Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- Passphrasen
- Sichere Nutzung von Passphrasen
- Weiterführende Informationen

Starke Passwörter

Hintergrund

Wir benutzen Passwörter täglich, z.B. um auf unsere E-Mails oder Smartphones zuzugreifen und Bankgeschäfte oder Einkäufe im Internet zu tätigen. Somit sind Passwörter einer unserer Schwachpunkte, denn sobald sie jemand stiehlt hat er Zugriff auf unsere Identität, unser Geld und unsere persönlichen Informationen. Also benötigen wir starke Passwörter um uns zu schützen. In diesem Newsletter werden wir erklären, wie man starke Passwörter erstellt, welche sich leicht merken lassen. Diese Art von Passwort nennt man auch Passphrase oder Passwortsatz.

Gastautor

Guy Bruneau ist Senior Security Consultant bei IPSS Inc., SANS Ausbilder und Mitarbeiter im Internet Storm Center ISC. Er ist zertifizierter GIAC Security Expert (GSE) und hat das SANS Cyber Guardian Programm erfolgreich absolviert. Sie können Guy Bruneau unter seinem Twitteraccount **@GuyBruneau** und auf **handlers.sans.org/gbruneau folgen**.

Passphrasen

Wir müssen uns der Herausforderung stellen, dass Cyberkriminelle ausgefeilte Methoden zum Erraten von Passwörtern (auch “Brute Force” genannt) entwickelt haben, und dass sie darin immer besser werden. Ihr Passwort ist somit in Gefahr, sobald es schwach oder leicht zu erraten ist. Ein starkes Passwort ist somit ein entscheidender Schritt um sich zu schützen. Je mehr Zeichen Ihr Passwort hat, um so sicherer ist es und um so schwieriger ist es für die Angreifer, es zu erraten. Leider kann man sich lange und komplexe Passwörter schlecht merken. Deshalb empfehlen wir Ihnen, Passphrasen zu nutzen. Dabei handelt es sich um einfache, leicht zu merkende Sätze, die sich jedoch schwer erraten lassen. Ein Beispiel:

Wo ist König Julian?

Die Passphrase ist nicht nur stark, weil sie 20 Zeichen lang ist, sondern sie enthält zudem noch Großbuchstaben und Sonderzeichen (Leerzeichen und Satzzeichen). Um die Passphrase noch stärker zu machen, können Sie Buchstaben auch durch Sonderzeichen ersetzen. Zum Beispiel könnten Sie das “a” durch ein “@” ersetzen oder das “o” durch eine Null. Falls eine Webseite die Anzahl an Zeichen in einem Passwort limitiert, nutzen Sie die maximale Anzahl von Zeichen die erlaubt sind.

Starke Passwörter

Sichere Nutzung von Passphrasen

Auch mit Passphrasen sollten Sie einen sicheren Umgang pflegen. Eine noch so sichere Passphrase hilft Ihnen nicht, wenn die bösen Jungs sie einfach stehlen bzw. kopieren können.

Die Nutzung von Passphrasen zählt zu den effektivsten Schritten, um Ihre Identität und Ihre Informationen im Internet zu schützen.

1. Benutzen Sie für jeden Zugang und jedes Endgerät eine andere Passphrase. Sie sollten also niemals die Passphrase Ihres Onlinebanking Zugangs zur Anmeldung in sozialen Netzwerken wie Twitter, Facebook oder Youtube nutzen. Damit sind Ihre anderen Zugänge sicher, falls die Zugangsdaten eines einzelnen Benutzerkontos gestohlen wurden. Für den Fall, dass Sie eine hohe Anzahl von Passphrasen verwalten müssen, empfehlen wir Ihnen den Einsatz eines Passwort Managers. Dieses spezielle Programm speichert all Ihre Passwörter in verschlüsselter Form und die einzige Passphrase, die Sie sich fortan merken müssen, ist die Ihres Computers und des Passwort Managers.

2. Teilen Sie Ihre Passphrase und die Strategie der Erstellung mit niemandem, auch nicht mit Ihren Arbeitskollegen. Denken Sie immer daran, eine Passphrase ist ein Geheimnis und somit nicht mehr sicher, sobald jemand Kenntnis davon erlangt. Sollten Sie versehentlich die Passphrase mit jemandem geteilt haben oder vermuten, dass sie gestohlen wurde, ändern sie diese sofort.

3. Wie bei Passwörtern gilt auch hier, vermeiden Sie einfach zu erratende oder weitbekannte Passphrasen. Der Ausspruch “Die Renten sind sicher” ist zum Beispiel keine gute Passphrase, da sie vielen Personen bekannt ist.

4. Benutzen Sie niemals öffentlich zugängliche Computer, wie z.B. in Hotels oder Bibliotheken, für Ihre Bankgeschäfte oder um auf Ihr Firmennetz zuzugreifen. Da jeder diese Computer verwenden kann, könnten diese mit Schadcode infiziert sein, der alle Tastatureingaben protokolliert. Nutzen Sie daher für die Arbeit oder Ihre Bankgeschäfte nur vertrauenswürdige Computer oder Mobilgeräte.

5. Seien Sie achtsam auf Webseiten, die Ihnen persönliche Fragen stellen (z.B. Name des Haustiers). Diese Fragen werden genutzt, falls Sie Ihre Passphrase vergessen haben und diese zurücksetzen lassen müssen. Das Problem in

Starke Passwörter

diesem Fall ist, dass die Antworten auf diese Fragen oft im Internet oder sogar auf Ihrer Facebook-Seite auffindbar sind. Stellen Sie sicher, dass Sie als Antwort auf persönliche Fragen nur Informationen nutzen, die nicht frei verfügbar oder sogar fiktiv sind. Viele Passwort Manager helfen Ihnen dabei, indem sie diese zusätzlichen Informationen speichern.

6. Viele Online-Accounts erlauben eine Zwei-Faktor-Authentifizierung, auch bekannt als “Besitz und Wissen”. Hierfür benötigen Sie mehr als nur Ihre Passphrase um sich anzumelden, wie z.B. einen weiteren Einmalcode der auf Ihr Mobiltelefon geschickt wird. Diese Option ist viel sicherer als eine Passphrase allein, daher sollten Sie diese starke Authentifizierungsmethode wann immer möglich nutzen.

7. Mobilgeräte erfordern häufig eine PIN, um darauf zuzugreifen. Eine PIN ist im Grunde genommen nichts anderes als ein Passwort. Je länger die PIN ist, desto sicherer ist sie. Viele aktuelle Mobilgeräte erlauben auch die Nutzung von Passphrasen anstelle von PINs.

8. Zu guter Letzt: Schließen, löschen oder deaktivieren Sie Ihr Benutzerkonto, wenn Sie es nicht mehr benötigen.

Weiterführende Informationen

2-Wege Authentifizierung: http://www.securingthehuman.org/ouch/2013#august2013
Passwortverwaltung: http://www.securingthehuman.org/ouch/2013#october2013
Social Engineering: http://www.securingthehuman.org/ouch/2014#november2014
Gängige Begriffe der IT-Sicherheit:
https://www.bsi-fuer-buerger.de/BSIFB/DE/Wissenswertes_Hilfreiches/Service/Glossar/glossar_node.html

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 http://www.securingthehuman.org.

Deutsche Ausgabe

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

Redaktionsleitung: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis