Der monatliche Security Awareness Newsletter für Jedermann

OUCH!

IN DIESER AUSGABE...

- **Passphrasen**
- **Sicherer Umgang mit Passphrasen**
- **Weiterführende Informationen**

Passphrasen

Hintergrund

Wir benutzen Passwörter tagtäglich, z.B. um auf unsere E-Mails zuzugreifen oder Überweisungen auf dem Smartphone zu tätigen um Waren zu bezahlen. Leider haben Passwörter sind jedoch auch Ihr größter Schwachpunkt: Wenn jemand Ihr Passwort errät oder anderweitig Kenntnis davon erlangt, kann er auf all Ihre Benutzerkonten zugreifen, das heißt er hat Zugriff auf Ihre E-Mails, kann Banktransaktionen tätigen oder Ihre digitale Identität stehlen. Die Nutzung starker Passwörter ist daher unabdingbar zum Schutz vor derartigen Gefahren.Solche starken Passwörter sind zumeist aber kompliziert, schwer zu merken und - insbesondere auf Smartphones - schwer zu tippen. Um genau diese Probleme zu vermeiden, wollen wir Ihnen in diesem Newsletter näherbringen, wie Sie starke Passwörter erstellen, die einfach zu merken und zu tippen sind - diese werden Passphrasen genannt.

Gastautor
My-Ngoc Nguyen (Aussprache Mi-Nop Wynn) ist zertifizierte SANS Trainerin und CEO/Principal Consultant von Secured IT Solutions. Ihre Kompetenz stellt Sie durch herausragende Zertifizierungen und Ihre mehr als 14 Jährige Erfahrung in der Entwicklung, Verbesserung und Durchführung von Cyber-Security-Programmen für verschiedene Branchen unter Beweis. Twitter: **@MenopN** LinkedIn: My-Ngoc “Menop” Nguyen.

Passphrasen

Wir stehen alle vor der Herausforderung, dass Cyber-Kriminelle hoch entwickelte und wirksame Methoden nutzen um Passwörter durch Brute Force (dt. rohe Gewalt) Attacken zu erraten. Hierbei werden automatisiert alle möglichen Buchstabenkonstellationen getestet um das Passwort zu erraten. Damit sind einfache oder leicht zu erratende Passwörter innerhalb von wenigen Minuten geknackt. Mit langen und komplexen Passwörtern versuchen wir uns davor zu schützen. Jedoch sind diese, wie bereits erwähnt, schwer zu merken und schwer zu tippen.Daher empfehlen wir die Nutzung von Passphrasen, also einer Abfolge von zufälligen Worten oder einen langen Satz, der sich leicht einprägen lässt. Um so mehr Wörter Ihre Passphrase hat, um so stärker ist sie. Diese Passphrasen lassen sich einfacher merken und schreiben, da sie nicht zwingend Sonderzeichen einsetzen müssen, die Komplexität kommt bei Passphrasen schon aus der Länge. Nachfolgend zwei Beispiele.

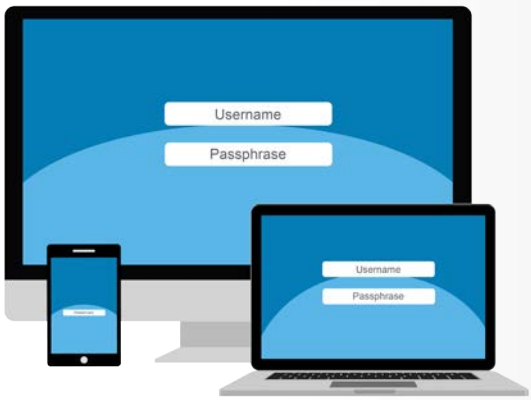
1. *Ich frühstücke um 8:30.*
2. *Xylophon-Klammer-Nähmaschine*

Diese Passphrasen sind deshalb schwer zu erraten, da sie nicht nur lang sind, sondern gleichzeitig Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen (in diesen Beispielen der Doppelpunkt und die Bindestriche) nutzen. Dies

© SANS Institute 2017

Passphrasen

fällt bei der Nutzung in einem Satz jedoch nicht schwer. Sie können die Passphrasen natürlich noch stärker machen, in dem Sie Buchstaben durch Sonderzeichen oder Zahlen ersetzen (z.B. a durch ein @ oder das i durch eine 1). Wenn eine Webseite die Passwortlänge beschränkt, dann nutzen Sie die maximale mögliche Länge.



Mit der Nutzung von Passphrasen können Sie sich starke Passwörter erstellen und besser merken.

Sicherer Umgang mit Ihren Passphrasen

Auch bei der Nutzung von Passphrasen ist Sorgfalt angebracht. Angreifer können diese vielleicht nicht mehr erraten, aber immer noch stehlen oder kopieren.

1. Nutzen Sie für jedes Benutzerkonto und Endgerät eine andere Passphrase. Nutzen Sie beispielsweise nie die Passphrasen Ihrer privaten Benutzerkonten (Facebook, Youtube oder LinkedIn) für Ihren Internet Banking Zugang oder für Ihre beruflichen Benutzerkonten. Denn geht eine Ihrer Passphrasen verloren, sind die anderen Benutzerkonten so weiterhin geschützt. Wenn Sie sich viele Passwörter merken müssen, nutzen Sie einen Passwort Manager. Diese spezielles Programm speichert Ihre Passwörter in einer gut verschlüsselten Datenbank. Sie müssen sich dann nur noch eine sehr starke Passphrase merken, die den Zugang zu Ihrem Passwort Manager schützt.
2. Teilen Sie niemanden Ihre Passphrasen oder die Methode welche Sie für die Generierung gewählt haben mit, dies beinhaltet auch Ihre Arbeitskollegen oder Vorgesetzten. Eine Passphrase ist ein Geheimnis - wenn irgendjemand davon erfährt ist es nicht mehr sicher. Wenn Sie Ihr Passwort irrtümlich mit jemandem geteilt haben, oder den Verdacht haben es sei kompromittiert oder gestohlen worden, dann ändern Sie es umgehend. Eine Ausnahme von dieser Regel wäre, wenn Sie Ihre Passphrase für den Passwort Manager an ein vertrauenswürdiges Familienmitglied weitergeben, damit er im Notfall auf die Passwörter zugreifen kann. Eine Möglichkeit, dieses wichtige Geheimnis weiterzugeben, wäre die Passphrase auf ein Stück Papier zu schreiben und an einem sicheren Ort (Safe) abzulegen. Stellen Sie dabei aber sicher, dass in diesem Passwortsafe keine beruflich genutzten Passphrasen enthalten sind.
3. Nutzen Sie keine öffentlichen Computer (z.B. Hotel, Internet Café) um sich an Ihren Benutzerkonten anzumelden. Da jeder diese Computer benutzen kann, sind diese mit hoher Wahrscheinlichkeit infiziert und erfassen Ihre Eingaben. Der Zugang auf Ihre Benutzerkonten sollte daher nur von vertrauenswürdigen Computern oder mobilen Endgeräten erfolgen.
4. Seien Sie vorsichtig bei der Eingabe von Sicherheitsfragen, welche auf Webseiten genutzt werden, falls Sie einmal Ihre Passphrase vergessen haben. Das Problem besteht meist darin, dass die Antworten auf diese Fragen meist im Internet zu finden sind, z.B. auf Ihrer Präsenz in Sozialen Medien (Facebook, Twitter). Nutzen Sie daher nur Fragen und/

© SANS Institute 2017

Passphrasen

oder Antworten die nicht öffentlich verfügbar oder die fiktiv sind. Wenn Sie sich die Fragen und Antworten nicht merken können, suchen Sie sich einfach einen Filmcharakter aus und erstellen Sie diese basierend auf dessen persönlichem Hintergrund. Ein weitere Möglichkeit wäre der bereits erwähnte Passwort Manager. Viele dieser Programme bieten eine Möglichkeit neben der Passphrase auch Sicherheitsfragen zu den Benutzerkonten zu speichern, so haben Sie alles an einem Ort. Dies macht nochmals überaus deutlich warum Sie für die Absicherung des Passwort Managers eine sehr starke Passphrase nutzen sollten.

5. Viele Online-Benutzeraccounts können mittels 2-Faktor (auch 2-Wege) Authentifizierung geschützt werden. Hier benötigen Sie neben der Passphrase auch noch einen weiteren Faktor zur Anmeldung, wie z.B. ein Einmalpasswort das per SMS an Ihr Smartphone gesendet oder in einer speziellen App (z.B. Google Authenticator) erzeugt wird. Dies bietet einen zusätzlichen Schutz und ist daher deutlich sicherer, als nur die Passphrase zu verwenden. Nutzen Sie daher immer diese Methode falls Sie Ihnen angeboten wird.
6. Der Zugriff auf Mobile Geräte ist meist über eine PIN gesichert. Sich eine PIN zu merken ist nichts anderes, als sich ein Passwort zu merken. Auch hier gilt, je länger die PIN um so sicherer ist sie. Auf vielen mobilen Endgeräten kann man aber auch Passphrasen oder biometrische Daten (z.B. Fingerabdruck) zum Entsperren verwenden.
7. Wenn Sie ein Benutzerkonto nicht mehr benötigen, schließen, löschen oder deaktivieren Sie dieses.

Weiterführende Informationen

Password Manager: https://securingthehuman.sans.org/ouch/2015#october2015
Two Step Verification: https://securingthehuman.sans.org/ouch/2015#september2015
Kampagne zur Absicherung seiner Benutzkonten (engl.): https://lockdownyourlogin.com
SANS SEC301 - 5 Tages SANS Kurs über Cyber Security Grundlagen: https://sans.org/sec301

Informieren Sie Sich

Abonnieren Sie den monatlichen OUCH! Security Awareness Newsletter, greifen Sie auf die OUCH! Archive zu und lernen Sie mehr über SANS Security Awareness Angebote unter securingthehuman.sans.org/ouch/archives.

Deutsche Ausgabe

Diese OUCH! Ausgabe wurde von Marek Kreul und René Wiedewilt aus dem Englischen übersetzt. Beide arbeiten für das CERT eines DAX-Konzerns und haben sich auf IT-Forensik spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

OUCH! wird durch das SANS Securing The Human Programm herausgegeben und unter der Creative Commons BY-NC-ND 4.0 Lizenz vertrieben. Die Erlaubnis zur Weitergabe dieses Newsletters oder Verwendung in einem Weiterbildungsprogramm wird gewährt, solange der Newsletter unverändert bleibt. Für Übersetzungen und weitere Informationen kontaktieren Sie bitte ouch@securingthehuman.org.

Redaktionsleitung: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley

© SANS Institute 2017