HAW HAMBURG

BACHELORTHESIS
Jan Pietsch

Evaluation von Authentifizierungsverfahren am Beispiel eines Versicherungsunternehmens

FAKULTÄT TECHNIK UND INFORMATIK
Department Informatik

Faculty of Computer Science and Engineering
Department Computer Science

HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN HAMBURG
Hamburg University of Applied Sciences

Jan Pietsch

Evaluation von Authentifizierungsverfahren am Beispiel eines Versicherungsunternehmens

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung
im Studiengang *Bachelor of Science Informatik Technischer Systeme*
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

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

Eingereicht am: 14. Dezember 2021

Jan Pietsch

Thema der Arbeit

Evaluation von Authentifizierungsverfahren am Beispiel eines Versicherungsunternehmens

Stichworte

Authentifizierung, IT-Sicherheit, Versicherungsunternehmen

Kurzzusammenfassung

Diese Arbeit befasst sich mit dem Vergleichen und der Vorstellung von unterschiedlichen Authentifizierungsverfahren. Dazu werden mehrere Verfahren der drei Kategorien Wissen, Besitz und Biometrie erklärt und anschließend mithilfe einer Nutzwertanalyse bewertet und verglichen. Die Verfahren werden anhand ihrer Sicherheit, Kosten und Benutzerfreundlichkeit für ein fiktives Versicherungsunternehmen analysiert.

Jan Pietsch

Title of Thesis

Evaluation of authentication methods using the example of an insurance company

Keywords

Authentication, IT-Security, insurance company

Abstract

This thesis deals with the comparison and the presentation of different authentication methods. For this purpose, several methods belonging to the three categories of knowledge, possession and biometrics are explained and then evaluated and compared with the help of a value benefit analysis. The methods are analyzed for a fictitious insurance company based on their security, costs and usability.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Bzw.	Beziehungsweise
FRR	False rejection rate
FAR	False acceptance rate
WLAN	Wireless local area network
AG	Aktiengesellschaft
DNA	deoxyribonucleic acid
EEG	Elektroenzephalografie
KI	Künstliche Intelligenz
OTP	One time password
AS	Authentifizierungs-Server
GSM	Global System for Mobile communications
SIM	Subscriber identity module

SMS	Short message service
2FA	2 Faktor Authentifizierung
API	Application Programming Interface

Glossar

Active Directory	Verzeichnisdienst von Microsoft zum Verwalten von Zugriffsrechten und Rollen der User im Intranet einer Firma
Kerberos Protokoll	Authentifizierungsdienst zwischen Hosts in offenen oder unsicheren Netzwerken unter Verwendung von kryptografischer Verschlüsslung
Hashing	Transformation eines Datensatzes in eine Zeichenkette mit fester kürzerer Länge bestehend aus Schlüssel und Werte Paaren
Deepfake	Authentisch wirkende Bilder oder Videos, die mithilfe künstlicher Intelligenz verändert oder verfälscht wurden
Open Source	Öffentliche Software, deren Quelltext von allen Personen genutzt und verändert werden darf
Bluetooth	Funkstandart zum Übertragen von Daten auf kurze Distanzen

1 Einleitung

1.1 Motivation

Authentifizierung ist das Prinzip der Überprüfung der Identität einer Person auf Authentizität, um Zugang zu einem zugriffbeschränkten System zu erhalten. Es ist eines der wichtigsten Themen in der IT-Sicherheit, da fast alle wichtigen Inhalte, Anwendungen und Geräte so geschützt sind, dass man sich zuerst authentifizieren muss, um auf sie zugreifen zu können. Diese Signifikanz führt dazu, dass die Authentifizierung ein beliebtes Ziel von Angriffen durch technisches oder soziales Hacking ist. Laut einer Studie mit dem Namen „Identity Security: A Work in Progress“ von 2020 haben 94 Prozent aller untersuchten Organisationen schon einmal Daten durch einen Identitätsbezogenen Angriff verloren [1], deshalb wird an bestehenden Authentifizierungsverfahren weiterhin geforscht. Zudem werden neue Arten der Authentifizierung erfunden und ausprobiert. Daher ist ebenso wichtig, dass Unternehmen sich über die Stärken und Gefahren verschiedener Authentifizierungsverfahren im Klaren sind. So können sie die sicherste und passendste Technik für ihr Unternehmen auswählen.

1.2 Problem und Zielstellung

Ziel der Arbeit ist es, anhand eines fiktiven Anwendungsszenarios verschiedene neuere Authentifizierungsverfahren zu bewerten und auf ihre Effektivität sowie den Nutzen für das Anwendungsszenario zu prüfen. Zu diesem Zweck wird eine Nutzwertanalyse für eine fiktive Firma erstellt werden.

Dazu werden folgende Forschungsfragen definiert, die diese Arbeit beantwortet:

1. Welche der Authentifizierungsverfahren kommen für das Anwendungsszenario in Frage?
2. Welche Authentifizierungsverfahren sind am besten für die Bedürfnisse der fiktiven Firma geeignet?
3. Wie viel sicherer sind die neuen Authentifizierungsverfahren verglichen mit der alten Authentifikationsmöglichkeit der fiktiven Firma?

1.3 Aufbau der Arbeit

Zuerst werden die für das Verständnis der Arbeit benötigten Grundlagen kurz zusammengefasst. Daraufhin folgt eine genauere Beschreibung des Anwendungsbeispiels, also des fiktiven Unternehmens. Dabei geht es um die Frage, warum das Unternehmen einen Bedarf nach einem neuen Authentifizierungsverfahren hat. Im nächsten Teil werden die Bewertungskriterien festgelegt, anhand derer die Authentifizierungsverfahren durch eine Nutzwertanalyse untersucht werden. Danach werden die Authentifizierungsverfahren, die für das Anwendungsbeispiel in Frage kommen, nacheinander vorgestellt. Im Hauptteil werden die Verfahren anhand einer Nutzwertanalyse nach den Kriterien Sicherheit, Kosten und Benutzerfreundlichkeit verglichen. Es werden die für die Firma am passendsten Verfahren ausgewählt. Darauffolgend wird beschrieben, wie sich der Wechsel vom alten zum neuen Verfahren in Bezug auf Kosten und technische Integration auswirkt. Zum Schluss wird geprüft, ob die Ziele der Arbeit erreicht worden sind, und es wird ein kurzer Ausblick auf die Zukunft der Authentifizierung gegeben.

1.4 Zielgruppe

Die Arbeit richtet sich an Personen, die sich mit IT-Sicherheit, insbesondere mit dem Unterthema der Authentifikation auseinandersetzen. Interessierte können versuchen die Nutzwertanalyse und ihre Kriterien auf ihr eigenes Beispiel anzupassen und anzuwenden. Außerdem ist diese Arbeit im weiteren Sinne für jeden Menschen mit einem Smartphone oder Computer interessant, der sich über die verschiedenen Authentifizierungsverfahren und ihre Risiken informieren möchte.

1.5 Einordnung und Abgrenzung

Es muss gesagt werden, dass das hier verwendete Anwendungsbeispiel sehr spezifisch ist und nicht universell auf jedes andere Unternehmen zutrifft. Es gibt bereits umfangreiches Material zum Thema Authentifizierung. Außerdem existieren Untersuchungen und Bewertungen der verschiedenen Verfahren, die zur Authentifizierung möglich sind. Solche Untersuchungen sind zum Beispiel „A Review on Authentication Methods [2]“ oder „A Survey on Password Attacks and Comparative Analysis on Methods for Secure Authentication [3]“. Des Weiteren existieren viele Arbeiten über einzelne oder Gruppen von Authentifizierungserfahren, die genauer ins Detail gehen und bestimmte technische Implementierungen von Authentifizierungsverfahren vorstellen. Diese Arbeit zielt darauf ab, eine Zusammenfassung der Methoden in einem größeren Ramen zu geben. Zudem werden die verschiedenen Verfahren auf ein bestimmtes Beispiel angewendet, um dem Lesenden einen Kontext zu bieten.

2 Grundlagen

2.1 IT-Sicherheit

IT-Sicherheit ist der Bereich der Informatik, der davon handelt, Unternehmen und ihre Informationen zu schützen und wirtschaftliche Schäden durch Manipulation, Diebstahl und Vernichtung von Daten und Dienstleistungen zu verhindern oder zumindest Maßnahmen und Konzepte zur Verringerung potenzieller Schäden zu entwickeln [4]. Grundsätzlich geht es darum, Informationen und Datenpakete von IT-Systemen zu beschützen. Zu diesem Zweck gib es verschiedene Schutzziele.

- Informationsvertraulichkeit („Confidentiality“): Schutz der Informationen vor unautorisierter Einsichtnahme
- Datenintegrität („Integrity“): Schutz der Daten vor Modifikation und Löschung
- Systemverfügbarkeit („Availability“): Schutz des Systems vor beabsichtigten Abstürzen oder sonstigen Störungen
- Authentizität („Authenticity“): Schutz vor Täuschungen durch das Sicherstellen der eindeutigen Identität eines Objektes oder Subjektes
- Verbindlichkeit („Non Repudiation“): Schutz vor Falschbehauptungen durch Beweisbarkeit der Durchführung aller Aktionen

Diese Schutzziele sollten Entwickler und Entwicklerinnen eines IT-Systems berücksichtigen, damit ihr System sicher ist. Erfolgreiche Angriffe sowie nicht autorisierte Zugriffe auf das IT-System verstoßen gegen die Schutzziele. Passive Angriffe nennt man Angriffe, die auf vertrauliche Informationen zugreifen, dadurch wird die Informationsvertraulichkeit gebrochen. Die Datenintegrität und Systemverfügbarkeit werden durch aktive Angriffe verloren. Das sind Angriffe, die Daten oder Systemressourcen verändern oder löschen [5].

2.2 Authentifizierung

Bei der Authentifizierung geht es darum sicherzustellen, dass eine Person auch wirklich diejenige ist, für die sie sich ausgibt. Es muss eine eindeutige Identifizierung durch wohldefinierte Eigenschaften sichergestellt sein [4]. Wichtig ist zu wissen, dass eine Person sich bei einem System authentisiert, wenn sie sich anmeldet und das System beziehungsweise ein Authentifizierungsserver die Person überprüft und dann authentifiziert [6]. Das Authentifizieren passiert meist durch im System gespeicherte Daten und Attribute zur Person. Es gibt drei Kategorien, in die Authentifizierungsverfahren sich einordnen lassen.

- Authentifizierung durch (geheimes) Wissen
- Authentifizierung durch (persönlichen) Besitz
- Authentifizierung durch (biometrische) Merkmale

Beim Authentifizieren durch Wissen besitzt ein Benutzer bzw. eine Benutzerin geheime Informationen. Mit diesen Informationen authentisiert er oder sie sich. Schwächen dieser Methode sind, dass es möglich ist, die Informationen zu vergessen. Außerdem können die Informationen dupliziert, gestohlen oder sogar erraten werden. Beliebte Beispiele einer Authentifizierung durch Wissen sind Passwörter, PINS und Sicherheitsfragen.

Authentifizierung durch Besitz bezieht sich auf einen Benutzenden, der sich durch Vorzeigen eines Gegenstandes authentisiert. Der Gegenstand kann physisch oder auch virtuell vorliegen. Nachteile der Methode sind eventuell hohe Herstellungskosten des Gegenstandes sowie die Gefahr von Verlust oder Diebstahl. Beispiele für Authentifizierung durch Besitz sind Schlüsselkarten, physische Schlüssel, SIM-Karten (beim mTAN Verfahren) und USB-Token.

Die letzte Kategorie Authentifizierung durch biometrische Merkmale beinhaltet Verfahren, bei denen der Benutzer sich durch einmalige Merkmale authentisiert. Solche Merkmale werden vom Benutzer immer mit sich geführt, können nicht weitergegeben werden und benötigen meist ein besonderes Gerät, um überprüft zu werden. Nachteile dieser Kategorie sind, dass Merkmale sich durch Unfälle oder Alter verändern können. Verlorene Merkmale sind oft unersetzbar. Außerdem kann es bei der Kontrolle der Merkmale zu Problemen beim Datenschutz

kommen. Fingerabdruck, Gesichtserkennung, Stimmerkennung und Tippverhalten sind einiger Beispiele für Merkmale der Authentifizierung durch biometrische Merkmale [7].

Biometrische Verfahren werden des Weiteren in zwei Unterkategorien eingeteilt: Die physischen Eigenschaften, die ein Mensch besitzt, und die dynamischen Eigenschaften, die sich auf das Verhalten des Menschen beziehen. Zu den physischen gehören Fingerabdruck, Gesichtsgeometrie und Netzhautmuster, während man bei den dynamischen von der Art und dem Rhythmus einer Stimme, dem Tippverhalten und der Gangart spricht [4].

Die Anforderungen, die ein biometrisches Merkmal aufweisen sollte, um als Authentifizierungsmethode verwendet werden zu können, sind folgende: Jedes Merkmal muss universell bei jeder Person vorhanden sein. Es muss unterschiedlich für jede Person sein. Es muss unveränderlich, fälschungssicher, quantitativ erfassbar, schnell und genau prüfbar sein. Zudem muss die Akzeptanz beim Nutzer bzw. der Nutzerin gegeben sein [7].

Da biometrische Verfahren bei der Authentifizierung oftmals nicht hundertprozentig erfolgreich sind, gibt es verschiedene Fehlerraten. Mithilfe derer lassen sich biometrische Verfahren besser bewerten.

