Technische Hochschule
Brandenburg
University of
Applied Sciences

Erhöhung der Phishing-Resistenz von Anmeldeverfahren durch Einsatz von FIDO2 und Passkey

Bachelorarbeit

zur Erlangung des Grades Bachelor of Science
des Fachbereichs Informatik und Medien der
Technischen Hochschule Brandenburg

vorgelegt von:
Divine Leopold Kenfack

Betreuer: Prof. Dr. Michael Pilgermann
Zweitgutachter: Msc. Jaykumar G. Soni

Brandenburg an der Havel, 24. Oktober 2023

Kurzfassung

In dieser Arbeit wurde die Sicherheit von Passkey im Vergleich zu herkömmlichen Authentifizierungsmethoden wie Passwörtern und 2FA untersucht. Es wurde gezeigt, dass Passkey eine sichere und benutzerfreundliche Methode ist, die das Risiko von Phishing-Angriffen minimiert. Passkey bietet eine starke Authentifizierung, bei der sowohl private als auch öffentliche Schlüssel erforderlich sind, um die Identität des Benutzers zu bestätigen. Dies macht es resistent gegen klassisches Phishing, bei dem Angreifer versuchen, Benutzer dazu zu bringen, ihre Zugangsdaten auf gefälschten Websites einzugeben.

Die Ergebnisse zeigen, dass Passkey eine vielversprechende Alternative zu herkömmlichen Authentifizierungsmethoden bietet und in verschiedenen Online-Diensten eingesetzt werden kann. Es wurde auch betont, dass Benutzer weiterhin wachsam sein sollten, um Phishing-Angriffen vorzubeugen, und zusätzliche Sicherheitsmaßnahmen wie das Öffnen von E-Mail-Anhängen nur von vertrauenswürdigen Absendern sollten in Betracht gezogen werden.

Insgesamt bietet Passkey eine höhere Sicherheit und Benutzerfreundlichkeit im Vergleich zu herkömmlichen Methoden und kann dazu beitragen, die Online-Sicherheit zu verbessern.

Schlüsselwörter

1. FIDO2
2. Passkey-Authentifizierung
3. Phishing-Schutz
4. Zwei-Faktor-Authentifizierung
5. Online-Sicherheit

Abstract

This study examined the security of Passkey compared to conventional authentication methods such as passwords and 2FA. It demonstrated that Passkey is a secure and user-friendly method that mitigates the risk of phishing attacks. Passkey provides robust authentication, requiring both private and public keys to confirm the user's identity, rendering it resistant to classical phishing attempts where attackers try to coax users into entering their credentials on fake websites.

The findings underscore that Passkey presents a promising alternative to traditional authentication methods and can be implemented across various online services. It also emphasized the importance of users remaining vigilant to prevent phishing attacks, suggesting additional security measures such as opening email attachments only from trusted sources.

Overall, Passkey offers enhanced security and user-friendliness compared to conventional methods, contributing to the improvement of online security.

Keywords

1. FIDO2
2. Passkey
3. Phishing Protection
4. Two-Factor Authentication
5. Online Security

Inhaltsverzeichnis

1 Einleitung

Wir haben alle bereits Passwörter erstellt, um uns auf diverse digitale Plattformen einzuloggen. Heutzutage ist es unvermeidlich, da fast alles digitalisiert wird, sei es bei Bankgeschäften, in Ausbildungssystemen, auf der Arbeit, beim Shopping usw. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt uns jedoch, komplexe Passwörter für verschiedene Plattformen zu nutzen, die sich stark voneinander unterscheiden müssen.[1]
Allerdings ist es mit großem Aufwand verbunden, sich all diese Passwörter zu merken. Im Durchschnitt haben Deutsche 78 Online-Accounts, Franzosen haben 127, Engländer haben 113 und Amerikaner haben 150.[2] Diese Anzahl wird in den kommenden Jahren definitiv weiter steigen, da alle vorhandenen Dienste vermehrt in Richtung Digitalisierung gehen.
Der zeitintensive Aufwand, sich mit Passwörtern bei einer Authentifizierung einzuloggen, ist nicht mehr effizient. Die meisten Passwörter sind nicht nur schwach und verursachen 81 Prozent der Sicherheitsvorfälle[3] oder werden gestohlen, sondern sie kosten auch viel Zeit und Ressourcen. Laut einer Umfrage von Yubico verbrauchen Anwender pro Jahr durchschnittlich etwa 10,9 Stunden für die Eingabe oder Zurücksetzung von Passwörtern, was Unternehmen im Durchschnitt 5,2 Millionen Dollar kostet.[4]

1.1 Die Motivation

Bei meinem Praktikum habe ich mich mit dem Thema "Einführung eines Passwortmanagers" bei der ehemaligen LBS Ostdeutsche Landesbausparkasse AG beschäftigt, was heute die LBS Landesbausparkasse NordOst AG ist. Dabei

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI). Sichere Passwörter erstellen.
[2] Georgina Bott, (04.05.2017). Haben wir ein Passwortproblem?
[3] W3C und Mountain View, Calif., (04.03.2019). W3C and FIDO finalize Web Standard for Secure, Passwortless logins.
[4] W3C und Mountain View, Calif., (04.03.2019). W3C and FIDO finalize Web Standard for Secure, Passwortless logins.

sollte den Mitarbeitenden ein Passwortmanager zur Verfügung gestellt werden, damit sie ihre Passwörter sicher verwahren können und die Sicherheitsrisiken minimiert werden. Zudem war es wichtig, den Authentifizierungsprozess für die Mitarbeitenden benutzerfreundlich zu gestalten, indem eine Browser-Erweiterung zum automatischen Ausfüllen verwendet wird.
Die Frage an dieser Stelle ist jedoch, ob diese Art der Passwortspeicherung tatsächlich sicherer ist. Als Motivation dieser Arbeit dient die Recherche nach der sichersten Authentifizierungsmethode für Online-Dienste und Anwendungen, die gleichzeitig benutzerfreundlich ist.

Die stetig wachsende digitale Landschaft bringt eine Vielzahl von Möglichkeiten, aber auch Herausforderungen mit sich. Insbesondere die zunehmende Bedrohung durch Phishing-Angriffe hat die Sicherheitsanforderungen für Online-Accounts erheblich verstärkt.[5] Das BSI hat in diesem Zusammenhang klare Empfehlungen ausgesprochen, um die Sicherheit von Online-Accounts zu erhöhen und vor Identitätsdiebstahl, Accountübernahmen und sensiblen Datenverlusten zu schützen.

Außerdem empfiehlt das BSI die Zwei-Faktor-Authentisierung (2FA) keinesfalls zu deaktivieren, unterstreicht die entscheidende Rolle dieser Sicherheitsmaßnahme. In einer Zeit, in der Cyberkriminelle immer raffinierter vorgehen, ist der Schutz der Online-Identität von größter Bedeutung. Die Implementierung der Zwei-Faktor-Authentisierung stellt sicher, dass der Zugriff auf Online-Dienste nicht allein auf Passwörtern basiert, die oft durch Phishing-Angriffe gefährdet sind. Die zusätzliche Sicherheitsebene, die durch die Zwei-Faktor-Authentisierung bereitgestellt wird, hilft, Identitätsdiebstahl und unbefugte Zugriffe zu verhindern.[6]

Besonders bemerkenswert ist, dass das BSI darauf hinweist, dass die Zwei-Faktor-Authentisierung nicht deaktiviert werden sollte, selbst wenn dies in bestimmten Situationen bequemer erscheinen mag. Die Bequemlichkeit darf nicht auf Kosten der Sicherheit gehen, insbesondere wenn es um Online-Banking, Online-Shopping oder Accounts mit umfassenden Rechten und Möglichkeiten

[5] Microsoft, (06.05.2023). Securing the Microsoft Online Services infrastructure.
[6] Bundesamt für Sicherheit in der Informationstechnik (BSI). Zwei-Faktor-Authentisierung.

geht. Hier zeigt sich der Wert der 2FA als wirkungsvolle Verteidigungslinie gegen die zunehmende Bedrohung durch Cyberkriminelle.[7]

Angesichts dieser ernsten Sicherheitslage und der Empfehlungen des BSI kommt die Frage auf, wie die Phishingsresistenz von Anmeldeverfahren weiter gesteigert werden kann? Hier setzt das Forschungsthema dieser Bachelorarbeit an: Die Erhöhung der Phishingsresistenz von Anmeldeverfahren durch den Einsatz von FIDO2 und Passkey. FIDO2 und Passkey repräsentieren einen neuen Ansatz, der über herkömmliche Authentifizierungsmethoden hinausgeht. Die Technologie bietet ein starkes Sicherheitsniveau, das auf kryptografischen Prinzipien beruht und das Potenzial hat, Phishing-Angriffe effektiv zu bekämpfen.

1.2 Die Zielsetzung

Diese Bachelorarbeit wird sich mit einer detaillierten Analyse der FIDO2- und Passkey-Technologie befassen, ihre Funktionsweise erklären und ihre Wirksamkeit im Vergleich zu anderen Authentifizierungsmethoden bewerten. Das Hauptziel wird darin bestehen, in der Bachelorarbeit eine präzise Antwort auf die Frage zu liefern, ob die Implementierung von FIDO2 und Passkey tatsächlich die Widerstandsfähigkeit gegen Phishing-Angriffe im Bereich der Anmeldeverfahren steigert? Durch diese Forschung wird nicht nur das Bewusstsein für die Notwendigkeit starker Sicherheitsmechanismen geschärft, sondern auch ein Beitrag zur Entwicklung sicherer Ansätze zur Abwehr von Cyberbedrohungen geleistet.

Am Ende dieser Arbeit wird auf folgende Fragen eingegangen:

1. Wie sicher ist FIDO2/Passkey im Vergleich zu bekannten Verfahren wie der Passworteingabe online?
2. Was macht FIDO2 sicherer als die anderen Verfahren?
3. Ist Passkey benutzerfreundlicher im Vergleich zum Einloggen mit einem Passwort? Falls ja, was macht Passkey benutzerfreundlich?

Zusätzlich ist eine Simulation eines Man-in-the-Middle-Angriffs in der Authentifizierungsmethode sowohl nur mit Passwörtern als auch mit der 2FA unter Verwendung von Authentifikatoren wie der Google Authenticator-App auf

[7] Bundesamt für Sicherheit in der Informationstechnik (BSI). Zwei-Faktor-Authentisierung

einem Mobilgerät und Passkey vorgesehen, um zu bewerten, welche Verfahren besser darauf reagieren.

1.3 Die Abgrenzung

Die Arbeit bleibt bewusst oberflächlich, insbesondere in Bezug auf den technischen Aspekt von Passkey. Die Arbeit stellt Passkey vor und hebt hervor, wie es sich in Bezug auf Sicherheit und Authentifizierung von herkömmlichen Methoden unterscheidet, jedoch ohne tiefgehende technische Einblicke in die Funktionsweise von Passkey.

Darüber hinaus sollte beachtet werden, dass das Phishing-Thema in dieser Arbeit lediglich als Vergleichsgrundlage dient, um zu zeigen, wie Passkey sich im Vergleich zu bekannten Authentifizierungsmethoden verhält. Die Arbeit vertieft sich nicht in die Techniken von Phishing-Angriffen.

Zusätzlich bleibt die Forschung auf den Bereich der Multi-Faktor-Authentifizierung (MFA) oberflächlich. Die Arbeit beschränkt sich auf den Vergleich von Passkey mit bis zu 2FA, ohne in die spezifischen Details von MFA-Implementierungen einzugehen. Dies dient dazu, die Arbeit klar auf den ausgewählten Forschungsbereich zu beschränken und die Ergebnisse in diesem Kontext zu präsentieren.

Es ist wichtig anzumerken, dass die gesamten Experimente auf einem lokalen Rechner (localhost) durchgeführt wurden, was die Untersuchung auf bestimmte Szenarien und lokale Umgebungen beschränkt. Diese Begrenzung sollte bei der Betrachtung der Ergebnisse berücksichtigt werden, da reale Umgebungen und Netzwerke möglicherweise unterschiedliche Bedrohungen und Herausforderungen aufweisen.

2 Vorstellung unterschiedlicher Authentifizierungsverfahren.

2.1 Was ist Authentifizierung?

In der Informationstechnologie (IT) bezieht sich der Begriff "Authentifizierung" auf den Prozess der Identifizierung einer Entität, um sicherzustellen, dass sie tatsächlich diejenige ist, die sie vorgibt zu sein. Dieser Prozess dient dazu, den Zugriff auf Systeme, Anwendungen, Daten oder andere Ressourcen zu kontrollieren und sicherzustellen, dass nur autorisierte Benutzer oder Geräte Zugang erhalten. Die Authentifizierung erfolgt durch die Überprüfung von Anmeldeinformationen oder Identifikationsmerkmalen.[8]

2.2 Die Wichtigkeit einer starken Authentifizierung

In der heutigen schnelllebigen technologischen Landschaft kann die Bedeutung der Authentifizierung nicht überschätzt werden. Nahezu jede Organisation, jedes System, jedes Netzwerk, jede Website und jeder Server ist auf irgendeine Form der Authentifizierung angewiesen, um ihre Vermögenswerte und sensiblen Daten zu schützen. Das Fehlen robuster Authentifizierungsmechanismen setzt Entitäten einer Vielzahl von Sicherheitsrisiken aus und macht sie anfällig für verschiedene Arten von Angriffen, die weitreichende Folgen haben können. Die Bedeutung der Authentifizierung im heutigen Kontext ist vielschichtig und aus verschiedenen überzeugenden Gründen von großer Bedeutung:[9]

- **Schutz vor Cyberangriffen:**

In einer digitalen Welt, die von Cyberbedrohungen geprägt ist, spielt die Authentifizierung eine entscheidende Rolle. Ohne angemessene Authentifizierungsmaßnahmen können bösartige Akteure Schwachstellen ausnutzen und Angriffe wie Phishing, Datenverletzungen und Spoofing starten.

[8] MiniOrange, (09.12.2022). What is Authentication? Different types of Authentications.
[9] NIST Special Publication 800-63B, (Juni 2017). Digital Identity Guidelines Authentication and Lifecycle Management.

Diese Angriffe können die Integrität einer Organisation, ihren Ruf und ihre finanzielle Stabilität gefährden.[10]

- **Eindämmung von Datenverletzungen:**

Die Verbreitung sensibler Daten in Verbindung mit der wachsenden Raffinesse von Cyberkriminellen hat zu einem Anstieg von Datenverletzungen geführt. Effektive Authentifizierungsstrategien tragen dazu bei, das Risiko unbefugten Zugriffs auf vertrauliche Informationen zu minimieren. Unzureichende Authentifizierung kann zu Datenverletzungen führen, die erhebliche finanzielle Verluste, rechtliche Haftungen und Rufschädigung nach sich ziehen können.[11]

- **Gewährleistung der Benutzeridentität:**

Die Authentifizierung stellt sicher, dass Benutzer tatsächlich diejenigen sind, die sie vorgeben zu sein, und gewährt autorisierten Personen die entsprechenden Zugriffsrechte. Durch die Verifizierung der Benutzeridentitäten können Organisationen Vertrauen und Verantwortlichkeit in ihren Systemen etablieren. Dies ist insbesondere in Branchen wie Finanzen, Gesundheitswesen und Regierung von großer Bedeutung, in denen eine sichere und genaue Benutzeridentifikation entscheidend ist.[12]

- **Verhinderung unbefugten Zugriffs:**

Die Authentifizierung verhindert unbefugten Zugriff auf Systeme, Anwendungen und Ressourcen. Ohne starke Authentifizierungsmechanismen könnten unbefugte Benutzer oder bösartige Akteure Zugang erlangen und sensible Daten, geistiges Eigentum und Geschäftsbetrieb gefährden.[13]

- **Einhaltung regulatorischer Vorgaben:**

Viele Branchen unterliegen strengen rechtlichen Rahmenbedingungen, die die Implementierung starker Sicherheitsmaßnahmen, einschließlich der Authentifizierung, vorschreiben. Die Nichterfüllung von Compliance-

[10] NIST Special Publication 800-63B, (Juni 2017). Digital Identity Guidelines: Authentication and Lifecycle Management.
[11] NIST Special Publication 800-63B, (Juni 2017). Digital Identity Guidelines: Authentication and Lifecycle Management.
[12] NIST Special Publication 800-63B, (Juni 2017). Digital Identity Guidelines: Authentication and Lifecycle Management.
[13] NIST Special Publication 800-63B, (Juni 2017). Digital Identity Guidelines: Authentication and Lifecycle Management.

