Die Lieblings-Passwörter der Deutschen Beruflich und privat

Benutzernamen und Passwörter sind die Schlüssel zu Online-Diensten und Benutzeraccounts. Häufig erhält man mit einem Zugang zu diesen Accounts Zugriff auf sensible Informationen – beruflich genauso wie privat. Die Sicherheitsexperten des Bonner Unternehmen Identeco recherchieren kontinuierlich in den dunklen Ecken des Internets nach Zugangsdatensammlungen und erfassen enthaltene Passwörter.
In einem aktuellen Whitepaper wertet Identeco nun aus, welche welche Passwörter im Jahr 2023 bisher in privaten und geschäftlichen Kontexten wurden.
Für den beruflichen Kontext haben die Mitarbeiter von Identeco die 40 DAX-Konzerne als Stichprobe analysiert. In diese Stichprobe fallen alle Kombinationen aus E-Mail-Adresse und Passwort, die den Hauptdomains der DAX-Konzerne zugeordnet werden konnten. Die erschreckende Erkenntnis: Offensichtlich verwenden viele berufliche Benutzer einfach den Firmennamen als Passwort!

Nicht nur interne Daten sind sensibel

„Viele denken bei der Passwortsicherheit zuerst an den Schutz der internen Daten“, sagt Identeco-CEO Matthias Wübbeling, „doch Mitarbeiter melden sich mit den Zugangsdaten auch bei externen Diensten an. Denken Sie zum Beispiel an eine digitale Ausschreibungsplattform. Wenn das Angebot für einen Großauftrag durch eine Übernahme Ihres Accounts in die Hände eines Mitbewerbers fällt, kann das immensen finanziellen Schaden verursachen.“

TOP 20 beruflicher Passwörter der Deutschen 2023

Pos.	Passwort
1.	[Name der Organisation]
2.	123456
3.	password
4.	9916691966@vV
5.	research
6.	pass1
7.	wealth
8.	Xchange1
9.	Password1
10.	1234567890

Pos.	Passwort
11.	3xp3rt444
12.	Welcome1
13.	12345
14.	Dextr1016
15.	optimist.3103
16.	12345678
17.	ka_dJKHJsy6
18.	stratfor
19.	thedancerfam
20.	1234

Auch privat schützen die Deutschen ihre Online-Konten und Daten mitunter nur mit schwachen Passwörtern.

Der Faktor Mensch – kein Unterschied: beruflich wie privat bedenklich

„Wir haben bei der Analyse beruflicher und privater Zugangsdaten häufig triviale Passwörter wie ‚password' oder ‚123456' gefunden", sagt René Neff IT-Sicherheitsexperte bei Identeco. Das erstaune wenig, denn auch bei international agierenden DAX-Unternehmen arbeiten schließlich „nur" Menschen an den Computern.

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

Zu viele Nutzer verwenden Passwörter mehrfach

„Die Häufigkeit der gefundenen Zugangsdaten bestätigt, was wir schon aus anderen Studien wissen", sagt Identecos Experte Frank Zickenheiner, „Viele Nutzer verwenden dasselbe Passwort für verschiedene Accounts." CEO Wübbeling ergänzt: „Mit mehrfach verwendeten Zugangsdaten können Hacker in Onlineplattformen und IT-Infrastrukturen eindringen, ohne dass das angegriffene Unternehmen selbst eine Sicherheitslücke hat – die gültigen Logindaten wurden ja bei einem anderen Anbieter gestohlen oder durch Phishing erbeutet."

Schutz vor Accountübernahme durch geleakte Zugangsdaten

Auf die Frage, wie Unternehmen sich und ihre Nutzer schützen können, antwortet Wübbeling eindeutig: „Wir finden mit Identeco jeden Monat hunderte Millionen Passwörter aus Datenleaks in den dunklen Ecken des Internets und schützen für unsere Kunden bereits jetzt mehr als 100 Millionen Accounts. Aus Anbietersicht ist jedes Onlinekonto eine Beziehung zu einem Kunden, die es wert ist, geschützt zu werden. Wir bieten eine umfassende Lösung für Onlinedienste. Dabei prüfen wir, ob eine Kombination aus E-Mail-Adresse und Passwort noch sicher ist oder bereits in kriminellen Kreisen kursiert. Das können wir beim Setzen des Passworts, bei der Anmeldung oder sogar völlig unabhängig von einer Benutzeraktivität."

Passwortregeln schützen nur begrenzt

Die Bonner Sicherheitsexperten weisen auf einen elementaren Sicherheitsaspekt hin: Auch ein Passwort, das allen aktuellen Sicherheitsempfehlungen entspricht, stellt ein Risiko dar, wenn es mehrfach verwendet wird. Deutlich wird dies am häufig gefundenen Passwort „ka_dJKHJsy6“. Formal erfüllt es alle relevanten Kriterien wie Groß-/Kleinschreibung, Ziffern und Sonderzeichen. Dennoch schafft es dieses Passwort in die Top-20 der Passwörter von DAX-Unternehmen.

Plattformanbieter und Arbeitgeber verantwortlich für Accountsicherheit

Die Anbieter von Onlineplattformen und Arbeitgeber sind laut Identeco verantwortlich für die Sicherheit ihrer Accounts. "Wir können es nicht den Verbrauchern aufbürden, in kriminellen Kreisen einen Überblick über geleakte Passwörter zu behalten", sagt Neff zu diesem heiklen Thema. "Vielmehr fordern alle relevanten IT-Sicherheitsstandards wie BSI Grundschutz, ISO 27001 oder das NIST Cybersecurity Framework von den Betreibern die kontinuierliche Überprüfung auf kompromittierte Logindaten."

Tipps zum Schutz vor Accountübernahme

Für einen sicheren Account gibt es laut Identeco mindestens fünf Tipps:

1. Verwenden Sie keine trivialen Passwörter.
2. Noch wichtiger: Verwenden Sie niemals ein Passwort mehrfach.
3. Nutzen Sie Passwortmanager zur Verwaltung Ihrer Passwörter.
4. Überprüfen Sie regelmäßig alle Accounts vor Bedrohungen aus Datenleaks.
5. Verwenden Sie wenn möglich Multi-Faktor–Authentifizierung

Für Endverbraucher empfehlen die Experten von Identeco hierzu den datenschutzkonformen und kostenfreien Leakchecker der Universität Bonn.

Link zum öffentlichen Leakchecker der Universität Bonn:
https://leakchecker.uni-bonn.de

Link zum Whitepaper:
https://identeco.de/de/blog/whitepaper_passwoerter_deutschland/
Pressematerial: https://identeco.de/de/press/

Über Identeco

Die Identeco GmbH & Co. KG (www.identeco.de) ist ein Spin-off der Universität Bonn und wurde 2020 mit dem Ziel gegründet, Benutzeraccounts datenschutzkonform vor betrügerischen Aktivitäten zu schützen. Zu den Kunden der ersten Stunde zählen das Business-Netzwerk XING und die Bonuspunkte-Plattform Payback.

Heute schützt Identeco mehr als 100 Millionen Benutzeraccounts vor der Übernahme mit geleakten Zugangsdaten. Das durch die Forschungsinitiative „StartUpSecure“ des

Bundesministeriums für Bildung und Forschung geförderte Unternehmen beschäftigt derzeit 21 Mitarbeiter.

Pressekontakt

Identeco GmbH & Co. KG
Dr. Frank Zickenheiner

frank@identeco.de
+49 (0) 228 504 437 82

Bonn, den 05.12.23