Engineer

Passwort

✳ Geheime Zeichenfolge zum Nachweis der anmeldenden Person

Was es ist

Ein Passwort ist eine Zeichenfolge, die eine Person im Gedächtnis oder in einem Passwortmanager aufbewahrt und vorlegt, um zu zeigen, dass ihr ein Konto gehört. Die Definitionen im NIST-Glossar stimmen im Kern überein: Buchstaben, Zahlen und andere Zeichen, die „zur Authentifizierung einer Identität oder zur Prüfung einer Zugriffsberechtigung verwendet werden“, in manchen Dokumenten auch zur Ableitung kryptografischer Schlüssel. Die aktuelle Richtlinie zur digitalen Identität, SP 800-63-4, nennt es den Faktor „etwas, das man weiß“. Sie merkt an, dass ihre erste Fassung dafür den Begriff „auswendig gelerntes Geheimnis“ (memorized secret) verwendete. Eine Passphrase aus einer Folge von Wörtern und eine ausschließlich aus Dezimalziffern bestehende PIN sind im weiteren Sinn ebenfalls Passwörter.

Dieselbe Zeichenfolge kann zwei Aufgaben erfüllen, die ähnlich wirken. Ein Anmeldepasswort wird an eine prüfende Stelle gesendet. Diese hält genug Informationen vor, um es zu erkennen, sollte aber niemals das Passwort selbst speichern. Ein Passwort zum lokalen Entsperren bleibt auf dem Gerät. SP 800-63B nennt diese Art Aktivierungsgeheimnis. Das übliche Beispiel ist die Entsperr-PIN eines Mehrfaktor-Authentifikators: Sie wird auf dem Gerät verwendet, um auf das dort im Authentifikator gespeicherte Geheimnis zuzugreifen.

Die Schwierigkeit ist, dass ein Passwort ein gemeinsames Geheimnis ist. Der Nutzer kennt es, der Dienst muss es erkennen, und jeder, der es erfährt, kann es genauso verwenden wie der Nutzer. Nichts in der Zeichenfolge bindet sie an die Website, die danach gefragt hat. Deshalb sagt SP 800-63B ausdrücklich, dass Passwörter nicht phishingresistent sind. Der Großteil der technischen Arbeit an Passwörtern zielt darauf ab, die Folgen dieses geteilten Wissens zu begrenzen, wenn es nach außen gelangt.

Das Konzept für eine Entscheidung nutzen

Nutzen Sie „Was ist ein Passwort?“ für eine konkrete Entscheidung. Wir können helfen, das Konzept mit dem System in Verbindung zu bringen, das Sie entwickeln oder einkaufen. Konten, Passwörter und Berechtigungen werden so geordnet, dass alle genau den beruflich erforderlichen Zugriff haben und ihn am Tag ihres Ausscheidens verlieren.

Unsere Leistungen entdecken Kontakt aufnehmen →

Die Annahmen hinter dem Begriff prüfen

Nutzen Sie die Erklärung und die verlinkten Arbeiten, um Fragen für Ihr Projekt zu formulieren. Wir können die Annahmen gemeinsam mit Ihnen prüfen, bevor ein Werkzeug ausgewählt wird. 1.000 RBAC-Regeln für sichere Linux-Server — 1,000 Zugriffsregeln zum Schließen einer Sicherheitslücke

1.000 RBAC-Regeln für sichere Linux-Server Kontakt aufnehmen →

Warum es wichtig ist

Ein Passwort ist oft der einzige Schutz eines Kontos. Zwei Arten des Ratens sind wichtig. Unterschiedliche Maßnahmen bremsen sie jeweils.

Online-Raten bedeutet, Passwörter am echten Anmeldeformular auszuprobieren. Dort gibt der Dienst das Tempo vor. SP 800-63B begrenzt aufeinanderfolgende Fehlversuche mit einem Authentifikator an einem Konto auf 100. Neue Passwörter müssen außerdem mit einer Sperrliste häufiger, erwartbarer und aus Datenlecks bekannter Werte abgeglichen werden. Kandidaten, die ein Angreifer zuerst ausprobieren würde, werden dadurch gar nicht akzeptiert.

