen im Alter von 13-20 Jahren auf diese Weise erraten wurden, wohingegen die Gruppe der über 50jährigen bei nur 7,3 Prozent lag. Übergreifend lässt sich feststellen dass die Qualität der Passworte, gemessen an der Möglichkeit, diese zu erraten, durchweg schlecht ist.

Selbstgewählte Passworte sind für den Nutzer stets am besten erinnerbar. Diese haben jedoch auch das größte Risiko, durch Dictionary- oder Brute Force-Angriffe aufgedeckt zu werden. Risikobehaftet ist ebenfalls die Verwendung eines Passwortes für mehrere/alle Zwecke, nur geringfügige Variationen z.B. durch angehängte Zahlen oder Sonderzeichen vorzunehmen oder sein(e) Passwort(e) niemals zu verändern.

Systemgenerierte Passworte sind oft so komplex, dass der Benutzer die Zeichenfolge notiert und sie in Arbeitsplatznähe deponiert (beispielsweise als Post-It am Monitor oder unter der

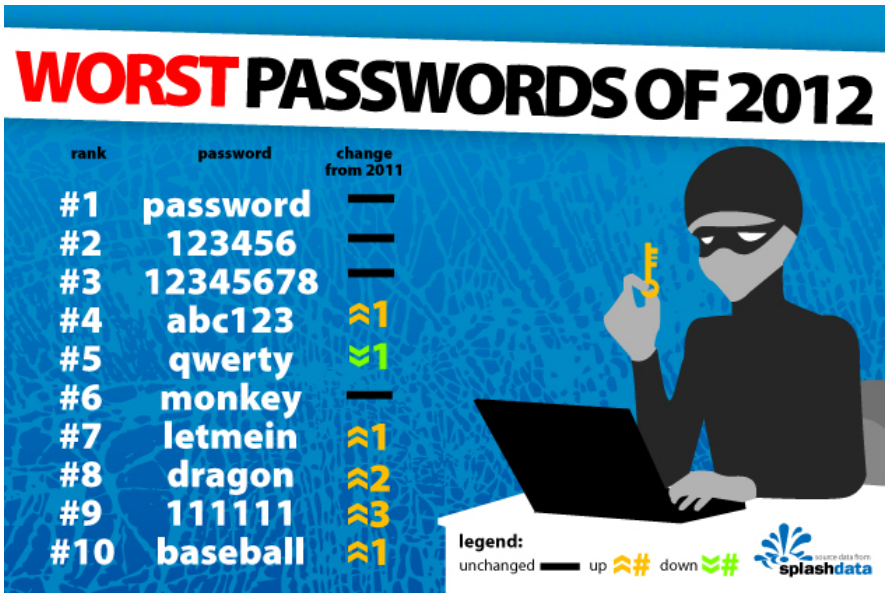

Abbildung 4.1.: Die Top 10 der schlechtesten Passworte

Schreibtischunterlage), was die Sicherheit der Zeichenfolge ad absurdum führt. Werden diese nicht notiert werden sie vergessen, wie [YBAG04] in seiner Studie unter 288 Studenten bewies. Auch die Autovervollständigung, die dem Nutzer bei manchen GUIs oder Webbrowsern das „lästige“ Erinnern von Passworten abnimmt kann leicht mittels Trojaner- oder Wurmangriffen ausgespäht werden (vgl. [Eck12]). Passwortverwaltungsprogramme, die es als Standalone-Programme oder Browser-Addons gibt bergen ebenfalls Risiken, z.B. das Vergessen des „einen“ Masterpassworts oder den Zugriff auf alle gespeicherten Passworte, sollte das Masterpasswort unsicher gewählt sein.

4.3. Beinflussung der Sicherheit durch menschliches Handeln

> „Die Hardware ist sicher; die Software ist sicher. Sogar das Netzwerk ist sicher. [...] Damit dieses wunderbare Computersystem etwas nützliches tun kann, muss es auf irgendeine Weise zu irgendeinem Zeitpunkt aus dem einen oder anderen Grund mit Benutzern interagieren. Und diese Interaktion ist das größte Sicherheitsrisiko von allen. Menschen stellen oft das schwächste Glied in der Sicherheitskette dar und sind chronisch verantwortlich für das Versagen von Computersystemen.“
> Bruce Schneier [Sch01, S. 249]

Sowohl [MS08] als auch [Sch01, Sch08b], [BSSW11] und [And08]stimmen darüber überein, dass der Mensch der größte Risikofaktor in Mensch-Computer-Interaktionen (engl. *human-computer interaction*, HCI) ist. Es ist nicht nur wichtig, Passwortrichtlinien und Sicherheitspolicies aufzustellen, sondern auch dafür zu sorgen, dass der Benutzer diese nicht - wissentlich oder unwissentlich - umgeht oder durch geschicktes Handeln Dritter Informationen preisgibt.

4.3.1. Social Engineering

Social Engineering, zusammengesetzt aus den englischen Worten für sozial und Ingenieurswissenschaft, bezeichnet nach [Had11] jede Art und Weise, eine Person zur Ausführung einer Handlung zu bringen. Diese kann im Interesse der Person liegen, muss sie aber nicht. Tatsächlich sind viele alltägliche menschliche Interaktionen eine Form des Social Engineering, sei es in der Kindererziehung, den Befragungstechniken der Polizei, oder der Art, wie ein Psychiater einen Patienten durch geschickte Fragenwahl zu einer bestimmten Einsicht oder Ansicht bringen kann. Social Engineering ist nicht von vornherein böswillig ausgerichtet und auch keine einzelne, zielgerichtete Aktion. Vielmehr handelt es sich um eine Sammlung von Aktionen, ähnlich eines Algorithmus.

Verschiedene der nachfolgenden Unterkategorien können, miteinander kombiniert, für Social Engineering verwendet werden.

Phishing Das Phishing, das laut Duden[4] als Kunstwort aus „phreaking“ und „fishing“ die Beschaffung persönlicher Daten anderer mittels gefälscher E-Mails oder Webseiten bezeichnet, ist die einzige technische Social Engineering-Maßnahme (engl. *computer-based social engineering* [BSF07]), die keinen persönlichen Kontakt erfordert wie das *human-based social engineering* (siehe unten). Phishing versucht den Benutzer über die Medien E-Mail und Internet dazu zu bringen, sicherheitsrelevante Informationen wie Passworte, aber auch Kontonummern und PINs oder TANs[5] auf einer gefälschten Webseite anzugeben. Entweder werden die Kunden über einen Link dorthin verwiesen oder die E-Mail enthält einen Anhang, der Malware (z.B. einen Trojaner) enthält[6]. Mittlerweile haben aktuelle Vorkommnisse gezeigt, dass die Angriffe immer authentischer werden. Waren vor Jahren gefälschte E-Mails und Webseiten noch anhand von Tippfehlern oder kryptischen Internetadressen zu erkennen, ist dies heute kaum noch möglich. Die Verursacher nutzen oft echte Emails von Banken und verändern lediglich die Links, wohlwissend um die Tatsache dass der Nutzer eher den Link benutzt als die Adresse der

[4] `http://www.duden.de/rechtschreibung/Phishing`

[5] PIN: personal identification number, TAN: transaction number

[6] ein populäres Beispiel hierfür ist der ILOVEYOU Wurm, der den Empfänger mit plausiblen Absender-, Betreff- und Nachrichteninhalten zum Öffnen des Anhangs verleitete.

Bank händisch einzutippen (nach [And08]). Das Bundesamt für Informationstechnik geht hier inzwischen aktiv auf die Nutzer zu und gibt Tipps, wie man gefälschte Emails oder Webseiten erkennen kann, siehe Abbildung 4.2.

Abbildung 4.2.: Beispiel des BSI für die Erkennung von gefälschten Webseiten [Bun13a]

Unabhängig davon, ob der Angreifer Zugang zu einem E-Mail Konto, einem Online Banking Account oder den Daten eines Internet-Versandhauses erlangt ist dies der erste Schritt zum Identitätsdiebstahl.

Identitätsdiebstahl Von Identitätsdiebstahl spricht man, wenn ein Täter seinem Opfer Daten entwendet, mit denen dieses sich im Rechtsverkehr identifizieren kann[7]. Mit benutzerbezogenen Daten (wie in Amerika z.B. der Sozialversicherungsnummer, in Deutschland eher Geburtsdatum, Anschrift und Kontonummer oder aber auch Kreditkartendaten) kann der Angreifer sich als die Person ausgeben, deren Daten er erschlichen hat, und sich damit Zugang zu weiteren Daten, Dienstleistungen oder Produkten verschaffen (engl. *spoofing*[8]). Julia Meyer hat in Ihrer Dissertation [Mey11] erstmals Identitäten in die „numerische Identität“ (erkennbare Übereinstimmung von Daten mit einer bestimmten Person), die „soziale Identität“ (Übereinstimmung von Selbstwahrnehmung und Wahrnehmung durch andere) und die „virtuelle Identität"(dauerhaftes, konsistent genutztes und somit wiedererkennbares Nut-

[7] `http://lexexakt.de/glossar/identitaetsdiebstahl.php`
[8] `http://www.dict.cc/?s=spoofing`

zerprofil, das jedoch den Nutzer selbst nicht zwangsläufig erkennen lässt) unterteilt. Spricht man von Identitätsdiebstahl, ist durch Phishing sowohl der Diebstahl von numerischen als auch virtuellen Identitäten möglich.

Informationssammlung

> „Wissen ist Macht." [Francis Bacon]

Grundsätzlich lässt sich eine große Menge Information heute bereits ohne Zuhilfenahme von Social Engineering -Techniken finden. Durch Suchmaschinen-Recherche, Firmenwebseiten, Rezensionen und Social Media[9] lassen sich Firmenstrukturen, Mitarbeiternamen und deren Stellung, oft auch Telefon- und Faxnummern oder Email-Adressen in Erfahrung bringen. Auch spezielle Formulierungen, interne Produktbezeichnungen oder intime Details wie Hobbies werden heute im Internet leichtfertig zur Verfügung gestellt.

Nach [MSD11] und [Had11] wird Information oft im direkten (Telefon-)Gespräch erfragt. Empfangsmitarbeiter und Service-Personal sind geschult, stets freundlich und hilfsbereit zu sein - wird das Anliegen mit entsprechender Glaubwürdigkeit vorgetragen, erscheint das Erfragte als wenig bis gar nicht „sicherheitsrelevant" und verwendet der Gesprächspartner soziale Heuristiken (siehe auch Kapitel 3.4, werden diese gerne und schnell helfen. Viele kleine Informationsschnipsel werden vom Social Engineer zusammengetragen und verwaltet, um sie später für einen anderen Zweck zu verwenden.

Eine klassische Art der Informationsbeschaffung ist die Observation - so lassen sich durch einfache Beobachtung Details ermitteln wie

- welche Art Schlüssel nutzen die Firmenangestellten, um ins Gebäude zu gelangen?
- wann kommt/geht Person X zur Arbeit, zum Mittagessen oder zum Meeting?
- wie sind die Namen der Kollegen, mit denen Person X im Bus über die Arbeit spricht?
- wie einfach kommt man als Lieferant oder als Putzkraft in das Gebäude?

Eine wenig beliebte aber in der Vergangenheit effektive (vgl. [MSD11]) Art der Informationsbeschaffung ist das Müll-durchwühlen (engl. *dumpster diving*). Papiere werden nur schlecht bis gar nicht geschreddert, Datenträger wie CDs und USB-Sticks nicht entwertet oder gelöscht, auf Post-Its finden sich eventuell noch Gesprächsnotizen. Wird solcher Müll von einer Fachfirma entsorgt ist diese eine potentielle Anlaufstelle, um an Daten zu gelangen.

[9] Social Media bezeichnet sowohl klassische Internetforen als auch Plattformen wie Facebook, Twitter, Google+, Xing, bei denen der Nutzer aktiv mit anderen Nutzern interagiert.

Alle vorgenannten Informationen helfen dem Social Engineer, sich ein Profil von der Firma und/oder deren Mitarbeiter zu machen (engl. *profiling*), das bei der darauffolgenden Arbeit von Wert ist.

Kommunikationsmodell Für den Social Engineer ist Kommunikation das A und O seiner Arbeit. Wie bereits in Kapitel 3.1, psychologische Grundlagen ausführlich beschrieben, findet Kommunikation immer statt - sowohl verbal als auch nonverbal und auf verschiedenen Ebenen. Aufgabe des Social Engineer ist es nun, den Beziehungsaspekt so zu wählen, dass der Sachaspekt in den Hintergrund tritt. Stets erfolgsversprechend ist hierbei die Vortäuschung eines Mangels oder einer Dringlichkeit (soziale Heuristik: Knappheit). Einem Mitarbeiter, der abends in „seiner“ Abteilung anruft, vorgibt auf Geschäftsreise zu müssen und wichtige Unterlagen zu benötigen, hilft man gerne weiter wenn dieser glaubhaft vermitteln kann, dass ihm die Angelegenheit „peinlich“ ist und er „wirklich sehr dankbar“ sei wenn er Hilfe bekäme. Bekräftigt wird diese Situation noch, wenn dieser vorgibt, dass diese Unterlagen „sehr wichtig und eilig“ seien und er ohne diese „seinen Job verlieren könnte“ [MSD11]. Hier teilt der Social Engineer über die Selbstkundgabe-Zunge Verzweiflung (vgl. Kapitel 3.1), Not und Hilflosigkeit mit und appelliert gleichzeitig über die Beziehungs-Zunge, indem er Wertschätzung und Dankbarkeit suggeriert.

Ein Social Engineer ist sich also über folgende Ziele einer Kommunikation (vgl. [Had11]) im Klaren:

- Die **Quelle** der Kommunikation ist der Social Engineer - er allein bestimmt, was, wie und worüber kommuniziert wird
- Der **Kanal** ist die Übermittlungsmethode - persönlich, telefonisch, schriftlich, per E-Mail oder Fax
- Die **Botschaft** ist der sachliche Inhalt, der übermittelt werden soll
- Der/die **Empfänger** sind das Ziel der Kommunikation
- Das **Feedback** ist die Rückmeldung, die der Social Engineer vom Empfänger erwartet - eine Reaktion in Form einer Auskunft oder Handlung.

Elizitieren Hat der Social Engineer ein Kommunikationsmodell für den gewünschten Zweck ausgearbeitet, ist das Elizitieren der nächste Schritt auf dem Weg zur Information. Elizitieren ist der Definition des Dudens[10] nach die Art und Weise jemandem etwas zu entlocken bzw.

[10] `http://www.duden.de/rechtschreibung/elizitieren`

jemanden zu einer Äußerung zu bewegen. Eine „leichte, lässige Konversation“ [Had11] kann unter Berücksichtigung von drei wichtigen Kriterien zum gewünschten Erfolg führen:

1. **Natürlichkeit:** weder der Social Engineer noch der Gegenüber sollen ein Unwohlsein verspüren. Dies ist besonders dann gegeben, wenn Kommunikationspartner sich in der Materie des Gesprächs gut auskennen.

2. **Selbst-Schulung:** der Social Engineer muss, um den ersten Punkt zu erfüllen, ein entsprechendes Wissen vorweisen können. Hierbei ist relevant nicht mehr Wissen vorzugeben, als von ihm in der aktuellen Situation angenommen werden kann. Eine ausführliche Recherche und hervorragende Vorbereitung sind obligatorisch.

3. **Keine Gier:** Das Ziel, Informationen zu erlangen, darf nicht in den Mittelpunkt rücken und für den Gegenüber ersichtlich werden. Stets gilt: „Wer fragt, führt das Gespräch“, doch kann es abhängig vom Gegenüber auch notwendig sein, diesen das Gespräch dominieren zu lassen und „nur“ zuzuhören.

4. **Erscheinungsbild:** Mimik, Gestik und das Gesamt-Äußere einer Person werden von Menschen bereits vor Beginn einer eventuellen Konversation wahrgenommen. Sucht der Social Engineer also den persönlichen Kontakt, sind diese Aspekte stets sorgsam zu wählen. Findet die Konversation telefonisch statt, kann die Stimmlage und Intonation ein Gespräch maßgeblich beeinflussen. Es reicht vollkommen aus, dass der Gegenüber sich *vorstellt*, er hätte einen netten/höflichen/interessanten Gesprächspartner.

Durch die Auswahl von Fragen, die den Gegenüber auf seiner bevorzugten Ebene abholt (siehe Kapitel 3.1, Kommunikation) kann ein erfahrener Social Engineer ein Gespräch auf fast jede erdenkliche Art steuern, um Informationen zu erhalten.

Pretexting Pretexting bezeichnet das Schaffen eines Szenarios, mit Hilfe dessen die Zielperson durch Schaffen von Vertrauen und Wohlempfinden zur Herausgabe von Informationen oder Ausführung einer Handlung animiert werden soll (nach [Had11]). Der Unterschied zum vorgenannten Elizitieren ist, dass das Pretexting die Eigenschaften beschreibt, die der Social Engineer als Person vorgeben muss, um die Zielperson zu überzeugen. Dies kann durch die entsprechende Wahl von Kleidung, Make Up, Accessoires und Visitenkarten, aber auch durch Dialekte und Redensarten passieren - auch gefälschte Internetprofile (Facebook etc.), Webseiten und E-Mail-Konten kommen vor. Bringt der Social Engineer persönliche Interessen mit ein, ist der Pretext (Vorwand) nicht zu komplex und wirkt noch dazu spontan, sind die Erfolgsaussichten am höchsten.

Trotzdem ist auch hier eine vorherige Recherche unumgänglich - will der Social Engineer sich als Außendienstmitarbeiter einer Lieferantenfirma ausgeben kann dies nur dann erfolgreich sein, wenn die Firma noch mit diesem Lieferanten zusammenarbeitet.

Psychologische Beeinflussung Die Arten der psychologischen Beeinflussung sind vielfältig und komplex. Hat der Social Engineer eine Verbindung mittels einer oder Kombinationen der nachfolgenden Methoden und Techniken aufgebaut, findet die konkrete Beeinflussung statt. Auch hier können aufgrund der Komplexität der Materie nur Grundzüge erläutert werden.

Der Social Engineer macht sich Grundprinzipien und Denkmuster des menschlichen Verhaltens und Handelns zu Nutze, in dem er sich auf den Kommunikationspartner explizit einstellt und ihn nach **Wahrnehmungstyp** (nach [GB76])kategorisiert. Es findet eine Unterscheidung zwischen visuellem, auditivem und kinästhetischem Denker statt - der jeweilige Denktyp ist entsprechend empfänglich auf Aussagen und Formulierungen, die den jeweiligen Sinn ansprechen. Weiterhin sind Erinnerungen an bildliche (visuelle), geräuschbezogene (auditive) oder gefühlsbezogene (kinästhetische) Faktoren geknüpft, den sogenannten Submodalitäten [Sei09]. Der Zusammenhang zwischen Wahrnehmungstyp und Submodalität kann aus Tabelle 4.1 entnommen werden.

Wie bereits zu Beginn der 1980er Jahre durch [GB76] festgestellt wurde kann der Wahrnehmungstyp dazu dienen, dem Gesprächspartner in seiner Welt zu begegnen indem man die selbe Sprache spricht, und „Information so zu verpacken, dass sie unwiderstehlich für ihn wird." Agiert der Social Engineer auf der selben Wahrnehmungsebene fühlt der Gesprächspartner sich wohl und verstanden und lässt den Gegenüber in seine Komfortzone.

Ein weiterer Faktor bei der psychologischen Beeinflussung sind **Mikroexpressionen**[11]. Hier handelt es sich um Gefühlsausdrücke im Gesicht des Gegenübers, die nur schwer zu steuern sind, oft nur ein Fünfundzwanzigstel einer Sekunde dauern und Reaktionen der Gesichtsmuskeln auf ein Gefühl sind. Außerdem sind diese nicht kulturell geprägt, sondern universell. Hier lassen sich sechs sogenannte Basisemotionen unterscheiden: Wut, Ekel, Angst, Freude, Traurigkeit, Überraschung und Verachtung.

Kennt der Social Engineer sich in dieser Materie aus, kann er leicht unterscheiden ob die Emotionen seines Gegenübers echt oder vorgetäuscht sind und was dieser tatsächlich von ihm hält. Außerdem kann er durch das gezielte Vortäuschen von Emotionen im eigenen Gesicht

[11] als wissenschaftlich betrachtet wurde dieser Ausdruck erstmals durch Dr. Paul Ekman (https://paulekman.com/) und Kollegen; seine Firma hat inzwischen ein Tool zur Erkennung von Mikroexpressionen erstellt.

Wahrnehmungstyp	Formulierungen	Submodalität
visuell	„Ich sehe, was Sie meinen.“ „Das sieht gut für mich aus.“ „Ich kann mir das vorstellen.“	Beleuchtung (hell, dunkel) Farbe (farbig, schwarz-weiß) Kontur (klar, verschwommen) Oberfläche (matt, glänzend) Form (rund, eckig) Größe (groß, klein) Entfernung (nah, fern) Position (links, rechts, oben, unten) Dimension (zweidimensional, dreidimensional)
auditiv	“Klar und deutlich…“ „Das sagt mir etwas…“ „Das hört sich gut für mich an.“	Lautstärke (laut,leise) Sprachtempo (langsam, schnell) Tonlage (tief, hoch) Tonalität (schrill, nasal, voll, dünn) Ort der Geräuschquelle (vorn, hinten, oben, unten)
kinästhetisch	“Wie hat sie das berührt?“ „Ich setze mich mit Ihnen in Verbindung.“ „Wie fühlt sich das an?“ „Ich wollte einfach mit Ihnen Kontakt aufnehmen.“	Intensität (schwach, stark) Temperatur (kalt, warm) Position (wo im Körper?) Qualität (angenehm, unangenehm)

Tabelle 4.1.: Wahrnehmungstypen und deren Submodalitäten nach [Sei09], [Had11]

Einfluss auf den Gegenüber nehmen - Traurigkeit kann z.B. zur Erregung von Mitleid, und so zur Erpressung einer Hilfestellung verwendet werden.

Die **Neurolinguistische Programmierung** (NLP) wurde maßgeblich durch [GB76] erarbeitet und sagt aus, dass eine jede Kommunikation auf Basis der fünf Sinne erfolgt. Die Wahrnehmung, Verarbeitung und Bewertung der Sinnesreize erfolgt für jeden Menschen unterschiedlich und beinflusst den kompletten Lebensprozess: Gefühle, das Denken, das Verhalten, die Handlungen, Bewegungen, physische, biologische und psychische Vorgänge. Der Sender einer Botschaft übernimmt bei NLP die Verantwortung, dass der Empfänger die Nachricht richtig - also für ihn als Person richtig - erhält. Konstruiert man die Botschaft also auf den Empfänger

abgestimmt kann man diesen, wie dies auch öfter behauptet und durch Social Engineers oder Verkaufsfachleute angewandt wird, beeinflussen und/oder manipulieren (vgl. [GB76], [Sei09]). Auf die entsprechenden Techniken soll an dieser Stelle nicht näher eingegangen werden.

Eine weitere, oft zitierte Art um Beeinflussung vorzubereiten - obwohl nicht für diesen Zweck vorgesehen - ist das Herstellen von **Rapport**. Rapport bezeichnet den intensiven, psychischen Kontakt zwischen zwei Personen, wie etwa zwischen Therapeut und Patient[12]. Rapport entsteht normalerweise auf natürlichem Wege, kann aber mittels verschiedenster Techniken absichtlich hergestellt werden. Beispiele solcher Techniken sind das Anpassen der Atmung an den Gegenüber, die Anpassung des Stimmenklangs und des Sprachmusters oder die Anpassung der Körpersprache an die Zielperson (nach [Had11]). So hat der den Rapport suchende stets die Aufmerksamkeit des Gegenübers.

Zusätzlich greift ein Social Engineer auch auf Heuristiken des menschlichen Handelns (nach Cialdini, siehe Kapitel 3, Psychologische Grundlagen) zurück. Unabhängig davon, welche Technik(en) der Social Engineer wählt - sie alle laufen darauf hinaus, im schlimmsten Fall kriminelle Handlungen durchzuführen. Der Gegenüber wird getäuscht oder bedroht, es werden Gefühle wie Schuld oder (Existenz-)Ängste geweckt.

4.3.2. beabsichtigtes/unbeabsichtigtes Aushebeln von Security Policies

> „It is important to challenge the view that users are never motivated to behave in a secure manner." Anne Adams, Martina A. Sasse [AS99, S. 45]

Unabhängig von den Angriffen, die jeder Person oder jedem Unternehmen durch Social Engineering drohen kann der Mitarbeiter selbst das größte Sicherheitsrisiko sein. Angestellte aller Gehaltsstufen sind gleichermaßen gefährdet sich unberechenbar zu verhalten. Verursacht durch private oder berufliche Probleme oder Demotivation können diese böswillig Firmeninterna nutzen um Schaden anzurichten - genauso verhält es sich jedoch auch bei Security Policies (siehe Kapitel 4.4.5) und Arbeitsanweisungen, die vom Mitarbeiter wissentlich oder unwissentlich mißachtet werden. Wie [And08] bestätigt gibt es stets eine Anzahl von Personen - in seiner Versuchsgruppe ca. ein Drittel - die Anweisungen nicht folgen wollen. [Sch07] berichtet von einer 65-prozentigen Quote von Sicherheitsangriffen durch Nachlässigkeit, Unwissenheit aber auch durch gezielte Manipulation, Industriespionage oder Bereicherungswunsch. Angela Sasse und Anne Adams untersuchten bereits in ihrer 1999 durchgeführten Studie [AS99] die **Ursachen** hierfür, auch [CMRW88, Sch01, MS08, IS10, Kay] geben Hinweise darauf:

[12] `http://www.duden.de/rechtschreibung/Rapport`

fehlende Informationen und verwirrende Sicherheitssysteme [AS99] stellen in Ihrer Studie fest, dass Benutzer ohne das Wissen einer korrekten Passwortwahl eigene Passwortregeln aufstellen, die sie für sicher halten, was diese nicht sind. Dies deutet auf fehlende Informationen über Sicherheitsrichtlinien hin - Benutzer können Sicherheitsrisiken nicht richtig einschätzen, die Sicherheitsbeauftragten können die Anliegen der Benutzer nicht nachvollziehen. Außerdem fühlen sich Nutzer nicht unmittelbar bedroht und empfinden Sicherheitsmaßnahmen daher schnell als mühselig und unnötig. [Sch01] untermauert diese These : damit Sicherheit effektiv ist soll sie für den Benutzer sichtbar sein, aber Benutzer möchten Sicherheit weder sehen, noch Sicherheitsentscheidungen treffen oder Computersicherheitsregeln umsetzen, weil sie dies als störend empfinden. Er sieht die Begründung darin, dass das unsicherste System dasjenige ist, das nicht benutzt wird - die Ursachen bei ungenutzten Sicherheitssystemem lägen häufig darin, dass sie zu verwirrend seien.

vorgegebene/erzwungene Passwortwechsel-Intervalle [And08] nennt als Konsequenz nach der Einführung von monatlich zu wechselnden Passworten eines Unternehmens, dass die Benutzer nacheinander so oft die Passworte änderten, bis die Historie (die Anzahl der nicht mehr zu verwendenden Passworte der Vergangenheit) erschöpft war und sie erneut ihr Favoritenpasswort auswählen konnten. Führte man monatliche Passwortwechsel ein und beschränkte die Anzahl der möglichen Passwortwechsel pro Zeiteinheit erhöhte dies die Anzahl der Rückfragen beim Help Desk respektive Administrator immens. [CMRW88] hat bereits 1988 vorgeschlagen auf studentischen Unix-Rechnern ein monatlich Passwortwechselintervall vorzugeben, kam jedoch zu dem Schluss, dass dies zu trivialeren Passworten führen würde. [KS08] gibt zu Bedenken, dass bei Zwangswechseln oft nicht nur teure Helpdesks einzurichten oder Fallback-Mechanismen einzubauen sind[13], deren Sicherheitseinschätzung ebenfalls kritisch zu betrachten ist.

zu viele Passworte Laut [AS99] reduziert die steigende Anzahl von zu merkenden Passworten deren Erinnerbarkeit und erhöht unsichere Arbeitspraktiken, wie das Niederschreiben. Die Passwortabfragen unterbrechen die Arbeitsabläufe und werden als störend empfunden. [GJ11] bemängelt weiterhin, dass die kontinuierlich steigende Anzahl von Online Accounts zu ebenso stark steigenden Passwort-Anzahlen führt, jede Passwortrichtlinie an sich jedoch keine Rücksicht darauf nimmt, dass der Nutzer sich auch weitere Passworte merken muss - diese sollten nicht nur Schutz vor Bedrohung sicherstellen, sondern auch die Verwendung multipler

[13] Fallback-Mechanismen bezeichen die Möglichkeit, das eigene Passwort ohne Zuhilfenahme Dritter durch z.B. Sicherheitsfragen auf ein neues Passwort zu ändern oder auf ein neues Initialpasswort zurückzusetzen.

Passworte berücksichtigen. [TS10] führt an, dass über 60 Prozent von Mitarbeitern sich ihre Passworte regelmäßig notieren.

Password Sharing Laut [MS08] ist es gängig, dass z.B. Sekretärinnen die Passwörter Ihrer Chefs wissen, um auch in dessen Abwesenheit wichtige Aufgaben übernehmen zu können, die Zugriff auf dessen Daten erfordern. [Kay] befragte 126 Probanden, ob diese ihr(e) Passwort(e) mit anderen Personen teilen würden - obwohl die Umfrage nach Meinung des Autors nicht representativ ist ergab sich, dass verheiratete oder in einer Beziehung lebende Personen durchschnittlich 2,8 Passworte mit dem Partner teilten, wohingegen nur 1,4 Passworte von Alleinstehenden geteilt wurden. Das Teilen von Passworten innerhalb einer Familie ist ebenso gängig wie das Teilen innerhalb von Freundeskreisen, z.B. für zeitlich begrenzten Zugang oder generell gemeinsame Nutzung von kostenpflichtigen Diensten. Unter Kollegen werden Passworte ebenfalls geteilt, zum Zweck der Vereinfachung von Arbeitsabläufen.

mangelhafte Passwortrichtlinien Passwortrichtlinien sind Leitsätze die ein Passwort erfüllen muss, um vom System akzeptiert zu werden. Oft sind diese in Unternehmen bereits in gekaufter Software vorimplementiert. Als Beispiel hierzu führe ich die Kennwortrichtlinie der SAP an, die öffentlich einsehbar ist (siehe Tabelle 4.2). Hier wurden zwar bereits Anpassungen vorgenommen um Passworte sicherer zu gestalten, indem z. B. die maximal mögliche Passwortlänge verändert wurde, doch lässt sich z.B. ohne weiteres ein Passwort wählen, das abcd 01 lautet. Dadurch, dass sich das neue Passwort im Standardfall nur um ein Zeichen vom vorherigen Passwort unterscheiden muss, kann der Nutzer sein Standardpasswort durch simple Zahlenvariation (mit z.B. der Monatsangabe) gezielt wählen, ohne sich stets neue Passworte zu merken. Nur durch Veränderung der Vorgaben durch einen Administrator kann die Passwortrichtlinie sicherer gestaltet werden. Wird dem Benutzer also vorgegeben, sein Passwort auf eine gewisse Weise auszuwählen und die Passwortrichtlinie geht mit diesen Informationen nicht konform kann der Benutzer diese Lücke ausnutzen, wodurch es zu schwächeren Passworten kommen kann (vgl. [ASL97],[IS10]).

Industriespionage [MS08] berichtet davon, wie sich eine verärgerte Mitarbeiterin an ihrer Firma rächt, in dem sie interne Firmeninformationen nutzt, um sich zu Zugang zu sensiblen Daten zu schaffen, die sie dann an die Presse verkauft. Nach [Sch01] versuchen Unternehmen auf vielfältige Weise, diesem Risiko entgegenzuwirken, z.B. durch Integritätsprüfungen der einzustellenden Personen oder der Verteilung von Vertrauenspositionen zur Reduzierung von anzurichtendem Schaden durch eine Einzelperson.

