HOCHSCHULE
MITTWEIDA
University of Applied Sciences

BACHELORARBEIT

Herr
Philipp Wenig

Optimierung von Brute-Force-Angriffen auf mobile Endgeräte mittels individueller Wörterbücher: Eine Analyse für Strafverfolgungsbehörden

Mittweida, August 2024

Fakultät **Angewandte Computer- und Biowissenschaften**

BACHELORARBEIT

Optimierung von Brute-Force-Angriffen auf mobile Endgeräte mittels individueller Wörterbücher: Eine Analyse für Strafverfolgungsbehörden

Autor:
Philipp Wenig

Studiengang:
IT-Forensik / Cybercrime

Seminargruppe:
CC20w1-B

Erstprüfer:
Prof. Dr. rer. pol. Ronny Bodach

Zweitprüfer:
Christian Hainzinger, M.Sc.

Einreichung:
Mittweida, 11.08.2024

Verteidigung/Bewertung:
Mittweida, 2024

Faculty of **Applied Computer Sciences and Biosciences**

BACHELOR THESIS

Optimizing brute force attacks on mobile devices using individual dictionaries: An analysis for law enforcement agencies

Author:
Philipp Wenig

Course of Study:
Digital Forensics / Cybercrime

Seminar Group:
CC20w1-B

First Examiner:
Prof. Dr. rer. pol. Ronny Bodach

Second Examiner:
Christian Hainzinger, M.Sc.

Submission:
Mittweida, 11.08.2024

Defense/Evaluation:
Mittweida, 2024

Bibliografische Beschreibung:

Wenig, Philipp:
Optimierung von Brute-Force-Angriffen auf mobile Endgeräte mittels individueller Wörterbücher: Eine Analyse für Strafverfolgungsbehörden. – 2024. – 54 S.
Mittweida, Hochschule Mittweida – University of Applied Sciences, Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2024.

Referat:

Die vorliegende Bachelorarbeit befasst sich mit der Frage, wie Brute-Force-Angriffe auf Smartphones im Umfeld von Strafverfolgungsbehörden gegenüber dem Standardvorgehen gängiger Mobilfunkforensik-Tools optimiert werden können. Zur Beantwortung dieser Frage wurde der aktuelle Stand der Wissenschaft in relevanten Themenbereichen analysiert und eine Online-Umfrage zur Passwortsicherheit durchgeführt. Zudem wurde ein praxisorientierter Vergleich vorgenommen, um zu ermitteln, wie häufig Menschen Passwörter auf Grundlage persönlicher Informationen erstellen. Auf Basis der erzielten Ergebnisse konnte festgestellt werden, dass die Benutzung von individuellen Wörterbüchern bei Brute-Force-Angriffen im Vergleich zum Standardvorgehen gängiger Forensik-Tools eine sinnvolle Alternative hinsichtlich Effizienz und Erfolgschancen darstellt.

Hinweis:

Zur besseren Lesbarkeit wird in dieser Arbeit das generische Maskulinum verwendet. Die verwendeten Personenbezeichnungen beziehen sich – sofern nicht anders kenntlich gemacht – auf alle Geschlechter.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AOT . . . . . Ahead-of-time

APFS . . . . . Apple File System

API . . . . . Application Programming Interface

ART . . . . . Android Runtime

ASCII . . . . . American Standard Code for Information Interchange

BSI . . . . . Bundesamt für Sicherheit in der Informationstechnik

CPU . . . . . Central Processing Unit

CSBW . . . . . Cybersicherheitsagentur Baden-Württemberg

CSV . . . . . Comma-separated values

DB4S . . . . . DB Browser for SQLite

DsiN . . . . . Deutschland sicher im Netz

DVM . . . . . Dalvik Virtual Machine

ext3 . . . . . Third Extended Filesystem

ext4 . . . . . Fourth Extended Filesystem

F2FS . . . . . Flash-Friendly Filesystem

FBE . . . . . File Based Encryption

FDE . . . . . Full Disk Encryption

FFS . . . . . Full Filesystem

HAL . . . . . Hardware Abstraction Layer

HPI . . . . . Hasso-Plattner-Institut

IP . . . . . Internet Protocol

JIT . . . . . Just-in-time

MD5 . . . . . Message-Digest Algorithm 5

MDM . . . . . Mobile Device Management

MSAB . . . . . Micro Systemation AB

OHA . . . . . Open Handset Alliance

OS . . . . . Operating System

PA . . . . . Physical Analyzer

PIN . . . . . Personal Identification Number

SEDB . . . . . Social Engineering Dictionary Builder

SHA-1 . . . . . Secure Hash Algorithm 1

SMS . . . . . Short Message Service

SoC . . . . . System-on-a-Chip

USB . . . . . Universal Serial Bus

UTF-8 . . . . . Unicode Transformation Format – 8 Bits

WWDC . . . . . Worldwide Developers Conference

1 Einleitung

In diesem Kapitel wird die Relevanz des Themas und die Zielsetzung der Arbeit definiert. Darüber hinaus wird die angewandte Methodik kurz erläutert und eine Abgrenzung des Themas vorgenommen. Abschließend wird der Aufbau der Arbeit vorgestellt.

1.1 Relevanz des Themas

Die Nutzung von Smartphones in Deutschland nimmt stetig zu. Im Jahr 2021 lag der Anteil der Smartphone-Besitzer in Deutschland bei 88,8%. Bei den 20- bis 49-Jährigen betrug dieser Anteil sogar über 95%. [1] Einer Studie aus dem Jahr 2019 zufolge sind 92% dieser Smartphones in Deutschland durch mehr oder weniger komplexe, individuelle Zugangscodes vor unbefugter Nutzung geschützt [2].

Was für die Nutzer eine erhöhte Datensicherheit bedeutet, stellt jedoch die Strafverfolgungsbehörden vor erhebliche Herausforderungen, da sie für die forensische Auswertung moderner Smartphones meist höhere Zugriffsrechte benötigen. Um die gespeicherten Daten auf diesen Geräten auslesen und analysieren zu können, ist in der Regel die Kenntnis des Gerätesperrcodes erforderlich. Wenn dieser nicht bekannt ist, kann der IT-Forensiker einen Brute-Force-Angriff durchführen, um den korrekten Sperrcode herauszufinden. Während diese Methode bei Sperrcodes mit wenigen Kombinationsmöglichkeiten, wie etwa Personal Identification Numbers (PINs) oder Wischmustern, häufig erfolgreich ist, sinkt die Erfolgswahrscheinlichkeit bei alphanumerischen Passwörtern aufgrund der Vielzahl möglicher Kombinationen erheblich.

Um diesem Problem zu begegnen, nutzen gängige Mobilfunkforensik-Tools wie Cellebrite für Brute-Force-Angriffe auf alphanumerische Passwörter bekannte, große Wörterbücher wie beispielsweise „rockyou.txt“ [3]. Diese Wörterbücher sind jedoch, abhängig von der Brute-Force-Geschwindigkeit des jeweiligen Geräts, oft schon nach wenigen Tagen erschöpft. Da Standard-Brute-Force-Listen, die alle möglichen Kombinationen enthalten, extrem umfangreich sind, stehen IT-Forensiker in Strafverfolgungsbehörden vor dem Problem, wie sie nach dem Durchlaufen erfolgloser Wörterbuchangriffe weiter vorgehen können, um die Chancen auf einen erfolgreichen Angriff zu maximieren.

1.2 Zielsetzung und Methodik

Diese Bachelorarbeit verfolgt das Ziel, das Sicherheitsbewusstsein der Bevölkerung im digitalen Raum, insbesondere in Bezug auf Passwortsicherheit, zu ermitteln und Trends in diesem Bereich zu identifizieren. Zudem wird die Verbreitung verschiedener Sperrarten bei mobilen Endgeräten untersucht, wobei der Schwerpunkt auf alphanumerischen Passwörtern liegt. Ein weiterer Untersuchungsgegenstand ist die Häufigkeit der Erstellung von Passwörtern auf Grundlage persönlicher Informationen und deren Potenzial, im Kontext von Brute-Force-Angriffen genutzt zu werden.

Daraus ableitend ergibt sich folgende zentrale Forschungsfrage:

Können Brute-Force-Angriffe auf Smartphones mit Passwort-Sperre durch die Nutzung individueller Wörterbücher, die auf Basis persönlicher Informationen erstellt werden, effizienter und erfolgversprechender gestaltet werden?

Zur Beantwortung dieser Fragestellungen werden drei wissenschaftliche Methoden angewendet. Zunächst erfolgt eine Literaturrecherche, um den aktuellen Stand der Wissenschaft in den relevanten Themenbereichen darzustellen. Anschließend wird eine Online-Umfrage durchgeführt, die vorrangig das Sicherheitsbewusstsein der Bevölkerung, die Verbreitung alphanumerischer Passwörter bei Smartphones und die Nutzung von Passwörtern, die auf persönlichen Informationen basieren, erfassen soll. Abschließend wird ein praxisorientierter Vergleich durchgeführt, um zu ermitteln, in welchem Ausmaß persönliche Informationen in Passwörtern aus öffentlich zugänglichen Passwortleaks verwendet wurden.

1.3 Abgrenzung

Aufgrund des streng definierten Rahmens dieser Arbeit wird eine klare Abgrenzung der zu behandelnden Themen vorgenommen. Zum einen wird nicht behandelt, wie spezialisierte Forensik-Tools vorgehen, um die hohen Zugriffsprivilegien erlangen zu können, die für die Durchführung eines Brute-Force-Angriffs notwendig sind. Dies wäre aufgrund der Blackbox-Problematik führender Forensik-Tool-Hersteller ohnehin schwierig umzusetzen [4]. Des Weiteren wird darauf verzichtet, eine eigene Software zur Generierung individueller Wörterbücher zu programmieren. Es existieren bereits verschiedene Open-Source-Tools zu diesem Zweck, sodass darauf zurückgegriffen werden kann. Diese Thematik wird im Ausblick (Kapitel 6.2) kurz thematisiert.

1.4 Aufbau der Arbeit

Im Kapitel 2 werden die theoretischen Grundlagen aller für die Forschungsfrage relevanten Themenbereiche analysiert. Dazu gehören die Architekturen moderner Smartphone-Betriebssysteme und die theoretischen Grundlagen von Brute-Force-Angriffen. Zudem wird der aktuelle Stand der Wissenschaft im Bereich der Gewohnheiten bei der Passworterstellung untersucht. Abschließend wird praxisorientiert der Einsatz von Brute-Force in der Digitalen Forensik analysiert.

Kapitel 3 widmet sich einer Online-Umfrage zum Thema „Gewohnheiten bei der Passworterstellung“. Ziel der Umfrage ist es, einen tieferen Einblick in die Gewohnheiten und das Sicherheitsbewusstsein der Bevölkerung in Bezug auf Passwortsicherheit zu erhalten.

In Kapitel 4 wird ein praxisorientierter Vergleich durchgeführt. Hierbei wird ein eigens erstelltes Wörterbuch mit Passwortlisten aus öffentlich zugänglichen Datenleaks verglichen. Ziel dieses Vergleichs ist es, herauszufinden, wie weit die Verwendung persönlicher Informationen bei der Erstellung von Passwörtern verbreitet ist.

In Kapitel 5 werden die erzielten Ergebnisse der eingesetzten wissenschaftlichen Methoden in Bezug auf die Forschungsziele zusammengefasst und diskutiert.

Abschließend wird in Kapitel 6 ein Fazit gezogen und die Forschungsfrage beantwortet. Zudem werden in einem Ausblick mögliche Erweiterungen erläutert.

2 Theoretische Grundlagen

In diesem Kapitel werden die theoretischen Grundlagen der Arbeit dargestellt. Hierfür wird eine umfassende Literaturrecherche durchgeführt, die sich auf die Architekturen mobiler Betriebssysteme und die theoretischen Grundlagen von Brute-Force-Angriffen konzentriert. Zudem wird ein Überblick über das Vorgehen bei Brute-Force-Angriffen im Umfeld von Strafverfolgungsbehörden gegeben. Um praxisrelevante Inhalte zu integrieren, werden in den Abschnitten 2.2.4 und 2.2.5 hauptsächlich die praktischen Erfahrungen des Verfassers aus seiner mehrjährigen Tätigkeit als IT-Forensiker bei einer Strafverfolgungsbehörde erläutert. Abschließend wird die bestehende Literatur zu menschlichen Gewohnheiten bei der Passworterstellung analysiert.

2.1 Architekturen mobiler Betriebssysteme

In den beiden folgenden Kapiteln werden die Architekturen aktueller Smartphone-Betriebssysteme untersucht. Da der Marktanteil der führenden Betriebssysteme iOS und Android im März 2024 zusammen bei 98,9% lag, wird auf die Untersuchung weiterer Betriebssysteme verzichtet [5].

2.1.1 iOS-Architektur

iOS ist das von Apple entwickelte Betriebssystem für das iPhone, den iPod touch und bis 2019 auch für das iPad. Dieses fortschrittliche Betriebssystem wurde erstmals 2007 mit der ersten Generation des iPhones eingeführt und hieß damals noch iPhone OS. Die aktuelle Version, iOS 17, wurde im Juni 2023 auf Apples Worldwide Developers Conference (WWDC) vorgestellt und am 18. September 2023 veröffentlicht. Der Marktanteil des proprietären Betriebssystems, das seit Version 10.3 das Apple File System (APFS) nutzt, lag im März 2024 bei 34,9% [5].

Die iOS-Architektur ist in der Abbildung 2.1 dargestellt und besteht aus folgenden fünf Schichten:

- Hardware
- Core OS Layer
- Core Services Layer
- Media Layer
- Cocoa Touch Layer [6]

Im Folgenden werden die einzelnen Architektur-Schichten beschrieben.

Hardware
Die Hardware-Schicht bezeichnet die physischen Komponenten des Smartphones, unter anderem die Rechenchips [6].

Core Operating System (OS) Layer
Die Core OS-Schicht interagiert direkt mit der Geräte-Hardware und ist für die Speicherverwaltung, Dateiverwaltung, Netzwerkverwaltung und Interprozesskommunikation zuständig [6].

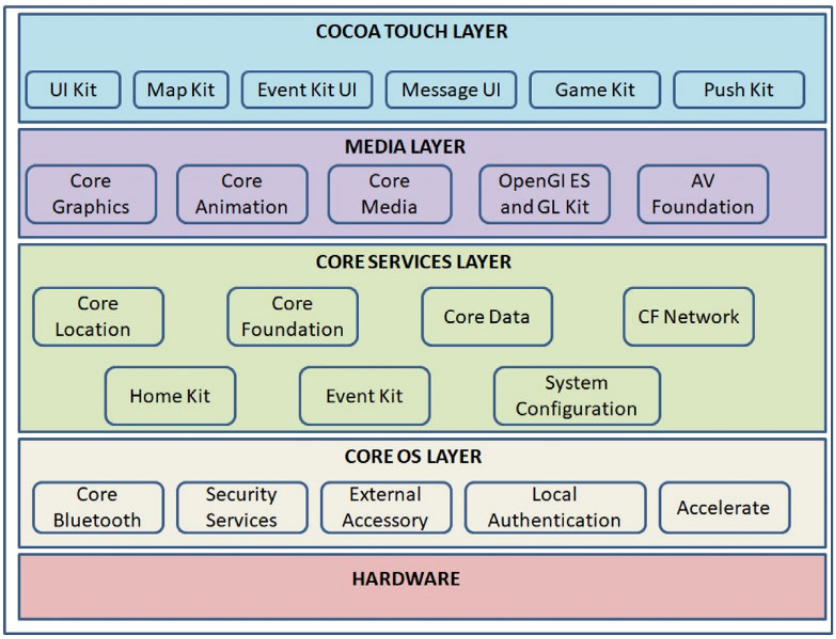


Abbildung 2.1: iOS-Architektur [6]

Core Services Layer
Die Core Services-Schicht stellt verschiedene grundlegende Systemfunktionen bereit, die für ein optimales Nutzererlebnis erforderlich sind. Dazu gehören Funktionen wie iCloud-Speicher, SQLite-Datenbanken, Standort-Dienste und In-App-Käufe. [6]

Media Layer
Die Media Layer ist für die Bereitstellung von Medienfunktionen verantwortlich und besteht aus drei verschiedenen Frameworks: Grafik-Framework, Video-Framework und Audio-Framework. Diese Frameworks ermöglichen den Zugriff auf gespeicherte Fotos und Videos sowie die Bearbeitung von Bilddateien durch Filter. Zudem unterstützt diese Schicht die Applikationsentwicklung. [6]

Cocoa Touch Layer
Die Cocoa Touch-Schicht stellt wichtige Frameworks für die Entwicklung von iOS-Apps und deren visuelles Erscheinungsbild zur Verfügung. Sie ist für grundlegende Schlüsseltechnologien wie Multitasking, Touch-Funktionen und Push-Benachrichtigungen verantwortlich. [6]

Das iOS-Sicherheitsmodell (Abbildung 2.2) ist im Vergleich zu Android restriktiver. Im Gegensatz zu Android ist iOS closed source und somit weder für Benutzer noch für Applikationsentwickler einsehbar. Da die Sicherheit des iOS-Betriebssystems für Apple einen besonders hohen Stellenwert hat, wurden diverse Sicherheitsmechanismen implementiert. Die Sicherheitsmechanismen auf Geräteebene umfassen unter anderem eine Gerätesperre in Form eines Passworts oder einer PIN mit selbst gewählter Länge und die Möglichkeit zur Fernlöschung mittels Mobile Device Management (MDM). Auf Systemebene setzt Apple auf Touch- bzw. Face-ID als Zugangssperre, einen sicheren Boot-Prozess und die Secure Enclave. [6] Die Secure Enclave ist ein sicheres, dediziertes Subsystem, das in die System-on-a-Chips (SoCs) integriert ist. Sie ist von der Central Processing Unit (CPU) isoliert und schafft dadurch eine zusätzliche Sicherheitsebene. Die Secure Enclave verfügt über einen eigenen Prozessor, der ausschließlich von diesem Subsystem genutzt wird, wodurch eine

vollständige Isolation vom Hauptsystem erreicht wird. Hier werden vor allem sicherheitskritische Operationen durchgeführt, wie die Verschlüsselung und Speicherung sensibler Daten, die Verarbeitung von Authentifizierungsinformationen sowie Fingerabdruck- oder Gesichtserkennungsdaten. [7]

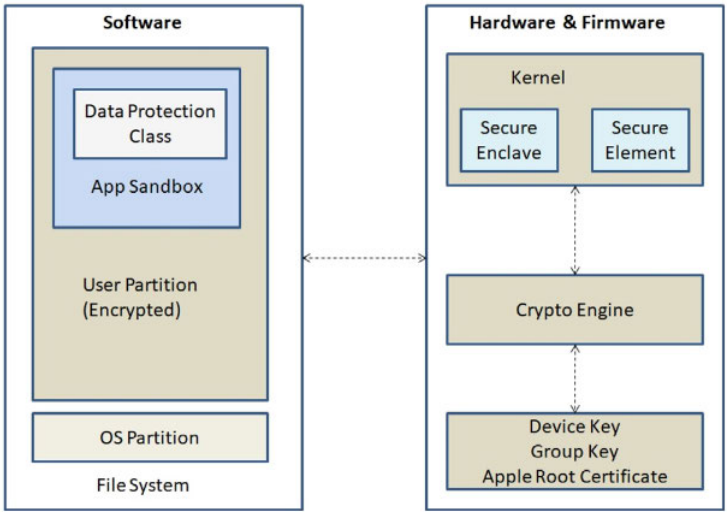


Abbildung 2.2: iOS-Sicherheitsarchitektur [6]

Auf Dateiebene setzt Apple auf die File Based Encryption (FBE) mit Datenschutzklassen. Dabei wird jede Datei mit einem eigenen Schlüssel verschlüsselt. Neben den erwähnten Sicherheitsmechanismen gibt es noch viele weitere Methoden, mit denen Apple iOS zu einem sicheren Betriebssystem machen will. Besonders hervorzuheben ist das Sandboxing-Verfahren. Bei diesem Isolationsmechanismus werden alle Applikationen isoliert in einer eigenen Umgebung gestartet, wodurch iOS-Applikationen weder untereinander agieren können noch über relevante Kernel-Kenntnisse verfügen. [6]

2.1.2 Android-Architektur

Android ist ein Open Source-Betriebssystem für mobile Endgeräte, das von der von Google gegründeten Open Handset Alliance (OHA) entwickelt wird. Die OHA ist ein Unternehmenszusammenschluss, der aus mehr als 80 Mitgliedern besteht und das Ziel verfolgt, offene Standards für das mobile Ökosystem zu schaffen. [8] Die Basis des Betriebssystems ist ein Linux-Kernel [6]. Im März 2024 lag der Marktanteil von Android bei 64% [5]. Anders als das iOS-Betriebssystem wird Android auf Smartphones verschiedenster Hersteller eingesetzt, die es an ihre Geräte anpassen und mit proprietärer Software, wie Google Maps und Google Play Store, ausliefern. Die aktuelle Android-Version ist Android 14, das seit Oktober 2023 offiziell verfügbar ist [9]. Bei den meisten modernen Android-Smartphones wird das Dateisystem Fourth Extended Filesystem (ext4) eingesetzt. Es können jedoch auch andere Dateisysteme wie das Third Extended Filesystem (ext3) oder das Flash-Friendly Filesystem (F2FS) zum Einsatz kommen. [10]

Die Android-Architektur ist in Abbildung 2.3 dargestellt und besteht aus den folgenden sechs Schichten:

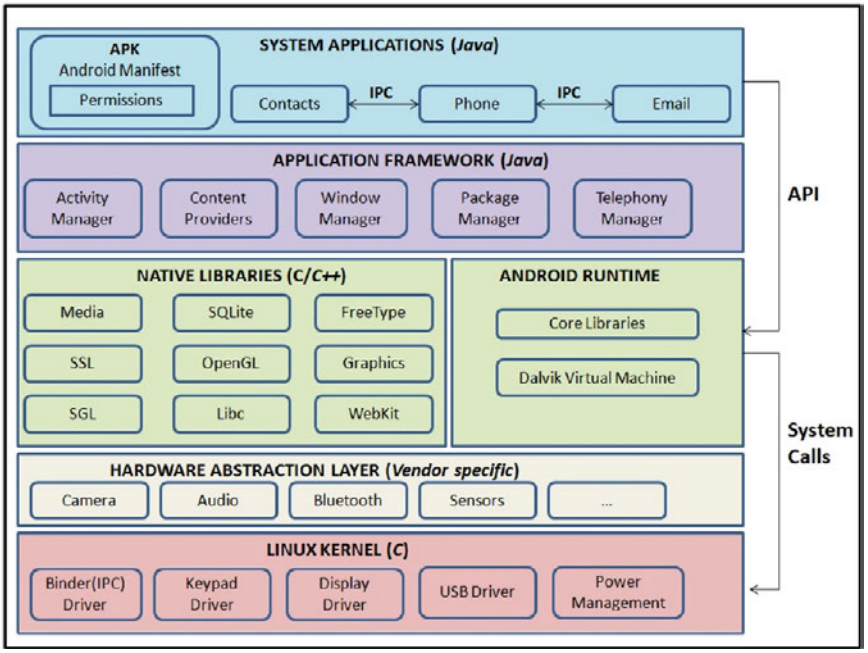


Abbildung 2.3: Android-Architektur [6]

Linux Kernel

Der Linux-Kernel bildet die Grundlage der Android-Plattform. Er stellt grundlegende Funktionen zur Verfügung, die von den darüber liegenden Schichten genutzt und aufgerufen werden können. [11] Der Kernel unterstützt und verwaltet zentrale Systemdienste wie Speicher, Netzwerk und Prozesse [6].

Hardware Abstraction Layer (HAL)

Die HAL fungiert als Schnittstelle für die Kommunikation der Applikationen bzw. des Android-Frameworks mit hardwarespezifischen Gerätetreibern wie Bluetooth oder Wi-Fi. Bei einem Aufruf einer Application Programming Interface (API) eines Frameworks für den Zugriff auf Gerätehardware lädt das Android-Betriebssystem das Modul für die entsprechende Hardwarekomponente. [11] Da die HAL hardwarespezifisch ist, hängt die Implementierung vom Smartphone-Hersteller ab [6].

