identeco

Whitepaper
Passwortsicherheit 2024
Die Passwörter der Deutschen

identeco

Editor: Dr. Matthias Wübbeling

Autoren: René Neff, Dr. Matthias Wübbeling, Dr. Frank Zickenheiner

Identeco GmbH & Co. KG

Joachimstr. 8, 53113 Bonn

+49 (0) 228 28628581

Präambel

Die Identeco GmbH & Co. KG analysiert seit vielen Jahren Datenleaks mit Logindaten von Privatpersonen und Unternehmen. Dabei stehen der Datenschutz im Sinne der DSGVO und die Verantwortung für die Accountsicherheit von Plattformanbietern und Unternehmen im Vordergrund. Die angebotenen Dienstleistungen und Produkte ermöglichen es unseren Kunden, die Anforderungen gängiger Standards wie BSI IT-Grundschutz, ISO 27000 und NIST Cyber Security Framework zum Schutz von Mitarbeiter- und Kundenaccounts zuverlässig zu adressieren.

Mit fast 50 Milliarden gesammelten Datensätzen besitzt Identeco eine umfangreiche Basis aktueller und historischer Logindaten zur Absicherung von Benutzeraccounts. Diese Daten wurden in Zusammenarbeit mit den Cyber Security Experten der Universität Bonn ausgewertet, um ein einheitliches Bild zur Lage der Passwortkultur in Deutschland zu erhalten. Der Auswertung dieses Whitepapers liegen dabei die im Jahr 2024 gesammelten Logindaten zugrunde. Die Schlussfolgerungen zu den tatsächlich verwendeten Passwörter in den betrachteten Branchen basieren ausschließlich auf den gefundenen, also in Datenleaks enthaltenen Daten. Es gibt keine hinreichenden Hinweise auf existierende Datenleaks bei den in diesem Whitepaper namentlich genannten Einrichtungen. Das Whitepaper zeigt hingegen die Bedeutung von Leakdaten für die Accountsicherheit sämtlicher Institutionen auf.

Inhalt

1. Einleitung

Die rapide Zunahme von Cyberangriffen auf eine Vielzahl von Akteuren, darunter Privatpersonen, Unternehmen oder öffentliche Institutionen wie Krankenhäuser, IT-Dienstleister der öffentlichen Hand sowie Verwaltungen, erfordert eine detaillierte Analyse der Bedrohungslandschaft. Besonders beunruhigend ist die Tatsache, dass zahlreiche dieser Angriffe auf gültigen Zugangsdaten (Logindaten) basieren. Solche Zugangsdaten werden auf unterschiedliche Arten geleakt, z.B. durch eine erfolgreiche Phishing-Attacke oder einen initiierten Data-Breach. Anschließend werden diese in kriminellen Strukturen als Tausch- und Handelsgut verwendet.

Dieses Whitepaper setzt sich mit den Aspekten geleakter Logindaten, den Herausforderungen schwacher und starker Passwörter sowie den Risiken von Account-Übernahmen auseinander. Im Rahmen der hier vorgestellten Untersuchung wurden daher insbesondere die Herausforderungen analyisiert, die mit gestohlenen oder geleakten Daten, insbesondere Logindaten, verbunden sind.

1.1 Accounts und Accountübernahmen

Unter einem “Account” verstehen wir im Folgenden ein Benutzerkonto, das einer Person oder einer Organisation auf einer digitalen Plattform oder in einem Online-Dienst zugewiesen wird. Dieses Konto ermöglicht es dem Benutzer, auf bestimmte Funktionen oder Inhalte der Plattform zuzugreifen, mit anderen Benutzern zu interagieren und oft auch eigene Daten zu speichern oder zu verwalten. Zu den besagten Diensten können E-Mail-Anbieter, Online-Shops, Social Media, aber auch Ausschreibungsplattformen oder das Active Directory eines Unternehmens gehören.

Unter einer “Account-Übernahme” verstehen wir gleichfalls im Folgenden die unrechtmäßige Aneignung der Funktionalitäten eines Benutzeraccounts. Meistens erfolgen Account-Übernahmen durch die Verwendung von gültigen Logindaten (vor allem durch die Kombination von E-Mail-Adresse und Passwort), die durch Datenleaks öffentlich zugänglich werden, weswegen dieses Paper besonderen Fokus auf geleakte Passwörter setzt.