Regel	Kommentar
Das Kennwort ist mindestens 3 Zeichen lang.	Mit Profilparameter [...] änderbar
Das Kennwort ist höchstens 40 Zeichen lang. Bis einschließlich SAP NetWeaver 6.40 waren Kennwörter höchstens 8 Zeichen lang.	Im SAP-System vordefiniert
Bis einschließlich SAP NetWeaver 6.40 können alle Zeichen des syntaktischen Zeichensatzes verwendet werden, also alle Buchstaben, Ziffern und einige Sonderzeichen, und es wird nicht zwischen Groß- und Kleinschreibung unterschieden. Nach SAP NetWeaver 6.40 können beliebige Unicode-Zeichen in Groß- und Kleinschreibung verwendet werden.Ab SAP Web AS 6.10 kann der Administrator vorgeben, wie viele Ziffern, Zeichen und Sonderzeichen neue Kennwörter enthalten müssen (siehe Profilparameter).	Mit Profilparametern [...] änderbar.
Die ersten drei Zeichen dürfen nicht in derselben Reihenfolge in der Benutzerkennung vorkommen. Keines der ersten drei Zeichen darf ein Leerzeichen sein. Die ersten drei Zeichen dürfen nicht identisch sein.	TEST
Das Kennwort darf nicht auf einer Liste nicht zulässiger Kennwörter stehen (Tabelle USR40).	Änderbar. Als Voreinstellung sind nur die Kennwörter PASS und SAP* von der Verwendung ausgeschlossen
Das Kennwort darf nicht mit den letzten x Kennwörtern des Benutzers identisch sein, wenn der Benutzer es selbst ändert. Bis einschließlich SAP NetWeaver 6.40 war die Kennworthistorie fest auf den Wert 5 gesetzt. Nach SAP NetWeaver 6.40 kann der Administrator die Größe der Kennworthistorie festlegen (bis zu 100 vom Benutzer gewählte Kennwörter).Der Administrator kann das Kennwort eines Benutzers auf ein beliebiges Initialkennwort zurücksetzen, somit auch auf eines der letzten x Kennwörter dieses Benutzers. Das ist erforderlich, da der Administrator die Kennwörter des Benutzers nicht kennen soll. Bei der ersten interaktiven Anmeldung wird der Benutzer aufgefordert, das Initialkennwort zu ändern.	Mit Profilparameter [...] änderbar.
Benutzer können ihr Kennwort erst nach einer Wartefrist erneut ändern. Bis einschließlich SAP NetWeaver 6.40 betrug die Wartefrist einen Tag. Ein vom Benutzer geändertes Kennwort konnte erst am nächsten Tag erneut vom Benutzer geändert werden. Nun kann das System alle Kennwortänderungen während der Wartefrist (Einheit: Tage) abweisen. Wenn der Administrator das Benutzerkennwort ändert, muss der Benutzer dieses Initialkennwort bei der Neuanmeldung ändern, unabhängig davon, wann er zuletzt sein Kennwort geändert hatte.	Mit Profilparameter [...] änderbar. Der Administrator kann das Kennwort weiterhin beliebig oft ändern.

Tabelle 4.2.: Auszüge aus der Passwortrichtline der SAP [SAP12]

Kosten- und Nutzenrechnung des Benutzers zur Sicherheitseinschätzung [SFH09] stellt fest, dass Benutzer eine implizite Kosten/Nutzenrechnung durchführen, ob sie einem Sicherheitsratschlag folgen - oder nicht. Während die Kosten den Aufwand dem Rat zu folgen entsprechen, ist die Vermeidung eines zu erwartenden Schadens (z.B. eines finanziellen Verlusts oder die Zeit und der Aufwand irrtümliche Bankbelastungen nach einem Angriff mit der Bank zu klären) der Nutzen. Damit ein Benutzer ein eventuelles Risiko besser bewerten kann müssen die tatsächlichen Fakten, z.B. die Anzahl der Opfer eines beliebigen Angriffes, entsprechend dokumentiert sein. Weiterhin sollten die Kosten für Sicherheitsmaßnahmen (und somit auch die Zeit, die der Nutzer hierfür aufwenden muss) in Relation zur Anzahl betroffener Personen stehen und die Sicherheitsmaßnahmen auf die Benutzer ausgerichtet sein, um unnötige

Information zu vermeiden. So kann der Benutzer zu einer positiven Sicherheitseinschätzung gelangen.

Den psychologischen Hintergrund für diese menschliche Handlungsweise kann man sowohl in der Feldtheorie nach Lewin, als auch in der Erwartungs-Wert-Theorie von Heckhausen und Heckhausen sehen (siehe Kapitel 3.2, Einflussfaktoren auf Handlungen). Beide Ansätze zur Motivation, Handlungen auszuführen, helfen die Sicherheitseinschätzungen von Benutzern nachzuvollziehen und sie gegegebenfalls zu modifizieren.

4.4. Maßnahmen zur Erhöhung der Sicherheit von Passworten

Wie im vorangegangenen Kapitel festgestellt ist die Bedrohung der IT-Sicherheit durch den Menschen als schwächstes aber wichtigstes Glied der Sicherheitskette groß - Unternehmen haben hier einen starken Handlungsbedarf. Klassische Sicherheitsmaßnahmen haben stets einen technischen Ansatz - die Möglichkeiten reichen von Verschlüsselungsmaßnahmen über Firewalls bis zur Anwendung klassischer Kryptographie. Für „human-based risks“ gelten jedoch andere Maßstäbe.

4.4.1. Kriterien zur Passwortwahl und -verwendung

Verschiedenste Quellen ([Eck12, Sta06, MS08, VPBS+07]) stimmem darin überein, zur Erhöhung der Passwortsicherheit einige Kriterien bei der Passwortwahl mit einzubeziehen. Diese Anforderungen gelten nur dann, wenn der Benutzer die Möglichkeit hat sein Passwort selbst auszuwählen. Nach [Eck12] steht und fällt die Sicherheit einer Passwortverwaltung mit der Wahl der Passworte und mit dessen Umgang ausserhalb des technischen Systems, woraus sich nachfolgende Kriterien ergeben:

- **Mindestlänge 8 Zeichen und kein zusammenhängendes Wort aus einem Wörterbuch** Die Mindestlänge des Passwortes orientiert sich an der Zeit, die man benötigt es mittels einer Brute Force-Attacke zu kompromittieren (siehe auch Tabelle 4.3). Es gilt: je länger die Zeichenzahl, desto sicherer ist das Passwort unter Berücksichtigung der weiteren Kriterien. Ein Begriff, der - ohne Berücksichtigung der Groß- und Kleinschreibung - in einem Wörterbuch zu finden ist kann leicht anhand einer Dictionary-Attacke ermittelt werden und ist somit unsicher.
- **kein/e Eigenname/n oder der eigene Vor- oder Nachname** Der eigene Name, der von Familienmitgliedern, Lebenspartnern oder Freunden kann durch Dritte leicht in Erfahrung gebracht werden (vgl. Kapitel 4.3.1) und ist deshalb keine sichere Grundlage für ein Passwort, auch nicht in Verbindung mit z.B. einer Ziffer.
- **enthält mindestens ein Sonderzeichen** Sonderzeichen erhöhen die möglichen Permutationen, aus denen ein Passwort bestehen kann. Je mehr Permutationen möglich sind, desto höher ist der Rechenaufwand bei z.B. einer Brute Force-Attacke und desto geringer die Wahrscheinlichkeit, dass das Passwort gehackt wird.
- **ist keine auf der Tastatur nebeneinander liegende oder im Alphabet aufeinander folgende Zeichenfolge** Diese Variante ist zwar leicht erinnerbar, aber auch sehr

naheliegend zu erraten - es gelten die selben Gründe wie bei zusammenhängenden Wörtern.

- **soll in regelmäßigen Abständen geändert werden** Je länger ein Passwort unverändert bleibt, desto höher ist die Wahrscheinlichkeit, dass es kompromittiert werden konnte. Wird das Passwort häufig gewechselt lässt sich das Risiko, dass ein Passwort unbemerkt mißbräuchlich verwendet wird, deutlich senken (vgl. [AS99]), und sollte es bereits passiert sein, wird dem Angreifer nun der Zugang verwehrt.

- **Der Systemdienst der Zugangskontrolle sollte frühzeitig überprüfen ob das benutzergewählte Passwort gegen die oben genannten Anforderungen verstösst** Wie bereits unter 4.3.2/Passwortrichtlinien genannt bietet heute fast jede kommerzielle Software anpassbare Tabellen, in denen unzulässige Passworte gespeichert werden können, damit der Benutzer sie nicht auswählen kann. Hier ist der Administrator gefragt, damit die Tabelle immer auf dem Laufenden ist und als unsicher bekannte Passworte sofort abgelehnt werden (z.B. die Passworte aus Abbildung 4.1).

- **das System sollte nur eine geringe Anzahl an Fehlversuchen beim Anmeldevorgang akzeptieren und den Zugang sonst sperren** Brute Force- oder Dictionary-Angriffe zielen darauf ab, möglichst viele verschiedenen Permutationen oder Wörter einer Länge in kurzer Zeit „auszuprobieren“. Hier greift eine Fehlversuchssperre ein und beschränkt die Anzahl der Möglichkeiten. Die Entsperrung kann in der Regel nur ein Administrator vornehmen - wichtig ist nun, dass das durch diesen neu vergebene Passwort, das meist trivial ist, umgehend individualisiert wird, um Mißbrauch zu vermeiden.

- **keine Mehrfachverwendung von Passworten** Wird ein Passwort kompromittiert erhält der Angreifer Zugriff auf alle Logins für die das Passwort (auch mit geringfügigen Variationen wie einer angehängten Ziffer) gilt. Die Sicherheit lässt sich nur dann gewährleisten, wenn alle verwendeten Passworte sich voneinander unterscheiden.

- **Geheimhaltung** Ein Passwort sollte stets geheim gehalten werden - dies schließt nicht nur das Mitteilen gegenüber anderen mit ein, sondern auch das schriftliche Notieren auf Zetteln am Schreibtisch oder im Portemonnaie, da diese gelesen, kopiert werden oder verloren gehen können. Sicherheit kann in Mobiltelefonen oder in (unverschlüsselten) Dateien auf dem eigenen Computer ebenfalls nicht gewährleistet werden, denn hier liegt das Hauptrisiko im Missbrauch durch Dritte, die sich unerlaubt Zugriff verschaffen.

4.4.2. Messbarkeit von Stärke und Qualität

Ein logischer Ansatz zur Sicherstellung von sicheren Passworten ist die Messung deren Stärke, dies ist aber eine komplexe Aufgabe. Eine einfache Möglichkeit ist, die Anzahl der möglichen Permutationen in Bezug auf die Passwortlänge (Permutationen = Zeichenanzahl $^{\text{Passwortlänge}}$) zu betrachten. Unter der Voraussetzung, dass ein Computer alle Permutationen innerhalb einer Brute Force-Attacke ausprobiert und erst das letzte Ergebnis dem gesuchten Passwort entspricht, ergeben sich, abhängig von der Rechenleistung des Computers, zeitliche Rahmen, in denen das Passwort kompromittierbar ist (siehe Abbildung 4.3[14]).

Zahlen \ Passwortlänge	5	7	9	15
Kombinationen	100.000,00000	10.000.000,00000	1.000.000.000,00000	1.000.000.000.000.000
max. Zeit in s	0,00005	0,00477	0,47705	477.053
max. Zeit in Tagen				5,52
Kleinbuchstaben (26 Zeichen)				
Kombinationen	11.881.376	8.031.810.176	5.429.503.678.976	1.677.259.342.285.730.000.000
max. Zeit in s	0,00567	3,83160	2.590	800.141.122.825
max. Zeit in Tagen			0,03	9.260.892,63
max. Zeit in Jahren				25.372,31
Groß- u. Kleinbuchstaben (52 Zeichen)				
Kombinationen	380.204.032	1.028.071.702.528	2.779.905.883.635.710	54.960.434.128.018.700.000.000.000
max. Zeit in s	0,18138	490,00000	1.326.162	26.219.024.312.714.200
max. Zeit in Tagen			15,35	303460929545,30
max. Zeit in Jahren				831.399.806,97

Abbildung 4.3.: Benötigte Zeit, um mittels einer Brute-Force-Attacke Passwörter zu kompromittieren

Die horizontale Spalte gibt die Passwortlänge an, die vertikale die Zusammensetzung des Passwortes sowie dessen maximal benötigte Kompromittierungsdauer bei einer Brute-Force-Attacke. Aus der Abbildung geht hervor welche Unterschiede sich bei der Verwendung von numerischen und alphabetischen Zeichenketten ergibt. Ist ein Passwort mit 5 Zeichen aus Ziffern bereits in 0,0004 Sekunden zu entschlüsseln, sind es bei Groß-/Kleinbuchstaben bereits 0,00567 Sekunden. Ein lediglich vier Zeichen längeres Passwort benötigt 2.590 Sekunden (43,17 Minuten), wenn es aus Kleinbuchstaben besteht - bei Groß- und Kleinbuchstaben 1.326.162 Sekunden, also 15,35 Tage. Ein durchschnittliches Passwort aus 9 Zeichen kann somit je nach Zeichenwahl des Benutzers mit einem handelsüblichen Computer in einem Zeitraum zwischen

[14] Quelle: `http://www.1pw.de/brute-force.html`, angenommene Rechenleistung: 2.096.204.400 Schlüssel pro Sekunde

0,477 Sekunden (nur Zahlen) und 47 Tagen (Groß-/Kleinschreibung, Zahlen[15]) entschlüsselt werden.

Eine weitere „Qualitätsmessungs-“ Maßnahme findet man auf diversen Internetseiten, beispielsweise während eines Registrierungsprozesses: sogenannte Password Strength Meter (siehe Abbildung 4.4). Hierbei ist zu beachten, dass diese Programme nicht die tatsächliche Qualität oder Stärke eines Passwortes messen (können), sondern lediglich angeben, wie sehr sich der Nutzer bereits an die vorgegebenen Richtlinien gehalten hat. Es handelt sich hiermit also um eine Maßnahme die dem Nutzer Sicherheit vermitteln soll - das Passwort kann hier nur so stark sein wie die vorgegebene Richtlinie. Im Gegenzug zum proaktivem Passwort-Checking (siehe Unterkapitel 4.4.4) findet kein Abgleich des Passwortes mit einem Wörterbuch unerwünschter Passworte statt.

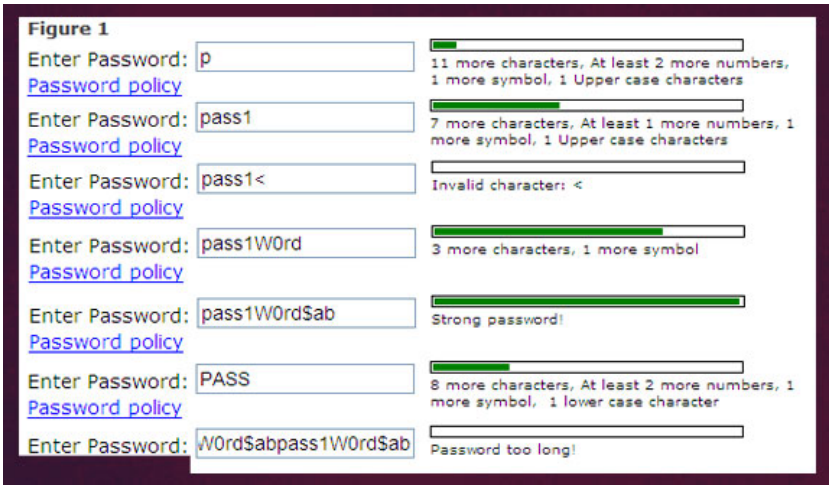

Abbildung 4.4.: Beispiel eines Password Strength Meters

Eine weitere, verwendbare Meßgröße der Passwortsicherheit ist die **Entropie**. Entropie bezeichnet im eigentlichen Sinn den mittleren Informationsgehalt einer Nachrichtenquelle, deren Nachrichten mit der Wahrscheinlichkeit ihres Auftretens gewichtet und aufsummiert werden [Eck12]. Um die Stärke bzw. Schwäche eines Passwortes mittels Entropie zu ermitteln wird die Häufigkeitsverteilung einer Sprache betrachtet und mit einem Markov-Prozessmodell (einem stochastischen Verfahren zur Prognose der Wahrscheinlichkeit von zukünftig eintretenden Ereignissen[16]) verknüpft. [MCTK] bestreitet die Sinnhaftigkeit mit der Begründung, dass sich

[15] die Kombination aus Groß-/Kleinschreibung und Ziffern ist nicht in Abbildung 4.3 enthalten, kann aber einfach rekapituliert werden: $(62 Zeichen^{9 Zeichen})$/Rechenleistung

[16] `http://www.mathematik.uni-ulm.de/stochastik/lehre/ss03/markov/skript/node3.html`

Passworte nicht an eine Häufigkeitsverteilung halten, da es sich nicht um Worte zum Kommunikationszweck handelt. Weiterhin sei das Erraten von Passworten kein Markovscher Prozess, da das Erraten des $i+1$-ten Zeichens nicht vom i-ten abhänge. Schließlich sei die Entropie des Erratens (guessing entropy) lediglich eine Untergrenze für die Anzahl der notwendigen Rateversuche für Passworte, aber kein Indikator für deren Qualität. Als Alternative entwickelte [MCTK] einen **Password Quality Indicator (PQI)**, der die Qualität eines Passwortes daran misst, wie sehr sich das Passwort von einem Wörterbucheintrag unterscheidet, wie lang es ist und wie groß der Umfang der verwendeten Zeichen ist. Die Verwendung des PQI hat sich bisher nicht durchgesetzt.

> „The PQI of a password is a pair $\lambda = (D, L)$, where D is the Levenshtein's editing distance (Levenshtein, 1965) of the password to the base dictionary words, and L is the effective password length." Ma, Campbell et. al. [MCTK, S. 584]

Mittlerweile hat sich der Ausdruck „schwaches" bzw. „starkes" Passwort stets in dem Zusammenhang durchgesetzt, wie schnell es durch Dictionary- oder Brute Force-Angriffe zu kompromittieren ist. Es gibt zum aktuellen Zeitpunkt keinen zufriedenstellenden Ansatz, die Qualität oder Stärke eines Passwortes zu messen.

4.4.3. Alternativen zum herkömmlichen Passwort

[AS99] stellte bereits heraus, dass benutzergewählte Passworte meist nicht den gängigen Sicherheitskriterien entsprechen und als sicherer erachtete, systemgenerierte Passworte durch den Nutzer abgewertet werden, indem sie notiert werden. Die Herausforderung liegt darin, die menschlichen Eigenheiten mit bestehenden Sicherheitskriterien zu vereinen und herkömmliche Passworte zu ersetzen.

mnemonische Passworte Leichter erinnerbare, automatisch generierte Passworte sind sogenannte mnemonische (mnemonisch kommt aus dem griechischen (mnemikos) und bedeutet „ein gutes Gedächtnis habend") [17] Passworte. Mnemonische Passworte stehen als Oberbegriff für einfach ableitbare oder merkbare Passworte und wird z.B. für Passworte verwendet, die „aussprechbar" sind. Es häufen sich z.B. Passwortgeneratoren für Konstrukte, bei denen sich Konsonanten und Vokale zu je 50 Prozent abwechseln um ein aussprechbares Passwort[18] zu bilden, das besser memorisierbar sein soll. Diese sind jedoch abhängig von der Zeichenauswahl genauso sicher wie herkömmliche.

[17] `http://www.duden.de/rechtschreibung/mnemonisch`
[18] Beispiele eines mnemonischen Passworts: „halebixu", „jilacoka", etc.

Passphrasen, Passphrasen-basierte und mnemonische, Passphrasen-basierte Passworte Eine Passphrase ist eine Folge von einzelnen Worten, die ohne Leerzeichen aneinandergereiht, idealerweise in Kombination mit Sonderzeichen oder Ziffern statt einem Passwort verwendet wird. Um die Passphrase besser erinnerbar zu gestalten soll der Benutzer ein Zitat, einen Spruch oder einen sonstigen, ihm selbst gut geläufigen Satz verwenden und diesen dann, gegebenenfalls abgekürzt oder ergänzt verwenden (z.B.: „DerHundrennttumdenBaum“). Hierdurch entstehen Passworte, die schnell länger als 8-12 Zeichen werden.

Als Variante hierzu wird oft geraten, nicht die vollständige Phrase, sondern nur deren Anfangsbuchstaben zu verwenden (analog zum vorgenannten Beispiel: „dHrudB“). So entstehen passphrasen-basierte Passworte, die durch die Aneinanderreihung von Begriffen entstehen und wie eine Eselsbrücke fungieren. [KRC06] empfiehlt hierfür folgende Vorgehensweise:

1. Denke an einen erinnerbaren Satz oder eine Phrase, die mindestens sieben bis acht Wörter enthält
2. Wähle einen Buchstaben, eine Ziffer oder ein Sonderzeichen um jedes Wort im Passwort zu repräsentieren.
3. Im Idealfall sollte das Passwort eine Mischung aus Klein- und Großbuchstaben, Zahlen, Interpunktion und Sonderzeichen enthalten.
4. Erinnere dich an die Phrase.

Die Begründung, warum diese Passwortart stärker als herkömmliche selbstgewählte Passworte seien liegt laut [KRC06] darin, dass diese nicht in Passwort-Wörterbüchern vorkommen, sie dem Benutzer dabei behilflich sind, unterschiedliche Zeichenarten in ihrem Passwort unterzubringen und die Anzahl der möglichen Passphrasen unendlich ist.

Eine Untersuchung von Studenten der Carnegie Mellon University [KRC06] wandte sich an insgesamt 290 Studenten ab 18 Jahren, die mindestens fünf passwortgeschützte Webseitenzugänge haben und mindestens einen Onlinekauf getätigt hatten, um benutzergewählte Passworte mnemonischen, Passphrasen-basierten Passworten (Definition siehe 4.4.3) gegenüberzustellen. In einem umfangreichen Fragebogen wurden die Passwortgewohnheiten der Studenten erfragt - eine Gruppe erhielt Empfehlungen zur sicheren Passwortwahl, die andere konnte ihr Passwort frei wählen. Die Untersuchung basierte auf drei Methoden: einer klassischen Dictionary-Attacke (Grundlage: Wörterbuch mit 1,2 Millionen Einträgen und ein für diesen Zweck erstelltes „mnemonisches Wörterbuch“ mit 400.000 Einträgen), einer Dictionary-Attacke unter Verwendung von John the Ripper[19] und einer Brute Force-Attacke. Die Auswertung

[19]John the Ripper ist ein Password Cracker für diverse Betriebssysteme. Erhältlich unter: `http://www.openwall.com/john/`

ergab: während 11 Prozent der benutzergewählten Passwörter mittels John the Ripper kompromittiert werden konnten wurden nur vier Prozent der mnemonische Passphrasen-basierte Passwörter aufgedeckt. Bei der Brute Force-Attacke lagen die Ergebnisse bei acht Prozent der klassischen und wiederum vier Prozent der mnemonischen Passworte. Zusammenfassend ergibt die Studie, dass mnemonische Passphrasen-basierte Passworte nur dann Sinn machen, wenn diese nicht auf Phrasen öffentlicher Herkunft (wie Literatur, Musik- und Filmtitel und -Zitate) zurückzuführen sind. Hieraus folgt der Schluss, dass nicht lediglich die Anwendung einer Passphrasentechnik zu einem starken Passwort führt, sondern wie auch bei anderen Passworten auf Richtlinien zu achten ist. Dies bestätigt [BS12] bei seiner Untersuchung der Sicherheit von „PayPhrases“, einer nur in den USA verwendeten Authentifizierungsmöglichkeit des Online-Versandhauses Amazon, bei dem der Nutzer sich durch die Wahl von zwei und mehr durch Leerzeichen getrennte Worte authentifiziert. [YBAG04] konnte in seiner Studie jedoch unabhängig davon untermauern, dass mnemonische Passworte genauso leicht erinnert werden wie selbstgewählte.

Im Zusammenhang mit mnemonischen Passworten wurde Google 2011 durch seine großangelegte Aktion zur Verbesserung der Passwortsicherheit populär, in der das Unternehmen zur Verwendung von Passphrasen-basierten Passwörtern riet (siehe [Goo11]). Es stellte sich heraus, dass gerade das von Google angeratene Passwort „2bon2btitq“, basierend auf dem Hamlet Zitat “To be or not to be, that is the question” schwächer als das des durchschnittlichen Google Benutzers ist. Dies basierte jedoch nicht auf der Tatsache, dass es sich um Passphrasen-basiertes Passwort handelt, sondern daran dass das Zitat sehr vielen Menschen bekannt ist und in der oben genannten Variante verwendet wird.

Einmal-Passworte Zusätzlich zu den bereits genannten Passwortarten gibt es einmalbenutzbare Passworte (One Time-Password (OTP)[20]), die auf dem S/Key-Verfahren[21] beruhen. Nach [Eck12, Poh03] ist S/Key ein Challenge-Response-Verfahren, vorrangig für entfernte Client-Server-Architekturen konzipiert und verwendet die One-Way-Hashfunktion „MD4“. Weitere Informationen sind im Anhang zu finden (siehe Anhang A).

Für OTPs gilt genau wie für herkömmliche Passworte: wird das Geheimnis s kompromittiert kann auch der Server keine Sicherheit mehr gewährleisten. Bei „beweglichen“ Passwortgeneratoren bedeutet der Verlust des Besitzes den Verlust des Geheimnisses.

[20] OTP ist unter dem Rfc1938 standardisiert
[21] S-Key ist ein Trademark der Firma Bellcore und unter Rfc1760 standardisiert

4.4.4. Proaktives Passwort-Checking

Proaktives Passwort-Checking bezeichnet die Vorabüberprüfung der Gültigkeit eines Passwortes im Rahmen von vorgegebenen Passwortrichtlinien. Anwendung findet dies heute bei vielen gängigen Internet-Registrierungsvorgängen (siehe auch Abbildung 4.5) und prüft in der Regel die Länge des Passwortes und das Vorhandensein von Groß- und Kleinschreibung, Zahlen oder Sonderzeichen. [RGT+] bestätigt, dass die Richtlinien nicht so streng vorgegeben werden wie sie sollten (vgl. Kapitel 4.4.1, Maßnahmen zur Erhöhung der Sicherheit von Passworten) um den Benutzer nicht zu verschrecken und bezeichnet dies als Zielkonflikt zwischen der gewünschten Sicherheit und der Benutzerfreundlichkeit.

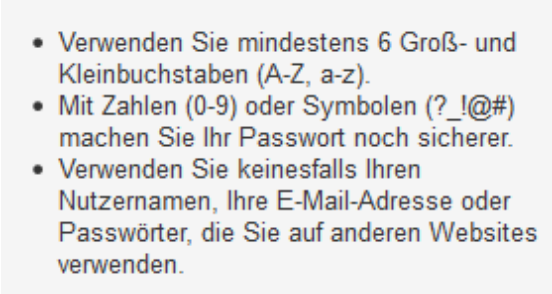

Abbildung 4.5.: proaktives Passwort-Checking bei einer Ebay-Neuanmeldung

Analog zu einem Dictionary-Angriff prüft das proaktive Passwort-Checking das Passwort nicht nur auf die vorgegebenen Kriterien, sondern gleicht es mit einem internen Wörterbuch (und den Permutationen der Einträge) ab. Da die Überprüfung in Echtzeit erfolgt ist die Größe der Wörterbuch-Datei ebenso relevant wie das effiziente Suchen darin. Bergadanos Eigenentwicklung ProCheck, ein Lernalgorithmus der gute von schlechten Passworten unterscheiden soll und auf Entscheidungsbäumen basiert, besitzt die schnellste Überprüfungsgeschwindigkeit und die beste Datenkompressionsrate (vgl. [GJN+]). [RGT+] stellt jedoch heraus, dass alle zum Überprüfungszeitpunkt 2001 existierenden Passwort-Checker Passworte mit niedriger Entropie (z.B. 12345abc) nicht erkannten, da Passworte, die nicht Teil des Wörterbuchs waren automatisch als sicher eingestuft oder ignoriert wurden.

Der Autor analysierte bei Passworten bis zu sieben Zeichen diejenigen, deren Entropie niedrig war. Er kommt zu dem Schluss, dass genau diejenigen, die aus mehr als fünf Ziffern und diejenigen, die fünf bis sieben Zeichen enthielten und ein Zeichen mehr als drei- bzw. zwei und mehr Zeichen mehrmals enthielten, eine niedrige Entropie haben müssen. Um die gängigen proaktiven Passwort-Checker aufzuwerten bietet er an, den herkömmlichen Algorithmus um

einen Entropie-basierten, simplen Algorithmus zu ergänzen, der ebendiese Kategorien von vornherein blockiert.

4.4.5. Sicherheitsrichtlinie - Security Policy

Eine Security Policy ist eine Dokumentation einer Sicherheitsstrategie, die durch die Leitungsebene eines Unternehmens festgelegt und durch ein Managementsystem für Informationssicherheit (ISMS) gelenkt wird. Sie enthält die Kernaussagen zu Sicherheitszielen und strategischen Vorgaben und beinhaltet mindestens:

- Sicherheitsziele der Behörde oder des Unternehmens,
- Beziehung der Sicherheitsziele zu den Geschäftszielen oder Aufgaben der Institution,
- angestrebtes Sicherheitsniveau,
- Leitaussagen, wie das angestrebte Sicherheitsniveau erreicht werden soll und
- Leitaussagen, ob und wodurch das Sicherheitsniveau nachgewiesen werden soll.

Ein für Informationssicherheit verantwortlicher Manager der obersten Leitungsebene wird zum Chief Information Security Officer (CISO), also Leiter der Informationssicherheit, benannt und ist gegenüber der Geschäftsführung berichtspflichtig (vgl. [Bun08]).

> “Die meisten Unternehmen bleiben leider beim ersten Satz stecken: "Wir haben die Security Policy geschrieben und ausgeteilt. Wir haben es „gesagt" und verstehen nicht, warum sich keiner daran hält".„ Klaus Schimmer [Sch07, S. 510]

Security Policies gelten als wichtige Grundlage in allen Sicherheitsbelangen, doch ist es die Aufgabe des Unternehmens, diese zu popularisieren und den Mitarbeitern als sinnvoll zu unterbreiten - z.B. durch Awareness-Maßnahmen. Nur dadurch kann die Sicherheit, insbesondere der Passworte, gewährleistet und verbessert werden. Für die Regularien, die Passworte betreffen, hat sich landläufig der Begriff Password Policy durchgesetzt.

4.4.6. Awareness und (Security) Awareness-Maßnahmen

Awareness wird oft als Gegenmaßnahme für Social Engineering-Angriffe genannt, bezeichnet jedoch klassisch den Begriff der Mitarbeitersensibilisierung in allen Sicherheitsangelegenheiten - die Mitarbeiter aller Hierarchieebenen sollen die Sicherheitsmaßnahmen, die in der unternehmensweiten Security Policy vorgegeben werden, an- und wahrnehmen und außerdem gegen äußere Beeinflussung immunisiert werden (vgl. [Weß08]). Als eine der ersten Awareness-Maßnahmen beschreibt [CMRW88] einen Password-Predictor - ein Programm das

in den späten 1980er Jahren nachts auf den Unix Rechnern der University of Western Ontario lief und Passworte per Dictionary-Angriff aufzudecken versuchte. Der Hinweis „Ihr Passwort ist nicht sicher“ wurde dem Benutzer nach erfolgreichem Guessing angezeigt und sollte diesen sensibilisieren, seine Passwortwahl zu überdenken.

Bei Awareness-Maßnahmen spielt Kommunikation (vgl. Kapitel 3.1) eine wichtige Rolle. Oft werden die Anweisungen zwar gehört, aber nicht verstanden und somit auch nicht angewendet, argumentiert [Sch07]. Ursache hierfür kann z.B. sein, dass die Security Policy zwar an die Mitarbeiter ausgegeben doch nicht erklärt, oder mißverständlich formuliert wurde.

[Weß08] führt an, dass reine Awareness-Maßnahmen nicht fruchten können, weil Social Engineering an sich nicht negativ ist (vgl. Kapitel 4.3.1). Weiterhin könnten viele klassische Awareness-Maßnahmen nur Wissen vermitteln, das Verhalten der Mitarbeiter aber nicht ändern.