Android Runtime (ART)

Die ART ist seit der Version 5.0 in die Android-Architektur implementiert und ersetzt die zuvor eingesetzte Dalvik Virtual Machine (DVM). Seitdem wird jede Android-Applikation als eigener Prozess in einer Instanz der ART ausgeführt. Zu den wichtigsten Merkmalen der ART gehören die Ahead-of-time (AOT)- und die Just-in-time (JIT)-Kompilierung sowie die optimierte automatische Speicherbereinigung. Die ART wurde so konzipiert, dass auf Geräten mit geringem Arbeitsspeicher mehrere Instanzen von virtuellen Maschinen ausgeführt werden können. [11]

Native Libraries

Einige der zentralen Systemkomponenten bzw. Systemdienste wie ART und HAL werden aus den Native Libraries erstellt, die in den Programmiersprachen C bzw. C++ geschrieben sind. Zudem gibt es verschiedene Java-basierte Bibliotheken, die Unterstützung bei der Applikationsentwicklung bieten, beispielsweise beim Zugriff auf Datenbanken. [6]

Application Framework

Das Application Framework bildet die Grundlage für die Programmierung von Android-Applikationen. Diese Anwendungsrahmen, die in Java geschrieben sind, werden von Applikationen aufgerufen, um auf die Hardware zuzugreifen. Wichtige Funktionen umfassen unter anderem den Activity Manager, den Location Manager und den Notification Manager. [6] Entwickler von Drittanbieter-Applikationen haben uneingeschränkten Zugriff auf die gleichen APIs, die auch von den Android-Systemapplikationen verwendet werden [11].

System Applications

Die System-Applikationen bilden zusammen mit den Drittanbieter-Applikationen die höchste Schicht der Android-Architektur. Dazu gehören beispielsweise die Short Message Service (SMS)-App, der Kalender und die „Internet"-App. Alle Applikationen greifen über die APIs des Application Frameworks auf die Gerätehardware zu. [12]

Android ist im Gegensatz zu Apples iOS ein quelloffenes (open source) Betriebssystem. Dies bietet zwar einige Vorteile wie Flexibilität und Portabilität, bringt jedoch auch sicherheitstechnische Risiken mit sich. Da die Software für jeden einsehbar ist, haben auch Nutzer mit böswilligen Absichten leichteren Zugang zu möglichen Angriffsstrategien und Schwachstellen. Deshalb müssen Android-Nutzer besondere Vorsichtsmaßnahmen ergreifen. Eine Möglichkeit, die Sicherheit eines Android-Smartphones zu erhöhen, ist die Installation einer Anti-Virus-Software. Zudem sollte die Option „Unbekannte Quellen" in den Einstellungen deaktiviert bleiben. Ist diese Option aktiviert, können Applikationen mit Schadsoftware jederzeit weitere schädliche Applikationen aus dem Internet herunterladen und aktivieren. Eine solche Einstellung existiert bei iOS nicht, da Applikationen dort grundsätzlich nur über den Apple App Store installiert werden können. [12]

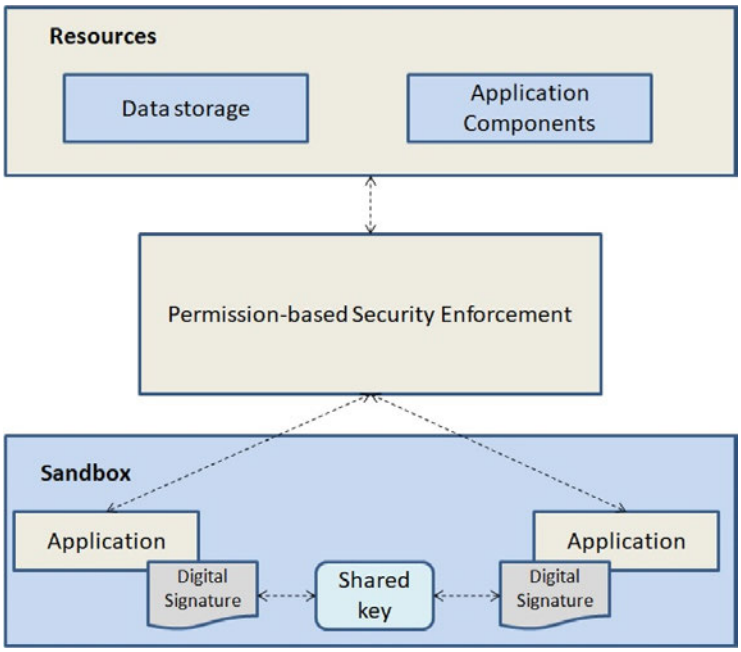


Abbildung 2.4: Android-Sicherheitsarchitektur [6]

In Abbildung 2.4 ist das Android-Sicherheitsmodell dargestellt. Ein grundlegender Sicherheitsmechanismus bei Android ist die Isolierung durch eine Sandbox-Umgebung. Dabei wird jede Anwendung in einer eigenen Sandbox ausgeführt, was bedeutet, dass eine Applikation nicht auf die Daten einer anderen Applikation zugreifen kann. Zudem ist jede Anwendung standardmäßig vom Android-Kernel

separiert, was die vollständige administrative Kontrolle über das Betriebssystem verhindert. Zwar können Android-Apps Zugriff auf System-Ressourcen erhalten, jedoch muss dieser Zugriff vom Nutzer ausdrücklich genehmigt werden. [6] Seit Android 7.0 setzt Android, wie auch iOS, auf eine dateibasierte Verschlüsselung (FBE) auf Dateiebene. Zuvor nutzte Android freiwillig und seit Android 6.0 standardmäßig die Full Disk Encryption (FDE). Der Vorteil der dateibasierten Verschlüsselung liegt darin, dass einzelne Dateien mit unterschiedlichen Schlüsseln verschlüsselt werden können. Dadurch lassen sich verschiedene Datenschutzklassen definieren, die unabhängig voneinander entschlüsselt werden. Bei der FDE hingegen wird nach der Entschlüsselung automatisch die gesamte Partition entschlüsselt. [13]

2.2 Grundlagen von Brute-Force-Angriffen

Bei Brute-Force handelt es sich um eine Methode aus dem Bereich der Kryptoanalyse [14]. In den folgenden Kapiteln werden die Definition, die mathematischen Grundlagen und der Einsatz von Brute-Force-Angriffen in der digitalen Forensik behandelt.

2.2.1 Definition

Brute-Force besteht im Wesentlichen darin, alle möglichen Schlüsselkombinationen systematisch auszuprobieren [14]. Sie ist eine kryptoanalytische Angriffsmethode, die in vielen Bereichen der Informatik Anwendung findet und nicht nur zum Knacken von Passwörtern eingesetzt wird. So wurden früher beispielsweise Brute-Force-Implementationen in Schachcomputern verwendet, um den optimalen nächsten Spielzug zu berechnen [15]. Die Abbildung 2.5 verdeutlicht die Einordnung von Brute-Force in die Wissenschaft der Kryptologie.

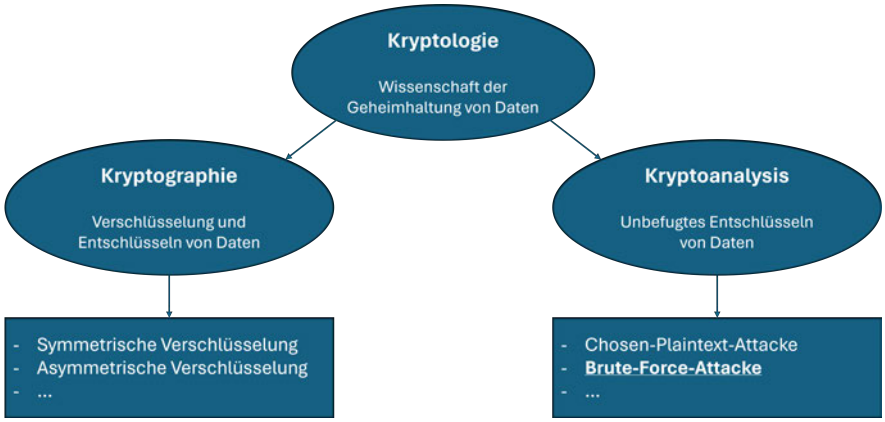


Abbildung 2.5: Einordnung von Brute-Force in die Kryptologie (Eigene Darstellung nach [14])

In der Informatik wird diese Methode auch als „Vollständige Suche“ bezeichnet. Brute-Force wird meist bei Problemen angewandt, für die kein effizienter Algorithmus zur Lösung bekannt ist. Zwar ist Brute-Force grundsätzlich ein langsames Verfahren, jedoch führt diese Methode immer zum Erfolg, sofern die Anzahl der möglichen Lösungen, die ausprobiert werden müssen, nicht zu groß ist und somit praktisch in einer sinnvollen Zeit umgesetzt werden kann. [14]

2.2.2 Mathematische Grundlagen

Um einschätzen zu können, ob Brute-Force eine praktikable Lösung für ein Problem darstellt, ist es wichtig zu wissen, wie die Anzahl der möglichen Lösungen berechnet werden kann. Zur Berechnung dieser Anzahl wird die enumerative Kombinatorik verwendet. Die Kombinatorik ist eine Teildisziplin der Mathematik, die sich mit der Bestimmung der Anzahl der Elemente einer endlichen Menge beschäftigt. [16] Im Folgenden wird die Berechnung basierend auf der Literatur von P. Tittmann [16] und R. Castro [17] mithilfe von Beispielszenarien aus der Mobilfunkforensik veranschaulicht:

Definition:
Sei M die Anzahl an Lösungskombinationen, n die Größe des Vokabulars und k die Passwortlänge, dann gilt:

$$M = n^k$$

In einem einfachen Beispiel, bei dem die Anzahl der möglichen Kombinationen einer vierstelligen PIN gefunden werden soll, ergibt sich folgende Berechnung. Das Vokabular n hat die Größe 10, da es bei einer PIN zehn verschiedene Möglichkeiten pro Stelle gibt (0, 1, 2, 3, ..., 9). Die Passwort- bzw. PIN-Länge k beträgt 4, da die gesuchte PIN vierstellig ist.

Somit ergibt sich folgende Berechnung:

$$M = 10^4$$
$$M = 10.000$$

Im oben genannten Beispiel gibt es also 10.000 verschiedene Möglichkeiten (0000 bis 9999). Ähnlich sieht die Berechnung einer sechsstelligen PIN aus. Die Variable n bleibt 10, da sich das Vokabular nicht verändert. Der Exponent k erhöht sich auf sechs, sodass die Berechnung $10^6 = 1.000.000$ ergibt. Bei einem Brute-Force-Angriff auf eine sechsstellige PIN gibt es also exakt 1.000.000 verschiedene Möglichkeiten (000000 - 999999). Wie diese Berechnung zeigt, ist die Anzahl der Möglichkeiten bei Zahlen-PINs aufgrund des geringen Vokabulars nicht besonders hoch. Anders sieht dies bei alphanumerischen Passwörtern aus.

In einem weiteren Beispiel wird versucht, ein neunstelliges Passwort durch einen Brute-Force-Angriff zu ermitteln. Die Berechnung der Anzahl der verschiedenen Möglichkeiten wird mit der gleichen Methode wie in den vorherigen Beispielen durchgeführt. Nun erhöht sich jedoch die Basis n erheblich. Je nach Eingabemethode stehen mehr oder weniger Sonderzeichen zur Verfügung, sodass in diesem Beispiel von einem Vokabular von 72 Zeichen ausgegangen wird, bestehend aus 26 Kleinbuchstaben, 26 Großbuchstaben, zehn Zahlen und zehn Sonderzeichen.

Somit ergibt sich folgende Berechnung für das Ausprobieren aller neunstelligen alphanumerischen Passwörter:

$$M = 72^9$$
$$M = 51.998.697.814.228.992$$

Bei einem neunstelligen Passwort gibt es somit fast 52 Billiarden verschiedene Möglichkeiten. Diese Information allein reicht jedoch nicht aus, um die Erfolgsaussichten eines Brute-Force-Angriffs zu bewerten. Stattdessen muss die maximale Zeit berechnet werden, die benötigt wird, um alle möglichen Kombinationen zu testen. Hierbei spielt die Prozessorleistung eine entscheidende Rolle. Die Berechnung der maximal benötigten Zeit kann wie folgt definiert werden.

Definition:
Sei t die maximale Dauer des Angriffs in Sekunden, n die Größe des Vokabulars, k die Passwortlänge und s die Anzahl an Kombinationen, die ein Prozessor pro Sekunde testen kann, dann gilt:

$$\mathrm{t} = \frac{n^k}{s}$$

Davon ausgehend, dass moderne Prozessoren etwa vier Milliarden Kalkulationen pro Sekunde durchführen können [17], sieht die Berechnung eines neunstelligen alphanumerischen Passworts folgendermaßen aus:

$$\mathrm{t} = \frac{72^9}{4.000.000.000}s$$

$$\mathrm{t} = \frac{51.998.697.814.228.992}{4.000.000.000}s$$

$$\mathrm{t} \approx 12.999.674s \approx 216.661m$$

$$\mathrm{t} \approx 3.611h \approx 150d$$

Daraus folgt, dass ein Brute-Force-Angriff auf ein neunstelliges alphanumerisches Passwort mit einem modernen Prozessor spätestens nach etwa 150 Tagen erfolgreich ist. Mit zunehmender Passwortlänge steigt die maximale Dauer des Angriffs jedoch erheblich an. Ein Brute-Force-Angriff auf ein zehnstelliges Passwort kann unter sonst gleichen Bedingungen bis zu 29 Jahre dauern, während ein elfstelliges Passwort sogar mehr als 2.100 Jahre in Anspruch nehmen kann.

Bei dieser Berechnung wird vorausgesetzt, dass die Länge des Passworts – neun, zehn oder elf Zeichen – bekannt ist. In der Praxis ist dies jedoch selten der Fall. Daher müssen bei einem Brute-Force-Angriff auf ein neunstelliges Passwort auch alle möglichen Kombinationen von achtstelligen, siebenstelligen und kürzeren Passwörtern getestet werden.

Im Folgenden wird deshalb eine realistische Berechnung dargestellt, wie lange es dauert, ein sechsstelliges Passwort zu finden, ohne zuvor die genaue Länge von sechs Zeichen zu kennen. Es wird angenommen, dass das Smartphone eine Mindestlänge des Passworts von vier Zeichen vorschreibt, wie es beispielsweise bei modernen Apple-Smartphones der Fall ist und alle Passwörter nacheinander in ihrem Wert aufsteigend getestet werden:

$$\mathrm{t} = \frac{72^4 + 72^5 + 72^6}{4.000.000.000} s$$

$$\mathrm{t} = \frac{26.873.856 + 1.934.917.632 + 139.314.069.504}{4.000.000.000} s$$

$$\mathrm{t} = \frac{141.275.860.992}{4.000.000.000} s$$

$$\mathrm{t} \approx 35,32 s$$

Ein Brute-Force-Angriff auf ein sechsstelliges Passwort dauert unter den gegebenen Umständen somit maximal etwa 35,32 Sekunden.

2.2.3 Sonderform der Brute-Force-Attacke: Der Wörterbuchangriff

Der Wörterbuchangriff (engl. Dictionary-Attack) ist eine spezielle Form des Brute-Force-Angriffs, bei der gängige Wörter, Wortkombinationen und andere Ausdrücke aus einem digitalen Wörterbuch verwendet werden, um Passwörter zu knacken. Im Gegensatz zu einem herkömmlichen Brute-Force-Angriff, bei dem alle möglichen Kombinationen, meist alphabetisch oder numerisch aufsteigend, getestet werden (vgl. Beispielszenarien aus Kapitel 2.2.2), wird bei einem Wörterbuchangriff jedes Wort aus einem Wörterbuch oder einer Wortliste nacheinander getestet. [18] In der Abbildung 2.6 ist ein exemplarischer Ausschnitt aus dem Wörterbuch rockyou.txt zu sehen [3].

Wörterbuchangriffe sind besonders sinnvoll, wenn ein herkömmlicher Brute-Force-Angriff aufgrund geringer Prozessorleistung oder der großen Anzahl möglicher Kombinationen an seine Grenzen stößt. Die dem Wörterbuchangriff zugrunde liegende Theorie ist, dass Menschen bei der Erstellung von Passwörtern häufig persönliche Faktoren wie Namen, Wohnort oder Hobbys nutzen oder Passwörter wählen, die häufig genutzt werden und sich leicht merken lassen. Solche Wörterbücher können aus verschiedenen Quellen stammen, meist werden jedoch frei im Internet verfügbare Wörterbücher verwendet, die aus geleakten Passwort-Hacks resultieren. Ein bekanntes Beispiel hierfür ist die eben bereits erwähnte rockyou.txt [3]. Das aktuell vermutlich größte verfügbare Wörterbuch, das

Abbildung 2.6: Auszug aus dem Dictionary „rockyou.txt“ [3]

jedoch eine Kombination vieler Wörterbücher ist und nicht einem einzelnen Leak entstammt, ist die rockyou2024.txt, die am 4. Juli 2024 in einem einschlägigen Forum veröffentlicht wurde. Diese Wortliste enthält fast zehn Milliarden verschiedene Wörter bzw. Wortkombinationen im Klartext. [19]

Eine weitere Möglichkeit besteht darin, die entsprechenden Wörterbücher selbst zu generieren. Hierfür existieren verschiedene Open-Source-Tools, wovon im Kapitel 6.2 drei Tools kurz vorgestellt werden. Der Vorteil dieser Methode liegt darin, dass persönliche Faktoren genutzt werden können, um maßgeschneiderte Wörterbücher zu erstellen. So können beispielsweise Namen, Geburtsdaten oder Hobbys in die Erstellung der Wörterbücher einfließen.

2.2.4 Brute-Force in der Computer- und Datenträgerforensik

In der Computer- und Datenträgerforensik spielen Brute-Force-Angriffe eine große Rolle. Sie werden eingesetzt, um Passwörter von Dateien oder Applikationen zu knacken oder Zugang zu gesperrten Geräten zu erlangen. IT-Forensiker stoßen in diesem Bereich häufig auf einzelne Dateien, die mit einem Passwort geschützt sind. Da diese Dateien ohne das entsprechende Passwort nicht eingesehen werden können, initiiert der IT-Forensiker einen Brute-Force-Angriff. Dabei kommen sowohl herkömmliche Brute-Force-Angriffe, häufiger jedoch Wörterbuchangriffe zum Einsatz.

Häufig liegen die Passwörter jedoch nicht im Klartext vor, weshalb nicht selten auch Rainbow-Table-Angriffe verwendet werden. Hierbei wird ein Klartext-Wörterbuch verwendet, dessen Begriffe mit kryptographischen Hashfunktionen (z. B. Message-Digest Algorithm 5 (MD5) oder Secure Hash Algorithm 1 (SHA-1)) „gehasht“ werden. Diese Hash-Wörterbücher, bekannt als „Rainbow Tables“, dienen dann als Grundlage für den Brute-Force-Angriff. Ist der Angriff erfolgreich, kann der betreffende Hashwert in das Klartextpasswort zurückgerechnet werden. Dieses Passwort kann der Forensiker dann zum Entsperren des Dienstes oder der Datei nutzen. [20]

Neben passwortgeschützten Dateien oder Applikationen mit Zugangssperre stellen auch Archivdateien (z. B. ZIP, RAR) und Verschlüsselungscontainer (z. B. Veracrypt, Truecrypt) häufig eine Herausforderung für Forensiker dar. Auch in diesen Fällen können Brute-Force-Attacken eingesetzt werden, um die Passwörter zu ermitteln. Weitere gängige Ziele eines Brute-Force-Angriffs durch Computerforensiker sind das BitLocker-Passwort sowie die Masterpasswörter von Passwortmanagern. Ein Beispiel hierfür ist der verbreitete Passwortmanager KeePass, deren Passwortdatenbank durch ein Masterpasswort gesichert werden kann [21]. Gelingt es dem Forensiker, dieses Passwort zu knacken, erhält er oft Zugang zu zahlreichen weiteren Passwörtern, die potenziell zu weiteren ermittlungsrelevanten Inhalten führen können.

Auch Windows-Anmeldekennwörter müssen gegebenenfalls geknackt werden, um eine vollständige Datensicherung zu ermöglichen. In der forensischen Praxis spielt das Windows-Anmeldekennwort bei den meisten PCs und Notebooks jedoch oft keine große Rolle, da die entsprechenden Festplatten oder Speicherriegel unverschlüsselt aus dem Gerät ausgebaut und einer Post-Mortem-Analyse unterzogen werden können, wobei Anmeldepasswörter nicht relevant sind. [22] Wenn der PC bzw. das Notebook jedoch mit der proprietären Windows-Verschlüsselungsmethode BitLocker gesichert ist, wird das Passwort relevant, da der zur Entschlüsselung notwendige Wiederherstellungsschlüssel im Dateisystem, in Absturzabbildern oder in Auslagerungsdateien gefunden werden kann. Zudem kann das Windows-Anmeldepasswort von Interesse sein, wenn der IT-Forensiker das Speicherabbild zur effizienteren Auswertung virtualisieren möchte, was insbesondere im Bereich der Wirtschaftskriminalität häufig vorkommt.

Die Anzahl der Versuche pro Sekunde variiert je nach Dienst, Applikation oder Dateiart erheblich. Üblicherweise sind von wenigen Tausend bis zu mehreren hunderttausend Versuchen pro Sekunde möglich. Bei einigen Diensten ist die Anzahl der Versuche pro Sekunde aufgrund von Sicherheitsvorkehrungen eingeschränkt. Gibt es vom Ziel jedoch keinerlei Beschränkungen, kann ein Brute-Force-Angriff so effizient durchgeführt werden, wie es der verwendete Prozessor erlaubt. In diesem Fall kann die Geschwindigkeit weiter gesteigert werden, indem mehrere Computer in einem Brute-Force-Cluster logisch zusammengeschlossen werden, um das Ziel gemeinsam anzugreifen. Viele Software-Produkte, die Brute-Force-Angriffe ermöglichen, unterstützen auch das Clustern von mehreren Computern zu diesem Zweck.

Um Brute-Force-Attacken auf Dateien, Anmeldepasswörter oder Applikationen durchführen zu können, wird eine spezielle Software benötigt. Ein Beispiel für eine weit verbreitete Open-Source-Software ist Hashcat, welche in der IT-Forensik häufig zum Einsatz kommt [23]. Eine kommerzielle Software, die auf Brute-Force-Attacken spezialisiert ist, ist das Passware Forensic Kit der Firma Passware [24].

2.2.5 Brute-Force in der Mobilfunkforensik

In der Mobilfunkforensik werden Brute-Force-Angriffe vor allem eingesetzt, um die Zugangssperren von Smartphones zu knacken. Um einen derartigen Angriff initiieren zu können, benötigt der Forensiker zunächst erhöhte Zugriffsrechte auf das Smartphone. Bei modernen Smartphones mit aktuellen Betriebssystemen sind komplexe Methoden erforderlich, um diese Zugriffsrechte zu erlangen. Zur Anwendung dieser Methoden wird ebenfalls eine spezielle forensische Software benötigt.

Einer der bekanntesten Hersteller von Softwareprodukten im Bereich der Mobilfunkforensik ist die israelische Firma Cellebrite. Auf eine kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN aus dem Jahr 2018 bestätigte die damalige Bundesregierung, dass die Polizei in Deutschland Softwareprodukte von Cellebrite zum Auslesen von sichergestellten bzw. beschlagnahmten Mobilgeräten nutzt [25]. In einem Artikel von heise.de aus dem Jahr 2019 wird ebenfalls erwähnt, dass ein Vertreter der Firma Cellebrite bestätigt hat, dass unter anderem die deutsche Polizei Softwareprodukte von Cellebrite verwendet [26].

Weitere Firmen, deren Produkte in der Mobilfunkforensik Verwendung finden, sind Magnet (ehemals Greyshift), Micro Systemation AB (MSAB) und Oxygen Forensics. Eine kostenfreie Software, die sich sowohl für computer- als auch mobilfunkforensische Untersuchungen eignet, ist Autopsy [27]. Aufgrund der bestätigten Nutzung in Deutschland sowie der persönlichen Erfahrungen des Verfassers dieser Arbeit wird im weiteren Verlauf speziell auf Brute-Force-Angriffe mit dem Softwareprodukt Premium Enterprise der Firma Cellebrite eingegangen.

Mit dieser Software ist es möglich, die erforderlichen hohen Zugriffsrechte auf Smartphones zu erlangen [28]. Welche Methoden Cellebrite nutzt, um diese Zugriffsrechte zu erlangen, ist nicht öffentlich bekannt. Damit versucht Cellebrite, wie auch andere Hersteller, die genutzten Hard- oder Software-Schwachstellen sowohl vor Mitkonkurrenten als auch vor den Smartphone- bzw. Betriebssystemherstellern geheimzuhalten. Aus diesem Grund existiert dazu auch keine wissenschaftliche Literatur. [4] Bekannt ist jedoch, dass durch den Forensiker keine speziellen Einstellungen am Smartphone, wie etwa die Aktivierung von Universal Serial Bus (USB)-Debugging, gesetzt werden müssen. Der Einsatz dieser Methoden erfolgt größtenteils vollautomatisch durch Cellebrite Premium Enterprise, eine Interaktion des Forensikers ist zumeist nicht erforderlich.

