Dirk Fox, Frank Schaefer

Passwörter – fünf Mythen und fünf Versäumnisse

Bis heute wird der Zugriff auf Daten und Anwendungen überwiegend durch einen Passwortschutz kontrolliert. Oft ist dieser Passwortschutz jedoch unzureichend, weil sich für die Gestaltung von und den Umgang mit Passworten hartnäckig unrichtige Überzeugungen halten und die falschen Prioritäten gesetzt werden.

1 Hintergrund

Die Diskussion der Sicherheit von Passwörtern begleitet die IT-Sicherheit von Anfang an – und wird uns, allen Fortschritten bei anderen Authentisierungsmethoden zum Trotz, zweifellos noch lange beschäftigen. Denn ein Passwortschutz ist technisch vergleichsweise einfach zu realisieren, und es wird immer IT-Systeme und Anwendungen geben, bei denen andere Zugriffsschutzverfahren entweder zu teuer oder aus anderen Gründen nicht geeignet sind.

Für die konkrete Ausgestaltung eines Passwortschutzmechanismus sind im Wesentlichen zwei zentrale Fragen zu beantworten:

- Was ist ein *sicheres Passwort* und wie bewirkt man die Wahl sicherer Passwörter?
- Wie müssen die *Prozesse* um und der Umgang mit Passwörtern gestaltet sein, damit daraus keine Sicherheitslücken entstehen?

Antworten auf diese beiden Fragen finden sich in der Praxis zumeist in einer „Password Policy", deren Regeln häufig auf allgemein akzeptierten, allerdings nicht weiter hinterfragten Glaubenssätzen basieren. Dabei werden für das erreichte Sicherheitsniveau des Schutzmechanismus oft wesentliche Aspekte ausgespart. Die aus Sicherheitsperspektive gefährlichsten dieser Mythen und Versäumnisse verbreiteter Passwort-Regelwerke sind Gegenstand des vorliegenden Beitrags.

Bevor diesen Fragen genauer nachgegangen wird, soll zunächst mit einem verbreiteten Missverständnis aufgeräumt werden: Gute Passwörter schützen keineswegs nur vor einem unberechtigten Zugriff auf Daten und Systeme. Immer wichtiger wird, das zeigen vor allem IT-forensische Analysen, eine zweite Funktion: Gute Passwörter verhindern, dass Dritte IT-Systeme unter dem Namen und der Identität einer anderen Person nutzen, der diese Aktivitäten anschließend zugerechnet werden. Das kann für die Betroffenen erhebliche Konsequenzen haben, nicht zuletzt bei strafrechtlich relevantem Verhalten (z. B. Download kinderpornographischer Darstellungen).

Auf Daten und Systeme können häufig zahlreiche Personen zugreifen, nicht zuletzt die Administratoren eines Systems. Unter einer bestimmten Identität (User-ID) sollte dies jedoch immer nur ein einziger, eindeutig bestimmbarer Nutzer können, damit dieser nicht für Aktivitäten Dritter verantwortlich gemacht werden kann.

Dirk Fox

Geschäftsführer der Secorvo Security Consulting GmbH und Herausgeber der DuD.
E-Mail: dirk.fox@secorvo.de

Prof. Dr. rer.nat. Frank Schaefer

lehrt an der Fakultät für Informatik und Wirtschaftsinformatik der Hochschule Karlsruhe Mathematik, IT-Sicherheit und Kryptographie.
E-Mail: frank.schaefer@hs-karlsruhe.de

2 Mythen

Mit unerschütterlicher Hartnäckigkeit halten sich einige Irrtümer über die geeignete Gestaltung von Passwortschutzmechanismen, die inzwischen Eingang in unzählige Passwort-Policies gefunden haben. Die – nach unserer Erfahrung – aus Sicherheitsperspektive schwerwiegendsten fünf dieser Mythen werden im Folgenden erläutert.

2.1 Mythos Passwortlänge

Für die Länge geeigneter Passwörter finden sich in der Literatur zahlreiche Empfehlungen. In vielen Policies sowie der aktuellen Fassung der Grundschutz-Kataloge werden mindestens acht Zeichen für alphabetische[1] Passwörter empfohlen (M 2.11 „Regelung des Passwortgebrauchs" [BSI_08]).