Hauptsächlich existieren zwei Typen von Fehlern: Eine berechtigte Person wird abgewiesen und eine unberechtigte Person wird zugelassen. Wenn berechtigte Nutzende abgewiesen werden, liegt das oft daran, dass die Authentifizierungskriterien zu streng sind. Wenn andererseits die Kriterien zu schwach sind, kann es dazu kommen, dass unberechtigte Benutzer authentifiziert werden. Die Maßangabe der Fehlerrate zur Ablehnung berechtigter Benutzer nennt man auf Englisch „false rejection rate“ (FRR), während die Maßeinheit der Fehlerrate zur Akzeptanz unautorisierter Benutzer „false acceptance rate“ (FAR) genannt wird [4].

Der Ablauf der biometrischen Authentifizierung beginnt mit der Erfassung und Vorverarbeitung von Messdaten durch einen biometrischen Sensor („Feature Extraction“). Dann werden die gemessenen Daten eines Nutzenden in einer Datenbank abgespeichert (Registrierung). Bei der Authentifizierung wird der Nutzende nach einer erneuten „Feature Extraction“ in der Datenbank gesucht (Identifikation) und die aktuellen gemessenen Daten werden mit den gespeicherten abgeglichen (Verifikation) [7].

2.3 Angriffstechniken auf Authentifikation

In diesem Unterkapitel werden verschiedene Angriffstechniken zum Erschleichen von Passwörtern oder Umgehen von Authentifizierung vorgestellt und kurz erklärt. Außerdem werden Möglichkeiten erläutert, wie ein Angreifender nach Inbesitznahme der Passwörter damit Schaden anrichten kann.

2.3.1 Social Hacking/Social Engineering

Unter dem Begriff „Social Hacking“ oder “Social Engineering” versteht man alle Vorgehensweisen, mit denen Personen überredet, getäuscht, manipuliert oder gelenkt werden, einem Angreifer Informationen oder Zugangsdaten zu verschaffen. Viele Mitarbeitende sind leichtgläubig und geben leicht nach, wenn der Angreifer genug Druck ausübt. Als Beispiel eines Social Hacking Angriffes könnte ein Angreifender den Support einer Firma anrufen und sich als neuer Mitarbeitender ausgeben, der seine Nutzerkennung und Passwort noch nicht erhalten hat. Durch Recherche auf der Website der Firma oder in sozialen Netzwerken sind Angreifende in der Lage Informationen herausfinden, wie zum Beispiel der Namen eines Chefs. Diese Informationen nutzen sie dann, um den Mitarbeitenden davon zu überzeugen, ihnen Zugangsdaten zu verschaffen [8].

Eine Form des Social Engineering ist Shoulder Surfing. Bei dieser Attacke versucht ein Angreifender einem Benutzer bzw. einer Benutzerin unauffällig dabei zuzugucken, wie sich dieser/diese anmeldet. Das Ziel der Attacke ist es, durch Ablesen der Tasteneingaben oder des Anmeldefensters auf dem Bildschirm die Logindaten des Benutzenden zu erhalten.

Phishing ist eine Form des Social Engineerings, bei der kein persönlicher Kontakt zum Opfer hergestellt wird, sondern der Angreifende eine Menge von E-Mails versendet, in denen er sich zum Beispiel als Mitarbeitender des Supports ausgibt, der alle Adressaten auffordert, ihre Passwörter zu bestätigen [9].

2.3.2 Cracking von Passwortdateien

Beim Cracking von Passwortdateien geht es darum, das Passwort eines Nutzenden zu erraten. Wenn er oder sie ein schwaches Passwort gewählt hat, lässt sich dieses manchmal schon nach einer Onlinesuche zur jeweiligen Person erraten. Alternativ kann man einen Computer das Passwort erraten lassen [8]. Das funktioniert auf verschiedene Arten.

Die Brute Force (auf Deutsch rohe Gewalt) Attacke, braucht lange Zeit und versucht durch Ausprobieren aller möglichen Tastenkombinationen das richtige Passwort zu finden. Bei kurzen Passwörtern kann das schnell gehen. Bei längeren Passwörtern mit großen Passworträumen dauert das mit heutiger Technologie allerdings Jahre.

Die Wörterbuch Attacke ist hingegen deutlich schneller. Diese testet alle Wörter im Wörterbuch als Passwort. Wenn Benutzende schwache Passwörter ohne Nummern oder Sonderzeichen gewählt haben, kann es gut sein, dass eine Wörterbuch Attacke erfolgreich ist. [9]

2.3.3 Abhören des Netzverkehrs (“Sniffer”)

In einem Broadcast Netzwerk wie zum Beispiel WLAN kann der Verkehr von Datenpaketen von jedem angeschlossenen Computer im Netzwerk mitverfolgt werden. Mithilfe von Tools wie „Wireshark“ ist es für einen Angreifenden möglich, jedes Datenpaket zu analysieren und durch geschicktes Aufdröseln der Inhalte vertrauliche Informationen zu stehlen. Mit Glück und Geduld erhält er oder sie sogar Zugangsdaten von Benutzern [8].

Mit diesen meldet sich der Angreifende selbst an, um dann vertrauliche Daten zu stehlen, zu modifizieren oder zu löschen. Das Wiedereinspielen oder Verschicken von abgefangenen Datenpaketen und Informationen nennt man eine Replay Attacke.

Außerdem kann ein Angreifender mithilfe der Zugangsdaten eine Man-in-the-Middle Attacke durchführen. Hierbei schaltet er sich zwischen die Kommunikation zweier Geräte oder Parteien und gibt sich als die jeweils andere Parteie aus. So kann er Teile der Kommunikation ändern oder löschen und so gezielt Schaden verursachen [9].

2.4 Nutzwertanalyse

Eine Nutzwertanalyse unterstützt das Management dabei, eine Entscheidung über eine Vielzahl verschiedener Produkte und Lösungen für ein Problem zu treffen. Mithilfe der Nutzwertanalyse sind Manager dazu in der Lage, eine große Anzahl an Entscheidungsalternativen durch verschiedene Kriterien zu bewerten und nach ihrer Präferenz durch Gewichtungen zu ordnen [10].

Man beginnt eine Nutzwertanalyse, indem man sein Problem klar formuliert. Im nächsten Schritt wird ein Zielsystem aufgestellt. Dabei unterteilt man sein Problem in verschiedene messbare Ziele. Die Zielhierarchie kennt Oberziele, die jeweils in kleinere Zwischen- oder Unterziele eingeteilt sind.

Nun gilt es, alle Alternativen aufzulisten und für jede Alternative einen Ergebniswert pro Unterziel herzuleiten oder zu messen. Die Ergebniswerte können zum Beispiel im Wertebereich 0 bis 100 Punkte liegen.

Jedem Unterziel wird dann ein Zielgewicht zugeschrieben. Die Summe der Zielgewichte der Unterziele eines Oberziels sollte 1 oder 100 Prozent ergeben. So kann für jedes Oberziel einer Alternative ein Wert errechnet werden. Auch die Oberziele erhalten alle wieder eine Zielgewichtung, so dass deren Summe 1 ergibt. Am Ende erhält man so für jede der Alternativen einen Gesamtwert.

Zum Schluss ordnet man die Alternativen nach ihrem Gesamtwert in einer Rangliste an. Das Management erhält auf diese Weise einen Überblick über alle alternativen Lösungen und deren jeweiligen Nutzen. Das verschafft Gesamtverständnis des Problems sowie der verschiedenen Lösungsverfahren [11].

Um bestimmte Alternativen schon vor Durchführung der Nutzwertanalyse auszuschließen, ist es möglich, sogenannte KO-Kriterien festzulegen. Diese Kriterien beschreiben verschiedenen Eigenschaften bzw. Werte, die alle Alternativen besitzen müssen bzw. nicht überschreiten dürfen. Werden die Werte von einer Alternative überschritten, so kann diese Alternative direkt als Lösung ausgeschlossen werden.

3 Anwendungsszenario

3.1 Vorstellung der Firma

Die Versi AG ist ein fiktives Unternehmen und hat ihren Sitz in Hamburg. Versi wurde 1985 von einer Gruppe von jungen Unternehmern gegründet. Mittlerweile hat die AG bereits fast 10.000 Mitarbeiter. Darunter 8 Mitglieder des Vorstands und einen Aufsichtsrat mit Vertretern der Anteilseigner und Arbeitnehmer. Der Rest des Unternehmens lässt sich in verschiedenen Mitarbeitergruppen einteilen, die gleichzeitig auch unterschiedliche Sicherheitsgruppen mit abweichenden Sicherheitsberechtigungen darstellen. Darunter sind die Beratungsabteilung, in der sich hauptsächlich Versicherungsexperten und -berater befinden, die Personalabteilung, die IT-Abteilung und die Logistikabteilung. Zudem heuert Versi unabhängige Dienstleister für Catering und Säuberung an.

Versi bietet Kunden in ganz Deutschland ein weites Spektrum an Versicherungen. Dazu gehören Renten-, Lebens-, Berufsunfähigkeit-, Kranken-, Unfall-, Schadensversicherungen und vieles mehr.

Das Unternehmen garantiert seinen Mitarbeitenden feste Strukturen und gute Aufstiegschancen. Zudem gibt es Unterstützung von erfahrenen Mentoren für die Neuzugänge. Im Großraumbüro in Hamburg, dem Hauptsitz der Firma, erhalten Mitarbeitende ihren eigenen Arbeitsplatz mit einem Computer mitsamt Tastatur, Maus und Headset sowie eine Grundausstattung an Büroutensilien. Innerhalb des Gebäudes gibt es verschiedenen Bereiche, die extra abgesichert sind. Beispiele hierfür sind der zentrale Computerraum und der Serverraum. Diese Räume sollen nur von bestimmten Zugangsberechtigten der IT-Abteilung benutzt werden und haben daher Tür-Codeschlösser mit Nummernfolgen, die den Berechtigten mitgeteilt werden. Wenn ein Putztermin ansteht, wird vorher der Reinigungsfirma der Code zugeschickt. Aus Sicherheitsgründen ändern sich die Codes in regelmäßigen Abständen.

Um ihre 10.000 Angestellten und deren Arbeitsrechner zu organisieren, benutzt die Versi AG eine Serverlandschaft aus Windows Servern. Das daraus entstehende Netzwerk wird durch Active Directory verwaltet. Damit ein Benutzender auf die Ressourcen der Firma zugreifen kann, muss er oder sie vom Active Directory Domain Controller authentifiziert werden. Mithilfe des eingebauten Kerberos-Protokolls meldet sich jeder Benutzer sich für die verschiedenen Dienste der Firma nur einmal an seinem Arbeitsplatz an.

Bisher hatte das Unternehmen zum Authentifizieren der Benutzenden auf traditionelle Benutzeraccounts und Passwörter gesetzt. Jeder Mitarbeitende hatte einen eigenen Account und ein Passwort, das beim Erstellen des Accounts generiert wurde, sich aber vom User ändern ließ.

Leider traten nach einiger Zeit Sicherheitslücken auf. Einzelne Personen hefteten sich Passwörter per Notizzettel an den Bildschirm oder suchten sich sehr einfache Passwörter (z.B. “Passwort”, “123456”) aus. Diese ließen sich durch Erraten oder Social Hacking finden. Nun ist das Unternehmen auf der Suche nach einer sicheren Methode, die auch die Kosten und Benutzerfreundlichkeit berücksichtigt.

4 Nutzwertanalyse

4.1 Festlegen von Bewertungskriterien

Der wichtige Teil, um die verschiedenen potenziellen Authentifizierungsverfahren überhaupt miteinander vergleichen zu können und in einer Rangfolge aufstellen zu können, ist das Festlegen von verständlichen und vergleichbaren Bewertungskriterien.

Die drei Oberkriterien, nach welchen die Authentifizierungsverfahren bewertet werden sollen, sind Sicherheit, Kosten und Benutzerfreundlichkeit. Da Sicherheit das Ziel von Authentifizierung ist, wird dieses Kriterium 50% der Bewertung ausmachen. Die anderen 50% bestehen aus Kosten mit 30% und Benutzerfreundlichkeit mit 20%, weil bei einem Unternehmen die Kosten eine große Rolle spielen und so der Benutzerfreundlichkeit übergeordnet sind (siehe Tabelle 1).

Tabelle 1: Oberkriterien der Nutzwertanalyse

	Sicherheit	**Kosten**	**Benutzerfreundlichkeit**
Zielgewichte	0,5	0,3	0,2
Berechnung	Siehe Tabelle 2	Siehe Tabelle 4	Siehe Tabelle 5

Das Kriterium Sicherheit soll bewerten, wie sicher ein Verfahren im Vergleich zu anderen Verfahren ist. Um die Bewertung durchzuführen, wird das Kriterium in die folgenden Unterkategorien eingeteilt. Das erste Unterkriterium ist der Aufwand in Zeit und Ressourcen, den ein Angreifender benötigt, um die Authentifizierung zu durchbrechen. Je höher der Aufwand, desto besser ist die Gesamtwertung. Beim zweiten Unterkriterium handelt es sich um die Einfachheit, mit der ein Angreifender durch Social Hacking, Shoulder Surfing oder Ausnutzen

anderer Benutzerfehler die Authentifizierung bestehen kann. Für die Bewertung von beiden Kriterien werden hier drei verschiedene Stufen gewählt (siehe Tabelle 3). Da das Unterkriterium „Aufwand Durchbruch“ einfacher zu messen ist als „Social Engineering“ macht es 60% der Kategorie Sicherheit aus (Siehe Tabelle 2).