Ist der vollständige Zugriff auf ein Smartphone hergestellt, kann der IT-Forensiker über die forensische Software einen Brute-Force-Angriff initiieren [29]. Hierfür ist es wichtig, die Art der verwendeten Zugangssperre zu kennen.

Je nach Hersteller, Modell und Software-Version des Smartphones gibt es dafür verschiedene Möglichkeiten:

- 4-stellige PIN
- 6-stellige PIN
- PIN ohne vorgegebene Länge
- Passwort (alphanumerisch)
- Wischmuster

Zusätzlich sind bei modernen Smartphones häufig biometrischen Zugangssperren wie

- Face-ID (Gesichtserkennung) und
- Touch-ID (Fingerabdruckscanner)

einstellbar. Diese spielen für eine Brute-Force-Attacke jedoch grundsätzlich keine Rolle, da eine biometrische Zugangssperre nicht als alleinige Sperrart genutzt werden kann. Eine biometrische Sperre muss immer mit einer nicht biometrischen Sperre kombiniert werden. Daher ist eine Brute-Force-Attacke auf die nicht biometrische Sperre stets möglich und für forensische Zwecke ausreichend.

Nach den Erfahrungen des Verfassers dieser Arbeit variiert die Anzahl der möglichen Versuche zwischen 150 Versuchen pro Tag und 10.000 Versuchen pro Minute. Einflussfaktoren hierfür sind die Konstellation aus Smartphone-Hersteller, Smartphone-Modell, genutztem Betriebssystem, Betriebssystemversion und Sicherheitspatchlevel sowie die Unterstützung durch die Brute-Force-Software für eben diese Konstellationen.

Nachdem der zuständige Forensiker die richtige Art der Zugangssperre in der Cellebrite-Software angegeben hat, stehen ihm verschiedene Konfigurationsmöglichkeiten für den bevorstehenden Brute-Force-Angriff zur Verfügung. Er kann beispielsweise wählen, ob der Angriff im „tethered-“ oder im „autonomous-“ Modus durchgeführt wird. Im tethered-Modus bleibt das Smartphone über ein Kabel mit dem Computer verbunden, während im autonomous-Modus das Brute-Force-Tool direkt auf das Smartphone geladen wird, was einen kabellosen Angriff ermöglicht.

Zuletzt kann der Forensiker festlegen, welche Begriffe oder Zahlenkombinationen für den Brute-Force-Angriff verwendet werden sollen. Wenn der Nutzer die Standardeinstellungen beibehält, wählt die Software die zu verwendende PIN- bzw. Passwortliste basierend auf der gewählten Art der Zugangssperre aus. Diese voreingestellten Listen bzw. Wörterbücher sind für den Forensiker jedoch nicht direkt einsehbar. Bei einer vier- oder sechsstelligen PIN kann anhand der Fortschrittsanzeige erkannt werden, dass alle möglichen Kombinationen (10.000 bzw. 1.000.000) durchprobiert werden. Um die Dauer des Brute-Force-Angriffs so kurz wie möglich zu halten, werden zunächst häufig genutzte und leicht zu merkende PIN-Kombinationen ausprobiert. Für eine vierstellige PIN sind dies beispielsweise:

- 0000
- 1111
- 1234

Bei einer sechsstelligen PIN werden zusätzlich mögliche Datumsangaben bevorzugt. So wird beispielsweise die PIN „300992“, die den 30.09.1992 darstellen könnte, der PIN „289987“ vorgezogen, obwohl diese chronologisch zuvor getestet werden würde. Erst nachdem häufig genutzte PINs und Kombinationen, die ein Datum darstellen können, getestet wurden, werden die restlichen Möglichkeiten durchprobiert.

Bei einem 3x3-Wischmuster, wie es von vielen Android-Smartphones unterstützt wird, gibt es exakt 389.112 verschiedene Kombinationsmöglichkeiten [30]. Diese Sperrmethode liegt hinsichtlich der Anzahl der möglichen Kombinationen zwischen der vierstelligen und der sechsstelligen PIN. Auch hier wird bei der von Cellebrite standardmäßig verwendeten Liste jede Möglichkeit abgedeckt. Ob bei Wischmustern ebenfalls häufig genutzte Kombinationen (z. B. Muster, die einen Buchstaben darstellen) in der Brute-Force-Reihenfolge vorgezogen werden, ist nicht bekannt.

Bei PINs ohne vorgegebene Länge lässt sich aus der kriminalpolizeilichen Praxis keine genaue Aussage darüber treffen, welche Zahlenkombinationen getestet werden. Sicher ist jedoch, dass nicht alle Möglichkeiten ausprobiert werden können, da die Anzahl der möglichen Kombinationen zu hoch ist.

Bei einem alphanumerischen Passwort können ebenfalls, wie in den mathematischen Grundlagen bereits erörtert, nicht alle Kombinationen getestet werden, da die Anzahl der Möglichkeiten zu groß ist. Es ist zu vermuten, dass Cellebrite als Standardliste eine der bekannten Passwortlisten oder eine Kombination dieser verwendet. Eine Möglichkeit ist das Wörterbuch rockyou.txt, das 14.341.564 verschiedene Passwörter aus über 32 Millionen gehackter Konten der Firma RockYou enthält [3]. Da eine Liste mit etwas über 14 Millionen Passwörtern bei einer Brute-Force-Geschwindigkeit von etwa 10.000 Versuchen pro Minute nach den Berechnungen aus dem Kapitel 2.2.2 bereits nach etwa einem Tag durchlaufen ist, stellt sich die Frage, wie in diesem Fall weiter verfahren wird.

Zusätzlich zu den Standardlisten, die von der Firma Cellebrite eingesetzt werden, gibt es für alle Arten von Zugangssperren die Möglichkeit, eigene Wörterbücher zu verwenden. Während dies bei Wischmustern sowie bei vier- und sechsstelligen PINs aufgrund der begrenzten Anzahl an Möglichkeiten meist keine Optimierung darstellen dürfte, kann dies bei alphanumerischen Passwörtern und PINs mit unbekannter Länge durchaus von Vorteil sein. Im Gegensatz zu den anderen Zugangssperren ist es bei Passwörtern und PINs mit unbekannter Länge definitiv nicht möglich, alle möglichen Kombinationen zu testen. Zu diesem Zweck können nicht nur bereits bekannte Wörterbücher wie die erwähnten rockyou.txt und rockyou2024.txt, sondern auch selbst erstellte Wörterbücher genutzt werden. Diese können mithilfe von Informationen aus dem Umfeld des Smartphone-Besitzers und einem geeigneten Tool zur Wörterbuchgenerierung erstellt werden.

Nachdem der Brute-Force-Angriff auf ein Smartphone erfolgreich gewesen ist, kann der Datenspeicher mithilfe einer der verfügbaren Auslesemethoden und der Software Premium Enterprise ausgelesen werden. Die am häufigsten verwendeten Auslesemethoden bei modernen Smartphones sind, in der Reihenfolge der auslesbaren Datenmenge aufsteigend, Logical Extraction, Full Filesystem (FFS) Extraction und Physical Extraction. [29] Da eine physische Sicherung, bei der der Datenspeicher Bit für Bit ausgelesen wird, bei aktuellen Smartphones mit FBE nicht mehr durchführbar ist, wird zumeist eine FFS-Extraction angestrebt [31].

Nachdem eine Datenextraktion durchgeführt wurde, kann das Abbild bzw. die Datensicherung mithilfe der Cellebrite-Software Physical Analyzer (PA) aufbereitet und untersucht werden [32]. Im PA kann dann ein Datenreport erstellt werden, der mithilfe der Software Cellebrite Reader eingesehen werden kann. Dieses Programm benötigt keine eigenständige Lizenz, sodass es auf einem beliebigen Computer ausgeführt werden kann. Der zuständige Ermittler kann den Report dann auf be- oder entlastende Beweise hin untersuchen. [33] Das Ausführen von Skripten, Verändern von Daten und Exkludieren von Inhalten ist im Cellebrite Reader aufgrund des forensischen Grundsatzes der Gewährleistung der Integrität der Daten nicht möglich [34].

2.3 Menschliche Gewohnheiten bei der Passworterstellung

Um herauszufinden, wie Brute-Force-Angriffe auf mobile Endgeräte effizient durchgeführt werden können, ist es wichtig zu verstehen, wie Menschen Passwörter erstellen. Eine repräsentative Umfrage aus dem Jahr 2019 unter 3.419 US-Bürgern ergab, dass 59% der Befragten einen Namen oder ein Geburtsdatum in ihre Passwörter für Online-Accounts einbeziehen. Ein Ausschnitt der Ergebnisse dieser Studie wird in Abbildung 2.7 dargestellt. [35]

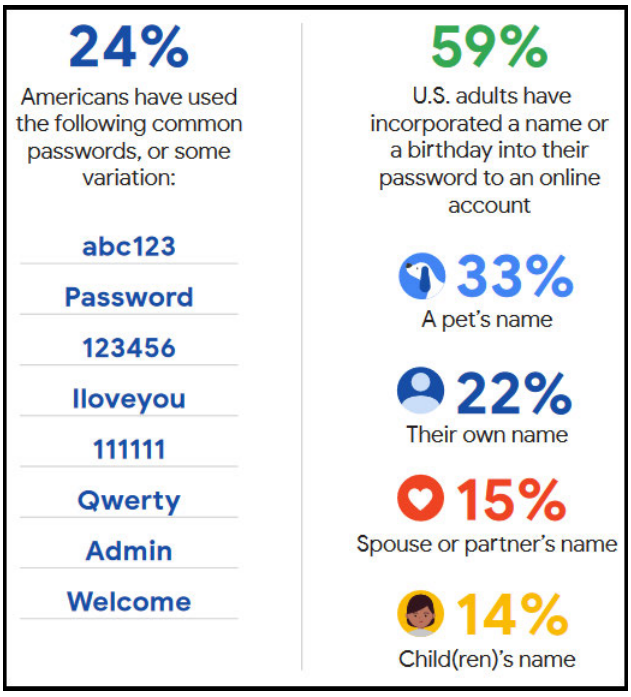


Abbildung 2.7: Ergebnisse der Studie „The United States of P@ssw0rd$“ [35]

Des Weiteren gaben 33% der Befragten an, bereits den Namen eines Haustiers für ein Passwort verwendet zu haben. Der eigene Name, der Name des Partners bzw. der Partnerin sowie der Name eines oder mehrerer Kinder wurden von 22%, 15% bzw. 14% der Befragten genutzt. [35]

Neben den Angaben darüber, welche persönlichen Informationen die Teilnehmer in Passwörter integrierten, enthält die Studie von Harris Poll und Google noch einige weitere interessante Details. So gaben 20% der Befragten an, das Passwort ihres E-Mail-Kontos mit anderen Menschen geteilt zu haben. Weitere 17% gaben an, das Passwort eines Online-Shopping-Accounts weitergegeben zu haben. Zudem bestätigten 6% der Befragten, dass ein ehemaliger Partner bzw. eine ehemalige Partnerin noch ein aktives Passwort von ihnen besitzt. [35]

Die Umfrage zeigt, dass sich viele Menschen nicht an die empfohlenen Richtlinien zur Erstellung sicherer Passwörter halten. In Deutschland ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) für die Erstellung solcher Richtlinien und Empfehlungen zuständig. Dieses empfiehlt, eine der beiden folgenden Strategien zu nutzen:

- Langes und weniger komplexes Passwort (mindestens 25 Zeichen, mindestens zwei Zeichenarten)
- Kürzeres und komplexes Passwort (mindestens acht Zeichen, alle vier Zeichenarten) [36]

Außerdem empfiehlt das BSI, Passwörter nicht auf der Basis persönlicher Informationen zu erstellen und einen Passwortmanager zur sicheren Verwaltung aller Passwörter zu verwenden [36].

Das Hasso-Plattner-Institut (HPI), das gemeinsam mit der Universität Potsdam die Digital-Engineering-Fakultät betreibt, hat ebenfalls Untersuchungen zum Thema „Passwortsicherheit und menschliche Passwortgewohnheiten“ durchgeführt [37].

So analysierte das HPI alle frei verfügbaren Datenleaks nach den am häufigsten genutzten Passwörtern. Aus fast 14 Milliarden Passwörtern wurden die folgenden zehn am häufigsten verwendet. [38] Die jeweiligen Anteile sind in Klammern angegeben:

1. **123456** (8,01 ‰)
2. **123456789** (3,84 ‰)
3. **password** (1,87 ‰)
4. **qwerty** (1,81 ‰)
5. **12345** (1,36 ‰)
6. **12345678** (1,15 ‰)
7. **111111** (1,14 ‰)
8. **qwerty123** (1,00 ‰)
9. **1q2w3e** (0,95 ‰)
10. **123123** (0,84 ‰) [38]

Diese Auflistung, die in der Abbildung 2.8 in Form eines Kreisdiagramms dargestellt ist, verdeutlicht, dass Menschen generell dazu neigen, einfache Passwörter zu verwenden. Dass dies nicht nur ein globales, sondern auch ein spezifisch deutsches Problem ist, zeigt die Liste des Herstellers der Passwortmanager-Software NordPass. Die fünf in Deutschland am häufigsten erfassten Passwörter von NordPass sind „admin“, „123456“, „zwieback“, „12345678“ und „123456789“. [39]

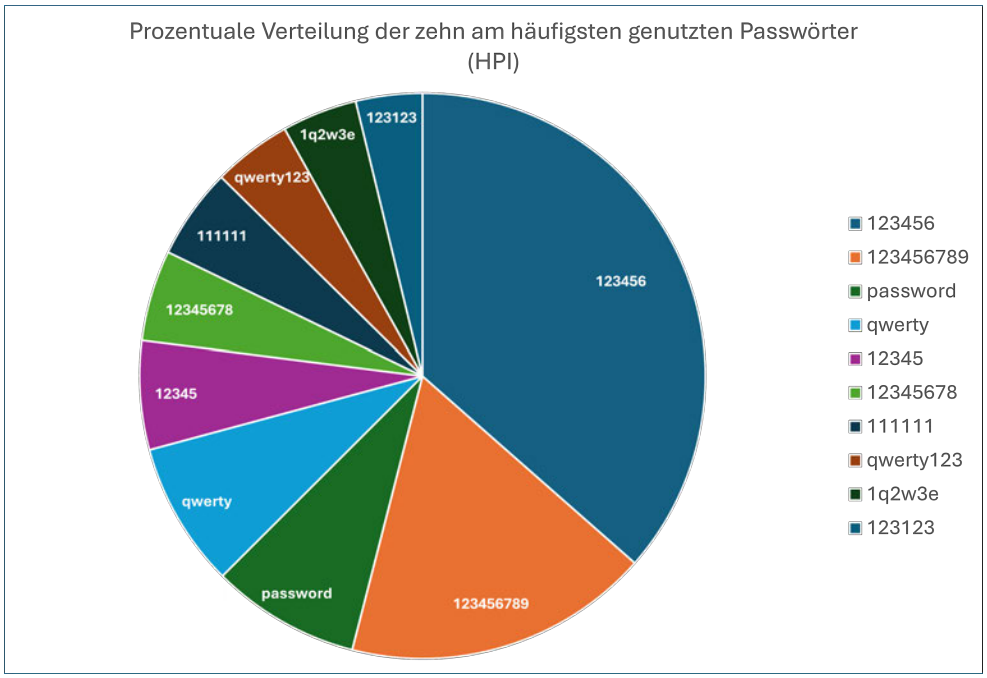


Abbildung 2.8: Die zehn häufigsten Passwörter in Datenleaks (Eigene Darstellung nach [38])

Andererseits zeigt eine Umfrage des Branchenverbands der deutschen Informations- und Telekommunikationsbranche Bitkom, dass das Bewusstsein für die Erstellung sicherer Passwörter durchaus vorhanden ist. So gaben im Jahr 2023 74% der Befragten an, bei der Erstellung neuer Passwörter auf eine Mischung aus Buchstaben, Zahlen und Sonderzeichen zu achten. 23% der Teilnehmer bestätigten, dass sie ihre Passwörter regelmäßig ändern. Zudem gab jeder vierte Befragte an, zur Erstellung neuer Passwörter einen Passwortgenerator zu verwenden. [40]

3 Durchführung einer Online-Umfrage

In den vorangegangenen Kapiteln wurde unter anderem der aktuelle Stand der Wissenschaft zum Thema Passwortsicherheit und Gewohnheiten bei der Passworterstellung analysiert. Obwohl diese Analysen durchaus aufschlussreich sind, können sich die technischen Hintergründe und das Sicherheitsbewusstsein in diesen Bereichen schnell verändern. Zudem wurden einige Fragen, die zur Beantwortung meiner Forschungsfrage notwendig sind, in der Literatur bislang nur unzureichend behandelt. In den folgenden Kapiteln wird auf die Ziele, die Methodenwahl, die Fragebogenkonstruktion sowie die Auswertung der Ergebnisse dieser empirischen Untersuchung eingegangen.

3.1 Ziele und Fragestellungen

Das Ziel der Untersuchung besteht darin, detailliert zu ergründen, wie die Bevölkerung beim Erstellen von Passwörtern vorgeht und wie ausgeprägt das Sicherheitsbewusstsein der Bevölkerung im digitalen Raum ist. Ein umfassendes und aktuelles Bild dieser Aspekte zu gewinnen, ist ein wesentlicher Bestandteil zur fundierten Beantwortung der zugrunde liegenden Forschungsfrage.

Im Detail sind dabei insbesondere die folgenden Fragestellungen von besonderer Bedeutung:

- Wie viele Menschen besitzen ein Smartphone und welche Maßnahmen ergreifen sie, um ihre mobilen Endgeräte vor unbefugtem Zugriff durch Dritte zu schützen?
- Wie viele Menschen erstellen Passwörter, die auf persönlichen Informationen basieren, wie etwa dem Namen des Partners, dem eigenen Geburtsdatum oder dem Namen eines Sportvereins?
- Welche spezifischen persönlichen Informationen werden häufig zur Erstellung von Passwörtern genutzt?
- Wie verbreitet ist die Praxis, dass Menschen dieselben Passwörter für verschiedene Geräte oder Online-Dienste verwenden?
- Wie häufig werden Passwort-Manager genutzt und welche Passwort-Manager sind dabei am weitesten verbreitet?
- Wie würden Menschen ihr eigenes Vorgehen bei der Erstellung eines neuen Passworts beschreiben?

Die Untersuchung dieser Fragestellungen ermöglicht es, ein tiefgehendes Verständnis über das Sicherheitsverhalten der Bevölkerung im digitalen Bereich zu erlangen. Dabei wird nicht nur die Praxis der Passworterstellung beleuchtet, sondern auch die Anwendung der verschiedenen Sicherungsmethoden und Passwortmanagern untersucht. Dies ist entscheidend, um fundierte Aussagen über den aktuellen Stand der digitalen Sicherheit und das Bewusstsein der Nutzer in diesem Bereich treffen zu können.

3.2 Wahl der empirischen Methode (Online-Umfrage)

Für die Untersuchung der genannten Fragestellungen wurde eine quantitative Online-Umfrage gewählt. Diese Entscheidung beruht auf mehreren wesentlichen Vorteilen, die sowohl die Zielsetzung der Forschung als auch die praktischen Aspekte der Datenerhebung optimal unterstützen.

Breite Erreichbarkeit und Repräsentativität

Durch eine Online-Umfrage kann eine große und vielfältige Stichprobe der Bevölkerung erreicht werden, um allgemeine Trends und Verhaltensweisen bei der Passworterstellung und Smartphone-Sicherung zu analysieren. Online-Plattformen ermöglichen den Zugang zu Teilnehmern aus verschiedenen demografischen Gruppen, was die Generalisierbarkeit der Ergebnisse erhöht. Trotzdem muss erwähnt werden, dass eine gewöhnliche Online-Umfrage ohne spezifisch ausgewählte Teilnehmer nicht als „repräsentativ“ oder völlig unverzerrt betrachtet werden kann [41].

Effizienz und Zeitersparnis

Online-Umfragen sind effizient und ermöglichen eine schnelle Datenerhebung im Vergleich zu persönlichen Interviews oder postalischen Befragungen. Sie erlauben es, zeitnah aktuelle Trends und Verhaltensmuster zu erfassen, die sich im digitalen Sicherheitsbereich schnell ändern können.

Anonymität und Ehrlichkeit der Antworten

Die Anonymität von Online-Umfragen fördert ehrliche und präzise Antworten, insbesondere bei sensiblen Themen wie Passwortnutzung und Sicherheitssoftware, da Teilnehmer eher bereit sind, in einem anonymen Umfeld ihr tatsächliches Verhalten zu offenbaren.

Standardisierung der Datenerhebung

Eine standardisierte Online-Umfrage ermöglicht eine konsistente Datenerhebung und erleichtert die Vergleichbarkeit und Analyse der Ergebnisse. Die einheitliche Struktur der Fragen unterstützt systematische Analysen und die Identifikation von Mustern und Zusammenhängen. Online-Umfrage-Tools bieten zudem oft integrierte Auswertemöglichkeiten.

Kosten-Nutzen-Verhältnis

Eine Online-Umfrage ist kostengünstig und bietet dennoch umfangreiche Analysemöglichkeiten, was besonders vorteilhaft im Rahmen einer akademischen Abschlussarbeit ist.

Fazit

Insgesamt bietet die quantitative Online-Umfrage die idealen Voraussetzungen, um die Forschungsfragen umfassend und effektiv zu beantworten. Sie ermöglicht eine breite Erreichbarkeit, gewährleistet Anonymität, ist effizient und kostengünstig und bietet standardisierte Analysemöglichkeiten. Dies stellt sicher, dass die erhobenen Daten aussagekräftig und so unverzerrt wie möglich sind.

3.3 Konstruktion des Fragebogens

Die Online-Umfrage kann grob in vier Teile gegliedert werden. Die Abbildung 3.1 zeigt den strukturierten Aufbau.

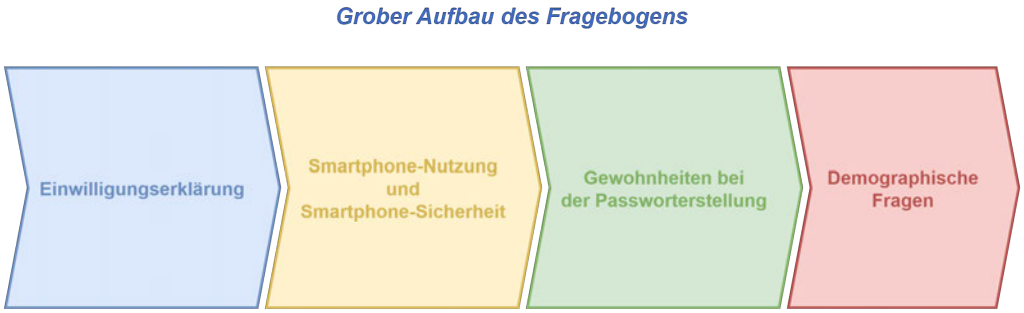


Abbildung 3.1: Strukturierte Gliederung der Online-Umfrage (Eigene Darstellung)

Auf den folgenden Seiten werden die einzelnen Fragen detailliert erläutert, einschließlich ihrer Hintergründe und Besonderheiten.

3.3.1 Fragebogen Teil 1: Einwilligungserklärung

Den Fragen vorangestellt ist eine Einwilligungserklärung, die Informationen über Art und Thematik der zugrundeliegenden Arbeit und Datenschutzhinweise enthält. Zudem wird darauf hingewiesen, dass sich Fragen zu Smartphones bzw. deren Nutzung auf das am häufigsten genutzte Smartphone des Teilnehmers beziehen. Zweitsmartphones wie etwa Firmen- oder Diensthandys werden in dieser Umfrage nicht berücksichtigt. Des Weiteren wird klargestellt, dass die Teilnehmer keine Passwörter in der Umfrage teilen sollen. Die Einwilligungserklärung ist dieser Arbeit als Anhang A beigefügt.

3.3.2 Fragebogen Teil 2: Smartphone-Nutzung und Smartphone-Sicherheit

Der zweite Teil des Umfrage trägt den Titel „Smartphone-Nutzung und Smartphone-Sicherheit“. Er besteht aus vier Fragen, die im Folgenden beschrieben werden.

