Passwörter: Die Schlüssel zu Computer und Internet

Kompakte Security-Infos für Unternehmen

Passwörter sind ein wichtiges Mittel gegen unberechtigte Zugriffe auf Computer, E-Mails oder Bankkonten. Ein sicheres Passwort ist also ein Muss! Aber der Umgang mit Passwörtern will gelernt sein.

Was ist ein sicheres Passwort?

Die Stärke oder Qualität eines Passworts definiert sich durch folgende Parameter:

- Die Anzahl der Zeichen (Länge) eines Passworts
- Die Art der verwendeten Zeichen wie z.B. nur Kleinschreibung, nur Zahlen, oder auch Sonderzeichen (P@sswor$T)
- Das verwendete Wort selbst. Existiert dies in einen Lexikon oder Wörterbuch, stellt es ein Risiko dar.
- Die Anzahl an verschieden Passwörtern, die ein User einsetzt
- Das Alter des Passwortes (seit der letzten Änderung)

Ist Ihr Passwort ein „Generalschlüssel“?

Eines gleich vorweg; Sie sollten **NICHT** dasselbe Passwort auf mehreren System oder Webseiten benutzen. Wird eine Webseite gehackt und dabei die Passwortliste erbeutet ist es ein leichtes den Usernamen (meist Email Adresse) und Ihr Passwort auf gängigen System wie Amazon, Ebay usw. auszuprobieren.

Ein einfacher Trick wäre hierbei das Passwort auf die betreffende Seite/Programm anzupassen um maschinelle Angriffe zu verhindern.

Beispiel:

- Ebay: ePasswortby oder ebPasswort
- Youtube: yPassworte oder youPassworte

Passwörter müssen auch regelmäßig geändert werden. Denn wenn Ihr Kennwort doch einmal in die falschen Hände gelangt, wird der Missbrauch zumindest zeitlich eingeschränkt.

Einfach mal alle Wörter durchprobieren

Die gängigste Methode des Passwortcrackens ist das simple „Ausprobieren“ von verschiedensten Passwörtern. Angefangen mit den Namen Ihrer Angehörigen, Hobbys zum Beispiel die Marke Ihres Autos wäre ein guter Anfang.

Um das Ganze aber etwas effizienter zu gestalten gibt es die passenden Tools um solch ein Ausprobieren etwas schnell zu erledigen. Dabei beginnt man mit einer „Dictionary“ Attacke, die einfach jedes Wort in einem Wörterbuch durchprobiert. Die deutsche Sprache besteht aus rund 300.000 Wörtern, Englisch aus rund 500.000 Wörtern.

Mit Hilfe eines Standard PC und der passenden Software können wir rund **1 Million Passwort Versuche pro SEKUNDE** erledigen. Somit wäre jedes deutsche und englische Wort in weniger als einer Sekunde durchprobiert. Gängig dabei ist auch ein zweiter Durchgang, wobei dann das erste Zeichen dann in Großschreibung probiert wird.

Deshalb sollten Sie niemals ein real existierendes Passwort benutzen!

Jedes Passwort kann herausgefunden werden

Wenn man bei der ersten Attacke kein Glück hatte, da das Passwort in keinen Wörterbuch existierte, startet man den zweiten, banaleren, aber mühsameren Versuch mit Hilfe einer sogenannten „Brute Force" Attacke.

Klingt sehr kompliziert, ist es aber nicht! Man probiert einfach alle möglichen Zeichenfolgen nacheinander durch. Man startet mit A dann B dann C... AA, AB, AC, AD... ABA, ABB, ABC...

Der entscheidende Unterschied liegt hierbei in der Anzahl der möglichen Kombinationen durch:

- Die Art der verwendeten Zeichen (a, A, 1, äöü, #+*@)
- Die Anzahl der Stellen/Länge des Passwort

Die folgende Tabelle zeigt den geschätzten **Zeitaufwand zum Herausfinden eines Passwortes** mit Hilfe von profesionellen Server System bei rund 1 Milliarde Versuche pro Sekunde:

	Passwortlänge						
Zeichenraum	**4 Zeichen**	**5 Zeichen**	**6 Zeichen**	**7 Zeichen**	**8 Zeichen**	**9 Zeichen**	**10 Zeichen**
26 [a-z]	<1 Sek.	<1 Sek.	<1 Sek.	8 Sek.	4 Min.	2 Std.	2 Tage
52 [A-Z;a-z]	<1 Sek.	<1 Sek.	20 Sek.	17 Min.	15 Std.	33 Tage	5 Jahre
62 [A-Z;a-z;0-9]	<1 Sek.	<1 Sek.	58 Sek.	1 Std.	3 Tage	159 Tage	27 Jahre
96 (+Sonderzeichen)	<1 Sek.	8 Sek.	13 Min.	21 Std.	84 Tage	22 Jahre	2108 Jahre

Rechenzeit eines Brute-Force-Angriffs bei 1 Milliarde Schlüsseln pro Sekunde
Quelle: Wikipedia.org

Wie man sieht, kann ein einfaches oder schwaches Passwort innerhalb weniger Minuten bis Sekunden durch einfaches Durchprobieren herausgefunden werden.

Beispiele für ein gutes, sicheres Passwort

Ihr Passwort sollte im Idealfall aus mindestens 8 Zeichen bestehen, Groß- und Kleinschreibung sowie Zahlen und Sonderzeichen enthalten.

Weiters sollten Sie verschiedene Kennwörter auf unterschiedlichen Plattformen benutzen, und diese auch regelmäßig alle 3-6 Monate ändern. Das beste Passwort ist ein rein zufälliges Kennwort, bestehend aus allen Zeichen und Sonderzeichen, die Ihre Tastatur hergibt. Wenn es sich um wirklich wichtige Daten handelt, sollten Sie daher ein rein zufällig generiertes Wort verwenden wie z.B.

Schlecht	**Gut**	**Besser**	**Stark**	**Sehr Stark**
admin	adqob2	UkXsix5	izle42iPWO	)%V1x&9)SYe
passwort	okpuw3	iWwZuh9	OtYu51ulnO	$laC%2a8&Ha
123456	iqgij4	IxclEs8	EsMu14alYO	§HF!!YX//!=
haus	agnij1	UcZjuL2	ArMO24anwA	§§x7§za$/$K

Wie können Sie sich Ihr Passwort leicht merken?

Ein einfacher und praktikabler Trick ist mit Hilfe von Eselsbrücken zu arbeiten.

Wählen Sie einen einfach zu merkenden Satz und machen Sie daraus Ihr Kennwort. Sprichwörter wie „Der Ball ist rund und das Runde muss ins Eckige" machen Sie daraus das Kennwort DBir&dRmiE. Mischen Sie den Buchstaben noch eine oder zwei Zahlen hinzu und fertig ist Ihr sicheres Passwort.

Passwort Safes oder Passwort Container

Alternativ gibt es auch sogenannte Passwort Safe Programme, wo Sie mit Hilfe eines Masterpassworts all Ihre Passwörter hochverschlüsselt auf Ihrem PC oder Handy speichern. Wichtig dabei ist natürlich das als Masterpasswort ein gutes Sicheres Passwort verwendet wird.

Stand: 06.06.2016

Quelle:https://www.wko.at/service/innovation-technologie-digitalisierung/Passwoerter__Die_Schluessel_zu_Computer_und_Internet.html