[Sch07] sieht als Sicherstellungmethode einen Drei-Punkte-Plan vor:

- **Motivation**: Maßnahmen zur Erhöhung der Sicherheit sollen weder Bremse noch Behinderung sein, sondern den Erfolg jedes einzelnen Mitarbeiters schützen.
- **Information**: jeder Mitarbeiter benötigt generelle Informationen über Gefahren und Richtlinien, um eventuelle Bedrohungen wahrzunehmen, korrekt einzuschätzen und an den richtigen Ansprechpartner weiterzugeben.
- **Sensibilisierung**: nur überzeugte Mitarbeiter arbeiten aktiv an der Umsetzung der Maßnahmen mit - die tägliche Informationsflut macht die Einschätzung von relevanten Informationen schwieriger und von Natur aus risikobereite Managementebenen müssen von der Gegenwärtigkeit von Bedrohungen überzeugt werden.

In einer Awareness Kampagne soll das Produkt „IT-Sicherheit“ dann nach der AIDA-Formel[22] wie in einer Werbekampagne gegenüber den Mitarbeitern vermarktet werden. Hier stehen Kreativität und eine gute Zeitplanung zunächst im Vordergrund, doch ist die Wahl des Kommunikationsmittels ebenso relevant wie die Unterstützung von Geschäftsführung und Management.

Klaus Schimmer als Kommunikationsspezialist der SAP beschreibt die 2004 unternehmensweit durchgeführte Kampagne zur Sicherheitspolicy als erfolgreich, da jeder Mitarbeiter durch Poster, Spiegelaufkleber, Emails und Schulungen persönlich angesprochen wurde und sich mit den Zielen identifizieren konnte. (siehe Abbildung 4.6). [Weß08] sieht nur dann eine Chance für Awareness-Maßnahmen, wenn diese typisches menschliches Verhalten berücksichtigen und

[22] AIDA steht für attention, interest, desire, action

mit einbeziehen. Ein umfassender Schutz durch z.B. Verhaltenschecklisten in Unternehmen sei kaum machbar, da nicht alle möglichen Social Engineering Angriffe vorhersehbar seien.

Abbildung 4.6.: Postermotiv der SAP zur Sicherheitspolicy-Einführung [Sch08a]

An dieser Stelle setzt [BW07] an und fügt zu den bereits genannten Punkten Motivation, Information und Sensibilisierung noch die Themen Nachhaltigkeit und Ritualisierung hinzu. Die wiederkehrende Auseinandersetzung mit dem Thema Sicherheit und IT-Sicherheit soll sowohl selbstverständlicher als auch alltäglicher Teil der Kommunikationskultur sein, weiterhin sollen bestimmte Handlungsweisen bis zur Gewohnheit „eingeübt“ werden, um einen höheren Sicherheitsstandard zu bilden. Ein wiederkehrender „Security Cup“ holt die Mitarbeiter auf der emotionalen Ebene ab und animiert, nicht zuletzt durch die Mitwirkung der firmeneigenen Mitarbeiter, ebenso wie ein auf mehrere Wochen angelegtes interaktives IT-Wissenquiz mit Preisen, zur Mitwirkung. [Lar07] zeigt zusätzlich zwei weitere Punkte auf - Ganzheitlichkeit, also die Beteiligung aller Organisationseinheiten die Sicherheit zu verantworten haben, sowie die Zielgruppenorientierung unter Kostenaspekten: Design und Layout sollen professionell und ansprechend wirken, jedoch nicht den Eindruck erwecken „Sicherheit koste viel, bringe aber wenig“.

Zusammenfassend lässt sich herausstellen, dass die Ziele von Awareness-Maßnahmen zwar leicht zu formulieren, die Umsetzung ebendieser aber schwierig ist. Die Umsetzung variiert, abhängig von Unternehmensgröße und -art, jedoch ist ist die Erfolgsmessung von Awareness-Kampagnen genauso schwierig wie die Messung von Sicherheit an sich. Wie auch [MP07] bereits feststellt ist es wichtig, gewonnene Erkenntnisse aus einer Kampagne aufzugreifen und zu verwerten um nachhaltige Effekte zu erreichen und dass einmalige Aktionen nicht ausreichen, um das Sicherheitsbewusstsein der Mitarbeiter langfristig zu steigern.

Sicherheitskampagne - Checkliste	
Positive emotional-affektive Ansprache	sympathischen „Vermittler“ oder Kommunikationsweg für die Information schaffen
	Auf Augenhöhe der Mitarbeiter, ohne „Zeigefinger“ kommunizieren
	Konzentration auf das Wesentliche
	Fokus auf die wichtigsten Themen und Regelungen legen
	die Kampagne modular aufbauen und möglichst ein Thema je Themenmodul umsetzen
	eine klare Zielsetzung definieren
	messbare Erfolgsfaktoren festlegen
Nutzung eines kommunikativen Maßnahmenmixes	Alle Mitarbeiter durch die Geschäftsleitung und die Führungskräfte informieren sowie zusätzlich persönlich ansprechen
	Information mit etablierten Kommunikationsinstrumenten verzahnen
	interaktive Elemente in die Kommunikation sowie Push- und Pull-Mechanismen in die Kommunikation einbauen
	Mitarbeiter aktiv einbinden
	Information und Spassfaktoren verbinden um damit zu emotionalisieren und zu motivieren
	einen erkennbaren Nutzen für die Mitarbeiter darstellen
Einbindung der Führungskräfte	Managementunterstützung sichern
	Vorabinformation für die Führungsebene und die Mitarbeitergremien vorbereiten
	Versorgung der Führungskräfte mit zusätzlichem Informationsmaterial sicherstellen
	Klare Aufgaben für die Führungskräfte definieren entsprechend der Führungsverantwortung: Vorbild, Motivation und Kontrolle

Tabelle 4.3.: Checkliste relevanter Erfolgsfaktoren für die Planung und Umsetzung einer Sicherheitskampagne nach [BW07]

4.5. Thesenüberprüfung und Bewertung

These 4.5.1 *Erhöhen vorgeschriebene Passwortwechsel innerhalb fester Zeiträume (z.B. monatlich, dreimonatlich) die Passwortsicherheit?*

Zur Überprüfung der vorgenannten These ist die Literatur sehr spärlich. Einzig [AS99] nimmt in Ihrer Studie kurz darauf Bezug wie die Probanden darauf reagierten und überprüft Ihre Ergebnisse später erneut (vgl. [IS10]). [CMRW88] erwähnt dies lediglich in einem Satz, [SFH09] überprüft den Sinn von Passwortrichtlinien an sich. Wie bereits in Kapitel 4.4.1, Kriterien zur Passwortwahl und -verwendung genannt ist das Ziel von temporär zu wechselnden Passworten, die Sicherheit zu erhöhen indem das Passwort regelmäßig gewechselt wird. Sollte es bereits unbemerkt kompromittiert worden sein (z.B. durch Keylogging oder Phishing) würde dies den Zugriff stoppen und wieder einen sicheren Zustand herstellen - hierdurch wird aber nicht die Ursache für die Kompromittierung an sich behoben. [SFH09] stellt fest, dass ein

Passwortwechsel nur dann sinnvoll ist, wenn er unmittelbar zwischen der Kompromittierung und dem geplanten Angriff/Exploit erfolgt.

Die Last für den Benutzer, sich „starke“ Passworte auszudenken, diese zu erinnern und zudem für möglichst alle Accounts unterschiedliche Passworte zu verwenden, die nicht aufeinander aufbauen, ist hoch (vgl. [IS10]) - bereits 2009 besaß ein Durchschnitts-Benutzer 25 Accounts, für die er durchschnittlich 6,5 Passworte verwendet. [SFH09] kommt daher zu dem Schluss, dass jedes der Regularien für Passworte in Bezug auf Länge, Wörterbuch- und Zeichenverwendung, als auch Wechselhäufigkeit und Wiederverwendung unnötiger Aufwand für den Benutzer ist, weil es nicht vor Phishing und Keylogging schützen kann. Die Ursache für die Missachtung der Regularien durch den Benutzer sieht der Autor darin, dass der Nutzer keinen Nutzen in den Sicherheitsrichtlinien sieht. Es gäbe nur Worst Case Szenarien, aber keine „echten Bedrohungen“, die den Aufwand lohnen, sich mit der Sicherheit des eigenen Passwortes auseinander zu setzen. [FH11] unterstützt diesen Gedanken, indem er auch bei Angreifern eine Suche nach Effektivität belegt die zu deutlich weniger Angriffen führt, als de facto, aufgrund z.B. schlecht gewählter Passworte, möglich wären.

> „Strength and Change Frequency is the *wrong* focus.“ Inglesant, Sasse et al. [IS10, S. 9]

Es ergibt sich aus dem Kontext, dass vorgeschriebene Passwortwechsel in Kombination mit weiteren Passwortrichtlinien wie der Wahl von „starken“ Passworten und neuen Passworten, die erheblich von den vorherigen abweichen sollen, benutzerunfreundlich sind (vgl.[IS10]) und zu einem Kreislauf führen: der Benutzer wird gezwungen, sein Passwort zu wechseln, wird durch technische Maßnahmen abgehalten, ein schwaches Passwort zu wählen, im Falle des Vergessens wird das Passwort wieder zurückgesetzt und er wählt ein neues. [KS08] berichtet davon, dass neue Passwörter nach einem erzwungenen Passwortwechsel bereits nach „kurzer Zeit“ vergessen werden.

Als Lösungsvorschlag wird ein ganzheitlicher Ansatz von Passwortrichtlinien angedacht - diese sollen so flexibel sein, dass sie den Benutzer nur vor den Risiken schützen, denen er sich tatsächlich gegenüber sieht. [ZH99] stellte bereits 1999 fest, dass die Passwortwechselhäufigkeit von der subjektiven Einschätzung des Nutzers abhängt, wie sensibel die zu schützenden Daten sind.

Aus den bestehenden Referenzen abgeleitet komme ich zu dem Schluss, dass die oben genannte These falsifiziert werden muss. Durch den erzwungenen Passwortwechsel kann weder das Risiko von Dictionary- oder Brute Force-Attacken, Phishing oder Keylogging abgemildert werden. Die Sicherheit des Passwortes wird nur durch dessen Auswahl gewährleistet.

Sobald die Passwortrichtlinie erlaubt, minimal abweichende Passworte nach einem Wechsel zu verwenden, führt der Wechselzwang sogar zu schwächeren Passworten (vgl. [AS99]). Die negativen Effekte - Erhöhung des Risikos, das Passwort zu vergessen, stärkere Belastung des Benutzers, sich weitere, einzigartige Passworte zu merken und diese nicht wiederzuverwenden, nicht zu vergessen die Kosten, die für den Benutzerservice in IT-Abteilungen entstehen - überwiegen und können als eine Ursache für das (unbeabsichtigte oder beabsichtigte) Aushebeln von Security-Policies betrachtet werden. Nur wenn der Benutzer selbst die zu schützenden Daten als sensibel und wichtig einordnet wird er sein Passwort angemessen auswählen und entsprechend oft wechseln, beobachteten [ZH99] und [GJ11]. Die zukünftige Aufgabe der Sicherheitsverantwortlichen liegt somit darin, die Nutzer durch entsprechende Motivation, z.B. durch Awarenessmaßnahmen, zur Wahl sicherer Passworte anzuhalten.

5. Sicherheit von passwortbasierten Authentifikationssystemen

Kapitel 2.2 beleuchtete bereits den Sicherheitsbegriff in Bezug auf IT-Systeme. Das Augenmerk dieser Arbeit liegt jedoch auf der Sicherheit von passwortbasierten Authentifikationssystemen, sodass zunächst relevante Definitionen erfolgen. Abstrahiert von der Gesamtheit passwortbasierter Authentifikationssysteme werden Single Sign-On-Systeme betrachtet, definiert sowie klassifiziert. Stellvertretend für alle verwendbaren Technologien erfolgt die Vorstellung von Kerberos sowie dessen Sicherheitsbewertung. Abschließend wird die These „erhöhen Authentifikationssysteme die Sicherheit?“ am Beispiel von Kerberos überprüft.

5.1. Definition Authentifikation

Authentifikation bezeichnet den Nachweis von Authentizität zwischen Benutzern, Prozessen oder Systemen (siehe Kapitel 2.2.1, vgl. [SPS11]). Je nach Quelle wird Authentifikation auch als Authentifizierung bezeichnet.

Nach [Sta06] erfolgt eine Authentifikation durch eine von drei Techniken (oder deren Kombinationen, siehe auch Anhang B):

- Etwas, dass man weiß (z.B. ein Passwort)
- Etwas, dass man besitzt (z.B. eine SmartCard)
- Etwas, dass man ist (z.B. biometrische Eigenschaften wie ein Fingerabdruck)

Im Rahmen dieser Arbeit wird die Authentifikation durch Wissen, im Speziellen durch Passworte (in Abgrenzung zur Authentifikation mit Hilfmitteln oder mittels biometrischer Merkmale) betrachtet.

Man unterscheidet zwischen einseitiger und gegenseitiger Authentifikation:

Bei der **einseitigen Authentifikation** (engl. *peer identity*, Abbildung 5.1) authentisiert sich Alice gegenüber Bob, indem sie ihre Identität beweist. Man bezeichnet Alice auch als *prover* (engl., der Beweisende), Bob als *verifier* (engl., der Überprüfende, nach [SPS11]). Als

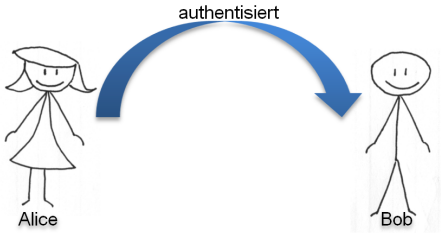

Abbildung 5.1.: einseitige Authentifikation zwischen Alice und Bob

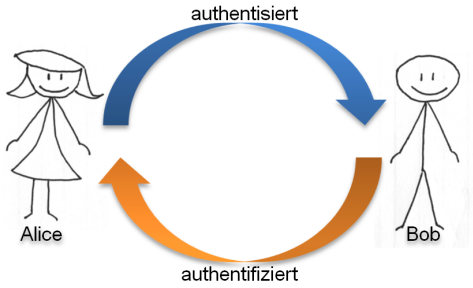

Abbildung 5.2.: gegenseitige Authentifikation zwischen Alice und Bob

klassisches Beispiel für einseitige Authentifikation lassen sich jegliche Anmeldungen, die mit Hilfe eines Passworts vorgenommen werden, sehen. Ist der Benutzer hier in Besitz des Passwortes kann er sich als rechtmäßiger Benutzer legitimieren. Im Englischen wird nicht zwischen Authentisierung und Authentifikation unterschieden - hier werden beide Begriffe als *authentication* bezeichnet (vgl. [Bal11]).

Gegenseitige Authentifikation (Abbildung 5.2) bedeutet, dass sich die Kommunikationspartner Ihre Identität gegenseitig beweisen. Zunächst authentisiert sich Alice bei Bob - nach der Verifikation authentifiziert sich Bob bei Alice, die wiederum Bob verifiziert. Beispiel hierfür ist die Anmeldung eines Clients gegenüber eines Servers.

Für beide Authentifikationsmodelle gilt: erst nach erfolgter Authentifikation erfolgt eine Nutzer-spezifische Authorisierung, welche individuell unterschiedliche Dienste und/oder Anwendungen durch Alice nutzbar macht - in der Regel durch eine rollenbasierte Rechteverwaltung.

Zusätzlich zur herkömmlichen Authentifikation gibt es die Zwei- und Multifaktor-Authentifikation, die mehrere Authentifikationstechniken kombiniert, um die Sicherheit zu erhöhen. Da diese Arbeit sich auf rein passwortbasierte Verfahren konzentriert werden diese hier nicht näher erläutert - einige Details finden sich jedoch in Anhang B. Interessante Aspekte finden sich auch rund um die Zwei-Kanal-Authentifikation, also die zusätzliche Übermittlung von PINs oder TANs über einen Kanal wie z.B. einem Mobiltelefon; eine kritische Sicherheitsanalyse um diesen Themenbereich bietet [And08], wird an dieser Stelle jedoch nicht näher betrachtet.

5.2. Definition Authentifikationssystem

Ein Authentifikationssystem bezeichnet ein System, das auf Basis einer Eingabe von Credentials Authentifizierungen für Prozesse, Subsysteme oder Programme vornimmt, für die der Benutzer eine Berechtigung besitzt. Die Authentifikation kann auf vielfache Art und Weise erfolgen - relevant ist jedoch, dass für jeden Zugriff eine erneute Authentifikation erforderlich ist.

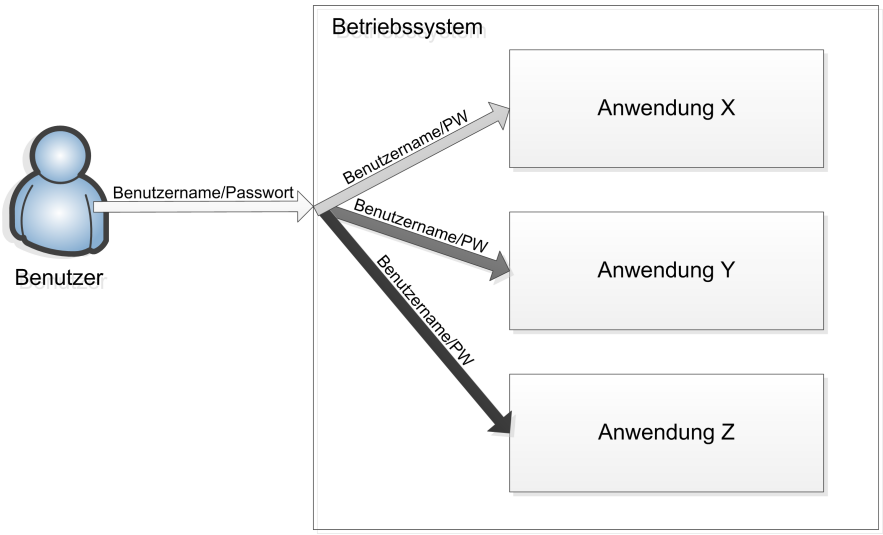

Abbildung 5.3.: Skizze eines passwortbasierten Authentifikationssystems

5.3. Definition Single Sign-On-System

Single Sign-On (Abkürzung: SSO, engl. für einmalige Anmeldung) ist ein Authentifikationsmechanismus, der es einem registrierten Benutzer ermöglicht mit nur einer einzigen Anmeldung Zugang zu allen für ihn freigegebenen *Service Provider*n (SP, engl., Dienstanbieter[1]) zu erhalten. Auf diese Weise wird der Aufwand für den Benutzer verringert - er muss sich nur *eine* Benutzername/Passwort-Kombination merken, anstatt mehrere Zugangsdaten zu verwalten oder erinnern. Der Aufwand für Administratoren verringert sich ebenfalls, da nur für ein einziges Benutzerprofil Daten hinterlegt/aktualisiert werden müssen. Das Single Sign-On System generiert bei der Anmeldung Authentifizierungsinformationen, die innerhalb des Systems an alle entsprechenden Anwendungen und Systeme weitergegeben werden.

[1] im Kontext dieser Arbeit bezeichnet ein Service Provider jede Entität, die dem Benutzer einen Dienst oder Inhalt anbietet (nach [PM03])

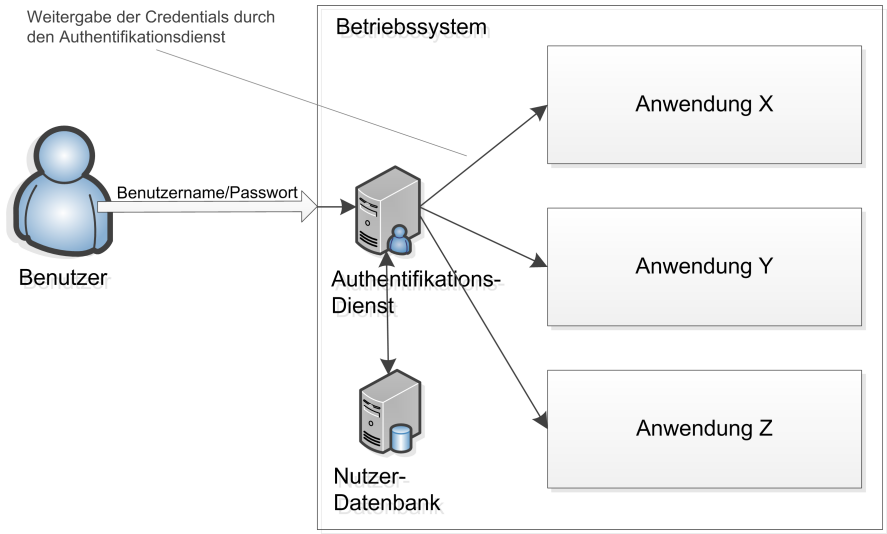

Abbildung 5.4.: Skizze eines Single Sign-On-Systems

5.3.1. Taxonomie von Single Sign-On Systemen

Es gibt mehrere Ansätze, Single Sign-On-Systeme zu klassifizieren und einzuordnen. Um einen Überblick zu verschaffen und eine Einordnung vorzunehmen, sollen an dieser Stelle drei Taxonomien beispielhaft vorgestellt werden. Diese dienen zur Einordnung der nachfolgend verwendeten Kerberos-Technologie.

[BT10] gibt eine Unterteilung in drei Kategorien vor:

- **Broker-basierte Architektur:** ein zentraler Server authentifiziert Subjekte und gibt Tickets an diese aus - mit deren Hilfe können Subjekte Zugang zu Anwendungen erhalten. Beispiel hierfür ist das Kerberos-Protokoll (siehe auch Kapitel 5.4).
- **Agenten-basierte Architektur:** vor jedem Anwendungs-Server wird ein Authentifizierungs-Agent vorgeschaltet, der als „Übersetzer“ zwischen den Credentials des Subjekts (z.B. ein X.509 publicKey-Zertifikat[2]) und dem Authentifikationsprotokoll des Anwendungs-Servers (z.B. ein passwortbasierter Mechanismus) fungiert.
- **Reverse-Proxy-basierte Architektur:** in der demilitarisierten Zone eines Netzwerkes befindet sich ein Proxy-Server, der die Credentials der Subjekte entgegennimmt und an entsprechende Authentifizierungsserver weitergibt.

[2] das X.509-Zertifikat ist ein Beispiel einer digitale Bescheinigung über die Zuordnung eines öffentlichen Signierschlüssels zu einer natürlichen oder juristischen Person (vgl. [Eck12].

Der Autor gibt an, dass diese Architektur-Arten häufig untereinander kombiniert werden, weswegen sie zur genauen Klassifizierung als ungeeignet erscheinen.

[PM03] unterteilt SSO in seiner Arbeit in Pseudo-SSO und True-SSO, die sich dadurch unterscheiden dass das Pseudo-SSO eine Komponente enthält, die alle Service Provider-abhängigen Credentials verwaltet und bei einer Anfrage zur Verfügung stellt. Im Gegensatz dazu stellt True-SSO einen zentralen *Authentication Service Provider* (engl., Abkürzung: ASP) zur Verfügung, der sich nach Anmeldung des Nutzers bei den SPs authentifiziert.

[RR12] und [Cle02] unterscheiden Single Sign-On-Systeme hingegen zunächst nach der Art des Einsatzes (Internet, Extranet oder Intranet), im Anschluss nach deren Architektur und der Anzahl von Zugangsdaten. Abschließend werden die sich daraus ergebenden, aktuell Verwendung findenden Protokolle aufgegliedert. Die von [RR12] und [Cle02] verwendete Taxonomie erscheint stimmig, schlüssig und umfassend, weswegen im Weiteren hiernach vorgegangen wird. Das vom Autor entwickelte Diagramm wurde um Web-Technologien erweitert, um ein weiteres Spektrum zu bieten (siehe Abbildung 5.5).

Einsatz-Orte So genannte Intranet bzw. *Enterprise Single Sign-On-Verfahren* (Abkürzung: ESSO) verbinden mehrere Systeme innerhalb eines Unternehmensnetzwerkes und machen diese dem Benutzer nach einmaliger Zugangsdateneingabe zugänglich. Extranet bzw. *Multi-Domain Single Sign-On-Systeme* verbinden nicht nur die Systeme eines Unternehmens, sondern auch die von Businesspartnern (z.B. Tochtergesellschaften) miteinander - wechselt der Benutzer zwischen den Ressourcen der verschiedenen Unternehmen ist keine neue Eingabe von Benutzerdaten notwendig. Internet bzw. *Web Single Sign-On-Systeme* sind browserbasierte Mechanismen, die mittels einmaligem Login Zugriff auf die, sich auf dem Webserver befindlichen Anwendungen, gewähren.

Architektur-Art *Simple SSO-Architekturen* besitzen nur eine Authentifikations-Instanz, bei der sich der Benutzer mit jeweils einem Zugangsdaten-Satz anmeldet. Verwendung findet dies z.B. in homogenen LAN- oder Intranetumgebungen. *Komplexe SSO-Architekturen* hingegen verwenden mehrere Authentifikationsstellen oder mehrere Sätze von Zugangsdaten pro Benutzer.

Credential-Arten Sieht ein komplexes Single Sign-On-Systeme nur einen Satz Zugangsdaten pro Benutzer vor kann dies auf zwei Arten realisiert werden (vgl. [RR12],[Cle02]):

- **Token-basiertes SSO-System:** Nachdem der Benutzer seine Zugangsdaten übermittelt hat überprüft der Server, ob diese Daten in der Credentials-Datenbank enthalten sind. In

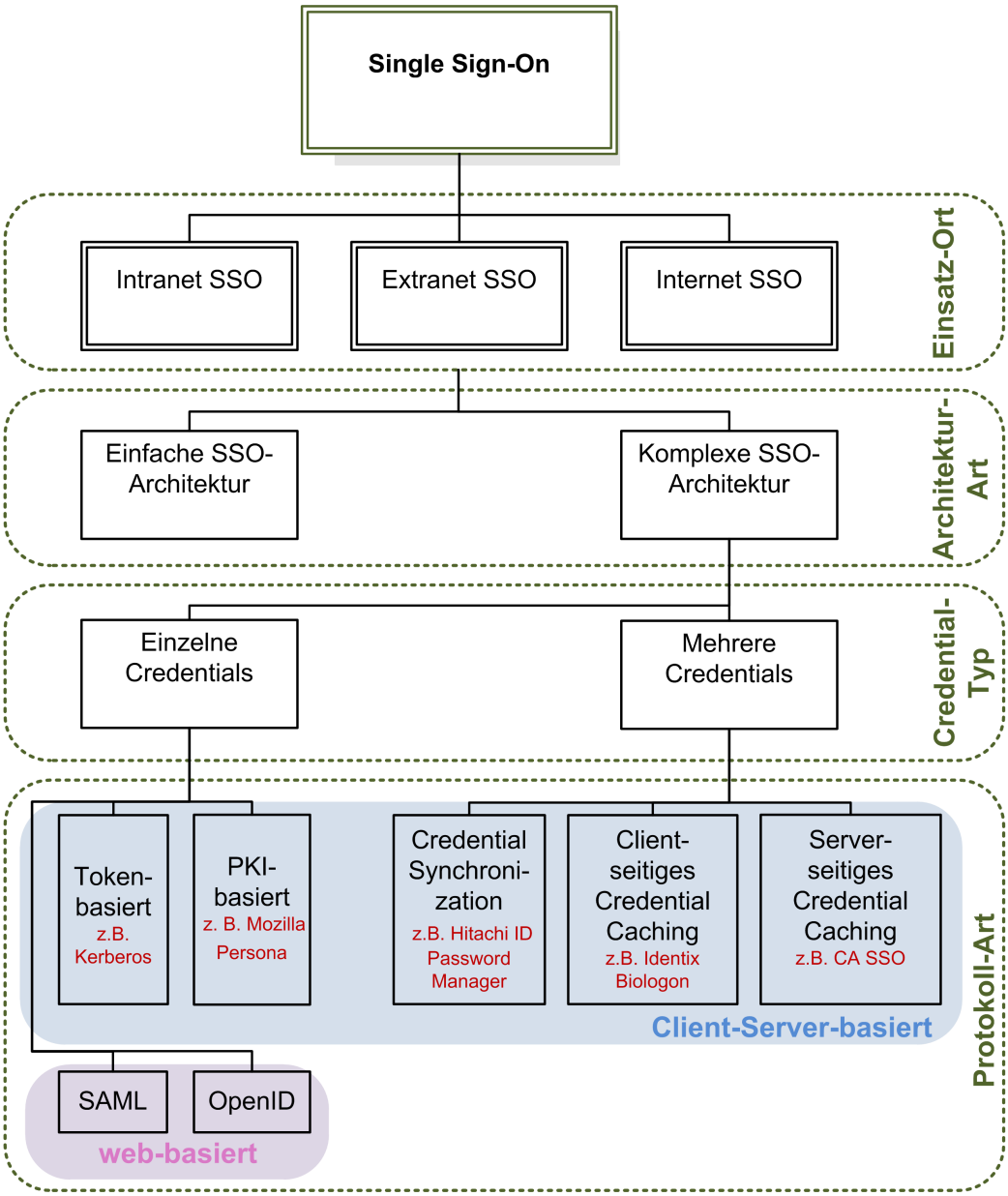

Abbildung 5.5.: Übersicht von Single Sign-On Arten nach [RR12]

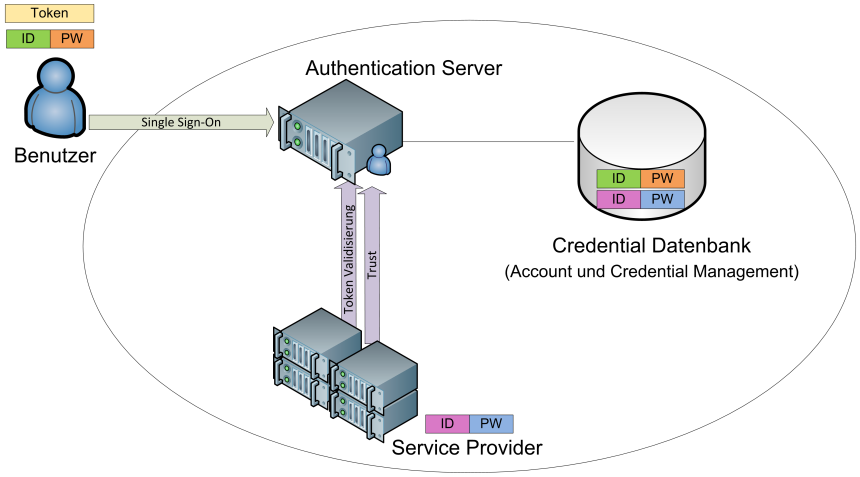

Abbildung 5.6.: Simples SSO mit einem Zugangsdatensatz, nach [Cle02]

diesem Fall erhält der Benutzer (bzw. der Client-PC) ein *Token* (engl., Symbol/Zeichen/-Marke, ebenfalls Verwendung findet in diesem Zusammenhang oft der Begriff Ticket), aufgrund dessen jede weitere Authentifizierungsstelle entscheidet, ob der Tokeninhaber Zugriff auf den Service Provider erhält. Im positiven Fall erhält der Benutzer dann ein zeitlich befristetes Token zur Benutzung der Anwendung. Beim Token-basierten SSO ist besonders wichtig, dass die Authentifizierungsstellen sich untereinander vertrauen - dies lässt sich beispielsweise durch Zertifikate realisieren, wie es in Abbildung 5.7 illustriert ist.

- **PKI-basiertes SSO-System:** Server/Ressourcen und Benutzer authentifizieren sich gegenseitig durch ihre jeweiligen Schlüsselpaare: während der Server sich gegenüber des Benutzers authentisiert, in dem er mit de m Server-Public-Key eine beliebige Nachricht entschlüsselt authentifiziert der Server den Benutzer, in dem er eine beliebige Nachricht mit dem Benutzer-Public-Key verschlüsselt. Sofern die Zertifizierungsstellen unterschiedlich sind, muss unter diesen Vertrauen bestehen. Um die Nachrichtenintegrität (siehe Kapitel 2.2.1, Integrität) auch auf unsicheren Kanälen (wie dem Internet) zu gewährleisten werden zufällige Schlüssel als Sitzungsschlüssel verwendet, die lediglich für die Dauer des Nachrichtenkanals bestehen und anschließend verworfen werden (vgl. [TS08]). Eine beispielhafte Übersicht bietet Abbildung 5.8.

Handelt es sich um ein komplexes SSO mit mehreren Zugangsdaten, wird zwischen drei Arten unterschieden:

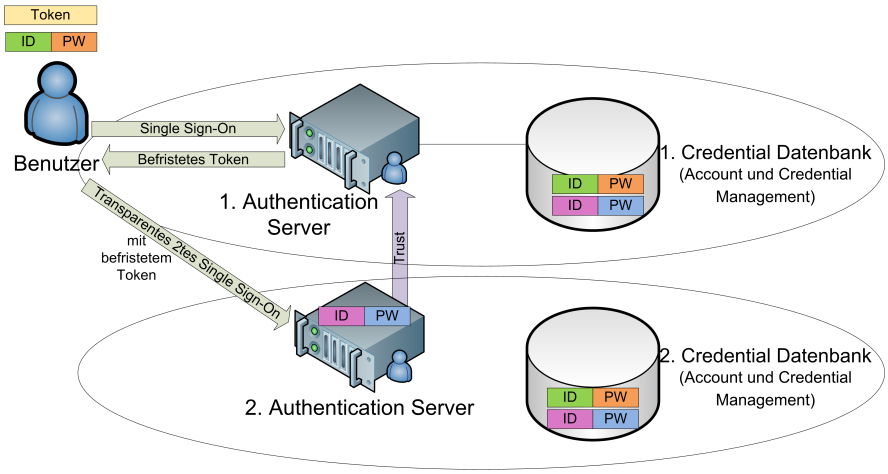

Abbildung 5.7.: Komplexes, Token-basiertes SSO-System nach [Cle02]

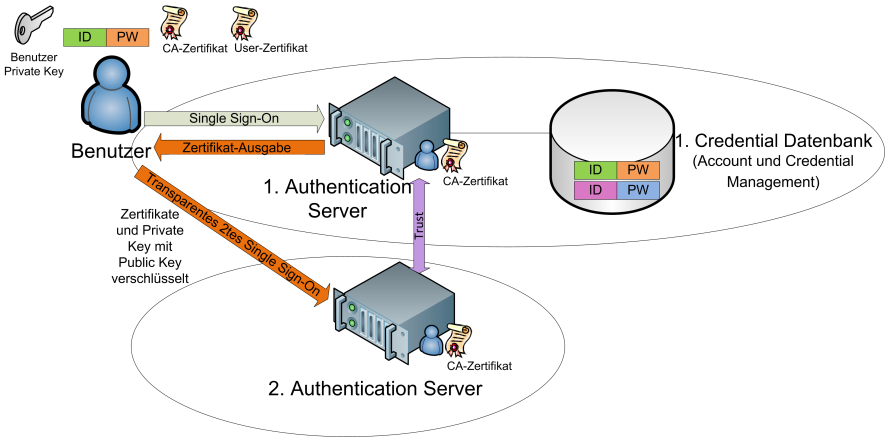

Abbildung 5.8.: Komplexes, PKI-basiertes SSO-System nach [Cle02]

- **Credential Synchronization:** Ein Satz von Zugangsdaten „maskiert“ mehrere Zugangsdatensätze mit Hilfe einer Synchronisationssoftware um dem Benutzer die Illusion zu geben, nur einen einzigen Satz Zugangsdaten zu verwenden.
- **Client-seitiges Credential Caching:** Sensible Benutzerdaten werden auf dem Client in einer Systemdatei namens *vaults* gespeichert, sodass der Benutzer sich überall automatisch anmelden kann ohne seine Credentials erneut einzugeben. Vaults kann, wie z.B. beim Windows Credentials Manager, neben Passworten auch Zertifikate und Tokens speichern.
- **Server-seitiges Credential Caching:** identisch mit dem Client-seitigen Credential Caching, nur dass der Speicherort ein zentraler Server, der die administrative Aufgabe der Speicherung, Verwaltung und Bereitstellung an SPs hat, anstelle des Clients ist.
- Die web-basierten Technologien werden im nächsten Kapitel näher erläutert.

5.4. Kerberos

In Anlehnung an die Taxonomie von [RR12] (vgl. Abbildung 5.5) untersucht diese Arbeit nicht alle Protokolle die für Single Sign-On-Systeme verwendet werden oder werden könnten sondern konzentriert sich lediglich auf Kerberos. Kerberos wurde ausgewählt, da es bereits seit den 1980er Jahren verwendet und hierdurch ausreichend erforscht ist. Zwei weitere, aktuellere Technologien (SAML, OpenID) sowie die Single Sign-On Variante der HAW sind in Anhang C zu finden.

5.4.1. Grundlagen und Definition

Das Kerberos-Authentifikationssystem wurde am Massachussetts Institute of Technology (MIT) entwickelt und trägt seinen Namen in Anlehnung an den Dreiköpfigen Höllenhund *Cerberus*[3] - eine Metapher für die drei verwendeten Komponenten Client, Server und *Key Distribution Center* (engl., Abkürzung: KDC, Schlüssel-Verwaltungs-Zentrale). Das Ziel von Kerberos ist die gegenseitige Authentifikation eines Clients mit einem anderen, unbekannten Partner innerhalb eines verteilten Systems über ein vermeintlich „unsicheres“ Netzwerk ohne Übertragung der Zugangsdaten des Benutzers.

Kerberos war zunächst im Rahmen des „Athena“-Projekts als zentrale Authentifikationsinstanz einer software-basierte Client-Server-Umsetzung geplant und wurde vom Planungsbeginn bis Version 3 ausschließlich hochschulintern verwendet. Ab Version 4 (1977/1978) war

[3] Cerberus ist laut griechischer Mythologie der Wächter über den Eingang zur Unterwelt, der Besucher hinein-, aber niemanden herauslässt.

Kerberos dann frei verfügbar, und die aktuelle Version 5 wird seit 1993 als internationaler Standard im RFC 1510[4] beschrieben. Dieser Abschnitt bezieht sich auf Kerberos in der Version 5 (vgl. [Eck12], [Hoi03]).

5.4.2. Architektur und Terminologie

Kerberos (V5) als Client-Server-Modell basiert auf dem Needham-Schroeder-Protokoll - um Zeitstempel erweitert - und bezeichnet einen reinen Authentifikations- und Schlüsselaustauschdienst. Es findet keine Rechteverwaltung oder Zugriffskontrolle statt [Eck12]. Wesentliche Unterschiede zu den Vorgängerversionen stellen die freie Wahl des Verschlüsselungsverfahrens sowie der Versand von Authentifikationsmerkmalen eines Benutzers dar.

Die Verwaltung der Authentifikationsinformationen erfolgt dezentral durch eine Hierarchie von Authentifikationsservern, die innerhalb ihres Verantwortungsbereichs (engl. *realm*, auch: Domäne) autonom agieren und kooperieren können. Auf diese Weise können auch bereichsübergreifende Zugriffe Benutzer-transparent erfolgen. Der Realm sorgt dafür, dass von vornherein definiert ist, auf welchen Subjekte nach erfolgreicher Authentifikation zugegriffen werden darf.

Principals (engl. für Auftraggeber) sind Arbeitsplatzrechner/Clients, Benutzer oder Server die authentifiziert werden und Sitzungsschlüssel mit dem Authentifikationsdienst oder anderen Principals austauschen. Der Authentifikationsdienst basiert auf symmetrischen Verfahren und wird von einem vertrauenswürdigen Server (engl. *trusted third party*, Abkürzung TTP, vertrauenswürdiger Dritter zur Verifikation der Echtheit der Kommunikationspartner [KS08]) erbracht. Relevant ist hier besonders, dass die unterschiedlichen Principals sind untereinander nicht „kennen“, aber da jeder einzelne sich gegenüber der TTP initial authentifiziert hat, ein Vertrauensverhältnis herrscht. Die beteiligten Principals verwalten ihre eigenen langlebigen und geheimen Schlüssel (engl. *master key*) sicher und synchronisieren sich zudem lose mit der Systemuhr des Authentifikationsdienstes (durch die Verwendung von Zeitstempeln[5]).

Jeder Principal wird durch das Tripel (Name, Instanz, Realm) eindeutig identifiziert: während bei Clients der Name der Benutzerkennung entspricht und die Instanz den Wert 0 oder auch ein spezifisches Attribut wie „root“ haben kann, bezeichnet der Name von Service Providern dessen Namen, und die Instanz die IP-Adressen der Rechner, auf denen sie installiert sind. Unterschiedliche Realms trennen unterschiedliche Authentifikationsbereiche voneinander, vertrauen sich aber untereinander.

```
jennifer@ATHENA . MIT . EDU
```

[4] `http://www.ietf.org/rfc/rfc1510.txt`, The Kerberos Network Authentication Service (V5)
[5] geringfügige Abweichungen werden akzeptiert.

```
jennifer/admin@ATHENA.MIT.EDU
daffodil.mit.edu
```

Listing 5.1: Beispielbezeichner nach [Mas02]

Das *Key Distribution Center* (KDC) ist der Authentifikationsdienst eines jeden Realms und besteht aus zwei Teilen - dem Authentication Server AS und dem Ticket-Granting-Server TGS (siehe auch Abbildung 5.9). Während der AS in seiner Datenbank Namen und Master Keys der Principals vorhält sorgt der TGS für die Erzeugung von Tickets zum Zugriff auf beliebige andere Principals im selben oder in anderen Realms. Beide Teile des KDC kommunizieren miteinander, jedoch nicht mit KDCs anderer Realms. Während der AS die Authentifizierungsphase repräsentiert und lediglich beim Login eines Nutzers verwendet wird ist der TGS häufig im Einsatz, um sowohl Initialtickets, als auch Tickets für Serverzugriffe zu erzeugen.

Die Authentifikation innerhalb eines Kerberos-Systems basiert auf Tickets, die im Kerberos-Kontext für eine Authentifikationsbescheinigung stehen. Jedes Ticket $T_{Client,Server}$ hat den Inhalt:

$$T_{Client,Server} = Server, Client, addr, timestamp, lifetime, K_{Client,Server}$$

wobei es sich bei $Server$ und $Client$ um die Namen von Server und zu authentifizierendem Principal handelt und $addr$ die IP-Adresse des Principals enthält. $lifetime$ und $timestamp$ bezeichnen die Gültigkeitsdauer und den Zeitstempel, also das Datum der Übermittlung. Beim Schlüssel $K_{Client,Server}$ handelt es sich um einen für den Zweck der Kommunikation zwischen Client und Server erzeugten Sitzungsschlüssel (engl.: *session key*). Das Ticket-Granting-Ticket ist das erste Ticket, das der Client nach erfolgreicher Authentifikation vom TGS erhält. Nur hiermit erfüllt ein Client die Voraussetzung sich bei anderen Servern zu authentifizieren - es hat eine beliebig lange, systemseitig zu belegende Gültigkeit.

Zusätzlich wird mittels eines Authentikators A_{Client}, der folgenden Aufbau hat, Authentifikationssicherheit gewährleistet (vgl. [Hoi03]):

$$A_{Client} = Client, addr, timestamp$$

Sind Authentikatoren veraltet (also älter als 5min) wird die gesamte Anfrage zurückgewiesen.

Die gesamte Kommunikation zwischen Clients, KDC und Servern findet über UDP/TCP und mit ASN.1 (Abstrakte Syntax-Notation 1) kodiert statt, die zur effizienten, maschinenlesbaren und plattformunabhängigen Spezifikation von Datentypen verwendet wird und im ISO-Standard X.680 spezifiziert ist[6]. Die Encodierungsart ist jedoch nicht BER (engl. Abkürzung

[6] `http://www.itu.int/rec/T-REC-X.690-200811-I/en` und Vorlesungsfolien Dr. Osman Ugus, `https://pub.informatik.haw-hamburg.de/home/pub/prof/ugus/IT-Sicherheit/V-Folien/ITS%20SS13%20Kap4.pdf`

für: basic encoding rules), sondern DER (engl. Abkürzung für: distinguished encoding rules, Untermenge von BER). Der Unterschied liegt darin, dass DER kodierte Werte auf Bitebene eindeutig sind, während es für die Kodierung eines Wertes mit BER mehrere Repräsentationen geben kann - somit eignet sich DER besonders für kryptographische oder plattformübergreifende Zwecke.

5.4.3. Authentifizierungsablauf

Abbildung 5.9 beschreibt einen beispielhaften Protokollablauf für den Login des Benutzers Alice in ein Kerberos-System. Nachdem Alice ihre Credentials eingegeben hat fordert der Client in **Schritt 1** ein Initialticket beim KDC an, indem er den Namen des zu authentifizierenden Principals zusammen mit einer Nonce[7] dorthin verschickt.

Die Authentifizierung von Alice ist nur erfolgreich, wenn das übermittelte Passwort mit dem beim AS für Alice verzeichneten Schlüssel K_{Alice} (i.d.R. mit MD5 verschlüsselter Hashwert) übereinstimmt. Der AS verwaltet die Hash-Werte sämtlicher Schlüssel, die mit dem geheimen Schlüssel des AS (z.B. mit einer AES-Verschlüsselung) wiederum verschlüsselt wurden, sodass keine Schlüsselverwaltung oder -speicherung auf den Clients stattfinden muss (vgl. [TS08]).

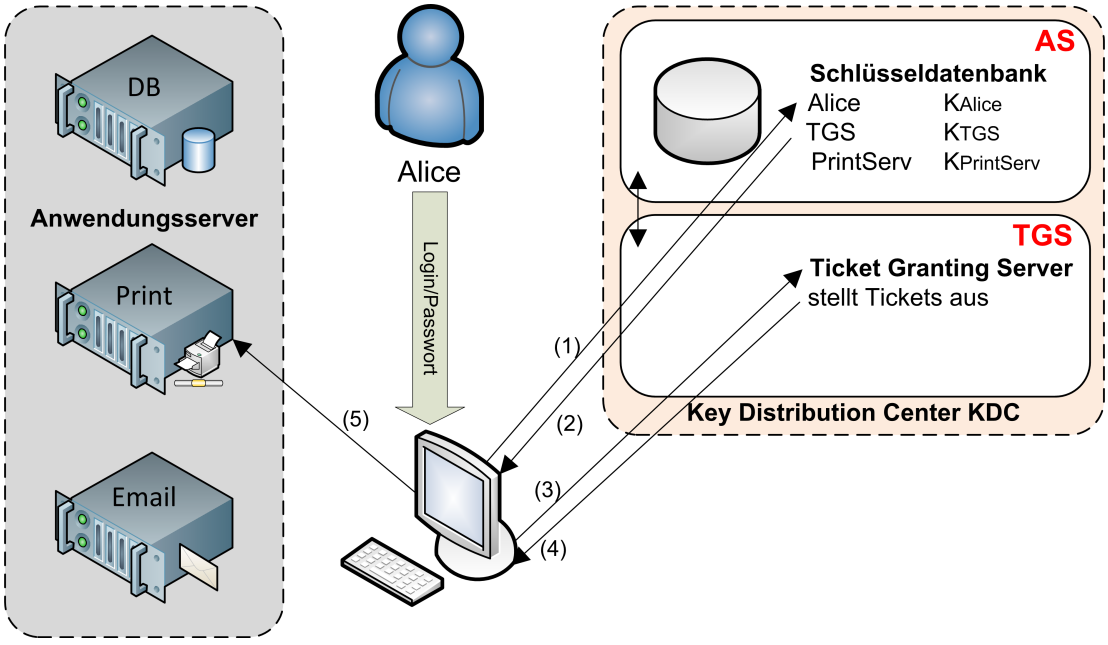

Abbildung 5.9.: Grob-Architektur und Protokollablauf eines Kerberos-Systems nach [Eck12]

[7] Eine Nonce steht für „number used once“ und beschreibt einen eindeutigen, noch nie verwendeten Indikator wie z.B. eine Zufallszahl, vgl. [Eck12]

Schritt Nr.	Von	An	Nachricht
1.	Client	KDC	Alice, TGS, Nonce1
2.	KDC	Client	$\{K_{Alice,TGS}, \text{Nonce1}\}^{K_{Alice}}, \{T_{Alice,TGS}\}^{K_{TGS}}$
3.	Client	TGS	$\{A_{Alice}\}^{K_{Alice,TGS}}, \{T_{Alice,TGS}\}^{K_{TGS,PrintServ}}$, Nonce2
4.	TGS	Client	$\{K_{Alice,PrintServ}, \text{Nonce2}\}^{K_{Alice,TGS}}$, $\{T_{Alice,PrintServ}\}^{K_{PrintServ}}$
5.	Client	Print	$\{A_{Alice}\}^{K_{Alice,PrintServ}}, \{T_{Alice,PrintServ}\}^{K_{PrintServ}}$

Tabelle 5.1.: Kerberos Protokollablauf für Abbildung 5.9

Nur dann, wenn Alice in der Schlüsseldatenbank vorhanden ist versendet der KDC in **Schritt 2** das Ticket-Granting-Ticket (TGT) $T_{Alice,TGS}$, das mit dem Schlüssel K_{TGS} des TGS verschlüsselt ist, zurück an Alice. Zusätzlich erhält sie den Sitzungsschlüssel und das übersandte Nonce zurück, welche mit Alice's privatem SchlüsselK_{Alice} verschlüsselt wurde. So kann sichergestellt werden, dass nur Alice an den Sitzungsschlüssel $K_{Alice,TGS}$ gelangen kann - die zurückgesandte Nonce verwendet Alice um Man-in-the-Middle- oder Replay-Attacken auszuschließen. Da Alice die Nonce selbst erzeugt hat kann sie so überprüfen, ob die Antwort wirklich vom TGS stammt.

Um sich beispielsweise mit einem Printserver zu verbinden gibt der Client in **Schritt 3** beim TGS an, dass er sich mit dem Printserver verbinden möchte, indem er das TGT, den Zielserver sowie eine neu generierte Nonce übersendet. Zusätzlich versendet er einen Authentikator A_{Alice}, der folgenden Aufbau hat:

$$A_{Client} = Client, addr, timestamp$$

Mit dem Authentikator, der mit dem Sitzungsschlüssel $K_{Alice,TGS}$ verschlüsselt wird beweist Alice ihre Authentizität gegenüber des TGS, der Zeitstempel ist ebenfalls ein Sicherheitskriterium - sind Authentikatoren veraltet (also älter als 5min) wird die gesamte Anfrage zurückgewiesen.

Der TGS entschlüsselt das TGT in **Schritt 4**, erhält hierdurch den Sitzungsschlüssel $K_{AliceTGS}$ und kann somit auch den Authentikator entschlüsseln und auf Gültigkeit überprüfen. Im erfolgreichen Fall erzeugt der TGS dann den Sitzungsschlüssel $K_{AlicePrintServ}$, den er mit der Nonce zusammen mit dem $K_{Alice,TGS}$ verschlüsselt. Außerdem wird das Ticket für den Zugriff auf den Printserver erzeugt und mit dem Schlüssel des Printservers $K_{PrintServ}$ verschlüsselt versandt.

In **Schritt 5** kann sich der Client dann unter Vorlage des Tickets $\{T_{Alice,PrintServ}\}^{K_{PrintServ}}$ und eines gültigen, mit dem Sitzungsschlüssel $\{A_{Alice}\}^{K_{Alice,PrintServ}}$ verschlüsselten Authentikators erfolgreich gegenüber des Printservers authentifizieren. In diesem Zusammenhang

lassen sich Ticket und Sitzungsschlüssel als Credentials des Clients für den Server bezeichnen (vgl. [Hoi03]).

Diese Basisfunktionalität von Kerberos ist für Version 4 und Version 5 bis auf einen Aspekt identisch. In Kerberos V5 findet in Schritt 1 eine sogenannte *Pre-Authentication* (engl. für Vorab-Authentifizierung) statt. Hier wird statt einer Nonce ein mit dem Client-Key verschlüsselter Zeitstempel versandt - so wird die Möglichkeit, sich als Principal Alice ein TGT mit Angabe des Benutzernamens Bob anzufordern, eliminiert (vgl. [Fei12]).

Wird optional eine wechselseitige Authentifikation zwischen den Principals gefordert (siehe Abschnitt 5.1 lässt sich Schritt 5 so erweitern, dass der Server zur Authentifizierung gegenüber des Clients den Zeitstempel im Authentikator um eins erhöht und mit dem Sitzungsschlüssel verschlüsselt zurücksendet. Dieser Schritt ist ursprünglich im Kerberos-Basisprotokoll vorhanden gewesen, das im nachfolgenden Kapitel kurz erklärt wird.

5.4.4. Single Sign-On Funktionalität von Kerberos

Das Kerberos-Basisprotokoll besteht ursprünglich nur aus den Principals, die miteinander kommunizieren wollen, sowie dem Authentication Server, der die Rolle der TTP übernimmt (nach [KS08]). Hier authentifiziert sich Alice zunächst gegenüber des Authentication Servers, nach Erhalt des TGT sendet er dies zusammen mit seinem Authenticator an den anderen Principal. Jetzt findet die Verifikation (als Teil der gegenseitigen Authentifizierung) statt, indem der Principal die entschlüsselte Systemzeit aus dem Authenticator (+1) an den Client zurücksendet - auf diese Weise kann Alice sicherstellen, dass der Principal derjenige ist, dessen Key in der Datenbank des Authentication Servers gespeichert ist. Der beispielhafte Ablauf ist in Abbildung 5.10 dargestellt.

Obwohl diese Methode logisch sicher ist (vgl. [Fei12]) muss dieser Vorgang bei jedem zu kontaktierenden Service wiederholt werden, was neben der Mehrfacheingabe des Passworts als sicherheitskritischem Element auch unkomfortabel ist. Hier greift der TGS als zwischengeschalteter Service wie unter Architektur beschrieben. Das durch diesen initial ausgestellte TGT sowie der Session Key gelten für alle anderen, im Realm befindlichen Principals. Jeder neue Principal kann, sofern er kerberisiert ist (also den Empfang und Versand von Tickets , auf diese Weise angesprochen werden.

Der Prozessablauf ändert sich insofern, dass der Client vor der Anfrage nach einem anderen Principal zunächst das TGT beantragt und lediglich an eben dieser Stelle sein Passwort zur initialen Authentifizierung angibt. Bei jeder nachfolgenden Anfrage dient das TGT als Authentifikation anstelle der eigentlichen Passworteingabe, denn der Beweis der Identität

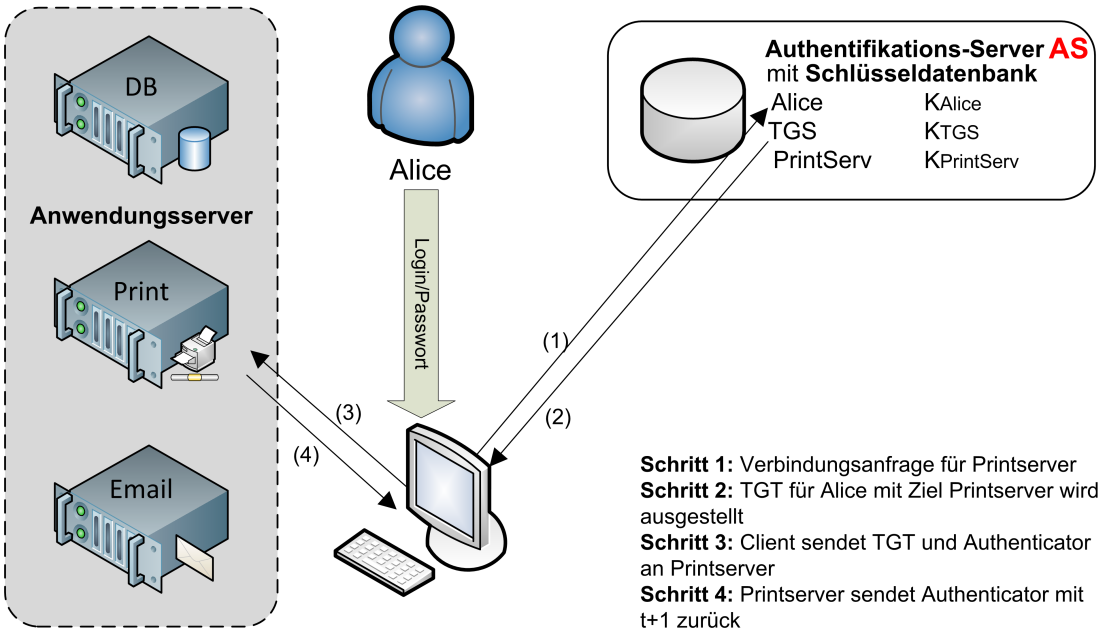

Abbildung 5.10.: Kerberos Basis-Protokoll nach [KS08]

lag bereits vor. Erst durch diese einmalige, für eine bestimmte Ticket-Lebensdauer gültige Authentifikation ist das Kriterium des Single Sign-On erfüllt.

5.5. Sicherheit von Kerberos

Kapitel 4.2 stellte bereits klassische Sicherheitsrisiken Passworte betreffend vor und erläutert diese im Detail. Diese gelten uneingeschränkt ebenso für die Gesamtheit passwortbasierter Authentifikationssysteme, da Passworte deren einziges Authentifikationsmerkmal sind. Sie sollen daher nur erneut genannt, aber kein weiteres Mal vorgestellt werden: Guessing (Dictionary-Angriffe), Brute-Force Attacken, Shoulder Surfing, Phishing und Social Engineering.

Sicherheitsrisiken, die Kerberos als stellvertretende Authentifikationstechnologie betreffen lassen sich in zwei Kategorien unterteilen: Technik-basierte Risiken und Risiken aufgrund des Einflusses menschlichen Handelns. Diese werden nachfolgender eingehender betrachtet - sofern Lösungen zu Sicherheitsrisiken bestehen werden diese ebenfalls genannt und stellen Maßnahmen zur Erhöhung der Sicherheit dar.

> „It is important to recognize that implementing Kerberos on your network does not guarantee perfect security.“ Jason Garman [Gar03, S. 55]

5.5.1. Technik-basierte Risiken

Schlüsselverwaltung Die Verwaltung der Benutzerschlüssel und Tickets erfolgt auf dem Clientrechner - Kerberos sieht jedoch keine Mehrbenutzerumgebungen vor, sodass Tickets die sich beispielsweise lokal im /tmp-Verzeichnis befinden, leicht kompromittiert werden können. Hier könnte mit dem manuellen oder automatisierten Löschen des Caches gegengesteuert werden (vgl. [TS08]).

Außerdem sind die Sitzungsschlüssel, die das KDC erzeugt keine Sitzungsschlüssel im eigentlichen Sinne, weil die Tickets für jegliche Kommunikationsverbindung mit dem Server, für den und solange sie gelten, verwendet werden können. Die maximal mögliche Gültigkeitsdauer eines Tickets kann bis zum 31.12.9999 betragen. Somit gilt der verwendete Sitzungsschlüssel ebenfalls entsprechend lange und kann angegriffen werden. Kerberos unterstützt seit Version 5 jedoch *Renewable* (engl., erneuerbar) Tickets (ausgenommen ist das TGT) - mittels eines vorab gesetzten Flags kann eine Zeit T_E angegeben werden, bis zu dieser ein neues Ticket angefordert worden sein muss. Geschieht dies nicht verweigert das KDC eine Ticketerneuerung (vgl. [Hoi03]). Daher sind bei einer zu kurz gewählten Gültigkeitsdauer häufigere Reauthentifizierungen notwendig.

Ebenfalls KDC-seitig drohen Probleme, da alle Schlüssel mit dem selben Server-Masterkey verschlüsselt werden. Wenn der Masterkey des KDC kompromittiert wird wird eine komplette Erneuerung aller Passworte notwendig. Fällt das KDC aus ist das gesamte System nicht mehr lauffähig, was es zum Single-Point-of-Failure macht. Abhilfe kann hier eine Ausfallsicherung des KDC in Form von redundant ausgelegten Servern schaffen (vgl. [Sta03], [Wie12]).

Systemzeit Die Aktualitätsprüfung der Zeitstempel in einem Authenticator ist als Sicherheitsmechanismus gegen Replay-Attacken gedacht - die Voraussetzung hierfür ist die Synchronisierung aller beteiligten Clients mit einer globalen Zeit. Ist es einem Angreifer jedoch möglich einen Server mittels einer falschen, also bereits abgelaufenen Zeit zu manipulieren kann ein bereits verwendeter Authenticator für Maskierungsangriffe mißbraucht werden. Diese Angriffsmöglichkeit ist nicht unwahrscheinlich, da viele Clients nicht vertrauenswürdige Synchronisationsprotokolle verwenden. Ein Challenge-Response-Verfahren mit Nonces würde dies verhindern, ist aber in Kerberos V5 nicht vorgesehen - auch die Verwendung von NTP (engl., Network Time Protocol, spezifiziert im RFC958[8]) bietet eine solche Möglichkeit.

Angriffe von außen Die Authentizitätsüberprüfung basiert auf IP-Adressen, die grundsätzlich fälschbar sind. Kann ein Angreifer einen Authenticator abfangen und in eine maskierte

[8] `http://tools.ietf.org/html/rfc958`, Network Time Protocol (NTP)

TCP/IP-Verbindung einschleusen bietet nur das (optional wählbare und somit nicht voreingestellte) Challenge-Response-Verfahren Schutz. Nach [Sch96] und [Gar03] besteht außerdem die Möglichkeit, Tickets eines/mehrerer Benutzer zu „sammeln“ und einen Dictionary-Angriff durchzuführen. Gegen Trojaner gibt es bisher keinen wirksamen Schutz: wird ein Client von einem Angreifer kompromittiert und erhält dieser dadurch Administratorrechte können Passwörter aufgezeichnet werden.

Zusätzlich sind die in Kerberos verwendeten kryptographischen Algorithmen öffentlich und hinreichend bekannt, sodass die durch das KDC erstellten Schlüssel Ziel einer Offline-Entschlüsselung werden können - die geheimen Schlüssel eines angefragten Services befinden sich immer beim damit verschlüsselten Ticket, dies gilt auch für den Masterkey des KDC, mit dem das TGT verschlüsselt ist (vgl. [KS08], [Hoi03], [Gar03]). Durch mehrere Schlüssel kann der verwendete Verschlüsselungsalgorithmus nachgebildet und mißbräuchlich verwendet werden.

Ein sogenannter Root-Level-Angriff, also ein direkter Angriff auf das KDC erlaubt einem Angreifer den vollen Zugriff auf das Authentifikationssystem - dieses ist zwar verschlüsselt, doch befindet sich der Masterkey physisch auch auf dem KDC(-Server). Da alle Kerberos-Implementationen vorsehen, dass Administratoren oder Root-Benutzern ein authentifizierungsloser Zugriff auf die Kerberos-Datenbank gestattet wird ist ebendiese gefährdet, wenn ein KDC (von mehreren oder mehreren redundanten) kompromittiert wird (vgl. [Gar03]).

[Gar03] gibt zusätzlich zu bedenken, dass die Kompromittierung eines Principal-Servers, der einen bestimmten Dienst oder eine Anwendung anbietet, einem Angreifer die Möglichkeit gibt sich als dieser Principal auszugeben und auf Daten zugreifen, die zwischen anderen Principals und diesem Dienstanbieter versendet wurden. Durch die Tatsache, dass Kerberos auf der Authentifikation durch Tickets beruht werden jedoch zu keiner Zeit Credentials von Principals über ein (unsicheres) Netzwerk versendet und können somit auf diese Weise nicht abgehört werden.

Während der Installationsroutine ist das System am angreifbarsten und muss explizit vor Angriffen geschützt werden (vgl. [Gar03]). Im laufenden Betrieb empfiehlt [Gar03] die Kerberos-Server in einem abgeschlossenen Raum mit strenger Zugangskontrolle unterzubringen.

5.5.2. Beeinflussung der Sicherheit durch menschliches Handeln

Passwort-Kompromittierung Ein wesentlicher Schwachpunkt des Kerberos-Konzepts ist die mögliche mißbräuchliche Verwendung des Benutzerpasswortes. Unabhängig von der Beschaffungsart kann nach dessen Beschaffung der gesamte Authentifikationsprozess unterlaufen werden und der Angreifer kann netzwerkweit aktiv werden, da es keine weiteren Einschrän-

kungen (außerhalb der nutzerseitigen Berechtigungen, die jedoch nicht durch Kerberos selbst erfolgen) gibt.