Offline-Raten beginnt, sobald eine Kopie der gespeicherten Passwortdaten nach außen gelangt ist. Es gibt kein Formular und keine Begrenzung. Die Richtlinie weist darauf hin, dass Angreifer offline viele Milliarden Hashes pro Sekunde berechnen können. Passwörter, die dem standhalten sollen, müssen „um Größenordnungen komplexer“ sein als solche, die nur einem Anmeldeformular gegenüberstehen. Deshalb entscheidet die Speicherung über das Ergebnis. SP 800-63B verlangt, Passwörter mit einem Salt und einem Passwort-Hashverfahren zu hashen. Es nimmt Passwort, Salt und Kostenfaktor entgegen und soll jeden Rateversuch teuer machen. Der Salt-Wert muss mindestens 32 Bit lang und so gewählt sein, dass Salt-Werte nur selten kollidieren. Dadurch teilen sich zwei Konten mit demselben Passwort keinen gespeicherten Hash. Der Kostenfaktor sollte so hoch sein, wie die prüfende Stelle es sich leisten kann, und im Laufe der Zeit steigen. Die Richtlinie empfiehlt außerdem, zu jedem Hash das verwendete Verfahren und dessen Kostenfaktor zu speichern, damit das System später auf ein stärkeres Verfahren wechseln kann.

RFC 9106 beschreibt Argon2, eine für diese Aufgabe entwickelte speicherintensive Funktion, und empfiehlt die Variante Argon2id: als Standard für alle Umgebungen einen Durchlauf über 2 GiB Speicher oder bei knappem Speicher drei Durchläufe über 64 MiB. Laut RFC maximiert die erste Einstellung die Kosten eines Angreifers auf spezialisierter Brute-Force-Hardware. Darauf kommt es nach dem Abfluss einer Hashdatei an. Das OWASP Password Storage Cheat Sheet nennt niedrigere praxistaugliche Mindestwerte und Ausweichverfahren für Systeme, die Argon2id nicht verwenden können. Für alle gilt derselbe Grundsatz: Schnelle Hashfunktionen wie SHA-256 sind ungeeignet, weil sie viele schnelle Rateversuche ermöglichen. Passwörter werden gehasht statt verschlüsselt, weil Verschlüsselung in beide Richtungen funktioniert und sich das Original daraus wiederherstellen lässt.

Wie es in der Praxis aussieht

Bevor ein unternehmensweites Passwortmanagement eingeführt wurde, wurden Zugangsdaten so gespeichert und geteilt, wie es jeder Person beliebte. Im Alltag sieht das selten wie ein dramatischer Einbruch aus. Häufiger sind es ein Passwort in einer Chatnachricht, ein von niemandem gewechselter gemeinsamer Zugang und eine langsam wachsende Summe kleiner Offenlegungen. Das System gab der Organisation einen einheitlichen Weg zum Speichern und Teilen von Zugangsdaten. Die Nutzung war für alle verbindlich: Ein Passwortmanager, den nur das halbe Team verwendet, hilft kaum, wenn das Risiko bei der anderen Hälfte liegt. Sobald die Zugangsdaten an einem verwalteten Ort lagen, wurde die Zugriffskontrolle einfacher und einheitlicher. SP 800-63B weist von der Dienstseite in dieselbe Richtung: Prüfende Stellen müssen Passwortmanager und automatisches Ausfüllen zulassen und sollten das Einfügen aus der Zwischenablage erlauben. Die Richtlinie nennt einen Passwortmanager als Weg zu einem eigenen Passwort für jeden Dienst.

Als ein zweiter Server aus Code bereitgestellt wurde, lieferte die Geschichte der ersten Maschine die Begründung. Sie war von Hand erstellt und erst danach um ihre Firewall ergänzt worden. Das lässt ein Zeitfenster, in dem ein frischer Host mit einer standardmäßigen Passwortrichtlinie aus dem Internet erreichbar ist. Die Korrektur ist die Reihenfolge: Die neue Maschine entsteht hinter ihrer Firewall, weil der Firewall-Play vor dem Server-Play läuft.

Bei einer Anmeldung an einem großen E-Mail-Anbieter meldete die Anwendung dem Nutzer, sein Passwort sei falsch. Das stimmte nicht. Dieser Anbieter verlangt für Drittanbieter-Clients ein anwendungsspezifisches Passwort. Ein Konto hatte dadurch zwei Passwortarten, und eine Meldung, die nur eine kannte, ließ den

Nutzer etwas erneut eingeben, das nie funktionieren konnte. Die überarbeitete Meldung nennt den Anbieter, erklärt die Anforderung eines App-Passworts und sagt, wo es erstellt wird. Ein Test prüft den Anbieternamen und die Art der Zugangsdaten.