1.2 Bedrohungslage und Herausforderungen durch geleakte Login Daten

Die Bedrohungslage durch geleakte Logindaten betrifft unterschiedliche Interessengruppen, darunter Verbraucher, Mitarbeiter von Unternehmen und Benutzer verschiedener Online-Plattformen. Eine besondere Herausforderung bei der Verarbeitung geleakter Passwörter liegt dabei im Bereich Datenschutz und DSGVO. Die Verarbeitung personenbezogener Daten, inklusive E-Mail-Adressen und zugehöriger Passwörter, steht oft im Widerspruch zu geltenden Datenschutzrichtlinien. Auch die Verarbeitung personenbezogener Daten in wohlwollender Absicht, wie etwa durch unternehmensinterne Sicherheitszentren (SOCs), können zu rechtlichen Konflikten führen, vor allem wenn Daten externer Personen ohne angemessene Zustimmung gesammelt und umfangreich analysiert werden. In dieser Hinsicht ist es unerlässlich, einen ausgewogenen Ansatz zu verfolgen und bereits in der Konzeptionsphase die Sicherheitsbemühungen rechtlich konform zu gestalten.

In diesem Whitepaper wird die gegenwärtige Situation in Bezug auf geleakte Logindaten beleuchtet. Ferner werden praxisorientierte Empfehlungen für den Umgang mit geleakten Logindaten und die Stärkung der Passwortsicherheit vorgestellt. In Abschnitt 2 werden die Datenbasis und die Methodik vorgestellt, die bei der Analyse der Passwörter Verwendung fanden. Danach werden gängige Industriestandards zur Passwortsicherheit zusammengefasst. Der vierte Abschnitt fokussiert endlich auf die Passwortkultur in den drei Bereichen privat genutzte Passwörter, Passwörter im wirtschaftlichen Kontext und Passwörter im Kontext des öffentlichen Dienstes. Anschließend werden in Abschnitt 5 allgemeine Maßnahmen zur Erhöhung der Accountsicherheit vorgestellt. Der Abschnitt 6 bildet eine zusammenfassende Diskussion.

2. Methodik und Datenbasis

Die Identeco GmbH und Co. KG sucht unablässig in diversen Quellen des Clear-, Deep- und Darknets nach geleakten Logindaten, arbeitet diese Daten datenschutzkonform auf und pflegt sie in die eigene Leak-Datenbank ein. Durch diese Methode sind mittlerweile fast 50 Milliarden Zugangsdaten in dieser enthalten. Die Grundlage der Analyse bildet eine umfassende Auswertung von etwa 57.000 Leakdateien, die im Verlauf des Jahres 2024 aus unterschiedlichen Quellen des Clear-, Deep- und Darknets gesammelt und analysiert wurden. Innerhalb dieses Datensatzes wurden in mehr als 30.000 Leakdateien relevante Identitätsdaten identifiziert. Insgesamt ergibt sich eine Datenmenge von 4,7 Milliarden Identitätsdaten, wovon schlussendlich 4,4 Milliarden Zugangsdaten als Basis für die vorliegende Analyse herangezogen wurden.

Für die vorliegende Analyse wurden ausschließlich Passwörter von Accounts erfasst, bei denen (mindestens) eine dazugehörige E-Mail-Adresse vorhanden ist. Diese Fokussierung ermöglicht eine gezielte Analyse von Zugangsdaten, die im deutschsprachigen Raum Verwendung finden, um so praxisrelevante Erkenntnisse im Bereich der Accountsicherheit zu gewinnen. Durch diese umfassende Datenbasis sind wir in der Lage, präzise Einblicke in die häufigsten Passwortmuster im deutschsprachigen Raum für das Jahr 2024 zu liefern.

Im Rahmen der eigentlichen Analyse wurden sorgfältige Schritte unternommen, um die Integrität der Daten und die Anonymität der Benutzer zu gewährleisten. Bei jeder Leakdatei wurden im ersten Schritt die Accountdaten von allen anderen Daten getrennt. Nicht als Accountdaten identifizierte Informationen wurden gelöscht und nicht weiterverarbeitet.