1. Frage: Sind Sie im Besitz eines Smartphones?

Die erste Frage dient als einfacher Einstieg in die Umfrage. Es handelt sich um eine dichotome Frage, also eine Frage, die genau zwei Antwortmöglichkeiten (Ja und Nein) bietet [42]. Sie zielt darauf ab, den Anteil der Smartphone-Nutzer in der Gesellschaft zu erfassen und gleichzeitig als Grundlage für die Fragen 2 bis 4 zu dienen. Wird die Frage mit „Ja“ beantwortet, folgt Frage 2; wird sie mit „Nein“ beantwortet, folgt Frage 5.

2. Frage: Wie lautet der Hersteller Ihres Smartphones?

Die zweite Frage ist eine Single-Choice-Frage. Single-Choice bedeutet, dass die Teilnehmer nur exakt eine Antwort aus den vorgegebenen Antwortmöglichkeiten auswählen können [43]. Es gibt zehn vordefinierte Antwortmöglichkeiten: „Apple“, „Samsung“, „Huawei“, „Xiaomi“, „OnePlus“, „Oppo“, „Google“, „Sony“, „ZTE“ und „Honor“. Zusätzlich gibt es ein offenes Antwortfeld. Wird dieses gewählt, kann der Teilnehmer eine eigene Antwort eintragen. Unabhängig von der Antwort folgt die 3. Frage.

3. Frage: Ist Ihr Smartphone mithilfe einer Gerätesperre gegen unbefugten Zugriff gesichert?

Auch diese Frage ist eine dichotome Frage mit den Antwortmöglichkeiten „Ja“ und „Nein“. Diese Frage soll ermitteln, wie viel Prozent der Smartphone-Besitzer ihr Gerät mit einer Sperre absichern und wie viele ihr Mobiltelefon ungesichert nutzen. Sie soll einen Beitrag zur Ermittlung des Sicherheitsbewusstsein der Teilnehmer hinsichtlich der auf dem Gerät gespeicherten Daten und Informationen leisten. Wird diese Frage bejaht, folgt Frage 4; bei einer Verneinung wird die nächste Frage übersprungen und mit Frage 5 fortgesetzt.

4. Frage: Welche Art von Gerätesperre ist an Ihrem Gerät eingestellt?

Die vierte Frage ist eine Multiple-Choice-Frage. Für die Teilnehmer ist, an die Frage anschließend, folgender Hinweis sichtbar:

„Achtung: Biometrische Zugangssperren wie Touch- oder Face-ID können nur in Kombination mit einer nicht-biometrischen Zugangssperre eingestellt werden. In diesem Fall bitte beide auswählen.“

Es stehen sieben vordefinierte Antwortmöglichkeiten sowie ein offenes Antwortfeld zur Verfügung. Eine Mehrfachauswahl ist möglich, da viele moderne Smartphones die Kombination biometrischer und nicht biometrischer Sperrarten erlauben. Zur Auswahl stehen folgende Optionen:

- Gesichtserkennung (Face-ID)
- Fingerabdrucksensor (Touch-ID)
- PIN (4-stellig)
- PIN (6-stellig)
- PIN (andere Länge)
- Passwort (alphanumerisch)
- Wischmuster
- Offenes Antwortfeld

Diese Frage soll die Verbreitung verschiedener Sperrarten bei modernen Smartphones erfassen und den prozentualen Einsatz biometrischer Sperrarten messen. Außerdem soll ermittelt werden, wie viele Menschen alphanumerische Passwörter auf ihren Smartphones verwenden, da dies einen zentralen Aspekt der Forschungsfrage darstellt. Unabhängig von der gewählten Antwort folgt die Frage 5.

3.3.3 Fragebogen Teil 3: Gewohnheiten bei der Passworterstellung und Passwortverwaltung

Der dritte Teil des Fragebogens befasst sich mit den „Gewohnheiten bei der Passworterstellung und Passwortverwaltung“. Dieser Abschnitt umfasst sechs Fragen, die im Folgenden vorgestellt werden.

5. Frage: Haben Sie jemals ein Passwort für ein Gerät oder einen Online-Dienst auf der Grundlage persönlicher Informationen erstellt?

Diese Frage ist erneut eine dichotome Frage mit den Antwortmöglichkeiten „Ja“ und „Nein“. Die Häufigkeit der Verwendung von Passwörtern, die auf persönlichen Informationen basieren, ist für die Beantwortung der Forschungsfrage von großer Bedeutung. Wird diese Frage mit „Ja“ beantwortet, folgt Frage 6; bei einer Verneinung folgt die siebte Frage des Fragebogens.

6. Frage: Auf Grundlage welcher persönlichen Informationen haben Sie in der Vergangenheit ein Passwort erstellt?

Die sechste Frage ist eine Multiple-Choice-Frage mit zwölf vordefinierten Antwortmöglichkeiten und einem offenen Antwortfeld. Um die Abgrenzung zu den vorherigen Fragen zur Smartphone-Sicherheit klarzustellen, wurde der Hinweis „auch PC- und Online-Passwörter“ hinzugefügt. Es können beliebig viele Antworten ausgewählt werden. Die definierten Antwortmöglichkeiten sind:

- Eigener Name
- Name des Partners / der Partnerin
- Name eines bzw. mehrerer Kinder
- Name eines Haustiers
- Eigenes Geburtsdatum
- Geburtsdatum des Partners / der Partnerin
- Geburtsdatum eines oder mehrerer Kinder
- Geburts- oder Wohnort
- Name oder Detail eines Hobbys
- Name oder Detail eines Sportvereins
- Name oder Detail des Berufs bzw. der Arbeitsstätte
- Datum eines speziellen Ereignisses (z.B. Hochzeitstag)
- Offenes Antwortfeld

Diese Frage ist ebenso wie die fünfte Frage von besonderem Interesse für das Erreichen der Ziele dieser Arbeit, da die Nutzung von Passwörtern basierend auf persönlichen Informationen direkt mit der Effektivität von Brute-Force-Angriffen unter Verwendung individueller Wörterbücher zusammenhängt. Unabhängig von den gewählten Antworten folgt hierauf Frage 7.

7. Frage: Nutzen Sie gleiche Passwörter bei verschiedenen Online-Diensten und/oder technischen Geräten?

Bei der siebten Frage handelt es sich um eine Ja/Nein-Frage. Sie soll erfassen, wie viele Menschen dasselbe Passwort für mehrere Geräte bzw. Online-Dienste verwenden. Die Beantwortung dieser Frage erweitert das Verständnis der Gewohnheiten bei der Passworterstellung. Unabhängig von der Beantwortung dieser Frage folgt darauf Frage 8.

8. Frage: Nutzen Sie einen Passwortmanager zum Speichern Ihrer verschiedenen Passwörter?

Auch für die achte Frage stehen die Antwortmöglichkeiten „Ja“ und „Nein“ zur Verfügung. Zur Verdeutlichung für die Teilnehmer werden die Beispiele KeePass, Password Safe und Browser hinter der Fragestellung genannt. Diese Frage zielt darauf ab, die Verbreitung der Nutzung von Passwortmanagern zu messen und dient als Einleitung für die neunte Frage. Wird die Frage mit „Ja“ beantwortet, folgt die neunte Frage. Bei einer Verneinung wird die neunte Frage übersprungen und das Umfrage-Tool leitet direkt zur zehnten Frage weiter.

9. Frage: Welchen bzw. welche Passwortmanager nutzen Sie?

Aufbauend auf die achte Frage soll hier die Angabe der von den Teilnehmern genutzten Passwortmanager im Vordergrund stehen. Aufgrund der Vielzahl möglicher Antworten wurde als Fragetyp eine offene Frage gewählt. Dies bedeutet, dass der Teilnehmer seine genutzten Passwortmanager selbst in ein Antwortfeld eintragen kann. Dieses Antwortfeld darf nicht leer bleiben. Erwartete Antworten umfassen klassische Passwortmanager für den Computer (z. B. KeePass), die Nutzung von browserinternen Passwortmanagern oder Passwortmanager, die sich auf bestimmte mobile Endgeräte beziehen, wie etwa der iOS-Schlüsselbund. Nachdem die Antwort eingetippt wurde, kann der Teilnehmer über die Schaltfläche „Weiter“ zur zehnten Frage gelangen.

10. Frage: Wie würden Sie Ihr grundsätzliches Vorgehen beim Erstellen von Passwörtern beschreiben?

Bei der zehnten Frage handelt es sich erneut um eine offene Frage. Um zu verhindern, dass weniger sicherheitsbewusste Teilnehmer direkt eines ihrer Passwörter in das Antwortfeld schreiben, wurde folgender Hinweistext an die Frage angehängt:

„(Achtung: Bitte machen Sie keine Angaben, die direkt auf eines Ihrer Passwörter schließen lassen.)“

Die Fragestellung wurde bewusst offen gestaltet, sodass für den Teilnehmer auf den ersten Blick nicht sofort klar ist, welche Antwort vom Fragesteller erwartet wird. Dies soll dazu beitragen, herauszufinden, wie der Teilnehmer grundsätzlich beim Erstellen neuer Passwörter vorgeht. Mögliche Antworten könnten die Nutzung bestimmter Tools zur Passworterstellung, die kombinierte Verwendung von Buchstaben, Zahlen und Sonderzeichen oder das Erstellen von Passwörtern mithilfe der Anfangsbuchstaben eines Satzes umfassen. Doch auch völlig andere Antworten sind bei dieser Frage denkbar.

3.3.4 Fragebogen Teil 4: Demografische Fragen

Abschließend werden Fragen zur Person gestellt, die für die weiterführende Auswertung und zu Interpretationszwecken erforderlich sind. Diese Fragen werden unter dem Begriff „Demografische Fragen“ zusammengefasst.

Demografische Frage 1: Wie alt sind Sie?

Zur Beantwortung dieser Frage steht ein offenes Antwortfeld zur Verfügung, in das der Teilnehmer sein aktuelles Alter eingeben kann. Es werden nur ein- und zweistellige, numerische Eingaben akzeptiert.

Demografische Frage 2: Wie ist Ihr Geschlecht?

Hierbei handelt es sich um eine Single-Choice-Frage. Es stehen die drei Antwortmöglichkeiten „Männlich“, „Weiblich“ und „Divers“ zur Verfügung.

Allgemein wurde versucht, den Fragebogen so flüssig und einfach verständlich wie möglich zu gestalten. Aus diesem Grund wurde auf komplexe Matrixfragen verzichtet und stattdessen einfache und klare Single-Choice-, Multiple-Choice- und dichotome Fragen verwendet. Die Fragen wurden nach Möglichkeit so formuliert, dass sie auch für technisch weniger versierte Personen klar und verständlich sind. Bei einigen Fragen wurden zudem kurze Hinweissätze oder Beispiele angegeben, um die Verständlichkeit zu erhöhen. Der logische Ablauf der Umfrage ist als Ablaufplan dieser Arbeit im Anhang angefügt (Anhang B).

3.4 Dauer, Tool und Verbreitung des Fragebogens

Nachdem mehrere Umfrage-Tools hinsichtlich Design, Kosten, Nutzerfreundlichkeit und Auswertemöglichkeiten getestet wurden, fiel die Wahl auf das Online-Tool empirio [44]. Empirio bietet standardisierte Auswertemöglichkeiten und die Möglichkeit, eine Mehrfachteilnahme gerätebezogen zu deaktivieren [45]. Diese Einstellung wurde gesetzt, um die Integrität der Ergebnisse zu wahren. Da für die Beantwortung der Forschungsfrage die Gewohnheiten aller Bevölkerungsgruppen relevant sind, ist die Umfrage grundsätzlich für jeden offen. Es gibt keine Personengruppen, die von der Teilnahme ausgeschlossen sind.

Um möglichst viele Teilnehmer zu erreichen, wurde der Link zum Fragebogen über folgende Kanäle geteilt:

- WhatsApp-Nachricht an Familie, Freunde und Bekannte
- WhatsApp-Status
- Instagram-Story
- Mailing-Listen von Vereinen
- Mailing-Listen der Stiftung Begabtenförderung (SBB)

Des Weiteren wurde die Umfrage in der empirio-Community veröffentlicht, sodass Menschen auch direkt über die Plattform teilnehmen können [46].

Die Dauer der Umfrage wurde auf 18 Tage festgesetzt. Nach einer kurzen Testphase, in der der Fragebogen an vier ausgewählte Personen unterschiedlichen Alters geschickt und um Feedback gebeten wurde, war die Umfrage vom 31.05.2024 bis einschließlich 17.06.2024 aktiv.

3.5 Darstellung der Ergebnisse

Am 17.06.2024 wurde die Umfrage um 23:59 Uhr beendet. Ab diesem Zeitpunkt war der Link zur Umfrage nicht mehr erreichbar und die Umfrage in der empirio-Community nicht mehr sichtbar. Insgesamt nahmen im festgelegten Zeitraum 430 Personen an der Umfrage teil. Die durchschnittliche Dauer zur Beantwortung des Fragebogens betrug 05:17 Minuten. Im Folgenden werden die Ergebnisse der einzelnen Fragen objektiv dargestellt; eine ausführliche Interpretation der Ergebnisse erfolgt in Kapitel 3.6.

1. Frage: Sind Sie im Besitz eines Smartphones?

Die erste Frage wurde naturgemäß von allen 430 Teilnehmern beantwortet. 98,6% der Teilnehmer (424 Personen) antworteten mit „Ja“. Die restlichen 1,4% (6 Personen) verneinten die Frage, besitzen also kein Smartphone. Die Ergebnisse dieser Frage sind in Abbildung 3.2 dargestellt.

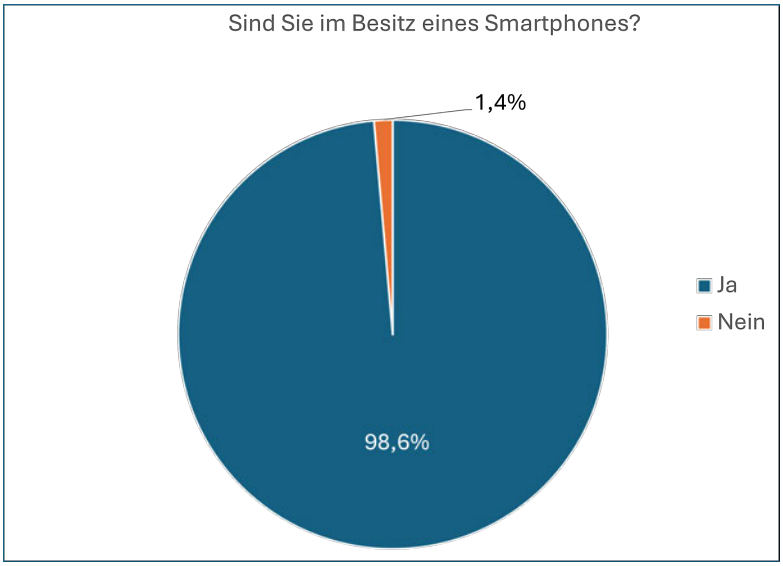


Abbildung 3.2: Auswertung der Ergebnisse von Frage 1 (Eigene Darstellung)

Dieses Ergebnis stimmt weitgehend mit früheren Umfragen überein. In einer Studie aus dem Jahr 2019 wurden etwas niedrigere Zahlen für Smartphone-Besitzer festgestellt, jedoch ist diese Erhebung mittlerweile fünf Jahre alt [1].

2. Frage: Wie lautet der Hersteller Ihres Smartphones?

Bei der zweiten Frage gab fast die Hälfte aller Befragten, nämlich 194 Personen (45,8%), an, ein Smartphone der Firma Apple zu besitzen. 122 Teilnehmer (28,8%) besitzen ein Samsung-Smartphone. Mit jeweils 5,7% (24 Personen) erhielten Geräte der Firmen Xiaomi und Google die drittmeisten Stimmen. Für ein Huawei-Smartphone entschieden sich 3,8% der Teilnehmer, was 16 Stimmen entspricht. Smartphones der Firmen OnePlus, Sony, Oppo, ZTE und Honor erhielten neun, zwei und dreimal jeweils eine Stimme. Die Verteilung der Antworten ist in der Abbildung 3.3 übersichtlich dargestellt.

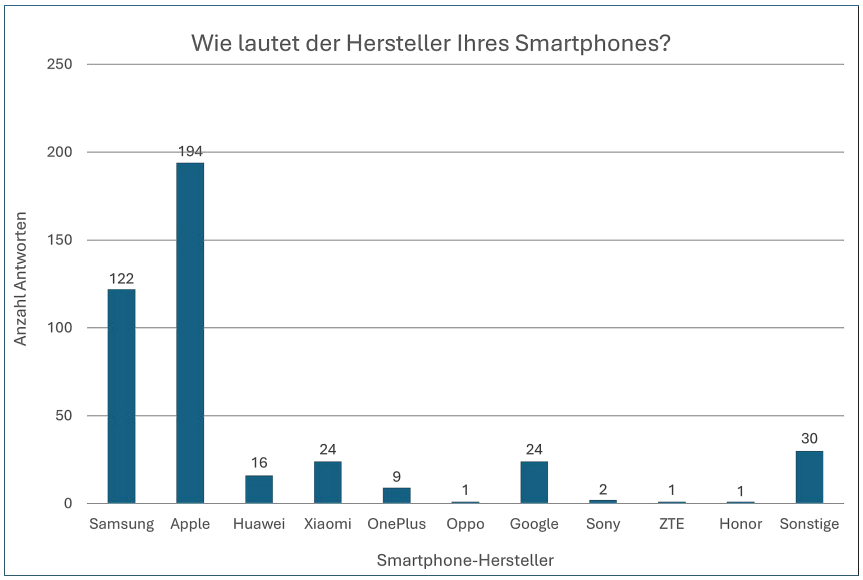


Abbildung 3.3: Auswertung der Ergebnisse von Frage 2 (Eigene Darstellung)

Zudem nutzten 30 Teilnehmer das freie Antwortfeld, was 7,1% aller Stimmen entspricht. In der Tabelle 3.1 werden die sonstigen Antworten nach Häufigkeit sortiert dargestellt:

Smartphone-Hersteller	Antworten
Motorola	10
Fairphone	8
NOTHING	3
Nokia	2
Gigaset	2
Blackberry	1
Poco	1
DOOGEE	1
Shiftphone	1
Irrelevante Angabe	1

Tabelle 3.1: Auswertung der Ergebnisse von Frage 2: „Sonstiges“ (Eigene Darstellung)

Unter „Sonstiges“ entfielen zehn Stimmen auf Motorola, acht Stimmen auf Fairphone und drei Stimmen auf NOTHING. Jeweils zwei Teilnehmer gaben an, ein Nokia- bzw. ein Gigaset-Smartphone zu besitzen. Die Hersteller Blackberry, Poco, DOOGEE und Shiftphone wurden jeweils einmal genannt. Eine Antwort enthielt eine nicht relevante Eingabe.

3. Frage: Ist Ihr Smartphone mithilfe einer Gerätesperre gegen unbefugten Zugriff gesichert?

Die dritte Frage beantworteten alle 424 Teilnehmer, die bei der ersten Frage angegeben haben, dass sie im Besitz eines Smartphones sind. Von diesen gaben 407 Teilnehmer an, dass ihr Smartphone mit einer Gerätesperre gesichert ist, während 17 Teilnehmer die Frage verneinten. Somit sind 96% der Geräte gesichert und 4% ungesichert. Die Abbildung 3.4 zeigt die Ergebnisse dieser Frage.

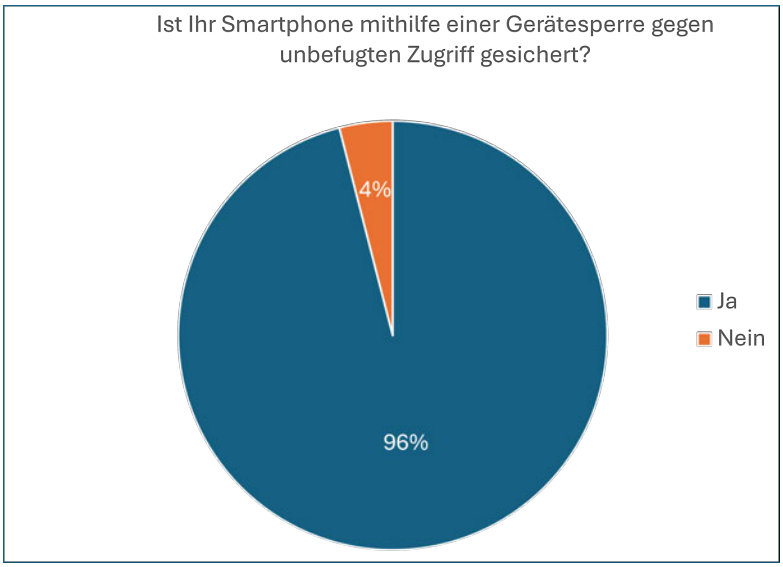


Abbildung 3.4: Auswertung der Ergebnisse von Frage 3 (Eigene Darstellung)

4. Frage: Welche Art von Gerätesperre ist an Ihrem Gerät eingestellt?

Diese Frage wurde nur den Teilnehmern gestellt, die bei der ersten Frage angegeben haben, ein Smartphone zu besitzen und bei der dritten Frage bestätigt haben, dass ihr Smartphone mit einer Gerätesperre gesichert ist. Von diesen 407 Personen wählten 186 (45,7%) die Gesichtserkennung und 171 (42%) die Fingerabdruckerkennung als Sperrart. In der Abbildung 3.5 werden die Resultate der vierten Frage veranschaulicht.

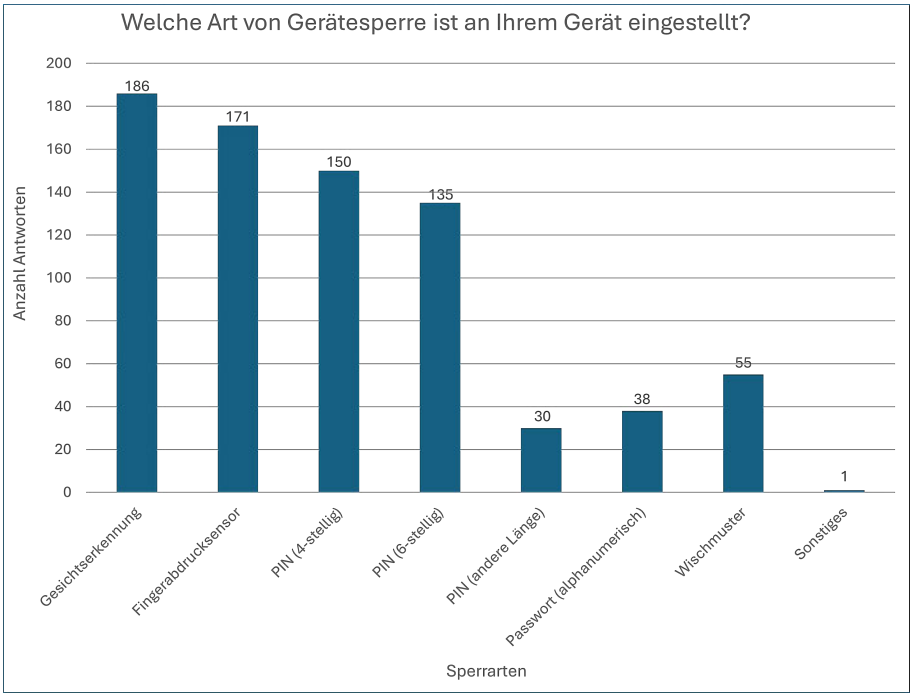


Abbildung 3.5: Auswertung der Ergebnisse von Frage 4 (Eigene Darstellung)

Daraus ergibt sich, dass 87,7% der Befragten eine biometrische Sperrart auf ihrem Smartphone verwenden. Die drei zahlenbasierten Sperrarten, nämlich die vierstellige PIN, die sechsstellige PIN und die PIN mit anderer Länge, erhielten 150, 135 und 30 Stimmen. Dies entspricht 36,9% für die

vierstellige, 33,2% für die sechsstellige und 7,4% für anderweitige PINs. Insgesamt entschieden sich somit 77,4% der Teilnehmer für eine zahlenbasierte Sperrart. Ein alphanumerisches Passwort wurde von 38 Teilnehmern genutzt, was 9,3% der Befragten entspricht. Weitere 55 Teilnehmer (13,5%) gaben an, ein Wischmuster als Sperrart zu verwenden. Eine Person wählte das offene Antwortfeld, gab jedoch keine Sperrart an, weshalb diese Antwort nicht weiter berücksichtigt wird.

5. Frage: Haben Sie jemals ein Passwort für ein Gerät oder einen Online-Dienst auf der Grundlage persönlicher Informationen erstellt?

Da sich diese Frage nicht ausschließlich auf Smartphones, sondern allgemein auf technische Geräte und Online-Dienste bezieht, wurde sie allen 430 Teilnehmern der Umfrage gestellt. 64,4% der Befragten, das sind 277 Personen, gaben an, bereits ein oder mehrere Passwörter auf Grundlage persönlicher Informationen erstellt zu haben. Etwas mehr als ein Drittel der Teilnehmer (35,6%, 153 Personen) verneinten diese Frage. Die Abbildung 3.6 stellt die Ergebnisse von Frage 5 dar.

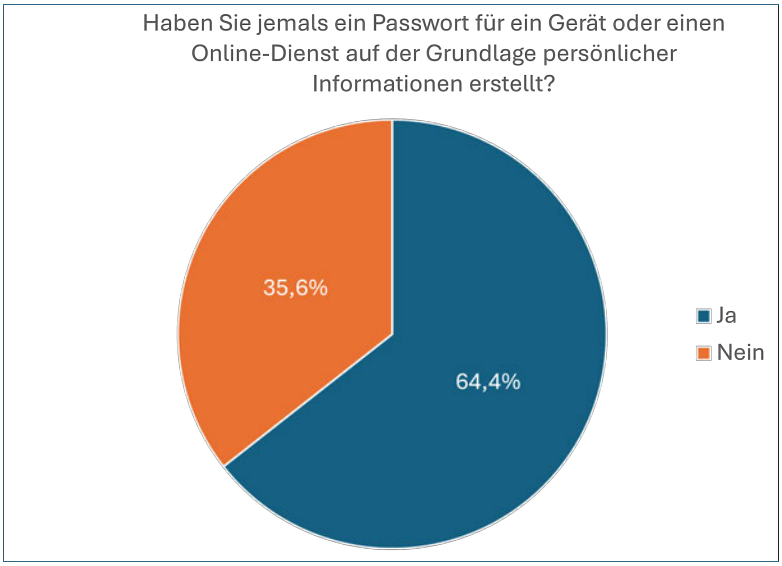


Abbildung 3.6: Auswertung der Ergebnisse von Frage 5 (Eigene Darstellung)

Diese Frage bildet die Grundlage für die sechste Frage, welche darauf abzielt, dieses Thema detaillierter zu untersuchen.

6. Frage: Auf Grundlage welcher persönlichen Informationen haben Sie in der Vergangenheit ein Passwort erstellt?

Die sechste Frage wurde an die 277 Teilnehmer gestellt, die die fünfte Frage mit „Ja“ beantwortet haben. Zur Auswahl standen zwölf vordefinierte Antwortmöglichkeiten sowie ein offenes Antwortfeld. Eine Mehrfachauswahl war bei dieser Frage möglich. Die meisten Stimmen erhielt die Antwortmöglichkeit „Eigenes Geburtsdatum“ mit 116 Personen. Dies bedeutet, dass 41,9% der Umfrageteilnehmer bereits ein oder mehrere Passwörter erstellt haben, in denen das eigene Geburtsdatum integriert wurde. Die Auswertung dieser Frage ist in Form eines Balkendiagramms in der Abbildung 3.7 zu sehen.

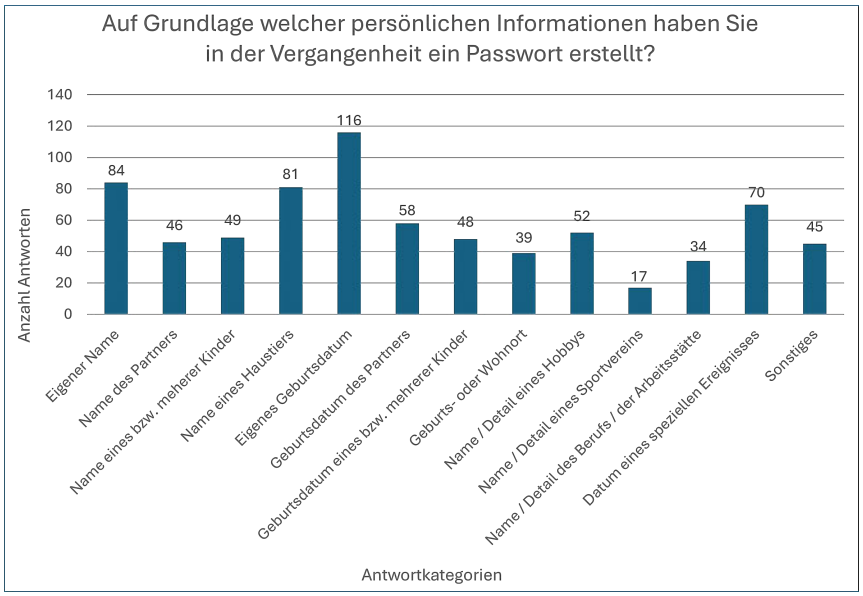


Abbildung 3.7: Auswertung der Ergebnisse von Frage 6 (Eigene Darstellung)

Die zweit-, dritt- und viertmeisten Antworten entfielen auf die Optionen „Eigener Name“ mit 84 Stimmen (30,3%), „Name eines Haustiers“ mit 81 Stimmen (29,2%) und „Datum eines speziellen Ereignisses“ mit 70 Stimmen (25,3%). Die nächsten sieben Antwortmöglichkeiten lagen mit ihren Stimmen nahe beieinander und erhielten jeweils zwischen 21% und 12% der Stimmen. So wählten 20,9% der Teilnehmer „Geburtsdatum des Partners/der Partnerin“, 18,8% entschieden sich für „Name oder Detail eines Hobbys“, 17,7% für „Name eines bzw. mehrerer Kinder“ und 17,3% für „Geburtsdatum eines oder mehrerer Kinder“. Weiterhin erhielten „Name des Partners/der Partnerin“, „Geburts- oder Wohnort“ und „Name oder Detail des Berufs bzw. der Arbeitsstätte“ jeweils 16,6%, 14,1% und 12,3% der Stimmen. Die wenigsten Stimmen unter allen zwölf Möglichkeiten erhielt die Option „Name oder Detail eines Sportvereins“ mit 17 Stimmen, was 6,1% aller Teilnehmer entspricht.

Weitere 45 Teilnehmer (16,3%) entschieden sich für „Sonstiges“ und nutzten das offene Antwortfeld. Diese Antworten wurden thematisch zusammengefasst und in der Tabelle 3.2 dargestellt.

Kategorie	Antworten
Name oder Details von Verwandten	14
Name oder Details von Freunden	9
Ortsnamen mit persönlichem Bezug	9
Eigener Spitz- oder Kosename	5
Eigenes Autokennzeichen	4
Telefonnummern und Mail-Adressen	4
Irrelevante Angaben	3

Tabelle 3.2: Auswertung der Ergebnisse von Frage 6: „Sonstiges“ (Eigene Darstellung)

7. Frage: Nutzen Sie gleiche Passwörter bei verschiedenen Online-Diensten und/oder technischen Geräten?

Die Frage nach der Nutzung gleicher Passwörter wurde von allen 430 Umfrageteilnehmern beantwortet. 289 Personen gaben an, dass sie gleiche Passwörter bei verschiedenen Online-Diensten und/oder technischen Geräten verwenden, während 141 Personen dies verneinten. Somit kann festgestellt werden, dass weniger als ein Drittel der Befragten vermeidet, gleiche Passwörter zu nutzen. In der Grafik 3.8 wird die Verteilung der Antworten in einem Kreisdiagramm dargestellt.

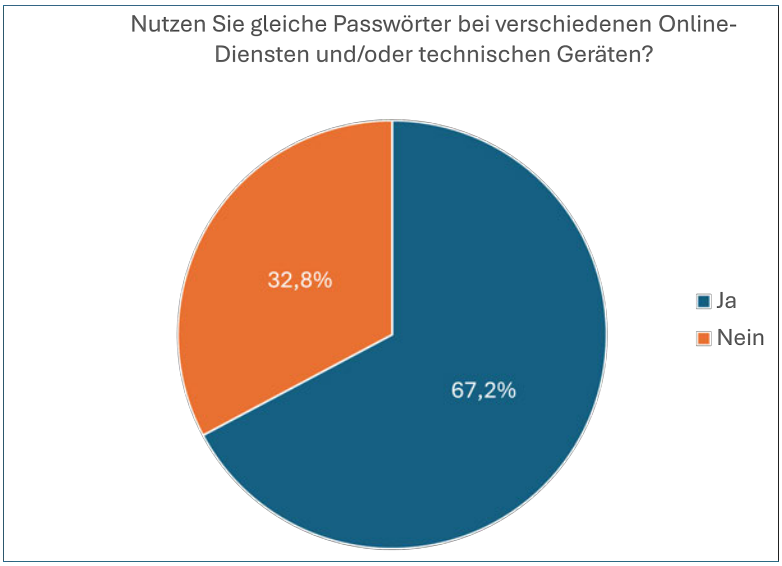


Abbildung 3.8: Auswertung der Ergebnisse von Frage 7 (Eigene Darstellung)

8. Frage: Nutzen Sie einen Passwortmanager zum Speichern Ihrer verschiedenen Passwörter?

Auch die achte Frage des Fragebogens wurde allen 430 Teilnehmern gestellt. Dabei gaben 265 Teilnehmer an, einen Passwortmanager zur Verwaltung ihrer Passwörter zu nutzen, während 165 Teilnehmer dies verneinten. Somit antworteten 61,6% der Befragten mit „Ja“ und 38,4% mit „Nein“. Die Abbildung 3.9 zeigt die prozentuale Verteilung der Antworten.

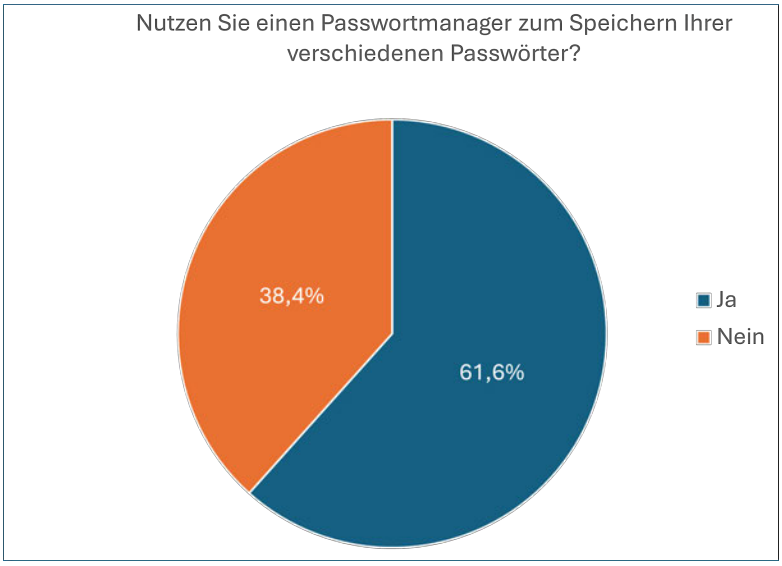


Abbildung 3.9: Auswertung der Ergebnisse von Frage 8 (Eigene Darstellung)

9. Frage: Welchen bzw. welche Passwortmanager nutzen Sie?

Bei der neunten Frage handelt es sich um eine offene Frage ohne Antwortvorgaben, die den 265 Umfrageteilnehmern gestellt wurde, die die Frage 8 mit „Ja“ beantwortet haben. Da die Antworten sehr vielfältig waren, wurden die Ergebnisse bereinigt. Diese Bereinigung umfasste unter anderem die Korrektur von Rechtschreibfehlern und das Filtern von Angaben, die keine relevanten Antworten auf die Frage darstellten. Zur ersten groben Übersicht der bereinigten Ergebnisse wurde die in Abbildung 3.10 dargestellte Wordcloud erstellt.

Abbildung 3.10: Wordcloud zu den Ergebnissen von Frage 9 (Eigene Darstellung)

Eine Wordcloud ist ein Visualisierungswerkzeug, bei dem häufige Antworten größer und weniger häufige Antworten kleiner dargestellt werden. Dadurch kann der Leser einen schnellen ersten Überblick über die Antworten und deren Häufigkeiten gewinnen. Allerdings sind Wordclouds nicht dafür geeignet, exakte Statistiken darzustellen. [47]

Aus diesem Grund werden alle Antworten, die häufiger als zweimal genannt wurden, zusätzlich in einem Balkendiagramm dargestellt. Dieses Diagramm ist in Abbildung 3.11 zu sehen.

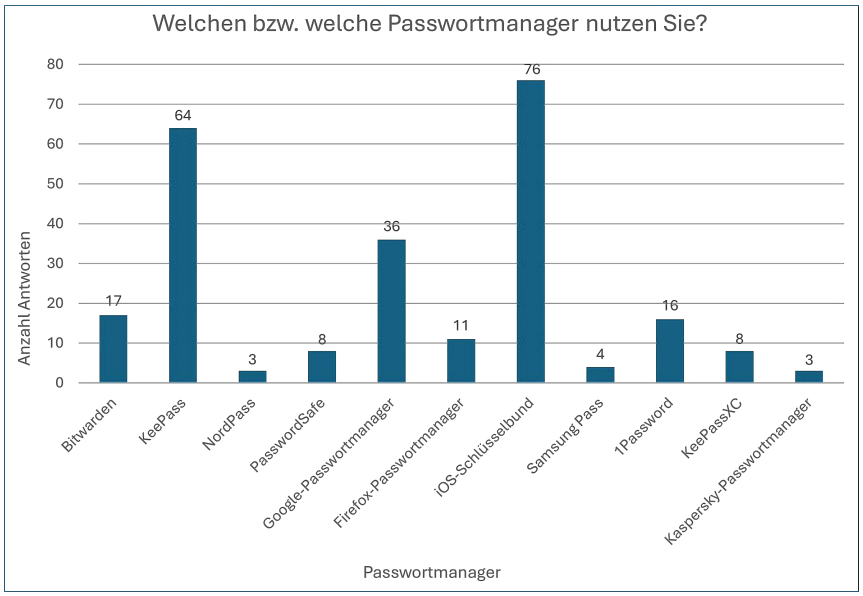


Abbildung 3.11: Auswertung der Ergebnisse von Frage 9 (Eigene Darstellung)

Neben den elf in Abbildung 3.11 dargestellten Antworten, die jeweils mindestens dreimal genannt wurden, gibt es 15 Antworten, die nur ein- oder zweimal erwähnt wurden. Diese sind in der Tabelle 3.3 zusammengefasst.

Passtwortmanager	Antworten		Passtwortmanager	Antworten
SafeInCloud	2		S-Trust	1
Enpass	2		Microsoft Edge Wallet	1
LastPass	2		Ecosia Passwortmanager	1
Avira Password Manager	2		Roboform	1
Keeper Passwortmanager	2		Opera-Passwortmanager	1
Password Depot	1		Vaultwarden	1
KeePassDX	1		Nextcloud Passwortmanager	1
Norton Passwortmanager	1		Irrelevante Angaben	4

Tabelle 3.3: Auswertung der Ergebnisse von Frage 9 mit wenigen Nennungen (Eigene Darstellung)

10. Frage: Wie würden Sie Ihr grundsätzliches Vorgehen beim Erstellen von Passwörtern beschreiben?

Die zehnte Frage ist ebenfalls eine offene Frage mit einem freien Antwortfeld. Aufgrund der Vielfalt der Antworten wurden diese in verschiedene Kategorien eingeteilt. Nach einer manuellen Analyse der Ergebnisse ergaben sich die folgenden Antwortkategorien:

- Begriff + Zahl / Sonderzeichen
- Gleiche / ähnliche / leicht veränderte Passwörter
- Lange Passwörter
- Generierte Passwörter
- Besondere Erstellungsmethoden
- Irrelevante Angaben

Im Abschnitt „Begriff + Zahl / Sonderzeichen“ werden Antworten kategorisiert, die auf die Erstellung von Passwörtern mithilfe eines Begriffs sowie Zahlen und/oder Sonderzeichen hinweisen. Insgesamt gaben 133 Personen Antworten, die dieser Kategorie zugeordnet werden konnten. Die Kategorie „Gleiche / ähnliche / leicht veränderte Passwörter“ umfasst Antworten, die darauf hinweisen, dass die Teilnehmer überwiegend oder ausschließlich gleiche Passwörter verwenden, welche höchstens leicht verändert werden. In diese Kategorie fallen 88 Antworten.

Unter „Lange Passwörter“ werden Antworten kategorisiert, bei denen die Teilnehmer angeben, dass sie vor allem auf die Länge der Passwörter achten. Diese Kategorie umfasst die Antworten von 31 Teilnehmern. Die Kategorie „Generierte Passwörter“ beinhaltet Antworten, bei denen die Passwörter mithilfe von Passwortmanagern oder Passwortgeneratoren erstellt werden. Darunter fallen beispielsweise auch die Passwortvorschläge von iOS bei der Vergabe neuer Passwörter. 92 Antworten entsprechen diesem Kriterium.

In die Kategorie „Besondere Erstellungsmethoden“ werden Antworten eingeordnet, bei denen die Teilnehmer spezifische Methoden und/oder Algorithmen zur Passworterstellung angeben. Beispiele hierfür sind das Zusammensetzen aller ersten Buchstaben der Wörter eines Satzes oder die Bildung eines Passworts aus einem festen Präfix und Suffix sowie einem dienstspezifischen Teil dazwischen.

Insgesamt wurden 77 Antworten dieser Kategorie zugeordnet. Unter „Irrelevante Angaben“ werden schließlich Antworten zusammengefasst, die keiner spezifischen Kategorie zugeordnet werden können und keine aussagekräftigen Informationen enthalten. Neun Antworten fielen in diese Kategorie.

Die Verteilung der Antwortkategorien wird in Abbildung 3.12 dargestellt.

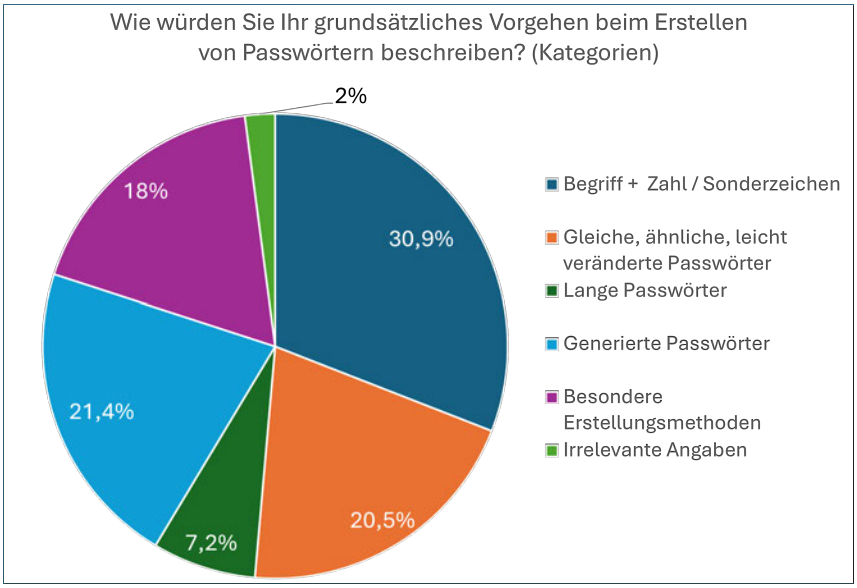


Abbildung 3.12: Auswertung der Ergebnisse von Frage 10 (Eigene Darstellung)

Im Folgenden werden exemplarisch für jede Kategorie zwei Antworten dargestellt. Etwaige Rechtschreibfehler wurden aus den Original-Antworten übernommen.

- **Begriff + Zahl / Sonderzeichen**
  - *„Etwas das ich gut kenne und leicht zu merken ist plus eine Jahreszahl und Satzzeichen“*
  - *„Wort, zeichen , zahlen Groß und Kleinschreibung “*
- **Gleiche / ähnliche / leicht veränderte Passwörter**
  - *„ich nehme oft die selben bzw. ähnliche Passwörter“*
  - *„Einfach zu merken, oft das gleiche“*
- **Lange Passwörter**
  - *„Grundsätzlich haben meine Passwörter mindestens 12 Zeichen“*
  - *„Minimum 16 Zeichen (sofern bei Applikation/Webservice möglich), alphanumerisch, kein Teil größer 4 Zeichen aus einer gängigen Sprache“*
- **Generierte Passwörter**
  - *„Ich lasse meinen Passwortmanager ein zufälliges Passwort generieren“*
  - *„Mit Passwortmanager generieren, dabei maximal mögliche Länge, Zeichen etc. voll ausreizen. “*
- **Besondere Erstellungsmethoden**
  - *„Sätze und Anfangsbuchstaben davon nehmen.“*
  - *„Anfangsbuchtabens eines liedes(immer gleich) +individuelle anpssung an die jeweilige mit pw zu versehene homepage“*
- **Irrelevante Angaben**
  - *„Individuell“*
  - *„Zufällig“*

Demografische Frage 1: Wie alt sind Sie?

Das Alter der Teilnehmer reicht von 15 bis 75 Jahren. Zur besseren Übersicht wurden die Altersangaben in 10-Jahres-Schritte eingeteilt. In Abbildung 3.13 wird die Altersverteilung der Umfrageteilnehmer anschaulich dargestellt.

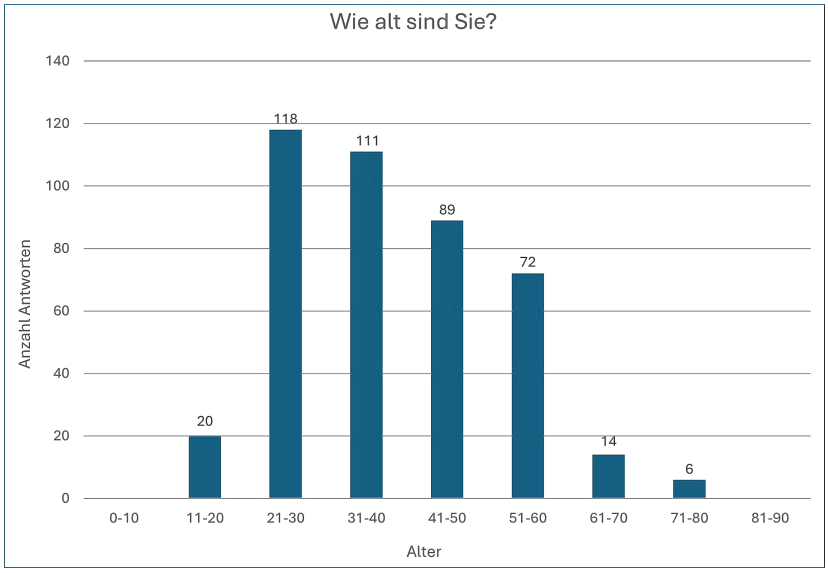


Abbildung 3.13: Altersverteilung der Teilnehmer (Eigene Darstellung)

Das durchschnittliche Alter aller Teilnehmer (arithmetisches Mittel) beträgt 38,6 Jahre, der Median liegt bei 37 Jahren.

Demografische Frage 2: Wie ist Ihr Geschlecht?

Die Auswertung der Frage nach dem Geschlecht der Teilnehmer zeigt, dass etwas mehr als die Hälfte der Teilnehmer weiblich sind (228 Personen, 53%). 46,1% der Teilnehmer (198 Personen) sind männlich. Vier Teilnehmer ordnen sich selbst in die Gruppe „Divers“ ein. Die Abbildung 3.14 zeigt die Geschlechterverteilung der Teilnehmer in einem Kreisdiagramm.

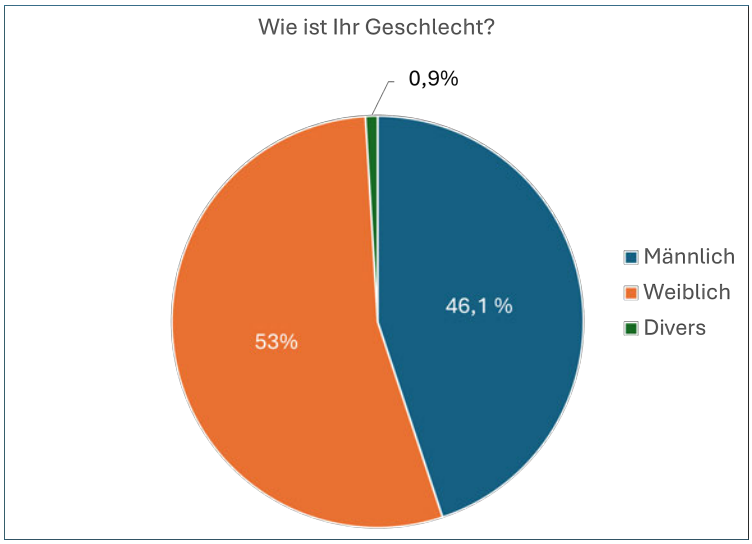


Abbildung 3.14: Verteilung des Geschlechts der Teilnehmer (Eigene Darstellung)

3.6 Interpretation der Ergebnisse

Nachdem im Kapitel 3.5 die Ergebnisse der Online-Umfrage objektiv analysiert wurden, sollen diese nun interpretiert werden. Hierbei werden die Ergebnisse in den richtigen Kontext gesetzt und mit dem aktuellen Stand der Wissenschaft verglichen. Dadurch können beispielsweise Trends oder Veränderungen im Umgang mit Passwortsicherheit aufgezeigt werden. Um die Daten effektiv analysieren zu können, wurden die Ergebnisse im Dateiformat Comma-separated values (CSV) vom empirio-Portal exportiert und in eine SQLite-Datenbank überführt. Anschließend wurden die Daten im Tool DB Browser for SQLite (DB4S) mit geeigneten SQLite-Abfragen umfassend analysiert.

Die erste Frage nach dem Smartphone-Besitz bejahten 98,6% der Teilnehmer. Nur sechs der 430 Personen gaben an, aktuell kein Smartphone zu besitzen. Laut einer Studie zur Smartphone-Nutzung, die die Nutzung nach Altersgruppen untersuchte, nutzten im Jahr 2021 88,8% der Befragten ein Smartphone [1]. Der Anteil der Smartphone-Nutzer in meiner Online-Umfrage liegt somit etwa 10% höher als der Durchschnitt im Jahr 2021. Dies könnte darauf zurückzuführen sein, dass die Altersstruktur meiner Umfrage unausgeglichen ist. Betrachtet man nur die Altersgruppe von 20 bis 59 Jahren, zeigt sich ein nur leicht erhöhtes Ergebnis gegenüber der Studie. 390 der 430 Teilnehmer liegen in diesem Altersbereich. Von diesen 390 Teilnehmern gaben 386 an, ein Smartphone zu besitzen, während vier Teilnehmer in diesem Altersbereich die Frage verneinten. Dies ergibt einen Prozentsatz von über 98%, während bei der Studie aus dem Jahr 2021 95% in dieser Altersgruppe angaben, ein Smartphone zu besitzen. In dieser Altersgruppe liegt das Ergebnis der Online-Umfrage also fast 4% höher. Dies könnte auch mit der Aktualität der Studie erklärt werden, da sich dieser Wert aufgrund der fortschreitenden Digitalisierung innerhalb von drei Jahren durchaus erhöhen kann. [1]

In der zweiten Frage wird die Verteilung der Smartphone-Hersteller und der damit verbundenen Betriebssysteme untersucht. In der Online-Umfrage gaben mehr als 45% der Teilnehmer an, ein Smartphone von Apple zu besitzen. Zudem nutzen 28,8% der Befragten ein Samsung-Smartphone. Somit entfallen über 73% der verwendeten Smartphones auf diese beiden Hersteller. Alle anderen Hersteller erhielten deutlich weniger Stimmen, wobei sich Google und Xiaomi mit jeweils nur 5,7% den dritten Platz teilen. Laut einer Studie, die die weltweiten Marktanteile der führenden Smartphone-Hersteller untersucht, belegen diese beiden Hersteller ebenfalls die ersten beiden Plätze bei den Verkaufszahlen. Die Unterschiede zwischen den Marktanteilen sind jedoch in der Online-Umfrage deutlich ausgeprägter. So betrug der Marktanteil von Samsung im 1. Quartal 2024 weltweit 20,8%, während Apple auf 17,3% kam. [48] Die großen prozentualen Unterschiede lassen sich vor allem dadurch erklären, dass die Studie weltweite Verkäufe untersucht, während sich die Online-Umfrage fast ausschließlich auf Deutschland bzw. den deutschsprachigen Raum konzentriert. Insbesondere im asiatischen Raum dürfte der Absatz von Apple-Smartphones deutlich geringer sein als hierzulande. Gründe hierfür sind unter anderem geowirtschaftlicher Natur, wie das Handelsblatt in einem Artikel aus dem April 2024 darlegt [49]. Außerdem dürfte die Verbreitung von asiatischen Marken wie etwa Xiaomi oder Huawei in Deutschland deutlich geringer sein als in Asien.

Die Frage nach einer eingerichteten Gerätesperre am Smartphone bejahten 96% der Teilnehmer der Online-Umfrage. 4% der Befragten gaben an, keine Gerätesperre zu nutzen. Auffallend ist, dass das Durchschnittsalter (arithmetisches Mittel) der Teilnehmer, die diese Frage mit „Nein“ beantworteten, bei 43 Jahren liegt, während das arithmetische Mittel aller Teilnehmer bei knapp über 38

Jahren liegt. Dies könnte darauf hindeuten, dass ältere Menschen im Durchschnitt weniger Wert auf die Sicherheit ihrer Smartphones legen oder ein geringeres Bewusstsein für entsprechende Sicherheitsmaßnahmen haben als jüngere Menschen. Um diese These zu stützen, wären jedoch umfangreichere Untersuchungen erforderlich, die den Rahmen dieser Arbeit überschreiten würden. Eine Studie aus dem Jahr 2020 ergab, dass 92% der Smartphones in Deutschland mit einer Gerätesperre gesichert sind [2]. Damit liegt das Ergebnis der Studie mit einer Abweichung von 4% sehr nahe an dem Ergebnis der Online-Umfrage.

In der vierten Frage geht es um die statistische Verteilung der verschiedenen Sperrarten bei Smartphones. Dabei entfielen 87,7% auf die biometrischen Sperrarten Gesichtserkennung und Fingerabdrucksensor. Für eine zahlenbasierte Sperrart entschieden sich 77,4% der Teilnehmer, und 9,3% der Befragten gaben an, ein alphanumerisches Passwort zu benutzen. Da eine biometrische Sperrart nicht allein eingestellt werden kann, sondern immer mit einer nicht-biometrischen Sperrart kombiniert werden muss, gab es mehr Antworten als Teilnehmer.

Von besonderem Interesse hinsichtlich der Forschungsfrage dieser Arbeit ist die Nutzung von alphanumerischen Passwörtern. Dieser Wert liegt mit 9,3% etwas höher als in einer Studie aus dem Jahr 2019, bei der 7% der Befragten angaben, ein alphanumerisches Passwort zu benutzen [2]. Dies könnte einen Trend darstellen, der darauf hinweist, dass zukünftig mehr Menschen ein alphanumerisches Passwort als Sperrart für ihr Smartphone verwenden. Ein Grund für das Steigen dieses Wertes könnte das gestiegene Sicherheitsbewusstsein der Bevölkerung in den letzten Jahren sein. So ist die Tatsache, dass lange Passwörter im Allgemeinen sicherer sind als kurze Zahlenkombinationen, heute vermutlich bekannter als noch vor vier Jahren. Ein weiterer Grund für die Zunahme könnte sein, dass durch die ebenfalls gestiegene Nutzung von biometrischen Sperrarten das Passwort nur noch selten eingegeben werden muss. Vor der Einführung von Gesichtserkennung und Fingerabdrucksensoren musste das Passwort bei jedem „Aufwecken“ des Smartphones eingegeben werden, was viele Nutzer als umständlich empfunden haben könnten. Durch die parallele Nutzung einer biometrischen Sperrart muss das Passwort jedoch nur selten eingegeben werden, beispielsweise nach einem Neustart oder wenn die biometrische Entsperrung mehrmals fehlschlug.

Für die erste These könnte sprechen, dass das durchschnittliche Alter von Menschen, die ein Passwort nutzen, mit 35,9 Jahren niedriger ist als der Durchschnitt der Menschen (38 Jahre), die kein Passwort nutzen. Diese Zahlen zeigen, dass die Problematik mit Brute-Force-Angriffen auf Passwörter existent ist und dass die Anzahl an Smartphones mit alphanumerischen Passwörtern in Zukunft voraussichtlich steigen wird.

Bei der fünften Frage ging es darum, ob die Umfrageteilnehmer bereits einmal ein Passwort auf Basis persönlicher Informationen erstellt haben. Diese Frage bejahten 64,4% der Befragten, während die restlichen 35,6% sie verneinten. Bei einer ähnlichen Fragestellung von web.de aus dem Jahr 2021 wählten bei der Single-Choice-Frage „Wie erstellen/generieren Sie Ihr Passwort?“ 17% der Befragten die Option „Ich nutze persönliche Informationen wie Geburtsdatum, (Spitz-)Namen, Haustiernamen oder Telefonnummern“ [50]. Das sind deutlich weniger als bei der Online-Umfrage.

Ein Grund für diese große Differenz könnte die Art der Fragestellung sein. Während die Frage in der Online-Umfrage eine dichotome Frage (Ja/Nein) ist, die die Teilnehmer direkt mit dieser Thematik konfrontiert und zum Nachdenken anregt, handelt es sich in der Umfrage von web.de nur um eine Option unter vielen. Außerdem konnte bei dieser Umfrage jeder Teilnehmer nur eine Option wählen,

sodass beispielsweise jemand, der Passwörter manchmal mithilfe von Fantasiewörtern erstellt und manchmal auf Basis von persönlichen Informationen, möglicherweise nur die Option „Ich verwende Fantasiewörter“ auswählt. [50]

Ein weiterer Grund könnte darin bestehen, dass Internetnutzer heute mit deutlich mehr Passwörtern konfrontiert sind als noch vor einigen Jahren. Daraus könnte der Trend entstehen, dass Menschen häufiger auf gleiche und einfach zu merkende Passwörter zurückgreifen, um den Überblick zu bewahren und Passwörter nicht zu vergessen. Um diese These zu beweisen, wären jedoch weiterführende Untersuchungen notwendig. Eine Studie zum Thema Passwortsicherheit kam jedoch bereits 2019 zu dem Ergebnis, dass es 75% der Befragten frustriert, den Überblick über alle Passwörter zu behalten [35].

Die sechste Frage schließt thematisch direkt an die fünfte Frage an und richtet sich an die 277 Teilnehmer, die die vorherige Frage mit „Ja“ beantwortet haben. Hier wurde gefragt, auf Basis welcher persönlichen Informationen die Teilnehmer bereits einmal ein Passwort erstellt haben. Dabei wählten 30,3% der Befragten die Antwortmöglichkeit „Eigener Name“ aus. Dieser Wert liegt etwas höher als in der bereits erwähnten Studie aus dem Jahr 2019, bei der 22% der Teilnehmer angaben, ihren eigenen Namen für ein Passwort verwendet zu haben. Die Zustimmungswerte für die Antwortmöglichkeiten „Namen eines oder mehrerer Kinder“ bzw. „Name des Partners“ sind mit 17,7% zu 14% bzw. 16,6% zu 15% nur geringfügig höher als in der Studie von Google und Harris Poll. [35]

Anders sieht es bei der Einbeziehung des Namens eines Haustiers aus, hier ist der Wert aus der Studie mit 33% etwas höher als die Zustimmung in der Online-Umfrage, bei der 29,2% der Befragten diese Antwortmöglichkeit auswählten [35]. Auffällig ist, dass sich die beiden vorgegebenen Antworten mit den höchsten Zustimmungen auf die Person selbst beziehen, nämlich der eigene Name (30,3%) und das eigene Geburtsdatum (41,9%). Unter Einbeziehung der Tatsache, dass diese Frage an 64,4% aller Umfrageteilnehmer gestellt wurde, gab somit insgesamt mehr als jeder Vierte (27%) an, das eigene Geburtsdatum in Passwörtern verwendet zu haben.

Diese Erkenntnisse sind von großer Bedeutung, da sie zeigen, dass allein mit der Kenntnis von Name und Geburtsdatum des Smartphone- oder Computerbesitzers eine realistische Chance besteht, das Passwort mithilfe eines Brute-Force-Angriffs zu knacken. Den vierthöchsten Zustimmungswert erhielt die Antwortmöglichkeit „Datum eines speziellen Ereignisses“ mit 25,3%. Alle anderen Antworten liegen im Bereich zwischen 21% und 12,3%. Einzig die Option „Name oder Detail eines Sportvereins“ liegt mit 6,1% abgeschlagen auf dem letzten Platz.

Für die praktische Arbeit von Strafverfolgungsbehörden bedeuten diese Werte, dass es durchaus sinnvoll für Ermittler und IT-Forensiker sein kann, persönliche Informationen des Beschuldigten im Rahmen des Ermittlungsprozesses zu notieren. Wird beispielsweise bei einer Hausdurchsuchung ein Haustier festgestellt, so kann es wertvoll sein, den Namen des Haustiers zu erfragen. Auch kann der Ermittler die Namen und Geburtsdaten von Partner bzw. Partnerin und ggf. den Kindern der beschuldigten Person notieren, da diese möglicherweise für einen anstehenden Brute-Force-Angriff relevant sein können.

Daran anschließend folgt die siebte Frage nach der Nutzung von gleichen Passwörtern bei verschiedenen Online-Diensten bzw. technischen Geräten. Diese Frage wurde von mehr als zwei Dritteln der Befragten bejaht, während 32,8% der Teilnehmer sie verneinten. In einer ähnlichen Studie

aus dem März 2023 gaben 51% der Teilnehmer an, teilweise die gleichen Passwörter für mehrere Online-Dienste zu verwenden, während 6% der Befragten angaben, für jeden Online-Dienst das gleiche Passwort zu verwenden. Diese Zahlen sind somit geringfügig niedriger als die Zahlen der Online-Umfrage. [51]

Die Frage nach der Bedeutung individueller Passwörter für jeden Online-Dienst wird in der Wissenschaft unterschiedlich beantwortet. So bezeichnet das BSI die Aussage „Ein individuelles Passwort pro Account!“ als Tipp zur Passwortsicherheit, der von jedem Internetnutzer beherzigt werden soll [52]. Anders sehen dies die Forscher der Ruhr-Universität Bochum in ihrem News-Artikel „Sieben Mythen über Passwörter“. Sie bezeichnen es als Mythos, dass man nie zweimal das gleiche Passwort benutzen sollte. Dies wäre zwar in einer idealen Welt der Fall, jedoch nicht praktisch umsetzbar. Stattdessen empfehlen sie, mit Ausnahme wichtiger Accounts wie Bankzugänge, Online-Accounts in Gruppen einzuteilen und für jede Gruppe ein individuelles Passwort zu nutzen. [53]

In der achten Frage geht es um die Nutzung von Passwortmanagern. Das BSI definiert Passwortmanager als Programme, die dabei helfen, Benutzernamen und verschiedene Passwörter zu verwalten [54]. Dabei gilt es, verschiedene Arten zu unterscheiden. Zum einen gibt es Desktop-basierte Passwortmanager, die auf einem Betriebssystem installiert werden und dort unabhängig genutzt werden. Beispiele hierfür sind 1Password oder KeePass. Moderne Smartphones haben häufig in das Betriebssystem integrierte Passwortmanager, wie den iOS-Schlüsselbund, der direkt in das Apple-Betriebssystem implementiert ist. Des Weiteren gibt es browserinterne Passwortmanager, bei denen ein Tool zur Verwaltung von Passwörtern in den Browser integriert ist. Beispiele hierfür sind Google Chrome, Mozilla Firefox und der Opera Browser. Häufig haben diese Tools auch eine Funktion zur Generierung von Passwörtern inkludiert.

In der Online-Umfrage wurde nach der Nutzung von Passwortmanagern gefragt. Dabei bejahten 61,6% der Teilnehmer die Frage nach der Nutzung mindestens eines solchen Tools, während 38,4% diese verneinten. Auffällig ist, dass das Durchschnittsalter der Nutzer von Passwortverwaltungstools mit 34 Jahren deutlich geringer ist als das Durchschnittsalter der Personen, die keine Passwortmanager verwenden (43 Jahre). Dies könnte darauf zurückzuführen sein, dass älteren Menschen die Definition und der Begriff möglicherweise nicht bekannt sind. Ein weiterer Grund könnte sein, dass die IT-Sicherheitskompetenzen bei jungen Menschen aufgrund gesellschaftlicher Faktoren tendenziell höher sind als bei älteren Menschen.

In einer Studie von Deutschland sicher im Netz (DsiN) aus dem Jahr 2021 wurden die Teilnehmer nach Bekanntheit und Nutzung von Passwortmanagern gefragt. Dabei antwortete zwar eine große Mehrheit (89,6%), dass sie derartige Tools kennen, jedoch stimmten nur 31,1% der Teilnehmer der Frage nach der Nutzung von Passwortmanagern zu. [55] Der Anstieg um etwa 30% innerhalb der drei Jahre spricht dafür, dass Tools zur Verwaltung von Passwörtern in den letzten Jahren an Popularität gewonnen haben. Dies könnte langfristig zur Erhöhung der Passwort-Sicherheit in der Bevölkerung beitragen.

Die neunte Frage im Fragebogen (Welchen bzw. welche Passwortmanager nutzen Sie?) baut direkt auf der Vorherige auf und wird nur den Teilnehmern angezeigt, die angegeben haben, einen Passwortmanager zu nutzen. Die beiden mit Abstand am häufigsten gewählten Antworten waren „iOS-Schlüsselbund“ mit 76 Stimmen und „KeePass“ mit 64 Stimmen. Browserinterne Passwortmanager (Google, Firefox, Microsoft Edge und Opera) wurden von 49 Teilnehmern genannt, was 18,5%

der Stimmen entspricht. Diese Zahl erscheint auf den ersten Blick recht gering, wenn man bedenkt, dass die meisten Menschen regelmäßig Browser verwenden. Möglicherweise ist diese geringe Anzahl darauf zurückzuführen, dass viele Menschen beim Speichern von Passwörtern im Browser nicht explizit an die Nutzung eines Passwortmanagers denken, obwohl im Fragebogen ein Hinweis darauf gegeben wurde.

Ein sinnvoller Vergleich mit ähnlichen Umfragen oder Statistiken ist nicht möglich, da diese oft stark veraltet sind und somit an Aussagekraft verloren haben. Aus der Online-Umfrage geht jedoch eindeutig hervor, dass Passwortmanager auf mobilen Endgeräten weit verbreitet und den Nutzern bewusst sind. Schließlich erhielt der in iOS integrierte Schlüsselbund die meisten Stimmen. Bei einigen Antworten gibt es sowohl eine Desktop- als auch eine mobile Variante, was eine eindeutige Zuordnung erschwert. Es kann jedoch angenommen werden, dass zumindest einige der Teilnehmer diese Applikationen auch auf ihrem Smartphone nutzen.

Die letzte Frage befasste sich mit dem grundsätzlichen Vorgehen der Teilnehmer beim Erstellen von Passwörtern. Die Antworten auf diese Frage sind sehr vielfältig und aufgrund der fehlenden Vergleichbarkeit schwer zu interpretieren. Auffällig ist, dass 92 Teilnehmer (21,4%) angaben, zumindest gelegentlich Passwörter von Passwortgeneratoren oder Passwortmanagern erstellen zu lassen. Ob sich diese 21,4% auch direkt auf die Passwort-Zugangssperre von mobilen Endgeräten übertragen lassen, ist fraglich, da bei Smartphones vermutlich eher auf Passwörter zurückgegriffen wird, die der Person auch unterwegs einfallen würden. Etwas mehr als 20% der Befragten wählten Methoden, die der Kategorie „Gleiche, ähnliche, leicht veränderte Passwörter“ zugeordnet wurden. Diese Passwörter sind besonders anfällig für Brute-Force-Angriffe, wobei auch hier nicht gesichert festgestellt werden kann, dass sich die Antworten direkt auf mobile Endgeräte übertragen lassen.

Zusammenfassend lässt sich feststellen, dass die Online-Umfrage viele interessante und für die Forschungsfrage relevante Erkenntnisse geliefert hat. Es wurde grundsätzlich festgestellt, dass Menschen dazu neigen, persönliche Informationen in die Erstellung von Passwörtern einzubeziehen. Diese Erkenntnis ist für die Beantwortung der Forschungsfragen elementar, da sie zeigt, dass Wörterbuchangriffe, deren Wörterbücher mithilfe persönlicher Informationen der betroffenen Person erstellt wurden, eine effektive Möglichkeit zur Optimierung der Brute-Force-Dauer darstellen können. Nicht alle Fragen und Antworten sind direkt für die Forschungsfrage relevant, doch sie tragen dazu bei, einen Gesamteindruck über den aktuellen Stand der Gewohnheiten bei der Passworterstellung und das Sicherheitsbewusstsein der Bevölkerung in Bezug auf Passwörter zu gewinnen. Diese Informationen können dann für weiterführende Überlegungen genutzt werden.

4 Praxisorientierter Vergleich

Nachdem bereits eine Literaturrecherche und eine quantitative Umfrage durchgeführt wurden, soll in den folgenden Kapiteln ein praxisbezogener Vergleich erfolgen.

4.1 Idee und Zielsetzung

Die Idee dieses Vergleichs besteht darin, ein besseres Verständnis dafür zu gewinnen, ob und in welchem Ausmaß persönliche Informationen als Grundlage für Passwörter dienen. Dazu wird eine Vergleichsliste erstellt, die mithilfe eines selbst programmierten Hilfstools mit zwei verschiedenen, öffentlich einsehbaren Passwortlisten aus echten Datenleaks verglichen wird. Im weiteren Verlauf dieser Arbeit wird die selbst erstellte Liste als „Vergleichsliste“ und die Listen aus Datenleaks als „Passwortlisten“ bezeichnet.

Folgende Kategorien sollen in der Vergleichsliste verwendet werden:

- Häufig genutzte Vornamen
- Häufig genutzte Nachnamen
- Namen beliebter Hobbys
- Namen von (international) bekannten Sportvereinen verschiedener Sportarten
- Namen bekannter Städte
- Namen aller Länder der Welt

Die Ergebnisse sollen anschließend in Form von prozentualen Trefferquoten dargestellt und interpretiert werden.

4.2 Layout der Vergleichsliste

Die Vergleichsliste ist eine Unicode Transformation Format – 8 Bits (UTF-8) kodierte Textdatei, die insgesamt 8.978 Begriffe umfasst. Da die Leaks von international genutzten Portalen stammen, werden überwiegend englischsprachige Namen, Sportarten und andere Begriffe verwendet.

Im Folgenden werden die verwendeten Begriffe aufgelistet:

- 1.000 internationale Vornamen (männlich) aus [56]
- 1.000 internationale Vornamen (weiblich) aus [56]
- 100 häufige deutsche Nachnamen aus [57]
- 4.994 häufige US-amerikanische Nachnamen aus [58]
- 414 bekannte europäische Fußballvereine aus [59]
- 64 Teamnamen aus der nordamerikanischen Eishockeyliga (NHL) aus [60]
- 29 Teamnamen aus der nordamerikanischen Baseballliga (MLB) aus [61]
- 42 Teamnamen aus der nordamerikanischen Football Liga (NFL) aus [62]
- 54 Teamnamen aus der nordamerikanischen Basketball Liga (NBA) aus [63]

- 197 bekannte Hobbys (englisch) aus [64]
- 93 bekannte Sportarten (englisch) aus [65]
- 419 große US-Städte aus [66]
- 500 einwohnerstärkste, europäische Städte aus [67]
- Alle Ländernamen (englisch) aus [68]
- Alle Jahreszahlen zwischen 1960 und 2020

Einige Begriffe wurden aufgeteilt, um einen sinnvollen Vergleich zu ermöglichen. So wurde beispielsweise der Name des US-amerikanischen Eishockeyclubs „Anaheim Ducks“ in die beiden Begriffe „Anaheim“ und „Ducks“ aufgespalten. Diese Vorgehensweise ist sinnvoll, da der vollständige Name inklusive Leerzeichen wohl nicht in einem Passwort vorkommen würde. Daher kann die Anzahl der tatsächlichen Begriffe leicht von den in den Quellen angegebenen Begriffen abweichen. Da in einem ersten Testlauf kurze Begriffe aus der Vergleichsliste zu einigen falsch positiven Treffern führten, wurden zudem alle ein- bis dreistelligen Begriffe entfernt. Die finale Vergleichsliste umfasst somit 8.978 Begriffe und wird als „vergleichsliste.txt“ abgespeichert.