Anforderungen kann zu rechtlichen Strafen, finanziellen Konsequenzen und möglichen Stilllegungen führen.[14]

- **Schutz des Rufes:**

Sicherheitsverletzungen können den Ruf einer Organisation beeinträchtigen und das Vertrauen von Kunden, Partnern und Stakeholdern untergraben. Robuste Authentifizierungsmaßnahmen zeigen ein Engagement für den Schutz sensibler Informationen und den Erhalt der Sicherheit und Privatsphäre von Benutzerdaten.[15]

- **Anpassung an sich entwickelnde Bedrohungen:**

Da sich Cyberbedrohungen weiterentwickeln, müssen auch Authentifizierungsmethoden angepasst werden. Die dynamische Natur der digitalen Landschaft erfordert ständige Innovation, um vor aufkommenden Angriffsvektoren und -techniken einen Schritt voraus zu sein.[16]

- **Sicherstellung der Geschäftskontinuität:**

Die Authentifizierung spielt eine entscheidende Rolle bei der Sicherstellung ununterbrochener Geschäftsbetriebe. Ein Sicherheitsverstoß kann den Betrieb stören, Ausfallzeiten verursachen und finanzielle Verluste zur Folge haben. Die Implementierung starker Authentifizierungsmaßnahmen trägt zur Aufrechterhaltung der Geschäftskontinuität bei.[17]

Zusammenfassend ist die Authentifizierung ein Eckpfeiler der modernen Cybersicherheit. Ihre Bedeutung wird durch die allgegenwärtigen Bedrohungen unterstrichen, denen Organisationen im digitalen Zeitalter ausgesetzt sind. Um einen Wettbewerbsvorteil zu wahren, sensible Daten zu schützen und sich gegen verschiedene Cyberbedrohungen abzusichern, müssen Organisationen robuste Authentifizierungsmethoden priorisieren und investieren, die sich mit der sich entwickelnden Sicherheitslandschaft abstimmen.

[14] NIST Special Publication 800-63B, (Juni 2017). Digital Identity Guidelines: Authentication and Lifecycle Management.
[15] NIST Special Publication 800-63B, (Juni 2017). Digital Identity Guidelines: Authentication and Lifecycle Management.
[16] NIST Special Publication 800-63B, (Juni 2017). Digital Identity Guidelines: Authentication and Lifecycle Management.
[17] NIST Special Publication 800-63B, (Juni 2017). Digital Identity Guidelines: Authentication and Lifecycle Management.

2.3 Verschiedene Authentifizierungsmethoden

In der heutigen digitalen Welt sind unterschiedliche Authentifizierungsmethoden von entscheidender Bedeutung, um die Sicherheit von Ressourcen und sensiblen Daten zu gewährleisten. Hier sind einige gängige Authentifizierungsmethoden und wie sie funktionieren:

1. **Passwortbasierte Anmeldung:**

Die am häufigsten genutzte herkömmliche Anmeldeauthentifizierungsmethode, die im täglichen Gebrauch von Online-Diensten verwendet wird, ist die passwortbasierte Anmeldung. Hierbei müssen Sie eine Kombination aus Ihrem Benutzernamen/Mobilnummer und einem Passwort eingeben. Die Person wird nur dann autorisiert, wenn beide Elemente verifiziert wurden. Doch aufgrund der Nutzung mehrerer Online-Dienste ist es für Endbenutzer schwierig, alle Benutzernamen und Passwörter im Blick zu behalten. Dies führt dazu, dass Benutzer mit Fällen konfrontiert sind, wie das Vergessen von Passwörtern oder die Verwendung desselben Passworts für mehrere Dienste. Cyberkriminelle nutzen solche Schwachstellen aus und führen Aktivitäten wie Phishing und Datenverletzungen aus. Dies ist der grundlegende Grund, warum die herkömmliche passwortbasierte Authentifizierung an Zustimmung verliert und mehr Organisationen auf fortschrittliche zusätzliche Sicherheitsfaktoren setzen.[18]

2. **Zwei-Faktor-Authentifizierung (2FA):**

Bei der 2FA muss der Benutzer zwei verschiedene Authentifizierungsfaktoren bereitstellen, um sich anzumelden. Dies kann beispielsweise die Kombination aus einem Passwort und einem Einmalpasswort (OTP) sein, das per SMS oder einer Authentifizierungs-App generiert wird. 2FA bietet ein höheres Maß an Sicherheit als die alleinige Verwendung von Passwörtern.[19]

3. **Biometrische Authentifizierung:**

Biometrische Authentifizierung verwendet individuelle physische Merkmale wie Fingerabdrücke, Handflächen, Retinas, Stimmerkennung und Gesicht. Diese Merkmale werden in einer Datenbank gespeichert und bei jedem Zugriffsversuch

[18] Adams, A., Sasse, M. A. (1999). Users are not the enemy, Communications of the ACM (S.40-46).
[19] Bundesamt für Sicherheit in der Informationstechnik (BSI). Zwei-Faktor-Authentisierung.

eines Benutzers auf ein Gerät oder Gelände (Organisation, Schule, Unternehmen) überprüft. Biometrische Technologie wird hauptsächlich von privaten Unternehmen, Flughäfen und Grenzübergangsstellen eingesetzt, wo Sicherheit oberste Priorität hat.[20]

4. **Zertifikatbasierte Authentifizierung:**

Die zertifikatbasierte Authentifizierung identifiziert Personen, Server, Workstations und Geräte mithilfe einer elektronischen digitalen Identität. Ein digitales Zertifikat funktioniert ähnlich wie ein Führerschein oder ein Reisepass. Es enthält eine digitale Identität des Benutzers, die einen öffentlichen Schlüssel und eine digitale Signatur der Zertifizierungsstelle enthält.[21]

5. **Tokenbasierte Authentifizierung:**

Die tokenbasierte Authentifizierung ermöglicht es Benutzern, ihre Anmeldeinformationen nur einmal einzugeben und im Gegenzug eine einzigartige verschlüsselte Zeichenkette zu erhalten. Dieser digitale Token bestätigt, dass Ihnen bereits Zugang gewährt wurde. Tokenbasierte Authentifizierung wird in vielen Anwendungsfällen eingesetzt, z. B. bei RESTful APIs, die von vielen Frameworks und Clients genutzt werden.[22]

Diese unterschiedlichen Authentifizierungsmethoden bieten jeweils verschiedene Stufen der Sicherheit und Benutzerfreundlichkeit. Je nach den Anforderungen und dem Schutzbedarf einer Organisation können geeignete Methoden ausgewählt und implementiert werden, um den Zugriff auf Ressourcen zu sichern und unbefugte Zugriffe zu verhindern.

2.4 Das Problem mit Passwörtern

Passwörter sind zweifellos die am häufigsten verwendete Methode zur Authentifizierung von Benutzern in der digitalen Welt. Das Grundkonzept ist einfach: Ein Benutzer gibt seinen Benutzernamen und sein Passwort ein, und

[20] Jain, A. K., Ross, A., & Nandakumar, K. (2011). Introduction to biometrics, In Advances in biometrics (S. 1-22).
[21] John R. Vacca (2002). Public Key Infrastructure: Building Trusted Applications and Web Services.
[22] Clauß, S. (2002). Token-based authentication. In Encyclopedia of cryptography and security (S. 659-660).

wenn diese Informationen mit den in der Datenbank des Dienstes gespeicherten übereinstimmen, wird der Zugriff gewährt. Leider sind Passwörter anfällig für eine Vielzahl von Angriffen.

Eine der Hauptursachen für das Versagen von Passwörtern als Sicherheitsmechanismus ist die menschliche Natur. Viele Benutzer neigen dazu, schwache Passwörter zu erstellen, da sie sich leicht merken lassen. Diese Passwörter bestehen oft aus Wörtern aus dem Wörterbuch, Namen von Haustieren oder Geburtstagen, die für Angreifer leicht zu erraten sind. Selbst wenn Benutzer komplexere Passwörter erstellen, verwenden sie diese oft für mehrere Dienste, was bedeutet, dass eine Kompromittierung bei einem Dienst automatisch andere gefährdet.

Die Verwendung von schwachen oder wiederverwendeten Passwörtern ist nicht die einzige Schwäche von Passwörtern. Ein weiteres Problem sind Brute-Force-Angriffe, bei denen Angreifer automatisch eine große Anzahl von Passwortkombinationen ausprobieren, um das richtige Passwort zu erraten. Dies kann bei schwachen Passwörtern effektiv sein.

2.5 Die Zwei-Faktor-Authentifizierung (2FA)

Um die Sicherheit von Passwörtern zu erhöhen, wurde die 2FA entwickelt. Dieses System erfordert neben dem Passwort einen zweiten Authentifizierungsfaktor, um auf ein Konto zuzugreifen. Dieser zweite Faktor kann etwas sein, das der Benutzer besitzt (z. B. ein Mobiltelefon) oder etwas, das der Benutzer ist. Zum Beispiel biometrische Daten wie Fingerabdrücke.

Die 2FA hat zweifellos dazu beigetragen, die Sicherheit von Online-Konten zu verbessern. Selbst wenn ein Angreifer das Passwort errät oder stiehlt, kann er sich ohne den zweiten Faktor nicht anmelden. Dies hat viele Konten vor unbefugtem Zugriff geschützt. Es gibt jedoch immer noch einige Schwachstellen in diesem System.

Zum einen erfordert die 2FA zusätzliche Anstrengungen seitens der Benutzer. Sie müssen nicht nur ihr Passwort kennen, sondern auch den zweiten Faktor bereithalten oder aktivieren. Dies kann als lästig empfunden werden,

insbesondere wenn Benutzer sich häufig bei verschiedenen Diensten anmelden müssen.

3 FIDO2

3.1 Die Definition von FIDO

FIDO steht für "Fast Identity Online" und wurde von der FIDO Alliance entwickelt. Die FIDO Alliance ist ein Konsortium von Unternehmen und Organisationen, das sich für starke und sichere Authentifizierungsmethoden einsetzt und im Juli 2012 gegründet wurde.[23]

3.2 Die Geschichte von FIDO2

3.2.1 Die Entwicklung des FIDO-Konsortiums und die Notwendigkeit von FIDO2

Das FIDO-Konsortiums entstand im Jahr 2012. Angesichts der wachsenden Bedrohungen durch Passwortdiebstahl, Phishing-Angriffe und andere Sicherheitsrisiken erkannten Experten die Schwächen herkömmlicher Passwörter. Das Konsortium wurde ins Leben gerufen, um die Entwicklung von sichereren und benutzerfreundlicheren Authentifizierungsmethoden voranzutreiben. FIDO2 steht als Ergebnis dieser Bemühungen im Mittelpunkt.

3.2.2 Die Evolution von FIDO zu FIDO2: Ein Überblick

Die ersten Schritte des FIDO-Konsortiums führten zur Einführung von FIDO UAF (Universal Authentication Framework). Dabei lag der Fokus auf der Integration von biometrischen Daten für eine stärkere Sicherheit. Allerdings stellte sich heraus, dass ein umfassenderer Ansatz notwendig war. FIDO U2F (Universal Second Factor) wurde daraufhin entwickelt, um die 2FA zu verbessern. FIDO2, als nächster evolutionärer Schritt, kombiniert zwei Protokolle: das Web Authentication API (WebAuthn) und das Client-to-Authenticator Protocol (CTAP). Dies ermöglicht eine noch robustere und vielseitigere Authentifizierungsmethode.

[23] Fitzwilliam Anderson, (06. Juni 2023). FIDO-Authentifizierung: Die Geschichte der Fido Alliance, das Versprechen von FIDO2 und Passkeys.

3.2.3 Die Forschung und Entwicklung im FIDO-Konsortium

Die Entwicklung von FIDO2 basierte auf intensiver Forschung und Kooperation innerhalb des Konsortiums. Experten aus verschiedenen Disziplinen brachten ihr Wissen in die Entwicklung ein. Dabei wurden nicht nur technische Aspekte berücksichtigt, sondern auch Benutzerfreundlichkeit und Skalierbarkeit. Diese umfassende Herangehensweise trug dazu bei, ein Authentifizierungssystem zu schaffen, das den Anforderungen moderner digitaler Welt gerecht wird.[24]

3.3 Wie funktioniert FIDO2?

3.3.1 Die Kryptografie hinter FIDO2: Public Key Cryptography

Der Kern von FIDO2 liegt in der Public Key Cryptography (Asymmetrische Kryptografie). Anstelle eines gemeinsamen Passworts erzeugt der Benutzer ein Schlüsselpaar: einen privaten Schlüssel, der auf dem Authenticator gespeichert wird, und einen öffentlichen Schlüssel, der an den Dienst übermittelt wird. Während der Registrierung wird der öffentliche Schlüssel mit dem Benutzerkonto verknüpft.

3.3.2 Das Registrierungsverfahren von FIDO2

3.3.2.1 Registrierung eines Authenticators

Die Authentifizierung mit FIDO2 beginnt mit der Registrierung eines Authentifikators – einem physischen Gerät wie zum Beispiel ein USB-Sicherheitsschlüssel oder einer biometrischen Methode, die zur Authentifizierung des Benutzers verwendet wird. Ein Authentifikator kann beispielsweise ein Sicherheitsschlüssel, ein Fingerabdruckleser oder ein Gesichtsscanner sein.

3.3.2.2 Generierung eines Schlüsselpaars

Während der Registrierung erzeugt der Authentifikator ein asymmetrisches Schlüsselpaar – einen privaten Schlüssel und einen öffentlichen Schlüssel. Bei der Verwendung biometrischer Authentifizierungsmethoden wie Fingerabdruck-

[24] N. Bindel, C. Cremers and M. Zhao, (Mai 2023). FIDO2, CTAP 2.1, and WebAuthn 2: Provable Security and Post-Quantum Instantiation. *2023 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 2023, (S. 1471-1490).

erkennung oder Gesichtserkennung wird der private Schlüssel in der Regel auf dem Gerät gespeichert, auf dem die Authentifizierung durchgeführt wird. Bei Verwendung eines FIDO2-Schlüssels bleibt der private Schlüssel ausschließlich auf dem FIDO2-Schlüssel (auch als Sicherheitsschlüssel bekannt) und verlässt den Schlüssel selbst nicht. Dies ist ein grundlegender Aspekt des FIDO2-Sicherheitsmodells.
Der öffentliche Schlüssel wird mit einer eindeutigen Kennung (Attestation) an den Dienst übertragen, bei dem der Benutzer sich registriert.

3.3.2.3 Verknüpfung des öffentlichen Schlüssels mit dem Benutzerkonto

Der öffentliche Schlüssel wird mit dem Benutzerkonto beim Dienst verknüpft. Dies ermöglicht es dem Dienst, den Benutzer anhand seines Authenticators zu identifizieren.

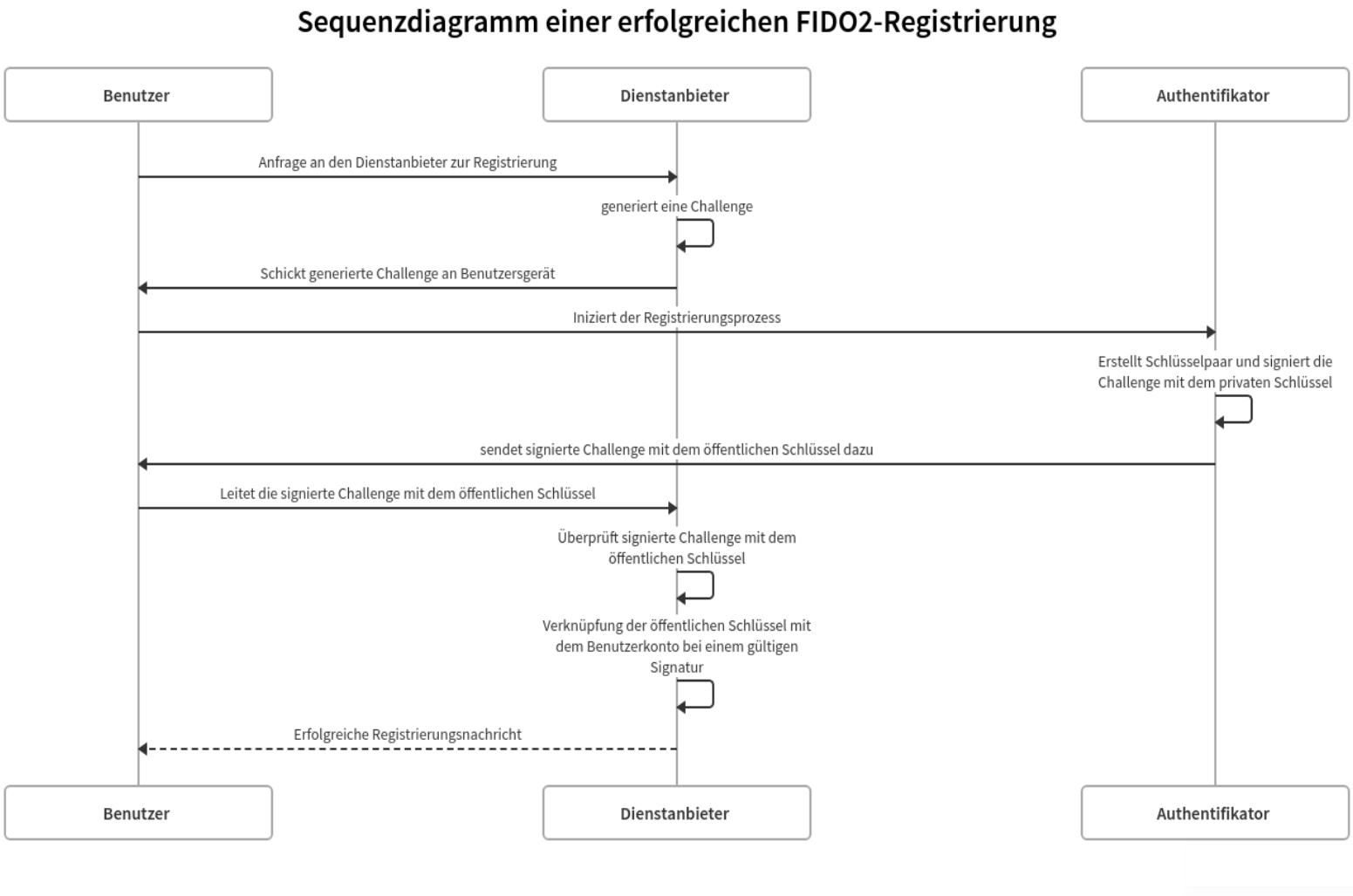


Abbildung 1: Sequenzdiagramm einer erfolgreichen FIDO2-Registrierung

3.3.3 Der Authentifizierungsvorgang

3.3.3.1 Herausforderung erstellen

Wenn der Benutzer sich später anmelden möchte, sendet der Dienst eine zufällige Challenge.

3.3.3.2 Signierung der Herausforderung

Der Authenticator erhält die Herausforderung und verwendet seinen gespeicherten privaten Schlüssel, um die Herausforderung zu signieren. Die Signatur eine eindeutige Antwort auf die Challenge.

3.3.3.3 Übermittlung der signierten Antwort

Die signierte Antwort wird an den Dienst zurückgesendet.

3.3.3.4 Verifizierung der Antwort

Der Dienst verwendet den zuvor mit dem Benutzerkonto verknüpften, öffentlichen Schlüssel, um die erhaltene signierte Antwort zu überprüfen. Wenn die Signatur verifiziert werden kann, weiß der Dienst, dass der Authenticator legitim ist und der Benutzer erfolgreich authentifiziert wurde.

3.3.3.5 Zugriff gewähren

Nach erfolgreicher Verifizierung gewährt der Dienst dem Benutzer den gewünschten Zugriff oder die gewünschte Funktion.

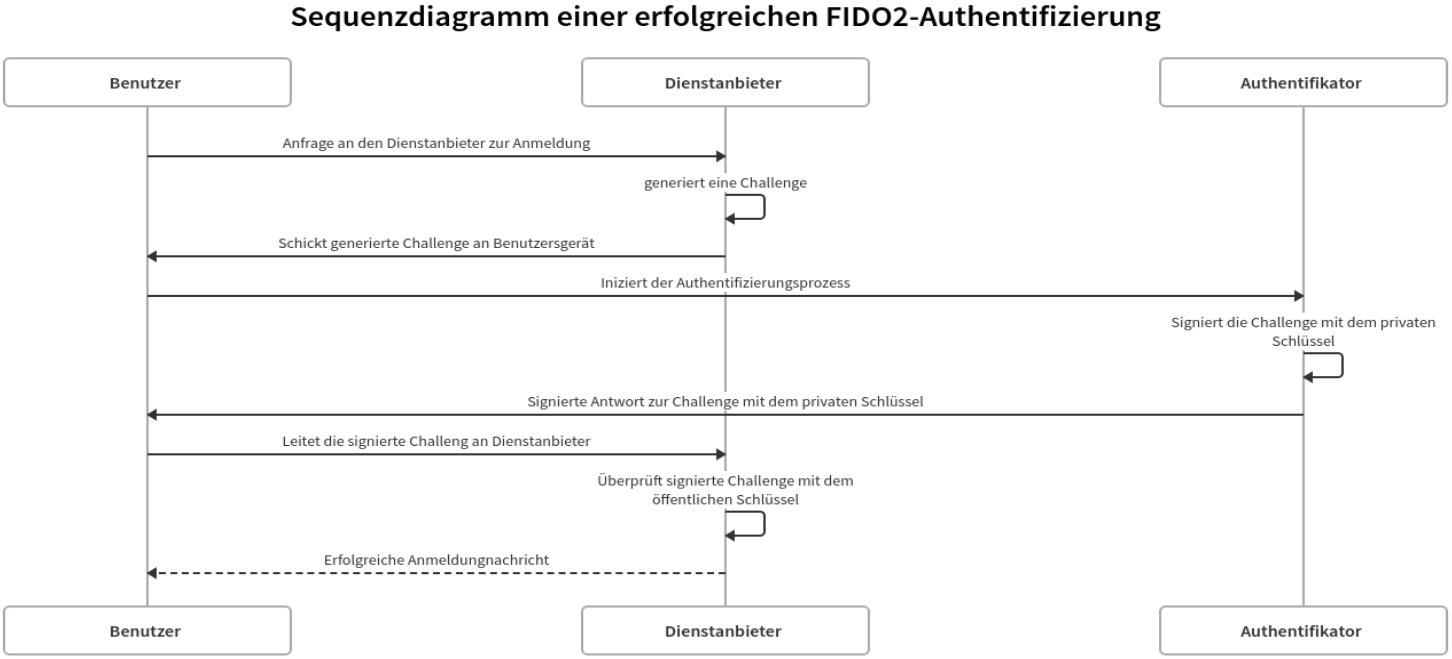


Abbildung 2: Sequenzdiagramm einer erfolgreichen FIDO2-Authentifizierung

4 Passkey

4.1 Die Einleitung für Passkey

Die digitale Welt hat sich zu einem Raum entwickelt, in dem unsere persönlichen Daten und Identitäten ständig gefährdet sind. Cyberschurken sind äußerst geschickt darin, Millionen von Konten zu übernehmen, und meistens nutzen sie dazu den Schwachpunkt des Passwortsystems. In einer Welt, in der fast jede Facette unseres Lebens digitalisiert ist, sind Passwörter zu einem entscheidenden Bindeglied zwischen unserer Online-Identität und den böswilligen Absichten von Cyberkriminellen geworden. Die täglichen Nachrichtenberichte über Datenverstöße und Kontoübernahmen sind ein alarmierender Beweis für die Dringlichkeit, mit der wir uns der Sicherheit unserer Online-Identitäten widmen müssen.

Analysen von Passwort-Leaks zeigen, dass die klassische Passwort-Authentifizierung jedoch erhebliche Schwächen aufweist, da viele Nutzer dazu tendieren, schwache Passwörter zu wählen und diese dann auch gleich bei mehreren Webdiensten einzusetzen, was Hacker leicht ausnutzen können. Dieses Problem wird durch die Tatsache verschärft, dass es schwierig ist, sich eine große Anzahl von komplexen Passwörtern zu merken. Die rettende, aber umständliche Zwei-Faktor-Authentifizierung wird aus Bequemlichkeit oft ignoriert.[25] In diesem Kontext stellt diese Arbeit die Passkey-Technologie vor, die eine moderne Alternative zur herkömmlichen Passwort-Authentifizierung bietet.

4.2 Die Geburt der Passkeys

Die Passkey-Technologie hat das Potenzial, die Herausforderungen bei der 2FA zu überwinden und die Art und Weise, wie wir uns online authentifizieren, grundlegend zu verändern. Statt auf Passwörter zurückzugreifen, erhalten Benutzer für jeden ihrer Accounts einen individuellen Passkey. Dieser Passkey

[25] R. Eikenberg, (2023). Passkeys im Einsatz.

wird sicher auf ihrem Gerät gespeichert und kann verwendet werden, um sich bei verschiedenen Diensten anzumelden, ohne ein Passwort eingeben zu müssen.

Die Idee hinter den Passkeys ist die Verwendung von Public-Key-Kryptografie. Jeder Benutzer hat ein kryptografisches Schlüsselpaar, das aus einem öffentlichen und einem privaten Schlüssel besteht. Der öffentliche Schlüssel wird an den Dienst übergeben, mit dem sich der Benutzer anmelden möchte, während der private Schlüssel nur dem Benutzer bekannt ist.

4.3 Wie Passkey funktioniert?

Die Passkey-Technologie bringt eine signifikante Veränderung in der Art und Weise, wie Menschen sich online authentifizieren, da sie auf dem Konzept von FIDO2 basiert. Anstelle traditioneller Passwörter, die oft Schwachstellen aufweisen und von Cyberkriminellen leicht geknackt werden können, verwendet Passkey Public-Key-Kryptografie, um eine sicherere und benutzerfreundlichere Methode der Authentifizierung zu bieten.

4.3.1 Die Public-Key-Kryptografie: Der Schlüssel zum Passkey

Die Grundlage von Passkeys ist die Public-Key-Kryptografie, eine bewährte Methode zur Verschlüsselung von Daten und zur Sicherstellung der Identität von Benutzern. Bei der Public-Key-Kryptografie gibt es zwei Schlüssel: einen öffentlichen und einen privaten. Der öffentliche Schlüssel kann frei verteilt werden und wird normalerweise mit dem Benutzerkonto verknüpft, während der private Schlüssel geheim bleibt und nur dem Benutzer bekannt ist.

4.3.2 Schritt 1: Schlüsselpaar generieren

Der erste Schritt zur Verwendung von Passkeys besteht darin, ein einzigartiges Schlüsselpaar zu generieren. Dieses Schlüsselpaar wird normalerweise auf dem Gerät des Benutzers erstellt, beispielsweise auf einem Smartphone oder einem Sicherheitschip im Computer. Dieses Schlüsselpaar besteht aus einem

öffentlichen Schlüssel, der mit dem Benutzerkonto verknüpft wird, und einem privaten Schlüssel, der geheim gehalten wird.

4.3.3 Schritt 2: Verknüpfung mit dem Benutzerkonto

Der öffentliche Schlüssel wird nun mit dem Benutzerkonto verknüpft. Dies geschieht normalerweise, wenn der Benutzer sich bei einem Dienst anmeldet und den öffentlichen Schlüssel mit seinem Konto verknüpft. Der Dienst speichert diesen öffentlichen Schlüssel in seiner Datenbank.

4.3.4 Schritt 3: Anmeldung mit einem Passkey

Wenn der Benutzer sich bei einem Dienst anmelden möchte, sendet der Dienst eine zufällige Challenge an das Gerät des Benutzers. Diese Challenge ist eine einzigartige Anfrage, die jedes Mal unterschiedlich ist.

4.3.5 Schritt 4: Signieren der Challenge

Das Gerät des Benutzers verwendet den privaten Schlüssel, um die Challenge digital zu signieren. Dies bedeutet, dass das Gerät eine verschlüsselte Antwort erstellt, die nur mit dem öffentlichen Schlüssel des Benutzers überprüft werden kann. Die signierte Challenge wird dann an den Dienst zurückgesendet.

4.3.6 Schritt 5: Überprüfung durch den Dienst

Der Dienst empfängt die signierte Challenge und verwendet den zuvor mit dem Benutzerkonto verknüpften öffentlichen Schlüssel, um die Signatur zu überprüfen. Wenn die Überprüfung erfolgreich ist, weiß der Dienst, dass der Benutzer im Besitz des privaten Schlüssels ist und somit legitim ist. Die Anmeldung wird genehmigt, und der Benutzer erhält Zugriff auf sein Konto.

4.4 Die Vorteile von Passkeys

4.4.1 Die höhere Sicherheit

Passkeys bieten eine höhere Sicherheit, da sie auf Public-Key-Kryptografie basieren. Selbst wenn ein Angreifer das Passwort eines Benutzers kennt, kann er ohne den privaten Schlüssel keinen Zugriff auf das Konto erhalten. Dies macht Passkeys äußerst robust gegenüber Brute-Force-Angriffen und Phishing-Versuchen.

4.4.2 Die Benutzerfreundlichkeit

Passkeys sind benutzerfreundlich, da sie keine Notwendigkeit für das Merken komplexer Passwörter oder das Aktivieren von Zwei-Faktor-Authentifizierungscodes erfordern. Die Anmeldung erfolgt mit nur einem Klick oder einer biometrischen Verifizierung, was den Prozess erheblich beschleunigt.

4.4.3 Der Phishing-Schutz

Passkeys sind phishingsicher, da sie für jeden Dienst eindeutig sind und nicht zwischen verschiedenen Domains geteilt werden. Selbst wenn ein Benutzer auf eine gefälschte Website gelockt wird, kann der Angreifer den Passkey nicht verwenden, da er nicht für diese Domain erstellt wurde.

4.4.4 Der Schutz der Privatsphäre

Passkeys schützen die Privatsphäre der Benutzer, da keine sensiblen Informationen über das Netzwerk übertragen werden. Die Signierung der Challenge erfolgt lokal auf dem Gerät des Benutzers, und der private Schlüssel verlässt nie das Gerät

4.4.5 Die Skalierbarkeit

Passkeys sind skalierbar und können für eine Vielzahl von Diensten und Anwendungen verwendet werden. Ein Benutzer kann Passkeys für E-Mail, soziale Medien, Bankkonten und mehr verwenden, ohne sich Gedanken über die Verwaltung von Dutzenden von Passwörtern machen zu müssen.

Passkeys können auch über die iCloud von Apple und die Herstellercloud von Google zwischen Geräten im selben Produktuniversum synchronisiert werden und lassen sich aufgrund der Cloudspeicherung auch dann wiederherstellen, wenn alle Geräte verloren gehen.

Daher ist es möglich, Passkeys auf modernen Handys ab iOS 16 auf iPhones, ab macOS 13 auf Macs und ab Android 9 auf Android-Telefonen zu speichern.[27] Auf diese Weise können Sie sicherstellen, dass Sie jederzeit von Ihrem Cloud-System darauf zugreifen können, falls Unannehmlichkeiten auftreten. Dies bietet eine zusätzliche Sicherheitsebene für die Passkey-Authentifizierung und erleichtert die Verwendung über verschiedene Geräte hinweg.

Insgesamt bietet die Passkey-Technologie eine vielversprechende Alternative zu herkömmlichen Passwörtern und trägt dazu bei, die Sicherheit unserer digitalen Identitäten erheblich zu verbessern. Mit der wachsenden Integration von Passkey-Technologien in Webdiensten und Betriebssystemen könnte dies den Beginn einer bedeutenden Phase in der Online-Sicherheitsentwicklung markieren.

4.4.6 Wo wird FIDO2/Passkey aktuell verwendet?

Passkey, auch bekannt als FIDO2-basierte Passwortlose Authentifizierung, wird von einer wachsenden Anzahl von Webdiensten unterstützt. Diese Methode zur Authentifizierung von Benutzern bietet erhebliche Vorteile in Bezug auf Sicherheit und Benutzerfreundlichkeit. Es ist wichtig zu beachten, dass die Verfügbarkeit von Passkey-Unterstützung je nach Region und Website variieren kann. Benutzer sollten die Sicherheitseinstellungen ihrer Online-Konten regelmäßig überprüfen und die neuesten Empfehlungen zur Verbesserung der Sicherheit befolgen. Eine aktuelle Liste von Webdiensten, die Passkey verwenden, finden Sie auf der offiziellen Website der FIDO Alliance unter https://passkeys.directory/. Diese Liste wird ständig aktualisiert, da immer mehr Websites diese fortschrittliche Authentifizierungsoption implementieren. Hier sind einige Beispiele für Webdienste und Online-Plattformen, die bereits Passkey-Authentifizierung unterstützen:

[27] Google Identity. Passkey-Unterstützung für Android und Chrome.

