Passwörter Verwalten

Passwort tipps

Zusammenfassung:

Der Text gibt Tipps für sichere Passwörter und Schutzmaßnahmen vor Passwortmissbrauch. Es empfiehlt die Verwendung von komplexen Passwörtern, die aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Die Methode des "Passwort-Merksatzes" wird vorgestellt, bei der ein Satz als Passwort verwendet oder daraus abgeleitet wird.

Es wird betont, einfache Passwörter wie Wörter, Namen oder Geburtsdaten zu vermeiden. Für Dienste sollten individuelle Passwörter genutzt werden. Ein Passwortmanager wird als Lösung für das Merken mehrerer Passwörter empfohlen.

Passwortfallen wie das Ersetzen von Buchstaben durch Zahlen sollten vermieden werden. Zwei-Faktor-Authentifizierung wird als zusätzlicher Schutz vorgeschlagen.

Der Text warnt vor Passwortmissbrauch und gibt Tipps zur Vermeidung von unberechtigtem Zugang, darunter das Erraten von Passwörtern, Brute-Force-Angriffe und Phishing. Schutzmaßnahmen wie persönliche Informationen schützen, Firewalls nutzen und Geräte aktualisieren werden empfohlen.

Schließlich werden fünf Schutzmaßnahmen für den sicheren Umgang mit Passwörtern aufgeführt, darunter die Verschlüsselung sensibler Inhalte und das sichere Löschen von Informationen. Der Text schließt mit Verweisen auf weiterführende Informationen zu Datenschutz und Internetverhalten.

Ist Situation

Ich habe meine Passwörter auf einem Blatt Papier stehen zu Hause. Daher das ich aber ein Password habe und dies immer bisschen Abändere kann ich mir diese auch sehr gut merken. Mein Password enthält zahlen, Buchstaben und Sonderzeichen. Trotzdem denke ich das dies nicht die beste Lösung ist, da sobald man ein Password gehackt hat kann man die anderen auch herausfinden. Ich bin schon dran an dem seit dem ich mich besser mit Datenschutz auskenne auch andere Passörter zu benutzen.

Aufgabe Ist-Situation beurteilen

Ich denke das es nicht so sicher ist, da sobald man das Password für den Laptop hat man alles Passwörter von irgendwelchen Webseiten hat. Ich mache dies Selber, da ich zwar nicht denke das mich jemand hackt aber trotzdem weiss ich das dies nicht so sicher ist. Ausserdem denke ich das wen die Webseiten gehackt werden das sie die Passwörter auch herausfinden können.

Artikel:

Der Artikel warnt vor dem Speichern von Passwörtern im Browser aufgrund von Sicherheitsrisiken bei Hackerangriffen oder Diebstahl. Es wird empfohlen, die Autofill-Funktion zu deaktivieren und

stattdessen einen Passwortmanager zu verwenden. Dieser verschlüsselt und sichert Zugangsdaten, wodurch das Risiko von Password-Stealern minimiert wird.

Es wird darauf hingewiesen, dass verschiedene Webbrowser unterschiedliche Standards in Bezug auf Privatsphäre haben. Mozilla Firefox und Safari werden als sicherere Optionen mit eigenen Sicherheitsfunktionen für Passwörter genannt.

Link

Das Speichern von Passwörtern im Browser ist bequem, aber riskant. Schadprogramme können die Kennwörter auslesen, und ohne ausreichenden Schutz kann jeder, der Zugriff auf den Computer hat, auf gespeicherte Zugangsdaten zugreifen. In Firefox können Anmeldedaten leicht angezeigt werden, es sei denn, ein Master-Passwort ist festgelegt.

Aufgabe Passwortmanager

Ich habe mich für SecureSafe entschieden, da ich diesen Passwortmanager noch nicht kenne. SecureSafe läuft auf den Betriebssystemen Windows, Android, MacOS und iOS. Bei SecureSafe gibt es keinen Quellcode ist somit nicht Open Source. SecureSafe implementiert Schutzmassnahmen gegen Brute-Force-Angriffe, um das systematische Durchprobieren aller möglichen Passwörter zu verhindern. Der Schutz gegen Brute-Force-Angriffe wird mit PBKDF2, dies macht das Programm gegen Angriffe Widerstandsfähiger. Zu dem Keylogger Schutz steht zwar nichts, aber ich habe ChatGPT gefragt und der hat geschrieben «SecureSafe verfügt über Schutzmassnahmen gegen Keylogger-Angriffe, bei denen die Aufzeichnung von Tastatureingaben verhindert wird.». Ich denke die Zwischenablage ist durch das Automatische Löschen geschützt, dies kann man einstellen, um zu verhindern das sie jemand anders lesen kann. SecureSafe schliesst sich auch nach einer Zeit selbst, dies kann man auch selber einstellen. SecureSafe braucht für die Authentifizierung Benutzername, Passwort und mTAN (kostenpflichtig). mTAN bedeutet das es einen zusätzlichen Schutz bietet. Da sind manche schon sicherer als dieser Passwortmanager, da sie noch SMS-Bestätigungen haben usw. Mit SecureSafe kann man auch seine eigenen Passwörter generieren, die dann wahrscheinlich sehr sicher sind. Die Passwörter von SecureSafe werden in einer Cloud gespeichert, die wie ich das CH interpretiere in der Schweiz ist. SecureSafe verschlüsselt ihr Datenbank mit AES256. AES256 bedeutet das es ein Symmetrischer Verschlüsselungsalgorithmus ist. Bei SecureSafe braucht man einen Wiederherstellungscode um sein Password wieder herzustellen. Ich habe leider keine Informationen über Synchonisation gefunden. SecureSafe transportiert ihre Passwörter mit CSV. CSV macht das die Passwörter in einem kommagetrennten Format gespeichert werden, somit kann man sie importieren und exportieren.