Die extrahierten Accountdaten wurden anschließend einem von Identeco entwickelten Anonymisierungsprozess unterzogen. Dabei werden die zu den jeweiligen Passwörtern gehörenden E-Mail-Adressen gelöscht, um zu gewährleisten, dass keine Passwörter mehr zu einer spezifischen E-Mail-Adresse zuordenbar sind. Das Ergebnis dieses Prozesses ist eine Liste, die nur noch aus Passwörtern und der zugehörigen Top-Level-Domains besteht. Durch die Analyse der Top-Level-Domains lassen sich die Namen von Unternehmen oder Institutionen erkennen, die entweder direkt oder in Form eines Teils eines Passworts vorkommen.

In einem weiteren Schritt wurden Passwörter, die auf eine spezifische Person oder Institution hinweisen, durch neutrale Platzhalter ersetzt. Beispielsweise wurden Passwörter der Form “identeco123rulez” durch den Platzhalter [Name der Organisation] ersetzt. Diese Anonymisierung dient vor allem dem Schutz sensibler Informationen und der Wahrung von Sicherheitsinteressen und, um sicherzustellen, dass keine Rückschlüsse auf einzelne Personen, Unternehmen oder Institutionen gezogen werden können.

Die folgende Analyse will vor allem auf drei Bereiche fokussieren: den privaten Gebrauch von Passwörtern sowie den Gebrauch von Passwörtern im wirtschaftlichen Kontext und im öffentlichen Bereich. Um den privaten Kontext abzubilden, wurde auf die Domains von häufig im privaten Kontext verwendeten E-Mail-Providern fokussiert. Öffentliche Einrichtungen werden beispielhaft repräsentiert durch Bundesministerien, nachgelagerte Bundesbehörden und durch Domains, die zu den zehn größten deutschen Städten gehören. Als repräsentative Auswahl für deutsche Unternehmen wurden die 40 im DAX gelisteten Unternehmen ausgewählt. Diese gezielte Auswahl ermöglicht eine präzise Analyse und die Identifikation spezifischer Muster und Trends bei geleakten Passwörtern für das Jahr 2024.

3. Industriestandards zur Accountsicherheit

Die Sicherheit von Passwörtern und Benutzerkonten bildet das Rückgrat jedes effektiven Schutzsystems gegen Account-Takeover-Angriffe. Internationale Standards wie ISO/IEC 27001 respektive 27002 definieren Anforderungen, um die Integrität und Vertraulichkeit von Zugangsdaten zu Accounts zu gewährleisten und gleichzeitig den Datenschutz der Benutzer und Unternehmensdaten zu wahren.

Ein wesentlicher Aspekt ist die Betonung von starken Passwörtern in Bezug auf Länge und Komplexität. Ebenso wichtig sind einzigartige Passwörter für Systeme und Dienste.

Ein wesentlicher Paradigmenwechsel der letzten Jahre betrifft die periodische Änderung von Passwörtern. Basierend auf aktuellen wissenschaftlichen Erkenntnissen fordert die ISO/IEC 27002 nicht mehr explizit den regelmäßigen Wechsel von Passwörtern. Stattdessen setzen aktuelle Sicherheitsrichtlinien auf die Implementierung starker und komplexer Passwörter. Es hat sich gezeigt, dass ein erzwungener häufiger Wechsel des Passwortes dazu führt, dass Benutzer unsichere Passwörter wählen und Passwörter unsicher notiert werden. Mit dieser Änderung soll daher die Sicherheit erhöht werden.

Die Anforderung, bereits in der Vergangenheit verwendete Passwörter abzulehnen und einen notwendigen Passwortwechsel, z.B. nach einem Sicherheitsvorfall, zu erzwingen, bleibt bestehen.

Eine neue Anforderung an ein Passwortmanagementsystem ist das Erkennen und Sperren von häufig verwendeten Passwörtern sowie von kompromittierten Logindaten. Ein wesentlicher Aspekt, um der massiven Zunahme von Datenlecks und Phishing-Kampagnen der letzten Jahre zu begegnen.

Die Integration von Multi-Faktor-Authentifizierung (MFA) wird gemäß NIST SP 800-63 als effektive Maßnahme hervorgehoben, um zusätzlichen Schutz vor unberechtigtem Zugriff zu bieten. MFA hat sich als wirksames Mittel zur Erhöhung der Sicherheit von Benutzerkonten erwiesen. Meist wird eine Kombination aus Passwort und Hardware- oder Software-Token verwendet.