Handelt es sich bei dem kompromittierten Benutzer um einen Administrator ist das gesamte Kerberos-System gefährdet: der Angreifer kann auf einfache Weise ein (durch die meisten Implementationen vorgegebenes) Backup des Gesamtsystems erstellen, Principals anlegen oder verändern. Nur durch die Einschränkung der Administratorrechte auf einen möglichst kleinen Personenkreis lässt sich dies umgehen, empfiehlt [Gar03] ebenso wie monatliche Passwortwechsel.

Es ist möglich die Sicherheit von Kerberos mit Multifaktor-Authentifikation zu erweitern, z.B. durch eine SmartCard (hierfür gilt das RFC4556[9].) Es gibt auch einige weitere Ansätze, wie die Optimierung des Protokolls durch einen doppelten Zeitcheck in Kombination mit Smart-Card-Technologie, um Passwort- und Replay-Attacken zu vermeiden (vgl. [Jia09]).

5.6. Thesenüberprüfung und Bewertung

These 5.6.1 *Erhöhen Single Sign-On-Systeme die Sicherheit?*

Um die vorstehende These zu überprüfen sollen Vorteile und Nachteile - die Sicherheit betreffend - abgewogen werden. Der Vergleich bezieht sich auf Single Sign-On-Systeme am Beispiel von Kerberos als auch auf SSO im Allgemeinen.

Grundsätzlich gilt für alle verteilten Systeme, also Client-Server-Architekturen: Probleme entstehen dadurch, dass das komplette System sicher sein muss - ist nur eine Komponente unsicher kann das System als Ganzes angreifbar sein (vgl. [TS08]).

Ein Single Sign-On-System das Kerberos verwendet muss das KDC zur Sicherung der Verfügbarkeit (siehe Kapitel 2.2.1) redundant und ausfallsicher auslegen (vgl. [Sta03], [Wie12]). [TS10] merkt an, dass es aufgrund der Vielzahl von Benutzer-Passwörtern ein sehr attraktives Ziel für Hacker und Cracker ist - es muss also sichergestellt werden, dass nur berechtigte Clients Zugriff darauf haben können. Fällt das KDC aus, sind viele Anwendungen für viele Benutzer unerreichbar, was den gleichen Effekt wie ein Denial-of-Service-Angriff hat.

Die Installation eines Kerberos-SSO ist aufwändig, da alle Applikationen, Server und Clients „kerberisiert“ werden müssen - d.h., der Versand und Empfang von Tickets sowie die Ver- und

[9] `http://www.ietf.org/rfc/rfc4556.txt`, Public Key Cryptography for Initial Authentication in Kerberos (PKINIT); PKINIT musste 2008 aufgrund schwerwiegender Sicherheitslücken überarbeitet werden - Angreifer konnten gegenüber der Principals vorgeben, Service Provider oder KDC zu sein oder auf Schlüssel zugreifen, die seitens des KDC zur Ticketverschlüsselung verwendet werden (vgl. [CJS+08])

Entschlüsselung müssen beherrscht werden. Weiterhin muss ein sicheres Verschlüsselungsverfahren gewählt werden; die vom MIT angebotende Kerberos-Implementierung unterstützt zwar einige, die Algorithmen sind jedoch öffentlich und daher nur eingeschränkt sicher.

Ein weiterer Sicherheitsnachteil bezieht sich nicht auf Kerberos, dafür aber auf SSO im Allgemeinen: [KS08] führt an, dass ein Single Sign-On-System, das nicht wie Kerberos auf Tickets basiert [und somit auf die Übertragung von Credentials über ein Netzwerk zurückgreift] allen Applikationen die Nutzer-Credentials zur Verfügung stellt. Dies kann bei Manipulation oder fehlerhafter Implementierung zu einer kritischen Sicherheitslücke führen - es ist ebenfalls nicht auszuschliessen, dass Applikationen die Credentials untereinander delegieren.

Die Vorteile der Verwendung von Kerberos als Single Sign-On-System liegen vor allem darin, dass sein Lebenszyklus bereits seit Ende der 1970er Jahre besteht. Während dieser Zeit konnte die Technologie kontinuierlich verbessert werden, Schwachstellen und Sicherheitsprobleme wurden stetig überarbeitet (vgl. [BSSW11]). Die aktuellste Version Kerberos V5 löst gezielt Sicherheitsprobleme der Vorgängerversionen; die in Kapitel 5.5 genannten Sicherheitslücken sind bekannt und können daher entsprechend bei der Verwendung von Kerberos berücksichtigt werden.

Kerberos zeichnet zudem aus, dass es keine direkte Passwortübertragung gibt und zwischen den Principals kein Austausch von Credentials stattfindet. Auf diese Weise ist das Abhören des Datenverkehrs um Passwörter zu „erschnüffeln“, wie es in unsicheren Netzwerken generell möglich ist, erfolglos.

Nicht zuletzt dadurch, dass Microsoft Kerberos V5 bereits seit Jahrzehnten als Standardauthentifizierungsdienst für Windows (ab 2000) verwendet ist Kerberos akzeptiert und mittlerweile auch in Sun's Java[10], der schwedischen Kerberos-Variante Heimdal[11] und als Modul im Apache HTTP-Server[12] zu finden, um nur einige wenige zu nennen.

Allgemeine Sicherheitsvorteile von Single Sign-On-Systemen nennt auch [RR12]: Single Sign-On-Systeme sind einfacher und sicherer, da Sie alle benötigten Services auf lediglich einen Zugang pro Benutzer zusammenfassen, die Anzahl der Passworte auf eines reduzieren und ein zentrales Rollenmanagement zur Definition der Ressourcen-Zugangskontrolle bieten. Die sicherheitsrelevante Verwaltung eines Single Sign-On-Systems ist somit einfacher und weniger komplex als das vieler einzelner Komponenten mit separater Zugangsdatenverwaltung, argumentiert [Sta03].

[Wie12] führt zudem an, dass die Angriffsfläche für Angreifer kleiner wird, da es nur einen Datenspeicher und ein Authentifizierungssystem gibt - es ist einfacher, ein System

[10] http://docs.oracle.com/javase/jndi/tutorial/ldap/security/gssapi.html
[11] www.h5l.org
[12] http://modauthkerb.sourceforge.net/

abzusichern als viele verschiedene (vgl. auch [Gar03]). Der Zugriff auf die IT-Landschaft eines Unternehmens und somit unternehmenskritische Daten erfolgt kontrolliert und auf Basis der Unternehmens-Sicherheitspolitik, bestätigt auch [Sta03].

Laut [RR12] verringert SSO [durch die Reduktion der Zugangsdatensätze pro Benutzer] zudem die Anzahl von Phishing-Angriffen, sofern es sicher implementiert wurde[13].

Zusammenfassend ergibt sich, dass im Falle von SSO im Allgemeinen und Kerberos im Speziellen die Vorteile die Nachteile überwiegen. Die landläufige Kritik, nach der primären Authentifikation seien Angreifer „Tür und Tor geöffnet“ lässt sich jedoch nicht grundsätzlich entkräften, da die Authentifikation mit Passworten als schwach eingestuft werden muss. Sicherheitskritische Daten können jedoch durch eine Re-Authentifikation geschützt werden. Hervorzuheben ist jedoch, dass die eventuelle Kompromittierung von Passworten nicht von der Kerberos- oder anderen SSO-Technologien, sondern ausschließlich von der Passwortstrategie des Benutzers abhängig ist (vgl. hierzu auch [KS08] und Kapitel 4.3).

Es bestätigt sich, dass die Verwendung von Single-Sign-On-Systemen als Vertreter passwortbasierter Systeme am Beispiel von Kerberos V5 unter Berücksichtigung der bekannten Sicherheitsschwachstellen für verteilte Systeme durchaus empfehlenswert ist. Die These „erhöhen Single Sign-On-Systeme die Sicherheit“ kann somit, im direkten Vergleich mit herkömmlichen passwortbasierten Authentifikationssystemen verifiziert werden.

Diese Arbeit sieht vor, die untersuchten Thesen abschließend zur These „erhöhen vorgegebene Passwortwechsel die Sicherheit von Single Sign-On-Systemen“ zusammenzufassen und zu untersuchen. Da die erste These jedoch falsifiziert wurde kann aus dieser, in Kombination mit der verifizierten zweiten jedoch logisch kein Nutzen gezogen werden, weswegen diese Untersuchung entfällt.

[13] Hieraus folgt implizit, dass bei der Verwendung von nur einem Zugangsdatensatz die Belastung des Nutzers, sich mehrere komplexe Passworte zu merken, sinkt. Ergo folgt logisch, dass die Bereitschaft des Benutzers, sich *ein* komplexes und dadurch qualitativ hochwertigeres Passwort für ein Single Sign-On-System auszudenken und dieses zu merken, steigt.

6. Schluss

Dieses Kapitel bildet den Abschluss der Bachelorarbeit und fasst die Arbeit und die gewonnenen Erkenntnisse zusammen. Zusätzlich bietet es einen Ausblick auf aktuelle Arbeiten, die dieses Thema weiterführen.

6.1. Zusammenfassung

Sicherheit ist ein menschliches Grundbedürfnis und auch in der Informations- und Kommunikationstechnologie ein immer wichtiger werdender Schwerpunkt. Während der Mensch die eigene Sicherheit intuitiv einschätzt und subjektiv unabhängig von tatsächlichen Gegebenheiten empfindet gelten für die Sicherheit der IKT Richtlinien und Standards, um einen gleichbleibenden Sicherheitslevel zu gewährleisten.

Die Psychologie hilft uns zu verstehen, warum Menschen sich nicht selten sicherheitskritisch verhalten und damit gegen Regeln und Anweisungen verstossen, die die Sicherheit der Mitarbeiter und zu verarbeitetenden Daten schützen sollen. Der Ursprung liegt in Heuristiken, die seit Urzeiten das Fortbestehen sichern sollte, aber noch keine Anpassung an die heutige schnelllebige Zeit gefunden hat - offensichtlich unsichere Handlungen werden nicht als solche erkannt, weil andere Ziele im Vordergrund stehen. Diese unterbewusst gesteuerten Verhaltensweisen lassen sich nur schwerlich abschalten, müssen also in die Planung und Durchführung von Sicherheitsmaßnahmen mit einbezogen werden.

Die Authentifizierung mittels Passworten ist heute allgegenwärtig doch galt es innerhalb dieser Arbeit zu beurteilen, ob die Sicherheit durch erzwungene Passwortwechsel erhöht wird. Durch den Zusammenhang menschlichen Verhaltens und dessen Einfluss auf die Konstruktion und Erinnerbarkeit von Passworten stellt sich heraus, dass die die verwendenden Techniken, Passworte sicher zu gestalten und deren Sicherheit zu erhöhen durchweg durchdacht, jedoch mit dem menschlichen Verhalten nicht problemlos vereinbar sind. Die Herausforderung liegt darin, den „human factor“ in Sicherheitsüberlegungen mit einzubeziehen. Unter anderem aus diesem Grund erhöhen erzwungene Passwortwechsel die Sicherheit in keinerlei Hinsicht.

Das Passwort ist der Single-Point-of-Failure eines jeden passwortbasierten Authentifikationssystems, wodurch dieses nur so sicher ist wie das Passwort selbst. Single Sign-On Systeme

als deren benutzerfreundlicher Vertreter bieten einen komfortablen Zugang zu allen benötigten Ressourcen, sind aber ebenso anfällig für die Kompromittierung der Benutzerpasswörter, da nach der initialen Anmeldung mittels Passwort i.d.R. keine erneute Authentifikation erfolgt. Grundsätzlich ist der Schutz eines einzigen Zugangs einfacher als der vieler, sodass zumindest in technischer Hinsicht deutlich weniger Schutzmechanismen zu implementieren sind als bei einer Architektur aus einzelnen Applikationen mit jeweils eigener Benutzerdatenverwaltung, wodurch Single Sign-On-Systeme sicherer als herkömmliche passwortbasierte Authentifikationssysteme sind.

6.2. Fazit

Diese Arbeit konnte am Beispiel von Kerberos herausstellen, dass der Faktor Mensch ein wesentlicher und nicht zu vernachlässigender Schwerpunkt in der Sicherheit passwortbasierter Authentifikationssysteme ist. Nur unter dessen Einbeziehung kann die Sicherheit eines jeden Systems, dass auf Passwortverwendung beruht, gewährleistet werden, da die Passwortsicherheit maßgeblich von der Sicherheitseinschätzung und der damit verbundenen Passwortwahl des Benutzers abhängt. Um es mit den Worten Bruce Schneiers zu sagen:

> „Für soziale Probleme gibt es keine technischen Lösungen." Bruce Schneier [Sch01, S. 380]

Die zukünftige Herausforderung liegt nach Meinung der Autorin darin, unmotivierte Benutzer zu mehr Sicherheitsbewusstsein zu erziehen ohne diese zu langweilen oder abzuschrecken - ebenso jedoch auch seitens der Software-Designer die Sicherheitsaspekte weniger transparent zu gestalten, um Mißbrauch durch Unwissenheit zu verhindern.

Bei der Untersuchung der zweiten These stellte sich heraus, dass Single Sign-On-Systeme sicherer als herkömmliche passwortbasierte Authentifikationssysteme sind, jedoch ist die Authentifikation via Passwort als schwächste aller Authentifikationstechniken (Wissen, Besitz, biometrische Merkmale) einzustufen.

Der aktuelle Trend führt voraussichtlich darin, die Authentifizierung zu verstärken indem auf die Kombination von Authentifikationstechniken zurückgegriffen wird (siehe auch Anhang B). Auf diese Weise kann die Sicherheitsbeeinflussung durch menschliches Handeln (siehe Kapitel 4.3) reduziert werden.

Als persönliches Fazit möchte die Autorin hinzufügen, dass die Anfertigung der Arbeit Anlass dazu gegeben hat, eigene Handlungsweisen in Bezug auf Passwortstrategien und deren Sicherheit zu überbedenken und diese Informationen an Familie und Freunde weiterzugeben.

6.3. Ausblick

> „I expect the interaction between security and psychology to be a big research area over the next five years, just as security economics has been over the last five. This is not just because of the growing number of attacks that target users instead of (or as well as) technology. For example, terrorism is largely aboutmanipulating perceptions of risk; and even outside the national-security context, many protection mechanisms are sold using scaremongering.“ Ross Anderson [And08, S. 22]

Einige Kolleginnen und Kollegen der Informatik beschäftigen sich bereits seit Jahren sowohl mit den Themen Sicherheit als auch dem Zusammenhang von Sicherheit und Psychologie, wie es auch der Ansatz dieser Arbeit ist. Einige zukunftsweisenden Arbeiten sollen nachstehend, kategorisiert nach deren Schwerpunkt, kurz genannt werden, sofern sie nicht bereits im Hauptteil der Arbeit argumentativ verwandt wurden. Diese geben dem interessierten Leser die Möglichkeit den aktuellen Trend, die Passwortsicherheit und Single Sign-On-Entwicklung betreffend, zu verfolgen.

6.3.1. Arbeiten zur Passwortsicherheit

Honeywords

Ronald L. Rivest ist amerikanischer Mathematiker und Kryptologe und besonders als Mitbegründer[1] des asymmetrischen RSA-Verfahrens zur Verschlüsselung bekannt.

Jüngst veröffentlichte er die Arbeit „Honeywords - Making Password-Cracking Detectable“ (siehe [RJ13]) und schlägt darin vor, zusätzlich zu den korrekten Benutzerpassworten in gehashten Passwortdateien auch weitere Zeichenketten abzuspeichern, die sogenannten Honeywords. Honeywords sind falsche Passwörter, deren Verwendung durch einen zusätzlichen Server (dem „honeychecker“) überwacht werden soll.

Wird eine Passwortdatei kompromittiert und kann diese durch den Angreifer entschlüsselt werden wird der Versuch, sich mit einem Honeyword Zugriff zu verschaffen bemerkt und löst einen Alarm aus.

Anstatt das Hashen von Passworten komplexer zu gestalten, was zu einem höheren Zeitaufwand beim Authentifizierungsprozess führen würde nahm Rivest sogenannte „Honeypot Accounts“ als Anregung für seine Arbeit. Honeypots sind falsche Benutzeraccounts, deren Verwendung auf einen Angriff von außen hinweist.

[1] Zusammen mit Adi Shamir und Leonard Adleman

Der Vorteil von Honeywords liegt laut Rivest darin, dass der Überwachungsserver einfach zu implementieren und abzusichern ist. Weiterhin gilt die Möglichkeit, Zugriffe auf die gehashte Passwortdatei zu sichten und darauf reagieren zu können für alle Benutzer, wohingegen Honeypots nur die eventuelle Kompromittierung der gefälschten Accounts aufdecken kann. Hat der Angreifer eine Möglichkeit zu erkennen, ob es sich um einen falschen Benutzerzugang handelt (z.B. durch eine Liste von Mitarbeiternamen) kann ein Zugriff auf einen regulären Benutzerzugang nicht bemerkt werden.

Studie zur rationalen Passwortwahl und -kategorisierung

[DJG12] verwendet die Vermutung, dass es Faktoren (oder Constraints, engl. für Bedingungen) außerhalb des Sicherheitsbewusstseins gibt die das Passwortverhalten beeinflussen, als Basis seiner Arbeit. Die Studie untersucht unter anderem psychologische Hintergründe, wie Benutzer auf Anreize reagieren und warum Security Policies aufgrund Kosten-Nutzen-Abwägungen der Benutzer scheitern können. Weiterhin sollte untersucht werden, ob Benutzer ihre Passworte an die Sicherheitslevel der entsprechenden Dienste anpassen.

Untersucht wurden drei Kategorien von Benutzern: sechs Informatiker (computer scientists), sechs Administratoren und zehn Studenten. Für jede Gruppe sollten beeinflussende Faktoren ermittelt werden.

Die Untersuchung ergab unter anderem, dass nur die Informatiker sich erwartungsgemäß verhielten und unterschiedliche Passworte für unterschiedliche Dienste, angepasst und abhängig von Sicherheitseinstufung und Verwendungshäufigkeit wählten. Sowohl Administratoren als auch Studenten nahmen keine nennenswerten Unterscheidungen der Passworte vor.

Auch die Annahme, dass durch das Wissen über sichere Passwortgestaltung und -verwendung die Wiederverwendung von Passworten bei sicherheitsrelevanten Diensten geringer wäre erfüllte sich lediglich bei der Informatikergruppe. Administratoren und Studenten bewiesen, dass hier kein Zusammenhang besteht und lagen in den Ergebnissen gleichauf.

Es ergab sich zudem, dass die Informatikergruppe die korrekte und sichere Verwendung von Passworten als Teil ihrer Arbeit und ihres Aufgabengebietes sieht, die anderen Gruppen stufen dies jedoch als Kosten ein, die sie von der Erfüllung ihrer Arbeit/Aufgabe abhält. Die Wahl eines einfachen, leicht zu erinnernden Passwortes führt diese Nutzer zu einer subjektiven Gewinneinschätzung.

Zusammenfassend gibt die Studie Aufschluss darüber, dass Gruppen von Personen unterschiedlicher (Vor-) Bildung sich unterschiedlich bezüglich der Wahl und Verwendung von Passworten verhalten, abhängig von nicht komplett untersuchten, aber parallel ablaufenden Bedingungen. Der Autor hofft, unter anderem aufgrund der geringen Teilnehmerzahl inner-

halb seiner Studie, auf weitere Studien in diese Richtung zur zukünftigen Verbesserung der Sicherheit.

6.3.2. Arbeiten zur Sicherheit von Single Sign-On-Systemen

Der Trend von Single Sign-On-Systemen geht momentan in Richtung Web-SSO, also der Nutzung eines einzelnen Zugangsdatensatzes um verschiedenste Dienste des Internets zu nutzen, für die eine Authentifizierung notwendig ist.

Aktuell finden Technologien wie SAML und OpenID Anklang (nähere Informationen sind im Anhang C zu finden), die in reiner oder abgewandelter Form von Portalen wie Google, Facebook etc. verwendet werden. Die nachfolgenden Arbeiten befassen sich sowohl mit der Sicherheit als auch mit den psychologischen Aspekten in diesem Kontext.

Einzig die Arbeit zur erfolgreichen Fälschung von SAML Assertions soll hier nicht genannt werden, weil diese bereits im Anhang C.1, aktuelle Schwächen von SAML, erläutert wird.

6.3.3. Behavioral biometrics for persistent single sign-on

Single Sign-On-Systeme haben durch die einmalige Identifizierung einen Single-Point-of-Failure Charakter. [BSGM+11] hebt hervor, dass das Risiko des Mißbrauchs besonders hoch ist, wenn der Benutzer sein Gerät (PC, Tablet o.ä.) im eingeloggten Zustand unbeaufsichtigt lässt. Die Autoren erarbeiten ein Persistant SSO (PSSO) für die häusliche Umgebung (z.B. sogenannte Smart Homes), das verhaltensabhängige Biometrie nutzt.

Anstatt eine feste Dauer einzuführen, die nach einer bestimmten maximalen Nutzungszeit bzw. eines Inaktivitätszeitraums ein automatisches Abmelden verursacht soll die Benutzeridentität durchgehend unauffällig gemessen werden. Dies erfolgt dadurch, dass sich der Benutzer zunächst via Webbrowser authentifiziert - die Überprüfung der Identität erfolgt permanent durch einen sogenannten „Behaviour Monitor“, der mit dem genutzten Gerät gekoppelt ist. Der Datenverkehr wird mittels SAML abgewickelt.

Single Sign-On mit OTP

OTP steht für Einmal-Passworte, die mittels Hilfmittel generiert werden (siehe auch Anhang A). [TJ09] kombiniert klassisches Single Sign-On mit dieser Technologie, um die Authentifizierung zu verstärken. Die Java-basierte Lösung kann mit minimalem Aufwand und ohne zusätzliche Hard- oder Software in bestehende Systeme integriert werden.

SSO-Design für eine Anwendung in der Cloud

[RB11] konstruiert eine Cloud[2]-basierte Single Sign-On-Lösung, die Rechnerkapazität und Datenspeicher in die Cloud verlegt, während die Authentifikation auf einem SSO-Server verbleibt. Der Autor sieht den Vorteil darin, dass die Authentifikation unangetastet von Ressourcenerweiterungen oder -verringerungen bleibt und zudem bestehende Infrastrukturen unverändert bleiben.

[2]Cloud bzw. Cloud Computing (Rechnerwolke) beschreibt den Ansatz, Rechnerkapazität, Datenspeicher oder komplette Betriebssysteme oder Anwendungen dynamisch über ein Netzwerk zur Verfügung zu stellen. Dem Benutzer ist dabei nicht klar, wo sich seine Daten tatsächlich befinden, was zur Begriffsbildung beigetragen hat.

Anhang

A. Einmal-Passworte

Einmal-Passworte bzw. One Time-Passwords (OTP) werden vom Client zum Server übertragen wie herkömmliche Passworte auch. Die Unterscheidung liegt jedoch darin, dass der Benutzer über ein Geheimnis s verfügt, dass zwar zur Generierung des OTP verwendet, jedoch nicht übermittelt wird.

Authentifikationsablauf Wie in Abbildung A.1 zu sehen wird in der Initialisierungsphase mit einem zwischen Benutzer und Client vereinbartem Geheimnis s, das länger als 8 Zeichen sein soll, sowie einer kryptographisch sicheren Hashfunktion f und einem Seedwert k eine Folge von einmal benutzbaren Passworten $p_i, .., p_n$ erzeugt.

Es gilt: $p_i = f^i(s|k)$ für $i = 1, .., n$. Durch das S/Key-Verfahren werden dem Server stets nur Einmalpassworte übermittelt, nicht aber das Geheimnis s.

Übermittelt der Client in der anschließenden Authentifizierungsphase nun den Benutzernamen erhält er neben dem Index i auch den Serverseed k. Hiermit führt das S/Key-Verfahren auf dem Clientrechner die kryptographische Hashfunktion f i-mal auf das Geheimnis s aus, konkateniert das Ergebnis mit dem Seed k und liefert ein 64bit langes Einmalpasswort p_i zurück, das dann an den Server übermittelt werden kann.

Im Anschluss überprüft der Server dann, ob gilt: $f(p_i - 1) = p_i$ - dies ist möglich da die Passwortkonstruktion $p_i = f^i(s|k) = f(f^i - 1(s|k)) = f(p_i - 1)$ gilt - der Server kann effizient berechnen ob $f(p_i - 1) = p_i$ ist.

Die Ausgabe der i Einmalpassworte erfolgt in je 6 Blöcken à maximal 4 Buchstaben. Hier handelt es sich um Begriffe, die aus einem 2048 Wörtern starkem englischen Wörterbuch entnommen wurden. Alternativ zu dieser ursprünglich Software basierten Lösung finden auch sogenannte Hardwaretoken oder Applikationen auf Handys/Organizern, die mit OTPs bzw. zeitlich begrenzten OTPs arbeiten und als Passwortgenerator fungieren, Anwendung (vgl. [BSSW11], siehe auch Abbildung A.2).

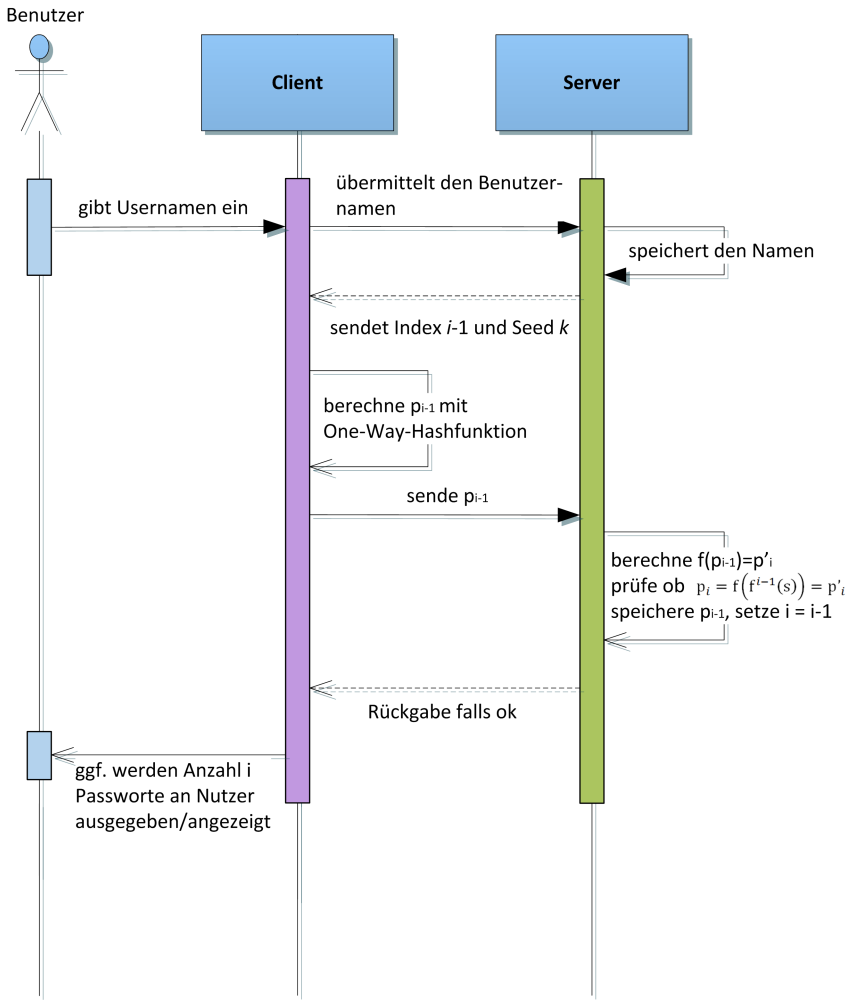

Abbildung A.1.: Sequenzdiagramm der Client-Server-Kommunikation beim S/Key Verfahren

Abbildung A.2.: Auswahl von hardwarebasierten OTP-Token der Firma RSA [RSA12]

B. Zwei- und Multi-Faktor-Authentifikation

Zwei-Faktor-Authentifikation bedeutet, dass zur eindeutigen Identitätsfeststellung mehr als eine der Authentifikationstechniken Wissen, Besitz und biometrische Merkmale verwendet wird. Auf diese Weise soll die Sicherheit erhöht sowie die Vorteile der verschiedenen Techniken genutzt werden. Die häufigste Kombination ist die von Wissen und Besitz, wie z.B. der Authentifikation eines Bankkunden an einem Geldautomaten. Hier stellt die Bankkarte den persönlichen Besitz, die Kenntnis der PIN das Wissen dar. Bislang sind Authentifikationen über biometrische Daten wie z.B. einem Fingerabdruck in Kombination mit anderen Techniken noch selten, da hier die Schwierigkeit besteht aktuelle Werte mit Referenzwerten zu vergleichen (vgl. [Eck12]).

Beispiele für Zwei-Faktor-Authentifikation:

- Online Banking mit Passwort und PIN-Abfrage[1] - Der Anmeldevorgang erfolgt zunächst mit Kontonummer und einem sechsstelligen Passwort - im Anschluss wird eine sechsstellige PIN abgefragt. Um automatisierte Eingaben zu vermeiden, werden stets nur zwei von sechs Ziffern (randomisiert) abgefragt.
- Zugang zum Schufa-Verbraucherservice[2] - nach einer Registrierung mit gültigem Personalausweis online oder persönlich vor Ort erhält man Benutzername und Initialpasswort. Nach dem Anmelden mit diesen Daten erfolgt eine zweite Abfrage mittels der sogenannten XS-Card, die per Post zugesandt wird. Wie in Abbildung B.1 zu sehen werden im Anschluss drei beliebige Felder der Karte abgefragt, um die Identifikation abzuschließen.
- [Vie09] entwickelte ein System namens OPUS, welches nach der Eingabe des Benutzernamens einen Passcode als SMS an eine bei der Registrierung angegebene Handynummer versendet. Auf diese Weise muss keine Passwort, sondern lediglich der Benutzername erinnert werden, jedoch neben dem Wissen um den Benutzernamen auch der Besitz des registrierten Handys vorhanden sein.

[1] auf diese Weise bei der `http://www.ing-diba.de`

[2] die Schufa ist eine Auskunftei über die persönliche Kreditwürdigkeit jeder Person, die in Deutschland gemeldet ist.