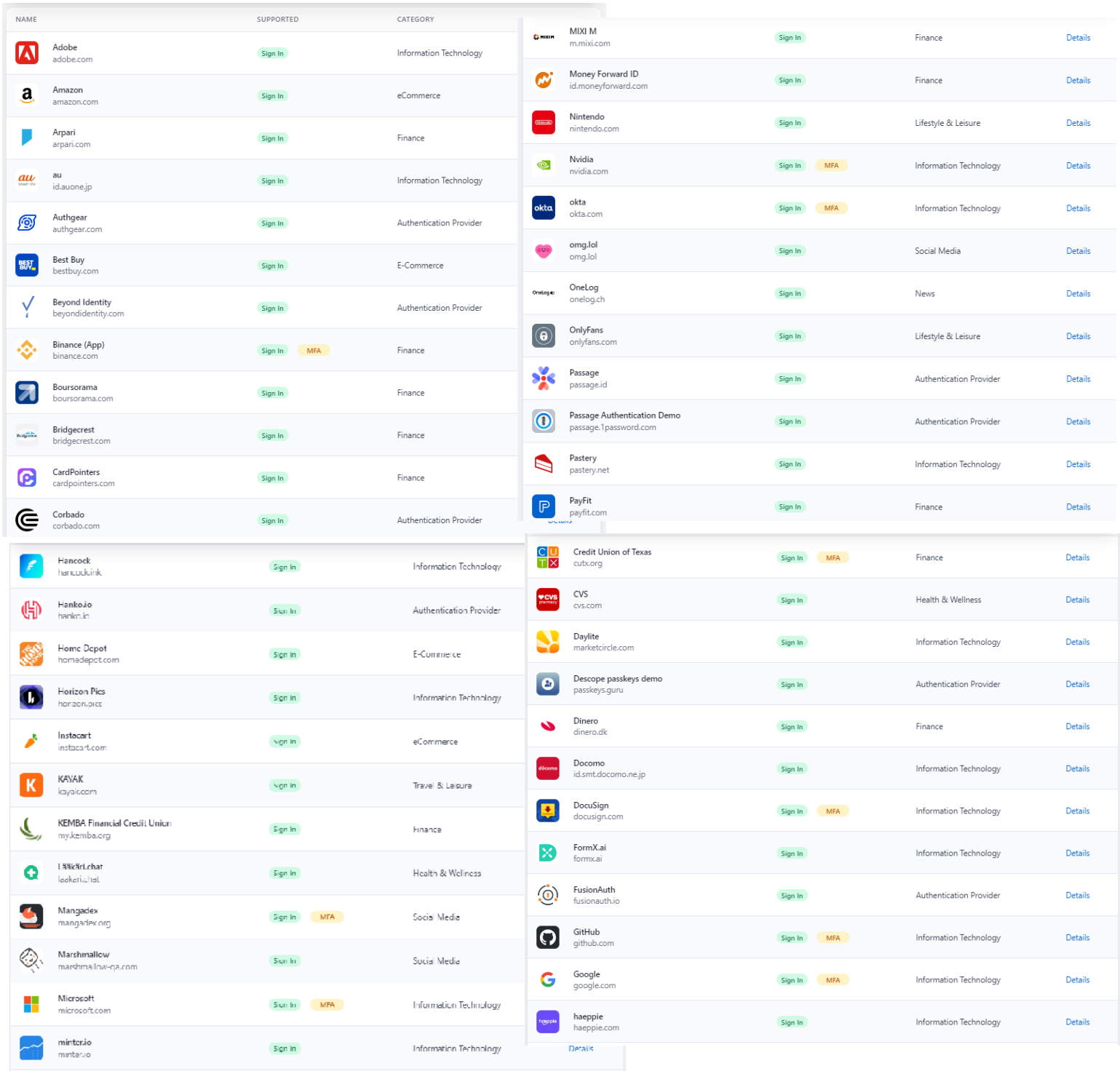
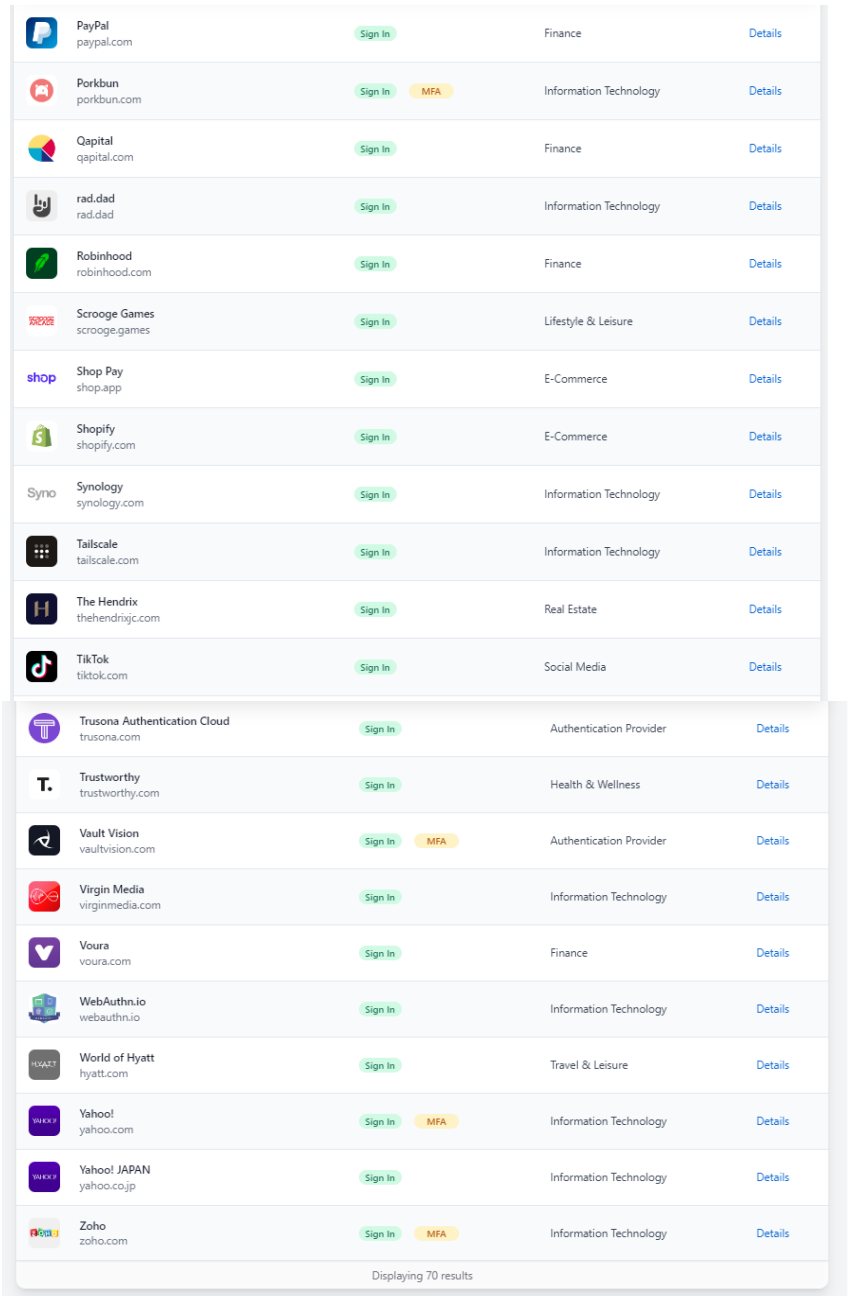


Abbildung 3: Webdienste und Online-Plattformen, die Passkey-Authentifizierung unterstützen, basierend auf Informationen von https://passkeys.directory/



PayPal paypal.com	Sign In		Finance	Details
Porkbun porkbun.com	Sign In	MFA	Information Technology	Details
Qapital qapital.com	Sign In		Finance	Details
rad.dad rad.dad	Sign In		Information Technology	Details
Robinhood robinhood.com	Sign In		Finance	Details
Scrooge Games scrooge.games	Sign In		Lifestyle & Leisure	Details
Shop Pay shop.app	Sign In		E-Commerce	Details
Shopify shopify.com	Sign In		E-Commerce	Details
Synology synology.com	Sign In		Information Technology	Details
Tailscale tailscale.com	Sign In		Information Technology	Details
The Hendrix thehendrixjc.com	Sign In		Real Estate	Details
TikTok tiktok.com	Sign In		Social Media	Details
Trusona Authentication Cloud trusona.com	Sign In		Authentication Provider	Details
Trustworthy trustworthy.com	Sign In		Health & Wellness	Details
Vault Vision vaultvision.com	Sign In	MFA	Authentication Provider	Details
Virgin Media virginmedia.com	Sign In		Information Technology	Details
Voura voura.com	Sign In		Finance	Details
WebAuthn.io webauthn.io	Sign In		Information Technology	Details
World of Hyatt hyatt.com	Sign In		Travel & Leisure	Details
Yahoo! yahoo.com	Sign In	MFA	Information Technology	Details
Yahoo! JAPAN yahoo.co.jp	Sign In		Information Technology	Details
Zoho zoho.com	Sign In	MFA	Information Technology	Details

Displaying 70 results

Abbildung 4: Webdienste und Online-Plattformen, die Passkey-Authentifizierung unterstützen, basierend auf Informationen von https://passkeys.directory/

5 Phishing-Schutz durch Passkeys im Vergleich zur herkömmlichen Anmeldung

Hier wird die bemerkenswerte Fähigkeit von Passkeys zur Abwehr von Phishing-Attacken untersucht und sie mit herkömmlichen Anmeldeverfahren vergleichen, sowohl mit Passwörtern als auch mit der 2-Faktor-Authentifizierung (2FA) unter Verwendung von Authentifikatoren wie der Google Authenticator-App auf einem Mobilgerät.

5.1 Der Phishing-Schutz durch Passkeys

Eines der herausragendsten Merkmale von Passkeys ist ihre Phishing-Resistenz. Dies liegt an ihrer Fähigkeit, den Identitätsdiebstahl durch gefälschte Anmeldeseiten erheblich zu erschweren. Hier ist, wie Passkeys Phishing verhindern.

5.1.1 Die Anbindung an die Domain

Passkeys sind eng an die Domain des Webdienstes gebunden. Wenn man sich bei einem Dienst wie Google anmeldet, wird der Passkey speziell für die URL der Anmeldseite von Google generiert. Wenn ein Angreifer versucht, das Opfer auf eine gefälschte Google-Anmeldeseite umzuleiten, wird Ihr Passkey nicht funktionieren, da er nur für die legitime Google-Domain erstellt wurde.

5.1.2 Die schwierige Nachahmung

Phishing-Angriffe erfordern oft die Erstellung gefälschter Anmeldeseiten, die denen der legitimen Dienste ähneln. Da Passkeys spezifisch für Domains sind, ist es für Angreifer viel schwieriger, gefälschte Anmeldeseiten für verschiedene Websites zu erstellen, die die Passkeys des Benutzers akzeptieren würden.

5.1.3 Die digitale Signatur

Passkeys verwenden Public-Key-Kryptografie, um die digitale Signatur der Anmeldungsanfrage zu überprüfen. Da diese Signatur nur mit dem privaten Schlüssel des Benutzers erstellt werden kann, kann sie nicht von Phishern repliziert werden, die keinen Zugriff auf den privaten Schlüssel haben.

5.2 Vergleich mit der herkömmlichen Google-Anmeldung

5.2.1 Die Anmeldung mit Passwort

Bei der herkömmlichen Anmeldung mit einem Passwort besteht die Hauptgefahr darin, dass Benutzer dazu verleitet werden können, ihre Anmeldedaten auf gefälschten Websites preiszugeben. Phisher können Benutzer mit gefälschten E-Mails oder Links austricksen und dazu bringen, ihre Anmeldedaten auf gefälschten Anmeldeseiten einzugeben.

5.2.2 Die Anmeldung mit 2FA und Authentificator-App

Bei der Verwendung von 2FA mit einer Authenticator-App ist die Sicherheit höher als bei einem einfachen Passwort. Der Benutzer muss neben seinem Passwort auch einen einmaligen Code eingeben, der von der Authenticator-App generiert wird. Dieser Code ändert sich alle Sekunden und ist daher schwieriger zu stehlen. Dennoch können Benutzer dazu verleitet werden, den Code auf gefälschten Websites einzugeben, wenn sie einer Phishing-E-Mail oder einem gefälschten Link folgen.

Fazit

Passkeys bieten im Vergleich zur herkömmlichen Anmeldung bei Google mit Passwörtern oder 2FA einen erheblichen Vorteil beim Schutz vor Phishing-Angriffen. Durch die enge Bindung an Domains, die Verwendung von Public-Key-Kryptografie und die Unmöglichkeit, gefälschte digitale Signaturen zu erstellen, machen Passkeys es für Phisher äußerst schwierig, erfolgreiche Angriffe durchzuführen. Während herkömmliche Anmeldeverfahren nach wie vor sinnvoll

sind, zeigt die Phishing-Resistenz von Passkeys, dass sie eine vielversprechende Option zur Verbesserung der Online-Sicherheit darstellen.

6 Demonstration einer Man-in-the-Middle-Attacke in einer Passkey-unterstützenden Umgebung im Vergleich zu einer Passwort-unterstützenden Umgebung und 2FA unterstützenden Umgebung (Handy).

Die Sicherheit von Online-Konten und die Verwaltung persönlicher Daten sind von zentraler Bedeutung in unserer zunehmend digitalisierten Welt. Phishing-Angriffe sind nach wie vor eine erhebliche Bedrohung, bei denen Angreifer versuchen, sensible Informationen von ahnungslosen Opfern zu stehlen. Daher ist es von entscheidender Bedeutung, die Wirksamkeit der von uns verwendeten Authentifizierungsmethoden zu verstehen.

Um die erhöhte Phishing-Resistenz der Passkey-Authentifizierung im Vergleich zu anderen Authentifizierungsmethoden praktisch zu demonstrieren, wird einer sogenannte Man-in-the-Middle-Angriff simuliert. In diesem Szenario wird eine Phishing-E-Mail erstellt und eine Person namens Josephine Tanko ins Visier nehmen. Frau Tanko ist 56 Jahre alt und verfügt über begrenzte IT-Kenntnisse. Frau Tanko repräsentiert einen Nutzertyp, der sich nicht gut mit Informationstechnologie auskennt und Schwierigkeiten mit technikbezogenen Angelegenheiten haben könnte.

Diese E-Mail wird als unser Werkzeug dienen, um zu veranschaulichen, wie Cyberangreifer leicht verwundbare Nutzer ausnutzen können, um unberechtigten Zugriff auf deren persönliche Informationen zu erlangen. Im nachfolgenden Kapitel dieser Arbeit werde ich die Effektivität verschiedener Login-Methoden, die zuvor besprochen wurden, kritisch analysieren und vergleichen.

6.1 Versuchsaufbau

Für den Versuch wurde ein Lenovo IdeaPad Flex 5 Notebook verwendet, auf dem Windows 11 als Betriebssystem installiert war. Um die Website zu klonen, wurden die verschiedenen Login-Seiten kopiert und lokal in einer Datei gespeichert, die

sowohl die E-Mail-, Passwort- als auch 2FA-Seiten enthielt. Diese Seiten wurden anschließend mit Visual Studio Code geöffnet, und alle erforderlichen Bearbeitungen fanden dort statt.

Darüber hinaus wurde für das Projekt ein Backend und ein Frontend verwendet. Das Backend wurde in Node.js mit Express entwickelt. Dies ermöglichte die Erstellung von Routen, um Weiterleitungen durchzuführen, sowie die Erstellung eines Konto-Objekts zur Erfassung der Benutzerdaten. Im Backend-Projekt wurden Routen erstellt, um die Weiterleitungen zwischen den verschiedenen Seiten durchzuführen und die Benutzerdaten zu verarbeiten.

Es wurde sichergestellt, dass die eingegebene E-Mail-Adresse auf den weiteren Seiten übertragen wurde. Dies gewährleistete, dass die Daten auf den gefälschten Seiten dynamisch und realistisch erschienen.

6.1.1 Die Erstellung der Phishing-Email

Das Ziel hierbei ist, eine Sicherheitswarnungs-E-Mail für das Opfer zu erstellen, in der ihr mitgeteilt wird, dass ihr Konto in Gefahr ist und sie aus Sicherheitsgründen aufgefordert wird, sich in ihr Konto einzuloggen und ihr Passwort zu ändern, um weitere mögliche Probleme zu vermeiden. Der Call-To-Action-Button in Rot in der E-Mail wird das Opfer jedoch nicht zur offiziellen Google-Login-Website führen, sondern zu unserer täuschend echt aussehenden Login-Seite, die geklont wurde.

Um eine täuschend ähnliche E-Mail zu erstellen, wurde eine Sicherheitswarnungs-E-Mail (siehe Abbildung 5) identisch erstellt, sodass sie genauso aussieht (siehe Abbildung 6), um sie wirklich ähnlich aussehen zu lassen wie die E-Mails, die von Google gesendet werden. Alles in dieser E-Mail ist identisch mit dem, was wir von Google erhalten. Diese E-Mail wird später in dieser Form an das Opfer gesendet.

