identeco

Whitepaper

Passwortsicherheit 2023

Die Passwörter der Deutschen

Editor: Dr. Matthias Wübbeling

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

Identeco GmbH & Co. KG

Joachimstr. 8, 53113 Bonn

kontakt@identeco.de

+49 (0) 228 28628581

Präambel

Die Identeco GmbH & Co. KG analysiert seit vielen Jahren Datenleaks mit Logindaten von Privatpersonen und Unternehmen. Dabei stehen by-design der Datenschutz im Sinne der DSGVO und die Verantwortung zur Accountsicherheit von Plattformanbietern und Unternehmen analog zu gängigen Standards, wie BSI IT-Grundschutz, ISO 27001 und NIST Cyber Security Framework, im Vordergrund.

Mit über 30 Milliarden gesammelten Datensätzen besitzt Identeco eine umfangreiche Basis aktueller und historischer Logindaten zur Absicherung von Benutzeraccounts. Der Auswertung dieses Whitepapers liegen dabei die in 2023 gesammelten Logindaten zugrunde. Die Schlussfolgerungen auf tatsächlich verwendete Passwörter in den betrachteten Branchen basieren dabei 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 die Bedeutung von Leakdaten für die Accountsicherheit jeglicher Einrichtungen.

Inhaltsverzeichnis

Präambel 2
1. Einleitung 4
2. Datenbasis der Analyse und Methodik 5
3. Industriestandards zur Accountsicherheit 6
4. Private Accounts 8
5. DAX Unternehmen 10
6. Öffentliche Einrichtungen 12
7. Erhöhung der Accountsicherheit 13
8. Fazit 15

1. Einleitung

Die rapide Zunahme von Cyberangriffen auf diverse Akteure, sei es auf Privatpersonen, Unternehmen oder öffentliche Institutionen wie Krankenhäuser, IT-Dienstleister der öffentlichen Hand oder Verwaltungen, erfordert eine detaillierte Analyse der Bedrohungslandschaft. Besonders beunruhigend ist die Feststellung, dass zahlreiche dieser Angriffe auf legitimen Zugangsdaten beruhen. Dieses Whitepaper setzt sich mit den Aspekten geleakter Logindaten, den Herausforderungen schwacher und starker Passwörter sowie den Risiken von Account Takeover auseinander.

Im Rahmen der Untersuchung wurden Herausforderungen fokussiert, die mit gestohlenen oder geleakten Daten verbunden sind. Die Quelle dieser Informationen, sei es durch Datenlecks oder Phishing-Angriffe für kriminelle Zwecke gewonnen, bringt interpretatorische Schwierigkeiten mit sich. Es ist zwar auf der einen Seite nicht möglich, auf sämtliche Passwörter von Deutschen oder der Mitarbeiter deutscher Unternehmen zu schließen, jedoch können durch geschickte Anwendung von Stichprobenprinzipien mit einer gewissen Wahrscheinlichkeit Rückschlüsse auf die tatsächliche Sicherheitslage gezogen werden. Ein einzelnes, gültiges Passwort passend zu einem Account kann heute schon genügen, um einem Angreifer den Zugang zum gesamten Unternehmensnetzwerk zu ermöglichen.

Die Bedrohungslage betrifft unterschiedliche Interessensgruppen, darunter Verbraucher, Mitarbeiter von Unternehmen und Benutzer verschiedener Online-Plattformen. Besonderes Augenmerk gilt den geleakten Passwörtern, die nicht nur einzelne Nutzer gefährden, sondern auch erhebliche Probleme im Bereich Datenschutz und DSGVO aufwerfen. Die Verarbeitung personenbezogener Daten, inklusive E-Mail-Adressen und zugehöriger Passwörter, steht oft im Widerspruch zu geltenden Datenschutzrichtlinien. Selbst wohlwollende Absichten, wie die Etablierung unternehmensinterner 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, der bereits in der Designphase die relevanten Sicherheitsbemühungen mit rechtlich konformem Handeln in Einklang bringt. In diesem Whitepaper wird die gegenwärtige Situation beleuchtet, und es werden praxisorientierte Empfehlungen für den Umgang mit geleakten Logindaten und die Stärkung der Passwortsicherheit vorgestellt.