Sichere Speicherungs- und Transporttechniken, wie sie in ISO/IEC 27001 und 27002 beschrieben werden, spielen auf technischer Ebene eine entscheidende Rolle. Hierbei kommen Verfahren wie Hashing, Salting und TLS zum Einsatz, um Passwort-Hashes zu schützen und die Widerstandsfähigkeit gegenüber Brute-Force- und Man-in-the-Middle-Angriffen zu erhöhen.

Im Umgang mit geleakten Logindaten bietet die Datenschutz-Grundverordnung (DSGVO) keine expliziten Vorgaben. Dennoch fordert sie von Unternehmen, angemessene Sicherheitsmaßnahmen zu treffen, um personenbezogene Daten von Mitarbeitern und Kunden zu schützen. Interne Richtlinien sollen entwickelt werden, um angemessen auf Sicherheitsvorfälle zu reagieren, die die Sicherheit personenbezogener Daten beeinträchtigen.

Präventive Maßnahmen, wie die Verhinderung der Mehrfachverwendung von Passwörtern gemäß dem OWASP ASVS, sind ebenso von großer Bedeutung für E-Commerce-Plattformen. Es sollen Mechanismen implementiert werden, um Benutzer daran zu hindern, bereits kompromittierte Passwörter (weiter) zu verwenden.

Die Auditierung und Überwachung von Benutzerkonten gemäß der ISO/IEC 27000-Reihe ist unerlässlich, um verdächtige Aktivitäten zu identifizieren und kriminellen Missbrauch der eigenen IT-Infrastruktur zu verhindern. Echtzeit-Überwachung von Anmeldeaktivitäten trägt dazu bei, Account-Takeover-Angriffe frühzeitig zu erkennen und zu bekämpfen.

Insgesamt bieten internationale Standards eine umfassende Grundlage für die Entwicklung von Sicherheitsrichtlinien, die auch den geltenden Datenschutzanforderungen gerecht werden. Ein

ganzheitlicher Ansatz, der diese Anforderungen berücksichtigt, ermöglicht es Unternehmen, ihre Infrastruktur robust und den Umgang mit Unternehmens- sowie Kundendaten sicher zu gestalten.

4. Unterschiede in der Passwortkultur

Die vorliegende Studie legt besonderen Fokus auf die Verwendungsweisen von Passwörtern in drei unterschiedlichen Bereichen: 1. Passwortgebrauch im Privaten Kontext, 2. Passwortgebrauch im wirtschaftlichen Kontext und 3. Passwortgebrauch im Kontext des öffentlichen Dienstes. Diese Unterscheidung offenbart unterschiedliche Passwortkulturen innerhalb der drei hier untersuchten Gruppen. Die hier analysierten Datensätze bestehen ausschließlich aus Daten, die im Jahr 2024 gefunden wurden.

4.1 Private Accounts

Um die Passwörter zu privaten Accounts zu analysieren, wurde sich auf gängige Mailprovider für den deutschsprachigen Raum beschränkt. Für die Analyse der Passwörter privater Accounts wurden fast eine Milliarde Datensätze ausgewertet. Die große Menge an Datensätzen lässt sich dadurch erklären, dass Benutzer mit ihren E-Mail-Adressen mehrere Accounts bei verschiedenen Online-Plattformen, wie Onlineshops, Streaming-Diensten und Social-Media-Plattformen haben.

Insgesamt ergibt sich unter den Top 20 der privat genutzten Passwörter im Vergleich zu der Identeco Studie aus dem letzten Jahr ein stabiles Bild. Elf Passwörter der Top 20 aus diesem Jahr stimmen mit den Top 20 der gefundenen Passwörter aus dem letzten Jahr überein. Auffällig ist erneut, dass die Sicherheitspraktiken im Vergleich zu anderen Organisationsformen erheblich nachlässiger sind. Die Vorgaben vonseiten der Plattformen beschränken sich häufig lediglich auf eine Minimallänge des Passworts, wobei diese Maßnahme wenig Auswirkung auf die tatsächliche Komplexität der gewählten Passwörter hat. So finden sich unter den Top20 gefundenen Passwörtern einfache Zahlenfolgen wie “123456789” und “1111111”, aber auch das sehr einfache “password”.

