Hauptsitz Zederhaus
Zederhaus 155 | 5584 Zederhaus

Office Puch/Hallein
Urstein-Süd 19, Stiege 3 | 5412 Puch bei Hallein

Office Sonnberg
Gewerbezeile 68 | 4202 Sonnberg

INHALTSVERZEICHNIS

Passwort-Guide

INTRO

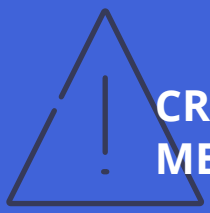
Passwörter haben grundlegende Bedeutung beim Schutz der IT-Systeme und Daten. Die richtige Auswahl und der richtige Umgang mit Passwörtern können über die Sicherheit vor unbefugten Zugriffen und Manipulationen entscheiden.

Mögliche Probleme, die durch ein geknacktes Passwort auftreten können, sind:

- Identitätsdiebstahl
- Zugriff auf weitere Passwörter und sensible Daten
- Sperre zu eigenen Konten
- Phishing Angriff
- Installation von Spyware
- Verkauf Ihrer Daten an Datenbroker

Daher müssen Passwörter ausreichend komplex sein und regelmäßig geändert werden, um nicht durch diverse Cracking Methoden erraten werden zu können.

Dieser Guide verschafft Ihnen einen Einblick in die Thematik und gibt Aufschluss über wichtige Regeln, die bei der Passwortvergabe zu beachten sind.



CRACKING-METHODEN

Unter »Cracking« versteht man verschiedene (oft automatisierte) Vorgehensweisen, zur Entschlüsselung von Passwörtern. Passwort-Cracking-Tools nutzen oftmals ihre eigene Rechenleistung und ermitteln durch simples Ausprobieren und speziellen Algorithmen die verschlüsselten Zugangscodes.

DIEBSTAHL DER PASSWÖRTER DURCH AUSLESEN DER HASH-ALGORITHMEN

Ein Hash-Algorithmus ist eine Einweg-verschlüsselung, die ein Klartext-Passwort in eine Folge von Buchstaben, Zahlen und Sonderzeichen umwandelt. Diese gehashten Versionen des Passworts werden oft im System oder Netzwerk gespeichert. Durch Softwareschwach-stellen oder gezielte Exploits verschaffen sich Hacker Zugriff auf diese Daten und können in weitere Folge eine Vielzahl an weiteren Passwörtern einfach auslesen ohne jedes einzelne davon extra knacken zu müssen.

BRUTE-FORCE-ANGRIFFE

Bei einem Brute-Force-Angriff werden Computerprogramme verwendet, die in unzähligen Zyklen verschiedenste Wort- und Zeichenkombinationen generieren und abgleichen. Nach dem Prinzip von Versuch und Irrtum wird so versucht, das Passwort zu knacken. Dabei werden oft ganze Wörterbücher und Wortlisten durchgespielt. Die Methode ist einfach, aber effektiv. Moderne Rechner sind dabei in der Lage ein achtstelliges alphanu-merisches Passwort oder eine ID in nur wenigen Sekunden zu knacken.

MASKENANGRIFFE

Maskenangriffe sind durch einen verrin-gerten Arbeitsaufwand, im Vergleich zu Brute-Force-Angriffe, gekennzeichnet. Dem Hacker sind bereits Teile des Passwortes bekannt und er kann seine automatisierte Abfrage zielgerichteter definieren. Maskenangriffe können nach bestimmten Wörtern, Zahlen innerhalb eines gewissen Bereichs oder nach der Gesamtlänge des Passworts gefiltert werden.

SOCIAL ENGINEERING

Unter diesem Terminus wird die Manipulation von Menschen gekenn-zeichnet um sich Zugang zu schützens-werten Daten zu verschaffen. Unter falschen Vorwänden werden Personen dazu gebracht, sensible Daten preis zu geben. Beispielsweise geben sich Hacker als technischer Support an, um das Vertrauen der Mitarbeiter zu gewinnen und sich Zugang zu ihrem Computer zu verschaffen. Im Zeitalter der sozialen Medien werden auch häufig anhand von Quizes persönliche Daten gesammelt. Daher ist hier auch Vorsicht geboten.

SPIDERING

Spidering bezeichnet eine Art personalisierte Wortliste, anhand derer die Angriffe durchgeführt werden. Hacker durchforsten Social-Media-Konten, Marketing-Kampagnen oder andere Unternehmensunterlagen (z.B.: Handbücher, Schulungsunterlagen etc.) und sammeln Schlüsselwörter für den Brute-Force-Angriff.