Im nächsten Abschnitt erhalten Sie Informationen über die verwendete Datenbasis und die verwendeten Analyseverfahren. Anschließend werden die Einschätzungen und Auswirkungen der Sicherheitslage von Verbrauchern, öffentlichen Einrichtungen und Konzernen sowie in den Daten enthaltene Besonderheiten diskutiert.

2. Datenbasis der Analyse und Methodik

Die Grundlage der Analyse bildet eine umfassende Auswertung von etwa 36.000 Leakdateien, die im Verlauf des Jahres 2023 aus unterschiedlichen Quellen des Clear-, Deep- und Darknets gesammelt und analysiert wurden. Innerhalb dieses Datensatzes wurden in mehr als 12.000 Leakdateien relevante Identitätsdaten identifiziert. Insgesamt ergibt sich eine Datenmenge von 3,1 Milliarden Identitätsdaten, wovon schlussendlich 2,9 Milliarden Zugangsdaten als Basis für die vorliegende Analyse herangezogen wurden.

Um eine präzise Auswertung zu gewährleisten, wurden bestimmte Maßnahmen ergriffen. Insbesondere wurden Firmen-, Ministerien- und Städtenamen, selbst wenn sie nur als Teil eines Passworts verwendet wurden, vollständig ersetzt und zusammengefasst. Diese Anonymisierung dient vor allem dem Schutz sensibler Informationen und der Wahrung von Sicherheitsinteressen.

Es ist wichtig anzumerken, dass ausschließlich Passwörter von Accounts erfasst wurden, bei denen (mindestens) eine dazugehörige E-Mailadresse vorhanden war. Diese Fokussierung ermöglicht eine gezielte Analyse von Zugangsdaten, um 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 2023 zu liefern.

In 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. Jegliche nicht als Accountdaten identifizierte Informationen wurden sicher gelöscht und nicht weiterverarbeitet.

Die extrahierten Accountdaten durchliefen anschließend den Identeco eigenen Anonymisierungsprozess. Dabei werden eindeutige E-Mailadressen von den zugehörigen Passwörtern separiert und sicher gelöscht, um eine klare Trennung zu gewährleisten. Das Ergebnis ist eine Liste bestehend aus Passwörtern und den zugehörigen Top-Level-Domains. Durch die Auswertung der Top-Level-Domains können Unternehmen- und Institutionsnamen, die direkt oder auch als Teil eines Passwortes verwendet werden, identifiziert werden. Im weiteren Prozess wurden die Passwörter durch neutrale Platzhalter ersetzt, die eine Rückverfolgung auf einzelne Personen, Unternehmen oder Institutionen ermöglichen würden.

Um die Analyse auf den deutschsprachigen Raum zu begrenzen, wurden gezielt bestimmte Domains ausgewählt, die von besonderem Interesse sind. Hierzu gehören Top-Level-Domain-Endungen de, at und ch. Zudem wurden häufig im privaten Kontext verwendete E-Mailprovider in der Untersuchung einbezogen. Öffentliche Einrichtungen werden beispielhaft repräsentiert durch Bundesministerien, nachgelagerte Bundesbehörden und eine Liste großer deutscher Städte. Als repräsentative Auswahl für Unternehmen wurden die 40 im DAX gelisteten Unternehmen ausgewählt. Diese gezielte Auswahl ermöglicht eine präzise Analyse und die Identifikation spezifischer Mustern und Trends geleakten Passwörter für den deutschen Sprachraum im Jahr 2023.

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 ISO/IEC 27001 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 berücksichtig, ermöglicht es Unternehmen, ihre Infrastruktur robust und den Umgang mit Unternehmens- sowie Kundendaten sicher zu gestalten.

4. Private Accounts

Für die Analyse der Passwörter privater Accounts, wurden fast eine Milliarde Datensätze ausgewertet. Als Stichprobe haben wir E-Mailadressen betrachtet, die Mailprovidern zugeordnet werden können, die von deutschen Benutzern regelmäßig verwendet werden. Die große Menge an Datensätzen lässt sich einfach erklären: Mit ihren E-Mailadressen haben Benutzer mehrere Accounts bei verschiedenen Online-Plattformen, wie Onlineshops, Streaming-Diensten und Social-Media.