TOP 20 privater Passwörter in Deutschland 2024

Pos.	Passwort	Pos.	Passwort
1.	123456	11.	111111
2.	password	12.	123456a
3.	12345	13.	654321
4.	12345678	14.	1q2w3e4r5t
5.	abc123	15.	monkey
6.	123456789	16.	dragon
7.	1234567	17.	ashley
8.	qwerty	18.	princess
9.	iloveyou	19.	q1w2e3r4t5y6
10.	password1	20.	a123456

https://identeco.de

Solche simplen Passwörter sind für Benutzer natürlich vor allem leicht zu merken, werden aber aufgrund ihrer häufigen Verwendung und ihrer Einfachheit bei Brute-Force-Angriffen oft als erste Optionen ausprobiert. Aufgrund der weiten Verbreitung solcher Passwörter sind solche Angriffe auf

Accounts dementsprechend häufig erfolgreich.

Ebenfalls auffällig sind lokale Einflüsse sowie die deutsche Begeisterung für den Fußball in die Passwortwahl. So sind Städtenamen wie „Berlin“, „Hamburg” oder „Dortmund“ recht häufig in den Passwörtern vertreten, aber auch “borrussia” , dessen Hauptkonkurrent “schalke04” oder einfach nur “fussball”.

Der Datensatz zeigt auch, dass viele Passwörter, die für die betrachteten Accounts verwendet werden, auf amerikanischen Tastaturen erstellt wurden. So ist zwar die Zeichenkombination “qwertz” vertreten, die einem deutschen Tastaturlayout entspricht, aber sogar häufiger tritt ihr auf amerikanischen Tastaturen erstellte Version “qwerty” auf. Bei dieser Buchstabenkombination handelt es sich um die ersten Buchstabentasten von oben links nach rechts auf der amerikanischen Tastatur.

Im privaten Bereich ist zudem eine Zunahme der Verwendung von Passwortstrategien zu beobachten, bei denen Passwörter in Anlehnung an den Namen eines gewählten Dienstes vergeben werden. So findet man zwar nicht unter den Top 20, aber durchaus häufig, z.B. Variationen des Namens “Netflix” als Passwort.

4.2 DAX Unternehmen

Um die Passwortkultur innerhalb von wirtschaftlich genutzten Accounts zu analysieren, wurden insbesondere Passwörter betrachtet, die zu Domains von DAX-Unternehmen gehören. Auffällig in diesem Kontext ist wie im letzten Jahr, dass Variationen des Namens der Organisation mit deutlichem Abstand am meisten als Passwort Verwendung finden. Sehr häufig findet man auch Varianten des Namens der Plattform LinkedIn. Dies lässt einige Rückschlüsse zu. Einerseits lässt dies darauf schließen, dass auch im beruflichen Kontext Variationen der Dienste, bei denen man sich anmeldet, als Passwort verwendet werden. Andererseits weist dies auf die Bedeutung der Networking-Plattform LinkedIn im wirtschaftlichen Bereich hin. Zu guter Letzt zeigt diese Beobachtung, dass die Daten aus dem LinkedIn-Leak von Anfang des Jahres 2023 mittlerweile im Netz Verbreitung gefunden haben.

TOP 20 beruflicher Passwörter in Deutschland 2024

Pos.	Passwort	Pos.	Passwort
1.	[Name der Organisation]*	11.	1234567
2.	[linkedin]**	12.	123456789
3.	123456	13.	sunshine
4.	password	14.	christian
5.	12345678	15.	london
6.	liverpool	16.	Welcome1
7.	12345	17.	chelsea
8.	111111	18.	d9189498
9.	Password1	19.	Martina
10.	softwaremagazine	20.	research

https://identeco.de

* Variationen des Organisationsnamens wurden durch einen Platzhalter ersetzt.
** Variationen des Namens „LinkedIn“ wurden durch einen Platzhalter ersetzt.

Entgegen der Erwartung, dass Konzerne dieser Größe robuste Sicherheitsmaßnahmen implementieren, zeigen die Datenleaks viele Einträge mit sehr einfachen Passwörtern. Ähnlich wie im privaten Bereich werden in diesem Kontext ebenfalls triviale Passwörter verwendet, darunter sind “123456”, “password” und selbst das etwas komplexere “Password1” zu finden.