Tatsächlich ist die Vorgabe einer einheitlichen Passwortmindestlänge sachlich nicht zu begründen. Denn die erforderliche Passwortlänge hängt in erster Linie von dem zu Grunde liegenden Angreifermodell ab. Grob lassen sich drei Klassen von Modellen unterscheiden:

- *Modell A*: Kann ein Angreifer nur über eine definierte Schnittstelle (wie z. B. bei einem Geldautomaten oder einer Web-Applikation) zugreifen? In diesem Fall genügt ein vergleichsweise kurzes Passwort, da die Zahl der Rateversuche z. B. über die Reaktionszeit der Anwendung begrenzt werden kann.

1 Mit „alphabetischen Passwörtern" werden hier Zeichenfolgen aus Groß- und Kleinbuchstaben (also 52 verschiedenen Zeichen) bezeichnet.

- *Modell B*: Erlaubt die Anwendung eine Offline-Attacke, wie beispielsweise bei einer abgefangenen, Passwort geschützten ZIP- oder Office-Datei? Dann müssen die Anforderungen an das Passwort so gewählt werden, dass ein Rate-Angriff mit realistischen Ressourcen in dem Zeitraum, in dem die geschützten Daten für den Angreifer einen Wert darstellen, mit höchster Wahrscheinlichkeit nicht zum Erfolg führt.
- *Modell C*: Muss angenommen werden, dass ein Angreifer in den Besitz des Passwortspeichers eines Systems (wie z. B. der SAM-Datei unter Windows) gelangen kann, sodass er mit einem Passwortcracker alle darin gespeicherten Passworte quasi „parallel" attackieren kann?[2] Dann müssen die Passwortanforderungen ein erfolgreiches Cracken auch nur eines einzigen der im Speicher abgelegten Passwort-Hashwerte verhindern. In diesem Fall bestimmt das schwächste gewählte Passwort die Sicherheit des Systems.[3]

Im zweiten und dritten Fall ist außerdem zu berücksichtigen, dass die Passwortmindestlänge regelmäßig an die steigende Leistungsfähigkeit von Cracking-Tools angepasst wird. Es zeigt sich, dass deren Mächtigkeit regelmäßig unterschätzt wird (siehe Tabelle).

Erst kürzlich wurde ein Passwort-Cracker vorgestellt, der unter Nutzung der Rechenleistung zweier Grafikkarten die Brute-Force-Suche nach einem alpha-numerischen[4] sechsstelligen Passwort mit Sonderzeichen auf einem Standard-PC auf 6 Minuten und nach einem achtstelligen auf 33 Tage senkt [ArDe_09].

Tabelle 1 | Cracking-Aufwand für ein vier- bzw. sechsstelliges Passwort auf einem handelsüblichen PC

Passwort	2003	2007
Vier Zeichen		
h2TU	0h 1m 40s	0h 0m 1s
G6_W	0h 1m 41s	0h 0m 1s
Sechs Zeichen		
cL9ge!	15h 13m 9s	0h 33m 57s
-6nC3$	16h 11m 26s	0h 37m 19

Fazit: Während bei Web-Applikationen (mit Login-Verzögerung oder Sperrung nach mehreren Fehleingaben) ein nur vierstelliges alpha-numerisches Passwort einen ausreichenden Schutz bieten kann, sollte ein Windows-Passwort heute nicht weniger als zehn Zeichen lang sein, um einem Cracker-Angriff auf die Passwort-Hash-Tabelle widerstehen zu können.

2.2 Mythos Loginsperre

Die meisten Unternehmen sperren den Zugang zu internen Systemen nach einer begrenzten Zahl von Login-Fehlversuchen. Oft liegt dieser Wert – in Übereinstimmung mit den Empfehlungen der Maßnahmenkataloge des BSI zum IT-Grundschutz (M 2.11 „Regelung des Passwortgebrauchs" [BSI_08]) – bei drei; eine Aufhebung der Sperrung ist nur mit Administrator-Berechtigung möglich.

Die Konsequenz ist bekannt: Nach dem Ende der Urlaubszeit und in den Tagen nach jedem erzwungenen Passwortwechsel steigt die Zahl der Passwortrücksetzungen erheblich. Sie summieren sich nach einschlägigen Untersuchungen auf 20-50 % aller Hotline-Anrufe [Smith_02]. Der Aufwand für eine Passwortrücksetzung ist erheblich: Nach einer Studie von Forrester Research aus dem Jahr 1999 („A digital Certificate Roadmap") liegen die Gesamtkosten bei 80 US$ je Vorgang.

Login-Sperren sind jedoch nicht nur teuer, sondern auch gefährlich. Denn wenn Passwortrücksetzungen der „Normalfall" sind, schleifen sich häufig Prozesse ein, die ein offenes Einfallstor für Angreifer darstellen. So lässt sich bei Sicherheitsaudits immer wieder beobachten, dass eine Passwortrücksetzung entweder mit einfach zu recherchierenden Angaben (z. B. dem Geburtsdatum oder der Personalnummer) oder ganz ohne Angaben zur Autorisierung gelingt. Nur selten werden hinterlegte Informationen erfragt, die nur dem wirklichen Account-Inhaber bekannt sein können. Oft verzichten Hotline-Mitarbeiter auch auf eine vorgeschriebene Autorisierung, wenn der Anrufer große Dringlichkeit behauptet oder eine plausible Geschichte erfindet. Sehr selten werden Passwort-Rücksetzungen dokumentiert (Anrufzeitpunkt, Telefonnummer des Anrufers, Begründung), so dass erfolgreiche Social Engineering-Angriffe auf den Rücksetzungsprozess nicht einmal Spuren hinterlassen.

Eine weitere Gefahr wird regelmäßig unterschätzt: Wenn ein Account nach wenigen Fehlversuchen gesperrt wird, kann ein Angreifer oder auch ein verärgerter Mitarbeiter mit vergleichsweise geringem Aufwand ausgewählte Mitarbeiter oder auch ein ganzes Unternehmen für Stunden lahm legen, indem er durch Passwort-Fehleingaben die Sperrung möglichst vieler Mitarbeiteraccounts verursacht.

Dabei sorgt eine Login-Sperre im Angreifermodell A nicht einmal für einen Sicherheitsgewinn. So ist ein Sechser im Lotto wahrscheinlicher, als mit 100 Versuchen ein sechsstelliges, alphabetisches Passwort zu erraten. Sinnvoller als eine komplette Sperre ist es, den Login-Prozess nach einigen Fehlversuchen zu verzögern oder den Account kurzzeitig (für wenige Minuten) zu deaktivieren. Wenn das System eine solche Reaktion auf Fehleingaben nicht unterstützt, hilft es oft schon, die Zahl der zulässigen Fehlversuche auf zehn oder 20 zu erhöhen, um die Menge der Passwortrücksetzungen signifikant zu senken, denn den meisten Nutzern fällt dann das richtige Passwort rechtzeitig vor der Sperrung wieder ein.

Einen deutlich wirksameren Schutz bei Angriffsversuchen auf einen Account bewirkt die Anzeige des letzten (erfolgreichen) Logins sowie Anzahl und Zeitpunkt zurückliegender Fehlversuche (siehe auch die IT-Grundschutz-Maßnahmenempfehlung M 4.15 „Gesichertes Login" [BSI_08]). Einen legitimen Nutzer wird es alarmieren, wenn das System ihm nach seiner erfolgreichen Anmeldung Logins oder Login-Versuche meldet, an die er sich nicht erinnern kann.

2.3 Mythos Passwortkomplexität

Im Zentrum der Diskussion um Passwortsicherheit steht meist die Komplexität eines Passworts. Das ist grundsätzlich auch richtig, denn der Aufwand für einen

2 Dazu kann es genügen, dass der Angreifer in den Besitz eines Laptops ohne Vollverschlüsselung gelangt: Darauf findet sich im Verzeichnis C:WINDOWS\System32\Config\ die SAM-Datei mit den Passwort-Hashwerten aller Accounts, die sich an diesem oder über diesen Laptop jemals angemeldet haben.

3 In einigen Betriebssystemen, insbesondere unter Unix, werden Passwort-Hashtabellen durch „salting" (Salzen) vor einer solchen Attacke geschützt. Dazu wird jedem Passwort vor der Berechnung des Hashwertes ein Zufallswert („Salt") angehängt, damit die Hashwerte gleicher Passworte sich unterscheiden. Der Passwort-Cracker muss dann jeden Eintrag einzeln analysieren. Salting verhindert auch, dass die Analyse durch vorausberechnete „Rainbow-Tables" (Time-Memory-Tradeoff-Angriffe) beschleunigt werden kann [Nohl_08].

4 Unter einem „alpha-numerischen" Passwort wird eine Zeichenfolge aus Groß- und Kleinbuchstaben sowie Ziffern (also 62 verschiedenen Zeichen) verstanden.

Passwort-Cracker, der jede Zeichenkombination ausprobiert („Brute Force"), steigt mit der Größe des Suchraums.