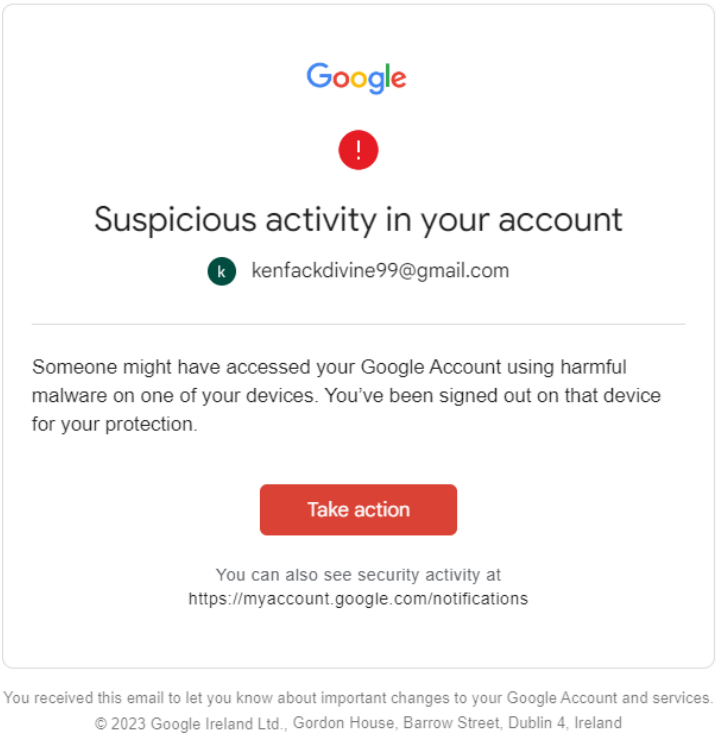


Abbildung 5 : Echte Sicherheitswarnungs-E-Mail

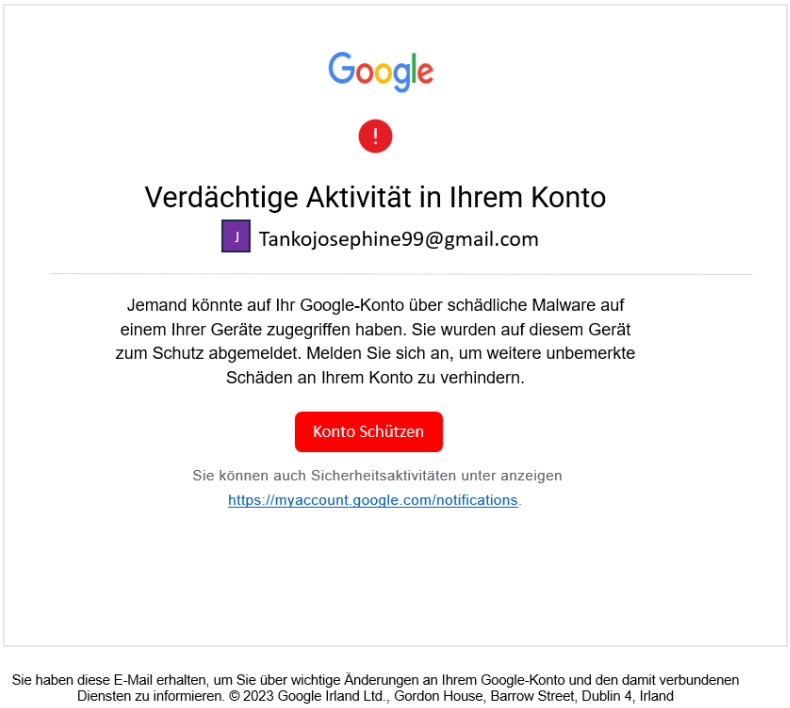


Abbildung 6: Phishing E-Mail, die dem Opfer geschickt werden wird

6.1.2 Der Versand und das Öffnen der Phishing-E-Mail

Nachdem die Phishing-E-Mail erstellt wurde, müssen wir einen E-Mail-Server mit einer E-Mail verwenden, die identisch mit der von Google Security Alert ist, um den Anschein zu erwecken, dass sie von Google stammt. Dafür werde ich einen Trick mit der E-Mail-Adresse von Google anwenden, um sie auf den ersten Blick sehr real aussehen zu lassen.

Die Original-E-Mail lautet "no-reply@accounts.google.com" (siehe Abbildung 7). Ich entfernte einfach ein "c" und das "s" am Ende des Wortes "account" , sodass die abschließende Absender-E-Mail-Adresse "no-reply@acount.google.com" lautet.

Diese E-Mail wird es für den Absender schwieriger machen, Zweifel an ihrer Herkunft zu hegen.

Abbildung 7: Originale Sicherheitswarnungs-E-Mail-Adresse

6.2 Phishing-Resistenz von Passkeys: Eine empirische Untersuchung und Vergleichsanalyse

Nachdem das Opfer die E-Mail-Adresse erhalten hat, die wir im besten Fall simulieren, wird das Opfer auf die Schaltfläche "Konto schützen" klicken. Die Antwort darauf ist die Weiterleitung auf unsere identisch geklonte Google-Anmeldemaske (siehe Abbildung 8). Diese Seite sieht genauso aus wie die originale Google-Seite.

Nach dem Eintreffen auf dieser Seite wurden drei verschiedene Szenarien beobachtet und bewertet, wie einfach es für den Angreifer ist, auf die Anmeldedaten des Opfers zuzugreifen.

Unser Beispiel-Szenario hier erfolgt in Echtzeit, das bedeutet, dass es parallel im Hintergrund aktiv gearbeitet wird, während das Opfer seine Informationen auf der geklonten Seite eingibt. Die Informationen werden verwendet, die im

Hintergrund gesammelt werden, um später auf der echten Google-Anmeldeseite die Anmeldung durchzuführen.

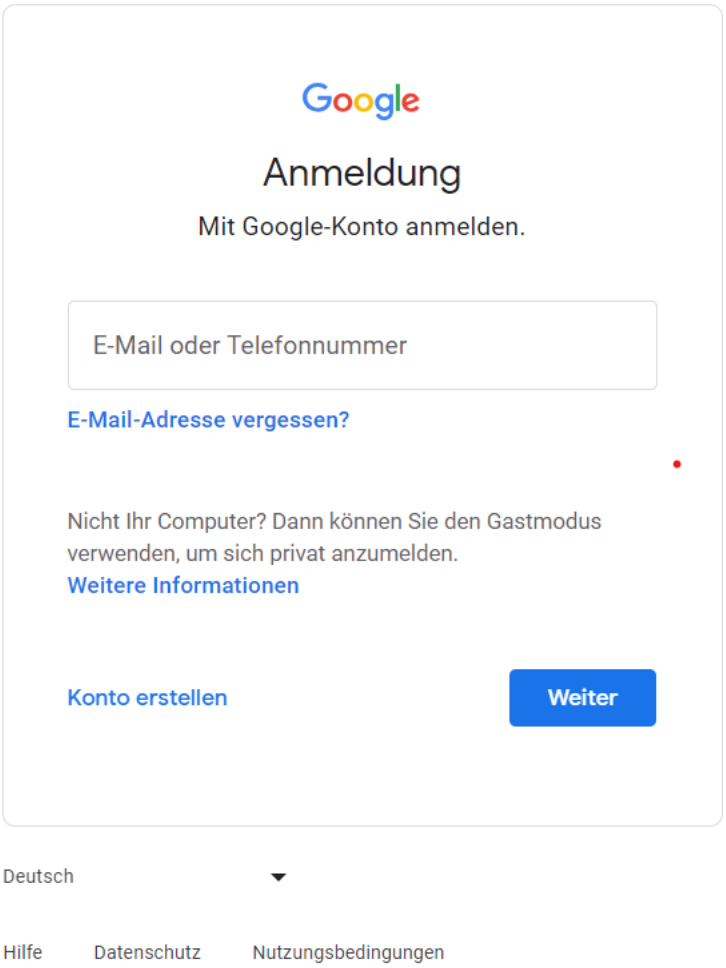


Abbildung 8: Identisch geklonte Google-Maske

Im Backend wird das Skript mit dem Befehl "node app.js" durchgeführt, wie in Abbildung 9 dargestellt. In dieser PowerShell-Konsole können alle Informationen, die vom Opfercomputer eingegeben werden, in Echtzeit auf unserem eigenen Computer angezeigt werden. Die zu diesem Zeitpunkt angezeigten Informationen können, wie bereits erwähnt, verwendet werden, um sich bei Google anzumelden und somit das Opfer anfällig zu machen. Sobald eine E-Mail-Adresse auf unserer geklonten Seite eingegeben wird, werden die Informationen aus den leeren Feldern abgerufen und auf der PowerShell-Befehlszeile angezeigt.

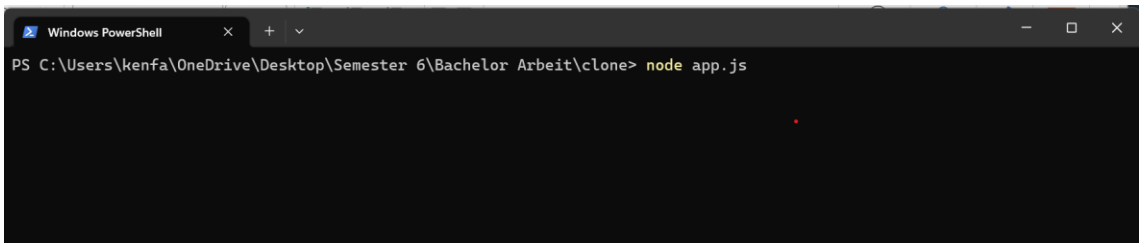


Abbildung 9: Ausführung des Scripts auf der PowerShell-Befehlszeile

Da für diese Simulation der Code von meinem Computer ausgeführt wird, haben wir eine Adresse, die lokal in meinem Netzwerk verfügbar ist. Es ist auch möglich, das Programm über das Internet für andere verfügbar zu machen. Dafür müsste nur ein Server gekauft oder gemietet werden, von dem aus es ausgeführt wird. Dies fällt jedoch nicht in meinem Rahmen, weshalb alles lokal zu Bildungszwecken durchgeführt wird. Wie in Abbildung 10 zu sehen ist, kannr unser Programm lokal auf dem „localhost 3000"ausgeführt werden.

Nun kann beobachtet werden, wie die geklonte Google-Anmeldeseite auf dem „localhost 3000" läuft, wie in Abbildung 11 gezeigt, nachdem das Programm ausgeführt wurde. Dies ist die Seite, auf der das Opfer landen wird.

Abbildung 10: Ausgabe der Adresse auf der die Seite zu erreichen ist

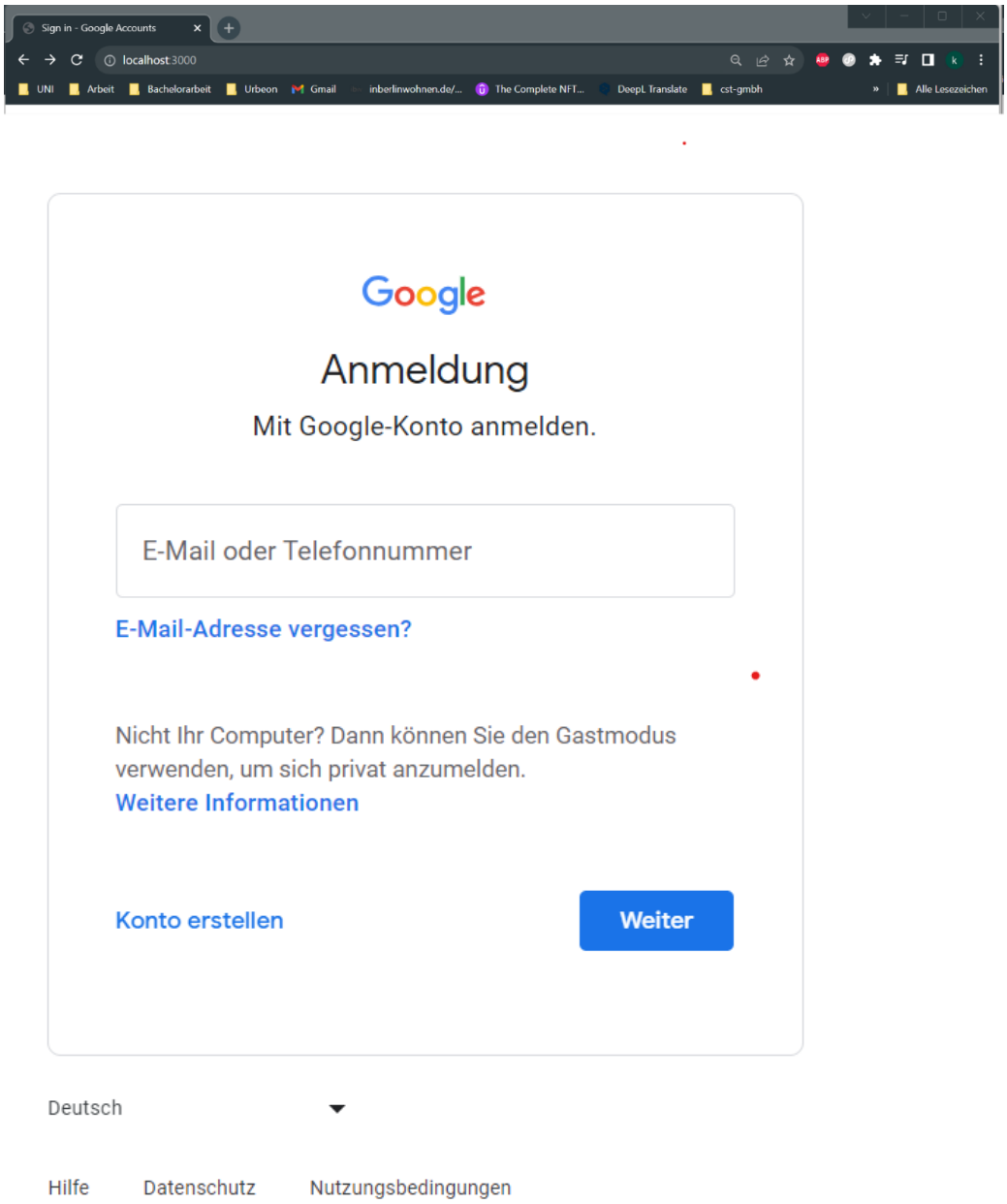


Abbildung 11: Identisch geklonte Google-Maske die auf localhost 3000 läuft

Nun geheich in die Untersuchung, in der ich meinen Fokus auf drei Hauptauthentifizierungsszenarien richte, um ihre Sicherheit und Widerstandsfähigkeit gegenüber einem Man-In-The-Middle-Angriff zu bewerten. Das Ziel besteht darin, die Schwächen und Stärken dieser Authentifizierungsmethoden im Hinblick auf Phishing-Angriffe aufzudecken.

Josephine Tanko, die hier als Opfer ist, wird sich mit den folgenden zuvor erstellten Anmeldinformationen anmelden können, die speziell für diese Untersuchung bereitgestellt wurde.

Email: Tankojosephine99@gmail.com
Passwort: Bachelor23#

6.2.1 Scenario 1: Anmeldung mit E-Mail-Adresse und Passwort

In diesem ersten Szenario werden wir beobachten, wie einfach es ist, die Informationen des Opfers zu erhalten, wenn es die traditionelle Authentifizierungsmethode verwendet, bei der die E-Mail-Adresse und das Passwort erforderlich sind.

Nachdem das Opfer die E-Mail erhalten und auf den Handlungsaufruf-Button geklickt hat, landet es Eile auf der geklonten Seite. In diesem Moment gibt Josephine Tanko ihre E-Mail-Adresse ein, wie in Abbildung 12 unten zu sehen ist.

