Wie sicher sind Passwörter? Der Hacker weiss es

Passwörter begleiten uns heute durch sämtliche Lebensbereiche. Was einst als die sicherste und verbreitetste Methode zur Authentifizierung und Autorisierung galt, ist heute ein heikles Unterfangen. Denn damit Passwörter wirklich zum Schutz von elektronischen Daten und IT-Infrastruktur beitragen, sollten sie einer regelmässigen Prüfung unterzogen werden.

Schwache Passwörter stellen immer noch ein grosses Problem für Unternehmen dar. Der Data Breach Investigations Report 2021 von Verizon zeigt, dass zudem der Diebstahl von Zugangsdaten vehement zugenommen hat. Benutzerpasswörter werden in der Regel nicht im Klartext, sondern als sogenanntes Hash, einem digitalen Fingerabdruck, abgelegt. Hashes können von Hackern beispielsweise mittels NTLM-Relaying-Angriff dazu benutzt werden, das ursprüngliche Klartext-Passwort zurückzurechnen. Im Fachjargon spricht man von «Passwort-Cracking». Genau dieser Methode bedienen sich auch Cyber-Security-Unternehmen, wie «terreActive», in Mission für ihre Kunden: Man stellt dem Kunden einen «guten Hacker» zur Verfügung, der die Passwörter auf Herz und Nieren prüft. Der Kunde muss lediglich die Hashes aller Mitarbeitenden zusammentragen und sie dem Security-Provider übergeben. «Der Hacker» versucht, daraus die Passwörter wiederherzustellen. Je schneller ihm dies gelingt, desto schlechter ist es um die Qualität der Passwörter im Unternehmen bestellt.

Passwort-Cracking für mehr Sicherheit

Ein Unternehmen sollte also regelmässig überprüfen, ob die Passwörter robust genug sind, um einem Hackerangriff standzuhalten. Analysiert werden Passwörter von normalen und privilegierten Benutzern sowie von Service-Accounts. Engagiert ein Unternehmen einen Security Provider für einen Passwort-Check, sollten die Ziele – nämlich Schwachstellen frühzeitig zu identifizieren und Klarheit zu gewinnen – von Beginn an definiert sein. Die zentralen Fragen für Unternehmen lauten:

- Wie sieht es mit der Qualität der Passwörter im Unternehmen generell aus?
- Wie hoch ist das Risiko, dass Benutzerkonten kompromittiert werden könnten?
- Werden die internen Passwortrichtlinien eingehalten?
- Weisen die Richtlinien Schwachstellen hinsichtlich Mindestlänge oder Komplexität auf?
- Wo gibt es Verbesserungspotenzial?

Highspeed Cracking-Station

Um die Hashes in einer vertretbaren Zeit zu knacken, benötigt man eine ausserordentliche Rechenleistung. Entsprechend teuer und technisch anspruchsvoll ist der Bau einer Cracking-Station. «terreActive» verfügt über so eine Station, die an einem firmeneigenen, speziell gesicherten Ort gelagert wird. Aufgrund der Sensibilität der Daten wird das Projekt in den Räumen des Kunden durchgeführt. Die Cracking-Station, auf der später die Passwort-Hashes eingespeist werden, wird für den Zeitraum des Projektes vom Security-Provider an den Kunden ausgeliehen und «air-gapped» – also in völliger Isolation zu anderen Systemen sowie zum Internet betrieben. Nach Abschluss des Cracking-Vorganges, der je nach Menge der Passwörter Tage oder Wochen dauern kann, werden alle Ergebnisse und Auswertungen gelöscht, die Festplatte ausgebaut und dem Kunden übergeben. Die Erfahrungen zeigen, dass bei einem Passwort-Cracking bis zu 80 Prozent der Passwörter geknackt werden. Unter den Benutzern findet sich in der Regel ein beträchtlicher Anteil von administrativen sowie privilegierten Accounts. Diese sind eine besonders wertvolle Beute für einen Angreifer, denn mit einem Administratorzugang hat man die beste Möglichkeit, sich im internen Netzwerk auszubreiten.

iStock.com/AndreyPopov

Nutzen für CISO und Management

Der verfasste Abschlussbericht enthält, neben einer Analyse der Ergebnisse und einer Standortbestimmung, wertvolle Details wie Statistiken zu gecrackten Passwörtern und betroffenen Benutzerkonten. Enthalten sind ebenfalls Empfehlungen für zukünftige Schutzmassnahmen, ergänzt mit Hinweisen zu sicheren Passwörtern und -richtlinien, die als Hilfsmittel für die Kommunikation mit den Mitarbeitenden im Rahmen eines Awareness-Trainings eingesetzt werden können. ■

TerreActive AG, CH-5001 Aarau
✆ +41 (0)62 834 00 55
info@terreactive.ch, www.security.ch