Was aber zeichnet ein „gutes Passwort" aus? Im Idealfall ist das Passwort von einer zufälligen Zeichenfolge nicht zu unterscheiden, enthält also keine Namen, Worte oder Wortfragmente irgendeiner Sprache. Da sich eine solche „Zufallsähnlichkeit" nicht technisch überprüfen lässt, stellen Password-Policies meist technisch durchsetzbare Anforderungen, z. B. – in Übereinstimmung mit den Empfehlungen der IT-Grundschutzkataloge (M 2.11 „Regelung des Passwortgebrauchs" [BSI_08]) – die Verwendung von mindestens einem Sonderzeichen oder einer Ziffer.

Natürlich ist ein Passwort, das neben Buchstaben auch Ziffern und Sonderzeichen enthält, grundsätzlich komplexer als ein rein alphabetisches und damit aufwändiger zu erraten. Denn für einen Angreifer vergrößert sich der Suchraum, wenn er für jede Stelle des Passworts nicht nur 52 alphabetische Zeichen, sondern zusätzlich zehn Ziffern und zumindest die über die Tastatur leicht erreichbaren 22 Sonderzeichen ausprobieren muss. Allerdings zeigt eine einfache Rechnung, dass ein nur ein Zeichen längeres alphabetisches Passwort noch schwerer zu finden ist: Ein neunstelliges alphabetisches Passwort kann $2{,}8\times10^{15}$ Werte annehmen, ein achtstelliges aus Buchstaben, Ziffern und Sonderzeichen lediglich $2{,}5\times10^{15}$.

Hinzu kommt, dass Nutzer dazu neigen, Ziffern und Sonderzeichen ihrem Passwort voranzustellen oder sie an das Ende anzuhängen. Auch erfreuen sich einige Sonderzeichen (wie „.", „-", „!" oder „?") besonderer Beliebtheit, treten also weit häufiger auf als eher exotische und auf der Tastatur schwierig erreichbare Sonderzeichen. Besonders häufig stehen – trainiert durch die deutsche Rechtschreibung – ein erzwungener Großbuchstabe an der ersten Stelle (26 mögliche Zeichen), die Ziffer (10 mögliche Zeichen) und ein Satzzeichen als Sonderzeichen (meist eines aus vier bevorzugten Zeichen) an den beiden letzten. Für den Angreifer verringert sich dadurch der Suchaufwand im Vergleich zu einem gleichlangen alphabetischen Passwort selbst dann noch erheblich, wenn er bei den beiden letzten Stellen alle Sonderzeichen und Ziffern (32 Zeichen) durchprobiert.

Schlimmer noch: Besonders bei sechs-, acht- und zehnstelligen Passwörtern wählen Nutzer gerne Datumsangaben (Geburtsdatum, Hochzeitstag etc.) – Ziffern und ein Sonderzeichen („.") sind darin automatisch enthalten. Da die gewählten Datumswerte in der Regel nicht länger als 100 Jahre zurückliegen, verringert sich der Suchraum auf 36.500 Möglichkeiten – da ist sogar ein nur vierstelliges alphabetisches Passwort um den Faktor 200 sicherer ($7{,}3\times10^{6}$ Möglichkeiten).

Will man sich wirksam vor einem Passwort-Cracker schützen, muss zudem die Komplexität des „simpelsten möglichen Passworts" als Maßstab herangezogen werden. Da zeigt sich die Schwäche der oben beschriebenen Komplexitätsanforderungen: Auch „12345678" ist ein gültiges Passwort – für einen Passwortcracker ein Witz.

Daraus folgt: Komplexitätsregeln führen in der Praxis häufig dazu, dass sich der zu berücksichtigende Suchraum für einen Angreifer *verkleinert*.[5] Zudem ist eine größere Passwortmindestlänge deutlich wirkungsvoller als die Erzwingung eines (vermeintlich) komplexeren Passworts.

2.4 Mythos Passwortwechsel

Regelmäßige Passwortwechsel sollen der Tatsache Rechnung tragen, dass ggf. auch komplexe Passwörter fester Länge einem Offline-Angriff mit vielen Ressourcen nicht standhalten. Ferner soll der durch einen erfolgreichen, aber unbemerkten Passwort-Hack entstehende Schaden begrenzt werden.