TOP 20 privater Passwörter der Deutschen 2023

Pos.	Passwort	Pos.	Passwort
1.	123456	11.	1234
2.	123456789	12.	abc123
3.	password	13.	iloveyou
4.	12345678	14.	000000
5.	123123	15.	fuk19600
6.	12345	16.	password1
7.	1234567	17.	654321
8.	111111	18.	123321
9.	qwerty	19.	qwerty123
10.	1234567890	20.	0000

Bei der eingehenden Analyse der TOP 20 der im privaten Kontext verwendeten Passwörter wird deutlich, dass die Sicherheitspraktiken im Vergleich zu anderen Organisationsformen erheblich nachlässiger sind. In den meisten Fällen beschränken sich die Vorgaben lediglich auf eine minimale Passwortlänge, wobei diese Maßnahme wenig Auswirkung auf die tatsächliche Komplexität der gewählten Passwörter hat. Unter den herausragenden Top 20 Passwörtern im privaten Kontext finden sich altbekannte und unsichere Kombinationen wie "123456", "password", "111111". Das vergleichsweise sentimentale "Iloveyou" ist in unserer Analyse sogar häufiger vertreten, als "ficken", das in den letzten Jahren immer wieder zu den Top-Passwörtern gehörte.

Diese simplen Passwörter sind für Benutzer natürlich vor allem leicht zu merken. Leider werden sie aufgrund der häufigen Verwendung und aufgrund ihrer Einfachheit bei Brute-Force-Angriffen oft als erste Optionen ausprobiert. Ihre weitreichende Verbreitung macht die damit geschützten Accounts zu besonders anfälligen Zielen für derartige Angriffe, die nicht selten aufgrund ihrer Häufigkeit und Vorhersehbarkeit durchaus erfolgreich sind. Es ist damit auch klar, dass eine stärkere Sensibilisierung der Benutzer hinsichtlich der Auswahl sicherer Passwörter und die Implementierung strengerer Sicherheitsrichtlinien seitens der Online-Plattformen durchaus erforderlich sind, um die persönlichen Daten und die Accounts der Benutzer effektiver zu schützen.

Die Passwortwahl der deutschen Benutzer spiegelt nicht nur Sicherheitsgewohnheiten der

Benutzer wider, sondern offenbart auch interessante kulturelle Nuancen. Ein faszinierendes Element, das sich durchaus in den Passwörtern widerspiegelt, ist die ausgeprägte Liebe zum Fußball. Dies manifestiert sich beispielsweise in der Verwendung von "schalke04" als Passwort, was nicht nur auf die Unterstützung des einen bestimmten Fußballvereins hinweist, sondern auch auf eine gewisse Verbundenheit zu diesem.

Ebenso ist die Verwendung des größten Rivalen von Schalke, der Stadt Dortmund, als Passwort auffällig. Interessanterweise zeigt sich in der Wahl von Städtenamen als Passwort aber auch eine unerwartete Richtung: Dortmund ist unter den Passwörtern deutlich häufiger vertreten als die deutsche Hauptstadt Berlin. Diese Beobachtung wirft Fragen auf, die über die bloße Einwohnerzahl hinausgehen. Man könnte nun also spekulieren, ob dies darauf zurückzuführen ist, dass Dortmund generell beliebter ist als Berlin oder ob es allein am Fehlen eines so prominenten Fußballvereins in Berlin liegt.

Diese Aspekte geben nicht nur Einblicke in die Entscheidungfindung der Benutzer im Umgang mit digitaler Sicherheit, sondern zeichnen auch ein Bild kultureller Präferenzen und regionaler Identität. Insgesamt verdeutlichen sie, dass die Wahl von Passwörtern für Benutzer nicht nur eine technische Angelegenheit ist, sondern vor allem eine Facette der individuellen und kollektiven Kultur widerspiegelt. Es betont die Notwendigkeit, Sicherheitsbewusstsein nicht nur auf technischer, sondern auch auf individueller und kultureller Ebene zu betrachten.

Auffällig ist ebenfalls, dass erstaunlich 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 fast genauso häufig tritt ihr auf amerikanischen Tastaturen erstellter Bruder "qwerty" auf. Bei "qwerty" handelt es sich um die ersten Buchstabentasten von oben links auf der englischen Tastatur.

