itEXPERsT
Your Data Guard

Dipl. Ing. Christian Perst
Ger. zert. Sachverständiger, IT-Forensiker
IT-Security-Consultant

www.itEXPERsT.com

Den Hackern mit sicheren Passworten ein Schnäppchen schlagen - neue Erkenntnisse, Teil 2

Das Cyberkriminelle Passwörter hacken, um Daten und Identitäten zu stehlen, ist bekannt und wurde im letzten Teil beschrieben. Insbesondere die Passwortlänge und die Vielfalt der verwendeten Zeichen im Passwort spielen bei solchen Hackereinbrüchen eine große Rolle.

Was aber macht ein sicheres Passwort aus und wie gelange ich zu einem solchen?

Die Sicherheit eines Passwortes wird durch verschiedene Faktoren beeinflusst. Dazu zählen unter anderem:

- Länge des Passwortes
- Erstellung des Passwortes
- Zahlenraum
- Passwortverwendung
- und von größter Wichtigkeit die
- Passwortverwaltung

Die Länge des Passwortes

Unsere Computersysteme werden immer leistungsfähiger, dadurch werden Cyberattacken immer einfacher und vor allem gehen sie immer schneller vonstatten. Ungefähr alle 18 Monate verdoppelt sich die PC-Leistung. Dieser Technologiefortschritt ist die Grundlage einer neuen digitalen Wende, die bei der Erstellung eines sicheren Passwortes berücksichtigt werden muss.

Zur Sicherung eines Otto-Normalverbraucher-Accounts galt bisher die Regel, ein Kennwort von mindestens acht Zeichen zu verwenden. Hoch sensible Daten wie Firmenkonten sollten durch ein zwölf-stelliges Passwort geschützt werden. Diese Empfehlungen gehören aber der Vergangenheit an. Nunmehr gelten Passwörter mit einer Länge von mindestens zehn Zeichen bzw. 14 oder besser 16 Zeichen als sicher. Je länger ein Passwort ist, desto sicherer wird es. Wie man sich ein solches jedoch merken soll und wie es zu verwahren ist, darauf kommen wir später.

Die Erstellung eines sicheren Passwortes

Kennwörter aus dem Lexikon sind tabu! Ebenso Wörter, die einen persönlichen Bezug zu sich selber, wie beispielsweise das Geburtsdatum, der Name des Haustieres oder der Mädchenname der Ehefrau, haben. Diese sind nur allzu leicht zu erraten. Idealerweise werden für ein Passwort zufällige ausgewählte Zeichen verwendet. Um zu solch einer zufälligen Zeichenfolge zu kommen, kann man einen Satz zur Hand nehmen. Von diesem nimmt man entweder die Anfangs- oder aber auch die Endbuchstaben und fügt sie zu einem Kennwort zusammen. Leichter zu merken ist dieses Passwort, wenn der Satz für einen selbst von Bedeutung ist. Mit etwas Kreativität ersetzt man dann noch einige der Buchstaben durch Zahlen oder Sonderzeichen, wie z. B. statt „i“ eine „1“ oder statt „A“ eine „8“ oder „@“.

Als Beispiel hier ein Ausspruch von Henry Ford:

Alles kann immer noch besser gemacht werden, als es gemacht wird.

Nimmt man nun von jeden Wort den Anfangsbuchstaben, dann ergibt sich folgende Zeichenfolge: Akinbgw,aegw.

Das „eine“ können wir durch „1“ ersetzen. Wir ändern noch ein paar Zeichen, damit nicht jeder Satz mit einem Großbuchstaben beginnt und mit einem Punkt aufhört.

Das ergibt: `akINbgw,@eGW.`

Hat der Ausspruch eine Bedeutung für einen selbst, dann wäre dies ein gut zu merkendes und sicheres Passwort. Jedoch handelt es sich hier um einen sehr geläufigen Ausspruch Fords und somit ist der Satz sehr bekannt, was zum Nachteil für ein sicheres Passwort werden kann.

Zahlenraum

Wie bereits in ersten Teil erwähnt, ist es von großer Wichtigkeit, dass möglichst viele Zeichenarten für ein Passwort verwendet werden. So sollte es Groß- und Kleinbuchstaben, Zahlen und auch Sonderzeichen, falls es das System zulässt, wie `!"#$%&'()*+,-./:;<=>?[]^_{}~,` enthalten.

Ist es nun besser ein kurzes Kennwort mit möglichst vielen verschiedenen Zeichen zu verwenden? Oder eher ein längeres Passwort, welches dann aber nur aus beispielsweise Buchstaben besteht?

Ein längeres Kennwort, das nur aus einer Zeichenart besteht, ist sicherlich einfach im Gedächtnis zu behalten als ein kürzeres, das Sonderzeichen enthält.

Hier bringt ein Rechenbeispiel Klarheit. In der Tabelle wird die Anzahl der möglichen Passworte dargestellt.

Anzahl der Passworte	Nur Buchstaben	inkl. Sonderzeichen
Größe des Zahlenraums	52 (a-z,A-Z)	95 (a-z,A-Z,0-9,+ Sonderz.)
6-stelliges Passwort		735 Mrd.
8-stelliges Passwort	5345 Mrd.	
10-stelliges Passwort		5,9 * 10 E +19
12-stelliges Passwort	3,9 * 10 E +20	
14-stelliges Passwort	1,1 * 10 E +24	4,8 * 10 E +27
16-stelliges Passwort	2,8 * 10 E+27	4,4 * 10 E +31

Sicherer ist es ein Kennwort, das nur aus Groß- und Kleinbuchstaben besteht, wenn es um mindestens zwei Zeichen länger ist, als eines mit Sonderzeichen. Fast 10-mal länger braucht es, dieses zu hacken. Verwenden Sie allerdings ein gleich langes Kennwort mit Sonderzeichen, dann würde es bis zu 5000-mal länger dauern, bis dieses wiederum geknackt wird.

Passwortverwendung

Niemals sollte ein Passwort für mehrere Konten verwendet werden. Wurde ein Zugang geknackt, kann es dem Angreifer so gelingen, auch in andere Konten, die Sie verwenden, einzudringen. Verwenden Sie dasselbe Passwort gleichzeitig für Ihr E-Mail-Konto, ihr Facebook-Konto oder gar für Ihren Zugang beim Finanzamt und/oder Ihrer Bank, kann der Angreifer so leicht Ihre Identität stehlen. Das wiederum kann für Sie sowohl finanzielle als auch rechtliche Konsequenzen haben, da es recht schwierig werden kann, einen Identitätsdiebstahl zu beweisen. Folglich sollte pro Konto und Zugang nur ein Passwort verwendet werden.

Viele werden einwenden, dass man sich ja gar nicht ein eigenes Kennwort für jeden einzelnen Anbieter und jeden einzelnen Zugang merken kann. Aber das brauchen Sie auch gar nicht. Sie können ihre gesamte Passwort-Sammlung durch einen modernen Passwort-Manager verwalten.

Passwort-Manager

Wenn Sie nun sichere und viele (pro Konto eines) Kennwörter, mit einer möglichst großen Anzahl von Zeichen inklusive Sonderzeichen, verwenden wollen, dann werden Sie um eine intelligente Kennwortverwaltung nicht herum kommen. Ein Passwort-Manager ist ein kleines Programm, das all ihre Passwörter sammelt und verschlüsselt abspeichert. Wie ein Safe, wird der Passwort-Manager durch ein sogenanntes Masterpasswort geschützt. Solange der Safe nicht durch dieses Masterpasswort entsperrt wurde, sind ihre Daten vor unbekannten Zugriffen sicher. Sollte ein Angreifer dennoch Zugriff auf die verschlüsselten Daten bekommen, ist das aufgrund der Verschlüsselung nicht weiter tragisch. Entsperren Sie dann den Safe mit dem Masterpasswort, geben Sie diesen Schlüssel zur Entschlüsselung ein und ändern ihre Passwörter. Auch diese müssen Sie sich dann weder merken oder selbst erstellen. Sie brauchen nur die Länge des Kennwortes und die Zeichen, die es enthalten soll, festlegen. In wenigen Sekunden wird ein neues zufälliges Kennwort generiert.

Was also spricht nun noch gegen sichere Passwörter, die mindestens 16 Zeichen lang sind? Nichts!

Bespiele für solche Passwörter sind:

```
eef1She1Tohroomo ohR4cohro6Cai1Ok jooC9aebaVeob7ah ieQuoh5ohx0uumeH
Thi7raeNu7lea1Uh EiJashaePhariel7 seeYae8iv8aeyai5 kuiKae2iNi6mowoH
seec2eiNee0thio7 beedoh3eiLaethoo haiqueeThee6loh4 choh9Quah4ahked8
```

Mit Sonderzeichen:

```
phi2OoquaiM7oeg# dae!shou}x-ei8Ju Eemo6Eeng-ie6phi adaiWaichae6heo{
thoo6Fie)n<eichu Phae2ein0UG>ai<j ohwa"Qu5Ieheishe pae3Zie|sh7ae1Oo
ohw.oh2Riey2jo`G uthai0Ceimushie- rai6tooYa*baexei boh4Am0de#yaen8p
```

Verwenden Sie einen Passwort-Manager, müssen Sie sich nur noch ein einziges Passwort merken. Das Masterpasswort, dieses sollte allerdings sehr komplex sein und darf nicht abhandenkommen. Sie sollten sich dieses Passwort daher auf ein Blatt Papier notieren. Dieses Blatt stecken dann in einen Briefumschlag stucken und zukleben. Den Umschlag verwahren Sie dann am besten in einem Safe oder Schließfach. Das ist außerordentlich wichtig, denn verlieren oder vergessen Sie ihr Masterpasswort, haben Sie wahrlich keinerlei Möglichkeiten mehr, um an Ihre einzelnen Passwörter zu gelangen. Es sei denn Sie versuchen in Ihren eigenen Passwort-Manager einzudringen. Wenn Sie aber wirklich ein komplexes sicheres Passwort verwendet haben, wird es beim Versuchen bleiben.

Hier finden Sie Beispiele kostenloser Open-Source Passwort-Manager, deren Verwendung ich Ihnen nur empfehlen kann.

http://www.itexperst.at/wie-waehle-ich-sichere-passwoerter-3991.html#verwalten

Dipl. Ing. Christian Perst berät Unternehmen in Belangen der IT-Sicherheit. Er ist in der Hackerabwehr und als Datendetektiv tätig (IT-Penetrationstest und IT-Forensik/Datenforensik/Computerforensik). Im Bereich der IT-Forensik ist er gerichtlich beeideter Sachverständiger.

http://www.itEXPERsT.at