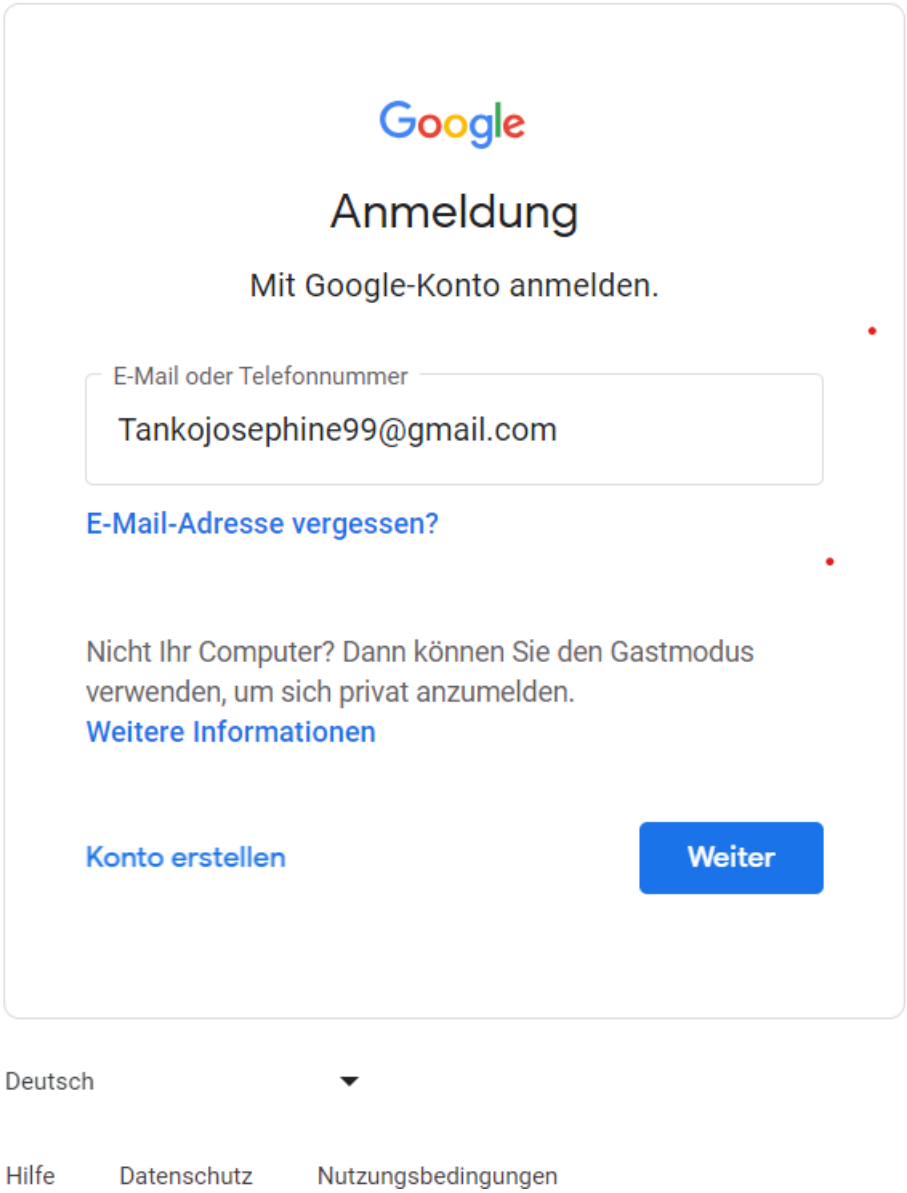


Abbildung 12: Eingabe der E-Mail-Adresse des Opfers

Nachdem sie diese Informationen eingegeben hat, empfangen wir im Hintergrund alles, was sie eingegeben hat, wie in Abbildung 13 unten zu sehen ist.

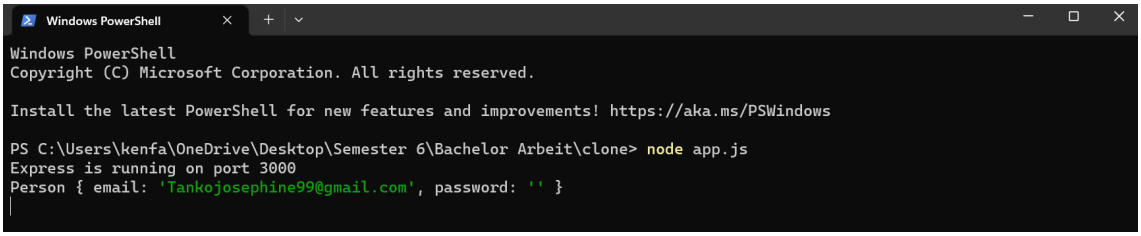


Abbildung 13: Empfang der E-Mail-Adresse von der Seite im Backend

Nachdem sie ihre E-Mail-Adresse eingegeben hat, wird sie bald zur zweiten Phase der traditionellen Authentifizierung geleitet, bei der sie ihr Passwort eingeben muss (siehe Abbildung 14).

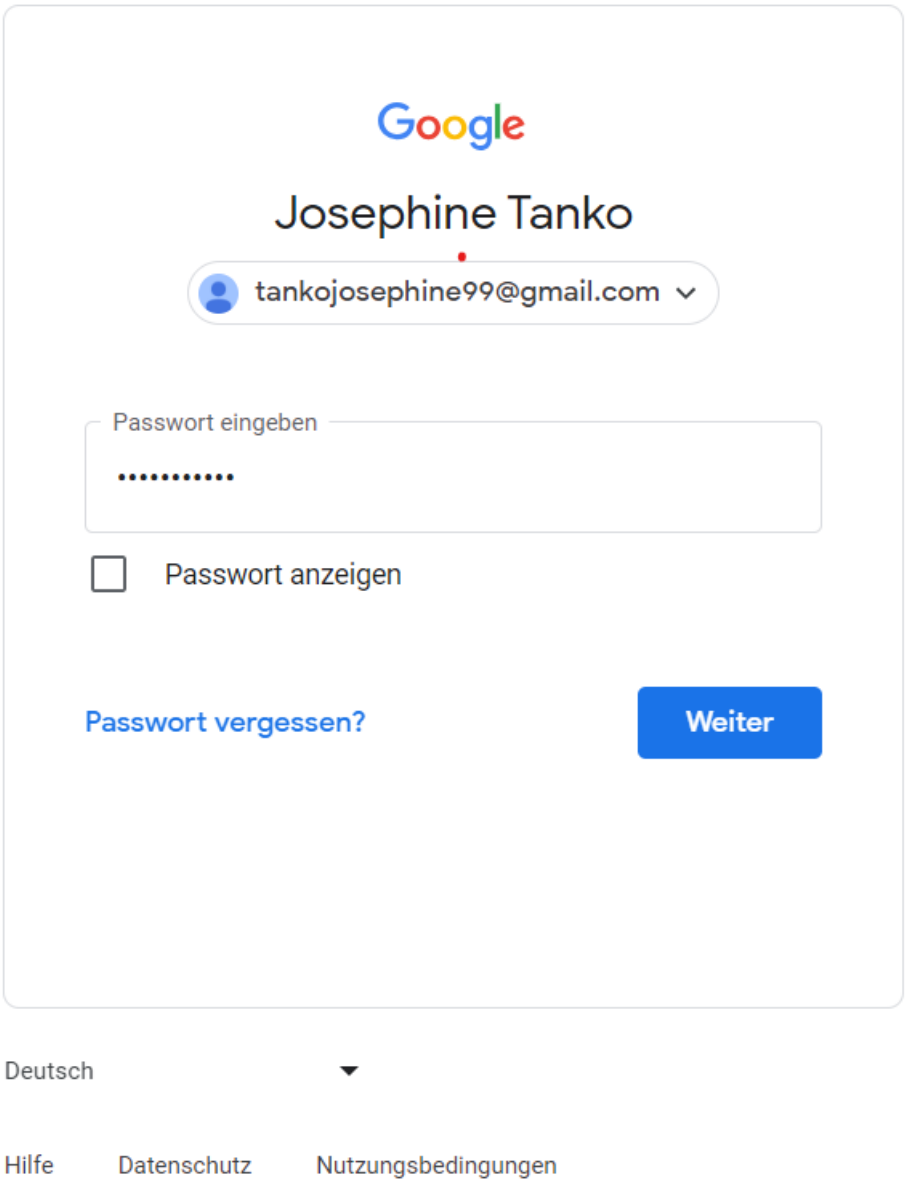


Abbildung 14: Eingabe des Passwortes des Opfers

Nachdem sie ihr Passwort eingegeben hat, verfügen wir schließlich über alles, was wir benötigen, um uns anzumelden, wie in Abbildung 15 unten auf der PowerShell-Befehlszeile zu sehen ist. Dadurch kann ich die volle Kontrolle über ihr Konto übernehmen (siehe Abbildung 16), und somit schließe ich diesen Teil der Untersuchung ab.

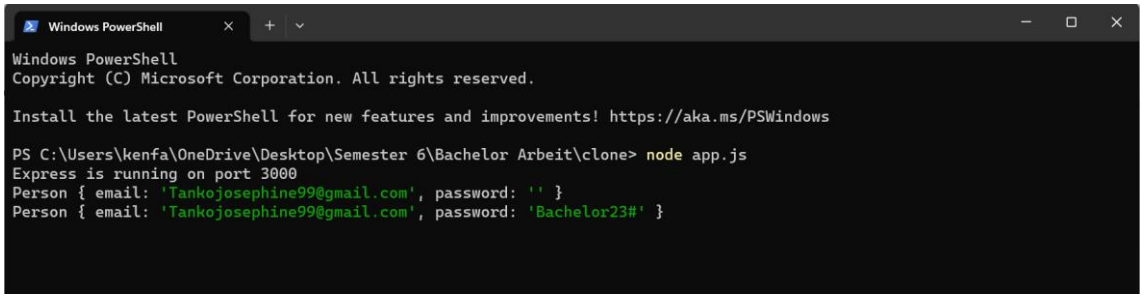


Abbildung 15: Empfang sowohl der E-Mail als auch des Passwortes.

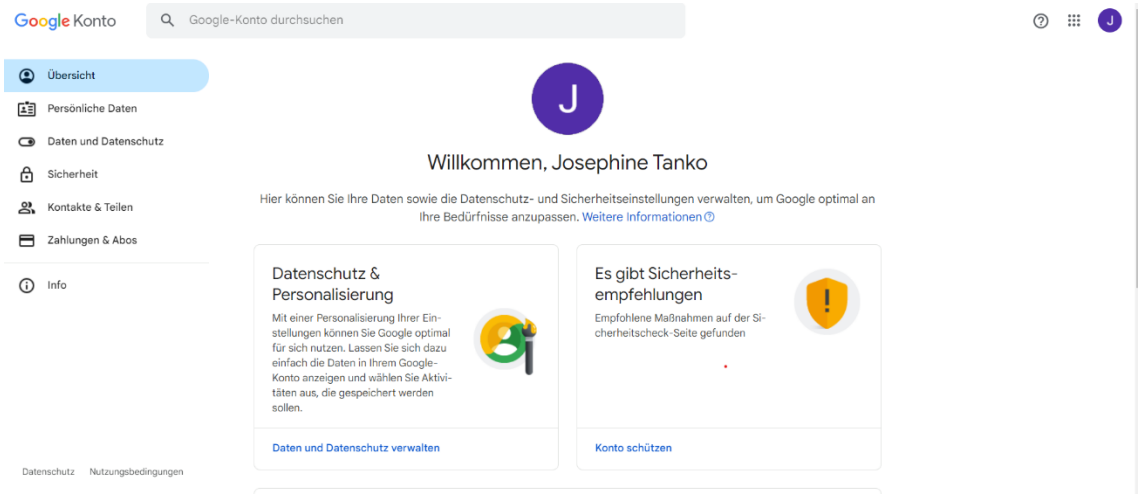


Abbildung 16: Angreifer meldet sich erfolgreich mit den erhaltenen Zugangsdaten auf der echte Google-Seite und hat vollmacht und Zugriff darauf

6.2.2 Scenario 2: Anmeldung mit E-Mail-Adresse, Passwort und 2FA in der Google App auf einem Handy

In diesem Szenario werde ich bewerten, wie einfach es ist, die Anmeldeinformationen unseres Opfers zu erhalten, wenn sie zusätzlich zur traditionellen Authentifizierungsmethode eine 2FA verwendet. In unserem Fall nutzt das Opfer ihre Google-App als ihre 2FA-Methode.

Nachdem sie ihr Passwort eingegeben hat, um zu bestätigen, dass sie die tatsächliche Person ist, fordert Google sie auf, ihre Identität zu bestätigen, indem sie zur Gmail-App geht und die Authentifizierung bestätigt. Dadurch wird die 2FA abgeschlossen, und am Ende habe ich Zugriff auf ihr Konto.

In diesem Szenario wird das Opfer denken, dass es sich auf der normalen Google-Seite befindet, was jedoch nicht der Fall ist, da es seine Informationen auf der geklonten Login-Seite eingibt.

Im Unterschied zum Szenario 1 wird es eine neue Seite für die 2FA-Authentifizierung geben und nach Abschluss wird das Opfer nicht auf sein Konto umgeleitet, da die geklonte Seite gefälscht ist. Der Angreifer hingegen wird bereits Zugang erhalten haben, da er parallel die Informationen auf der echten Google-Seite und auf der 2FA-Bestätigung eingibt, die das Opfer einfach für ihn durchführt, ohne tatsächlich zu wissen, dass sie es tut.

Die folgenden Screenshots sollen veranschaulichen, wie dies in einem Man-in-the-Middle-Angriff abläuft und wie es in einem solchen Szenario aussehen wird.

Zuerst erhält das Opfer eine E-Mail, die vorgibt, eine Sicherheitswarnung von Google zu sein, wie bereits zuvor gesehen.

Dann klickt sie auf die Schaltfläche"Passwort schützen" und landet auf der geklonten Seite. Dann gibt das Opfer die E-Mail-Adresse ein.

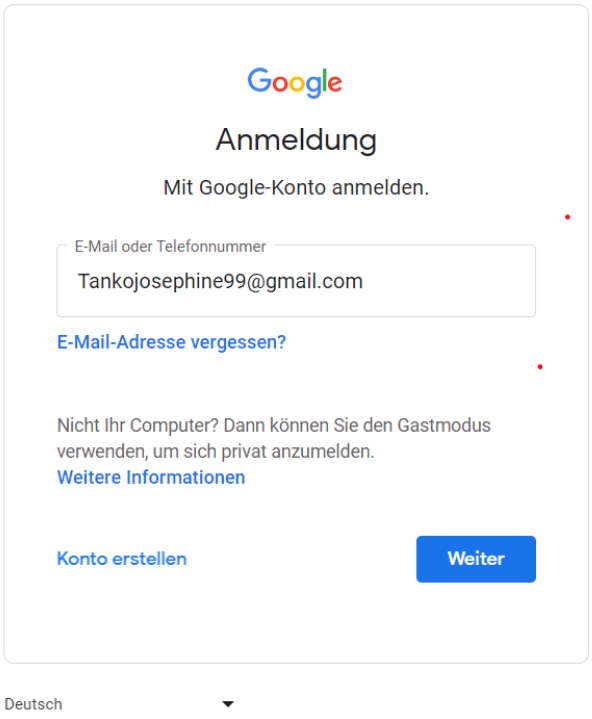


Abbildung 17: Opfer gibt ihre E-Mail ein auf der geklonten Seite ein

Nachdem sie ihre E-Mail-Adresse eingegeben hat, empfängt der Angreifen die eingegebenen Informationen, wie in Abbildung 18 unten zu sehen ist.

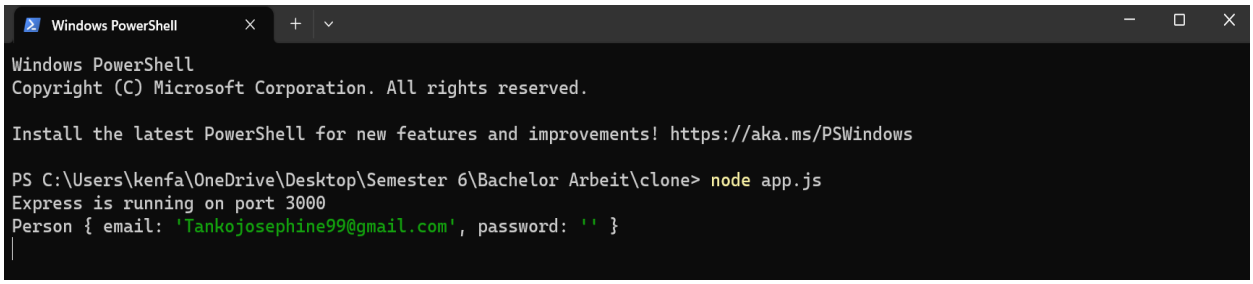


Abbildung 18: Empfang der eingegebenen E-Mail-Adresse

Dann gibt das Opfer das Passwort ein, wie in Abbildung 19 zu sehen.

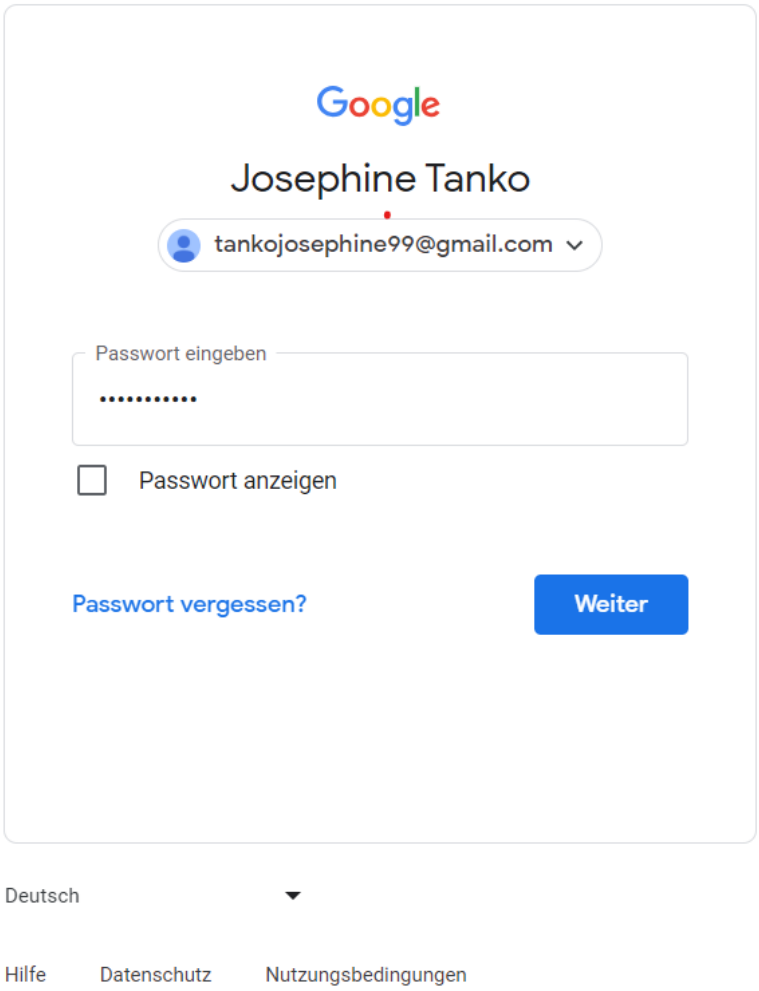


Abbildung 19: Opfer gibt ihr Passwort ein

Der Angreifer empfängt die Informationen auf der Backend-Seite, wie in Abbildung 20 unten zu sehen ist.

