Passwörter

Wovor schützen gute Passwörter ? Und wovor nicht ?

Prinzipiell sind gute Passwörter natürlich unvermeidbar. Was ein gutes Passwort ist, behandeln wir weiter unten. Es soll aber schon darauf hingewiesen sein: Passwörter hindern Behörden fast nie davor, in ungesicherte Social-Media Accounts wie Instagram, Twitter, Reddit, Tiktok und so weiter, hinein zu kommen. Dafür reicht ihnen ein richterlicher Beschluss, denn dort liegen eure Daten unverschlüsselt und deshalb brauchen sie dafür euer Passwort nicht.

Generell gilt

- Passwörter nicht wiederverwenden
- Starke Passwörter verwenden
- Einen Passwort Manager benutzen
- 2-Faktor-Authentifizierung

Passwortmanager

Ein Passwortmanager speichert alle Passwörter in einer, mit einem Hauptpasswort, verschlüsselten Datenbank. Dadurch liegen eure Passwörter nicht einfach in Klartext auf eurem System und ihr müsst sie euch nicht alle selbst merken.

Da ihr euch Passwörter nicht mehr selbst merken müsst, ist es kein Problem und auch empfohlen, dass ihr für jeden Account ein eigenes, starkes Passwort generiert, was mit dem Passwortmanager selbst sehr einfach zu machen ist.

Der Passwortmanager speichert dann auch die Zuordnung zu Webseiten & Apps, für die ihr das jeweilige Passwort generiert habt. Das erschwert so auch Phishing, weil das Passwort auf einer falschen URL nicht als Vorschlag angezeigt wird.

Wie oben schon erwähnt ist der Passwortmanager selbst durch ein starkes Hauptpasswort, und/oder andere Faktoren geschützt (s. unten 2-Faktor-Authentifizierung). Dies ist damit das einzige Passwort, das ihr euch wirklich merken müsst und kann dementsprechend auch etwas

komplexer sein, denn es gilt: lieber ein starkes Passwort merken, als viele unsichere (und wahrscheinlich sehr ähnliche) Passwörter.

Starke Passwörter

Okay, aber zumindest ein starkes Passwort für den Passwortmanager braucht ihr ja trotzdem...

Tip

Wie du ein starkes Passwort mithilfe von Diceware einfach erstellen kannst erklären wir dir übrigens hier.

Wann ist ein Passwort denn stark? Eine Wichtige Grundvoraussetzung ist, dass das Passwort zufällig generiert ist. Alles was du dir ausdenkst, egal wie clever dein System sein mag, ist als unsicher zu betrachten. Deine Passwörter sollten also zufällig generiert sein. Eine Möglichkeit dazu ist ein Passwortmanager, eine weitere ist Diceware zeigen wir weiter unten.

Um zu klären wie ein sicheres Passwort aussehen muss, wenn es zufällig generiert wurde, schauen wir uns an wie lange es dauert ein Passwort zu cracken.

Zeit zum cracken eines Passworts

Tatsächlich kommt es sehr auf die genauen Umstände an. Die Berechnungen hier nehmen ein konkretes Szenario an. Das hier gezeigte Szenario geht von relativ guten Konditionen für die Angreifer aus. Das heißt, in der Praxis dauert es eher noch länger.

Technische Details

Wir gehen von einem MD5 gehashten Passwort aus und davon, dass die Angreifer die Hardware zur Verfügung haben die für das Training von ChatGPT verwendet wurde: 10000 NVIDIA A100 GPUs.

Kaufpreis: ca. 9000€ pro Stück für die günstigere Variante mit 40GB Speicher. Insgesamt also 90 Mio. Euro. Auch zur Miete ist diese Masse an Hardware auf Dauer nicht günstiger. Weitere details zum Szenario gibt es bei hive-systems welche die Berechnungen durchgeführt haben.

Zudem ist bei den Zeiten zu bedenken, dass diese für *ein* Passwort von *einer* Person sind. Die komplette Hardware ist damit beschäftigt, es kann währenddessen kein anderes Passwort gecrackt werden.

Wichtige Voraussetzung: Das Passwort muss zufällig generiert worden sein! Das heißt hier geht es um reines Character-Bruteforcing, also ohne auf die Zielperson optimierte Wortlisten.

a table shows the amount of time to password-cracking, according to above described scenario

Zeit zum cracken einer Passphrase

Ein zufälliges, ausreichend langes Passwort aus Buchstaben, Zahlen und Sonderzeichen ist jedoch für Menschen schwer zu merken. Deshalb empfehlen wir für die Passwörter die ihr euch merken müsst, beispielsweise das für für den Passwortmanager, Passphrasen zu verwenden. Diese bestehen aus Wörtern statt aus einzelnen Buchstaben. Damit können Menschen deutlich besser umgehen, sie sind aber nicht weniger sicher Passwörter. Siehe auch: xkcd 936

Technische Details

In der Informationstheorie muss zur Bewertung der Sicherheit immer angenommen werden, dass der Angreifer weiß nach welchem Verfahren wir das Passwort gebildet haben. Daher verwendet der Angreifer hier eine Wordlist-Attack. Ansonsten bleibt alles gleich.

Diceware: Das Erstellen zufälliger Passphrasen kann, wie schon erwähnt, mit Passwortmanagern geschehen, oder ganz analog mit Würfeln und einer möglichst großen Wortliste.

Info

Die Passphrase muss zufällig generiert worden sein. Beispielsweise mit Würfeln und Wortliste (Diceware), oder der jeweiligen Funktion des Passwortmanagers.

a table shows the amount of time to passphrase-cracking, according to above described scenario

2-Faktor Authentifizierung

2FA sorgt dafür, dass das bloße eingeben eines Passworts, nicht als vollständige Autorisierung genügt, da davon ausgegangen wird, das Passwörter eventuell korrumpiert sind. Deshalb wird eine zweite Instanz zur vollständigen Autorisierung angefordert. Das kann auf verschiedenen Kategorien beruhen:

- Wissen: Der alte Klassiker in Form eines Passworts oder Sicherheitsfragen wie "Wie lautet ihr Geburtsort?"
- Besitz: Ihr benötigt ein spezielles Ding, dass euch entweder eine Nummer anzeigt, oder was per USB in den Rechner gesteckt werden muss. Besitzt der/die Angreifer*in dieses "Ding" nicht, erfolgt auch keine Autorisierung. (Hardware-Token, *2FA-Apps*, *SMS*)
- Sein: Einzigartige biometrische Eigenschaften müssen verifiziert werden. (Biometrie)

Im Folgenden werden verschiedene Technologien aufgelistet, die für 2-Faktor Authentifizierung (2FA), aber auch als einfache 1-Faktor-Authentifizierung, genutzt werden können:

- Hardware-Token mit USB: Sie sehen aus wie normale USB-Sicks. Soll ein damit konfigurierter Service/Festplatte o.ä. entsperrt werden, muss auch dieser Stick in das genutzte Gerät gesteckt werden. Oftmals sind diese Token wiederum mit einem PIN geschützt, sodass es nicht reicht diesen zu klauen. Die PIN-Eingabe ist dabei oftmals auf x versuche limitiert. Da dies alles auf Hardware-Ebene umgesetzt und geschützt wird, ist es eine relativ sichere Möglichkeit der Authentifizierung. Der relevante Standards für Securitytoken dieser Art heißt FIDO2, der alte Standard U2F.
- Hardware-Token mit Screen: Diese USB-Stick großen Geräte haben einen kleinen Bildschirm, auf ein x-stelliger Code angezeigt wird (meist 4-6 stellig). Sie können mit bestimmten services verknüpft werden. Diese Services verlangen dann bei jeder Anmeldung (neben dem Passwort) auch den code, der gerade in diesem Moment auf dem Token angezeigt wird. Die Standard für Token dieser Art sind nicht Open-Source, weshalb wir dazu raten diese nicht zu verwenden.
- TOTP (2FA) Apps: Diese Apps können ebenfalls mit verschiedenen Services verknüpft werden und generieren dann für jeden Service jeweils alternierende Security-Codes.
- Biometrie: Schon lange berühmt in Hollywood. Soll der entsprechende Service entsperrt werden, fordert er eine Biometrische Verifizierung der Nutzenden (Fingerabdruck, Gesichtserkennung, Iris-Scan, Handabdruck, Stimmerkennung etc)
- SMS: Die wohl bekannteste Methode sind 2FA SMS. Zur Verifizierung der Identität der Nutzenden sendet der jeweilige Service eine SMS an die mit dem Account registrierte Telefonnummer. Da das Mobilfunknetz nicht als sicher zu betrachten ist, raten wir hiervon ab.

Biometrie

Biometrie wie Fingerabdrücke oder Gesichtserkennung sind nachweislich fälschbar. Wie einfach das geht hat Starbug vom CCC, bereits für Fingerabdruck-, Gesichts-, Iris- und Venenerkennung gezeigt.

Abgesehen davon können Behörden oder Cops euch zwingen Dinge mit Biometrie zu entsperren. Zur Herausgabe von Passwörtern dürfen sie das nicht.

Der wichtigste Punkt hierbei ist aber wohl, das ihr eure biometrischen Merkmal nie wieder ändern könnt. Ein korrumpiertes Passwort kann zurück gesetzt werden. Ein Fingerabdruck, oder das Gesicht jedoch nicht.

Fazit
Daher bietet Authentifizierung mit Biometrie keinen guten Schutz gegen Sicherheitsbehörden.

Version #2
Erstellt: 14 Januar 2025 18:53:30 von ESC-IT Migration Bot
Zuletzt aktualisiert: 15 Januar 2025 12:22:07 von ESC-IT Migration Bot