8 TIPPS FÜR EIN STARKES PASSWORT

MIND. 16 ZEICHEN

Die Länge des Passwortes ist der wichtigste Faktor im Bezug auf die Sicherheit des Zugriffes. Kurze Varianten können durch die großen Rechen-leistungen der Hacker relativ schnell erraten werden. Je länger das Passwort desto sicherer ist es, da deutlich mehr Eingabedurch-läufe nötig sind.

BUCHSTABEN, ZAHLEN UND SONDERZEICHEN

Ein möglichst abwechslungsreicher Mix aus Buchstaben, Zahlen und Sonder-zeichen erhöht die Sicherheit des Pass-wortes. Wiederholungen sollten dabei vermieden und eine große Variation der verwendeten Zeichen unterstützt werden.

GROSS- & KLEINSCHREIBUNG

Die Kombination aus Groß- und Klein-schreibung macht das Passwort sicherer. Dabei sollte ebenfalls eine möglichst große Abwechslung geschaffen werden.

ESELSBRÜCKEN & PERSÖNLICHE MERKSÄTZE

Ein Passwort, das auf einer Eselsbrücke beruht, ist wesentlich leichter zu merken. Wichtig dabei ist nur, dass es sich um keine gängige Phrase handelt. Dieser Merksatz sollte mit den vorangegangenen Punkten (Länge, Zeichenmix, Groß- & Kleinschreibung) angereichert werden, um ein hohes Sicherheitslevel zu erreichen.

ZUFÄLLIGE REIHENFOLGE / KEINE LOGIK

Programmierte Tools und Algorithmen basieren oftmals auf Logik.
Eine willkürliche Reihenfolge der Zeichen (Sonderzeichen, Zahlen, Buchstaben etc.) erschwert Hackern den schnellen Zugriff.

DIVERSITÄT

Für jede neue Website / für jeden neuen Zugang, sollte ein eigenes Passwort erstellt werden, damit ein bereits geknackter Zugriff nicht auf weitere Konten angewendet werden kann.

VOREINSTELLUNGEN ÄNDERN

Manche Institutionen und Webseiten bieten voreingestellte Passwörter bei einer Registrierung an. Dieser Service ist grundsätzlich hilfreich und praktisch, sollte jedoch langfristig gesehen mit einer eigenen, sicheren Kombination ausgetauscht werden.

GEHEIMHALTUNG & SICHERE AUFBEWAHRUNG

Besteht der Verdacht, dass das Passwort von Dritten ausgelesen wurde, oder in fremde Hände geraten ist, sollte es umgehend getauscht werden. Ebenfalls sollten Passwörter nicht öffentlich zugänglich (anhand Klebezettel o. ä.) aufbewahrt werden. Ein Passwort Manager verwaltet z.B. an einem sicheren digitalen Ort, alle Passwörter und kann anhand eines übergeordneten Master-Passwortes verwaltet werden.

TIPP: Passwort Manager verwenden

Passwort-Manager sind spezielle Programme, die alle Zugangsdaten zu Ihren Anwendungen sicher verwahren. Über ein komplexes „Masterpasswort“ erhält man Zugriff auf die Datenbank, und muss sich folglich nicht alle einzelnen Passwörter merken.

NO-GOS BEI PASSWÖRTERN

Die folgenden neun Punkte kennzeichnen schwache Passwörter, die schnell von Hackern geknackt werden können:

ZAHLENREIHEN
Beispiele: 1234567; 9899100

BUCHSTABENREIHEN
Beispiele: abcdefg; xxxxx

TASTATURMUSTER
Beispiele: yxcvb; qwertz

WIEDERHOLUNGEN
Beispiele: hallo!hallo; 123123

PERSÖNLICHE DATEN

Namen, Vornamen, Geburtsdaten, tel. Durchwahlen, KFZ-Kennzeichen etc. dürfen nicht verwendet werden. Sie sind leicht ausfindig zu machen und werden bei Versuchen, ein Passwort zu erraten, mit Sicherheit getestet.
Beispiele: alexander+lena; 1Juli1993

KOMBINATION AUS SIMPLES WORT + SONDERZEICHEN

Beispiele: !Autobahn!; passwort123

VERSAND PER E-MAIL

Der Versand von Passwörtern sollte nicht über Mail stattfinden, da man dabei nicht zu 100 Prozent sicher stellen kann, dass es in die richtigen Hände gelangt

ABLAGE AUF PAPIER

Auch in diesem Szenario, muss die Sicherheit der Daten beachtet werden – eine Dokumentation von Passwörtern auf Post-Its im Büro sind auch unternehmensfremden Personen leicht zugänglich und somit unangebracht

SPEICHERUNG IM WORD

Hacker können sich Zugriff auf digitale Dateien verschaffen und dort ganz einfach Textpassagen auslesen. Daher ist die Speicherung von Passwörtern in Word auch ungeeignet

SOLBYSEC
POWERED BY SOLBYTECH

www.solbysec.at | info@solbysec.at