Dr. Peter Mayer
Prof. Melanie Volkamer
Anne Hennig

Change Your Password – Lieber nicht zu oft!

Hintergrundwissen zum regelmäßigen Ändern von Passwörtern anlässlich des „Change Your Password Day“ 2023

Die eigenen Passwörter regelmäßig zu ändern ist ein oft anzutreffender Ratschlag. Gerade heute am „Change Your Password Day“ ist er wieder in vieler Munde. Die Gedanken hinter diesem Ratschlag sind einfach zu verstehen: Wenn das Passwort regelmäßig geändert wird, ist es erstens schwerer zu erraten (Stichwort bewegliches Ziel) und zweitens nutzt ein Passwort, das in falsche Hände geraten ist, dem Angreifer nur bis zur nächsten Änderung. Doch die Wissenschaft zeigt uns, dass beide diese Gedanken leider Missverständnisse sind:

Missverständnis 1: Regelmäßig geänderte Passwörter sind schwieriger zu erraten
Wissenschaftler der Carlton University zeigten in 2015 mit Hilfe eines mathematischen Modells, dass regelmäßiges Ändern den Erfolg eines typischen Rateangriffes nur wenig verringert. Sie schlussfolgern, dass der immense Mehraufwand des vorsorglichen Änderns von Passwörtern für Benutzer in keinem Verhältnis zur erzielten Schutzwirkung steht.

Missverständnis 2: Passwörter sind nur bis zur Änderung nützlich
Wissenschaftler der University of North Carolina at Chapel Hill untersuchten, wie Benutzer Passwörter wählten, wenn sie diese regelmäßig ändern mussten. Sie konnten zeigen, dass Benutzer oftmals vorhersehbare Änderungen durchführen, um das nächste Passwort zu wählen. Kennt ein Angreifer also ein Passwort kann er mit großer Wahrscheinlichkeit das nächste Passwort des Benutzers auch erraten.

Glücklicherweise verbreitet sich das Wissen um diese Missverständnisse immer mehr. Mehrere staatliche Stellen wie das amerikanische NIST oder das britische NCSC passen bereits Ihre Empfehlungen an. Sie empfehlen nur ein neues Passwort zu wählen, wenn das alte in die Hände eines Angreifers gerät, anstatt es vorsorglich zu wechseln. Die Behörden empfehlen Webdiensten stattdessen eine rigorose Überwachung der eigenen Server und den Einsatz von sogenannten Lock-out-Mechanismen (z.B. die Begrenzung der Anzahl der Versuche beim Login oder zusätzliche Überprüfungen bei Logins aus Ländern, von denen aus sich der Benutzer noch nie eingeloggt hat).

Besucheranschrift:
Karlsruher Institut für Technologie
Institut AIFB
Kaiserstr. 89, Geb. 05.20
76133 Karlsruhe

Postanschrift:
Karlsruher Institut für Technologie
Institut AIFB
Postfach 6980
76049 Karlsruhe

Karlsruher Institut für Technologie

Einfach eines ihrer Passwörter blindlings zu ändern ist zwar nicht zielführend, dennoch können Sie den „Change Your Password Day“ nutzen, um die Sicherheit Ihrer Passwörter zu verbessern!

- Installieren und beginnen Sie die Nutzung eines Passwortmanagers. Dieser kann für jedes Ihrer Benutzerkonten ein individuelles Passwort zufällig erstellen. Da der Passwortmanager es sich für Sie „merkt“, müssen Sie sich auch ums Vergessen keine Gedanken machen.

- Aktivieren Sie Zwei-Faktor-Authentifizierung für besonders wichtige Benutzerkonten (z.B. primärer E-Mail-Account). Eine Übersicht, welche Webseiten Zwei-Faktor-Authentifizierung unterstützen, finden Sie unter: https://2fa.directory/ (Englisch)

- Nehmen Sie sich die Zeit, tiefgehendere Informationen zu Passwörtern zu lesen: https://secuso.org/passwortsicherheit

- Nutzen Sie unsere Schulungsunterlagen zum Thema Passwortsicherheit, um mehr über das Vorgehen von Hacker:innen zu erfahren und, welche weiteren Missverständnisse es zum Thema Passwortsicherheit gibt: https://secuso.aifb.kit.edu/downloads/Schulungen/Modul_Passwortsicherheit.pdf

- Wie gut kennen Sie sich beim Schutz von Benutzerkonten aus? Machen Sie den Test und starten Sie unser Quiz: https://www.soscisurvey.de/pwd-fragebogen/?q=quiz