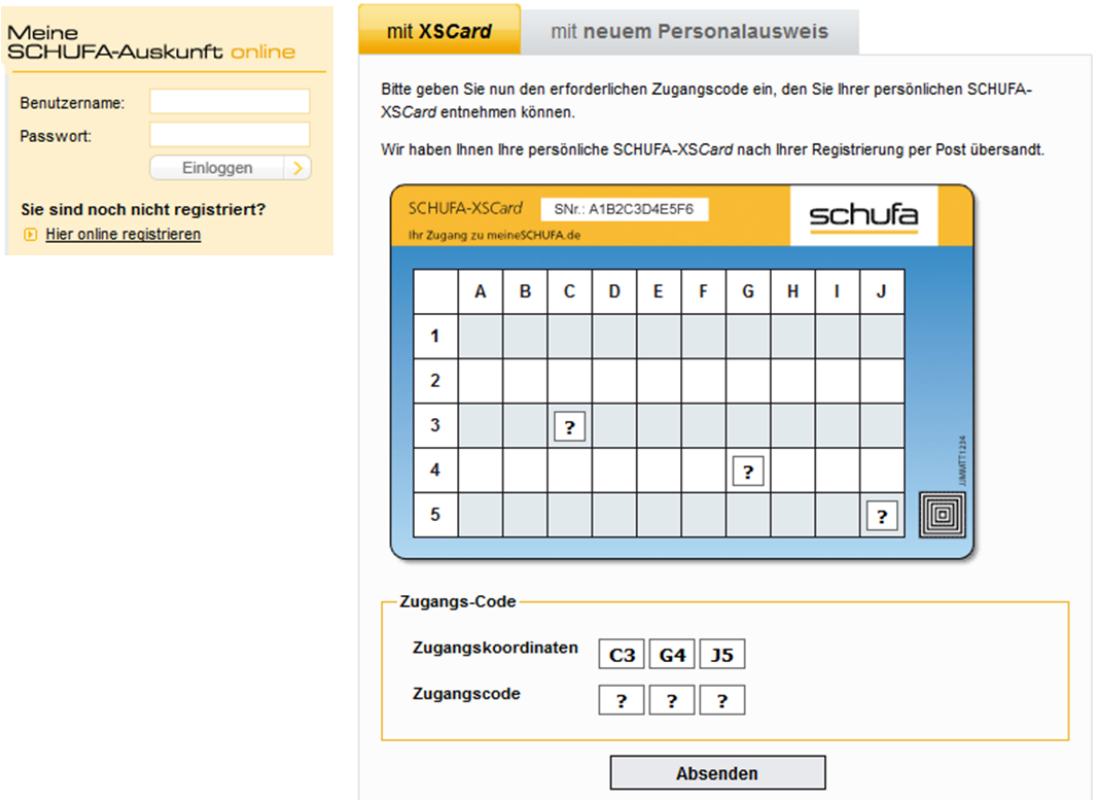

Abbildung B.1.: Anmeldevorgang beim Verbraucherportal der Schufa unter `http://www.meineschufa.de`

- Apple, Twitter, Google

C. weitere SSO-Technologien

C.1. Security Assertion Markup Language (SAML)

Grundlagen und Definition Seit des Durchbruchs des Internets und der damit verbundenen Masse an authentifizierungspflichtigen Webseiten wird auch der Wunsch der Benutzer nach Single Sign-On Lösungen im Internet, sogenanntem Web SSO, laut. Nach einem ersten Ansatz durch den Microsoft „Passport“ Dienst 1999 etablierte sich 2001 die Security Assertion Markup Language (SAML), von OASIS (Organization for the Advancement of Structured Information Standards)[1] als Framework zum Austausch von Authentifizierungs- und Autorisierungsinformationen entwickelt. Diese wurde 2002 erstmals publiziert, in der aktuellen Version 2.0 arbeitete das Liberty Alliance Project (LAP)[2] mit. SAML zählt zu SOA (Service-orientierte Architektur) und bietet anderen Services eine Plattform- und Programmiersprachen-unabhängige Schnittstelle (vgl. [Eck12],[Rus10]).

Architektur und Terminologie SAML ist ein Framework das auf XML (engl., Extensible Markup Language, erweiterbare Markup-Sprache) basiert und durch seine Flexibilität über Organisationsgrenzen hinweg einsetzbar ist. Der Zweck ist die Definition, Erweiterung und der Ausbau eines Standards zum Erzeugen und Austauschen von Authentifizierungs- und Authorisierungsinformationen mit dem Hintergrund eines offenen Standards. Anfragen und Antworten werden in Form eines XML-Dokuments zwischen dem Client, einem *Identity Provider* (IdP) und einem *Service Provider* (SP) ausgetauscht und mittels *Assertions* (engl., Bedingungen/Voraussetzungen, siehe unten) festgelegt (vgl. [OAS05a], [OAS05b]).

Der Identity Provider kann ein System oder eine administrative Domain sein, die Informationen über ein Subjekt[3] festlegt, z.B. die Bedingung dass der Benutzer authentifiziert sein und über bestimmte Attribute verfügen z.B. muss (z.B. soll der Benutzer eine Emailadresse haben

[1] `https://www.oasis-open.org/`

[2] inzwischen: Kantara Initiative, `http://kantarainitiative.org/` mit. Zusammenschluss aus namhaften Unternehmen (z.B. AOL, Deutsche Telekom, Sun, Intel, Oracle) seit 2001 mit gemeinsamer Vision von offenen Standards, die zugleich die Privatsphäre und Sicherheit der Nutzer u.a. durch eine universelle und starke Authentifikation sichern.

[3] im SAML-Kontext bezeichnet Subjekt den Benutzer.

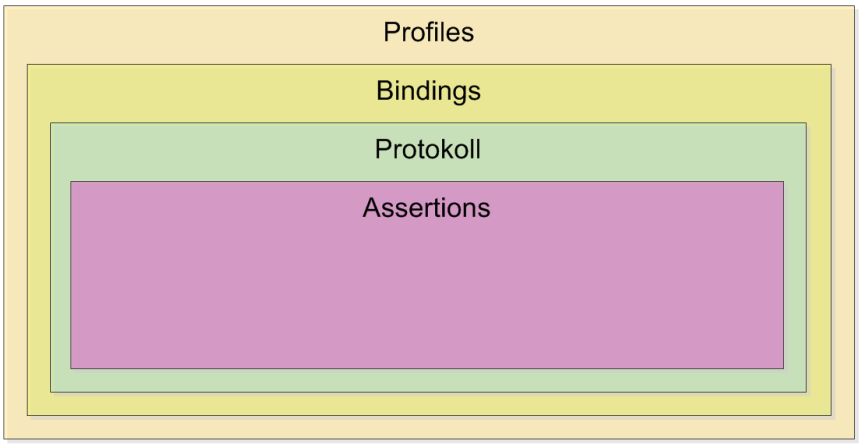

Abbildung C.1.: SAML-Komponentenübersicht nach [OAS05b]

und mittels Passwortverfahren authentifiziert worden sein). Identity Provider werden in SAML auch als *SAML Authorities* oder *Asserting Parties* bezeichnet.

Service Provider können ebenfalls Systeme oder administrative Domains sein, die jedoch von den Informationen abhängig sind die die IdPs ihnen zur Verfügung stellen - daher auch die alternative Bezeichnung *Relying Parties*. Der SP gibt die Richtlinien vor, ob er den gelieferten Assertions vertraut und unabhängig davon, auf welche Ressourcen das Subjekt Zugriff erhält.

Die Architektur von SAML basiert auf Komponenten die aufeinander aufbauen, siehe auch Abbildung C.1. *Assertions* sind in einem XML-Schema definierte Informationen über den Benutzer (auch: Principal), die vom SP angefordert und unaufgefordert zugeschickt werden. Wie in und in welcher Form diese benötigt werden gibt ein *SAML Protokoll* vor, wiederum in einem eigenen XML-Schema definiert. *Bindings* (engl., Bindung) bestimmen im Anschluss, mittels welches Nachrichtenprotokolls (z.B. HTTP, SOAP[4] die Daten versendet werden sollen. *Profiles* fassen dann bestimmte Kombinationen von SAML Protokollen, Bindings und Assertions zu einem Profil zusammen, ähnlich eines Use Cases, z.B. gibt es ein Web Browser SSO Profil. Profile können sich jedoch auch nur auf Attribute beziehen und definieren, wie Identitäts- und Attribut-Informationen innerhalb einer Assertion behandelt werden. Assertions als Authentifikationsbescheinigung sind konzeptionell mit einem Kerberos-Ticket vergleichbar (vgl. [Eck12]).

```
1 <saml:Assertion
2 MajorVersion= 1 MinorVersion=0
```

[4]Simple Object Access Protocol; XML verwendendes Netzwerkprotokoll das sich auf HTTP stützt, siehe auch http://www.w3.org/2000/xp/Group/

```
3  AssertionID=128.9.167.32.12345678
4  Issuer=Smith Corporation
5  IssueInstant=2001-12-03T10:02:00Z />
6  <saml:Conditions
7  NotBefore=2001-12-03T10:00:00Z
8  NotAfter=2001-12-03T10:05:00Z />
9  <saml:AuthenticationStatement
10 AuthenticationMethod=password
11 AuthenticationInstant=2001-12-03T10:02:00Z>
12 <saml:Subject>
13 <saml:NameIdentifier
14 SecurityDomain=smithco.com
15 Name=joeuser />
16 </saml:Subject>
17 </saml:AuthenticationStatement>
18 </saml:Assertion>
```

Listing C.1: Beispiel einer Assertion für *joeuser* nach [Eck12]

Zwei weitere Komponenten, die nicht in Abbildung C.1 illustriert sind, können ebenfalls zum Aufbau eines SSO-Systems verwendet werden: *Metadata* und *Authentication Context*. Metadaten geben an, wie Konfigurationsinformationen zwischen zwei kommunizierenden Entitäten definiert und ausgetauscht werden, während Authentication Context dem IdP zusätzliche Authentifizierungsinformationen bereitstellen kann, wie es z.B. bei Multifaktorauthentifikation notwendig ist.

Um die Authentifikation eines Benutzers sicherzustellen gibt es zwei Varianten - die IdP-initiated und SP-initiated Authentication. Der Unterschied besteht darin, dass bei der Nutzer bei der IdP-initiated Authentication nach der Ressourcenanfrage an den SP weitergeleitet wird, um sich zu authentifizieren, wohingegen bei der SP-initiated Authentication der IdP eine Anfrage an den SP schickt, die dieser beantwortet (siehe auch Abbildung C.2).

Identitätsmanagement

> „Identity management refers to the process of employing emerging technologies to manage information about the identity of users and control access to company resources. The goal of identity management is to improve productivity and security while lowering costs associated with managing users and their identities, attributes, and credentials.“ Spencer C. Lee [Lee03, S. 3]

Somit kann Web SSO mittels SAML als Identitätsmanagementsystem verstanden werden. Identität beschreibt im SAML-Kontext eine Menge von Attributen, die ein Subjekt umfassend

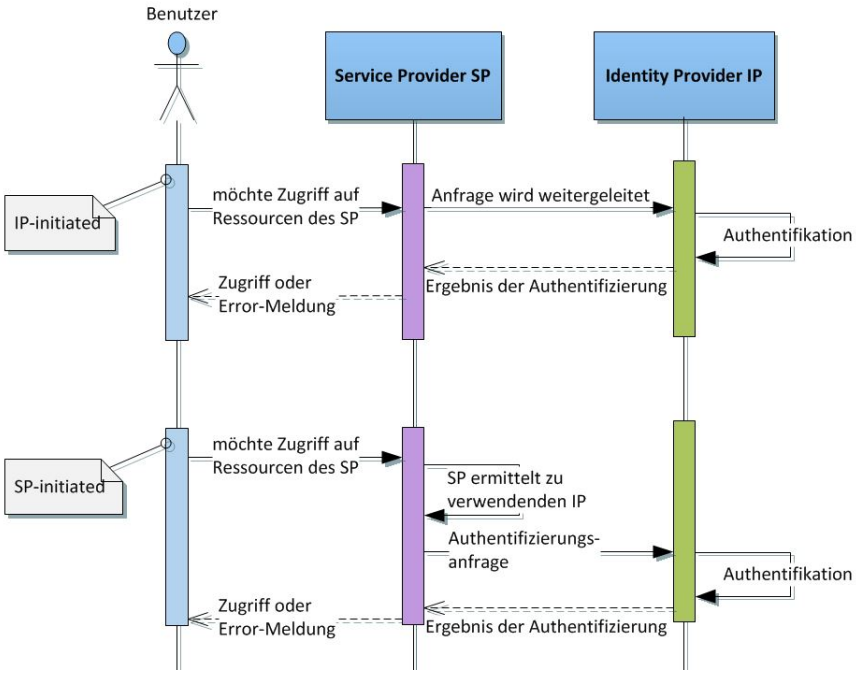

Abbildung C.2.: Sequenzdiagramm für IdP- und SP-initiated Authentication

beschreibt. Ziel von Identitätsmanagementsystemen ist die Schaffung einer *Federate Identity* (engl., föderierte/zusammengeschlossene Identität), eine für den Benutzer nicht sichtbare Verwaltung und Verwendung der authentifizierten Identität an unterschiedlichsten, Unternehmensgrenzen überwindenen SPs (*federated identity systems*), die durch den IdP gewährleistet wird. Der Benutzer empfindet eine stärkere Sicherheit und mehr Komfort, SPs können den Authentifizierungsaufwand an IdPs delegieren un eine gleichbleibende Sicherheit und Servicequalität gewährleisten. Eine Föderation von SPs entspricht zudem dem Grundgedanken von SOA (vgl. [Jäg11]).

Anwendungsmöglichkeiten [OAS05b] nennt vier grundlegende Anwendungsbereiche, die treibende Kraft bei der Entwicklung der SAML-Technologie waren. Um den Rahmen der Arbeit einzuhalten werden diese nur kurz angeschnitten.

- **Browser-Cookie Einschränkungen:** Cookies werden regulär verwendet, um eine Reauthentifizierung eines Nutzers zu verhindern. Diese sind aber nicht übermittelbar, um z.B. eine andere Domain zu informieren, dass der User bereits authentifiziert wurde, wie es bei SAML durch die Verwendung des IdP der Fall ist.

- **Web Services:** Web Services sind ein relativ junger Markt - Sicherheitskonzepte sind noch nicht komplett definiert. SAML stellt Standards zur Verfügung, wie Authentifizierung und Authorisierung mittels Assertions zwischen kommunizierenden Entitäten ausgetauscht werden können.
- **Federation:** Um Identitätsmanagement innerhalb organisatorischer Grenzen zu vereinfachen können viele einzelne Identitäten zu einer (oder zu wenigen) föderierten Identitäten (siehe auch Unterkapitel C.1) zusammengefasst werden.
- **SSO Interoperabilität:** unabhängig davon, welche SSO-Produkte innerhalb eines Unternehmens oder eines Konzerns bzw. zwischen einem Unternehmen und dessen Handelspartnern implementiert sind bietet SAML durch dessen offenen Standard die Möglichkeit, ohne Einschränkungen zu kommunizieren.

Populäre Frameworks [SMS+12] stellt in seiner Arbeit 14 Anbieter von SAML Frameworks vor (siehe Tabelle C.1), wovon bei einigen die SSO Funktionalität zwar implementiert ist, jedoch ausdrücklich aktiviert werden muss. [SMS+12] unterscheidet zwischen Web SSO Lösungen und WS-(für Web Service)-Lösungen. Ein Web Service ist eine im Netz bereitgestellte Komponente, die eine Abstraktionsebene einer Anwendungslogik darstellt. Auf den Dienst kann über Internetstandardprotokolle zugegriffen werden, für die Kodierungen der Nachrichten wird XML genutzt. Dies soll eine einfache Bereitstellung und hohe Verfügbarkeit von Web Services gewährleisten um unabhängig von Plattform und Programmiersprachen miteinander kommunizieren und arbeiten zu können.[5]

C.1.1. Sicherheit von SAML

Netzwerkkommunikation Um die Kommunikation zwischen Kommunikationspartnern abzusichern und Vertrauensbeziehungen zwischen den beteiligten Parteien aufzubauen empfiehlt OASIS[6] die Nutzung einer PKI und der Web Service Sicherheitsstandards (XML-Signature, XML-Encryption) um auf diese Weise digital signierte bzw. verschlüsselte Assertions auszustellen. Da der Transport über das Internet generell unsicher ist sollte man Standardverfahren wie SSL/TLS oder IPsec verwenden, um ihn abzusichern. Das Dokument schlägt Sicherheitsmaßnahmen für alle bekannten Threats vor und orientiert sich am IETF Threat Model[7].

[5] http://www.golem.de/specials/webservice/
[6] http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf
[7] http://tools.ietf.org/html/draft-rescorla-sec-cons-00

Framework/ Provider	Type	Language	Reference	Application
Apache Axis 2	WS	Java	http://axis.apache.org	WSO2 Web Services
Guanxi	Web SSO	Java	http://guanxi.sourceforge.net	Sakai Project (www.sakaiproject.org)
Higgins 1.x	Web SSO	Java	www.eclipse.org/higgins	Identity project
IBM XS40	WS	XSLT	www.ibm.com	Enterprise XML Security Gateway
JOSSO	Web SSO	Java	www.josso.org	Motorola, NEC, Redhat
WIF	Web SSO	.NET	http://msdn.microsoft.com	Microsoft Sharepoint 2010
OIOSAML	Web SSO	Java, .NET	http://www.oiosaml.info	Danish eGovernment (e.g. www.virk.dk)
OpenAM	Web SSO	Java	http://forgerock.com/openam.html	Enterprise-Class Open Source SSO
OneLogin	Web SSO	Java, PHP, Ruby, Python	www.onelogin.com	Joomla, Wordpress, SugarCRM, Drupal
OpenAthens	Web SSO	Java, C++	www.openathens.net	UK Federation (www.eduserv.org.uk)
OpenSAML	Web SSO	Java, C++	http://opensaml.org	Shibboleth, SuisseID
Salesforce	Web SSO	—	www.salesforce.com	Cloud Computing and CRM
SimpleSAMLphp	Web SSO	PHP	http://simplesamlphp.org	Danish e-ID Federation (www.wayf.dk)
WSO2	Web SSO	Java	www.wso2.com	WSO2 products (Carbon, ESB, . . .)

Tabelle C.1.: populäre SAML Frameworks nach [SMS+12]

Zugriffskontrolle Da es keine Bindung zwischen dem Subjekt und der ausgestellten Bescheinigung gibt besteht ohne die vorgenannten Sicherheitsmaßnahmen z.B. die Gefahr von Man-in-the-Middle-Angriffen, weil das Subjekt nicht nachweisen kann ob eine Bescheinigung aktuell ist oder es zur Nutzung berechtigt ist. Kerberos löst dieses Problem mit seinem Authentikator-Konzept.

Statt eines Subjekt-bezogenen Ansatzes unterstützt SAML die Möglichkeit einer Zugriffskontrolle, die auf Attributen basiert. Auf diese Weise wird der Zugriff auf eine Ressource durch spezifische Attribute limitiert. Hier kann auf die Sprachkonzepte von *XACML* (Extensible Access Control Markup Language) zurückgegriffen werden, welche ebenfalls XML-basiert ist und von OASIS entwickelt wurde. Hierdurch lassen sich Subjekt-bezogene Regeln (*Policies*) definieren (vgl. [Eck12]).

aktuelle Schwächen [SMS+12] erregte 2012 Aufsehen damit, dass es den Autoren gelungen war SAML Assertions zu fälschen. Die Angriffstechnik *XML Signature Wrapping* wurde bereits 2005 durch McIntosh und Austel entdeckt und kann bei Vorlage einer signierten Assertion verwendet werden um alle XML Signature Sicherheitsfunktionen auszuhebeln.

[SMS+12] ermittelt eine neue Art des Wrapping-Angriffes, indem die Assertion, die einen fiktiven User an einem Service Provider authentifiziert, wie folgt verändert wird: in der Response wird ein Wrapper eingebaut, der die Assertion ohne Signature enthält. Anschließend wird die eigentliche Assertion nach eigenen Wünschen verändert. Erhält der Service Provider die modifizierte Assertion, validiert er zunächst die Assertion (aus dem Wrapper) mit der Signature. Anschließend wird die überschriebene Assertion verarbeitet. Auf diese Weise trifft der Titel der Arbeit zu: „be whoever you want to be“.

Selbstverständlich bietet [SMS+12] auch Gegenmaßnahmen an, die zur Verbesserung der Technologien an die getesteten Framework-Hersteller (siehe Tabelle C.1 weitergereicht wurden. Gegenmaßnahme 1 lautet *Strict Filtering*: der Rückgabewert der Signaturverifikation sollte nicht mehr der boolesche Wert des Ergebnisses, sondern die Assertion selbst sein. Auf diese Weise ist eine Manipulation der Assertion wirkungslos. Diese Maßnahme ist jedoch aufgrund des XML Security Gateways[8] nicht in verteilten SOA-Umgebungen einsetzbar. Gegenmaßnahme 2 erfordert, geprüfte Elemente zu markieren, beispielsweise mit einer Zahl r, die als Attribut ebenfalls mit versendet wird. r kann eine beliebige Zufallszahl sein, sichert jedoch durch ihren Versand innerhalb der Assertion ab, dass es sich bei der Assertion wirklich um eine echte Response des IdP handelt. Hierfür müsste jedoch das SAML XML Schema erweitert werden, positiv ist aber die Verwendbarkeit in verteilten SOA-Umgebungen.

Die Erkenntnisse der Autoren wurden auch verwendet, um ein Penetration Test Tool für XML-Wrapper Angriffe zu konstruieren. Da es jedoch immer wieder zu Permutationen kommt, können Wrapper-Angriffe nicht grundsätzlich abgewehrt werden - daher raten die Autoren zu weiteren Schutzmaßnahmen.

Fazit SAML wickelt als Framework die Authentifizierung zwischen dem Client und Service Provider und Identity Provider ab, ist damit jedoch lediglich so sicher wie die Auftraggeber selbst. Orientiert man sich an den dem von OASIS herausgegebenen Sicherheitsmaßnahmen lässt sich die Datenübertragung sicher gestalten, Wrapper-Angriffe sind jedoch eine nicht zu vernachlässigende Bedrohung. Werden alle bekannten Sicherheitsrisiken richtig eingeschätzt

[8] XML Security Gateways sind hard- oder softwarebasierte Lösungen für unternehmensweiten Schutz vor schädlichem oder unerwünschtem Code in XML-codierten Datenströmen, z.B. von IBM (`http://www-03.ibm.com/software/products/de/de/xs40/`) oder Microdasys (`https://www.microdasys.de/flash/xsgdsde.pdf`)

und berücksichtigt ist SAML als recht sicher einzustufen. Dies beweist auch die Verwendung dieses Frameworks in zahlreichen Anwendungen, wie Tabelle C.1 zeigt.

C.2. OpenID

Grundlagen und Definition *OpenID* ist ein dezentrales Authentifizierungssystem das einem Benutzer erlaubt, seine Authentizität bei beliebigen Anbietern (Relying Parties) mittels eines *Identifiers* nachzuweisen. Der SP erhält keinerlei Information über die Credentials des Benutzers. Die Dezentralität macht eine zentrale Authorität (wie das KDC bei Kerberos oder den Identity Server bei SAML), die Service Provider oder OpenID Provider verwaltet, überflüssig. Entwickelt wurde das OpenID zugrundeliegende Protokoll von Brad Fitzpatrick - 2007 wurde die OpenID Foundation gegründet, die die Verwaltung von Urheberrechten und das Marketing betreut. Für Europa übernommt OpenID Europe diese Aufgabe. Im selben Jahr wurde die aktuell gültige Version 2.0 herausgegeben.

OpenID als offener Standard erlaubt es dem Anwender, zwischen unterschiedlichen Anbietern zu wechseln und unterschiedliche Identitäten zu erstellen und zu benutzen.

Architektur und Terminologie Die Grundlage von OpenID ist der Identifier, der in Form einer URL[9] nach dem HTTP oder HTTPS-Protokoll vorliegt und im Großen und Ganzen der folgenden Struktur entspricht:

http://Stefanie-Langer.myOpenId.com - alternativ auch
http://OpenIdProvider.com/benutzername

Der erste Teil „Stefanie-Langer“ ist ein frei gewählter Benutzername, der der Realität entsprechen kann, aber nicht muss. Hier ist die Eingabe einer beliebigen, einmaligen Zahlen- und Buchstabenkombination möglich. Ein Punkt trennt den Benutzernamen vom Namen des Anbieters, der danach folgt.

Ebenfalls möglich ist die Angabe des Identifier in *XRI* (engl. Abkürzung für Extensible Ressource Identifier), einem Schema zur Darstellung abstrakter Identifikatoren, das vom OASIS XRI Technical Committee entwickelt wurde, siehe Tabelle C.2.

Authentifizierungsablauf nach [Ope13] Nach [Ope13], [Rus10] und [Sys13] besteht die Architektur von OpenID aus drei Komponenten:

- dem Benutzer (an einem beliebigen Client) als reale Person,

[9] auch: URI für Uniform Resource Identifier

GCS Zeichen	Authorität des Identifiers	Beispiel
=	Einzelperson	`xri://=john.smith` `xri://=(mailto:abc@yahoo.com)`
@	Organisation	`xri://@joes.grill`
+	generische Wörterbuchkonzepte oder Tags	`xri://+tel`
$	spezifizierte Identifier	`xri://\protect\T1\textdollarv` (version)
!	persistente Identifier	`xri://!!1002`

Tabelle C.2.: XRI Global context Symbols (GCS) und Anwendungsbeispiele nach `http://www.oasis-open.org/committees/xri/faq.php`

- dem Service Provider, der eine authentifizierungspflichtige Ressource zur Verfügung stellt (z.B. ein soziales Netzwerk oder ein Bloganbieter),
- dem OpenID-Provider (OP). Der OpenID-Provider benötigt lediglich eine einmalige Registrierung, bei der beliebig viele Daten zusätzlich zum obligatorischen Benutzernamen und Passwort erfasst werden können.

Anhand der für diesen Zweck eigens bei myOpenID.com erstellten OpenID http://Stefanie-Langer.myOpenId.com wurde der in [Ope13] beschriebene Authentifikationsverlauf nachvollzogen und dokumentiert (vgl. Abbildung C.3). Die Anmeldung erfolgte beispielhaft auf den Portalen http://wiki.creativecommons.org/ und http://www.golem.de, Webseiten die die OpenID-Technologie unterstützen (siehe auch Tabelle C.3, bekannte OpenID-Anbieter und verwendende Webseiten).

Während des Besuchs einer Webseite, also der Relying Party (RP), steht dem Benutzer die Möglichkeit der Registrierung zur Verfügung, um spezielle privilegierte Dienste (z.B. die Schreibberechtigung in einem Forum) in Anspruch zu nehmen. Bei der Registrierung der oben genannten Webseiten bietet sich neben der klassischen Registrierung auch die Möglichkeit, sich mittels der bereits vorhandenen OpenID zu authentifizieren. Hierfür wählt der Benutzer die Registrierungsfunktion aus.

Die Authentifikation via OpenID gliedert sich nun in drei Phasen: der Initiierung und Feststellung (engl. *discovery*), der Assoziation und der Authentifizierung.

In der **Initiierung und Feststellung** wird je nach Webseite, die Authentifizierung mittels mehrerer OpenID-Anbieter angeboten. Der Benutzer wählt seinen OpenID Provider (OP) aus und gibt seinen Identifier (z.B. http://Stefanie-Langer.myOpenId.com) an und bestätigt den

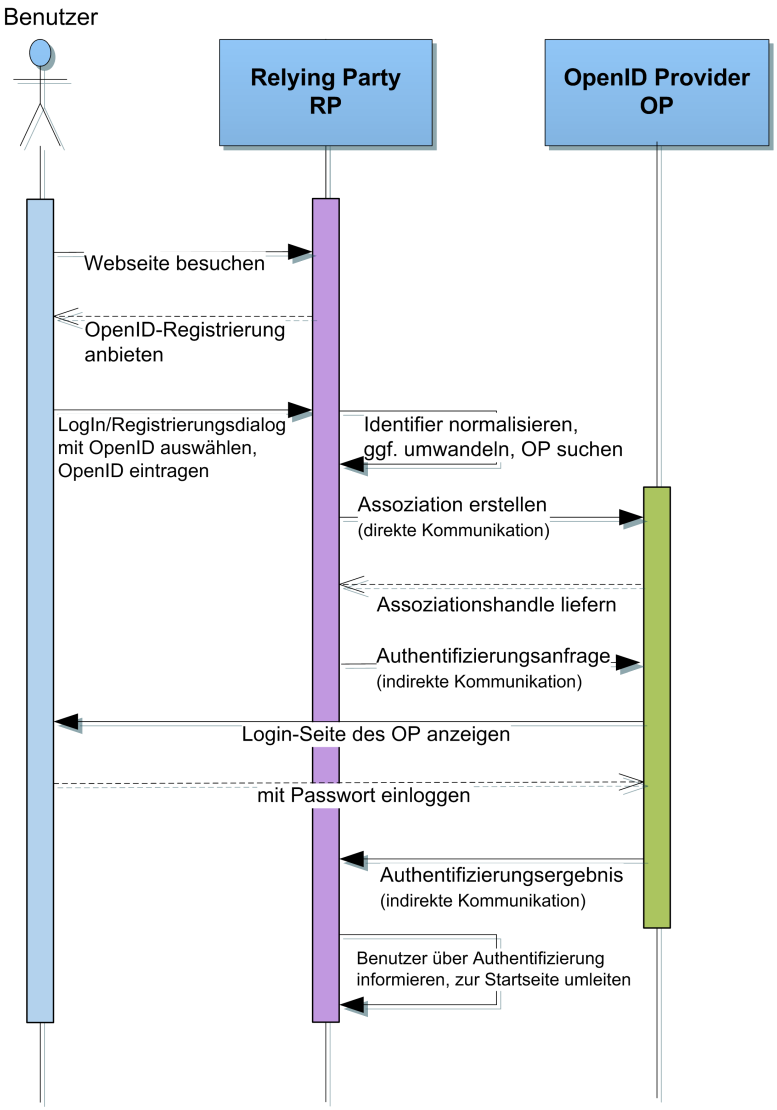

Abbildung C.3.: OpenID Authentifizierungsablauf nach [Rus10] und [Ope13]

Eintrag, z.B. mittels Button „weiter“. Die RP, also die besuchte Webseite normalisiert nun die Eingabe indem sie den Benutzernamen und den OP hieraus extrahiert.

In der **Assoziation** wird per direkter Kommunikation eine *Association Session Request* (ASR) an den OP (hier: myOpenId.com) versendet[10]. Eine Association Session Request enthält vier Parameter:

- openid.ns: enthält den Wert „http://specs.openid.net/auth/2.0“ und zeichnet die Request als gültig aus. Außerdem wird die aktuelle Version des OpenID-Standards übermittelt, um evtl. Kompatibilitätsprobleme zu vermeiden.
- openid.mode: gibt die Art der Mitteilung an, „associate“ für eine Association Session Request
- openid.assoc_type: gibt die Art der Verschlüsselung an, entweder HMAC-SHA1 oder HMAC-SHA256
- openid.session_type: Der Session Typ kann entweder unverschlüsselt oder per Diffie-Hellman-Algorithmus verschlüsselt (DH-SHA1, DH-SHA256) sein.

Durch die ASR wird ein *Shared Secret* zwischen RP und OP in Form eines HMAC-Schlüssels erstellt[11]. Wird in der ASR ein unverschlüsselter Session Type gewählt muss die Nachricht auf Transportebene verschlüsselt werden. Beide Kommunikationspartner können das Shared Secret unter Zuhilfenahme des im Session Type genannten Algorithmus berechnen.

In der **Authentifizierungsphase** wird die *Authentication Request* (AR) von der RP per indirekter Kommunikation, also über den Benutzer versendet[12]. Diese enthält die Parameter:

- openid.ns: enthält den Wert „http://specs.openid.net/auth/2.0“
- openid.mode: enthält den Wert „checkid_immediate“ oder „checkid_setup“
- openid.claimed_id: enthält den Identifier
- openid.identity: enthält den lokalen OP-Identifier, z.B. „myOpenId.com“
- openid.assoc_handle: enthält den Handle, also das Shared Secret das während der Assoziation zwischen RP und OP ausgehandelt wurde.

[10] Direkte Kommunikation bezeichnet nach [Ope13] eine Kontaktaufnahme zwischen RP und OP, durch die RP initiert. Die Kommunikation erfolgt mittels HTTP unter Verwendung von Web-Formularen und haben in der Regel die Form openid.<VARIABLE> = '<VALUE>'.

[11] HMAC-Schlüssel sind MAC-Schlüssel, die unter Verwendung kryptographischer Hashfunktionen erstellt wurden. Siehe auch `http://www.ietf.org/rfc/rfc2104.txt` HMAC: Keyed-Hashing for Message Authentication

[12] indirekte Kommunikation verwendet laut [Ope13] HTTP Redirects (Weiterleitung auf eine andere URL) oder HTML Form Submission.

- openid.return_to: gibt die Rücksprungadresse in Form einer URL an, zu der der Benutzer nach der Authentifizierung weitergeleitet werden soll.
- openid.realm: gibt einen URL-Raum an, in dem der Benutzer sich nach der Authentifizierung ohne neue Authentifikation bewegen kann - Wildcards sind erlaubt

Nach der OP-spezifischen Prüfung der Authentifizierung erhält die RP eine Assertion, die entweder positiv oder negativ ist. Um eine positive Assertion zu verifizieren wird die vorherige Assoziation benötigt, die von der RP auf folgende Kriterien überprüft wird:

1. Die openid.return_to Adresse muss identisch mit der eigenen URL sein
2. Die Informationen aus der discovery (Feststellungsphase) müssen mit den Daten der Assertion identisch sein
3. Die Assertion wurde von der RP vorher noch nie geprüft (die Sicherstellung erfolgt durch eine Nonce)
4. Die Signatur ist gültig und alle zu signierenden Felder wurden signiert

Optional kann eine Authentifizierung auch ohne Assoziation erfolgen, z.B. wenn das Shared Secret ungültig ist oder die Assoziationsphase ausgelassen wurde - dies stellt eher eine Ausnahme dar (und wird daher in Abbildung C.3 nicht berücksichtigt). In diesem Fall muss die RP die Assertion des OP trotzdem verifizieren. Dies geschieht, in dem die dem Nutzer zugesandte Assertion erneut zur RP, und von dieser (verschlüsselt mit einem in der Assertion enthaltenen Handle) an den OP versandt wird. Der OP prüft somit die von ihm versandte Assertion noch einmal gegen und versendet die Antwort an die RP.