Tabelle 2: Unterkriterium Sicherheit Gewichtung

	Aufwand Durchbruch	**Social Engineering**
Zielgewichte	0,6	0,4
Berechnung	Siehe Tabelle 3	Siehe Tabelle 3

Tabelle 3: Unterkriterium Sicherheit Beschreibung

Stufe	**Wert**	**Beschreibung Aufwand Durchbruch**	**Beschreibung Social Engineering**
Stufe 1	0	Das Verfahren ist fast gar nicht gegen Brute Force Attacken abgesichert, so dass man es mit herkömmlicher Rechenleistung per Brute Force überwinden könnte.	Benutzende notieren sich ihre Passwörter, da diese hochkompliziert sind. Zudem ist es einfach, Passwörter im Vorbeigehen abzulesen.
Stufe 2	50	Das Verfahren ist generell abgesichert. Es würde zwar lange dauern, ist aber noch realisierbar, es mithilfe von modernen Rechnern durch Brute Force zu überwinden.	Passwörter sind intuitiv genug, dass wenige Benutzende sich Notizen darüber machen und sonst nur an versteckten Orten. Es ist schwierig, das Passwort abzulesen.
Stufe 3	100	Das Verfahren ist sorgfältig gegen Brute Force Attacken geschützt und es würde Jahrhunderte dauern, es durch Brute Force mithilfe von aktuellen Rechenzentren zu überwinden.	Passwörter und Verfahren sind einfach genug, dass sich Benutzende keinerlei Notizen machen müssen. Am Arbeitsplatz befinden sich daher keine Hinweise für unautorisierte Personen.

Das Kriterium Kosten ist ein leicht nachvollziehbares Bewertungskriterium und wird daher nur in zwei Unterkriterien eingeteilt. Zum einen ist das die Höhe des erstmaligen Anschaffungspreises des Verfahrens, zum anderen handelt es sich um die laufenden Betriebskosten des Verfahrens pro Jahr. Je höher die Werte, desto positiver beeinflussen die Kosten die gesamte Nutzwertanalyse. Die Formeln zu Berechnung der Werte von 0 bis 100 sind so gewählt, da die Firma festgelegt hat, dass sie einmalig zu einem Maximalbetrag von 500.000€ bereit ist und pro Jahr maximal 50.000€ für Authentifizierung ausgeben möchte. Da die Versi AG langfristig plant, werden die jährlichen Betriebskosten mit 70% in die Bewertung einfließen. Der initiale Preis macht 30% aus, weil er nur einmalig zu zahlen ist (Siehe Tabelle 4).

Tabelle 4: Unterkriterium Kosten Gewichtung und Berechnung

	Anschaffungspreis	**Betriebskosten**
Zielgewichte	0,3	0,7
Berechnung	(500.000 – Preis) / 5.000	(50.000 – Preis pro Jahr) / 500

Benutzerfreundlichkeit oder Usability auf Englisch beschreibt, wie einfach und verständlich die Nutzenden des zu bewertenden Verfahrens mit diesem umgehen können und wie schnell sie eingearbeitet sind. Als Unterkriterien eignen sich daher der initiale Lernaufwand, der gering sein sollte und der benötigte Aufwand, das Verfahren täglich zu benutzen. Also wie schwierig es ist, sich die benötigten Informationen zu merken oder die benötigten physischen Gegenstände mit sich zu führen. Dabei spielt auch der Verwaltungsaufwand eine Rolle. In der Bewertung ist der tägliche Aufwand, der wiederholt eine Rolle spielt, wichtiger als der Initiale Lernaufwand, der für jeden User nur einmal aufzubringen ist (Siehe Tabelle 5).

Tabelle 5: Unterkriterium Benutzerfreundlichkeit Gewichtung

	Initialer Lernaufwand	**Täglicher Aufwand**
Zielgewichte	0,3	0,7
Berechnung	Siehe Tabelle 6	Siehe Tabelle 6

Tabelle 6: Unterkriterium Benutzerfreundlichkeit Beschreibung

Stufe	**Wert**	**Beschreibung Initialer Lernaufwand**	**Beschreibung Täglicher Aufwand**
Stufe 1	0	Das Verfahren ist komplex. Man benötigt einen langen Zeitraum, bis man es versteht und erfolgreich anwenden kann.	Die Mitarbeitenden müssen sich eine große und komplexe Menge von Informationen merken. Bzw. müssen sie komplexe Schritte ausführen und aufwendige Gegenstände mitbringen.
Stufe 2	50	Um das Verfahren anzuwenden und verstehen zu können, ist ein moderater Zeitaufwand notwendig.	Die Mitarbeitenden müssen in der Lage sein, sich moderat viele Informationen zu merken und etwas kompliziertere Schritte ausführen, damit das Verfahren funktioniert.
Stufe 3	100	Das Verfahren ist intuitiv und mit sehr geringem Aufwand verbunden, um es zu verstehen und anzuwenden.	Die Mitarbeitenden müssen sich nur sehr wenig merken und auch nichts Aufwendiges mitbringen. Der ganze Vorgang des Verfahrens ist verständlich und einfach.

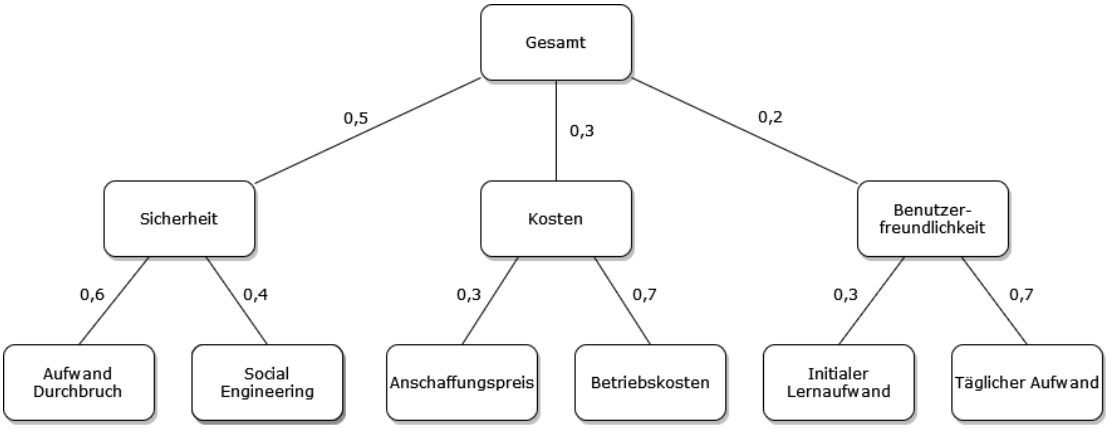

Abbildung 1: Übersicht und Gewichtung der Kriterien der Nutzwertanalyse

Um bestimmte Verfahren schon vor der Untersuchung auszuschließen, hat die Versi AG mehrere KO-Kriterien festgelegt. Die Kosten dürfen eine Summe von 500.000€ nicht überschreiten. Zudem darf keines der zu untersuchenden Authentifizierungsverfahren offensichtlich gegen das von Eckert [4] festgelegte Kriterium der biometrischen Authentifizierung „Fälschungssicherheit“ verstoßen. Des Weiteren muss das gesamte zur Authentifizierung benötigte Equipment in großer Menge erhältlich sein. Außerdem muss es kompakt und klein genug sein, um am Arbeitsplatz eines Mitarbeitenden nicht zu stören. Die letzte KO-Regel besagt, dass kein Authentifizierungsverfahren zu intrusiv sein darf. Das heißt, dass aus datenschutzrechtlichen Gründen keine Körperproben von Mitarbeitenden genommen werden dürfen.

4.2 Vorstellung und Eingrenzung möglicher Authentifizierungsverfahren

Im folgenden Abschnitt 4.3 werden verschiedene Authentifizierungsverfahren kurz vorgestellt und nach den oben beschriebenen Bewertungskriterien mit einer Nutzwertanalyse untersucht. Die vorzustellenden Verfahren sollen repräsentative oder interessante Verfahren der drei Kategorien der Authentifizierung sein. Dabei werden wissensbasierende, besitzbasierenden und biometrische Verfahren untersucht. Manche Verfahren lassen sich auch bereits ohne die Nutzwertanalyse ausschließen, da sie eindeutig gegen die von der Firma Versi definierten KO-Kriterien verstoßen. Der Vollständigkeit halber, werden diese Verfahren im Folgenden kurz dargestellt, obwohl sie für dieses Szenario von vornherein ausgeschlossen werden können.

Der Iris-Scan ist eines der genauesten Authentifizierungsverfahren mit geringen FAR und FRR. Dabei gleicht ein Scanner jedes Mal die Iris eines Benutzenden mit einer zuvor gespeicherten Aufnahme ab. Leider kann ein Scanner durch das Vorzeigen eines hochauflösenden Bildes getäuscht werden. Zudem ist ein solcher Scanner im Vergleich zu anderen Authentifizierungsverfahren deutlich teurer [12]. Damit verstößt das Verfahren gegen die KO-Regel, dass jede Authentifizierungsmethode nicht offensichtlich fälschbar sein darf und kommt somit für die Authentifizierung in der Firma nicht infrage.

Auch für einen anderen Teil des Auges, die Netzhaut, gibt es ein Authentifizierungsverfahren. Mit einem Scanner wird die Netzhautgeometrie analysiert und abgeglichen. Da die Netzhaut nicht immer sichtbar ist, wird sie mit einem Infrarotscanner sichtbar gemacht. Eine Netzhaut ist fast unmöglich zu fälschen. Bei kürzlich verstorbenen stirbt die Netzhaut zu schnell ab, als das man sie zum Authentifizieren benutzen könnte [13]. Im Gegensatz zu Iris-Scannern, die es schon einsatzbereit im Handel gibt, werden Retina-Scanner erst langsam im Handel verfügbar, da sie komplizierter und teurer sind [14]. Die Scanner können nicht in großer Menge eingekauft werden und verstoßen somit gegen die entsprechende KO-Regel.

Die Form und Geometrie der menschlichen Hand ist einzigartig und verändert sich selbst im Alter nicht mehr. Die Technologie, die Handgeometrie als Authentifizierungsverfahren verwendet, ist nicht für die Versi AG geeignet, da die einzelnen Scanner im Vergleich zu anderen Authentifizierungsverfahren größer und teurer sind [13]. Zudem ist es schwierig die

Technologie zu kaufen. Die folgende Quelle im Internet zeigt einen Typ von Handgeometrie Scanner, der zu einem Preis von 2.277$ pro Stück angeboten wurde und sehr sperrig war [15]. Das verstößt gegen die KO-Regel, die Geräte kompakt und klein zu halten. Des Weiteren ist der Preis hochgerechnet auf 10.000 Mitarbeitenden deutlich höher als das definierte Limit von 500.000€.

Bei der Stimmerkennung wird die Stimme zum einen nach der Stimmlage und zum anderen nach der Art des Sprechens analysiert. Stimmerkennung ist also eine Mischung aus verhaltensbasierter und angeborener Biometrie. Es wird dabei unterschieden, ob der Benutzer einen bestimmten Text sagen muss oder ob er frei sprechen darf [13]. Allerdings ist die Technologie teuer. Außerdem ist es möglich, das Verfahren durch vorher aufgenommene Audiodateien zu täuschen [12]. Auch dieses Verfahren verstößt gegen die KO-Regel der Fälschungssicherheit. Das macht es ungeeignet für die Versi AG.

Jeder Mensch hat einen einzigartigen primären Geruch, der nicht von Ernährung oder Pflegemitteln beeinflusst werden kann. Es ist möglich, den Geruch als Authentifizierungsverfahren zu verwenden. Es muss allerding noch viel geforscht und entwickelt werden, bis so ein Scanner kommerziell zu markgerechten Preisen angeboten wird [16]. Dadurch ist die Technologie noch nicht in großer Menge verfügbar und somit nicht für die Firma geeignet.

Eine weiteres Authentifizierungsverfahren ist das Abgleichen von DNA. Mittlerweile ist es möglich, DNA innerhalb von 10 Minuten zu prüfen. Allerdings wird dafür eine Blut-, Speichel- oder Haarprobe benötigt. Zudem ist das Testen teuer und wird daher wahrscheinlich erst einmal weiterhin nur von Behörden benutzt werden [13]. Die Voraussetzung einer Probe verstößt aus datenschutzrechtlichen Gründen gegen die entsprechende KO-Regel.

Eine weitere Methode der Authentifizierung sind Gehirnwellen. Es ist möglich, durch Sensoren die verschiedenen EEG-Wellen im Gehirn des Menschen zu lesen. Das Verfahren hat aber aktuell noch eine hohe FAR und FRR [17]. Es gibt EEG Headsets schon zu Preisen von 99 bis 1.000$. Allerdings versprechen diese nur Verbesserungen beim Lernen und bei Meditation und sind durch ihren Preis in ihrer Genauigkeit eingeschränkt. Genauere Geräte kosten von 1.000 bis zu 25.000$ und kommen für die Firma mit 10.000 Mitarbeitenden zu diesen Preisen aufgrund der KO-Regeln nicht in Frage [18].