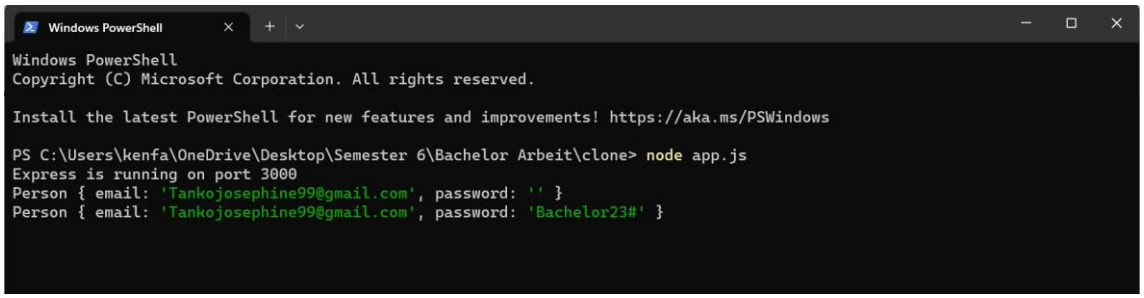


Abbildung 20: Empfang des eingegebenen Passwortes auf der Backend-Seite

Nachdem sie ihr Passwort eingegeben hat, gelangt sie auf die 2FA-Seite, auf der sie aufgefordert wird, auf ihr Telefon zu gehen, um ihre Authentifizierung zu bestätigen. Zu diesem Zeitpunkt sollte der Angreifer bereits auf der echten Google-Seite mit den erhaltenen Informationen aus den Abbildungen 18 und 20 eingeloggt sein und nur auf die Bestätigung durch das Opfer mit ihrem Telefon warten.

Die Nachricht, die das Opfer für die 2FA auf ihrem Telefon in der Google-App erhält, sieht aus wie in Abbildung 21 unten gezeigt. Das Opfer drückt dann auf "Ja, das bin ich", um die Authentifizierung zu bestätigen. Dadurch wird dem Angreifer auf der anderen Seite der Zugriff auf das echte Google-Konto gewährt, aber das Opfer bleibt auf der gefälschten Seite stehen und nichts passiert.
Indem das Opfer dies tut, hat der Angreifer die volle Kontrolle über das Konto, wie in Abbildung 22 unten zu sehen ist, und er hat die Möglichkeit, beispielsweise das Passwort des Opfers zu ändern und alles zu tun, was er möchte, da er die volle Kontrolle über das Konto des Opfers hat.

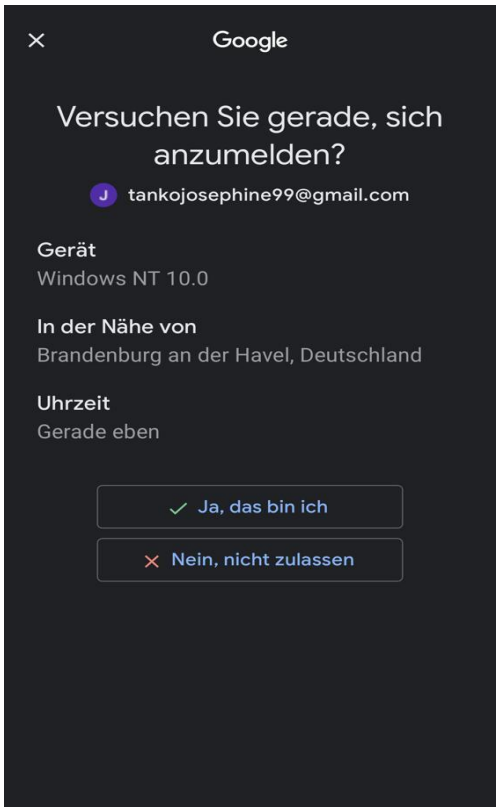


Abbildung 21: Nachricht zur 2FA-Bestätigung auf dem Mobiltelefon des Opfers

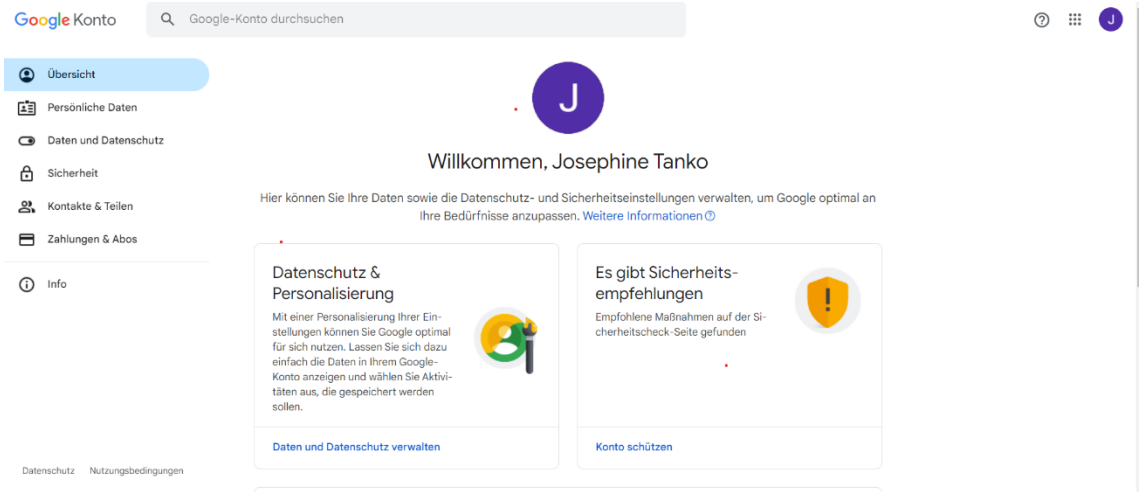


Abbildung 22: Angreifer erhält Zugriff auf das echte Google-Konto

6.2.3 Scenario 3: Anmeldung mit E-Mail Adresse und Passkey

In diesem Szenario soll beobachtet und bewertet werden, wie einfach das Passwort unseres Opfers in einem Man-in-the-Middle-Angriff gestohlen werden kann, wie bereits in den Szenarien 1 und 2 oben beschrieben.

Im Unterschied zu den Szenarien 1 und 2 wird sich das Opfer hier mit einem Passkey anmelden. Wir gehen davon aus, dass das Opfer bereits einen Passkey erstellt hat und sich für die Verwendung sogenannter Yubikey von der Firma Yubico als Authentifizierungsgerät entschieden hat.

Abbildung 23: **Yubico-Security Key NFC-Sicherheitsschlüssel für 2FA**

Auf diesem Yubikey wird bei der Erstellung eines Passkeys auf einem Webdienst unser privater Schlüssel gespeichert. Dieser private Schlüssel kann auch lokal auf modernen PCs gespeichert werden. In einem solchen Fall würde man beim Einloggen mit einem Passkey lediglich die PIN des Geräts verwenden, um die Identität zu bestätigen. Darüber hinaus können auch biometrische Daten wie ein Gesichtserkennungssystem oder ein Fingerabdrucksystem verwendet werden, sofern sie auf dem PC verfügbar sind.

Der Yubikey ermöglicht es, den gespeicherten verschlüsselten Passkey über verschiedene Geräte hinweg zu verwenden, insbesondere wenn man mobil ist. Andernfalls, wenn der private Schlüssel nur auf Ihrem PC gespeichert ist, können sie sich auf einem anderen PC nicht anmelden, da sie dort keine privaten Schlüssel haben. Es ist ratsam, für jeden Webdienst, bei dem der Passkey verwendet wird, einen Backup-Key auf einem FIDO2-Key zu erstellen, falls einer verloren geht. Beide können verloren gehen, und dies ist durchaus möglich.

Nachdem das Opfer die E-Mail erhalten hat, wird es auf die Schaltfläche "Konto schützen" klicken und zur gefälschten Login-Seite weitergeleitet. Dort gibt sie ihre E-Mail-Adresse ein, wie in Abbildung 12 zu sehen ist.

In der PowerShell wird die eingegebene E-Mail-Adresse erfasst wie es in Abbildung 18 zu sehen ist, was nicht schlimm ist, da der Angreifer sie bereits in seinem Besitz hatte und sie verwendet hat, um die Phishing-E-Mail zu senden.

Wenn das Opfer die Passwortmethode eingibt, mit der es sich normalerweise authentifiziert, nämlich mit dem Passkey, erwartet es normalerweise eine Benachrichtigung von dem Webdienst, der die Challenge sendet und verlangt, zu überprüfen, ob der FIDO2-Stick vorhanden ist, wie in Abbildung 24 zu sehen ist. In diesem Fall wird der Angreifer jedoch keinen Zugriff darauf haben. Um den Phishing-Prozess abzuschließen, benötigt er zu 100 % den Fido-2-Key des Opfers und wird daher beim Versuch, sich einzuloggen, keine Zugriffsberechtigung erhalten.

Wie bereits zuvor erläutert, sind für eine Authentifizierung mit Passkey sowohl öffentliche als auch private Schlüssel erforderlich. Einer kann nicht ohne den anderen arbeiten und da es keine Passwörter gibt, die in diesem Fall abgefischt werden können, ist die passwortlose Authentifizierungsmethode äußerst sicher vor diesem Angriff.

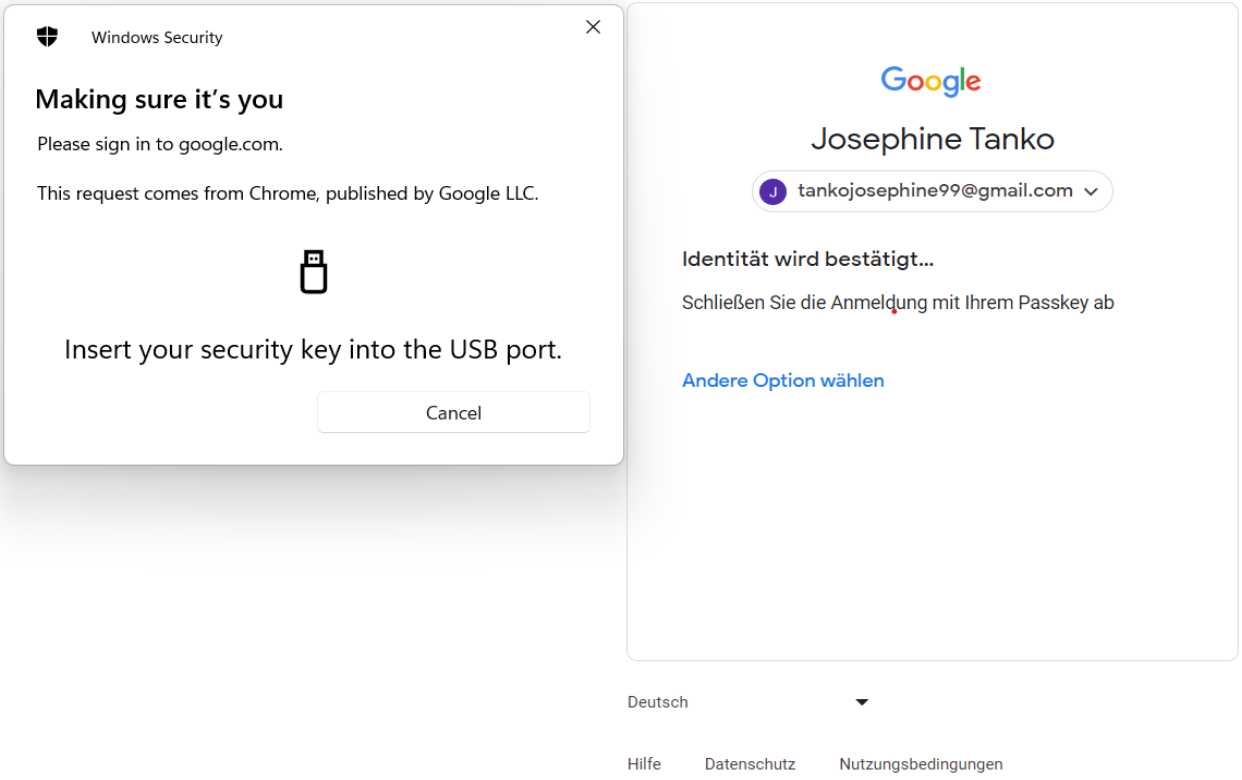


Abbildung 24: In diesem Szenario erwartet das Opfer normalerweise eine Benachrichtigung von dem Webdienst, der die Herausforderung sendet und verlangt, zu überprüfen, ob der FIDO 2-Stick vorhanden ist Passkey-

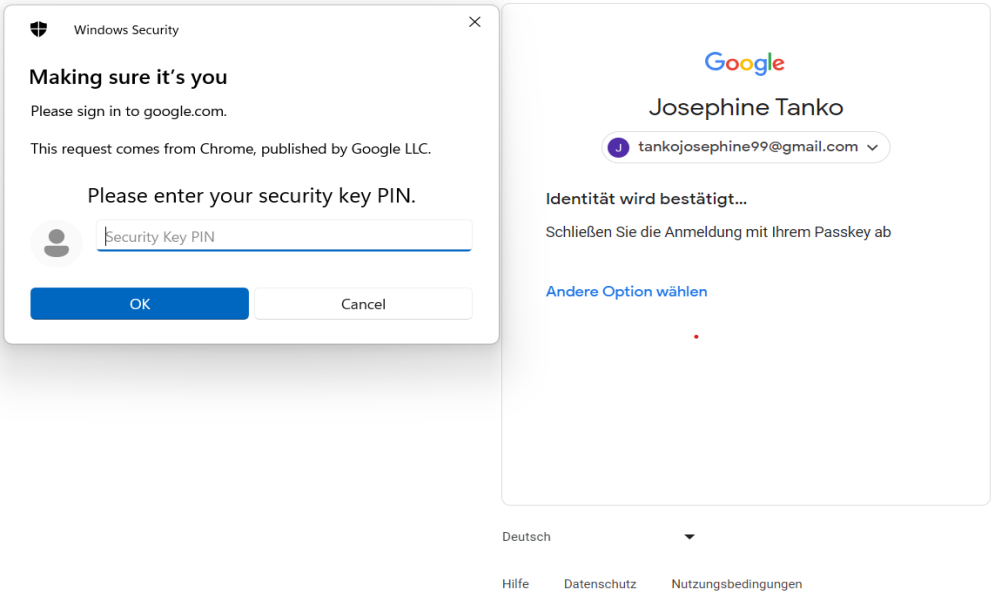


Abbildung 25: Nach der Bestätigung des Besitzes des FIDO2-Sticks wird der Benutzer aufgefordert, den PIN des Sticks einzugeben

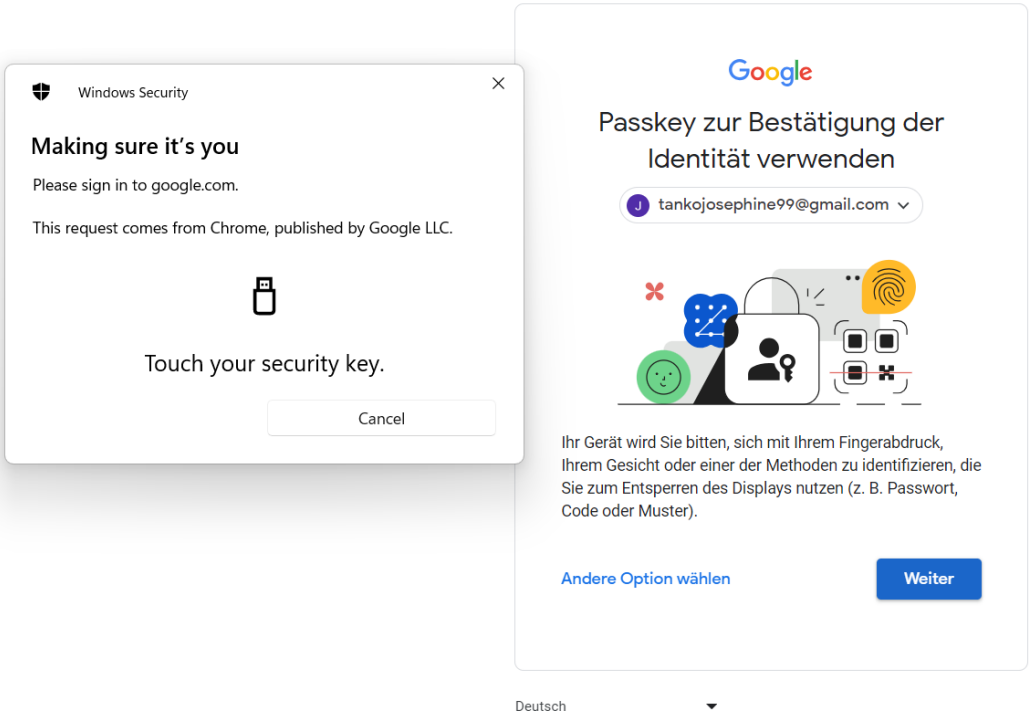


Abbildung 26: Nach der Eingabe des PINs wird der Benutzer aufgefordert, den FIDO2-Stick zu berühren, wenn dieser blinkt, um die Authentifizierung abzuschließen

Abbildung 27: Ein Yubikey, der in den USB-Anschluss eines Computers eingesteckt ist und bereit ist für die Bestätigung

Abbildung 28: Der Benutzer bestätigt die Authentifizierung, indem er den blinkenden Yubikey gemäß der Anzeige in Abbildung 26 berührt

7 Bewertung der Demonstration

Die vorgeführten Demonstrationen werfen ein Licht auf die Effektivität verschiedener Authentifizierungsmethoden und liefern wichtige Erkenntnisse. Wie die Demonstrationen verdeutlichen, bieten sowohl die Verwendung eines komplexen Passworts als auch die Implementierung einer 2FA einen gewissen Schutz vor Phishing-Angriffen. Es ist jedoch von entscheidender Bedeutung, sicherzustellen, dass die Website, auf der die Benutzer ihre Zugangsdaten und 2FA-Codes eingeben, tatsächlich die richtige ist.

Eine Anmeldung mit einem starken Passwort und 2FA trägt zweifellos zur Sicherheit von Konten bei. Dennoch darf man sich nicht in trügerischer Sicherheit wiegen, selbst wenn der zweite Faktor eingerichtet ist.

Im Gegensatz dazu bietet die Authentifizierung mit einem Passkey einen anderen Ansatz. Hier sind sowohl der private als auch der öffentliche Schlüssel erforderlich, um das sogenannte Challenge-Response-Verfahren zu authentifizieren. Bei FIDO 2 wird automatisch die Domain des Dienstes in die Authentifizierung einbezogen, was das Verfahren widerstandsfähiger gegenüber klassischem Phishing macht.

Die Abwesenheit eines Passworts bedeutet, dass auch kein Passwort gestohlen werden kann. Die Gefahr, aus Versehen Anmeldedaten auf einer Phishing-Website einzugeben, wird durch die Verwendung von Passkeys nahezu eliminiert. Die bisher als sicher geltenden 2FA-Methoden haben gezeigt, dass sie von Angreifern umgangen werden können, wie in dieser Arbeit dargestellt wurde.

Daher sollte FIDO 2, wo immer möglich, entweder als 2FA-Methode oder, noch besser, als passwortlose Variante eingerichtet werden, wie bereits in dieser Arbeit am Beispiel des Passkeys gezeigt wurde. Dies ermöglicht ein Höchstmaß an Sicherheit und minimiert das Risiko von Phishing-Angriffen erheblich.

8 Kritik von Passkey

Die Einführung von Passkey und FIDO2 als sichere Authentifizierungsmethoden hat zweifellos die Sicherheit von Benutzerkonten erheblich verbessert. Dennoch sollten wir beachten, dass keine Authentifizierungsmethode eine hundertprozentige Sicherheit bieten kann. Selbst bei der Verwendung von FIDO2 sind Benutzerkonten nicht vor bestimmten Bedrohungen, wie dem Diebstahl von Cookies, geschützt.

Cookies sind kleine Datensätze, die im Webbrowser gespeichert werden, wenn sich ein Benutzer bei einem Dienst anmeldet. Diese Cookies dienen dazu, die Benutzer zu identifizieren und die Interaktion mit der Webanwendung zu erleichtern. Einmal gestohlene Cookies können von Angreifern missbraucht werden, um die aktive Online-Sitzung eines Benutzers zu übernehmen, ohne Zugriff auf Benutzername und Passwort zu haben.

Ein typischer Angriff könnte darin bestehen, dass ein Angreifer eine gefährliche E-Mail sendet, die einen schädlichen Anhang enthält, der die Cookies aus dem Profil des Opfers extrahiert. Wenn der Angreifer diese gestohlenen Cookies erfolgreich in seinen eigenen Browser importiert, kann er auf alle Konten des Opfers zugreifen, bei denen der Benutzer nicht aktiv ausgeloggt ist. Für diesen Angriff sind weder Zugangsdaten noch ein zweiter Faktor erforderlich.[28]

Es gibt jedoch Möglichkeiten, sich gegen solche Angriffe zu schützen. Eine bewährte Methode besteht darin, sich nicht dauerhaft bei wichtigen Webdiensten anzumelden und sich nach jeder Nutzung auszuloggen. Dies schließt die aktuelle Sitzung und löscht alle damit verbundenen Cookies.

[28] Kathrin Stoll, (2023). Angriffe auf den zweiten Faktor-So schützen Sie sich.

9 Maßnahmen gegen Phishing

Darüber hinaus ist es von größter Bedeutung, aufmerksam auf E-Mails zu achten, insbesondere wenn der Absender unbekannt ist. Phishing-E-Mails werden immer raffinierter, sind jedoch oft anhand ungewöhnlicher Absenderadressen, schlechter Rechtschreibung oder kopierter Unternehmensdesigns großer Firmen zu erkennen.

Es sollte außerdem vermieden werden, auf Links in E-Mails von unbekannten Absendern zu klicken. Es ist ratsam, Browser-Erweiterungen wie Mitaka zu verwenden, um die Authentizität von Webseiten und E-Mail-Adressen schnell zu überprüfen.[29]

Anhänge sollten nur dann geöffnet werden, wenn der Absender bekannt ist und die Quelle vertrauenswürdig ist. Mit diesen Sicherheitsmaßnahmen kann zusätzlich ein Schutz und das Risiko von Phishing-Angriffen minimiert werden.

Die Verwendung separater E-Mail-Adressen für verschiedene Zwecke wird empfohlen, um das Risiko einer Kompromittierung der Haupt-E-Mail-Adresse zu minimieren. Zum Beispiel kann eine E-Mail-Adresse für persönliche Zwecke und eine andere für Online-Shopping verwendet werden.

Die Verwendung von VPNs (Virtual Private Networks) zur Sicherung von Netzwerkverbindungen, insbesondere bei der Nutzung öffentlicher Wi-Fi-Netzwerke, wird empfohlen. Dadurch wird das Abhören von Daten durch Dritte erschwert.
Die regelmäßige Überwachung von Konten und die Überprüfung von Kontoaktivitäten wird empfohlen. Im Falle verdächtiger Aktivitäten sollten diese sofort gemeldet werden.

Die Aufrechterhaltung der Kenntnisse über die neuesten Phishing-Techniken und Betrugsmethoden sowie die Sensibilisierung für diese Risiken sind der Schlüssel zur Prävention von Phishing-Angriffen.

[29] Kathrin Stoll, (2023). Angriffe auf den zweiten Faktor-So schützen Sie sich.

10 Diskussion und Fazit

Diese Arbeit hat sich mit der Analyse und Bewertung der Sicherheit und Benutzerfreundlichkeit von Passkey im Vergleich zu herkömmlichen Authentifizierungsmethoden auseinandergesetzt. Die Untersuchung ergab wichtige Erkenntnisse darüber, wie moderne Authentifizierungsverfahren die Sicherheit von Online-Konten erhöhen können und welche Vorteile sie gegenüber traditionellen Passwörtern bieten.

Im direkten Vergleich zur herkömmlichen Passworteingabe zeigt sich, dass Passkey erheblich sicherer ist. Dies liegt hauptsächlich an der Art der Authentifizierung. Während herkömmliche Passwörter anfällig für Phishing-Angriffe sind, bei denen Angreifer versuchen, Benutzer zur Eingabe ihrer Anmeldeinformationen auf gefälschten Websites zu verleiten, ist Passkey immun gegen diese Art von Angriffen. Passkey erfordert sowohl den Besitz der physischen Sicherheitsvorrichtung (z. B. eines FIDO2-Sticks) als auch die Bestätigung des Benutzers. Dieses Zwei-Faktor-Verfahren macht es äußerst schwierig für Angreifer, Zugriff auf ein Konto zu erlangen.

Die Überlegenheit von Passkey gegenüber herkömmlichen Methoden zeigt sich in seiner Benutzerfreundlichkeit. Passkey bietet nicht nur ein höheres Maß an Sicherheit, sondern ist auch benutzerfreundlicher. Das Fehlen der Notwendigkeit zur Erstellung und Verwaltung von Passwörtern erleichtert die Anmeldung erheblich. Benutzer müssen sich keine komplexen Passwörter merken oder sich Gedanken über deren Sicherheit machen. Dies trägt dazu bei, den Anmeldevorgang schneller und stressfreier zu gestalten. Passkey bietet auch den Vorteil der Interoperabilität und kann auf verschiedenen Plattformen und Geräten eingesetzt werden, was die Benutzerfreundlichkeit weiter erhöht.

10.1 Die Beantwortung der Zielsetzungsfragen

1 Wie sicher ist Passkey im Vergleich zu bekannten Verfahren wie der Passworteingabe online?

Passkey ist erheblich sicherer als herkömmliche Passworteingabe. Die physische

Präsenz der Sicherheitsvorrichtung und das Zwei-Faktor-Verfahren machen es äußerst resistent gegen Phishing-Angriffe und andere gängige Angriffsmethoden.

2 Was macht Passkey sicherer als die anderen Verfahren?

Die Sicherheit von Passkey liegt in der Kombination aus physischem Besitz (der Sicherheitsvorrichtung) und Benutzerbestätigung. Diese doppelte Sicherheitsschicht erhöht den Schutz erheblich. Passkey ist auch an die URL gebunden, was eine zusätzliche Sicherheitsebene bietet. Dies bedeutet, dass die Authentifizierung nicht nur auf dem Besitz eines Schlüssels oder biometrischer Daten beruht, sondern auch auf der Überprüfung der spezifischen Website oder URL, auf der die Anmeldung erfolgt. Diese enge Bindung an die URL schützt effektiv vor Angriffen, bei denen Benutzer auf gefälschten Websites dazu verleitet werden könnten, ihre Anmeldeinformationen preiszugeben. Mit Passkey wird die Authentizität der Website und die Identität des Benutzers gleichermaßen verifiziert, was die Sicherheit erheblich erhöht.

3 Ist Passkey benutzerfreundlicher im Vergleich zum Einloggen mit einem Passwort?

Ja, Passkey ist benutzerfreundlicher, da es keine komplexen Passwörter erfordert und den Anmeldevorgang beschleunigt. Benutzerfreundlichkeit ist ein wichtiger Aspekt, der dazu beiträgt, die Akzeptanz von Authentifizierungsmethoden zu erhöhen.
Die Benutzerfreundlichkeit von Passkey ergibt sich aus dem Fehlen der Notwendigkeit zur Passwortverwaltung, der Interoperabilität auf verschiedenen Plattformen und der schnellen Anmeldeprozedur.

Abschließend lässt sich sagen, dass Passkey eine vielversprechende Lösung zur Verbesserung der Online-Sicherheit und Benutzerfreundlichkeit darstellt. Es bietet einen robusten Schutz vor den gängigsten Angriffsmethoden und erleichtert gleichzeitig den Anmeldevorgang für Benutzer. Die steigende Unterstützung von Passkey durch Webdienste und Plattformen unterstreicht seine Relevanz für die Zukunft der Online-Sicherheit. Es ist anzunehmen, dass die Verbreitung von Passkey in den kommenden Jahren weiter zunehmen wird, da die Notwendigkeit einer sicheren Authentifizierung in der digitalen Welt unbestreitbar ist.

11 Literaturverzeichnis

Adams, A. S. (1999). *"Users are not the enemy." Communications of the ACM.* 40-46.

Aderson, F. (06. Juni 2023). *FIDO-Authentifizierung: Die Geschichte der Fido Alliance, das Versprechen von FIDO2 und Passkeys.* Von Prove: https://www.prove.com/blog/fido-authentication-the-history-of-the-fido-alliance-the-promise-of-fido2-and-passkeys abgerufen

Alliance, F. (kein Datum). *History of FIDO Alliance.* Von Fidoalliance.org: https://fidoalliance.org/overview/history/ abgerufen

Alliance, F. (kein Datum). *How FIDO works.* Von fidoalliance.org: https://fidoalliance.org/how-fido-works/ abgerufen

Alliance, F. (kein Datum). *Passkey.* Von fidoalliance.org: https://fidoalliance.org/passkeys/ abgerufen

Bundesamt für Sicherheit in der Informationstechnik(BSI). (kein Datum). *Bundesamt für Sicherheit in der Informationstechnik*. Von Sichere Passwörter erstellen: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html abgerufen

Bundesamt für Sicherheit in der Informationstechnik (BSI), B. f. (kein Datum). *Zwei-Faktor-Authentisierung*. Von Bundesamt für Sicherheit in der Informationstechnik (BSI): https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html#:~:text=Ein%20Benutzer%20AUTHENTISIERT%20sich%2 abgerufen

Bundesamt für Sicherheit in der Informationstechnik (BSI). (kein Datum). *Bundesamt für Sicherheit in der Informationstechnik (BSI).* Von Methoden der Cyber-Kriminalität.: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-

Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/methoden-der-cyber-kriminalitaet_node.html abgerufen

Clauß, S. (2002). *Token-based authentication. In Encyclopedia of cryptography and security.* 659-660: Springer.

Eikenberg, R. (2023). Passkeys im Einsatz. *C'T Magazin für Computer Technik*, S. 14.

Identity, G. (12. 09 2023). *Passkey-Unterstützung für Android und Chrome*. Von Passkey-Unterstützung für Android und Chrome: https://developers.google.com/identity/passkeys/supported-environments?hl=de#:~:text=Passkey%20support%20for%20Android%20apps,-Android%20apps%20support&text=Passkeys%20are%20supported%20on%20devices,API%20level%2028)%20or%20higher. abgerufen

Jain, A. K. (2011). *Introduction to biometrics. In Advances in biometrics.* 1-22: Springer.

Microsoft. (06. 05 2023). *Microsoft.* Von Securing the Microsoft Online Services infrastructure. abgerufen

MiniOrange. (29. 12 2022). *MiniOrange.* Von What is Authentication? Different types of Authentications: https://blog.miniorange.com/different-types-of-authentication-methods-for-security/ abgerufen

Nina Bindel, C. C. (Mai 2023). FIDO2, CTAP 2.1, and WebAuthn 2: Provable Security and Post-Quantum Instantiation. *2023 IEEE Symposium on Security and Privacy (SP),* (S. 1471-1490). San Francisco, CA, USA, 2023,: 10.1109/SP46215.2023.10179454. Von FIDO2, CTAP 2.1, and WebAuthn 2: Provable Security and Post-Quantum Instantiation. abgerufen

Paul A. Grassi, J. L. (Juni 2017). *NIST Special Publication 800-63B.* Von Digital Identity Guidelines Authentication and Lifecycle Management: https://doi.org/10.6028/NIST.SP.800-63b abgerufen

Stoll, K. (2023). Angriffe auf den zweiten Faktor- So schützen Sie sich. *C'T Magazin für Computer Technik*, S. 26,27,28 & 29.

Vacca, J. R. (2002). *Public Key Infrastructure: Building Trusted Applications and Web Services.* Auerbach Publications.

W3C und Mountain View, C. (04. März 2019). *W3.org.* Von https://www.w3.org/2019/03/pressrelease-webauthn-rec.html abgerufen

Abbildungsverzeichnis

Abkürzungsverzeichnis

FIDO2: Fast Identity Online 2
2FA: Zwei-Faktor-Authentifizierung (in Englisch "Two-Factor Authentication")
UAF: Universal Authentication Framework
API: Application Programming Interface
U2F: Universal 2nd Factor
CTAP: Client to Authenticator Protocol
URL: Uniform Resource Locators

Ehrenwörtliche Erklärung

Hiermit versichere ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen oder Hilfsmittel benutzt habe und dass die Arbeit in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt wurde.

Ort, Datum
Brandenburg an der Havel, 24/10/2023

Unterschrift