Portabilität und Integration OpenID bietet auf seiner Webseite Plugins und Module für viele gängige Frameworks (z.B. Drupal, Wordpress) und Programmiersprachen (PHP, Ruby, Java, C++) an. Außerdem arbeitet OpenID mit dem Identitätsmanagement-Anbieter Janrain[13]zusammen, der Komplettlösungen für Social Media Logins anbietet.

Einige Relying Parties bieten eine nachträgliche Integration einer neuen OpenID an. Eine oder mehrere OpenIDs lassen sich in den Kontoeinstellungen hinzufügen, um zusätzlich zur bestehenden Benutzername/Passwort-Lösung auch den Zugang per OpenID zu ermöglichen.

bekannte OpenID-Anbieter und verwendende Webseiten Obwohl OpenID bereits seit 2007 in der aktuellen Version angeboten wird sind die Anbieter und Unterstützer noch eher spärlich gesäht. Zwar verwenden auch Branchenriesen wie Yahoo, Google, IBM und Microsoft

[13] `http://www.janrain.com`

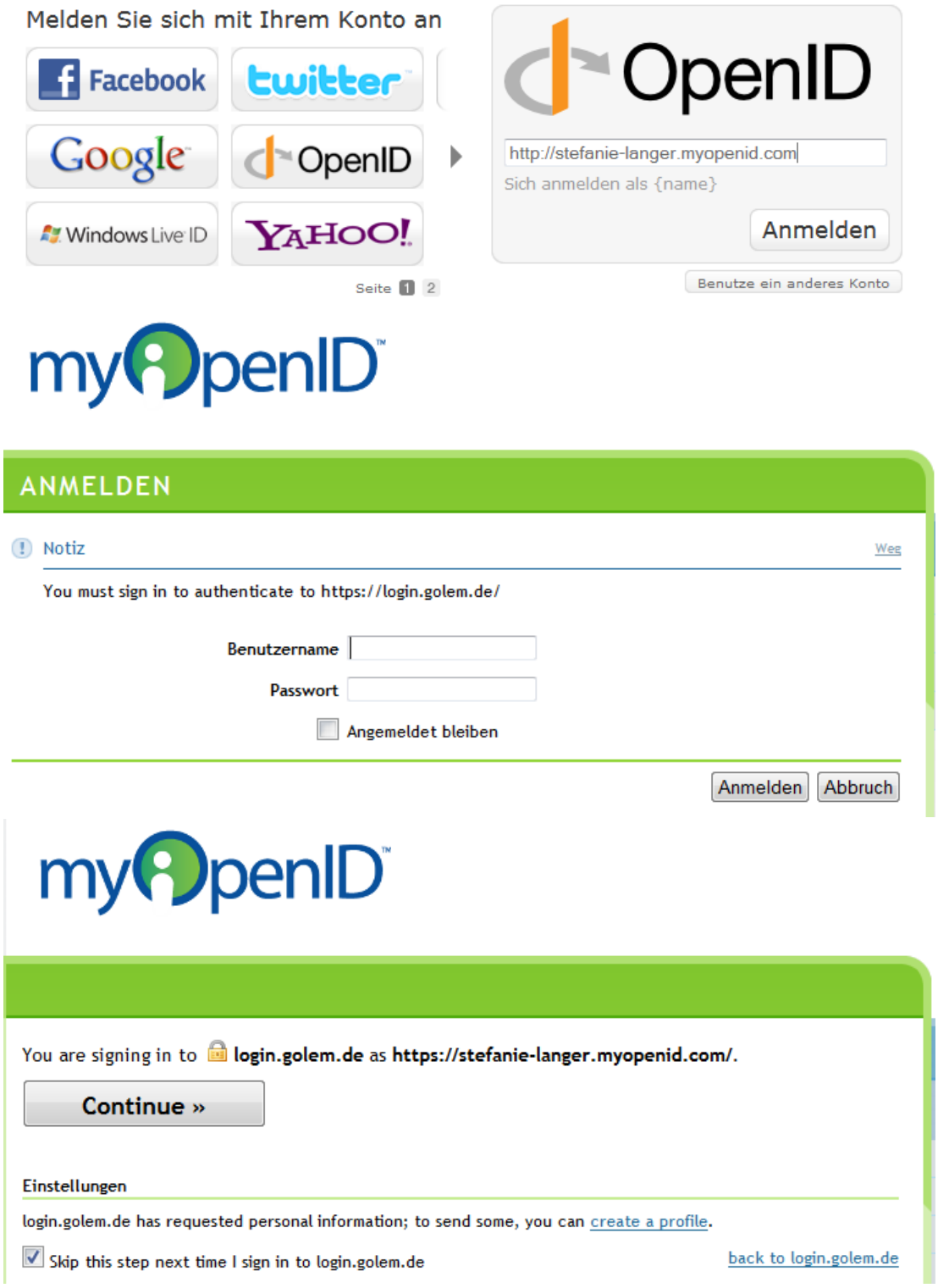

Abbildung C.4.: Ablauf der Authentifizierung bei `http://www.golem.de`

OpenID, doch geschieht dies implizit - der Benutzer weiss ohne explizite Recherche nichts von der Technologie. Stattdessen wird der Eindruck von schlichtem, passwortbasiertem Single Sign-On vermittelt, da der Benutzer nicht die OpenID, sondern z.B. seine Google Credentials verwendet.

Art	Name	URL
Provider	ClaimID	http://www.claimid.com
Provider	MyOpenID	http://www.myopenid.com
Provider	Symantec Personal Identity Portal	http://pip.verisignlabs.com
Provider	Xlogon	http://www.my.xlogon.net
Provider	MeinGuterName	http://www.meinguter.name
Provider	MyID (kostenpflichtig)	http://www.myid.com
Webseite	Slashdot (Internet-Informationsdienst)	http://www.slashdot.org
Webseite	SourceForge (Open Source Software Verzeichnis)	http://www.sourceforge.net
Webseite	Stack Overflow (Forum für Entwickler)	http://www.stackoverflow.com
Webseite	Books I am reading (Statistiken über gelesene Bücher)	http://www.booksiamreading.com
Webseite	Creative Commons Wiki (Wiki für Creative Commons Tools)	http://wiki.creativecommons.org
Webseite	Golem (News-Webseite zu Informatikthemen)	http://www.golem.de
Webseite	Bitbucket (Repository Dienst)	http://www.bitbucket.org
Webseite	Hampr (Bookmark Manager)	http://www.hampr.com

Tabelle C.3.: OpenID-Anbieter und unterstützende Webseiten nach `http://www.openId.com`

OpenID und OAuth Da es sich bei OpenID lediglich um ein Authentifizierungssystem handelt (im Vergleich zu beispielsweise SAML, das zum Austausch von Authentifizierungs- als auch Autorisierungsinformationen verwendet wird) wird es oft in Verbindung mit OAuth verwendet. OAuth ist ein dezentrales Autorisierungssystem und wurde 2007 erstmal spezifiziert[14]. Als Autorisierungssystem soll es dem Nutzer transparent erlauben den Zugriff auf seine Daten selbst zu steuern, indem er Relying Parties z.B. Zugriff auf eine andere Relying Party gibt - die Angabe der Credentials wird jedoch nicht benötigt.

Obwohl OpenID und OAuth oft miteinander verwendet werden handelt es sich bei OAuth nicht um eine OpenID-Extension, da sich die Entwickler so einen größeren Anwendungsbereich

[14]http://tools.ietf.org/html/rfc6749, The OAuth 2.0 Authorization Framework

Abbildung C.5.: Websucheninteresse für den Begriff OpenID (2004-dato) nach `http://www.google.com/trends/explore`

erhoffen. Durch die getrennten, sich aber ergänzenden Anwendungsbereiche werden diese beiden offenen Standards oft gemeinsam verwendet, z.B. bei Google[15].

aktuelle Entwicklung und Verwendung Durch die Ermittlung von OpenID-Provider fällt auf, dass einige Provider bereits nicht mehr existieren und viele Webseiten, die mit OpenID-Funktionalität gelistet sind[16] diese inzwischen nicht mehr anbieten. Trotz des großen Hypes Ende der 2000er Jahre hat sich OpenID mittels Benutzung eines Identifiers nicht durchgesetzt. Stattdessen werden aber Dienste, die implizit OpenID verwenden (wie Yahoo, AOL, Google) zusammen mit Facebook und Twitter (als sogenannte Gruppe der Social Sign-Ins) favorisiert, siehe auch Abbildung C.5 und C.6.

C.2.1. Sicherheit von OpenID

bekannte Schwächen Die OpenID-Spezifikation (vgl. [Ope13]) weist bereits auf einige Systemschwächen hin. *Eavesdropping* (engl. für Lauschen, Abhören) ist möglich, sofern verwendete Nonces nicht überprüft werden - auf diese Weise kann eine erfolgreiche Authentication Request abgehört und wiederverwendet werden. Maßnahmen hiergegen sind neben der Überprüfung von Nonces auch die Verschlüsselung mit TLS auf dem Übermittlungsweg.

Weiterhin sind Man-in-the-Middle-Attacken (MITM) möglich, sobald z.B. der MAC-Key kompromittiert würde, was einen Zugriff auf signierte Felder in der Association Session Request oder der Authentication Request ermöglicht. Wenn die DNS-Resolution oder die Transportschicht kompromittiert wird schützen Signaturen nicht, da der Angreifer sich als OP ausgeben und somit eigene Association Session Requests erstellen kann. Bei einer Manipulation

[15] `https://sites.google.com/site/oauthgoog/`
[16] z.B. auf`http://www.openidDirectory.com` oder `https://www.myopenid.com/directory`

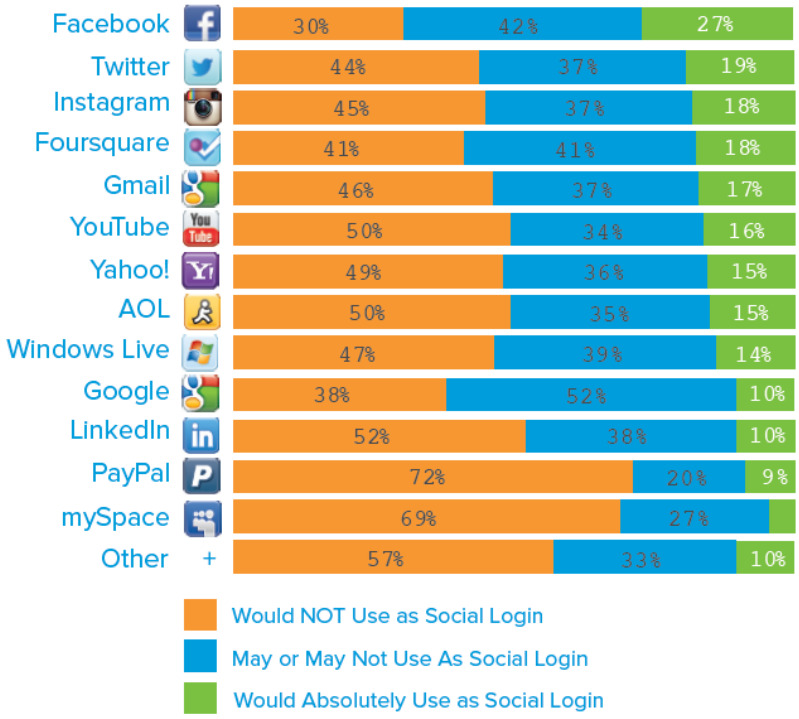

Abbildung C.6.: Studie des Identitätsmanagement-Tool Anbieters Jrain zum Thema Social Login, Fragestellung: Welchen Account würden Sie für [einen] Social Login nutzen? [Jan13]

während der Discovery-Phase kann der Angreifer einen beliebigen (falschen) OP angeben und muss das Original auf diese Weise nicht imitieren. Wenn der OP auch XRI unterstützt ist das XRDS Dokument, das Dokument dass der OP hält um entsprechende eingehende XRI-Informationen zu verwalten, ebenfalls ein Angriffsziel. Durch Verschlüsselung des Dokumentes lässt sich dies jedoch umgehen. Um MITM-Attacken grundsätzlich zu verhindern empfiehlt [Ope13] für OpenID-Provider ausdrücklich die Verwendung von TLS in Kombination mit Zertifikaten, die von einer vertrauenswürdigen Stelle ausgestellt wurden. Außerdem sollten Relying Parties nur Verbindungen zu OpenID-Providern eingehen, wenn die Verbindung mit TLS und Zertifikaten abgesichert ist.

Eine weitere Angriffsmöglichkeit sind wie bei allen anderen Technologien auch mit Spy- oder Malware infizierte Client-Rechner bzw. die darauf verwendeten Browser. Hier ist jedoch erneut der Benutzer für seine eigene Sicherheit zuständig. Um die Transparenz für den Nutzer zu erhöhen empfiehlt [Ope13] jedoch, Weiterleitungen und Eingabeaufforderungen deutlich sichtbar zu machen. Nur so kann der Benutzer leichter eventuelles Phishing bemerken, was

nach [Rus10] eines der größten Sicherheitsmankos von OpenID ist. Eine kompromittierte Relying Party, oder eine Relying Party die der Benutzer subjektiv für vertrauenswürdig hält kann den Benutzer zu jeder beliebigen Webseite weiterleiten, die visuell den Eindruck vermittelt der tatsächliche OP zu sein. Gibt der Benutzer dort seine Credentials ein sind sämtliche mit dieser OpenID verknüpften Dienste kompromittiert.

Maßnahmen der OpenID-Provider Um gegen Phishing, Trojaner oder Keylogger vorzugehen bieten einige OpenID-Anbieter zusätzliche Services an. MyOpenID bietet die Integration eines SSL-Zertifikates an, um die Passworteingabe komplett zu ersetzen - nur wenn sich ein entsprechendes Zertifikat auf dem Client befindet ist der Login möglich. Ein weiterer Service ist CallverifID (powered by Phonefactor) - hier wird der Benutzer bei einem Authentifizierungsversuch auf seinem vorher spezifizierten Telefon angerufen, um die Authentifizierung zu bestätigen. In Deutschland wird dieser Service nur für Festnetzanschlüsse angeboten.

Auch von Verisign werden SSL-Zertifikate angeboten - zusätzlich gibt es die Bereitstellung von sogenannten Security Tokens (entspricht einer Eigenentwicklung der RSA-Tokens, siehe Abbildung A.2).

XLogon rühmt sich mit seinem Phishingschutz, der allerdings zunächst manuell aktiviert werden muss. Zwei Methoden stehen zur Auswahl: ein „Schutz-Bookmark“, das in die Toolbar des Browsers eingefügt wird, prüft eingebettet Open-ID-Formulare mittels eines Klicks per JavaScript. Handelt es sich um ein Original-XLogon-Formular werden dessen Eingabefelder erst nach erfolgreicher Überprüfung freigegeben. Die andere Variante ist, dass eingebettete Logins komplett deaktiviert werden, sodass eingebettete Logins sofort als Täuschung erkannt werden können.

Fazit Zusammenfassend lässt sich sagen, dass OpenID ein Authentifizierungssystem ist, deren größte Schwäche das Phishing ist. Wie am Beispiel des XLogon zu sehen ist es durchaus möglich, dem entgegenzuwirken. Beim Test diverser OpenID Provider und Relying Parties fällt zudem mangelnde Benutzerfreundlichkeit ins Auge.

Eine weitere große Schwierigkeit bei der Verwendung von OpenID ist die Erinnerbarkeit durch den Nutzer. Die Identifier können beliebig ausgestaltet sein, wodurch Eingabefehler entstehen können. Durch die mögliche Vielfalt von Identifiern, die sich durch die freie Wahl von OpenID Providern ergibt wird das „Ein-Passwort-für-alle-Dienste“-Motto ad absurdum geführt.

Genau wie SAML ist OpenID durch die zusätzliche Eingabe von Passworten von der Sicherheit des Browsers, des Clients und der Passwortwahl abhängig. Beim Durchschnittsnutzer ist

nicht davon auszugehen, dass zusätzliche freiwillige Optionen wie die Verwendung von Zertifikaten verwendet werden. Zusätzlich bietet OpenID als reines Authentifizierungssystem (ohne OAuth) keinen Schutz vor mißbräuchlicher Datenverwendung durch den OpenID Provider. Daher ist OpenID als wenig sicher einzustufen und von der Verwendung abzuraten.

C.3. Single Sign-On an der HAW

An der Hochschule für Angewandte Wissenschaften (HAW), Department Technik und Informatik, wird ein hochschulinternes Client-Server-System betrieben. Beim Verzeichnisdienst handelt es sich um das eDirectory der Firma Novell, dass mit einem LDAP Server verbunden ist. Hier handelt es sich jedoch nicht um ein Single Sign-On-System im eigentlichen Sinne - der einmaligen Eingabe von Credentials zum Zugang zu allen Services - sondern um eine Single Sign-On Lösung, die mit mehreren Zugangsdatensätzen arbeitet, die jedoch miteinander synchronisiert werden. Dies erfolgt über den Dienst „HAW-Mailer“, dem hochschuleigenen Exchangeserver.

Die HAW nutzt eDirectory als Datenbank und Authentifizierungslösung. Die Autorisierung erfolgt extern und rollenbasiert mittels spezieller Benutzerverwaltungen, separat für Angestellte der Hochschule und Studierende. Durch XML-basierte, Anwendungsfall-basierte Konnektoren erfolgt der Datenaustausch zwischen dem eDirectory und anderen Anwendungen wie z.B. einem ActiveDirectory[17], das für die Verwendung des hochschuleigenen Exchangeservers notwendig ist. Zusätzlich zum fakultätsinternen eDirectory gibt es ein weiteres, zentrales eDirectory, dass zusätzliche Daten bereit hält. Sämtliche Daten werden zu Sicherheitszwecken zweifach repliziert.

Der Datenaustausch erfolgt mittels des LDAP-Protokolls, das nachfolgend kurz skizziert wird.

C.3.1. Lightweight Directory Access Protocol (LDAP)

Grundlagen und Definition LDAP (engl. für „leichtes Verzeichnis-Zugriffs-Protokoll“) ist ein Anwendungsprotokoll aus der Netzwerktechnik, dient der Authentifizierung und Autorisierung von Benutzern und findet bei Client-Server-Modellen Anwendung. Nach der Entwicklung an der Universität von Michigan erfolgte die erste Erwähnung im Rahmen des RFC1487[18];

[17] ActiveDirectory ist eine Marke von Microsoft.
[18] `http://tools.ietf.org/html/rfc1487`, X.500 Lightweight Directory Access Protocol

inzwischen ist LDAP ins seiner aktuellen Version LDAPv3 als Standard in den RFCs 4510, 4511 und 4513 spezifiziert worden[19].

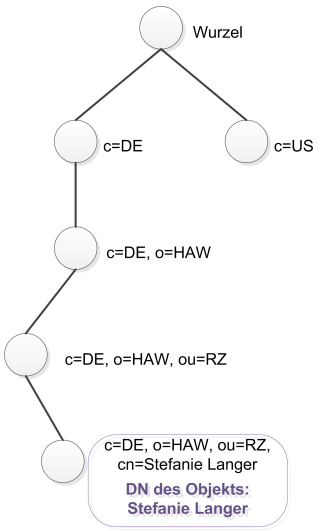

Abbildung C.7.: Baumstruktur eines Distinguished Name nach [Sch99]

Nach [Sch99] baut LDP im Vergleich zum Vorgänger DAP (engl. Directory Access Protocol) nicht mehr auf dem siebenschichtiges ISO/OSI-Referenzmodell, sondern auf dem TCP/IP-Referenzmodell auf. Der Unterschied liegt darin, dass im letzteren die Schichten eins und zwei (Bitübertragungs- und Sicherungsschicht) zu einer Netzzugangsschicht, sowie die Schichten fünf bis sieben (Sitzungsschicht, Darstellungsschicht, Anwendungsschicht) zu einer Anwendungsschicht zusammengefasst sind. Der Vorteil liegt hier darin, dass LDAP nicht mehr auf im Stack darunterliegende Schichten angewiesen ist, die eventuell im Netzwerk gar nicht derartig vorhanden sind. Weiterhin werden nicht alle der DAP-Funktionen benötigt und verwendet.

LDAP war zunächst ausschließlich als Zugriffsprotokoll für X.500-Server gedacht. Die Speicherung der Daten erfolgt in Objekten, die sowohl reale Personen oder Geräte (z.B. Drucker), als auch logische Objekte wie Gruppen seien können. Vorgegebene Verzeichnisschemata definieren *Objektklassen*, die wiederum standardisierte, vorgeschriebene oder optionale *Attribute* als Key-Value Paare zu jedem Objekt vorgeben. Jeder Wert eines Attributs hat einen *Relative Distinguished Name* (Abkürzung: RDN, engl. für: relativer bedeutender Name) - da die Anordnung in einer hierarchischen Baumstruktur (*Directory Information Tree*, DIT) erfolgt, ergibt der Pfad von der Wurzel bis zum Objekt den Distinguished Name (DN) des Objekts, der baumweit eindeutig ist und den Schlüssel zum Objekt bildet (siehe auch Abbildung C.7). Beschrieben wird er als String aus konkatenierten Attributname-Wert-Paaren.

Anstelle von einer Datenabfrage und Übermittlung per DAP entwickelte sich Anfang der 1990er Jahre ein Trend zur Übermittlung von Daten über LDAP zu einem LDAP Gateway (Server), der wiederum die erhaltenen Daten über DAP an einen X.500 Server leitete. Ab Mitte der

[19] `http://tools.ietf.org/html/rfc4510` Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map;
`http://tools.ietf.org/html/rfc4511`, Lightweight Directory Access Protocol (LDAP): The Protocol; RFC4513, `http://tools.ietf.org/html/rfc4513`, LDAP Authentication Methods; zusätzlich noch Schnittstellen zu anderen RFCs.

Attribut, Alias	Beschreibung	Beispiel
commonName, cn	Name eines Eintrags	Stefanie Langer
surName, sn	Nachname einer Person	Langer
organizationName, o	Name einer Organisation	HAW
organizationalUnitName, ou	Name einer Organisationseinheit	RZ (Rechenzentrum)
countryName, c	Abkürzung des Ländernames	de, us
telephoneNumber	Telefonnummer	04161 6520729
description	Beschreibung	Hochschule

Tabelle C.4.: LDAP-Attribute einer Objektklasse nach [Geb02] als Ergänzung zu Abbildung C.9

1990er Jahre wurde der Umweg über einen LDAP Gateway komplett ersetzt, indem sowohl der Client als auch der Server mit LDAP-Schnittstellen ausgerüstet wurden. LDAP-unterstützende Verzeichnisdienste (engl. *directory service*) haben durch die schnelle Durchsuchbarkeit des Verzeichnisbaums eine hohe Performance bei Lesezugriffen, jedoch eine schlechte bei Schreib- oder Änderzugriffen. [Apa13] empfiehlt daher, bei häufig zu ändernden Datenbeständen eher auf eine LDAP-Anbindung an ein relationales Datenbanksystem zurückzugreifen.

Architektur und Terminologie Das eDirectory von Novell ist ein proprietärer Verzeichnisdienst, der mittels LDAP-Schnittstelle kommuniziert und Anmelde- und Berechtigungsinformationen in Form von Benutzerkennungen passwortgeschützt speichert. Objekte, die Netzwerkressourcen, Benutzer, Anwendungen und Daten abbilden können in großer Menge gespeichert und verwaltet werden (vgl. [Doc13]). Novell bezeichnet seine plattformunabhängige Software als skalierbare, hochperformante und sichere Identitätsmanagement-Lösung.

Verzeichniszugriffe mittels LDAP lassen sich in drei Gruppen kategorisieren: lesen, schreiben und verbinden. Das Verbinden per Bind-Befehl entspricht der Authentifizierung am Server, der DN eines Objektes als (eindeutige) Benutzerkennung, unter Berücksichtigung einer zwingend notwendigen Passworteingabe.

Zusätzlich zum Lese- und Schreibzugriff werden folgende Operationen angeboten:

- Search: ermöglicht die Suche nach Objekten anhand derer Attributwerte (phonetisch oder per Wildcard)
- Compare: ermöglicht den booleschen Vergleich eines Wertes mit dem Referenzwert eines Attributes, z.B. für die Überprüfung von Passwörtern
- Add: fügt neue Einträge unter Berücksichtigung der Position ins Verzeichnis ein
- Delete: löscht einen Verzeichniseintrag

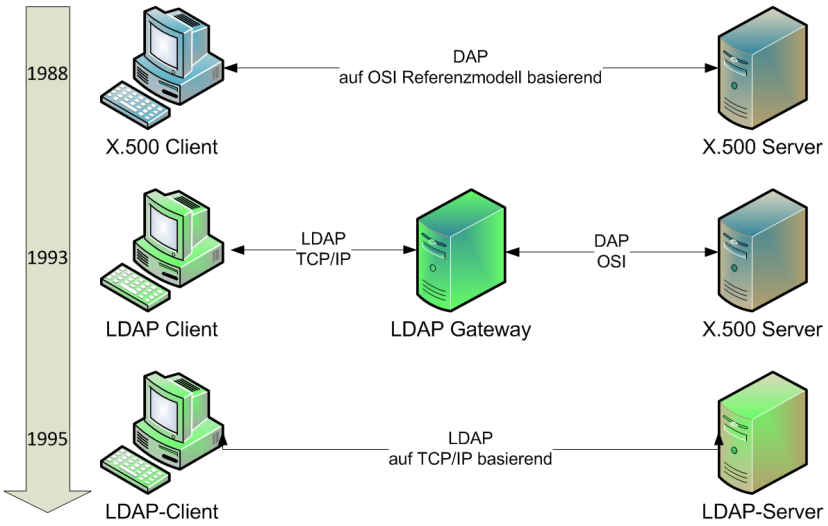

Abbildung C.8.: Entwicklungsprozess von DAP zu LDAP nach [Apa13]

- Modify: ermöglicht das Verändern, Hinzufügen oder Löschen von Attributwerten/Attributen
- ModifyRDN: ändert den RDN eines Objekts (wodurch sich die Position des darunterliegenden Teilbaums im Verzeichnis ändert)
- Abandon: bricht eine laufende Suchabfrage ab

LDAP Nachrichten, die mittels ASN.1 beschrieben werden, sind in einem sogenannten Envelope (engl. für Umschlag) namens LDAPMessage gekapselt, die folgenden Aufbau haben:

```
LDAPMessage ::= SEQUENCE {
   messageID       MessageID,
   protocolOp      CHOICE {

 bindRequest          BindRequest,
 bindResponse         BindResponse,
 unbindRequest        UnbindRequest
 searchRequest        SearchRequest,
 searchResponse       SearchResponse,
 modifyRequest        ModifyRequest,
 modifyResponse       ModifyResponse,
 addRequest           AddRequest,
```

```
addResponse          AddResponse,
delRequest           DelRequest,
delResponse          DelResponse,
modifyRDNRequest     ModifyRDNRequest,
modifyRDNResponse    ModifyRDNResponse,
compareDNRequest     CompareRequest,
compareDNResponse    CompareResponse,
abandonRequest       AbandonRequest

intermediateResponse  IntermediateResponse },
controls       [0] Controls OPTIONAL }

MessageID ::= INTEGER (0 ..  maxInt)
maxInt INTEGER ::= 2147483647 -- (2^^31 - 1) --
```

Listing C.2: Aufbau einer LDAPMessage nach RFC4511

Die MessageID, die nicht 0 sein darf, wird hierbei für die Dauer der Kommunikation konstant gehalten. Bei einem neuen Verbindungsaufbau wird diese durch den Client inkrementiert.

Authentifikationsablauf Die Authentifikation erfolgt durch die BindRequest des LDAP-Clients an den LDAP-Server oder die LDAP-Schnittstelle eines proprietären Verzeichnisdienstes (siehe auch Abbildung C.9). Da es sich um eine TCP-Verbindung handelt werden zunächst die einleitenden SYN- und ACK-Pakete im Rahmen des Three-Way-Handshake übermittelt. LDAP-spezifisch ist hierbei, dass neben dem ACK-Flag auch das PSH-(Push-)Flag gesetzt ist, wodurch keine Pufferung von Datenpaketen stattfindet, sondern jedes Paket sofort an den TCP-Port übermittelt wird.

Wurde die Verbindung erfolgreich aufgebaut versendet der Client ein *Bind Request* innerhalb einer LDAP-Message, die neben der Version des LDAP-Protokolls den Namen des angeforderten Objekts und die gewünschte Authentifikationsmethode enthält. RFC4513 unterscheidet zwischen zwei Arten von Bind Requests, der *Simple Bind Request* und der *SASL Bind Request*. Bei der **Simple Bind Request** bestehen drei Möglichkeiten der Authentifizierung:

1. anonyme Authentifizierung: sofern der Server anonyme Authentifizierung unterstützt erfolgt diese ohne Angabe von Benutzername oder Passwort (beides hat die Länge 0).
2. Unauthentifizierte Authentifizierung: hier wird zwar ein Benutzername, jedoch kein Passwort (Länge=0) übermittelt. Es findet keine Verifizierung des DN statt.

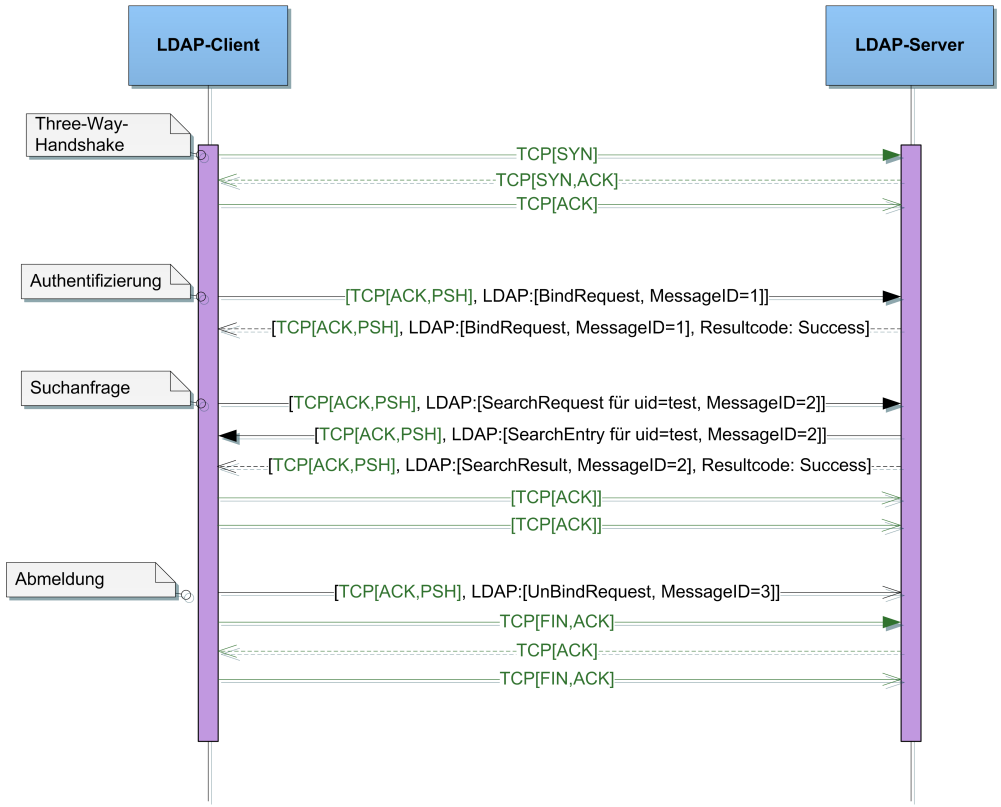

Abbildung C.9.: Authentifikationsablauf von LDAP nach [Geb02]

3. Name/Passwort Authentifizierung: Passwort und Benutzername werden übermittelt und mit dem DN und dem Passwortattribut abgeglichen.