Tatsächlich aber führt ein erzwungener regelmäßiger Passwortwechsel bei der überwiegenden Zahl der Nutzer dazu, dass die Qualität des Passwortschutzes sinkt. Das hängt nicht nur damit zusammen, dass relativ kurze Zeit gültigen Passworten eine geringere Bedeutung beigemessen wird und Nutzer weniger Zeit in die Auswahl investieren. Häufige Passwortwechsel motivieren Anwender außerdem darüber nachzudenken, wie sie die zu wechselnden Passworte so wählen können, dass sie sich leichter merken lassen.

Wenn eine Passwort-Historie die Wiederverwendung alter Passworte verhindert, werden daher häufig die letzten Stellen des Passworts als „Sequenz" gestaltet – und die verbleibenden unverändert gelassen. So ist es eine verbreitete (Un-) Sitte, bei einem alle 90 Tage fälligen Passwortwechsel eine „Quartals-ID" (z. B. „Q209") oder eine laufende Nummer anzuhängen, die das Passwort „hochzählt". Dadurch verkleinert sich für einen Angreifer nicht nur der Suchraum erheblich. Er kann auch aus einem gecrackten Passwort leicht das Bildungsgesetz ableiten und damit die zukünftigen Passworte vorhersagen – wodurch der intendierte Nutzen des Passwortwechsels komplett verloren geht. Da IT-Systeme (aus gutem Grund) Passwörter nicht im Klartext, sondern nur deren Hashwerte speichern, lässt sich eine nur geringe Abweichung eines neuen Passworts vom vorherigen systemseitig nicht erkennen.

Bei Nutzern, die kein einfaches Bildungsgesetz wählen, steigen nach jedem Passwortwechsel die Rücksetzungsanrufe – mit den oben bereits skizzierten Folgeproblemen.

In der Praxis ist es wesentlich wirkungsvoller, auf einen regelmäßigen Passwortwechsel zu verzichten und statt dessen die Passwortmindestlänge zu erhöhen. Selbst bei einem rein alphabetischen Passwort wächst der Cracking-Aufwand je Zeichen Länge um den Faktor 52 – aus einem 90-Tage-Schutz wird damit ein wirksamer Schutz für 14-Jahre.

2.5 Mythos Gedächtnis

Kaum eine Policy ohne ein „Notierverbot" für gewählte Passwörter: Das Aufschreiben eines Passworts gilt gemeinhin als Todsünde im Umgang mit Kennwörtern.

Tatsächlich aber verhalten sich Qualität (Entropie [Fox_08]) und Merkbarkeit eines Passworts umgekehrt propotional zueinander: Je höher die Entropie, desto schwieriger ist es, ein Passwort im Gedächtnis zu behalten. Zwar ist es zutreffend, dass das Notieren eines Passworts grundsätzlich das Risiko birgt, dass es einem Unberechtigten zur Kenntnis gelangt. In der Praxis ist jedoch auch hier das Angreifermodell entscheidend: In welcher Umgebung muss mit einem unbemerkten Eindringen eines Angreifers gerechnet werden? An welchen Aufbewahrungsorten eines notierten Passworts muss davon ausgegangen werden, dass ein Angreifer Zugriff erlangen kann?

Abhängig von der zu schützenden Anwendung bleiben zahlreiche Möglichkeiten, ein notiertes Passwort sicher aufzubewahren. Aber auch ein schlechter

5 Eine Analyse zahlreicher verbreiteter Passwort-Policies findet sich in [Wils_02].

Aufbewahrungsort ist noch einem schlechten Passwort vorzuziehen: Denn anders als ein Offline-Cracking-Angriff auf einen Passwortspeicher „skalieren" Angriffe auf Passwortnotizen nicht: Ein Angreifer muss jeden einzelnen Aufbewahrungsort identifizieren und Aufsuchen, um Kenntnis von dem dort notierten Passwort zu erhalten, während das Cracken von Hunderten von Passworten (zumindest im Angreifermodell C) ebenso schnell gelingt wie das eines einzigen. Besser ist es daher, das Notieren von Passworten zu regulieren – zumal in der Praxis davon ausgegangen werden muss, dass Mitarbeiter Passworte aufschreiben. Ohne klare Regeln tun sie dies mit hoher Wahrscheinlichkeit auf ungeeignete Weise.

3 Versäumnisse

Während viele Passwort-Policies in den Augen der Nutzer eher die Anmutung von Disziplinarmaßnahmen haben, weist das zugehörige Passwortschutzsystem häufig zahlreiche sicherheitskritische Fehler auf. Oft lassen sich diese Lücken durch vergleichsweise einfache Maßnahmen schließen und das erreichte Schutzniveau dadurch erheblich erhöhen. Die verbreitetsten Versäumnisse werden im Folgenden kurz vorgestellt.