4.3 Bewertung der Authentifizierungsverfahren

4.3.1 Aktuelle Authentifizierung in der Firma

Die Firma Versi hat für jeden Mitarbeitenden einen Benutzernamen, der sich aus Vor- und Nachnamen und gegebenenfalls einer Nummer, um Dopplungen zu vermeiden, zusammensetzt. Beim Erstellen eines neuen Benutzers bekommt der Mitarbeitende ein zufällig generiertes Passwort, welches aus Buchstaben, Ziffern und Zeichen besteht und eine Länge von Acht hat, zugewiesen. Das Passwort wird ihm oder ihr per E-Mail zugeschickt. Er oder sie hat dann später die Möglichkeit dieses zu ändern. Im Laufe der Zeit hat sich aber herausgestellt, dass die meisten Mitarbeitenden ihr Passwort gar nicht erst ändern und sich das 8-stellige Passwort notieren. Manche machen dies auf dem Handy, in einem Notizbuch oder aber im schlimmsten Fall sogar auf einem Notizzettel, den sie an ihren Monitor hängen. Andere Mitarbeitende ändern ihr Passwort oftmals zu etwas sehr Einfachem wie zum Beispiel ihrem Namen, einem Geburtstag oder sogar auch zu „Passwort“ um.

Das macht die Konten der Nutzenden nicht nur für Social Hacking und Shoulder Surfing sehr anfällig, viele Passwörter könnten auch durch Brute Force Angriffe, die nur nach Daten oder Wörtern im Duden suchen, geknackt werden. Beide Unterkategorien der Sicherheit gehören in die Stufe 1. Es müssen also dringend Lösungen oder Alternativen gefunden werden.

4.3.2 Authentifizierung durch Bilder – Erkennen

Ein interessantes Authentifizierungserfahren ist die Authentifizierung durch Bilder. Hierbei gibt es zwei verschiedenen Arten. Beim Erinnern, auch Recall auf Englisch, muss man sich Informationen direkt aus dem Gedächtnis rufen und sich mittels dieser authentifizieren. Zum Beispiel wird man aufgefordert, ein bestimmtes Muster zu malen oder verschiedenen Punkte auf einem Bild in einer bestimmten Reihenfolge anzuklicken. Beim Erkennen, Recognition auf Englisch, hat sich der Benutzende weniger zu merken, stattdessen bekommt er oder sie bei der Anmeldung meist eine Menge von Bildern, aus denen mehrere in einer bestimmten Reihenfolge auszuwählen sind [19].

Ein Beispiel eines Erkennungssystems ist Image Pass. Bei diesem handelt es sich um ein Authentifizierungsverfahren, bei dem ein Benutzender beim Erstellen seines Passwortes eine Auswahl von 30 Bildern bekommt. Diese Bilder sind gleich groß, stellen verschiedenen Motive dar und werden aus einer großen Menge von Bildern zufällig ausgewählt. Der Benutzende sucht sich dann fünf Bilder aus und platziert diese in einer Reihenfolge (siehe Abbildung 1), welche dann als Passwort zusammen mit sieben weiteren zufällig ausgewählten Bildern unter seinem Benutzernamen abgespeichert wird. Dasselbe Bild kann auch mehrmals verwendet werden. Zum Authentifizieren werden dem Benutzenden 12 Bilder gezeigt, daraufhin muss er oder sie die fünf vorab ausgewählten Bilder in der richtigen Reihenfolge anklicken [20].

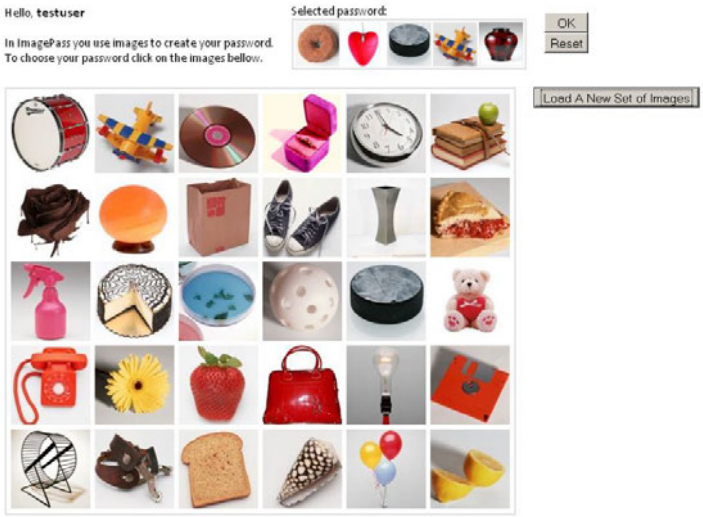

Abbildung 2: Image Pass Auswahl des Passworts
Quelle: [20]

Wenn man von einem Passwort der Länge fünf ausgeht und es 12 Bilder zur Auswahl gibt, existiert eine Menge von 12^5 = 248.832 verschiedenen Möglichkeiten von Passwörtern. Das richtige Passwort in fünf Versuchen herauszufinden ist sehr unwahrscheinlich. Um Brute Force Angriffe zu erschweren, werden den Bildern für die Authentifizierung zufällig gewählte IDs zugewiesen. Diese ändern sich nach fünf erfolglosen Authentifizierungsversuchen, so dass man die 12 verschieden IDs nicht mehrfach abfragen kann. Auf diese Weise werden auch Sniffer Attacken uneffektiver, da bei jeder Authentifizierung unterschiedliche IDs zwischen Benutzer

und Client hin und her geschickt werden. Außerdem ändert sich nach fünf Versuchen auch die Reihenfolge, in der die Bilder angezeigt werden. Dadurch sind physische Brute Force Attacken schwieriger, denn man kann nicht einfach immer dieselben Positionen abfragen [20].

Dieses Verfahren ist in die Sicherheitsstufe 2 einzuordnen, da es viele Vorkehrungen trifft. Trotzdem ist es möglich, beispielsweise eine KI zu trainieren, die 12 Bilder zu erkennen. Diese könnte durch physisches Klicken der Bilder die 248.832 Kombinationen ausprobieren und lösen. Solche Kombinationen lassen sich mittlerweile in weniger als einer Sekunde errechnen, wenn man davon ausgeht, dass ein guter Computer 170 Millionen Kombinationen pro Sekunde erstellen kann [21]. Damit diese Methode akzeptabel ist, muss das Auswahlfeld und die Anzahl der auszuwählenden Bilder erhöht werden. Bei einer Auswahl von 9x9, also 81 Bildern, und einer Auswahllänge von acht Bildern bräuchte ein Computer etwa 119 Tage. Wenn man die zusätzliche Rechenzeit der KI mit einbezieht, ist dies für heutige Verhältnisse eine akzeptable Zeit. Zusätzlich verringert sich auch die Stufe des anderen Sicherheitskriteriums Social Engineering. Denn während es noch intuitiv ist, fünf Bilder aus zwölf Bildern zu erkennen und anzuordnen, wird das bei acht aus 81 Bildern schon schwieriger, ist aber noch im Bereich des Möglichen. Außerdem ist das sogenannte Shoulder Surfing einfacher, denn es ist leichter sich zu merken, wie jemand mehrere Bilder auswählt, als die Tastatureingabe von einem textuellen Passwort nachzuvollziehen. Dieses Authentifizierungsverfahren ist also in Stufe 2 einzuordnen. Insgesamt beträgt der Wert für Sicherheit bei der Bildauthentifizierung – Erkennen also 50.

Der Preis dieses Verfahrens ist für ein Unternehmen in der Größe der Versi AG, das über eigene Programmierende verfügt, kein Problem. Im Zweifelsfall setzt die Firma eines ihrer Teams ein, um ein neues Authentifikationsverfahren zu entwickeln. Auch die Wartung und Instandhaltung des Programms können die hauseigenen Programmierenden übernehmen. Der Gesamtwert für die Kosten beträgt demnach 100.

Es ist erwiesen, dass es Menschen leichter fällt, große Mengen an bildlichen Daten zu erkennen, als sich lange Texte zu merken [22]. Das ist einer der Vorteile gegenüber traditionellen Passwörtern. Natürlich ist es etwas schwieriger, eine achtstellige Bildkombination zu erkennen als nur eine fünfstellige. Der „Tägliche Aufwand“ ist also nicht zu hoch und lässt sich der Stufe 2 zuordnen. Der „Initiale Lernaufwand“ ist allerdings klar Stufe 3 zuzuordnen, da man das

Prinzip hinter der bildbasierten Authentifizierung schnell und einfach verstehen kann. Außerdem ist es nicht kompliziert, sich ein solches Passwort einzurichten. Insgesamt hat das Oberziel Benutzerfreundlichkeit einen Wert von 0,3x100+0,7x50 = 65.

Tabelle 7: Bilder Erkennen Bewertungszusammenfassung

	Sicherheit	**Kosten**	**Benutzer-freundlichkeit**	**gesamt**
Zielgewichte	0,5	0,3	0,2	1
Werte	50	100	65	68

4.3.3 Authentifizierung durch Bilder – Erinnern

Der andere Typ von grafischen Passwörtern, ist das Recall Verfahren, auf Deutsch Erinnern. Recall lässt sich in zwei weitere Unterkategorien einteilen, nämlich zum einen das pure Recall Verfahren und zum anderen das cued Recall Verfahren, auf Deutsch Stichwort oder Hinweis. Beim puren Recall Verfahren muss ein Benutzender sich ohne jegliche Hinweise an ein Muster oder Symbol erinnern. Beim Passdoodle Verfahren zeichnet der Benutzer ein beliebiges Muster oder Symbol, welches er oder sie bei jeder Anmeldung wieder zeichnen muss [23].

Der Firma wird ein cued Recall Verfahren vorgeschlagen. Das ist ein Verfahren, bei dem der Benutzende sich zwar an eine Auswahl erinnern muss, es aber Hinweise gibt, die das Erinnern erleichtern [23].

Das Verfahren heißt PassPoint. Zum Beginn der Authentifizierung wird Passpoint ein beliebiges Bild übergeben, welches im besten Fall viele markante Merkmale hat. Um sich zu registrieren, klickt der Benutzende auf verschiedene Punkte im Bild. Diese Punkte werden in der angeklickten Reihenfolge gespeichert (siehe Abbildung 2). Wenn der Benutzende sich authentifizieren möchte, muss er die Punkte im Bild in derselben Reihenfolge erneut anklicken. Beim

Authentifizieren gibt es einen einstellbaren Bereich um den ausgewählten Bildpixel, in welchem der Klick noch akzeptiert wird [24].

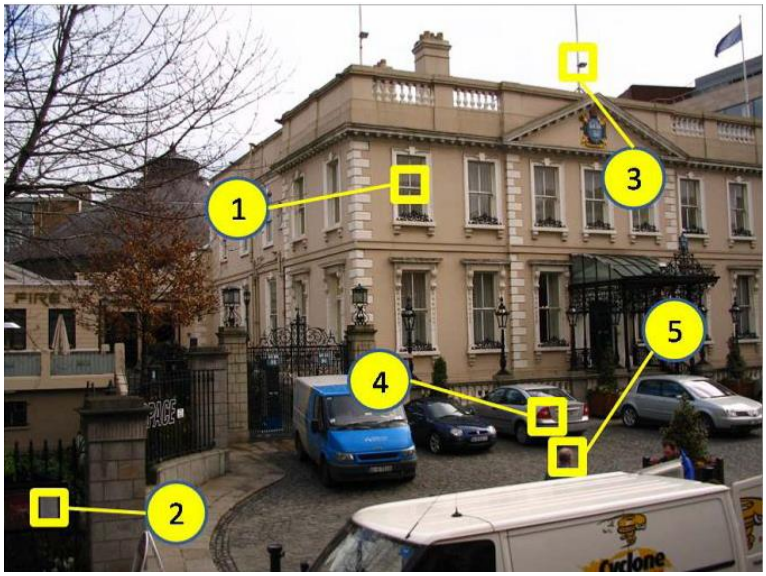

Abbildung 3: Ein Beispiel des Passpoint Verfahrens
Quelle: [23]

Um das Verfahren zu schützen, können die Passworteingaben nicht direkt gespeichert werden, sondern müssen gehasht werden. Dazu teilt PassPoint das Hintergrundbild in ein für den Benutzende unsichtbares Raster ein, dessen Felder groß genug für einen Klick und etwas Puffer sind. Damit der Benutzende seinen Passwortpunkt nicht zu nah an der Grenze zwischen zwei Feldern wählt, gibt es insgesamt drei Raster, die sich jeweils leicht überschneiden. Dadurch landet jeder Klick in mindestens einem Feld der drei Raster ungefähr in der Mitte des Feldes. Dieses Feld wird dann gehasht und abgespeichert. Beim Anmelden wird der Vorgang wiederholt, dabei werden die eingegebenen Werte werden mit den gespeicherten abgeglichen [24].

Für das erste Unterkriterium der Sicherheit „Aufwand Durchbruch“, kann man die Raumgröße der möglichen Passwörter errechnen und mit einem textuellen Passwort vergleichen. Wenn man ein Bild der Bildgröße von 640 x 480 Pixel benutzt und annimmt, dass jedes Feld im Raster 20 x 20 Pixel groß ist, dann gibt es 640x480/20x20 = 768 mögliche Felder. Bei einer Reihenfolge von sechs Punkten, die man auf dem Bild markieren muss, sind das $2{,}1 \times 10^{17} = 768^6$. Ein textuelles Passwort über alle Buchstaben, Ziffern und Zeichen mit einer Länge von

Acht wäre $95^8 = 6{,}6 \times 10^{15}$. Also gibt es mehr Passwort Kombinationen als bei textuellen Passwörtern. Wenn wir wieder von einer Geschwindigkeit von 180 Millionen Kombinationen pro Sekunde [21] ausgehen, würde es über 36 Jahre dauern, alle Kombinationen auszuprobieren. Das ist sicher genug für Stufe 3.