Die Verwendung von sogenanntem “Leetspeak” bei der Passwortwahl ist ebenfalls zu beobachten. Leetspeak bezeichnet die Technik, bestimmte Buchstaben durch ähnlich aussehende Zeichen zu ersetzen. Eine Leetspeakvariante von “Passwort” wäre dementsprechend “p@55W0rt”. Leetspeak-Passwörter sind zwar leicht zu merken, jedoch sind sie für geübte Angreifer nicht wesentlich sicherer als reguläre Wörterbucheinträge.

Obwohl die meisten Zugänge innerhalb der DAX-Infrastrukturen durch mehrere Faktoren gesichert sein sollten, stellt die Wiederverwendung von Passwörtern auch in DAX-Unternehmen ein nicht zu vernachlässigendes Risiko dar. So besteht die Möglichkeit, dass durch wiederverwendete Passwörter auf extern genutzten Plattformen erhebliche Schäden verursacht werden. Beispielsweise können über einen übernommenen LinkedIn-Account Falschmeldungen über die entsprechende Firma verbreitet werden oder über einen übernommenen Account auf einer Ausschreibungsplattform gefälschte Angebote abgegeben und Einblick in vertrauliche Informationen (wie z.B. Geschäftspartner) erhalten werden.

4.3 Öffentliche Einrichtungen

Die Passwortkultur innerhalb öffentlicher Einrichtungen wurde anhand der Domains der Bundesministerien, nachgeordneter Bundesbehörden und der zehn bevölkerungsreichsten deutschen Städte erhoben. Auffällig ist auch hier, dass sehr viele Passwörter Variationen des jeweiligen Organisationsnamens darstellen. Anders als im privaten und im wirtschaftlichen Gebrauch, stellt man im öffentlichen Dienst relativ selten den Gebrauch von Trivialpasswörtern fest.

TOP 20 der Passwörter öffentlicher Einrichtungen 2024

Pos.	Passwort	Pos.	Passwort
1.	[Name der Organisation]*	11.	#Padlet2019!
2.	12345678	12.	1aRispe
3.	12cas34	13.	1s8b3ll8
4.	Aphrodite	14.	48P475CZ
5.	Klinge	15.	abbracci
6.	Paulchen	16.	da00b3eb
7.	sommer	17.	alexander
8.	30408	18.	Banicina20
9.	123456	19.	Johannes
10.	1234567	20.	i32565nd

* Variationen des Organisationsnamens wurden durch einen Platzhalter ersetzt.

https://identeco.de

Man findet außerdem in den Top 50 der öffentlichen Einrichtungen die Passwörter “34454Meise09” und “34454#Meise!09” an denen man ein interessantes Phänomen illustrieren kann. Diese Passwörter sehen nahezu identisch aus, mit dem einzigen Unterschied von zusätzlichen Sonderzeichen im zweiten Fall. Es ist zu vermuten, dass beide Passwörter derselben Person zuzuordnen sind, die bei einem genutzten Dienst aufgrund verstärkter Passwortrichtlinien (mindestens ein Sonderzeichen, mindestens 14 Zeichen) eine einfach zu merkende Variation ihres Passwortstammes etabliert hat. Ferner kann man annehmen, dass die betreffende Person noch nicht ausreichend auf grundlegende IT-Sicherheitsmaßnahmen geschult wurde, da sie wiederholt Opfer von Betrugsversuchen zur Passwort-Ermittlung geworden ist.

Der Mangel an dedizierten IT-Ressourcen in öffentlichen Institutionen, kombiniert mit der fortbestehenden Problematik der Passwort-Mehrfachverwendung, stellt daher immer noch eine

erhebliche Bedrohung dar. Die gezielte Verwendung von Arbeitgebernamen und die offensichtliche Mehrfachverwendung in Passwörtern weist durchaus auf mögliche Schwächen im Sicherheitsbewusstsein der Benutzer hin und stellt auch in diesem Bereich potenzielle Angriffsvektoren für Cyberkriminelle dar. Diese Erkenntnisse betonen die Notwendigkeit, die Sicherheitsinfrastruktur und die Sensibilisierung für sicherheitsrelevante Praktiken in öffentlichen Einrichtungen zu verbessern.