Wo es schiefgeht

Ein Passwort für viele Konten. Schützt dasselbe Passwort mehrere Dienste, öffnet ein Einbruch beim schwächsten auch die übrigen. SP 800-63B nennt dies Password Stuffing: Ein von einer Website erbeutetes Passwort wird gegen die Konten derselben Person auf anderen Websites eingesetzt. Nutzer schützen sich durch ein eigenes Passwort je Dienst, was praktisch einen Passwortmanager bedeutet. Dienste schützen sich, indem sie neue Passwörter mit Werten aus früheren Datenlecks abgleichen.

Regeln, die Passwörter schwächer machen. Vorgaben zur Zusammensetzung wirken streng und liefern vorhersehbare Ergebnisse. Das Beispiel der Richtlinie ist ein Nutzer, der „password“ gewählt hätte: Die Forderung nach Großbuchstabe und Ziffer führt zu „Password1“, die zusätzliche Symbolpflicht zu „Password1!“. Die Richtlinie schließt Zusammensetzungsregeln, planmäßige Wechsel, vor der Anmeldung lesbare Hinweise und Sicherheitsfragen wie den Namen des ersten Haustiers aus. Sobald es Anzeichen einer Kompromittierung gibt, verlangt sie trotzdem einen Wechsel.

Ein schneller Hash oder derselbe Salt in jeder Zeile. Eine mit einer allgemeinen Hashfunktion verarbeitete oder durchgehend mit demselben Salt versehene Passworttabelle gibt einem Offline-Angreifer günstige Rateversuche, die er gegen alle Konten gleichzeitig prüfen kann. Systeme mit übernommenen alten Hashes können jedes Passwort bei der nächsten Anmeldung seines Nutzers mit dem neuen Verfahren erneut hashen, wie es das OWASP Cheat Sheet beschreibt. Die gespeicherte Verfahrenskennung zeigt, welche Zeilen noch das alte Verfahren verwenden.

Das Passwort wird gekürzt oder lässt sich nicht einfügen. SP 800-63B verlangt, das gesamte eingereichte Passwort zu prüfen, niemals nur einen abgeschnittenen Teil. Das Einfügen sollte erlaubt sein, damit Passwortmanager auch dort funktionieren, wo automatisches Ausfüllen nicht möglich ist. Einige Hashfunktionen haben eigene Grenzen: Laut OWASP Cheat Sheet verarbeitet bcrypt in den meisten Implementierungen höchstens 72 Eingabebytes. Dienste, die es verwenden, sollen diese Obergrenze durchsetzen.

Das Passwort liegt dort, wo es nie hingehörte. Ein in einen Chat eingefügtes, in ein Ticket geschriebenes oder in einem Log ausgegebenes Passwort ist eine Kopie außerhalb aller Schutzmaßnahmen des eigentlichen Speichers. Nur ein Wechsel kann dieser Kopie ihren Wert nehmen. Deshalb ist ein verwalteter Ort wichtiger als jede Regel darüber, wie ein Passwort aussehen soll.

Weiterführende Lektüre

- Passwort im NIST-CSRC-Glossar — Definitionen aus FIPS 140-2, SP 800-63-4 und weiteren Dokumenten, mit der Passphrase als Sonderfall.
- NIST SP 800-63B-4 — die aktuellen Regeln zum Auswählen, Prüfen und Speichern von Passwörtern, mit den Begründungen in Anhang A.
- RFC 9106 — Argon2 mit den beiden empfohlenen Argon2id-Einstellungen für Passwort-Hashing.
- OWASP Password Storage Cheat Sheet — Praxisparameter für Argon2id, scrypt, bcrypt und PBKDF2 sowie die Aktualisierung alter Hashes.

Glossar

Für Ihre tatsächlichen Rahmenbedingungen auswählen

Beschreiben Sie den Bereitstellungsweg, die Betriebsrisiken und die Bereitschaftsverantwortlichen. Wir können eine Änderung mit Prüfungen, einem Wiederherstellungsweg und klaren Zuständigkeiten abgrenzen.

Preise ansehen Kontakt aufnehmen →

Die Begriffe praktisch nutzbar machen

Fragen Sie, wie „Was ist ein Passwort?“ auf Ihre Organisation zutrifft. Ein konkretes Beispiel aus Ihrem bestehenden System reicht aus, um das Gespräch zu beginnen.

Unsere Leistungen entdecken

welcome@engineer.company +45 50 10 61 84 Kopenhagen, Dänemark

Nehmen Sie diese Seite mit

Kontaktkarte

Mit Sorgfalt und Liebe gestaltet von D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Copyright © 2025 – heute · Engineer ApS · Alle Rechte vorbehalten.

Gedruckt von https://engineer.company/de/glossary/password/