5. DAX Unternehmen

Die Analyse der Passwortwahl innerhalb der DAX-Unternehmen gibt weitreichende Einblicke in Sicherheitspraktiken und menschliches Verhalten im Kontext digitaler Authentifizierung in Unternehmen. Entgegen der Erwartung, dass Großkonzerne dieser Größe robuste Sicherheitsmaßnahmen implementieren, zeigen die Datenleaks viele Einträge, die Accounts der Unternehmen betreffen. Ähnlich wie im privaten Bereich werden in diesem Kontext ebenfalls triviale Passwörter verwendet, darunter "123456", "password" und selbst das etwas komplexere "Password1" – hier fehlt nur ein Sonderzeichen, um die meisten Komplexitätschecks zu überstehen.

Interessant ist die Beobachtung, dass selbst gemeinhin als sicher bezeichnete Passwörter mit komplexen Kombinationen von Sonderzeichen, Zahlen sowie Groß- und Kleinbuchstaben, nicht vor Datenleaks geschützt sind. Selbst Passwörter mit scheinbar hoher Komplexität, wie etwa "ka_dJKHJsy6", können also gestohlen werden und demnach nicht unweigerlich als "sicher" eingestuft werden. Diese Beobachtung ist natürlich nicht spezifisch für DAX-Unternehmen, sondern gilt allgemein und unterstreicht die Herausforderungen im Bezug auf die Sicherheit, selbst bei komplexen und vermeintlich sicheren Passwörtern.

Die Passwortwahl der Mitarbeiter bei DAX-Unternehmen weist zudem darauf hin, dass Mitarbeiter heute durchaus eine starke Bindung zu ihren Arbeitgebern haben. Passwörter, die den Firmennamen oder Variationen davon enthalten, wie beispielsweise "FIRMENNAMErules" oder "FIRMENNAME4ever", sind besonders häufig anzutreffen. Die Verwendung solcher Passwörter ist jedoch aus Sicht der Accountsicherheit nicht zu empfehlen, da sie durch schlussfolgernde Kombination bei Angriffen leicht erraten werden können.

TOP 20 beruflicher Passwörter der Deutschen 2023

Pos.	Passwort	Pos.	Passwort
1.	[Name der Organisation]	11.	3xp3rt444
2.	123456	12.	Welcome1
3.	password	13.	12345
4.	9916691966@vV	14.	Dextr1016
5.	research	15.	optimist.3103
6.	pass1	16.	12345678
7.	wealth	17.	ka_dJKHJsy6
8.	Xchange1	18.	stratfor
9.	Password1	19.	thedancerfam
10.	1234567890	20.	1234

Ein bemerkenswertes Phänomen ist neben dem eigenen Firmennamen die Nutzung von Passwörtern, die die Namen von Zulieferern beinhalten. Dies Passwortstrategie, die auch bei privaten Konten der Endverbrauchern zu erkennen ist, weist darauf hin, dass

Mitarbeiter der DAX-Unternehmen ähnliche Praktiken bei der beruflichen Passwortwahl anwenden. Beispielsweise zeigt das Passwort "stratfor" auf Platz 18, dass Unternehmen offenbar auf Informationen des geopolitischen Informationsdienstes Strategic Forecasting vertrauen, was in Zeiten von Informationskriegen eine interessante Erkenntnis darstellt.

Zusätzlich zeichnet sich unter den Top 20 Passwörtern im DAX eine optimistische und selbstbewusste Grundstimmung ab. Passwörter, die Variationen der Zeichenfolgen "expert" oder "optimist" enthalten, sind häufig anzutreffen. Die Verwendung von sogenanntem "Leetspeak", bei dem Buchstaben durch ähnlich aussehende Zahlen ersetzt werden, ist ebenfalls zu beobachten. Leetspeak-Passwörter bieten zwar eine gute Merkbarkeit, sind jedoch für geübte Angreifer nicht wesentlich sicherer als herkömmliche Passwörter aus Wörterbüchern.

