Empfehlungen zum Umgang mit Passwörtern

Die Frage des Umgangs mit Passwörtern ist auch aber keinesfalls ausschließlich eine technische Frage zu Länge und Komplexität von Passwörtern.

Insbesondere ist der Umgang mit Passwörtern eine Frage der so genannten „user awareness“. Erkennt der Benutzer den Wert der Dienste und Daten die über Benutzerkennung und Passwort geschützt sind, so wird er aus Eigeninteresse eher dazu bereit sein, sinnvolle und sichere Passwörter auszuwählen. Neben der auf der Web-Seite „Passwort ändern“ wiedergegebenen Richtlinie zur Bildung von Passwörtern finden Sie nachfolgend eine Reihe von Hinweisen und Anregungen zu möglichen Methoden der Passwortauswahl, wie sie auch an anderen Stellen (u.a. BSI) in ähnlicher Form veröffentlicht sind. Folgende Aspekte sollten seitens der DV-Koordinatoren gegenüber den Benutzern betont werden und können auch allgemein als Denkanstöße verstanden werden.

- Menschen neigen dazu, sich an Mustern zu orientieren. Ähnliche Dienste/Webseiten werden dazu führen, dass Benutzer Passwörter für ähnliche Angebote wiederverwenden, wenn der Benutzer das Passwort eher als ein Hindernis denn als Schutz seiner Daten und Identität auffasst. Ausnahmen – so zeigen auch Untersuchungen - werden dann gemacht, wenn der Benutzer in einem Angebot einen für ihn besonderen Wert erkannt hat bzw. die Kompromittierung für den Benutzer einen besonderen Schaden bedeutet. (Es ist anzunehmen, dass Benutzer sich die Login-Daten Ihres Online-Bankings merken können, weil das Bankkonto einen besonderen Wert für den Benutzer darstellt.)
- Es ist menschlich, dass Benutzer sich insbesondere dann an der minimalen Passwortlänge orientieren, wenn das Passwort eher als Hindernis denn als Schutz wahrgenommen wird. In diesem Sinne sollten wir daher die Verwendung längerer Passwörter stärker bewerben.
- Je länger ein Passwort ist, desto stärker schützt es vor „brute force“ Angriffen bei denen Passwörter systematisch automatisch ausprobiert werden. Es ist daher wichtig, dass insbesondere ins Internet angebotene Systeme so konfiguriert sind, dass sie „brute force“ Angriffen entgegenwirken (z.B. durch eine Maximalzahl erfolgloser Versuche oder die Verlangsamung der erneuten Eingabe nach wiederholt erfolglosen Versuchen). Da nicht jedes System derartige Konfigurationen unterstützt und aufgrund der Dezentralität und Heterogenität der IT-Angebote wird hier ein gleichmäßig hohes Niveau nur schwer umsetzbar sein. Desto wichtiger ist es daher, unsere Benutzer von einer Präferenz für längere Passwörter zu überzeugen.
- Da nicht immer für jeden abschätzbar ist, wie gut ein Passwort wirklich ist, sollte man sich nicht an dem vom System vorgegebenen maximalen Gültigkeitszeitraum halten und daher nach Möglichkeit Passwörter früher als vom System vorgegeben wechseln.
- Die sicherste Methode zum Aufbewahren von Passwörtern ist und bleibt es, sich die Passwörter zu merken. Wenn nicht schon unsere Benutzer durch den Einsatz von verschiedensten Systemen/Webseiten/Geräten etc. sich eine Vielzahl von Passwörtern merken müssen, so werden sich insbesondere IT-Administratoren eine größere Anzahl an Passwörtern merken müssen. Gut, wenn mehr als zwei Administratoren alle relevanten Passwörter kennen und vom

diesen stets mindestens zwei Administratoren zugegen sind. Das Vergessen wichtiger Systempasswörter kann den gesamten Betrieb von IT-Systemen gefährden. Nicht nur können Arbeiten und Zugriffe nicht mehr stattfinden, sondern es sind fast immer auch Dienstunterbrechungen notwendig, um – sofern möglich – Passwörter neu zu setzen. Deshalb will eine sinnvolle „Speicherstrategie von Passwörtern“ sowohl bei Benutzern als auch Administratoren von IT-Systemen gut überlegt sein. Das Risiko von untergegangenen Passwörtern muss insbesondere in Abhängigkeit von der Anzahl der erforderlichen Passwörter und deren Wachstumsrate, ihrer nötigen Komplexität und Länge, der Frequenz angestrebter Wechselrhythmen, der Wichtigkeit insbesondere in Punkto Anzahl von Nutzern und Systemen, der Möglichkeit und Aufwand des neu setzen können von Passwörtern untersucht werden.
- Um dem Nutzer die Notwendigkeit sicherer Passwörter besser zu veranschaulichen, können Passwortchecker verwendet werden, die die Qualität eines Passwortes nicht in den Kategorien gut-mittel-schlecht bewerten. Beispielseiten für solche Passwortchecker sind https://howsecureismypassword.net oder https://blog.kaspersky.de/password-check/ bzw. https://password.kaspersky.com/de/. Beiden Seiten bewerten ein eingegebenes Passwort in der Einheit [Zeit], so dass es dem Anwender besser möglich ist, die Qualität des Passwortes in Relation zu setzen. Grundsätzlich wird die Bewertung von Passwörtern anhand von Beispielen, mit denen Benutzer ohne umfassende IT-Erfahrung inhaltlich umgehen können, als sinnvoller angesehen als insbesondere die Bewertung der „Passwortsicherheit“ anhand von Schlüssellängen in Bits oder oberflächlichen Bewertungen ohne Bezugssystem (schwach, mittel, stark).