5. Erhöhung der Accountsicherheit

In Anbetracht der zunehmenden Bedrohungen durch Account-Übernahmen unter Verwendung geleakter Login-Daten empfehlen wir Benutzern folgende Maßnahmen für einen sicheren Umgang mit Passwörtern und Accounts:

1. Anlassbezogener Passwortwechsel

Es ist dringend erforderlich, ein Passwort sofort zu ändern, wenn Sicherheitsvorfälle auftreten oder sich Hinweise ergeben, dass die Integrität der Zugangsdaten gefährdet ist. Eine schnelle Passwortänderung hilft, potenzielle Risiken sofort zu beseitigen und die Sicherheit der Accounts zu gewährleisten.

Konkret: Ein Unternehmen überprüft die Passwörter ihrer Mitarbeiter und lässt umgehend die Passwörter aller Benutzer auf allen genutzten Plattformen ändern.

2. Passwort-Wiederverwertung vermeiden

Es wird dringend empfohlen, für jeden Dienst einzigartige Passwörter zu verwenden, die keine Überschneidung oder Ähnlichkeit mit bereits anderweitig genutzten Passwörtern aufweisen. Dies reduziert das Risiko, dass durch die Kompromittierung eines Accounts auf einer Plattform auch andere Konten gefährdet werden.

Konkret: Ein Benutzer verwendet ein Passwort ausschließlich für sein Online-Banking-Konto, ohne es für andere Dienste zu verwenden.

3. Passwortmanager nutzen

Die Verwendung eines Passwortmanagers wird empfohlen, um die Einrichtung, Verwaltung und Verwendung individueller sicherer Passwörter für jeden Dienst zu erleichtern. Ein Passwortmanager erleichtert nicht nur die Verwaltung, sondern fördert auch die Verwendung komplexer und einzigartiger Passwörter.

Konkret: Der Passwortmanager generiert automatisch ein komplexes und einzigartiges Passwort für jeden Onlinedienst.

4. Bewusste Komplexität von Passwörtern

Falls der Einsatz eines Passwortmanagers nicht möglich ist, sollte umso mehr auf einzigartige und

komplexe Passwörter geachtet werden. Verwenden Sie möglichst lange Passwörter und integrieren Sie Sonderzeichen, Groß- und Kleinbuchstaben sowie Zahlen, um die Sicherheit Ihrer Zugangsdaten zu erhöhen.

Konkret: Ein individuelles Passwort wie “Sich3r#Zug@ng2024” lang als auch komplex und dennoch leicht zu merken.

5. Multi-Faktor-Authentifizierung aktivieren

Wo immer möglich sollte Multi-Faktor-Authentifizierung (MFA) aktiviert werden. Bei MFA wird ein zusätzliches Sicherheitselement, wie zum Beispiel eine temporär generierte PIN oder ein biometrisches Merkmal zur Authentifizierung bei einem Account erfordert. Dies stellt eine zusätzliche Sicherheitsebene dar und erschwert den unbefugten Zugriff erheblich.

In einigen Bereichen ist Multi-Faktor-Authentifizierung bereits gesetzlich verpflichtend, so zum Beispiel beim Online-Banking. Für Mobiltelefone gibt es spezielle Apps, die eine einmalige PIN zur Authentifizierung generieren.

MFA empfehlen wir für private Accounts, aber auch dringend für gewerbliche Accounts. Trotz Firmenrichtlinien kann aber eine solche zusätzliche Sicherheitsmaßnahme bei externen Accounts nicht immer umgesetzt oder überprüft werden.

Konkret: Zusätzlich zum Passwort wird bei einer Multi-Faktor-Authentifizierung eine temporäre PIN oder eine biometrische Authentifizierung erfordert, um auf den jeweiligen Account zuzugreifen.