Obwohl Typ 1 und Typ 2 des Simple Bind Requests möglich sind, rät der RFC4513 explizit von deren Verwendung ab und empfiehlt, Clientseitige leere Angaben von Benutzername und/oder Passwort zu unterbinden, sowie solche Requests auf Serverseite zu blockieren.

Alternativ zum Simple Bind Request unterstützt LDAP die Authentifikation via *SASL* (**SASL Bind Request**). SASL (engl. Abkürzung für: Simple Authentication and Security Layer) wird im RFC4422[20] spezifiziert und bezeichnet ein Framework, dass zur Authentifizierung in offenen oder geschlossenen Netzwerken verwendet werden kann und zwischen der TLS-Schicht (sofern vorhanden) und der LDAP-Schicht liegt. Ziel der Anwendung ist das Aushandeln von Kommunikationsparametern[21], die von der IANA (engl. Abkürzung für Internet Assigned Numbers Authority) vorgegeben und verwaltet und z.B. auch von SMTP, IMAP oder POP3

[20] `http://tools.ietf.org/html/rfc4422`, Simple Authentication and Security Layer (SASL)
[21] im Rahmen eines Challenge-Response-Verfahrens

verwendet wird. Auf diese Weise muss kein vollständiges Authentifizierungs- und Datenverschlüsselungsverfahren implementiert werden.

Bei der Übermittlung eines SASL Bind Request müssen folgende Parameter zwingend angegeben werden:

- Version („3“)
- AuthenticationChoice („sasl“)
- gewünschter SASL-Mechanismus

SASL kann auf Wunsch des Nutzers eine niedrigere Sicherheitsschicht, wie z.B. TCP verwenden. Auf die näheren Details des SASL-Protokolls wird diese Arbeit jedoch nicht weiter eingehen.

Auf ein Bind Request antwortet der Server nach erfolgreichem Datenabgleich mit einer Bind Response („Result Code: success“). Im Anschluss kann dann eine Datenabfrage, Veränderung oder Löschung von Objekten oder Attributen stattfinden.

populäre LDAP-Server Implementierungen Neben dem bereits erläuterten eDirectory von Novell gibt es noch andere Softwarelösungen für Verzeichnisdienste unter Verwendung von LDAP, sowohl proprietär als auch Open Source, siehe Tabelle C.5.

Art	Name	Hersteller	URL
proprietär	Apache Directory	Apache	www.directory.apache.org
proprietär	Oracle Directory Server Enterprise Edition	Oracle	http://www.oracle.com/technetwork/middleware/id-mgmt/overview/index-085178.html
proprietär	Red Hat Directory Server	Red Hat	http://www.redhat.com/products/identity-management/directoryserver/
proprietär	Active Directory (Teil von Windows Server 2012)	Microsoft	http://technet.microsoft.com/de-de/windowsserver/hh534429.aspx
proprietär	DirX Directory	Siemens	http://www.siemens.de/staedte/gesundheitswesen/identity_solutions/Seiten/home.aspx
Open Source	389 Directory Server	Sourceforge	http://de.sourceforge.net/project/389-directory-server/
Open Source	OpenLDAP	OpenLDAP Project	http://www.openLDAP.org

Tabelle C.5.: populäre Verzeichnisdienstsoftware

Verwendung von LDAP [Geb02] nennt drei besondere Funktionalitäten für LDAP. Zunächst existiert die an der HAW verwendete Variante als Authentifikation für **Single Sign-On** - eine LDAP-Anfrage ist einfach zu realisieren, sodass mit jedem Programm/Gerät nach einem

kurzen Kontakt mit dem Server eine Authentifikation realisiert werden kann. Der Vorteil liegt in der einheitlichen Benutzer/Passwort-Kombination für alle im Verzeichnis gelisteten Services. Zusätzlich können die Benutzerrechte durch Administratoren einfach vergeben werden (z.B. alle Rechte für eine Gruppe von Studenten einer bestimmten Fachrichtung setzen).

Neben der Verwendung für Authentifizierungs- und Autorisierungszwecke im Netzwerk findet LDAP auch noch als **Verzeichnisdienst** für Email-Client-Adressbücher (z.B. beim Mozilla Firefox) oder auch für die Kommunikation mit Web- oder Mailservern (z.B. Apache Tomcat, Apache HTTP Server, Apache James) Anwendung.

Schlussendlich lässt sich ein LDAP-Verzeichnisdienst auch als **Single Point of Administration** bewerten, da sich verschiedene heterogene Netzwerke mit einer gemeinsamen, leicht zu wartenden und Redundanz vermeidenden Benutzerverwaltung verbinden lassen. So kann ein System unabhängig vom Netzwerk verwaltet werden.

Sicherheit

Im Gegensatz zu anderen Verfahren befinden sich auf LDAP Clients keine - vorher zu übertragenden - lokal gespeicherten Dateien („passwd“ und „shadow“), die eine Angriffsfläche für Attacken bieten. Auch wird die komplette Netzwerkkommunikation je nach Systemeinstellung über SASL oder z.B. TLS verschlüsselt - lediglich beim Simple Bind Request - der einfachsten Verbindung, siehe Anhang C.3 - findet eine unverschlüsselte Übertragung - auch des Passwortes - statt.

Der RFC4513[22] geht sehr ausführlich auf mögliche Attacken, wie Man-in-the-Middle, ein - herausgestellt wird die Notwendigkeit von gegenseitiger Verifizierung von Client und Server. Novell als Hersteller des eDirectory stellt ebenfalls einige Methoden heraus, wie z.B. die LDAP Authentifizierung nur über sichere Verbindungen auszuführen und das entsprechende Netzwerk gegen Eavesdropping oder Sniffing zu schützen; außerdem wird empfohlen, den Zugang zum LDAP Server über einen DNS-Namen anstelle von IP-Adressen durchzuführen.

Fazit Äquivalent zur Kerberos-Technologie handelt es sich bei LDAP in Kombination mit Verzeichnisdiensten wie eDirectory um ein als sicher eingeschätztes Protokoll zur Authentifizierung. Durch den langen Anwendungszeitraum sind „Kinderkrankheiten“, mit denen aktuelle Technologien noch kämpfen, größtenteils beseitigt und Sicherheitslücken wurden bereits effektiv geschlossen. Es sind zum Zeitpunkt dieser Arbeit keine Sicherheitsvorfälle im Zusammenhang mit LDAP oder eDirectory bekannt.

[22] http://tools.ietf.org/html/rfc4513, Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms

Die Anwendung von LDAP in Verbindung mit dem eDirectory von Novell ist somit uneingeschränkt empfehlenswert.

Literaturverzeichnis

[AM05] Adloff, Frank ; Mau, Steffen: *Theorie und Gesellschaft.* Bd. 55: *Vom Geben und Nehmen: Zur Soziologie der Reziprozität.* Frankfurt and New York : Campus, 2005. – ISBN 3593377578

[And08] Anderson, Ross: *Security engineering: A guide to building dependable distributed systems.* 2. Auflage. Indianapolis and IN : Wiley Pub., 2008. – ISBN 0470068523

[Apa13] Apache: *Some Background. Directories, directory services and LDAP — Apache Directory.* Version: 2013. http://directory.apache.org/apacheds/basic-ug/1.2-some-background.html, Abruf: 23.05.2013

[AS99] Adams, Anne ; Sasse, Martina A.: Users are not the enemy. In: *Communications of the ACM* 42 (1999), Nr. 12, 40–46. dx.doi.org/10.1145/322796.322806, Abruf: 14.05.2013

[Ase12] Asendorpf, Jens B.: *Persönlichkeitspsychologie: Für Bachelor.* 2. Auflage. Berlin and Heidelberg : Springer-Verlag Berlin Heidelberg, 2012. – ISBN 9783642198830

[ASL97] Adams, Anne ; Sasse, Martina A. ; Lunt, Peter: *Making Passwords Secure and Usable.* Version: 1997. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.25.8977, Abruf: 12.04.2013

[Bal11] Balzert, Helmut: *Lehrbuch der Softwaretechnik: Entwurf, Implementierung, Installation und Betrieb.* 3. Auflage. Heidelberg : Spektrum Akademischer Verlag, 2011 (SpringerLink : Bücher). – ISBN 3827422469

[Ben12] Bender, Stephan: *Die 5 Axiome der Kommunikationstheorie von Paul Watzlawick.* Version: 03.02.2012. http://www.paulwatzlawick.de/axiome.html, Abruf: 21.03.2013

[Bon12] Bonneau, Joseph: *The science of guessing: analyzing an anonymized corpus of 70 million passwords.* Version: 2012. http://ieeexplore.ieee.org/

xpl/articleDetails.jsp?reload=true&arnumber=6234435, Abruf: 21.03.2013

[Bru06] Brunnstein, Jochen: *ITIL-Security-Management realisieren: IT-Service Security-Management nach ITIL - so gehen Sie vor.* 1. Auflage. Wiesbaden : Vieweg, 2006. – ISBN 3834801658

[BS12] Bonneau, Joseph ; Shutova, Ekaterina: *Linguistic properties of multi-word passphrases.* Version: 2012. http://www.cl.cam.ac.uk/~jcb82/doc/BS12-USEC-passphrase_linguistics.pdf, Abruf: 18.04.2013

[BSF07] Baumann, Uwe ; Schimmer, Klaus ; Fendl, Andreas: *Faktor Mensch: Die Kunst des Hackens oder warum Firewalls nichts nutzen.* Version: 05.10.2007. https://www.sicher-im-netz.de/files/images/Fibel_Faktor_Mensch2007.pdf, Abruf: 28.03.2013

[BSGM+11] Bhargav-Spantzel, Abhilasha ; Gross, Thomas ; Mustafić, Tarik ; Messerman, Arik ; Camtepe, Seyit A. ; Schmidt, Aubrey-Derrick ; Albayrak, Sahin: Behavioral biometrics for persistent single sign-on. In: ACM (Hrsg.): *DIM '11 Proceedings of the 7th ACM workshop on Digital identity management*, 2011, 73–82

[BSHL12] Badke-Schaub, Petra ; Hofinger, Gesine ; Lauche, Kristina: *Human Factors: Psychologie sicheren Handelns in Risikobranchen.* 2. Auflage. Berlin and Heidelberg : Springer-Verlag Berlin Heidelberg, 2012. – ISBN 978–3–642–19886–1

[BSSW11] Borges, Georg ; Schwenk, Jörg ; Stuckenberg, Carl-Friedrich ; Wegener, Christoph: *Identitätsdiebstahl und Identitätsmissbrauch im Internet: Rechtliche und technische Aspekte.* Berlin and Heidelberg : Springer-Verlag Berlin Heidelberg, 2011. – ISBN 9783642158339

[BT10] Bertino, Elisa ; Takahashi, Kenji: *Identity Management: Concepts, technologies, and systems.* Boston and MA and London : Artech House, 2010. – ISBN 978–1–60807–039–8

[Bun02] Bundeszentrale für politische Bildung: *Sicherheit und Freiheit | bpb.* Version: 2002. http://www.bpb.de/apuz/27040/sicherheit-und-freiheit, Abruf: 04.04.2013

[Bun08] Bundesamt für Sicherheit in der Informationstechnik: *BSI-Standard 100-1 - Managementsysteme für Informationssicherheit (ISMS).* 05.06.2008

[Bun13a] Bundesamt für Sicherheit in der Informationstechnik: *BSI für Bürger: Beispiele Phishing-Angriffe.* Version: 2013. https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Phishing/BeispielePhishingAngriffe/beispielephishingangriffe_node.html, Abruf: 29.03.2013

[Bun13b] Bundesministerium der Justiz: *BDSG - Paragraph 9.* Version: 2013. http://www.gesetze-im-internet.de/bdsg_1990/__9.html, Abruf: 03.04.2013

[BW07] Bleyer, Lutz ; Waldthausen, Christa: Wer wird FIDUCIA Security Champ? Erfolgreiche Security Awareness Kampagnen der Fiducia IT AG. In: *Datenschutz und Datensicherheit - DuD* 31 (2007), Nr. 7, 506–509. dx.doi.org/10.1007/s11623-007-0175-0, Abruf: 15.02.2013

[CJS+08] Cervesato, Iliano ; Jaggard, Aaron D. ; Scedrov, Andre ; Tsay, Joe-Kai ; Walstad, Christopher: Breaking and fixing public-key Kerberos. In: *Information and Computation* 206 (2008), Nr. 2-4, 402–424. http://ftp.cis.upenn.edu:21/pub/papers/scedrov/pkinit.pdf, Abruf: 16.05.2013

[Cle02] Clerq, Jan d.: *Single Sign-On Architectures.* Version: 2002. http://www.esat.kuleuven.be/cosic/seminars/slides/SSO.pdf, Abruf: 19.04.2013

[CMRW88] Carroll, John M. ; Mowat, Robert B. ; Robbins, Lynda E. ; Wiseman, David: The password predictor—a training aid for raising security awareness. In: *Computers & Security* 7 (1988), Nr. 5, 475–481. dx.doi.org/10.1016/0167-4048(88)90200-3, Abruf: 15.02.2013

[DJG12] Duggan, Geoffrey B. ; Johnson, Hilary ; Grawemeyer, Beate: Rational security: Modelling everyday password use. In: *International Journal of Human-Computer Studies* 70 (2012), Nr. 6, 415–431. dx.doi.org/10.1016/j.ijhcs.2012.02.008, Abruf: 16.03.2013

[Doc13] Documentation, Novell: *Novell eDirectory 8.8 SP7 Administration Guide.* https://www.netiq.com/de-de/documentation/edir88/pdfdoc/edir88.zip. Version: 2013

[Eck12] Eckert, Claudia: *IT-Sicherheit: Konzepte, Verfahren, Protokolle.* 7. Auflage. München : Oldenbourg, 2012. – ISBN 348670687X

[Ehl08] Ehle, Hermann: *Was wir Menschen brauchen: Ein Werkbuch für die Seelsorge.* Norderstedt : Books on Demand, 2008. – ISBN 9783833477218

[Fei12] Feiler, Mathias: *Das Kerberos-Protokoll: Eine Einführung in die Logik des Protokolls zu den Chemnitzer Linuxtagen 2012.* Version: 2012. http://www.openafs.at/sites/default/files/Kerberos_protokoll_clt2012_v1.6.0_0.pdf, Abruf: 13.06.2013

[FH11] Florêncio, Dinei ; Herley, Cormac: *Where do all the Attacks go?* Version: 2011. http://research.microsoft.com/pubs/149885/WhereDoAllTheAttacksGo.pdf, Abruf: 21.02.2013

[Gar03] Garman, Jason: *Kerberos: The definitive guide.* 1. Auflage. Sebastopol and CA and Farnham : O'Reilly, 2003. – ISBN 9780596004033

[GB76] Grinder, John ; Bandler, Richard: *The structure of magic.* Palo Alto (Calif.) : Science and Behavior Books, 1976. – ISBN 9780831400491

[Geb02] Gebert, Dirk: *ARIS und LDAP: ARIS und LDAP Möglichkeiten zur Verwendung eines Verzeichnisdienstes im ARIS Toolset.* Trier, Hochschule Trier - Trier University of Applied Sciences, Diss., 2002. http://www.hochschule-trier.de/uploads/tx_rfttheses/ARIS-LDAP.doc, Abruf: 24.05.2013

[GJ11] Grawemeyer, Beate ; Johnson, Hilary: *Using and managing multiple passwords: A week to a view.* Version: 2011. http://dl.acm.org/citation.cfm?id=1994160, Abruf: 12.04.2013

[GJN+] Graveman, Richard ; Janson, Phil ; Neumann, Clifford ; Gong, Li ; Bergadano, F. ; Crispo, B. ; Ruffo, G.: Proactive password checking with decision trees. In: ACM (Hrsg.): *CCS '97 Proceedings of the 4th ACM conference on Computer and communications security*, 67–77

[GK08] Geiger, Walter ; Kotte, Willi: *Handbuch Qualität: Grundlagen und Elemente des Qualitatsmanagements: Systeme - Perspektiven.* 5. Auflage. Wiesbaden : Friedr. Vieweg, 2008. – ISBN 9783834894298

[Goo11] Google: *google-pword.png (PNG-Grafik, 505 × 791 Pixel).* Version: 2011. http://www.lightbluetouchpaper.org/wp-content/uploads/2011/11/google-pword.png, Abruf: 21.03.2013

[Had11] Hadnagy, Christopher: *Die Kunst des Human Hacking: social engineering*. 2. Auflage. Heidelberg : mitp, 2011. – ISBN 9783826691676

[Hoi03] Hoier, Nils: *Seminararbeit Authentifikation Kerberos*. Hamburg, Universität der Freien und Hansestadt Hamburg, Diss., 28.05.2003. http://www.informatik.uni-hamburg.de/RZ/lehre/18.415/, Abruf: 19.04.2013

[IEE11] IEEE Computer Society: *Compatible Time-Sharing System (1961-1973): Fiftieth Anniversary Commemorative Overview*. Version: 2011. http://www.multicians.org/thvv/7094.html, Abruf: 11.04.2013

[IS10] Inglesant, Philip ; Sasse, Angela ; Department of Computer Science (Hrsg.): *The True Cost of Unusable Password Policies: Password Use in the Wild*. Version: 2010. http://www.cl.cam.ac.uk/%7Erja14/shb10/angela2.pdf, Abruf: 21.02.2013

[Jäg11] Jäger, Michael: *Single Sign-On / Identity Management: Ein Überblick*. Version: 09.01.2011. http://www.mni.thm.de/thm_repository/reposforschung/repos_isa/identity-management-jaeger_1307527751.pdf, Abruf: 12.05.2013

[Jan13] Janrain: *2013 Consumer Research: The Value of Social Login*. Version: 2013. http://www1.janrain.com/rs/janrain/images/Industry-Research-Value-of-Social-Login-2013.pdf, Abruf: 22.05.2013

[Jia09] Jian, Yang: An Improved Scheme of Single Sign-on Protocol. In: Conference Publishing Services (Hrsg.): *IAS '09 Fifth International Conference on Information Assurance and Security*, 2009, S. 495–498

[Kay] Kaye, Joseph '.: Understanding Self-reported Password Sharing Strategies. In: ACM (Hrsg.): *CHI '11 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2619–2622

[Kie08] Kielholz, Annette: *Online-Kommunikation: Die Psychologie der neuen Medien für die Berufspraxis*. Berlin : Springer, 2008. – ISBN 9783540763284

[Kli10] Klipper, Sebastian: *Konfliktmanagement für Sicherheitsprofis: Auswege aus der "Buhmann-Falle" für IT-Sicherheitsbeauftragte, Datenschützer und Co ; mit 25 Tabellen.* 1. Auflage. Wiesbaden : Vieweg + Teubner, 2010. – ISBN 9783834810106

[KRC06] Kuo, Cynthia ; Romanosky, Sasha ; Cranor, Lorrie F.: *Human Selection of Mnemonic Phrase-based Passwords.* Version: 2006. http://repository.cmu.edu/cgi/viewcontent.cgi?article=1043&context=isr, Abruf: 20.03.2013

[KS08] Kriha, Walter ; Schmitz, Roland: *Internet-Security aus Software-Sicht: Grundlagen der Software-Erstellung für sicherheitskritische Bereiche.* Berlin and Heidelberg : Springer, 2008. – ISBN 9783540222231

[Lar07] Lardschneider, Michael: Security Awareness — Grundlage aller Sicherheitsinvestitionen: Bei der Münchener Rückversicherungs-Gesellschaft. In: *Datenschutz und Datensicherheit - DuD* 31 (2007), Nr. 7, 492–497. dx.doi.org/10.1007/s11623-007-0172-3, Abruf: 15.02.2013

[Lee03] Lee, Spencer C. ; SANS Institute InfoSec Reading Room (Hrsg.): *An Introduction to Identity Management.* Version: 2003. http://www.sans.org/reading_room/whitepapers/authentication/an_introduction_to_identity_management_852, Abruf: 12.05.2013

[Mas02] Massachussetts Institute of Technology: *Kerberos V5 System Administrator's Guide.* Version: 11.09.2002. http://web.mit.edu/kerberos/www/krb5-1.2/krb5-1.2.6/doc/admin.html, Abruf: 03.05.2013

[MCTK] Ma, Wanli ; Campbell, John ; Tran, Dat ; Kleeman, Dale: Password Entropy and Password Quality. In: IEEE Computer Society (Hrsg.) ; IEEE Technical Committee on Scalable Computing (Hrsg.): *2010 4th International Conference on Network and System Security (NSS)*, 583–587

[Mey11] Meyer, Julia ; - Recht-Steuern-Wirtschaft - Verlag C.H.Beck (Hrsg.): *Identität und virtuelle Identität natürlicher Personen im Internet - Zusammenfassung.* Version: 2011. http://rsw.beck.de/CMS/?toc=ZD.60&docid=324445, Abruf: 28.03.2013

[MP07] Mix, Markus ; Pingel, Miriam: Be better — Be secure: Security Awareness in der Bosch-Gruppe. In: *Datenschutz und Datensicherheit - DuD* 31 (2007), Nr. 7, 498–501. dx.doi.org/10.1007/s11623-007-0173-2, Abruf: 15.02.2013

[MS08] Mitnick, Kevin D. ; Simon, William L.: *Die Kunst des Einbruchs: Risikofaktor IT*. Heidelberg : Redline, 2008. – ISBN 9783826617461

[MSD11] Mitnick, Kevin D. ; Simon, William L. ; Dubau, Jürgen: *Die Kunst der Täuschung: Risikofaktor Mensch*. [Heidelberg] : mitp, 2011. – ISBN 9783826615696

[Mül11] Müller, Klaus-Rainer: *IT-Sicherheit mit System: Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement - Sicherheitspyramide - Standards und Practices - SOA und Softwareentwicklung*. 4. Auflage. Wiesbaden : Vieweg+Teubner Verlag / Springer Fachmedien Wiesbaden GmbH, Wiesbaden, 2011. – ISBN 3834881783

[OAS05a] OASIS: *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. Version: 2005. http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf, Abruf: 10.05.2013

[OAS05b] OASIS: *Security Assertion Markup Language (SAML) 2.0 Technical Overview*. Version: 2005. https://www.oasis-open.org/committees/download.php/11511/sstc-saml-tech-overview-2.0-draft-03.pdf, Abruf: 10.05.2013

[Ope13] OpenID: *OpenID Authentication 2.0 - Final*. Version: 2013. http://openid.net/specs/openid-authentication-2_0.html, Abruf: 18.05.2013

[PM03] Pashalidis, Andreas ; Mitchell, Chris J.: A Taxonomy of Single Sign-On Systems. In: *INFORMATION SECURITY AND PRIVACY, 8TH AUSTRALASIAN CONFERENCE, ACISP 2003* 2727 (2003), 249–264. dx.doi.org/10.1007/3-540-45067-X_22

[Poh03] Pohlmann, Norbert: *Firewall-Systeme: [Firewall-Elemente und Sicherheitskonzepte ; Verschlüsselungs- und Authentikationsverfahren ; Security Audit, Bedrohungsprofile, IT-Kostenschätzung]*. Version: 2003. https://www.internet-sicherheit.de/fileadmin/docs/publikationen/firewall-systeme/firewall-systeme-271-286.pdf, Abruf: 15.03.2013

[RB11] Revar, Ashish G. ; Bhavsar, Madhuri D.: Securing user authentication using single sign-on in Cloud Computing. In: IEEE (Hrsg.): *NUiCONE '11 Nirma University International Conference on Engineering*, 2011, 1–4

[RGT+] Raskin, Victor ; Greenwald, Steven J. ; Timmerman, Brenda ; Kienzle, Darrell ; Yan, Jianxin J.: A note on proactive password checking. In: ACM (Hrsg.): *NSPW '01 Proceedings of the 2001 workshop on New security paradigms*, 127

[RJ13] Rivest, Ronald L. ; Juels, Ari: *Honeywords: Making Password-Cracking Detectable.* Version: 2013. http://people.csail.mit.edu/rivest/pubs.html#JR13, Abruf: 08.05.2013

[RR12] Radha, V. ; Reddy, D. H.: A Survey on Single Sign-On Techniques. In: *Procedia Technology* 4 (2012), 134–139. dx.doi.org/10.1016/j.protcy.2012.05.019, Abruf: 16.03.2013

[RSA12] RSA: *RSA SECURID AUTHENTICATORS: The gold standard in two-factor authentication.* Version: 2012. http://www.rsa.com/products/securid/datasheets/2305_h9061-sid-ds-0212.pdf, Abruf: 29.04.2013

[Rus10] Russer, Martin: *Web-Authentifizierung mit Open-ID.* Erlangen-Nürnberg, Universität Erlangen-Nürnberg, Diss., 21.07.2010. https://www4.cs.fau.de/Lehre/SS10/PS_KVBK/papers/10.v2.martin.russer.ausarbeitung.pdf, Abruf: 10.05.2013

[SAP12] SAP: *SAP-Bibliothek - Identity-Management: Kennwortregeln.* Version: 2012. http://help.sap.com/erp2005_ehp_04/helpdata/de/d2/141fb593c742b5aad8f272dd487b74/frameset.htm, Abruf: 29.03.2013

[Sch96] Schneier, Bruce: *Applied cryptography: Protocols, algorithms, and source code in C.* 2. Auflage. New York : Wiley, 1996. – ISBN 0470226269

[Sch99] Schoenherr, Oliver: *Konzeption und Entwicklung eines Java-Backends fuer einen LDAP Server*, Fachhochschule für Technik und Wirtschaft Berlin, Diss., 13.07.1999. http://inet.cpt.haw-hamburg.de/thesis/completed/oliver_schoenherr.pdf, Abruf: 23.05.2013

[Sch01] Schneier, Bruce: *Secrets & lies: IT-Sicherheit in einer vernetzten Welt.* 1. Auflage. Heidelberg : Dpunkt-Verl., 2001. – ISBN 3898641139

[Sch07] Schimmer, Klaus: Sicherheit beginnt im Kopf: Sensibilisieren - aber wie? In: *Datenschutz und Datensicherheit - DuD* 31 (2007), Nr. 7, S. 510–514

[Sch08a] Schimmer, Klaus: Wenn der Hacker zweimal fragt! Wie bereite ich meine Mitarbeiter auf Social Engineering Angriffe vor? In: *Datenschutz und Datensicherheit - DuD* 32 (2008), Nr. 9, S. 569–573

[Sch08b] Schneier, Bruce: *The Psychology of Security*. Version: 2008. http://www.schneier.com/essay-155.pdf, Abruf: 15.02.2013

[Sch13] Schulz von Thun Institut Hamburg: *Kommunikationsquadrat*. Version: 2013. http://www.schulz-von-thun.de/index.php?article_id=71, Abruf: 21.03.2013

[Sei09] Seidl, Barbara: *NLP: Mentale Ressourcen nutzen*. 2. Auflage. München : Haufe Verlag, 2009. – ISBN 978–3–448–10064–8

[SFH09] Somayaji, Anil ; Ford, Richard ; Herley, Cormac: So long, and no thanks for the externalities: the rational rejection of security advice by users. In: ACM (Hrsg.): *NSPW '09 Proceedings of the 2009 workshop on New security paradigms workshop*, 2009, 133–144

[Shi07] Shirley, R.: *RFC 4949 - Internet Security Glossary, Version 2*. Version: 2007. https://tools.ietf.org/html/rfc4949, Abruf: 24.04.2013

[SMS+12] Somorovsky, Juraj ; Mayer, Andreas ; Schwenk, Jörg ; Kampmann, Jörg ; Jensen, Meiko ; Ruhr-Universität Lehrstuhl für Netz- und Datensicherheit (Hrsg.): *On Breaking SAML: Be Whoever You Want to Be*. Version: 2012. http://www.nds.rub.de/media/nds/veroeffentlichungen/2012/08/22/BreakingSAML_3.pdf, Abruf: 11.05.2013

[SPS11] Spitzer, Stephan ; Pramateftakis, Michael ; Swoboda, Joachim: *Kryptographie und IT-Sicherheit: Grundlagen und Anwendungen*. 2. Auflage. Wiesbaden : Springer Fachmedien Wiesbaden, 2011. – ISBN 9783834814876

[Sta03] Stadler, Bernhard: "Mehrzweckwaffe" Single Sign-On. In: GI (Hrsg.): *INFORMATIK 2003 - Mit Sicherheit Informatik*, Bd. 36, 2003 (LNI), S. 333–336

[Sta06] Stamp, Mark: *Information security: Principles and practice*. 2. Auflage. Hoboken and N.J : Wiley-Interscience and Wiley, 2006 // 2011 // 2006. – ISBN 9780471738480

[Sys13] System Architecture @ Humboldt University Berlin: *OpenID*. Version: 2013. http://sarwiki.informatik.hu-berlin.de/OpenID, Abruf: 21.05.2013

[TJ09] Tiwari, Paras B. ; Joshi, Shashidhar R.: Single sign-on with one time password. In: IEEE (Hrsg.): *AH-ICI 09 First Asian Himalayas International Conference on Internet*, 2009, S. 1–4

[TS08] Tanenbaum, Andrew S. ; Steen, Maarten v.: *Verteilte Systeme: Prinzipien und Paradigmen.* 2. Auflage. München [u.a.] : Pearson Studium, 2008 (Informatik). – ISBN 9783827372932

[TS10] Tsolkas, Alexander ; Schmidt, Klaus: *Rollen und Berechtigungskonzepte: Ansätze Für Das Identity- Und Access Management Im Unternehmen.* Wiesbaden : Vieweg+Teubner and Vieweg + Teubner Verlag, 2010. – ISBN 9783834812438

[Vie09] Viega, John: *The myths of security: What the computer security industry doesn't want you to know.* 1. Auflage. Beijing and Cambridge and Sebastopol and CA : O'Reilly, 2009. – ISBN 9780596523022

[Vle12] Vleck, Tom van: *Password Generator: modeled after Morrie Gasser's original generator.* Version: 2012. http://www.multicians.org/thvv/gpw.html, Abruf: 20.03.2013

[VPBS+07] Vu, Kim-Phuong L. ; Proctor, Robert W. ; Bhargav-Spantzel, Abhilasha ; Tai, Bik-Lam ; Cook, Joshua ; Eugene Schultz, E.: Improving password security and memorability to protect personal and organizational information. In: *International Journal of Human-Computer Studies* 65 (2007), Nr. 8, S. 744–757. http://www.sciencedirect.com/science/article/pii/S1071581907000560, Abruf: 16.03.2013

[Weß08] Wesselmann, Bettina: Maßnahmen gegen Social Engineering: Training muss Awareness-Maßnahmen ergänzen. In: *Datenschutz und Datensicherheit - DuD* 32 (2008), Nr. 9, S. 601–604

[Wie12] Wiesner, Mike: *Kerberos als unternehmensweites Single-Sign-On.* Version: 2012. http://de.slideshare.net/mike.wiesner/kerberos-als-unternehmsweites-single-sign-on, Abruf: 17.06.2013

[Wit06] Witt, Bernhard C.: *IT-Sicherheit kompakt und verständlich: Eine praxisorientierte Einführung.* 1. Auflage. Wiesbaden : Vieweg, 2006. – ISBN 9783834801401

[YBAG04] Yan, J. ; Blackwell, A. ; Anderson, R. ; Grant, A.: Password memorability and security: empirical results. In: *IEEE Security & Privacy Magazine* 2 (2004), Nr. 5, S. 25–31. dx.doi.org/10.1109/MSP.2004.81

[ZH99] Zviran, Moshe ; Haga, William J.: Password Security : An Empirical Study. In: *JSTOR: Journal of Management Information Systems, Vol 15* No. 4 (Spring, 1999) (1999), Nr. 15, 161–185. http://www.jstor.org/discover/10.2307/40398409?uid=3737864&uid=2134&uid=369001211&uid=2&uid=70&uid=3&uid=369001201&uid=60&sid=21101819435751, Abruf: 13.03.2013

Tabellenverzeichnis

Abbildungsverzeichnis

Verzeichnis der Quellcodes

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Hamburg, 26. Juni 2013 Stefanie Langer