3.1 Inaktive Accounts

Nicht aktiv genutzte Accounts sind bei Angreifern aus mehreren Gründen besonders begehrt: Da eine illegitime Nutzung eines bestehenden Accounts in der Regel am ehesten dem Inhaber auffällt, birgt der Zugriff auf einen inaktiven Account für einen Angreifer die Chance auf eine über einen längeren Zeitraum unbemerkte Nutzung.

Hinzu kommt, dass inaktive Accounts häufig über ein geringeres Schutzniveau verfügen: Entweder wurden sie vom Account-Inhaber noch nie genutzt und sind daher noch mit dem Initialpasswort geschützt, oder der Account-Inhaber ist aus dem Unternehmen ausgeschieden, und seitdem vorgenommene Verschärfungen der Passwort-Policy (wie z. B. eine Erhöhung der Passwort-Mindestlänge) wurden vom Account-Inhaber nicht umgesetzt.

Daher sollten alle Accounts regelmäßig auf Nutzung überprüft und ungenutzte Accounts spätestens drei Monate nach der letzten Nutzung gesperrt werden. Durch einen systematischen Prozess sollte zudem sichergestellt sein, dass Accounts ausgeschiedener Mitarbeiter zum Zeitpunkt des Ausscheidens automatisch gesperrt werden.

3.2 Initialpasswörter

Die meisten Anwendungen erlauben es einem Nutzer heute, jederzeit und ohne Mitwirkung eines Administrators sein eigenes Passwort zu wählen und zu ändern. Aber nur ein kleiner Teil der Applikationen ist so konfigurierbar (und auch so konfiguriert), dass der Nutzer sein Initialpasswort gleich beim ersten Login durch ein neues Passwort ersetzen muss.

Dabei ist das ein wichtiger Schutzmechanismus: Initialpasswörter werden in der Regel nicht vom Anwender gewählt, sondern vom System oder Systemadministrator vorgegeben. Im schlimmsten Fall werden bei der Einrichtung eines neuen Accounts einheitliche „Startpassworte" vergeben – unter Verwendung des immer gleichen Personenmerkmals (Geburtsdatum, Nachname o. ä.) oder sogar als unternehmensweites Einheits-Passwort. Nicht selten wird dasselbe Passwort auch bei einer Passwort-Rücksetzung verwendet.

Ein solches Standard-Passwort ist in der Regel ein „offenes Geheimnis" – nicht nur im jeweiligen Unternehmen. Wird das Initialpasswort daher nicht gleich nach dem ersten Login geändert oder bleibt der Account eine Zeit lang ungenutzt, können Unberechtigte auf den Account meist über einen gewissen Zeitraum unbemerkt zugreifen.

Im Idealfall werden Initialpasswörter individuell vergeben und sind mindestens so gut wie die insgesamt angestrebte Passwortqualität. Falls dies nicht der Fall sein sollte, muss ein zügiges Ändern des Initialpasswortes erzwungen werden.

3.3 Trivialpasswörter

Einfache Passwörter sind leicht zu merken. Daher wählen Nutzer bevorzugt solche Passwörter, die zwar den Anforderungen an Länge oder Komplexität des Passworts genügen, aber ein triviales „Bildungsgesetz" besitzen. Aus diesem Grund prüfen Passwort-Cracking-Programme zunächst typische Trivialpasswörter ab, bevor sie mit dem Durchprobieren aller zulässigen Zeichenkombinationen („Brute Force") beginnen.

Obwohl dies bekannt ist, wird die Wahl trivialer Passwörter in den meisten Anwendungen nicht technisch verhindert. Zwar kann das in der Regel auch nur eingeschränkt gelingen; dennoch sollten z. B. gültige Datumsangaben, Tastenfolgen wie „Qwertzui", lexikalische Begriffe sowie Namen, Marken, Initialpasswörter etc. abgewiesen werden. Dazu lassen sich Wörterbücher leistungsfähiger Passwort-Cracking-Tools nutzen, die um unternehmenstypische Begriffe wie Firmenname, Firmensitz oder Produktbezeichnungen erweitert werden.

Noch wirksamer ist die Überprüfung von wesentlichen Eigenschaften trivialer Passwörter: Hat es das Format eines Datums (nur Ziffern oder Ziffern und Punkte)? Kommt ein Zeichen mehrfach vor? Folgen benachbarte Zeichen im Alphabet aufeinander? Liegen mehr als zwei benachbarte Zeichen auf der Tastatur nebeneinander?

Ideal wäre die Bestimmung der Passwort-Entropie, damit ausschließlich Passworte einer festgelegten Mindestqualität genutzt werden [Maus_08]. Wenn eine solche Online-Analyse bei der Passworteingabe vom System nicht unterstützt wird, sollten die zentral gespeicherten Passwort-Hashwerte von Zeit zu Zeit einer Analyse mit einem Passwort-Cracker unterzogen werden. Dabei dürfen vor allem „Alt-Accounts" nicht ausgeschlossen werden: Hinter solchen Accounts mit aus „historischen Gründen" schwachen Passwörtern stecken in der Regel Mitarbeiter, die lange im Unternehmen sind – und aufgrund ihrer Position Zugriff auf besonders kritische Unternehmensdaten haben.

3.4 Passwortweitergabe

Ein Passwort ist ein Geheimnis – und ein Geheimnis darf man nicht teilen, wenn es eins bleiben soll. In der Praxis verstoßen Mitarbeiter in Unternehmen regelmäßig gegen dieses Grundprinzip – meist mit den Führungskräften als schlechtes Vorbild: Aus nachvollziehbaren Gründen lassen viele Führungskräfte Ihre E-Mails von ihrem Sekretariat vorfiltern – und geben ihnen dazu die Zugangsdaten ihrer E-Mail-Box. In zahlreichen Unternehmen sind die Mitarbeiter überzeugt, dass Administratoren ohnehin auf ihr Passwort zugreifen können – der perfekte Nährboden für eine „Social Engineering"-

Attacke, bei der der Angreifer sich als IT-Hotline ausgibt und das Passwort des Nutzers erfragt.

Eine Untersuchung von Infosecurity Europe[6] zeigte Anfang 2007, dass die Weitergabe von Passwörtern in Unternehmen verbreiteter ist, als gemeinhin angenommen. Zwar können sich befragte Mitarbeiter in der Regel nicht daran erinnern, ihr eigenes Passwort weitergegeben zu haben – aber über 29 % der Befragten versicherten, das Passwort von mindestens einem Kollegen zu kennen. 39 % würden ihr Passwort an einen Kollegen von der IT-Abteilung weitergeben, knapp 33 % auch an ihren Chef.

Abgesehen von seltenen Ausnahmen, in denen es keine praktikable Alternative gibt, sind Passwortweitergaben hingegen verzichtbar:

- Anstatt das E-Mail-Passwort an das Sekretariat weiterzugeben, richtet man für Führungskräfte ein gemeinsam genutztes Funktionspostfach ein (z. B. sekretariat.vorstand@firma.de), an dem erkennbar ist, dass mehrere Personen darauf Zugriff haben.
- Im Urlaubsfall sorgt man für eine Abwesenheitsmeldung oder eine automatische Weiterleitung an einen Vertreter.
- Müssen Kollegen auf gemeinsam genutzte Daten zugreifen können, gehören diese nicht auf ein persönliches Laufwerk, sondern in ein Serververzeichnis mit passenden Zugriffsrechten.

Schließlich muss die Weitergabe eines Passworts im Notfall sorgfältig organisiert sein: In einem verschlossenen Umschlag hinterlegt sollte das Passwort erst nach einer Prüfung durch einen Verantwortlichen herausgegeben und unmittelbar nach dem erforderlichen Zugriff geändert werden.

3.5 Mehrfachnutzung

Ein Passwort lässt sich leichter merken als viele verschiedene – daher verwenden IT-Nutzer bevorzugt dasselbe Passwort für unterschiedliche Systeme. Diese Tendenz verstärkt sich nicht nur mit der Zahl der Passwörter, sondern auch, wenn an einzelne Passworte höhere Anforderungen gestellt werden (Ausschluss von Trivialpasswörtern, Komplexität, Länge).

Häufig werden daher dienstlich genutzte Passwörter auch zur Authentisierung bei Web-Diensten oder auf dem privaten PC verwendet. In der oben zitierten Befragung von Infosecurity Europe gaben 58% der Befragten an, ihr dienstliches Passwort auch privat zu nutzen. Ein für verschiedene Dienste und Systeme verwendetes Passwort ist dabei allerdings nur so sicher vor Ausspähung wie die diesbezüglich am schlechtesten geschützte Anwendung.