Ausblick: Passwordless und Passkeys

Im Jahr 2024 konnten wir vermehrt Online-Plattformen beobachten, die neben dem klassischen Login mit Benutzername und Passwort auch moderne Authentifizierungsverfahren wie Passkey anbieten. Passkeys basieren auf kryptografischen Schlüsselpaaren, die deutlich sicherer sind als Passwörter und nicht in Datenlecks kompromittiert werden können. Moderne Smartphones und Laptops integrieren diese Funktionalität komfortabel und ermöglichen eine schnelle Authentifizierung durch biometrische Merkmale wie Fingerabdruck oder Gesichtserkennung. Im Gegensatz zur klassischen Multi-Faktor-Authentifizierung, bei der mehrere Schritte notwendig sind, vereinen Passkeys Sicherheit und Benutzerfreundlichkeit in einem nahtlosen Prozess. Experten sehen in ihnen eine zukunftsweisende Alternative, die langfristig die Abhängigkeit von Passwörtern reduzieren könnte.

Doch bis zu einer breiten Etablierung von Passkeys gibt es noch zahlreiche Herausforderungen. So setzen viele Plattformen nach wie vor auf klassische Logins als Fallback-Lösung, was die potenziellen Sicherheitsvorteile einschränken kann. Auch die sichere Wiederherstellung von Passkeys, etwa bei Geräteverlust, ist noch nicht einheitlich geregelt. Zusätzlich braucht es Zeit, bis Nutzer die neuen Technologien akzeptieren und sich an deren Nutzung gewöhnen. Daher werden uns klassische Login-Daten wohl noch lange erhalten bleiben, bis sich passwortlose Verfahren als Standard durchgesetzt haben.

Diese Tipps zielen darauf ab, die individuelle Sicherheit im Umgang mit Passwörtern zu stärken und helfen dabei, potenzielle Schwachstellen in der Accountsicherheit zu minimieren. Die konsequente Anwendung dieser Empfehlungen ermöglicht es Benutzern, einen entscheidenden Beitrag zur Sicherheit ihrer persönlichen und beruflichen Accounts zu leisten.

6. Fazit

Das vorliegende Whitepaper bietet einen Einblick in die durch Passwörter verursachten Sicherheitsprobleme deutscher Verbraucher, Unternehmen und öffentlicher Einrichtungen. Aus der hier vorgelegten Analyse lassen sich Erkenntnisse gewinnen, die als umfassendes Feedback und Handlungsleitfaden für Unternehmen dienen können.

Insgesamt zeigt die Analyse, dass die Sicherheit von Accounts und Passwörtern nicht nur technische Aspekte umfasst, sondern auch stark von individuellem Verhalten, regionalen Präferenzen und kulturellen Einflüssen geprägt ist. Daher ist es entscheidend, bei der Passwortsicherheit nicht nur technologische Aspekte, sondern auch kulturelle und individuelle Eigenarten zu berücksichtigen. Daraus ergibt sich, dass Schulungen, Aufklärungskampagnen und benutzerfreundliche Sicherheitswerkzeuge unerlässlich sind, um eine nachhaltige Verbesserung der Account- und Passwortsicherheit zu erreichen.

Insbesondere aus der Sicht von Online-Diensten ist jeder Account eine Beziehung zu einem Kunden und als solcher wert, geschützt zu werden. Aus diesem Grund bietet Identeco seit vielen Jahren für Online-Plattformen umfassende Lösungen zur Account-Sicherheit an. So können beispielsweise beim Setzen oder Verwenden eines Passworts oder sogar unabhängig von einer Benutzeraktivität präventiv geprüft werden, ob eine Kombination aus E-Mail-Adresse und Passwort noch sicher ist oder bereits in kriminellen Kreisen kursiert.

Für Online-Plattformen, Unternehmen und öffentliche Einrichtungen fordern alle gängigen Standards im Bereich der IT-Sicherheit zwingend den Einsatz von Produkten zur Sicherstellung der Account-Sicherheit. Solche Produkte werden konform zu den Richtlinien der DSGVO von der Identeco GmbH & Co. KG angeboten. Durch diese Dienste ermöglicht Identeco, die Account-Sicherheit in allen Bereichen zu erhöhen, ohne durch unnötige Passwortwechsel oder False Positives bei der Überprüfung der Kompromittiertheit den Benutzer fälschlicherweise zu irritieren. Die Identeco GmbH & Co. KG überwacht bereits erfolgreich mehr als 100 Millionen Benutzerkonten für ihre Kunden.

Diese Studie wurde von Identeco in Zusammenarbeit mit der Rheinischen Friedrich Wilhelmsuniversität Bonn vorgelegt.

UNIVERSITÄT BONN