Shoulder Surfing ist leider auch hier noch ein Problem, denn der Benutzende hat bei der Anmeldung das Bild auf seinem Bildschirm. Während er auf die Punkte anklickt, könnte ihm jemand dabei zuschauen. Allerdings ist es schwieriger, sich Punkte in einem Bild innerhalb weniger Sekunden einzuprägen. Desweitern ist es für User mühsamer, sich Notizen zu ihren grafischen Passwörtern zu machen. Dafür müssten sie sechs Punkte auf einem Bild genaustens beschreiben. Dadurch ist PassPoint auf Stufe 2 der Unterkategorie Social Engineering einzuordnen. Insgesamt wird das Ziel Sicherheit mit der Punktzahl 100x0,6+50x0,4 = 80 bewertet.

Die Kosten sind auch bei PassPoint ähnlich wie schon bei Image Pass, da Passpoint keine extra Hardware benötigt und das Unternehmen hier die eignen Programmierer zum Entwickeln und Warten eines ähnlichen Programms einsetzen kann. Daher wird für das Ziel Kosten 100 eingetragen.

Der „Initiale Lernaufwand“ des Verfahrens ist in Stufe 2 einzuordnen, da - obwohl PassPoint leicht zu erklären ist - es eine komplette Umstellung für Mitarbeitende darstellt, die textuelle Passwörter gewöhnt sind. Der „Tägliche Aufwand“ gehört jedoch in die Stufe 3. Denn in einer Studie zum Vergleich zwischen Passpoint und alphanumerischen Passwörtern stellte sich heraus, dass es Unterschiede in der Anzahl der Fehlversuche nach jeweils einer, zwei und sechs Wochen zu Gunsten grafischer Passwörter gab [24]. Zudem ist es für das Gehirn des Menschen leichter, sich Bilder zu merken als Texte, da das Sehen der primäre Sinn bei vielen täglichen Aktivitäten in unserem Leben ist [22]. Nach einer Eingewöhnungsphase ist es also einfacher, sich ein grafisches Passwort zu merken. So beträgt die Gesamtwertung von PassPoint 87.

Tabelle 8: Bilder Erinnern Bewertungszusammenfassung

	Sicherheit	**Kosten**	**Benutzer-freundlichkeit**	**gesamt**
Zielgewichte	0,5	0,3	0,2	1
Werte	80	100	85	87

4.3.4 Alternative – sichere Passwörter

Das Problem, das die Versi AG mit ihrer aktuellen Authentifizierung hat, gibt es auch in vielen anderen Organisationen. Wird den Benutzenden die Freiheit gegeben, ihr eigenes Passwort zu wählen, erstellen sie oft schwache und leicht zu erratende Passwörter [25]. Aber das heißt nicht automatisch, dass textuelle Passwörter schlecht sind.

Eine weitere Lösungsidee ist es, die Mitarbeitenden des Unternehmens einen verpflichtenden Kurs über Passwortsicherheit absolvieren zu lassen und die Passworterstellung und -änderung einzuschränken.

Denn wenn man sicherstellt, dass jedes Passwort mindestens acht Zeichen enthalten muss, gibt es bei 95 Zeichen (Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen), $95^8 = 6{,}6 \times 10^{15}$ mögliche Kombinationen, wofür ein Rechner mit 180 Millionen Kombinationen pro Sekunde über ein Jahr bräuchte [21]. Dieser Zeitraum wird länger je länger das Passwort ist. Allerdings handelt es sich dabei lediglich um die Zeit, die der Computer braucht, um all möglichen Passwortkombinationen auszuprobieren. Wenn das Passwort zu einfach gewählt wurde, also zum Beispiel nur Kleinbuschstaben oder bestimmte Wörter aus dem Wörterbuch gewählt wurden, können es gezielte Brute Force Attacken und Wörterbuchangriffe immer noch entschlüsseln.

Das Ziel muss es also sein, den Benutzenden beizubringen, dass ihr Passwort nicht im Wörterbuch zu finden ist und im idealen Fall aus einer Mischung von Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen besteht. Zusätzlich sollte der Inhalt des Passwortes auch nicht direkt mit dem Benutzer verbunden sein wie zum Beispiel der Name eines Haustiers. Das

verringert die Wahrscheinlichkeit, dass das Passwort erraten werden kann [22]. Es bietet sich für die Firma an Regeln für das Erstellen des Passwortes festzulegen, die ein User einhalten muss, um ein valides Passwort zu erstellen. So müssen die Passwörter eine bestimmte Mindestlänge haben und mindestens drei der vier Zeichen Großbuchstaben, Kleinbuchstaben, Ziffer oder Sonderzeichen enthalten.

Damit Benutzende sich diese komplizierteren Passwörter auch merken können, gibt es verschiedene Lösungsversuche. Einer davon ist das Mnemonische Passwort. Bei diesem Prinzip denkt der User sich einen längeren Satz aus und benutzt den ersten Buchstaben jedes Wortes im Satz als Teil des Passworts. Beispielsweise wird der Satz „Der Geburtstag von Peter und Laura ist am 7. Januar“ dann zu „DGvP&Lia7J“ verdichtet. Solche Passwörter sind sicher, aber trotzdem einfach zu merken. Erst bei mehreren Passwörtern dieser Art wird es schwieriger, sich diese ins Gedächtnis zu rufen [26].

Dadurch, dass den Mitarbeitenden durch die Teilnahme am Kurs im Idealfall die Relevanz von sicheren Passwörtern bewusst gemacht wurde und sie nun sichere mnemonische Passwörter benutzen, die die Regeln von Mindestlänge und Zeichenwahl einhalten, erreichen beide Unterkategorien des Ziels Sicherheit die Stufe 3.

Der Preis eines solchen Kurses über Passwortsicherheit lässt sich im Internet pro Mitarbeiter schon ab 7€ finden. Eine Manager Lizenz kostet 29€ pro Monat. Mit dieser kann ein Manager beliebig vielen Benutzenden Kurse zuweisen und deren Ergebnisse einsehen [27]. Der Initialpreis ist kostenlos, aber im Jahr fallen 348€ für die Manager Lizenz an. Das entspricht (50.000-348) / 500 = 99,3 Punkten in der Kategorie der jährlichen Kosten und 100 Punkten für die einmaligen Kosten. Insgesamt lassen sich die Kosten also auf 99 Punkten runden.

Dadurch, dass die Mitarbeitenden den Kurs erst absolvieren müssen, und nicht jeder Absolvent des Kurses die gelernten Dinge auch anwenden wird, ist der „Initiale Lernaufwand“ auf Stufe 2 einzuschätzen. Der „Tägliche Aufwand“ für die Mitarbeitenden ist nicht allzu hoch, da sie sich nur eine Phrase einprägen müssen. Da das Einprägen von Passwörtern aber eines der Hauptprobleme der Mitarbeitenden beim aktuellen Authentifizierungserfahren in der Firma ist, wird der „Tägliche Aufwand“ in Stufe 2 eingruppiert.

Tabelle 9: Passwort Bewertungszusammenfassung

	Sicherheit	**Kosten**	**Benutzer-freundlichkeit**	**gesamt**
Zielgewichte	0,5	0,3	0,2	1
Werte	100	99	50	90

4.3.5 Tippverhalten

Das Tippverhalten ist ein biometrisches Authentifizierungsverfahren und zählt zum Typ der verhaltensbasierten biometrischen Verfahren. Beim Tippverhalten wird die einmalige Art, wie ein User seine Tastatur betätigt, analysiert, damit er so identifiziert und authentifiziert werden kann. Dabei ist es nicht wichtig, ob der User das Zehnfingersystem beherrscht oder nur mit zwei Fingern schreibt [13]. Das funktioniert, indem die Zeit zwischen dem Drücken und Loslassen einer Taste, dem Gedrückt halten einer Taste sowie die Pause zwischen dem Drücken einer neuen Taste gemessen und gespeichert wird. Die Authentifizierung durch Tippverhalten kann in zwei Bereiche aufgeteilt werden. Zum einen statisch bzw. strukturierter Text und zum anderen dynamisch bzw. freier Text. Beim statischen Tippverhalten wird eine oder mehrere Phrasen Text analysiert, während beim dynamischen Tippverhalten die Tastatureingaben vom User über eine längere Zeit überwacht werden [28]. Für die Zwecke der Versi AG reicht das statische Tippverhalten, da das Verfahren lediglich zur Anmeldung eingesetzt werden soll. Durch Eingabe einer kurzen Phrase sollen sich die Mitarbeitenden anmelden können. Die beim Registrieren erfassten Daten werden dann einem neuronalen Netz zur Klassifizierung und Speicherung übergeben. Dieses wurde vorher mit einer Menge an Texten von verschiedenen Menschen trainiert, um zu lernen, verschiedene Benutzende zu unterscheiden. Ein solches Verfahren wird „Multi-class classifcation“ genannt. Der andere Ansatz, auch „Anomaly detection“ genannt, besteht daraus, ein Modell mit Tippdaten von nur einem Benutzenden zu trainieren, um den einen Benutzenden mit hoher Genauigkeit identifizieren zu können. Allerdings muss für jeden Benutzenden ein eigenes neuronales Netz trainiert werden. Zudem muss die

betroffene Person viele Repetitionen des Textes tippen, um genug Trainingsdaten zu erstellen [29]. Der Aufwand ist also vergleichsweise hoch.

Da die Authentifizierungsdaten aus einer großen Menge an Messungswerten bestehen, die miteinander verrechnet und verglichen werden, ist es unwahrscheinlich, dass man per Brute Force authentifiziert werden kann. Der Angreifer müsste verschiedene Sätze und Phrasen wiederholt mit minimalen Werteveränderungen prüfen lassen. Deshalb ist das Sicherheitskriterium „Aufwand Durchbruch“ Stufe 3.

Das Sicherheitskriterium „Social Engineering“ wird ebenfalls der Stufe 3 zugeordnet. Shoulder Surfing ist fast unmöglich, denn die Phrase, die der Benutzer eingibt, ist unwichtig. Das Tippverhalten eines anderen Menschen zu beobachten, ist extrem schwierig. Auch Notizen für die Authentifizierung, die Benutzer sich eventuell machen, sind überflüssig, da Tippverhalten eine biometrische Eigenschaft ist und sich daher nicht gemerkt werden muss. Außerdem hat Tippverhalten wie jedes Biometrisches Authentifizierungsverfahren eine False Acceptance Rate (FAR) und eine False Rejection Rate (FRR). Ein bereits im Jahr 2012 erschienener Artikel, in welchem Forschungsergebnisse zum Tippverhalten als Authentifizierung analysiert wurden, zeigt, dass die meisten Ausführungen von Tippverhaltensauthentifizierung eine geringe FAR und FRR erreichen [28].

Der Preis für Tippverhalten ist in Vergleich zu anderen biometrischen Authentifizierungsverfahren günstiger, da man keine zusätzliche Hardware benötigt, weil die Software auch auf einer herkömmlichen Tastatur funktioniert [13]. Eine Internetrecherche hat ergeben, dass bereits Softwarelösungen für unbegrenzte User mit bis zu 1.000 Authentifizierungen per Benutzende für 100$ monatlich angeboten werden [30]. Also 1.200$ oder 1.025€ im Jahr. Einen initialen Preis gibt es nicht. Damit kommen wir für das Ziel Preis auf einen Wert von 98.

Eine Studie von 2004 [31] zeigt, dass es mehrere Tippverhaltens Systeme gibt, die zur Authentifizierung eines Benutzers unter zehn Wörter Benutzereingabe brauchen und trotzdem ausreichende Sicherheit haben. Des Weiteren stellt eine Arbeit, die die Benutzerfreundlichkeit von biometrischer Authentifizierung am Arbeitsplatz untersucht [32], fest, dass Spracherkennung, Fingerabdruckauthentifizierung und mehre andere Authentifizierungsverfahren im Vergleich zu Authentifizierung durch Tippverhalten schwieriger zu benutzen sind. Initial muss man, damit das Tippverhalten analysiert werden kann, meist mehrere Zeilen Text schreiben. Daher ist

der initiale Lernaufwand auf Stufe 2 einzuschätzen. Der tägliche Aufwand gehört jedoch in die Stufe 3, weil sich der Benutzende nichts merken muss und außer seinen Händen nichts mit sich führen muss. Zudem ist der Text, der zu Anmeldung eingegeben wird, mittlerweile kurz genug, so dass er sich im Aufwand fast nicht von einem längeren textuellen Passwort unterscheidet. Ein Softwareanbieter stellt zum Beispiel eine Lösung bereit, die vier kurze Wörter zu Authentifizierung eines Benutzernden benötigt [33]. Insgesamt wird die Tippverhalten Authentifizierung mit 96 Punkten bewertet.

Tabelle 10: Tippverhalten Bewertungszusammenfassung

	Sicherheit	**Kosten**	**Benutzer-freundlichkeit**	**gesamt**
Zielgewichte	0,5	0,3	0,2	1
Werte	100	98	85	96

4.3.6 Fingerabdruck

Der Fingerabdruck ist eines der ältesten Authentifizierungsverfahren der Welt. Bereits im antiken China 7000 bis 6000 vor Christus, wurden Dokumente mit Lehmsiegeln mit dem Fingerabdruck des Absenders signiert. Doch zur Authentifizierung wurden sie bewiesenermaßen erst benutzt, nachdem Mitte des 19. Jahrhunderts durch Studien festgestellt wurde, dass Fingerabdruckmuster ein Leben lang unverändert bleiben und es keine zwei identischen Fingerabdrücke gibt [34].