Denkbare und unter der vorgenannten Abwägung zu betrachtende Speichermöglichkeiten sind insbesondere

- Aufschreiben von Passwörtern und versiegelte Ablage in einem Tresor, ggf. zusätzliches Auftrennen von Passwörtern und Ablage an zwei verschiedenen Orten.
- Einsatz von Software: Passwort-Manager können bei geeigneter Auswahl und richtigem Einsatz in der o.a. Bewertung als geeignet erscheinen.

Beim Einsatz von eigenständigen Programmen als Passwort-Safe bzw. verschlüsselnden Passwort-Managern soll beachtet werden, dass

- wenige, besonders bedeutsame Passwörter nicht dort gespeichert werden dürfen und weiterhin gemerkt werden müssen (z.B. „Finanzdaten“ wie Bankkonten-Login, SAP-Zugang von anderen “Logins“ trennen.)
- das Passwort zum Passwort-Manager muss zur Gruppe der besonders bedeutsamen Passwörter gehören. Es muss durch seine Länge und Komplexität „brute-force-Angriffen“ voraussichtlich länger standhalten als der für andere Passwörter im Passwort-Manager definierte Wechselrhythmus.
- aufgrund des Passwortmanagers für jeden dort gespeicherten Login ein eigenes Passwort verwendet wird und kein Passwort-Recycling stattfindet.
- alle im Passwort Manager gespeicherten Logins bei Abhandenkommen keinen großen Schaden anrichten und einfach neu zu beschaffen sind.
- in den Fällen bei denen eine E-Mail zum Passwort-Recovery bei einem Dienst hinterlegt ist und das Passwort zu diesem Dienst im Passwort-Manager hinterlegt ist, besondere Maßnahmen zum Schutz der Identität notwendig sind. In diesen Fällen darf dann das E-Mail-Passwort zur hinterlegten E-Mail Adresse nicht im Passwort-Manager gespeichert werden. Dieses E-Mail

Passwort muss ebenfalls zu den wenigen besonders bedeutsamen Passwörtern gehören und gemerkt werden. Hintergrund ist, dass bei Offenlegung des Inhaltes des Passwort-Managers die Angreifer den berechtigten Benutzer aussperren werden, wenn die kompromittierten Kennungen für weiteren Missbrauch verwendet werden.

- Ein möglicher Passwortmanager ist das Produkt KeePass http://keepass.info/
- Das Produkt zeichnet sich nicht nur dadurch aus, dass es kostenfrei verfügbar ist und u.a. durch eine große Anzahl an Portierungen für unterschiedliche Plattformen aus, wobei allerdings eine belastbare Bewertung von Qualität und Sicherheit des Originals und seiner Portierungen nicht möglich ist.
- Produkte, die cloud-basiert Passwörter managen, sind aufgrund der Speicher- und Datenschutzproblematik trotz der scheinbar einfachen Verwendung definitiv nicht zu empfehlen. Hierzu gehört auch die Option „XXXXX“ bei deren Verwendung alle Zugangsdaten bei Google und damit im Zugriff von Google und Geheimdiensten sind.

Wenn es doch eine „Cloud-Lösung“ sein muss, dann ist der Cloud-Storage der TU Clausthal ganz sicher die bessere Lösung (z.B. um dies mit keepass zu kombinieren).

Passwörter im Browser

In fast allen Web-Browsern (Firefox, Internet-Explorer, Chrome etc.) gibt es Funktionen zum automatischen Speichern von Eingaben in Formularfeldern. Es ist zumeist auch möglich, Eingaben in Passwort-Feldern zu speichern. Zwar werden die Eingaben in Passwort-Feldern maskiert, jedoch ist es selbst für weniger geübte Personen einfach möglich, die Eingaben im Klartext sichtbar zu machen.

Die meisten Browser (Firefox, Chrome, IE, Opera) bieten entweder von Haus aus oder über ein in wenigen Augenblicken lokal installierbares Add-On die Möglichkeit an, gespeicherte Formulardaten in Passwort-Feldern innerhalb weniger Sekunden ohne besondere Vorkenntnisse auszulesen.

Es wird empfohlen, Funktionen zum automatischen Speichern von Formulardaten nur selektiv und das Speichern von Eingaben in Passwort-Feldern nicht zu benutzen.