Daher sollte grundsätzlich gelten: Dasselbe Passwort darf nie zugleich auf mehreren Systemen genutzt werden, die in der Verantwortung unterschiedlicher „Betreiber" liegen. So gehört ein dienstliches Passwort weder ins Web noch auf den Privat-PC. Nutzt man verschiedene Anwendungen im Verantwortungsbereich desselben Betreibers (z. B. des Arbeitgebers), sollten sich die Passwörter zumindest durch ein Prä- oder Postfix, das beispielsweise die jeweilige Anwendung kennzeichnet, unterscheiden.

Für Web-Anwendungen bietet das für zahlreiche Plattformen verfügbare Open Source Tool *PasswordMaker* eine elegante Lösung:[7] Aus einem Masterpasswort und der URL eines Dienstes leitet es mit einer auswählbaren Einwegfunktion ein jeweils individuelles Webseitenpasswort ab. Damit genügt es, sich das Master-Passwort einzuprägen.

4 Fazit

So einfach der gute, alte Passwortmechanismus auf den ersten Blick erscheint, so umfangreich sind doch die Herausforderungen in der Praxis und im Detail. In diesem Beitrag standen grundsätzliche Anforderungen an Passwörter und ihre Handhabung im Mittelpunkt, ohne technische Details bei deren Implementierung zu berücksichtigen. Auch dort können Fußangeln lauern, wie der „Kennworthinweis" unter Windows Vista zeigt: Wer eine solche „Erinnerungshilfe" im System hinterlegt, erhält den Tipp nach mehreren Fehlversuchen angezeigt – der Angreifer natürlich auch.

Bei der Beurteilung der Qualität von Passwörtern stellt außerdem die Kontextabhängigkeit eine schwer kalkulierbare Größe dar: U-BKaT.M. ist sicher für sehr viele Menschen ein gutes Passwort – für den Mitarbeiter Thomas Müller der Universitäts-Bibliothek Karlsruhe wohl eher nicht.

Umgekehrt wird aber ein Schuh daraus: Gute Passwörter kann man aus den Anfangsbuchstaben eines Satzes gewinnen: GPkmadA1Sg. Untersuchungen belegen, dass ihre Qualität fast so gut ist wie die echt zufällig gewählter Passwörter [YBAG_00].

Literatur

[Ande_01] Anderson, Ross: *Security Engineering, Chapter 3: Passwords*, S. 35-50, 2001, http://www.cl.cam.ac.uk/~rja14/book.html (10.06.2009)

[ArDe_09] Arbeiter, Stefan; Deeg, Matthias: *Bunte Rechenknechte*. c't 6/2009, S. 204-206.

[BSI_08] Bundesamt für Sicherheit in der Informationstechnik (BSI): *IT-Grundschutz-Kataloge*, 10. Ergänzungslieferung, Oktober 2008 http://www.bsi.bund.de/gshb (10.06.2009)

[Fox_08] Fox, Dirk: *Entropie*. Gateway, DuD 8/2008, S. 543.

[Maus_08 Maus, Thomas: *Das Passwort ist tot – lang lebe das Passwort!* DuD 8/2008, S. 537-542.

[Nohl_08] Nohl, Karsten: *Kunterbuntes Schlüsselraten*. c't 15/2008, S. 190-193, http://www.heise.de/security/Von-Woerterbuechern-und-Regenboegen--/artikel/113681/0 (10.06.2009)

[Smith_02] Smith, Richard E.: *Brief Recommendations for a Sane Password Policy*, 09.08.2002, http://www.cryptosmith.com/sanity/pwrecom.html (10.06.2009)

[ThKr_09] Thanner, Constance; Krumm, Markus: *Passwort 2010*. KES, 2/09, S. 6 ff. http://www.kes.info/aktuell/akheft/artikel1.htm (10.06.2009)

[Wils_02] Wilson, Sam: *Combating the Lazy User: An Examination of Various Password Policies and Guidelines*, SANS Institute, 16.09.2002, https://www.sans.org/reading_room/whitepapers/authentication/combating_the_lazy_user_an_examination_of_various_password_policies_and_guidelines_142 (10.06.2009)

[YBAG_00] Yan, Jianxin; Blackwell, Alan; Anderson, Ross; Grant, Alasdair: *The memorability and security of passwords – some empirical results,* September 2000, University of Cambridge, Computer Laboratory Technical Report no 500, http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-500.pdf (10.06.2009)

6 Befragung von 300 Passanten und IT-Profis in London, März 2007.

7 PasswordMaker: http://passwordmaker.org/