Abschließend sei darauf hingewiesen, dass, obwohl die meisten Zugänge innerhalb der DAX-Infrastrukturen vermutlich durch mehrere Faktoren gesichert sein sollten, die Wiederverwendung von Passwörtern ein nicht vernachlässigbares Risiko darstellt. Im schlimmsten Fall könnte durch wiederverwendete Passwörter auf extern genutzten Plattformen ein signifikanter Schaden verursacht werden. Stellt man sich einen übernommenen Account eines Unternehmens auf einer Ausschreibungsplattformen vor, könnte damit ein Konkurrent Einsicht in die eigenen Angebote erhalten oder gefälschte Angebote abgegeben werden, und so neben dem Einblick in vertrauliche Informationen auch einen deutlichen wirtschaftlichen Schaden verursachen.

6. Öffentliche Einrichtungen

Im Gegensatz zu DAX-Unternehmen verfügen öffentliche Einrichtungen, insbesondere Kommunen, oft nicht über eine eigenständige, vollwertige IT-Abteilung. Daher ist es nicht zwingend ein Versäumnis der Kommunen selbst, wenn sie Opfer von Hacking-Angriffen und Datenleaks werden. Ein deutliches Beispiel hierfür ist ein Hackingangriff auf den IT-Dienstleister Südwestfalen IT im November 2023, der zu einem flächendeckenden IT-Ausfall in über 70 Kommunen in Nordrhein-Westfalen führte. Trotz dieser Herausforderungen bleibt das grundlegende Problem des Passwort-Reuse bestehen und stellt eine fortlaufende Sicherheitsgefahr in allen Infrastrukturen dar.

TOP 20 der Passwörter öffentlicher Einrichtungen 2023

Pos.	Passwort	Pos.	Passwort
1.	Albert2001	11.	2710877
2.	schwabea	12.	cliff
3.	[Name der Organisation]	13.	hasenmaus
4.	652626	14.	rWJVHGmG
5.	efvj2ti	15.	xyjewati
6.	0132559004	16.	030408
7.	biskupn	17.	4802
8.	bundesanstalt06	18.	9q5r35j
9.	meidericher	19.	habitat
10.	0010054006	20.	keineahnung

Verwendete Passwörter im öffentlichen Dienst zeigen, dass die Wahl der Passwörter im Vergleich offenbar etwas mehr durchdacht wird. Triviale Zahlenkombinationen und Buchstabenfolgen sind eher selten anzutreffen. Ähnlich wie im DAX werden auch bei öffentlichen Einrichtungen Teile des Arbeitgebernamens als Passwörter verwendet. Interessanterweise sind regionale Eigenheiten in den Passwörtern erkennbar. Beispiele hierfür sind gewählte Passwörter wie "schwabea" (in Anspielung auf die Selbstbezeichnung Schwabe), "kölschemädche" oder "1fc1Colonia". Überraschenderweise finden sich auch Passwörter wie "jesus" und "maria" unter den häufig genutzten Passwörtern im öffentlichen Dienst. Geographische Bezeichnungen wie "marienforst" lassen zudem Rückschlüsse auf den Standort einer Dienststelle zu.

Die Sicherheitsrelevanz dieser Erkenntnisse für öffentliche Einrichtungen wird somit umso deutlicher. Der Mangel an dedizierten IT-Ressourcen in diesen Institutionen, kombiniert mit der fortbestehenden Problematik der Passwort-Mehrfachverwendung, stellt eine erhebliche Bedrohung dar. Die gezielte Verwendung regionaler Begriffen, religiösen Anspielungen und Arbeitgebernamen in Passwörtern weist durchaus auf mögliche Schwächen im Sicherheitsbewusstsein der Benutzer hin und stellt auch in diesem Bereich potenzielle Angriffsvektoren für Cyberkriminelle dar. Die Notwendigkeit, die Sicherheitsinfrastruktur und die Sensibilisierung für sicherheitsrelevante Praktiken in

öffentlichen Einrichtungen zu verbessern, wird durch diese Erkenntnisse verstärkt betont.

7. Erhöhung der Accountsicherheit

In Anbetracht der ständig wachsenden Bedrohungen im digitalen Raum empfehlen wir Benutzern folgende Maßnahmen für einen sicheren Umgang mit Passwörtern und Accounts:

1. Kein Passwort-Reuse

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

2. Unterstützung durch Passwortmanager nutzen

   Die Verwendung eines Passwortmanagers wird empfohlen, um das einfache Setzen, Verwalten und Nutzen individueller sicherer Passwörter pro Dienst zu ermöglichen. Ein Passwortmanager erleichtert nicht nur die Verwaltung, sondern fördert auch die Verwendung von komplexen und einzigartigen Passwörtern. Beispiel: Der Passwortmanager generiert automatisch ein komplexes und einzigartiges Passwort für jeden Onlinedienst.