Webseite Passwort sichern

Browser-Passwortmanager sind in der Regel auf verschiedenen Betriebssystemen verfügbar, darunter Windows, MacOS, iOS, Linux und Android. Die genaue Verfügbarkeit kann je nach Browser variieren. Die meisten gängigen Browser wie Chrome, Firefox, Safari und Edge sind proprietär, was bedeutet, dass der Quellcode nicht öffentlich verfügbar ist. Browser implementieren oft Massnahmen gegen Brute-Force-Angriffe, indem sie die Anzahl der Versuche begrenzen oder Verzögerungen zwischen den Versuchen einführen. Die meisten Browser schützen sich gegen Keylogger-Angriffe auf Systemebene, jedoch bieten sie möglicherweise keine spezifischen Schutzmassnahmen für den Passwortmanager auf Browser-Ebene. Browser-Passwortmanager bieten normalerweise keinen speziellen Schutz für die Zwischenablage. Es liegt in der Verantwortung des Betriebssystems und der Benutzer, sicherzustellen, dass die Zwischenablage sicher ist. Browser haben oft keine automatische Sperre für den Passwortmanager. Die Sicherheit hängt oft von den Einstellungen des Betriebssystems

und der Browsersicherheit ab. Die Authentifizierung erfolgt normalerweise durch das Master-Passwort des Benutzers oder durch die Anmeldung am Betriebssystem, manchmal braucht es dies aber auch nicht, denn dann klickt man einfach das man das gesicherte Password jetzt abrufen möchte. Die meisten modernen Browser bieten eine automatische Passwortgenerierungsfunktion für die Erstellung sicherer Passwörter. Die Passwortdatenbank des Browsers wird normalerweise lokal auf dem Gerät gespeichert. In der Regel wird eine starke Verschlüsselung verwendet für die Browser. Browser bieten oft Mechanismen zur Wiederherstellung von Passwörtern, normalerweise durch Authentifizierung über andere gespeicherte Informationen oder über das Betriebssystem. Moderne Browser bieten oft Synchronisationsfunktionen, mit denen Passwörter über verschiedene Geräte hinweg synchronisiert werden können. Browser ermöglichen normalerweise den Export von Passwörtern, häufig im CSV- oder XML-Format, um sie in anderen Passwortmanagern zu verwenden.

Aufgabe Passwortmanager anwenden

Ich habe mich für Enpass entschieden da ich diesen noch nicht kenne. Ich habe mich auch für diesen entschieden da er Übersichtlichkeit und Flexibel sein soll.

Zuerst muss ich mir ein Konto machen. Dann Stellen ich sicher, dass die Sicherheitsfunktionen, Synchronisationsoptionen und andere relevante Einstellungen nach meinem bedarf sind. Dann beginne ich mit dem Hinzufügen einer meiner Passwörter und es wird gespeichert. Der Password Manager kann auch selbst Passwörter generieren. Dann habe ich dies mit meinem Handy verbunden, in dem ich mich mit dem gleichen Konto angemeldet habe und es hat funktioniert.

Ich erkenne den Nutzen in dem ich meine Passwörter nicht mehr irgendwie zu Hause rumliegen habe sondern auf einer App die ich immer bei mir habe und auch sicher sein kann das sie niemand anders kennt. Ausserdem muss ich mir meine Passwörter nicht immer merken und kann dadurch auch sehr starke Passwörter benutzen.

Aufgabe Soll-Situation

Ich möchte den Passwort Manager anfangen zu benutzen da er für mich sehr Benutzer freundlich aussieht und mir daher auch recht gut gefällt. Mir gefällt es ausserdem das ich mir meine Passwörter dadurch nicht mehr merken müsste, also möchte ich anfanden den Password Manager zu benutzen. Ich fange an auch meine zukünftigen Passwörter in den Password Manager zu schreiben und auch die Funktion zu benutzen Passwörter generieren zu lassen zu benutzen.