4.3 Wahl der Passwortlisten

Um realistische Ergebnisse zu erzielen, werden für den Vergleich keine zusammengesetzten Wörterbücher, sondern echte Passwortlisten aus Datenleaks verwendet. Die erste der beiden Passwortlisten ist die rockyou.txt. Diese Liste enthält 14.341.564 einzigartige Passwörter aus mehr als 32 Millionen geleakten Benutzerkonten des Online-Spiele-Entwicklers RockYou. Der Datenleak stammt aus dem Jahr 2009 und wird seitdem von Sicherheitsforschern, Penetrationstestern und IT-Systemadministratoren zur Überprüfung der Sicherheit von IT-Systemen genutzt. Andererseits ist die Passwortliste aber auch bei Hackern und Cyberkriminellen beliebt, um mittels Brute-Force-Angriffen unbefugten Zugriff auf Online-Dienste zu erlangen. Die rockyou.txt ist in verschiedenen Tools und Betriebssystemen integriert, wie etwa in der Linux-Distribution Kali und den Passwort-Cracking-Tools John the Ripper und Hashcat. [69]

Die zweite Passwortliste, die für den Vergleich genutzt wird, ist die 8fit-pass.txt. Diese Textdatei enthält 1.133.603 Passwörter und stammt aus einem Sicherheitsvorfall im Jahr 2018, bei dem neben Passwörtern auch E-Mail-Adressen, Geschlechtsinformationen, Internet Protocol (IP)-Adressen und Profil-Thumbnail-Bilder aus den 8fit-Benutzerkonten extrahiert wurden [70]. In der Tabelle 4.1 werden Informationen der beiden Passwortlisten gegenübergestellt.

Dienst / Webseite	Branche	Anzahl Passwörter	Quelle
RockYou	Spieleentwicklung	14.341.564	[3]
8Fit	Fitness-Applikation	1.133.603	[71]

Tabelle 4.1: Vergleich: Verwendete Leaks

4.4 Erstellung des Skripts

Um die Vergleichsliste mit den beiden Passwortlisten vergleichen zu können, wurde ein kurzes Skript in der Programmiersprache Python erstellt. Das Programm trägt den Namen „vergleich.py“. Es besteht aus fünf verschiedenen Funktionen, die im Folgenden kurz erläutert werden sollen.

Funktion 1: „load_words“

In der ersten Funktion wird die Vergleichsliste mit UTF-8-Kodierung im Lesemodus geöffnet. Anschließend wird jede Zeile einzeln eingelesen, führende und nachfolgende Leerzeichen werden entfernt und die Begriffe in einer Liste gespeichert. Sollte die Liste nicht gefunden werden oder ein anderer Fehler auftreten, wird der Vorgang mit einer Fehlermeldung abgebrochen.

Funktion 2: „load_passwords“

In der zweiten Funktion wird ebenso mit der für den Vergleich eingesetzten Passwortliste verfahren. Im Gegensatz zur Vergleichsliste wird die Passwortliste jedoch in Latin-1-Kodierung geöffnet, da einige der Passwörter aus den Leaks aufgrund des Zeichensatzes Probleme mit der UTF-8-Kodierung verursachten. Anschließend werden die einzelnen Zeilen nacheinander eingelesen und die Passwörter in einer Liste gespeichert. Auch hier werden die Leerzeichen am Anfang und Ende der Zeilen mithilfe der line-strip()-Methode entfernt. Kann die Liste nicht gefunden werden oder sollte ein anderer Fehler auftreten, wird das Programm mit einer Fehlermeldung beendet.

Funktion 3: „find_matching_passwords“

In der dritten Funktion findet der eigentliche Vergleichsprozess statt. Im ersten Schritt wird die Vergleichsliste in ein Set umgewandelt, da Sets schnellere Suchoperationen ermöglichen und somit die Suchgeschwindigkeit erhöhen. Anschließend wird jeder Begriff aus der Vergleichsliste ohne Berücksichtigung der Groß-/Kleinschreibung (case-insensitive) mit jedem Passwort aus der Passwortliste verglichen. Wird ein übereinstimmendes Wort gefunden, wird das Passwort zusammen mit dem gefundenen Begriff aus der Vergleichsliste einer Ergebnisliste hinzugefügt. Da bei einem Treffer die Vergleichsschleife durch einen break-Befehl abgebrochen wird, sind Mehrfachtreffer nicht möglich.

Funktion 4: „safe_print“

Diese Funktion stellt sicher, dass es zu keinen Problemen mit nicht darstellbaren Zeichen kommt. Sie wurde hinzugefügt, nachdem der Vergleich in Testdurchläufen in seltenen Fällen abrupt mit der Fehlermeldung „UnicodeEncodeError“ beendet wurde. Tritt dieser Fehler nun auf, wird der Text in American Standard Code for Information Interchange (ASCII) kodiert, wobei nicht darstellbare Zeichen durch ein Fragezeichen ersetzt werden.

Funktion 5: „main“

Die fünfte Funktion steuert den Programmablauf, indem sie die anderen Funktionen aufruft und die Ergebnisse verarbeitet.

Im letzten Teil des Skripts werden die Namen der Vergleichs- und Passwortlisten definiert, sodass für die beiden Vergleiche separate Programme erstellt werden können. Diese Programme werden „vergleich_rockyou.py“ und „vergleich_8fit_pass.txt“ genannt.

4.5 Durchführung des Vergleichs

Nachdem die beiden Python-Skripte programmiert, die Vergleichsliste erstellt und die beiden Passwortlisten ausgewählt wurden, konnten die Vergleichsprozesse durchgeführt werden. Hierfür wurde die Kommandozeile auf einem Computer mit aktuellem Windows-Betriebssystem gestartet und zum entsprechenden Speicherort navigiert. Am Beispiel des Vergleichs mit der Passwortliste rockyou.txt wurde folgende Eingabe ausgeführt:

*.../*Verzeichnisname*>* ***py vergleich_rockyou.py > ergebnisse_rockyou.txt***

Dabei ist „py vergleich_rockyou.py“ für den Programmstart und „> ergebnisse_rockyou.txt“ für die Umleitung der Ausgabe in eine Textdatei verantwortlich. Eine Eingabe der Namen der Vergleichliste und der Passwortliste ist nicht nötig, da beide bereits im Python-Skript definiert wurden.

4.6 Darstellung und Interpretation der Ergebnisse

Der erste Vergleich wurde mit der rockyou.txt durchgeführt. Der Vergleichsprozess dauerte 6 Stunden und 25 Minuten. Von den 14.341.564 Passwörtern konnten 4.528.115 Übereinstimmungen gefunden werden, was einer Trefferquote von 31,6% entspricht. Das bedeutet, dass 31,6% aller Passwörter aus der rockyou.txt-Liste einen oder mehrere Begriffe aus der Vergleichsliste enthalten. In der Abbildung 4.1 ist die Trefferquote visuell dargestellt.

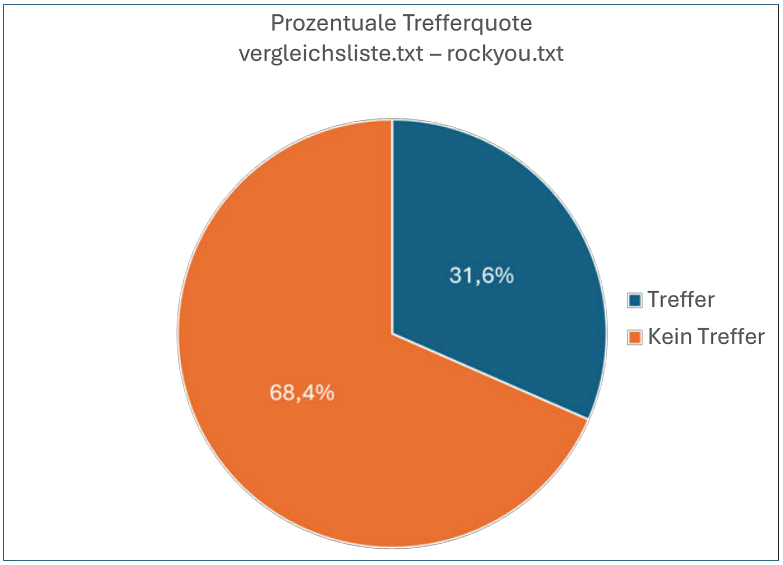


Abbildung 4.1: Prozentuale Trefferquote rockyou.txt (Eigene Darstellung)

Für den zweiten Vergleich wurde die 8fit-pass.txt verwendet. Dieser Abgleich zwischen der Vergleichsliste und der Passwortliste dauerte eine Stunde und fünf Minuten. Von den 1.133.603 Passwörtern enthielten 411.249 ein oder mehrere Wörter aus der Vergleichsliste, was einer Trefferquote von 36,3% entspricht. Die Abbildung 4.2 veranschaulicht diese Trefferquote.

Kombiniert man die Ergebnisse beider Vergleiche, ergeben sich 4.939.364 Treffer bei insgesamt 15.475.167 Passwörtern, was einem Trefferanteil von 31,9% entspricht. Auf den ersten Blick lässt sich somit feststellen, dass fast ein Drittel aller Passwörter auf Basis persönlicher Informationen

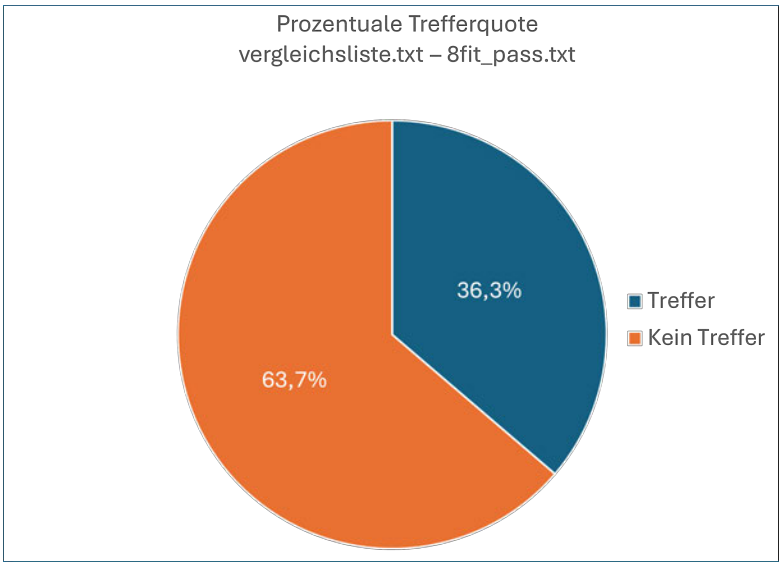


Abbildung 4.2: Prozentuale Trefferquote 8fit_pass.txt (Eigene Darstellung)

erstellt wurde. Für eine korrekte Interpretation der Ergebnisse ist es jedoch notwendig, die Treffer aus den beiden Ergebnislisten genauer zu analysieren. Die Abbildung 4.3 zeigt einen exemplarischen Ausschnitt aus der Ergebnisliste des Vergleichs mit der rockyou.txt.

```
lasvegas (gefundenes Wort: vegas)
danielle1 (gefundenes Wort: danielle)
seven7 (gefundenes Wort: seven)
harrison (gefundenes Wort: harris)
joseph1 (gefundenes Wort: joseph)
jonasbrothers (gefundenes Wort: jonas)
nickjonas (gefundenes Wort: jonas)
soccer7 (gefundenes Wort: soccer)
kay2004 (gefundenes Wort: 2004)
kay1991 (gefundenes Wort: 1991)
justin4me (gefundenes Wort: justin)
```

Abbildung 4.3: Beispielhafter Ausschnitt aus der Ergebnisliste (Eigene Darstellung)

Bei einer manuellen Untersuchung der Ergebnisse zeigt sich, dass die Treffer in verschiedene Kategorien unterteilt werden können. Die erste Kategorie umfasst die korrekten Treffer, die augenscheinlich den größten Anteil ausmachen. Diese Passwörter enthalten eines der Begriffe oder Zahlen aus der Vergleichsliste. Die zweite Kategorie, die ebenfalls dem Untersuchungsziel entspricht, sind die Mehrfachtreffer. Diese Passwörter enthalten zwei oder mehr Begriffe aus der Vergleichsliste. Die dritte Kategorie sind die Zufallstreffer. Zwar enthalten diese Passwörter einen Begriff aus der Vergleichsliste, jedoch ist es unwahrscheinlich, dass dieser Begriff bewusst vom Passwortersteller gewählt wurde. Im Sinne der Zielsetzung stellen diese Zufallstreffer keine tatsächlichen Treffer dar. In der Tabelle 4.2 sind zur Veranschaulichung für jede Kategorie vier Beispiele aufgeführt.

Aufgrund der scheinbar großen Anzahl an korrekten Treffern kann das Ergebnis durchaus als aussagekräftig angesehen werden. Allerdings gibt es auch Gründe, warum eine differenziertere Interpretation notwendig ist, anstatt sich ausschließlich auf die prozentualen Trefferquoten zu verlassen.

Korrekte Treffer	Korrekte Mehrfachtreffer	Zufallstreffer
ralph013 (Ralph)	rachelthomas (Rachel / Thomas)	december2612 (Ember)
iluvsara22 (Sara)	1981will (1981 / Will)	legalizate (Aliza)
69sabrina (Sabrina)	davidsmith87 (David / Smith)	NOTWORKING (King)
jvliverpool44 (Liverpool)	denmark2006 (Denmark / 2006)	NOTTODAYFUCKER0 (Otto)

Tabelle 4.2: Vergleich: Beispiele je Trefferkategorie

1. Die Zufallstreffer

Der erste Grund hierfür sind die bereits erwähnten Zufallstreffer. Manche Passwörter wurden zwar als Treffer erkannt und finden sich in der Ergebnisliste wieder, sind jedoch keine korrekten Treffer im Sinne der Zielsetzung. Betrachtet man beispielsweise das Passwort „NOTTODAYFUCKER0“ aus der Tabelle 4.2 genauer, so wurde dieses Passwort vermutlich nicht auf Basis persönlicher Informationen erstellt. Das Match mit dem Begriff „Otto“ ist inhaltlich nicht korrekt, beeinflusst jedoch das Ergebnis hinsichtlich der prozentualen Trefferquote, wenn auch in vermutlich überschaubarem Ausmaß. Ein Filtern der Zufallstreffer aus den Ergebnislisten würde die Quote der tatsächlich korrekten Treffer erhöhen, ist jedoch technisch nicht einfach umzusetzen und konnte daher in dieser Arbeit nicht berücksichtigt werden.

2. Die Vergleichsliste

Der zweite Grund für die Notwendigkeit einer differenzierten Auseinandersetzung mit den Ergebnissen liegt im Aufbau der Vergleichsliste. Obwohl versucht wurde, diese Liste möglichst objektiv und mit wissenschaftlichem Hintergrund zu erstellen, ist sie in gewisser Weise willkürlich und keinesfalls als vollständig zu betrachten. Nimmt man beispielsweise den Namen des Formel-1-Rekordweltmeisters „Lewis Hamilton“, so fällt auf, dass der Begriff „Hamilton“ in den beiden Passwortlisten insgesamt 407 Mal vorkommt. Teilweise sind die Passwörter ergänzt mit „Lewis“, „formula“ oder „mercedes“, was darauf schließen lässt, dass tatsächlich der Formel-1-Rennfahrer gemeint ist und dieser eine Art Vorbild oder Idol für den Passwortersteller darstellt. Auch diese Passwörter wären korrekte Treffer im Sinne der Zielsetzung. Da die Rubrik „Sportliche Idole“ in der Vergleichsliste jedoch nicht existiert, findet das Tool keinen Treffer und diese Passwörter beeinflussen die prozentuale Trefferquote nicht.

3. Die Intention des Passworterstellers

Eine weitere Schwierigkeit dieses Vergleichs ist, dass die Intention der Ersteller bei der Wahl eines Passworts grundsätzlich nicht bekannt ist. Nimmt man als Beispiel das reale Passwort „december25“ aus der rockyou.txt, so ist die Intention ausschlaggebend, ob es sich um ein Passwort handelt, das auf Basis persönlicher Informationen erstellt wurde oder nicht. Einerseits könnte der Ersteller das Passwort gewählt haben, weil am 25. Dezember der 1. Weihnachtsfeiertag bzw. in den USA der „Christmas Day“ gefeiert wird und dieses Passwort deshalb leicht zu merken ist. Andererseits könnte der Ersteller es gewählt haben, weil der 25. Dezember für ihn einen besonderen Tag darstellt, etwa den Hochzeitstag, den eigenen Geburtstag oder den Geburtstag seines Kindes. In diesem Fall wäre das Passwort tatsächlich auf Basis persönlicher Informationen erstellt. Wurde es jedoch nur deshalb gewählt, weil es der Tag des „Christmas Days“ ist und es sich somit leicht merken lässt, handelt es sich um keinen validen Treffer.

Zusammenfassend lässt sich feststellen, dass die Ergebnisse durchaus aussagekräftig sind, jedoch stets im Hinblick auf mögliche Fehlertoleranzen interpretiert werden müssen. Eine korrekte Interpretation der Ergebnisse ist dringend erforderlich, um den statistischen Zahlen keinen überhöhten Wert beizumessen. Das Beispiel mit dem Passwort „december25“ zeigt, dass die Intention hinter den Passwörtern, die bei keinem der fast 15,5 Millionen verglichenen Passwörter abschließend bekannt ist, eine große Rolle spielt. Trotzdem zeigt eine manuelle Untersuchung der Treffer, dass sehr viele Passwörter auf Basis persönlicher Informationen erstellt werden. Diese Tatsache deutet darauf hin, dass Brute-Force-Angriffe mithilfe personalisierter Wörterbücher eine sinnvolle und effektive Alternative zu Brute-Force-Angriffen mit öffentlich einsehbaren Dictionaries darstellen.

5 Zusammenfassung der Ergebnisse

In diesem Kapitel werden die Ergebnisse der durchgeführten Methoden bezogen auf die in der Einleitung aufgeführten Forschungsziele diskutiert und analysiert.

Das Sicherheitsbewusstsein der Bevölkerung im Hinblick auf Passwörter

Das Sicherheitsbewusstsein der Bevölkerung im digitalen Raum, insbesondere in Bezug auf Passwörter, wurde umfassend analysiert. Statistiken aus nahezu 14 Milliarden Passwörtern des HPIs zeigen, dass sich unter den zehn am häufigsten verwendeten Passwörtern immer noch viele einfache und unsichere Passwörter wie „password“, „qwerty“ und „123456“ befinden [38]. Ähnliche Ergebnisse liefert das Unternehmen Nordpass in ihrer Analyse der am häufigsten genutzten Passwörter in Deutschland [39]. Diese Analysen verdeutlichen, dass allgemein bekannte Empfehlungen zur Erstellung sicherer Passwörter, wie sie etwa vom BSI für Deutschland veröffentlicht werden, häufig ignoriert werden [36].

Andererseits zeigt sich ein zunehmendes Bewusstsein für die Notwendigkeit sicherer Passwörter, beispielsweise anhand der Nutzung von Passwortgeneratoren. Eine Studie von Bitkom zur Passworterstellung ergab, dass im Jahr 2023 25% der Menschen Passwortgeneratoren zur Erstellung sicherer Passwörter nutzten, im Vergleich zu 20% im Jahr 2022 [40]. Auch die durchgeführte Online-Umfrage dieser Arbeit ergab, dass 21,4% der Teilnehmer Passwortgeneratoren verwenden. Eine weitere Umfrage von DsiN aus dem Jahr 2021 zeigt, dass 31,1% der Befragten einen Passwortgenerator nutzen [55].

Diese und weitere Analysen in dieser Arbeit deuten darauf hin, dass sich das Sicherheitsbewusstsein der Bevölkerung in den letzten Jahren positiv entwickelt hat. Diese Entwicklung könnte durch die anhaltende Aufklärung seitens öffentlicher Stellen sowie durch die gestiegenen Mindestanforderungen vieler Online-Dienste, insbesondere in Bezug auf die Passwortkomplexität, gefördert worden sein.

Die Verbreitung von alphanumerischen Passwörtern bei Smartphones

Um die Relevanz des Themas dieser Arbeit für die forensische Praxis im Umfeld von Strafverfolgungsbehörden zu beurteilen, ist das Wissen über die Verbreitung von alphanumerischen Passwörtern bei Smartphones von besonderem Interesse. Eine Studie aus dem Jahr 2019 ergab, dass 6% der Befragten aus Deutschland und 7% der Befragten weltweit eine alphanumerische Gerätesperre auf ihrem Smartphone verwenden [2]. Weitere aktuelle Studien zu diesem Thema liegen nicht vor.

Die durchgeführte Online-Umfrage ergab, dass 9,3% der Teilnehmer ein alphanumerisches Passwort auf ihrem Smartphone nutzen. Diese Ergebnisse deuten darauf hin, dass die Nutzung dieser Sperrmethode in den letzten Jahren zugenommen hat und dieser Trend wahrscheinlich weiter anhalten wird. Gründe hierfür könnten unter anderem das steigende Sicherheitsbewusstsein der Bevölkerung sowie die sinkende Häufigkeit der notwendigen Eingabe von PINs und Passwörtern aufgrund parallel genutzter biometrischer Sperrmethoden sein. Daraus lässt sich ableiten, dass Brute-Force-Angriffe auf Smartphones mit alphanumerischen Passwörtern in Zukunft eine noch größere Rolle im Alltag von IT-Forensik-Abteilungen im Umfeld von Strafverfolgungsbehörden spielen könnten.

Die mathematische Notwendigkeit für effiziente Brute-Force-Methoden

In den mathematischen Grundlagen von Brute-Force (Kapitel 2.2.2) wurde mithilfe von beispielhaften Berechnungen auf Grundlage der Kombinatorik gezeigt, dass das Durchprobieren aller möglichen Kombinationen, anders als bei vierstelligen und sechsstelligen PINs oder Wischmustern, aus zeitlichen Gründen nicht möglich ist [17]. Es wurde demonstriert, dass selbst mit einem modernen Prozessor, der 4 Milliarden Passwörter pro Sekunde verarbeiten kann, das Durchprobieren aller möglichen Kombinationen eines elfstelligen Passworts über 2.100 Jahre dauern würde. Diese Berechnungen verdeutlichen, dass intelligente und effiziente Methoden erforderlich sind, um die Erfolgschancen von Brute-Force-Angriffen zu erhöhen. Besonders bei Smartphones ist dies von großer Bedeutung, da die typischen Brute-Force-Geschwindigkeiten auf mobilen Geräten, wie in Kapitel 2.2.5 beschrieben, weit unter den theoretischen Leistungsfähigkeiten der eingesetzten Prozessoren liegen.

Die Nutzung von Passwörtern auf Grundlage persönlicher Informationen

In den theoretischen Grundlagen dieser Arbeit wurden die menschlichen Gewohnheiten bei der Passworterstellung untersucht. Eine repräsentative Studie von Harris Poll in Kooperation mit Google ergab, dass mehr als die Hälfte der US-amerikanischen Bevölkerung persönliche Informationen in ihren Passwörtern verwenden [35]. Ähnliche Werte wurden auch in der durchgeführten Online-Umfrage festgestellt, bei der über 64% der Befragten angaben, Passwörter auf Grundlage persönlicher Informationen erstellt zu haben. Beim praxisorientierten Vergleich im Kapitel 4 wurde zudem ermittelt, dass etwa 31,9% aller Passwörter aus den beiden verwendeten Passwortlisten persönliche Faktoren beinhalten. Diese Ergebnisse verdeutlichen, dass die Erstellung von Passwörtern auf Grundlage persönlicher Informationen weit verbreitet ist.

6 Fazit und Ausblick

In diesem Kapitel soll ein Fazit zu der Arbeit gezogen werden, gefolgt von einem Ausblick auf offene Punkte und mögliche zukünftige Erweiterungen.

6.1 Fazit

Im Kapitel 1.2 der Einleitung wurde folgende zentrale Forschungsfrage definiert:

Können Brute-Force-Angriffe auf Smartphones mit Passwort-Sperre durch die Nutzung individueller Wörterbücher, die auf Basis persönlicher Informationen erstellt werden, effizienter und erfolgversprechender gestaltet werden?

Vergleicht man die Ergebnisse der drei verwendeten Methoden, lässt sich eindeutig feststellen, dass viele Menschen persönliche Informationen als Grundlage für Passwörter bei Online-Diensten und technischen Geräten verwenden. Dies geht sowohl aus der Analyse des aktuellen Stands der Wissenschaft als auch aus den Ergebnissen der Umfrage und des praxisorientierten Vergleichs hervor. Zudem wurde in den mathematischen Grundlagen von Brute-Force (Kapitel 2.2.2) verdeutlicht, warum bei alphanumerischen Passwörtern effiziente Methoden erforderlich sind, um überhaupt eine realistische Chance auf einen erfolgreichen Angriff zu haben. Darüber hinaus ergab sowohl die Literaturrecherche als auch die Umfrage, dass die Verwendung von alphanumerischen Passwörtern bei mobilen Endgeräten zunimmt, wodurch die Forschungsfrage für die IT-forensische Praxis von großer Relevanz ist.

Abschließend lässt sich somit zusammenfassen, dass der Einsatz personalisierter Wörterbücher für Brute-Force-Angriffe auf Smartphones mit alphanumerischen Passwörtern eine sinnvolle Alternative zu frei verfügbaren Wörterbüchern wie rockyou.txt darstellen. Dass sie tatsächlich eine Optimierung hinsichtlich Effizienz und Erfolgschancen darstellen, kann aufgrund der Ergebnisse zwar angenommen, jedoch nicht zweifelsfrei geklärt werden.

Dies bedeutet jedoch nicht, dass frei verfügbare Wörterbücher wie die rockyou.txt, die 8fit_pass.txt oder ähnliche Wortlistkombinationen für Brute-Force-Angriffe ungeeignet sind. Die Analyse bestehender Passwortleaks, unter anderem durch das HPI, hat gezeigt, dass viele vermeintlich „einfache“ Passwörter immer wieder verwendet werden, sodass auch diese Wörterbücher zum Erfolg führen können [38]. Vielmehr konnte in dieser Arbeit gezeigt werden, dass personalisierte Wörterbücher eine wertvolle Ergänzung zu den herkömmlichen Methoden vieler Mobilfunkforensik-Tools darstellen. Angesichts der hohen Brute-Force-Geschwindigkeiten, die inzwischen bei vielen Smartphonemodellen möglich sind, werden ohnehin mehrere Wörterbücher benötigt, falls die anfänglich verwendeten erfolglos durchlaufen werden.

6.2 Ausblick

Nachdem die Forschungsfrage im vorangegangenen Kapitel beantwortet wurde, stellt sich die Frage, wie IT-Forensiker diese personalisierten Wörterbücher erstellen können. Ein verbreitetes Tool ist das Python-Tool pydictor. Dieses quelloffene Programm kann kostenfrei bei GitHub heruntergeladen und

genutzt werden. Mit pydictor können sowohl zahlenbasierte als auch alphanumerische Wörterbücher individuell erstellt werden. Besonders interessant ist das integrierte Tool Social Engineering Dictionary Builder (SEDB), welches speziell für die Wörterbuchgenerierung aus Social-Media-Profilen entwickelt wurde. Die Entwickler beschreiben ihre Software selbst als „*A powerful and useful hacker dictionary builder for a brute-force attack*“. [72]

Weitere Tools, die sich zur Generierung von individuellen Wörterbüchern eignen, sind BruteList [73] und wordlist-generator [74]. Auch besteht die Möglichkeit, ein eigenes Tool zu programmieren. Dies ist zwar etwas zeitaufwändiger, bietet jedoch den Vorteil, dass es den eigenen Wünschen und Anforderungen aus der Praxis optimal angepasst werden kann.

Eine Weiterentwicklung dieser Thematik könnte zudem eine automatisierte Übernahme von Schlagwörtern in das Wörterbuchgenerator-Tool darstellen. Standardmäßig ist der IT-Forensiker in Strafverfolgungsbehörden darauf angewiesen, relevante Informationen zum Smartphone-Besitzer von den zuständigen Ermittlern zu erhalten. Diese Begriffe kann der Forensiker dann in das Tool mit den geeigneten Parametern eintragen, welches das Wörterbuch generiert. Eine Möglichkeit zur Automatisierung könnte darin bestehen, ein Tool zu entwickeln, das die relevanten persönlichen Informationen des Smartphone-Besitzers automatisiert vom Ermittler an den Forensiker überträgt und in das Python-Tool integriert.

Anhang A: Einwilligungserklärung Online-Umfrage

Einwilligungserklärung

Sehr geehrte Teilnehmerin,
sehr geehrter Teilnehmer,

In dieser Umfrage geht es um das Thema "Gewohnheiten bei der Passworterstellung". Sie wurde im Rahmen meiner Bachelorthesis im Studiengang "IT-Forensik/Cybercrime" erstellt. Bei Fragen zum Thema Smartphone-Nutzung bzw. Smartphone-Sicherheit bitte ich Sie, sich auf ihr am häufigsten genutztes Smartphone zu beziehen.

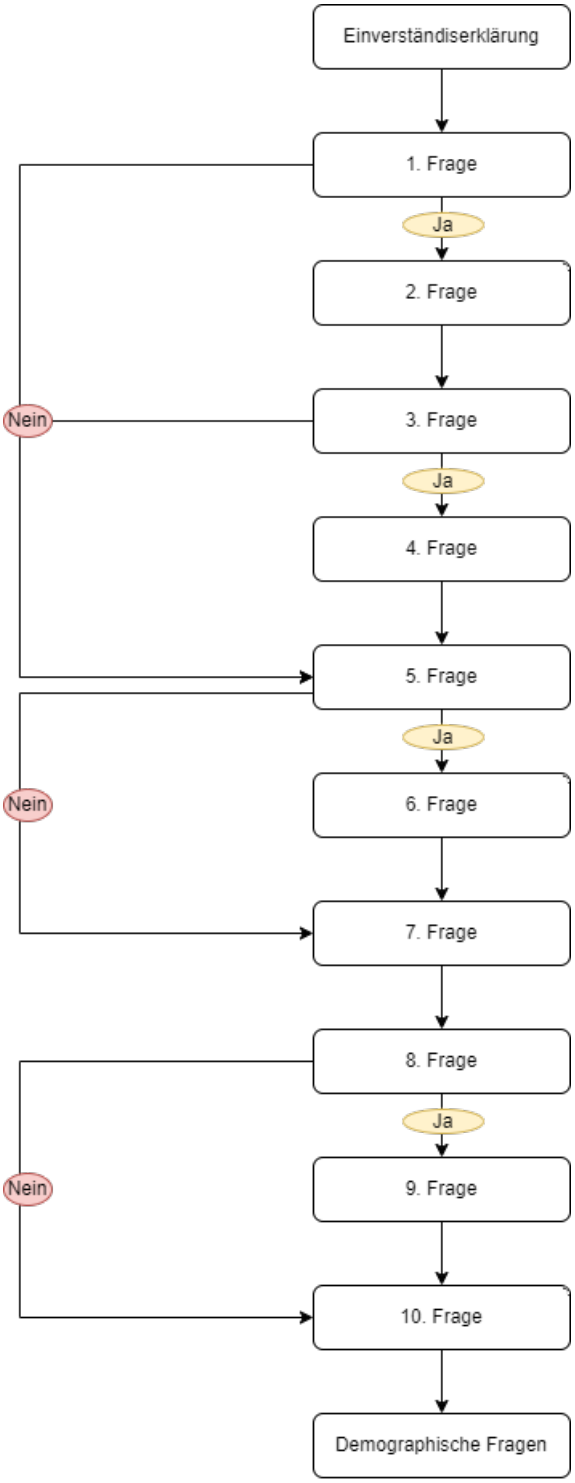
Innerhalb der Umfrage werden personenbezogene Daten (Alter und Geschlecht) abgefragt. Diese dienen zur weiterführenden Auswertung und Interpretation der Ergebnisse. Dem Ersteller ist bewusst, dass es sich hierbei um ein sensibles Thema handelt. In diesem Zusammenhang wird darauf hingewiesen, dass Sie niemals Ihre persönlichen Passwörter teilen sollten, auch nicht in dieser Umfrage. Ihre Angaben werden selbstverständlich streng vertraulich behandelt. Namen und Kontaktdaten werden nicht erfasst. Eine Zuordnung Ihrer Angaben zu Ihrer Person ist somit nicht möglich.

Zur Ausübung Ihrer Rechte (Auskunft, Korrektur, Löschung, Widerruf, etc.) oder Fragen zur Umfrage können Sie mich unter pwenig@hs-mittweida.de kontaktieren.

Vielen Dank im Voraus für Ihre Teilnahme,

Philipp Wenig

Anhang B: Ablaufplan Online-Umfrage



Literaturverzeichnis

[1] „Statista - Anteil der Smartphone-Nutzer in Deutschland nach Altersgruppe im Jahr 2021“. (Nov. 2021), Adresse: https://de.statista.com/statistik/daten/studie/459963/umfrage/anteil-der-smartphone-nutzer-in-deutschland-nach-altersgruppe/ (besucht am 24. 03. 2024).

[2] „Statista - Wie sperren Sie Ihr Smartphone?“ (Jan. 2020), Adresse: https://de.statista.com/statistik/daten/studie/1115282/umfrage/nutzung-von-sicherheitssperren-des-smartphones/ (besucht am 24. 03. 2024).

[3] „Kaggle - rockyou.txt“. (Jan. 2019), Adresse: https://www.kaggle.com/datasets/wjburns/common-password-list-rockyoutxt (besucht am 04. 06. 2024).

[4] J. Ottmann, J. Pollach, N. Scheler, J. Schneider, C. Rückert und F. Freiling, „Zur Blackbox-Problematik im Bereich Mobilfunkforensik“, Juli 2021. DOI: 10.1007/s11623-021-1487-1. Adresse: https://doi.org/10.1007/s11623-021-1487-1 (besucht am 05. 05. 2024).

[5] „Statista - Marktanteile der führenden mobilen Betriebssysteme an der Internetnutzung mit Mobiltelefonen in Deutschland von Januar 2009 bis Mai 2024“. (Juni 2024), Adresse: https://de.statista.com/statistik/daten/studie/184332/umfrage/marktanteil-der-mobilen-betriebssysteme-in-deutschland-seit-2009/ (besucht am 05. 05. 2024).

[6] S. Garg und N. Baliyan, „Comparative analysis of android and iOS from security viewpoint“, *Computer Science Review*, Mai 2021, ISSN: 15740137. DOI: 10.1016/j.cosrev.2021.100372. Adresse: https://linkinghub.elsevier.com/retrieve/pii/S1574013721000125 (besucht am 04. 05. 2024).

[7] *Apple Inc. - Sicherheit der Apple-Plattformen*, Mai 2024. Adresse: https://support.apple.com/de-de/guide/security/welcome/web (besucht am 06. 05. 2024).

[8] *Open Handset Alliance - Alliance Members*. Adresse: https://www.openhandsetalliance.com/oha_members.html (besucht am 07. 05. 2024).

[9] *Android - Android 14*. Adresse: https://www.android.com/intl/de_de/android-14/ (besucht am 07. 05. 2024).

[10] C. Hummert und D. Pawlaszczyk, *Mobile Forensics – The File Format Handbook*. Springer International Publishing, Mai 2022. DOI: 10.1007/978-3-030-98467-0. Adresse: https://link.springer.com/10.1007/978-3-030-98467-0 (besucht am 27. 07. 2024).

[11] *Android Developers - Plattformarchitektur*. Adresse: https://developer.android.com/guide/platform?hl=de (besucht am 07. 05. 2024).

[12] A. Mos und M. M. Chowdhury, „Mobile security: A look into android“, Juli 2020. DOI: 10.1109/EIT48999.2020.9208339. Adresse: https://ieeexplore.ieee.org/document/9208339/ (besucht am 12. 05. 2024).

[13] T. Groß, M. Ahmadova und T. Müller, „Analyzing android's file-based encryption“, Aug. 2019. DOI: 10.1145/3339252.3340340. Adresse: https://dl.acm.org/doi/10.1145/3339252.3340340 (besucht am 12. 05. 2024).

[14] N. Pohlmann, *Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung*. Springer Fachmedien Wiesbaden, 2022. DOI: 10.1007/978-3-658-36243-0. Adresse: https://link.springer.com/10.1007/978-3-658-36243-0 (besucht am 14. 05. 2024).

[15] J. Schaeffer, P. Lu, D. Szafron und R. Lake, „A re-examination of brute-force search“, Mai 2000. Adresse: https://www.researchgate.net/publication/2330753_A_Re-Examination_of_Brute-Force_Search (besucht am 09. 05. 2024).

[16] P. Tittmann, *Einführung in die Kombinatorik*. Springer Berlin Heidelberg, 2019. DOI: 10.1007/978-3-662-58921-2. Adresse: http://link.springer.com/10.1007/978-3-662-58921-2 (besucht am 15. 05. 2024).

[17] R. Castro. „Mathematik der Passwörter: PIN vs. Kennwort“. (Sep. 2014), Adresse: https://www.welivesecurity.com/deutsch/2014/09/02/mathematik-der-passworter-pin-vs-kennwort/ (besucht am 24. 03. 2024).

[18] R. Laufenburg. „Wörterbuchangriff (Dictionary-Attack) - Wie Sie sich vor Wörterbuchangriffen schützen“, PC-SPEZIALIST Blog. (Okt. 2021), Adresse: https://www.pcspezialist.de/blog/2021/10/13/woerterbuchangriff/ (besucht am 20. 05. 2024).

[19] V. Petkauskas. „RockYou2024: 10 billion passwords leaked in the largest compilation of all time“, Cybernews. (Juli 2024), Adresse: https://cybernews.com/security/rockyou2024-largest-password-compilation-leak/ (besucht am 20. 07. 2024).

[20] „Proton - Was ist ein Rainbow-Table-Angriff und wie kann man ihn verhindern?“ (Juni 2024), Adresse: https://proton.me/blog/de/what-is-rainbow-table-attack (besucht am 29. 07. 2024).

[21] D. Reichl, *Keepass password safe - masterkey*. Adresse: https://keepass.info/help/base/keys.html (besucht am 29. 07. 2024).

[22] BSI, *Leitfaden IT-Forensik, Version 1.0.1*, März 2011. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.html (besucht am 27. 06. 2024).

[23] *hashcat - advanced password recovery*. Adresse: https://hashcat.net/hashcat/ (besucht am 21. 05. 2024).

[24] *Passware kit forensic*. Adresse: https://www.passware.com/kit-forensic/filetypes/ (besucht am 21. 05. 2024).

[25] *Deutscher Bundestag - Bundesregierung_Antwort_1901434*, März 2018. Adresse: https://dserver.bundestag.de/btd/19/014/1901434.pdf (besucht am 03. 06. 2024).

[26] V. Lux. „Cellebrite hilft deutschen Behörden (Seite 2)“, heise online. (Feb. 2019), Adresse: https://www.heise.de/news/Border-Security-Die-neusten-Standards-der-Sicherheitsindustrie-4308630.html (besucht am 03. 06. 2024).

[27] *Autopsy - digital forensics*. Adresse: https://www.autopsy.com/ (besucht am 20. 07. 2024).

[28] *Cellebrite - Cellebrite Premium*. Adresse: https://cellebrite.com/de/cellebrite-premium-de/ (besucht am 03. 06. 2024).

[29] *Cellebrite - Cellebrite Premium Produktübersicht*. Adresse: https://cellebrite.com/wp-content/uploads/2021/03/ProductOverview_CellebritePremium_A4_web_de.pdf (besucht am 03. 06. 2024).

[30] K. Gürayer. „Android-Sperrmuster oft einfach zu erraten – so geht's sicherer“, GIGA. (März 2016), Adresse: https://www.giga.de/extra/sicherheit/news/android-sperrmuster-oft-einfach-zu-erraten-so-geht-s-sicherer/ (besucht am 04. 06. 2024).

[31] H. Mahalik und P. Lorentz. „Cellebrite - android data collection simplified“. (Juli 2020), Adresse: https://cellebrite.com/en/android-data-collection-simplified/ (besucht am 06. 08. 2024).

[32] *Cellebrite - Cellebrite Physical Analyzer*. Adresse: https://cellebrite.com/de/cellebrite-physical-analyzer-de/ (besucht am 24. 07. 2024).

[33] *Cellebrite - Cellebrite Reader*. Adresse: https://cellebrite.com/de/cellebrite-reader-de/ (besucht am 26. 07. 2024).

[34] *Cybersicherheitsagentur Baden-Württemberg (CSBW) - Auf Spurensuche: IT-Forensik*. Adresse: https://www.cybersicherheit-bw.de/auf-spurensuche-it-forensik (besucht am 25. 07. 2024).

[35] *Harris poll - the united states of p@ssw0rd$*, Okt. 2019. Adresse: https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf (besucht am 24. 03. 2024).

[36] *BSI - Sichere Passwörter erstellen*. Adresse: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen.html?nn=131366 (besucht am 09. 06. 2024).

[37] *HPI - Organisation*. Adresse: https://hpi.de/das-hpi/organisation.html (besucht am 07. 06. 2024).

[38] *HPI - Identity Leak Checker*. Adresse: https://sec.hpi.de/ilc/statistics (besucht am 08. 06. 2024).

[39] Nordpass, *200-most-common-passwords-de.pdf*. Adresse: https://s1.nordcdn.com/nord/misc/0.78.0/nordpass/top-200-2023/200-most-common-passwords-de.pdf (besucht am 08. 06. 2024).

[40] „Statista - Passwörter: Online-Dienste 2023“. (Dez. 2023), Adresse: https://de.statista.com/statistik/daten/studie/1092721/umfrage/passworterstellung-fuer-online-dienste-in-deutschland/ (besucht am 09. 06. 2024).

[41] J. Schwenkenbecher. „Forschungsmethoden: Wann ist eine Umfrage »repräsentativ«?“, Spektrum.de. (Aug. 2023), Adresse: https://www.spektrum.de/news/wann-ist-eine-umfrage-repraesentativ/2166723 (besucht am 21. 07. 2024).

[42] N. Baur und J. Blasius, *Handbuch Methoden der empirischen Sozialforschung*. Springer Fachmedien Wiesbaden, 2014. DOI: 10.1007/978-3-531-18939-0. Adresse: https://link.springer.com/10.1007/978-3-531-18939-0 (besucht am 14. 06. 2024).

[43] „empirio - Was sind Single-Choice Fragen?“ (Juli 2023), Adresse: https://www.empirio.de/empiriowissen/single-choice-frage-definition (besucht am 10. 08. 2024).

[44] *empirio - Kostenlos und einfach Umfragen erstellen*. Adresse: https://www.empirio.de/ (besucht am 17. 06. 2024).

[45] *empirio - Funktionen*. Adresse: https://www.empirio.de/funktionen (besucht am 17. 06. 2024).

[46] *empirio - Community Umfragen*. Adresse: https://www.empirio.de/umfragen (besucht am 07. 08. 2024).

[47] A. R. „Wordcloud: Definition und Funktion“, Weiterbildung Data Science | DataScientest.com. (Feb. 2023), Adresse: https://datascientest.com/de/wordcloud-definition (besucht am 07. 07. 2024).

[48] „Statista - Smartphones: Marktanteile der Hersteller weltweit Q1 2024“. (Juli 2024), Adresse: https://de.statista.com/statistik/daten/studie/173056/umfrage/weltweite-marktanteile-der-smartphone-hersteller-seit-4-quartal-2009/ (besucht am 09. 07. 2024).

[49] T. Jahn und C. Kerkmann. „Smartphones: China straft Apple ab – iPhone-Absatz fällt um fast 20 Prozent“. Section: Technik - IT + Telekommunikation. (Apr. 2024), Adresse: https://www.handelsblatt.com/technik/it-internet/smartphones-china-straft-apple-ab-iphone-absatz-faellt-um-fast-20-prozent/100034492.html (besucht am 09. 07. 2024).

[50] „Statista - Passwörter: Methoden der Erstellung in Deutschland 2021“. (Juni 2021), Adresse: https://de.statista.com/statistik/daten/studie/818733/umfrage/methoden-der-passworterstellung-in-deutschland/ (besucht am 09. 07. 2024).

[51] „Statista - Online-Dienste: Nutzung von unterschiedlichen Passwörtern in Deutschland 2023“. (Apr. 2023), Adresse: https://de.statista.com/statistik/daten/studie/818713/umfrage/nutzung-von-unterschiedlichen-passwoertern-fuer-unterschiedliche-dienste-in-deutschland/ (besucht am 10. 07. 2024).

[52] *BSI: Sichere Passwörter*. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Checklisten/sichere_passwoerter_faktenblatt.pdf?__blob=publicationFile&v=4 (besucht am 10. 07. 2024).

[53] J. Weiler. „Ruhr-Universität Bochum: Sieben Mythen über Passwörter“. (Feb. 2019), Adresse: https://news.rub.de/wissenschaft/2019-02-01-it-sicherheit-sieben-mythen-ueber-passwoerter (besucht am 10. 07. 2024).

[54] *BSI: Passwörter verwalten mit einem Passwort-Manager*. Adresse: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/Passwort-Manager/passwort-manager.html?nn=131360 (besucht am 10. 07. 2024).

[55] C. Kastrop, „DsiN-SicherheitsIndex 2021“, Juni 2021. Adresse: https://www.sicher-im-netz.de/dsin-sicherheitsindex-2021 (besucht am 18. 06. 2024).

[56] ArulJohn. „GitHub - popular-baby-names 2022“. (2022), Adresse: https://github.com/aruljohn/popular-baby-names/tree/master/2022 (besucht am 18. 06. 2024).

[57] PenTestical. „GitHub - german-names“. (2024), Adresse: https://github.com/PenTestical/german_names (besucht am 18. 06. 2024).

[58] zeraye. „GitHub - surnames-list“. (2020), Adresse: https://github.com/zeraye/names-surnames-list/blob/master/surnames-list.txt (besucht am 18. 06. 2024).

[59] H. Mathien. „Kaggle - European Soccer Database“. (2016), Adresse: https://www.kaggle.com/datasets/hugomathien/soccer?resource=download (besucht am 18. 06. 2024).

[60] *National Hockey League (NHL) - Teams*, NHL.com. Adresse: https://www.nhl.com/info/teams/ (besucht am 18. 06. 2024).

[61] *Major League Baseball (MLB) - Teams*, MLB.com. Adresse: https://www.mlb.com/team (besucht am 18. 06. 2024).

[62] *National Football League (NFL) - Teams*, NFL.com. Adresse: https://www.nfl.com/teams/ (besucht am 18. 06. 2024).

[63] *National Basketball Association (NBA) - Teams*, NBA.com. Adresse: https://www.nba.com/teams (besucht am 18. 06. 2024).

[64] mbejda. „Github gist - compiled list of hobbies“. (Okt. 2015), Adresse: https://gist.github.com/mbejda/453fdb77ef8d4d3b3a67 (besucht am 19. 06. 2024).

[65] foone. „Github gist - a list of all sports“. (Mai 2021), Adresse: https://gist.github.com/foone/cf963e6849a77042489b20e304a4fb9d (besucht am 19. 06. 2024).

[66] norcal82. „Github gist - major us city names“. (Aug. 2014), Adresse: https://gist.github.com/norcal82/4accc0d968444859b408 (besucht am 19. 06. 2024).

[67] „World Population Review - Europe Cities by Population 2024“. (2024), Adresse: https://worldpopulationreview.com/continents/europe/cities (besucht am 13. 07. 2024).

[68] „Britannica - list of countries in the world“. (Juli 2024), Adresse: https://www.britannica.com/topic/list-of-countries-1993160 (besucht am 13. 07. 2024).

[69] T. Jester. „Understanding RockYou.txt: A tool for security and a weapon for hackers“, Keeper Security Blog. (Aug. 2023), Adresse: https://www.keepersecurity.com/blog/2023/08/04/understanding-rockyou-txt-a-tool-for-security-and-a-weapon-for-hackers/ (besucht am 17. 07. 2024).

[70] „8fit - 8fit Sicherheitsinformationen“. (Okt. 2021), Adresse: https://8fit.zendesk.com/hc/de/articles/360017746394-Hinweis (besucht am 17. 07. 2024).

[71] hacxx-underground. „GitHub - 8Fit.com Partial 1.1M Email:Pass Dehashed January 2021“. (2021), Adresse: https://github.com/hacxx-underground/Files/commit/fbd7cc0d763aeaaba9aa3fb7275e30e23bc5cdec (besucht am 15. 07. 2024).

[72] LandGrey, *GitHub - pydictor*, 2017. Adresse: https://github.com/LandGrey/pydictor (besucht am 29. 07. 2024).

[73] calebgcc, *GitHub - brutelist*, 2022. Adresse: https://github.com/calebgcc/brutelist (besucht am 30. 07. 2024).

[74] J4NN0, *GitHub - wordlist-generator*, 2018. Adresse: https://github.com/J4NN0/wordlist-generator (besucht am 30. 07. 2024).

Eidesstattliche Erklärung

Hiermit versichere ich – Philipp Wenig – an Eides statt, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe.

Sämtliche Stellen der Arbeit, die im Wortlaut oder dem Sinn nach Publikationen oder Vorträgen anderer Autoren entnommen sind, habe ich als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt oder anderweitig veröffentlicht.

Mittweida, 11. August 2024	
Ort, Datum	Philipp Wenig