Fingerabdrücke bestehen aus verschiedenen Senkungen und Erhöhungen in der Haut der Fingerkuppe. Dadurch bildet sich ein komplexes Muster von Kanälen. Zur Authentifizierung und Identifikation werden sogenannte Minuzien betrachtet. Dabei handelt es sich um die vielen verschiedenen Endungen und Verzweigungen in den Rillen der Fingerkuppe. Fingerabdruckscanner extrahieren durch verschieden Algorithmen die Minuzien aus dem gescannten Fingerabdruck (siehe Abbildung 3). Diese werden dann unter einem Benutzenden in einer Datenbank

gespeichert. Bei jeder Authentifizierung werden die Minuzien wieder extrahiert und mit dem in der Datenbank gespeicherten Profil abgeglichen [35].

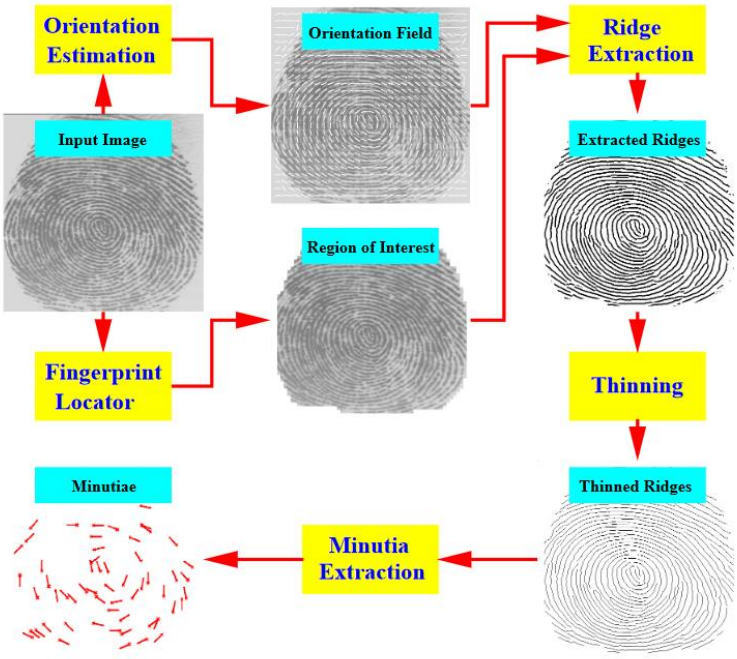

Abbildung 4: Extrahieren der Minuzien aus dem Fingerabdruck
Quelle: [35]

In der Unterkategorie „Aufwand Durchbruch“ schneidet das Fingerabdruck Verfahren gut ab. Biometrische Authentifizierungsverfahren sind weniger anfällig für Brute Force Attacken oder Wörterbuchangriffe als Passwort basierte Verfahren [36]. Daher ist das Verfahren in Stufe 3 einzugruppieren. In der Unterkategorie „Social Engineering“ erreicht das Verfahren nur die Stufe 2. Denn während Fingerabdrücke einzigartig sind, so hinterlassen Menschen Fingerabdrücke überall. Dadurch ist es möglich, eine Kopie eines Fingerabdruckes zu machen und den Scanner damit auszutricksen [12]. Dazu muss man jedoch erst einmal den richtigen Fingerabdruck eines Benutzers identifizieren und ihn dann von einer Oberfläche extrahieren.

Im Vergleich zu anderen biometrischen Verfahren ist das Fingerabdruckverfahren heutzutage weit verbreitet und daher auch günstiger. Beim Internethändler Amazon kann man Scanner bereits zum Preis von 28,21€ erwerben [37]. Werden diese für alle 10.000 Mitarbeitenden der

Versi AG angeschafft, entspricht das einem Initialpreis von 282.100€. Der Initialpreis bekommt daher einen Wert von (500000-282100) / 5000 = 44. Der Wert für die jährlichen Kosten beträgt 100, da - sobald die Geräte da sind - höchstens von Zeit zu Zeit defekte Geräte ersetzt werden müssen. Die Gesamtwertung der Kosten liegt also bei 83.

Die Benutzerfreundlichkeit des Fingerabdruckverfahrens ist hauptsächlich positiv, da die Benutzenden keine Informationen kennen oder Gegenstände mit sich führen müssen. Es ist lediglich erforderlich, den ausgewählten Finger unverletzt zu halten. Damit ist der „Tägliche Aufwand“ auf Stufe 3 einzuschätzen. Ein Nachteil dieses Verfahrens ist, dass Mitarbeitende aufgrund des Datenschutzgesetzes nicht verpflichtet sind, ihren Fingerabdruck speichern zu lassen. Sollte die Firma dies dennoch tun, kann gegen sie geklagt werden [38]. Das senkt den Initialen Lernaufwand auf Stufe 2. Die Benutzerfreundlichkeit wird also mit 85 Punkten bewertet. Die Gesamtwertung liegt gerundet bei 82 Punkten.

Tabelle 11: Fingerabdruck Bewertungszusammenfassung

	Sicherheit	**Kosten**	**Benutzer-freundlichkeit**	**gesamt**
Zielgewichte	0,5	0,3	0,2	1
Werte	80	83	85	82

4.3.7 Smart Card

Smart Cards sind Plastik Karten mit einem eingebauten Chip, der einen eigenen Mikroprozessor und Speicher besitzt. Sie können dazu benutzt werden, die Identität eines Nutzers zu bestätigen und zählen damit zur Kategorie der Authentifizierung durch Besitz. Der Chip ist in der Lage, kryptografische Schlüssel zu speichern und zu präsentieren. Dazu muss die Karte mit einem Kartenlesegerät und einer dazugehörigen Software gelesen werden. Außerdem können mit dem gespeicherten Schlüsseln Informationen signiert oder verschlüsselt über das Internet verschickt werden. Zusätzlich können Smart Cards auch benutzt werden, um Schlösser zu

öffnen und Arbeitszeiten zu registrieren. Daher ist der Einsatz von Smart Cards eine gängige Methode der Authentifizierung bei vielen Firmen [39] [40].

Für die Unterkategorie „Social Engineering“ erreicht das Authentifizierungsverfahren Smart Card die Stufe 3. Denn ohne in ein Kartenlesegerät gesteckt zu werden, sind die Kontakte des Chips in der Karte nicht mit Strom versorgt, so dass die Karte keine Informationen preisgeben kann. Das heißt, dass Angreifer ohne direkten Zugriff auf die Karte nichts ausrichten können [40]. Auch in der Kategorie „Aufwand Durchbruch“ ist dieses Verfahren der Stufe 3 zuzuordnen, da es schwierig ist, ohne Zugriff auf einen Schlüssel abgefangene Informationen zu entschlüsseln. Die Gesamtbewertung der Chip Karte beträgt somit 100.

Beim Preis ist diese Authentifizierung schon kostspieliger. Ein Kartenlesegerät kostet beim Internethändler Amazon 14,50€ [41], während 100 Smart Access Cards für 46,90€ angeboten werden [42]. Ein Kartendrucker kostet ungefähr 1.000€ und bedruckt jede Karte für 36 Cent in Farbe [43]. Insgesamt ergibt sich daraus für 10.000 Mitarbeitende eine Summe von 154.290€, wenn man davon ausgeht, dass jede Person eine solche Karte erhält. Dies führt zu einer Wertung in der Unterkategorie „Initialpreis“ von (500000-154290) / 5000 = 69 Punkten. Der Preis pro Jahr erhält eine Bewertung von 100, da selbst bei 100 neuen Mitarbeitenden pro Jahr die voraussichtlichen Kosten von 100€ nicht überschreiten werden. Die Kosten bekommen also einen Gesamtwert von 91.

Für das Oberziel Benutzerfreundlichkeit wird das Authentifizierungsverfahren Smart Card auf Stufe 2 in beiden Unterkategorien eingeschätzt, denn jeder Benutzende muss zusätzlich ein Kartenlesegerät am Arbeitsplatz haben und darf die Karte nicht verlieren. Trotzdem ist die Bedienung des Authentifizierungsverfahrens eher einfach. Der Wert für Benutzerfreundlichkeit liegt also bei 50 Punkten. Der Gesamtwert der Chip Karte beträgt 87 Punkte.

Tabelle 12: Smart Card Bewertungszusammenfassung

	Sicherheit	**Kosten**	**Benutzer-freundlichkeit**	**gesamt**
Zielgewichte	0,5	0,3	0,2	1
Werte	100	91	50	87

4.3.8 Gesichtserkennung

Gesichtserkennung ist ein biometrisches Verfahren, welches die Gesichtsgeometrie analysiert, um einen Benutzenden zu identifizieren. Gesichtserkennung ist weit verbreitet und bereits vielerorts im Einsatz, um Terroristen und andere Kriminelle zu identifizieren. Das Verfahren kann Probleme bei veränderter Beleuchtung, anderer Gesichtsbehaarung und Brillen haben. Es ist ein bezahlbares Verfahren, weil lediglich eine Kamera sowie die passende Software benötigt werden [44].

Da auch dieses biometrische Verfahren nicht aus einem deterministischen Passwortbereich besteht, sondern aus komplexen Gesichtsdaten, ist das Verfahren in Stufe 3 des „Aufwand Durchbruch“ einzuordnen. Für der Kategorie „Social Engineering“ erhält es die Stufe 2. Denn obwohl die Gesichtserkennung eines der am weitesten verbreiteten biometrischen Verfahren ist, gelang es bereits, Gesichtserkennung durch Deepfakes zu täuschen [45]. Der Gesamtscore des Ziel Sicherheit ist also 80.

Um das Verfahren in der Firma einführen zu können, müsste jedem Benutzenden eine Webcam zu Verfügung gestellt werden. Die Software für Gesichtskennung ist als Open Source verfügbar und verursacht daher keine zusätzlichen Kosten. Anpassung und Installation der Technologie können die internen Informatiker der Versi AG durchführen. Eine Webcam kostet bei einem Onlinehändler 33,99€ [46]. Für 10.000 Mitarbeitenden liegt der Gesamtpreis bei 339.900€, was einer Bewertung des Anschaffungspreises von (500000-339900) / 5000 = 32 Punkten entspricht. Mit dem Preis pro Jahr in Stufe 3 bei 100 Punkten beträgt die Bewertung des Ziel Preis 80 Punkte.

Die Benutzerfreundlichkeit des Verfahrens ist sehr hoch, da Gesichtserkennung nicht lange dauert und intuitiv zu benutzen ist. Beide Unterkategorien des Ziels Benutzerfreundlichkeit werden also in Stufe 3 eingruppiert. Sie erhalten eine Wertung von 100 Punkten. Damit beträgt die Gesamtwertung 84 Punkte.

Tabelle 13: Gesichtserkennung Bewertungszusammenfassung

	Sicherheit	**Kosten**	**Benutzer-freundlichkeit**	**gesamt**
Zielgewichte	0,5	0,3	0,2	1
Werte	80	80	100	84

4.3.9 Phone as a Token

Laut einer Statistik der Firma Statista betrug die Anzahl der Smartphone Besitzer im Jahr 2020 in Deutschland rund 60,7 Millionen. In der Altersgruppe der 14- bis 49-Jährigen gab es bereits einen Smartphone Nutzeranteil von 95 Prozent [47]. Bei einer so großen Menge an Smartphone-Nutzern, bietet es sich an, ein Authentifizierungsverfahren mithilfe des Handys einsetzten. Ein solches ist „Phone as a Token“.

Bei dem Verfahren gibt es mehrere Möglichkeiten. Für die Versi AG wird die beliebteste Methode vorgestellt. Es handelt sich dabei um das One-Time-Password auch OTP genannt [48]. Bei dieser Methode benötigt der Benutzende einen Computer und ein Handy mit einer SIM-Karte. Er oder sie meldet sich an, indem ein Benutzername eingetippt wird. Dadurch wird eine Anfrage an einen Authentifizierungsserver (AS) geschickt. Dieser muss mit dem Global System for Mobile Communications (GSM) verbunden sein. Der AS schickt dann ein einmaliges Passwort an die unter dem Nutzernamen gespeicherte Telefonnummer. Das OTP ist computergeneriert und besteht meistens aus einer Anordnung zufälliger Zahlen und Buchstaben. Der Nutzende kann das Passwort auf dem Handy lesen und manuell in den Computer eingeben. Sollten Computer und Handy Bluetooth besitzen kann dieser Schritt auch automatisch erfolgen. Daraufhin sendet der Computer das Passwort zurück an den AS und der AS authentifiziert den Benutzenden [49] (siehe Abbildung 4).

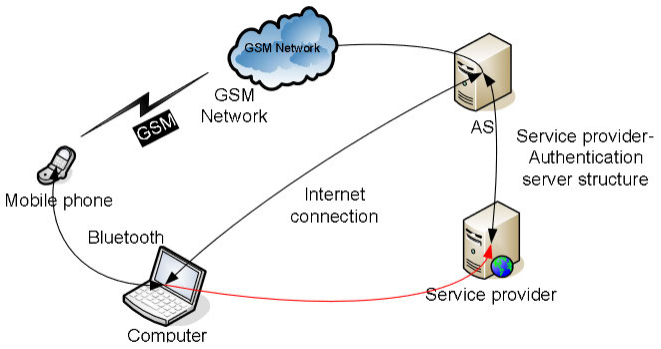

Abbildung 5: OTP Authentifizierungskreis Quelle: [49]

Das One-Time-Password ist, wie der Name schon sagt, ein Passwort, das genau einmal verwendet wird und danach unbrauchbar ist. Es wird vom AS zufällig generiert und hat deshalb nicht die Schwäche, die ein von Menschen ausgewähltes Passwort haben kann. Dadurch erhält das Authentifizierungsverfahren die Stufe 3 in der Unterkategorie „Aufwand Durchbruch“. Für die Unterkategorie „Social Engineering“ wird dem Verfahren die Stufe 2 zugewiesen. Denn dadurch, dass die Authentifizierung innerhalb einer kurzen Zeitspanne erfolgt und das OTP jedes Mal ein anderes ist, macht sich ein Benutzender keine Notizen zum Passwort. Auch durch Shoulder Surfing sind keine wichtigen Informationen zu gewinnen. Abgesehen davon, dem Benutzenden das Handy zu stehlen, gibt es also wenig Möglichkeiten für Social Engineering. Trotzdem könnte es passieren, dass ein Angreifer das Handy eines Benutzernden abfängt oder es schafft, eine neue SIM-Karte zu beantragen. Dadurch kann er Zugriff auf das OTP erhalten. Endgültig erreicht das Ziel Sicherheit einen Wert von 80 Punkten.

Obwohl fast jede Person zumindest ein Handy mit SIM-Karte besitzt, kann die Firma von ihren Mitarbeitenden nicht verlangen, ihr privates Mobiltelefon für Firmenzwecke zu verwenden. Der Arbeitgeber ist verpflichtet, alle für die Arbeit benötigte Mittel bereitzustellen [50]. Das bedeutet, dass jeden Mitarbeitenden ein Diensthandy eingekauft werden muss. Damit ein Mitarbeiter das „Phone as a Token“-Verfahren benutzen kann, reicht ein einfaches Tastenhandy für ca. 20€ mit zusätzlich einer Prepaid SIM-Karte für 10€ zum Empfangen von SMS. Natürlich ist ein solches Mobiltelefon mit der Verbreitung von Smartphones nicht mehr zeitgemäß.

Für die Versi AG stellt sich daher die Frage, ob es Sinn machen könnte, aktuelle Firmenhandys auf breiter Front im Unternehmen einzusetzen. Da dann solche Firmenhandys nicht ausschließlich zur Authentifizierung eingesetzt würden, würden sie auch nicht unter das Budget der Aktualisierung des Authentifizierungssystems fallen. Für das „Phone as a Token"-Verfahren reichen in der einfachen Variante 30€ pro Mitarbeitenden. Das wären 300.000€ und für die Unterkategorie „Anschaffungspreis" (500.000-300.000) /5.000 = 40 Punkte. Zusätzlich muss die Versi AG nur dafür sorgen, dass der Authentifizierungsserver in der Lage ist, SMS zu versenden und es ein System zur Authentifizierung gibt. Dazu kann das bestehende Authentifizierungssystem von den internen Informatikern und Technikern angepasst werden. Zudem muss die Versi AG eine SMS-Flatrate kaufen, mit der SMS unbegrenzt in alle Netzte geschickt werden können. Die Firma DeutschlandSIM bietet eine solche Flatrate beispielsweise ab 9,99€ im Monat an [51]. Das wären 119,88€ pro Jahr. Da diese Kosten noch unter 500€ liegen, werden die jährlichen Kosten immer noch mit 100 Punkten bewertet. Das Ziel Kosten erreicht also insgesamt 82 Punkte.

Da die Benutzenden ein zusätzliches Firmenhandy mit sich führen müssen, entsteht ein erhöhter Transportbedarf. So ist die Unterkategorie „Täglicher Aufwand" der Stufe 2 zuzuordnen. Die Mitarbeitenden müssen sich keine weiteren Informationen merken. Zudem ist der Vorgang der Authentifizierung simpel und dauert meist weniger als ein paar Minuten. Der „Initiale Lernaufwand" liegt also in Stufe 3. Der Benutzerfreundlichkeit dieses Authentifizierungsverfahrens wird ein Wert von 65 Punkten zugeteilt. Der Gesamtwert des Verfahrens beläuft ich daher auf 78 Punkte.

Tabelle 14: Phone as Token Bewertungszusammenfassung

	Sicherheit	**Kosten**	**Benutzer-freundlichkeit**	**gesamt**
Zielgewichte	0,5	0,3	0,2	1
Werte	80	82	65	78

5 Evaluation

5.1 Vergleich mit dem alten Verfahren der Firma

Im vorangegangenen Kapitel wurden mehrere Authentifizierungsverfahren vorgestellt und mithilfe einer Nutzwertanalyse einzeln analysiert. Zudem wurde die Situation der Firma Versi AG erläutert und ihre aktuelles Authentifizierungsverfahren beschrieben. In diesem Kapitel sollen die einzelnen Verfahren gegenübergestellt und die Ergebnisse des Vergleichs gezeigt werden.

Tabelle 15: Vergleich der Authentifizierungsverfahren

Authentifizierungsverfahren	**Kategorie**	**Bewertung**
Grafisches Passwort – Erkennen	Wissen	68
Grafisches Passwort – Erinnern	Wissen	87
Textuelles Passwort – Alternative	Wissen	90
Phone as a Token	Besitz	78
Smart Card	Besitz	87
Fingerabdruck	Biometrie	82
Gesichtserkennung	Biometrie	84
Tippverhaltensanalyse	Biometrie	96

Das Verfahren, das sich am besten für die Versi AG eignet, ist das biometrische Authentifizierungsverfahren Tippverhaltensanalyse mit einer Gesamtbewertung von 96. Mit einem Score von 90 ist das Authentifizierungsverfahren Textuelles Passwort, das Verfahren, das am zweit besten zur Firma Versi passt. Den ersten Platz der Kategorie Besitz belegt das Verfahren Smart Card mit einem Score von 87. Am schlechtesten hat das besitzbasierte Verfahren „Phone as a Token“ mit einem Score von 78 abgeschnitten. Nun könnte man annehmen, dass die Firma

offensichtlich die Tippverhaltensanalyse implementieren sollte. Doch dabei handelt es sich lediglich um eine Ein-Faktor-Authentifizierung. Eine Zwei-Faktor-Authentifizierung ist deutlich sicherer [52].

5.2 Festlegen eines neuen Verfahrens

Zwei-Faktor-Authentifizierung (2FA) erweitert die normale Authentifizierung um einen weiteren Faktor. Zum Beispiel muss ein User sich bei einer 2FA nicht nur mit seinem Benutzernamen und Passwort anmelden, sondern lässt sich zusätzlich noch mit seinem Fingerabdruck authentifizieren. Wichtig dabei ist, dass die zwei Faktoren aus verschiedenen Kategorien der Authentifizierungsverfahren Wissen, Besitz oder Biometrie stammen. 2FA ist um ein Vielfaches sicherer als die Ein-Faktor-Authentifizierung und wird daher vom Bundesamt für Sicherheit in der Informationstechnik empfohlen [6].

Da die 2FA eine Kombination aus zwei verschiedenen Kategorien der Authentifizierung ist, bietet es sich für die Versi AG an, aus jeder der drei Kategorien, das Authentifizierungsverfahren mit der besten Bewertung zu wählen. Also die Tippverhaltensanalyse aus der Biometrie, das Smart Card Verfahren aus der Kategorie Besitz und das textuelle Passwort Verfahren aus der Kategorie Wissen. Für die 2FA sind dann drei verschiedene Kombinationen möglich.

Bei der ersten Möglichkeit muss ein Benutzender, nachdem er oder sie einen Benutzernamen eingegeben hat, wie auch schon vorher bei der Versi AG praktiziert ein Passwort eingeben. Dieses sollte aber anders als vorher den in der Bewertung der Authentifizierungsverfahren spezifizierten Anforderungen entsprechen. Im zweiten Schritt muss der Benutzende eine Smart Card durch das mit dem Computer verbundenen Kartenlesegerät ziehen. Danach ist er oder sie erfolgreich authentifiziert.

Die zweite Möglichkeit ähnelt der ersten. Anstelle von einem Passwort wird der User jetzt aufgefordert vier kurze Wörter einzugeben, die dann durch die Tipperhaltensanalyse verifiziert werden. Nach dem Verwenden der Smart Card ist auch hier der Benutzende authentifiziert.

Die finale Möglich kombiniert das textuelle Passwort und die Tippverhaltensanalyse. Da beide Verfahren Texteingaben erfordern, bietet es sich an, den Benutzenden nur einmal Text

eingeben zu lassen. Während der Benutzende Benutzername und Passwort eingibt, wird gleichzeitig das Tippverhalten aufgenommen und verifiziert. Stimmen die Eingabedaten des Benutzenden und die Art der Eingabe mit den abgespeicherten Daten überein, ist der Benutzende erfolgreich authentifiziert.

Die dritte Möglichkeit hat sichtbare Vorteile gegenüber den ersten beiden Kombinationen. Nicht nur muss der Benutzende keinerlei Besitztümer mit sich führen, um sich anzumelden, er oder sie kann sich außerdem um einiges schneller anmelden. Dadurch wird die die Benutzerfreundlichkeit erheblich erhöht. Diese 2FA ähnelt in ihrer Benutzerfreundlichkeit einer Ein-Faktor-Authentifizierung. Für die Authentifizierung der Benutzenden der Versi AG eignet sich also eine Zwei-Faktor-Authentifizierung mit den Faktoren Tippverhaltensanalyse und textuellem Passwort am besten.

Natürlich gibt es auch Authentifizierungsverfahren mit mehr als zwei Faktoren, die sogenannte Multi-Faktor-Authentifizierung. Doch mit jedem weiteren Faktor wird das Authentisieren eines Nutzenden tendenziell teurer und komplizierter. [6]. Außerdem wird der Zeitaufwand, den der Benutzende zum Anmelden braucht, erhöht und er oder sie müsste sich mit einem weiteren Verfahren vertraut machen. Aufgrund ihrer Mitarbeitenden, die sich nicht gerne komplexere Passwörter ausdenken und benutzen, hat sich die Versi AG gegen drei oder mehr Faktoren bei der Authentifizierung entschieden.

5.3 Aufwand und Kosten des Wechsels der Verfahren

Nachdem das passende Authentifizierungsverfahren für die Versi AG gefunden wurde, wird nun kurz beschrieben, wie sich die Umstellung auf die Firma finanziell auswirkt und welche technischen Voraussetzungen für die Integration des Verfahrens erfüllt werden müssen.

Für die Tippverhaltensanalyse gibt es bereits eine Kosteneinschätzung. 1.025€ pro Jahr würde dieses Verfahren bei dem externen Anbieter TM3 Software GmbH mit der Software KeyTrac kosten. Das bestehende Authentifizierungssystem, welches zuvor die Authentizität eines Benutzenden mittels Benutzername und Passwort geprüft hat, muss dementsprechend von den hauseigenen Informatikern und Technikern angepasst werden. Zudem wird ein Kurs über

Passwortsicherheit eingekauft, der für alle Mitarbeitenden verpflichtend ist. Für eine Manager Lizenz eines solchen Kurses betragen die jährlichen Kosten der Versi AG 348€. Insgesamt summieren sich die Kosten für die Firma pro Jahr auf 1.373€.

Die Versi AG hat bislang zum Authentifizieren der Mitarbeiter die Lösung von Microsoft „Active Directory“ eingesetzt und möchte diese auch weiterhin ergänzt durch 2FA verwenden. Da „Active Directory“ keine Authentifizierungsmethode zum Authentifizieren durch Tippverhalten anbietet, muss das System entsprechend angepasst werden. „Active Directory“ bietet die Möglichkeit, zusätzliche Authentifizierungsmethoden zu konfigurieren [53]. Die Entwickler folgen der Anleitung von Microsoft, um einen Adapter für das neue Authentifizierungsverfahren zu entwickeln. Die Software KeyTrac, die die Versi AG zur Tipperhaltens Authentifizierung eingekauft hat, bietet eine API an [54]. Diese API erwartet die Anmeldedaten eines Benutzenden und vergleicht diese dann bei Eingang mit den Registrierungsdaten dieser Person. Danach gibt sie eine Prozentzahl mit der Übereinstimmung der beiden Tippverhalten zurück. Die Entwickler schreiben eine Anwendung, die die Benutzername und Passwort erwartet, und das aus der Anmeldung des Benutzenden entstandene Tippverhalten speichern kann. Die Benutzerdaten werden daraufhin von Active Directory verifiziert und das Tippverhalten wird an die API von KeyTrac zu Überprüfung des Verhaltens geschickt.

6 Schlussbetrachtung

6.1 Diskussion

Im Rahmen dieser Arbeit wurden verschiedene Verfahren der drei Kategorien der Authentifizierung untersucht. Des Weiteren wurden Themen wie Multi-Faktor-Authentifizierung angesprochen. Im Zuge der Arbeit wurde eine Metrik entwickelt, um verschiedene Authentifizierungsverfahren zu bewerten und auf ein Fallbeispiel in Form einer fiktiven Firma anzuwenden. Stärken und Schwächen vieler Authentifizierungsverfahren wurden durchleuchtet und aufgezeigt.