3. Bewusste Komplexität von Passwörtern

   Falls der Einsatz eines Passwortmanagers nicht möglich ist, sollte bewusst 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. Beispiel: Ein individuelles Passwort wie "Sich3r#Zug@ng2023" ist sowohl lang als auch komplex.

4. Anlassbezogener Passwortwechsel bei Sicherheitsvorfällen oder Hinweisen auf Kompromittierung

   Es ist dringend erforderlich, ein Passwort sofort zu ändern, wenn Sicherheitsvorfälle passieren oder Hinweise auftauchen, dass die Integrität der Zugangsdaten gefährdet ist. Ein rascher Passwortwechsel trägt dazu bei, potenzielle Risiken unverzüglich zu beheben und die Sicherheit der Accounts zu gewährleisten. Beispiel: Nach der Überprüfung geleakter Passwörter in Unternehmen werden betroffene Passwörter der Benutzer auf allen Plattformen umgehend geändert.

5. Multi-Faktor-Authentifizierung aktivieren

   Wo immer möglich, sollte die Multi-Faktor-Authentifizierung aktiviert werden. Dies stellt eine zusätzliche Sicherheitsebene dar und erhöht die Schwierigkeit für unbefugte Zugriffe erheblich. Beispiel: Neben dem Passwort ist auch eine temporäre PIN oder biometrische Authentifizierung erforderlich, um auf das Konto zuzugreifen. Trotz Firmenrichtlinien kann das bei externen Konten nicht immer umgesetzt oder überprüft werden.

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.

8. Fazit

Das vorliegende Whitepaper bietet einen Einblick in die durch Passwörter verursachten Sicherheitsprobleme deutscher Verbraucher, Unternehmen und öffentlicher Einrichtungen. Im Zuge der umfassenden Diskussionen über Account- und Passwortsicherheit ergeben sich mehrere herausragende Erkenntnisse, die als umfassendes Feedback und Handlungsleitfaden für Unternehmen dienen können.

Insgesamt zeigt die Diskussion, 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. Ein umfassender Ansatz, der technologische, kulturelle und individuelle Aspekte berücksichtigt, ist entscheidend, um die Sicherheitspraktiken in der digitalen Welt effektiv zu stärken. Schulungen, Aufklärungskampagnen und benutzerfreundlichen Sicherheitswerkzeugen sind unerlässlich, um eine nachhaltige Verbesserung der Account- und Passwortsicherheit zu erreichen.

Aus Anbietersicht ist jeder Account eine Beziehung zu einem Kunden, die es wert ist, geschützt zu werden. Darum bietet Identeco seit vielen Jahren für Online-Plattformen eine umfassende Lösung, die beim Setzen oder Verwenden eines Passworts oder sogar unabhängig von einer Benutzeraktivität präventiv prüft, ob eine Kombination aus E-Mail-Adresse und Passwort noch sicher ist oder bereits in kriminellen Kreisen kursiert.

Durch die angebotenen Dienste ermöglicht Identeco die Accountsicherheit in allen Bereichen zu erhöhen, ohne durch unnötige Passwortwechsel oder False Positives bei der Überprüfung der Kompromittiertheit den Benutzer zu irritieren und von dem tatsächlichen Problem abzulenken. Alle gängigen Standards im Bereich der IT-Sicherheit fordern für Online-Plattformen, Unternehmen und öffentliche Einrichtungen zwingend den Einsatz von Produkten zur Sicherstellung der Accountsicherheit, wie Identeco sie, konform zu den Richtlinien der DSGVO, anbietet. Die Identeco GmbH & Co. KG überwacht bereits erfolgreich mehr als 100 Millionen Benutzerkonten für ihre Kunden.

ProSBAcT

Mit Forschung zu mehr Sicherheit!

- Schutz vor Account Takeover
- Anonymisierte Daten
- DSGVO-konformer Datenabgleich

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung