

Passwörter-Raten

Überblick

Die Verwendung schwacher Passwörter und das übermäßige Teilen von Informationen in Social Media sind zwei der größten Risiken in der modernen Sicherheitslandschaft. Schwache Passwörter bergen das Risiko eines unbefugten Zugriffs auf das Netzwerk und die sensiblen Daten einer Organisation. Cyberkriminelle nutzen häufig automatisierte Tools, um Anmeldedaten in Sekunden zu erraten. Sobald Akteurinnen und Akteure mit schlechten Absichten sich Zugriff auf das Netzwerk einer Organisation verschaffen, können sie Geld sowie sensible Daten stehlen oder die Kontrolle über Systeme übernehmen.

Diese Gruppenaufgabe legt den Schwerpunkt darauf, wie Angreifende öffentlich zugängliche Informationen verwenden, um die Passwörter oder Sicherheitsfragen von Menschen zu knacken. Die Teilnehmenden lernen, dass Passwörter nicht „123456“ lauten müssen, um unsicher zu sein. Die Verwendung persönlicher Details wie Namen von Haustieren, Geburtsdaten oder der Lieblingssportmannschaft machen es Akteurinnen und Akteure mit schlechten Absichten einfach, sich Zugriff auf Konten zu verschaffen.

Rollen

Moderation:

Steuert den Ablauf der Übung, leitet Diskussionen und bezieht, für eine aktive Mitarbeit, alle mit ein.

Teilnehmende:

Besprechen die Ideen und reagieren gemäß den Regeln der Übung auf das Szenario.

Einführung

Stellen Sie den Teilnehmenden das Szenario vor: Ihr Team wurde als „ethische Hacking-Gruppe“ beauftragt, die Sicherheit einer fiktiven Abteilung zu testen. Sie haben Mitarbeitende identifiziert, die Social Media aktiv nutzen. Ihr Ziel ist es, den öffentlichen Social-Media-Feed der Personen durchzugehen und ihr Passwort zu erraten, bevor echte Kriminelle das tun.

Teil 1: Identifizieren von Warnsignalen

 **Dauer:** 15 Minuten

Materialien:

- Timer oder Stoppuhr
- Szenario-Handouts
- Stifte
- Blätter

Anweisungen:

- Teilen Sie die Anwesenden in fünf Gruppen ein.
- Teilen Sie jeder Gruppe eine Person zu.
- Weisen Sie die Gruppen an, potenzielle Stichwörter wie Namen von Haustieren, Straßen, in denen die Personen als Kind gewohnt haben, wichtige Daten und Hobbys zu unterstreichen.
- Weisen Sie die Gruppen an, diese Stichwörter probeweise zu kombinieren, um das Passwort der Person zu erraten. Dabei können Symbole, Zahlen und Sonderzeichen einbezogen werden.
- Geben Sie den Gruppen 15 Minuten Zeit, die Beiträge zu lesen, zu besprechen und fünf Passwort-Vorschläge auf den Blättern zu notieren.

Teil 2: Diskussion

🕒 **Dauer:** 10 Minuten

Die Enthüllung:

Bevor mit den Fragen begonnen wird, enthüllt die moderierende Person das richtige Passwort jeder Person und erklärt die Logik dahinter.

Fragen:

- Welche geteilte Information machte das Passwort der Person leicht zu erraten?
- Sind Ihnen „falsche Spuren“ aufgefallen, also Informationen, die die Person geteilt hat und die ein wahrscheinliches Passwort hätten sein können, es aber nicht waren?
- Wie fühlt es sich an, dass Fremde offensichtlich aus nur einigen wenigen Beiträgen so viel über Sie erfahren können?

Mögliche Antworten/Prompts:

- **Teilen von übermäßig vielen Informationen:** Kriminelle suchen nach Lebensereignissen (neues Auto, neues Haustier, Abschluss), denn diese Wörter verwenden Menschen am häufigsten in Passwörtern.
- **Passwort-Muster:** Viele Menschen verwenden vorhersehbare Muster (Name + Jahr), die sehr einfach zu erraten sind, wenn man ihre Interessen kennt.
- **Wichtigste Erkenntnis:** Wenn Fremde es erraten können, kann ein Computer es in wenigen Sekunden knacken. Persönliche Informationen sollten niemals Teil Ihres Passworts sein.