6.2 Fazit

Insgesamt wurden 15 verschiedene Authentifizierungserfahren untersucht. Einige davon sind aufgrund von KO-Kriterien direkt ausgeschieden. Damit wurde die Forschungsfrage, welche Authentifizierungsverfahren für die fiktive Firma in Frage kommen, erfolgreich beantwortet. Auch die Forschungsfrage, welches Verfahren am besten für die Firma geeignet ist, wurde ausführlich durch die Nutzwertanalyse und die Erläuterung beantwortet. Die dritte Frage, wie viel sicherer das neue Verfahren im Vergleich zum alten ist, wurde beantwortet, indem die alten Zustände in der Firma erläutert und auf ihre Sicherheit analysiert wurden. Auch das neue Verfahren wurde untersucht und seine Vorteile gegenüber dem alten Verfahren wurden dargestellt.

6.3 Ausblick

Authentifizierung ist ein wichtiger Bestandteil der IT-Sicherheit und das wird auch in Zukunft so bleiben. Besonders die Entwicklung von biometrischer Authentifizierung ist noch in vollem Gange. Es wird an neuen Verfahren geforscht und immer mehr Verfahren kommen in der Realität und im Alltag zum Einsatz. Mithilfe von Multi-Faktor-Authentifizierung und stetigen Fortschritten in Authentifizierungsrelevanten Technologien wird die Zukunft hoffentlich sicherer denn je.

Literaturverzeichnis

[1] D. Reasearch, "IDENTITY SECURITY: A WORK IN PROGRESS," Identity Defined Security Alliance, 2020.

[2] S. Z. S. Idrus, E. Cherrier, C. Rosenberger and J.-J. Schwartzmann, "A Review on Authentication Methods," *Australian Journal of Basic and Applied Sciences,* pp. 95-107, 2013.

[3] M. Raza, M. Iqbal, M. Sharif and W. Haider, "A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication," *World Applied Sciences Journal 19,* pp. 439-444, 2012.

[4] E. Claudia, IT-Sicherheit, Berlin/Boston: Walter de Gruyter GmbH, 2018.

[5] M. Hübner, „IT-Sicherheit Kapitel 1," HAW Hamburg, Hamburg, 2021.

[6] Bundesamt für Sicherheit in der Informationstechnik, „Zwei-Faktor-Authentisierung," Das BSI, [Online]. Available: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html. [Zugriff am 26 September 2021].

[7] M. Hübner, „IT-Sicherheit Kapitel 5," HAW Hamburg, Hamburg, 2021.

[8] M. Hübner, „IT-Sicherheit Kapitel 2,“ HAW Hamburg, Hamburg, 2021.

[9] A. Jesudoss and N. P. Subramaniam, "A survey of authentication attacks and countermeasures in a distributed environment," *Indian Journal of Computer Science and Engineering (IJCSE),* pp. 71-77, April/Mai 2014.

[10] K. Schulz, „Die Lieferantenauswahl eines Industrieunternehmens für dessen Just-in-Time Produktion mittels Nutzwertanalyse,“ *Hochschule Mittweida University of Applied Sciences,* pp. 1-100, 2012.

[11] M. Hübner, „BW1 SS 04 Kapitel 2,“ HAW Hamburg, Hamburg, 2004.

[12] R. Saini and N. Rana, "COMPARISON OF VARIOUS BIOMETRIC METHODS," *International Journal of Advances in Science and Technology (IJAST),* pp. 24-30, März 2014.

[13] D. Bhattacharyya, R. Ranjan, F. A. A. and M. Choi, "Biometric Authentication: A Review," *International Journal of u- and e- Service, Science and Technology,* pp. 13-28, September 2009.

[14] Axon Wireless, "The key differences between the biometric iris and retina scanner device," 4 März 2020. [Online]. Available: https://www.axonwireless.com/biometric-iris-and-retina-scanner-device/. [Accessed 2 Oktober 2021].

[15] AMG Time, "HandPunch 4000 Biometric | Hand Punch 4000," 2021. [Online]. Available: https://amgtime.com/hardware-amg-handpunch-4000. [Accessed 2 Oktober 2021].

[16] P. Inbavalli and G. Nandhini, "Body Odor as a Biometric Authentication," *(IJCSIT) International Journal of Computer Science and Information Technologies*, pp. 6270-6274, 2014.

[17] G.-C. Yang, "Next-Generation Personal Authentication Scheme Based on EEG Signal and Deep Learning," *Journal of Information Processing Systems*, pp. 1034-1047, Oktober 2020.

[18] B. Farnsworth, "EEG Headset Prices – An Overview of 15+ EEG Devices," Imotions, 17 Juli 2019. [Online]. Available: https://imotions.com/blog/eeg-headset-prices/. [Accessed 2 Oktober 2021].

[19] H. K. Saroh and F. U. Kha, "Graphical Password Authentication Schemes: Current," *IJCSI International Journal of Computer Science Issue*, pp. 437-443, März 2013.

[20] M. Mihajlov, B. Jerman-Blazič and M. Ilievski, "ImagePass - Designing Graphical Authentication for Security," in *7th International Conference on Next Generation Web Services Practices*, Seoul, 2011.

[21] „Datenschutz.org,“ 26 Juli 2021. [Online]. Available: https://www.datenschutz.org/brute-force/. [Zugriff am 23 September 2021].

[22] P. Jadhao and L. Dole, "Survey on Authentication Password," *International Journal of Soft Computing and Engineering (IJSCE)*, Mai 2013.

[23] M. Masrom, F. Towhidi and A. H. Lashkari, "Pure and Cued Recall-Based Graphical User," in *2009 International Conference on Application of Information and Communication Technologies*, Baku, Azerbaijan, 2009.

[24] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy and N. Memon, "PassPoints: Designandlongitudinal evaluation of a graphical password system," in *Int. J. Human-Computer Studies 63* , 2005.

[25] A. Adams and M. A. Sasse, "Users are not the enemy," *Communications of the ACM*, pp. 40-46, 1999.

[26] H. Bhanbhro, S. R. Hassan, S. Z. Nizamani and S. S. T. B. M. Alassafi, "Enhanced Textual Password Scheme for Better Security and Memorability," *International Journal of Advanced Computer Science and Applications*, pp. 209-215, 7 November 2018.

[27] E-SEC GmbH, „exploodo," E-SEC GMBH, 10 Juni 2021. [Online]. Available: https://stores.exploodo.com/de/infoguard-ag/security-awareness/course/e-sec.passwordsecurity. [Zugriff am 24 September 2021].

[28] S. P. Banerjee and D. L. Woodard, "Biometric Authentication and Identification using KeystrokeDynamics: A Survey," *Journal of Pattern Recognition Research 7 (*, pp. 16-139, 1 Juli 2012.

[29] K. S. Killourhy and R. A. Maxion, "Comparing anomaly-detection algorithms for keystroke dynamics," *2009 IEEE/IFIP International Conference on Dependable Systems Networks*, pp. 125-134, 2009.

[30] TM3 Software GmbH, "KeyTrac," TM3 Software GmbH, 2016. [Online]. Available: https://www.keytrac.net/en/pricing. [Accessed 24 September 2012].

[31] A. Peacock, K. Xian and M. Wilkerson, "Typing patterns: a key to user identification," *IEEE Security & Privacy*, pp. 40-47, 8 Oktober 2004.

[32] C. Maple and P. Norrington, "The usability and practicality of biometric authentication in the workplace," *First International Conference on Availability, Reliability and Security (ARES'06),* 8 Mai 2006.

[33] typingdna, "typingdna," typingdna, [Online]. Available: https://www.typingdna.com/verify. [Accessed 27 November 2021].

[34] L. O'Gorman, "Fingerprint Verification," in *Biometrics,* Boston, Springer, 1996, pp. 43-64.

[35] L. Hong, A. Jain, S. Pankanti and R. Bolle, "Identity Authentication Using Fingerprints," 15 Juli 1998.

[36] R. M. Bolle, J. H. Connell and . N. K. Ratha, "Biometric perils and patches," *Pattern Recognition,* pp. 2727-2738, 2002.

[37] „amazon," amazon, 1998. [Online]. Available: https://www.amazon.de/ARCANITE-Fingerabdruckleser-Windows-360-Grad-Sensor-Sicherheitsgerät-AKFSD-07/dp/B07VK71TST/. [Zugriff am 25 September 2021].

[38] Haufe Online Redaktion, „Haufe," 28 August 2020. [Online]. Available: https://www.haufe.de/personal/arbeitsrecht/datenschutz-zeiterfassung-per-fingerabdruck-zulaessig_76_509656.html. [Zugriff am 25 September 2021].

[39] HYPR Corp, "hypr," HYPR Corp, [Online]. Available: https://www.hypr.com/smart-card-authentication/. [Accessed 25 September 2021].

[40] Virtual Solution AG, „Virtual Solution," Virtual Solution AG, [Online]. Available: https://www.virtual-solution.com/glossar/smartcard/. [Zugriff am 25 September 2021].

[41] Amazon, „Amazon,“ Amazon, [Online]. Available: https://www.amazon.de/CSL-Chipkartenleser-Status-LED-Bus-Powered-10-kompatibel/dp/B01ATKK0ZU. [Zugriff am 25 September 2021].

[42] Amazon, „Amazon,“ Amzaon, [Online]. Available: https://www.amazon.de/Keycard-Schlüsselkarte-Proximity-Schreibgeschützte-Zugangskarte/dp/B07X5KRRVC/. [Zugriff am 25 September 2021].

[43] S&K Solutions GmbH & Co. KG, "All About Cards," S&K Solutions GmbH & Co. KG, [Online]. Available: https://www.allaboutcards.de/management/products/zxp-series-3-single-dual-sided. [Accessed 25 September 2021].

[44] R. Bhatia, "Biometrics and Face Recognition Techniques," *International Journal of Advanced Research in Computer Science and Software Engineering,* pp. 93-99, Mai 2013.

[45] S. Tariq, S. Jeon and S. S. Woo, "Am I a Real or Fake Celebrity?," Suwon, Korea, 2021.

[46] Amazon, „Amazon,“ Amazon, [Online]. Available: https://www.amazon.de/Stereo-Mikrofon-NexiGo-USB-Webkamera-Online-Unterricht-Desktopgerät/dp/B08931JJLV/. [Zugriff am 25 September 2021].

[47] F. Tenzer, „Anzahl der Smartphone-Nutzer in Deutschland bis 2020,“ Statista, 10 März 2021. [Online]. Available: https://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/. [Zugriff am 26 September 2021].

[48] T. V. N. Rao and K. Vedavathi, "Authentication Using Mobile Phone as a Security," *(IJCSET) International Journal of Computer Science & Engineering Technology,* pp. 569-574, Oktober 2011.

[49] S. Hallsteinsen, I. Jørstad and D. V. Thanh, "Using the mobile phone as a security token for unified authentication," *2007 Second International Conference on Systems and Networks Communications (ICSNC 2007),* pp. 68-68, 25-31 August 2007.

[50] Manpower, „Smartphone im Job – was ist eigentlich erlaubt und wo sind die Fallen?," ManpowerGroup 2021, [Online]. Available: https://www.manpower.de/neuigkeiten/der-joblog/detail/smartphone-im-job-was-ist-eigentlich-erlaubt-und-wo-sind-die-fallen-177/. [Zugriff am 4 Dezember 2021].

[51] DeutschlandSIM, „SMS Flatrate in alle Netze," DeutschlandSIM, [Online]. Available: https://www.deutschlandsim.de/info/tarife_handys/sms_flatrate_in_alle_netze. [Zugriff am 26 September 2021].

[52] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen and Y. Koucheryavy, "Multi-Factor Authentication: A Survey," *MDPI,* 5 Januar 2018.

[53] Microsoft, "Konfigurieren zusätzlicher Authentifizierungsmethoden für AD FS," Microsoft, 24 November 2021. [Online]. Available: https://docs.microsoft.com/de-de/windows-server/identity/ad-fs/operations/configure-additional-authentication-methods-for-ad-fs. [Accessed 27 November 2021].

[54] TM3 Software GmbH, "KeyTrac," TM3 Software GmbH, [Online]. Available: https://www.keytrac.net/en/technology. [Accessed 27 November 2021].

A Anhang 1: Nutzwertanalyse Datentabelle

Authentifizierungs-	Sicherheit			Kosten			Benutzerfreundlichkeit			Finales Ergebnis
verfahren	Aufwand Durchbruch	Social Engineering	gesamt	Anschaffungspreis	Betriebskosten	gesamt	Initialer Lernaufwand	Täglicher Aufwand	gesamt	gesamt
Bilder - Erkennen	50	50	50	100	100	100	100	50	65	68
Bilder - Erinnern	100	50	80	100	100	100	50	100	85	87
textuelle Passwörter	100	100	100	100	99	99,3	50	50	50	89,79
Tippverhalten	100	100	100	100	97	97,9	50	100	85	96,37
Fingerabdruck	100	50	80	44	100	83,2	50	100	85	81,96
Smart Card	100	100	100	69	100	90,7	50	50	50	87,21
Gesichterkennung	100	50	80	32	100	79,6	100	100	100	83,88
Phone as a Token	100	50	80	40	100	82	100	50	65	77,6

Erklärung zur selbstständigen Bearbeitung einer Abschlussarbeit

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen sind unter Angabe der Quellen kenntlich gemacht.

Ort Datum Unterschrift im Original