Nur Hundert Klicks bis zum Hacker-Glück

Wiesbaden, 17. November 2016 – Wie vielen Versuchen muss ein Passwort standhalten? Ein Passwort, das durch ein Datenleck gestohlen und offline mit spezieller Hardware zu knacken versucht wird, muss zirka einer Milliarde Versuchen widerstehen können. Das klingt nach viel. Ein Passwort, dass durch einen herkömmlichen Online-Angriff geknackt werden soll, muss immerhin noch eine Million Versuche bewältigen. Das ist immer noch reichlich. Aber wie sieht es mit lediglich 100 Versuchen aus? Das ist die Anzahl der Fehlversuche, die die neuesten Leitlinien des National Institute for Standards and Technology (NIST) empfehlen, bevor eine Sperrung ausgelöst werden soll. Das klingt zunächst einmal sicher, denn jeder, so sollte man annehmen, kann ein Passwort erstellen, das 100 Versuchen von Hackern wiederstehen kann. Vielleicht aber auch nicht!

Laut aktueller Studien aus China und Großbritannien hat ein Angreifer mit nur einigen wenigen personenbezogenen Daten eine 1:5 Chance, ein Passwort zu erraten, bevor die vom NIST empfohlene Sperrung eintritt.

Die Forscher der Chinesischen Fujian Normal und der Peking Universität sowie der britischen Lancaster University haben mit TarGuess Bezugssysteme entwickelt, die intelligent die persönlichen Informationen einzelner Benutzer berücksichtigt, auf die auch ein Angreifer potenziell Zugriff haben könnte.

TarGuess-I beispielsweise geht davon aus, dass personenbezogene Daten, wie etwa Name und Geburtstag, bekannt sind. Den Forschern zufolge kann so eine etwa 20 Prozent höhere Erfolgsrate bei 100 Versuchen, eine 25 Prozent höhere Rate mit 1.000 Versuchen und 50 Prozent bei 1.000.000 Versuchen. Dies deutet darauf hin, dass die Mehrheit der Nutzerkennwörter äußerst anfällig für Angriffe ist.

Die vielen Millionen User, die bereits Opfer von Angriffen oder Datenlecks bei Adobe, Yahoo, LinkedIn und anderen wurden und deren persönliche Informationen nun öffentlich zugänglich sind, haben außerdem einen weiteren Verlust zu beklagen: den des "Schwester-Passworts". Diese geben auch hackern Hinweise darauf, wie die Nutzer ihre Kennwörter erstellen. Gemäß der TarGuess Bezugssysteme steigen dadurch die Chancen der Hacker zusätzlich. TarGuess-III und IV Prognosen, welche auch die Schwester-Passwörter einbeziehen, erreichen Erfolgsraten von bis zu 73 Prozent bei nur 100 Versuchen.

Mehr Vorsicht ist geboten

Michael Veith, Sicherheitsexperte bei Sophos, empfiehlt: „Website-Betreiber sollten mindestens den neuesten NIST Richtlinien folgen. Sie sollten Anwendern ein Tool zur Messung der Passwortstärke bereit stellen und keinesfalls erlauben, Passwörter wie 12345 zu verwenden. Ferner sollen sie Limits für das Einloggen definieren und den Zugriff bei Überschreitung sperren. Auch eine 2-Wege-Authentifizierung macht das Leben sicherer. Auf diese Weise können Kriminelle mit einem geknackten Passwort nicht viel anfangen. Endverbrauchern hingegen raten wir: nutzen Sie unbedingt einen Passwort-Manager. Er kreiert hervorragende Passwörter, verwahrt sie sicher und lässt sie den Anwender bei Bedarf bequem nutzen. So benötigen Hacker wesentlich mehr als nur 100 Klicks bis zum Glück.“

Weitere Statistiken und Forschngsergebnisse stehen im Sophos Naked Security Blog unter: http://bit.ly/2eCpUtU

Über Sophos
Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos' Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.
Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Christiane Capps, +49-174-3335550
Ulrike Masztalerz, +49-30-55248198
sophos@tc-communications.de