Fazit

🕒 **Dauer:** 5 Minuten

Schließen Sie die Übung ab, indem Sie die Konzepte in Zusammenhang mit der Realität Ihrer Organisation stellen. Erklären Sie, dass diese Personen zwar fiktiv waren, echte Cyberkriminelle jedoch automatisierte Tools verwenden, die genau das können, was die Teilnehmenden manuell erledigt haben – nur viel schneller.

Nutzen Sie die Gelegenheit, mögliche Fragen der Teilnehmenden rund um die Erstellung starker Passwörter, den Schutz von Konten und sichere Online-Gewohnheiten zu beantworten. Beachten Sie folgende Best Practices:

- Verwenden Sie individuelle Passwörter für jedes Konto.
- Bei der Erstellung neuer Passwörter ist Länge wichtiger als Komplexität. Verwenden Sie Passphrasen, also ganze Sätze, als starke Passwörter. Diese können Leerzeichen, Sonderzeichen, Zahlen und andere Symbole enthalten. Beispiel: *Bären! essen täglich gelbe Äpfel*
- Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) zum Schutz Ihres Kontos. Ihrer Anmeldung mit einem starken Passwort fügt MFA einen zweiten Verifizierungsschritt hinzu, z. B. einen Code, der an Ihr Mobilgerät gesendet wird, eine PIN oder einen Fingerabdruck.
- Befolgen Sie die Passwort-Richtlinien Ihrer Organisation.

Antwortschlüssel für die Moderation

Person 1: Sarah Miller

Antwort: **Vegas2018!**

Sarah verwendet den Namen ihrer Heimatstadt und ihr Abschlussjahr. Eine einfache Suche liefert die Informationen, mit denen Cyberkriminelle ihr Konto knacken können.

Person 2: Fatima Al-Sayed

Antwort: **SternenbeobachterZin4**

Fatima verwendet den Namen ihres Haustiers (Zina) und ihr Hobby (Sternenbeobachtung). Dies ist ein „Verhaltenswarnsignal“, das zeigt, dass schwache Passwörter häufig persönliche Informationen enthalten.

Person 3: Elena Rodriguez

Antwort: **SophiaParis7**

Elena verwendet Namen und Alter ihrer Tochter sowie ein Reiseziel. Das kann auf den ersten Blick sicher erscheinen, doch die Einbeziehung von Familienmitgliedern und Reiseinformationen machen das Passwort anfällig für Hacking-Angriffe.

Person 4: Arjun Nair

Antwort: **Arjun2004Kombi**

Arjun verwendet seinen Vornamen und Informationen zu seinem Auto. Das Passwort ist lang, doch da es seinen eigenen Namen enthält, ist es extrem anfällig. Seine Liebe für das Auto ist auf seinem Social-Media-Profil leicht zu finden und lässt sich dazu verwenden, sein Passwort zu erraten.

Person 5: David Chen

Antwort: **Cooper_liebt_Wandern**

David verwendet den Namen seines Haustiers und eine gemeinsame Aktivität. Wenn man sein Social-Media-Profil durchgeht, lässt sich diese schwache, offensichtliche Passphrase leicht erraten. Die Unterstriche bieten nicht genügend Sicherheit.

Anhang: Szenario-Handout Teil 1

Schneiden Sie entlang der Linien, um einzelne Karten für die Teilnehmenden zu erhalten, und geben Sie jeder Gruppe eine Karte.

Person 1



Sarah Miller

@sarah_miller

202 Follower 125 gefolgt

Beiträge Antworten Medien



Sarah Miller @sarah_miller · 1 T.

Kaum zu glauben, dass mein bester Freund Bell heute schon 3 wird! #Hundegeburtstag



12 5 89



Sarah Miller @sarah_miller · 2 T.

Hab gerade mein Traumauto gekauft! Einen hellblauer Mustang. So einen wollte ich schon seit meinem Abschluss 2018 haben.

1 12



Sarah Miller @sarah_miller · 3 T.

Bin gerade am Red Rock Canyon. So schön, mal wieder in meiner Heimatstadt Las Vegas zu sein!



1 5 5

Person 2



Fatima Al-Sayed

@fatimaa

342 Follower 392 gefolgt

Beiträge Antworten Medien



Fatima Al-Sayed @fatimaa · 1 T.

Meine Katze Zina sitzt am liebsten auf meinen Entwürfen, wenn ich arbeite.



12 5 89



Fatima Al-Sayed @fatimaa · 2 T.

Ein Wochenende mit Sternbeobachtung am Al-Qudra-See.

1 12



Fatima Al-Sayed @fatimaa · 3 T.

Wunderschöner Sonnenuntergang an der Küste von Jumeirah heute.



7 5 53



Anhang: Szenario-Handout Teil 2

Schneiden Sie entlang der Linien, um einzelne Karten für die Teilnehmenden zu erhalten, und geben Sie jeder Gruppe eine Karte.

Person 3



Elena Rodriguez

@erodriguez

445 Follower 803 gefolgt

Beiträge Antworten Medien



Elena Rodriguez @erodriguez · 1 T.

Alles Gute zum Geburtstag, Sophia, meine kleine Prinzessin! Kaum zu glauben, dass sie heute schon 7 wird.



12 5 89



Elena Rodriguez @erodriguez · 2 T.

Endlich in Paris! Davon habe ich schon als Kind geträumt.

4 2



Elena Rodriguez @erodriguez · 3 T.

Morgenroutine: Ein doppelter Espresso und ein Spaziergang auf der Maple Street. Bester Start in den Tag!



1 1 4

Person 4



Arjun Nair

@arjun_nair

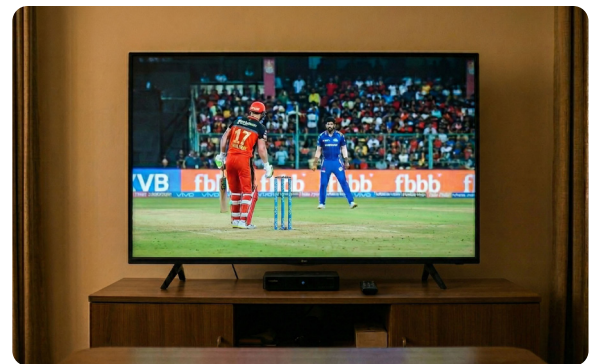
645 Follower 762 gefolgt

Beiträge Antworten Medien



Arjun Nair @arjun_nair · 1 T.

Heute IPL-Finale! Auf geht's Bangalore!



12 5 89



Arjun Nair @arjun_nair · 2 T.

Kann es kaum erwarten, auf meiner Reise nächsten Monat den Himalaya zu sehen!

3 2



Arjun Nair @arjun_nair · 3 T.

Mein erstes Auto war ein blauer Kombi, Baujahr 2004. Er hat so viele Reisen überlebt!



1 5 5



Anhang: Szenario-Handout Teil 3

Schneiden Sie entlang der Linien, um einzelne Karten für die Teilnehmenden zu erhalten, und geben Sie jeder Gruppe eine Karte.

Person 5



David Chen

@david_chen

956 Follower 243 gefolgt

Beiträge Antworten Medien



David Chen @david_chen · 1 T.

Cooper hat den Wanderweg am Blue Ridge dieses Wochenende geliebt.



2 1 89



David Chen @david_chen · 2 T.

Mein erstes Auto war eine silberfarbene Limousine, Baujahr 1992. Ich vermisse dieses Auto.

1 12



David Chen @david_chen · 3 T.

Heute schaue ich das Lakers-Spiel – hoffentlich können sie den Sieg nach Hause holen!



4 6 5

