Institut für Informatik und Gesellschaft, Abteilung Telematik
Albert-Ludwigs-Universität Freiburg

Benutzbare Benutzerauthentifizierung
Security and Usability of Passwords

Ausarbeitung im Seminar
Technologien der Informationsgesellschaft

Bearbeiter:	Matthias Bernauer
Matrikelnummer:	150 31 53
Aufgabensteller:	Prof. Dr. Günter Müller
Betreuer:	Dipl.-Inf. Martin Kähmer
Abgabedatum:	28. Oktober 2006

Zusammenfassung

Studien bescheinigen den klassischen Passwörtern entweder eine schlechte Benutzbarkeit oder einen schlechten Grad an Sicherheit, denn je einfacher die Passwörter für den Benutzer zu merken sind, desto einfacher sind sie in der Regel für einen Angreifer zu erraten [Vu06]. Daher wird die Bedeutung von Kennwörtern in einer Gegenüberstellung zu alternativen Authentifizierungsmechanismen dargestellt. Sichere Methoden zur Konstruktion von Passwörter werden analysiert und die Umsetzung unter dem Gesichtspunkt ihrer Benutzbarkeit erläutert. Auf der Grundlage erfolgter Studien werden Methoden und Verhaltensweisen zur Steigerung der Sicherheit und Anwendungsfreundlichkeit von Passwörtern genannt und diskutiert. Alternative Ansätze und Trends zur Authentifizierung werden vorgestellt.

Inhaltsverzeichnis

1 Einleitung

Passwörter stellen die klassische Methode der Benutzerauthentifizierung dar. Die steigende Anzahl von Anwendungsprogrammen und multimedialen Dienstleistungen, mit welchen sich der herkömmliche Nutzer zunehmend auseinandersetzen muss, erfordern in der Regel die Angabe von Kennwörtern, um diese Dienste nutzen zu können. Mit den zunehmenden Möglichkeiten, alltägliche Tätigkeiten und Geschäftsprozesse über das Internet abwickeln und erledigen zu können, muss der Benutzer einer Vielzahl von Sicherheitsanforderungen gerecht werden.

Nahezu jedes Dienstleistungsportal erfordert die vorherige Registrierung, die dem Anwender Bemühungen zur Erstellung neuer Authentifizierungsdaten abverlangt. Sei es die Anmeldung zu einem gewöhnlichen Diskussionsforum, der Zugang zu einer Internetauktion oder die Nutzung des elektronischen Bankaccounts, so setzt jeder Anbieter von Diestleistungen bei unterschiedlichster Art der Dienste die Identifizierung des Teilnehmers voraus. Neben persönlichen Daten erfordert die Registrierung gewöhnlich die Angabe eines eindeutigen Nutzernamens sowie eines dazugehörigen Passwortes. Dabei kommen nicht selten restriktive Vorgaben zum Einsatz, die den Anwender dazu zwingen, Passwörter und Loginnamen nach gewissen Richtlinien zu generieren. Diese Einschränkungen reichen von der Vorgabe des zu verwendenden Zeichensatzes bis zur Festlegung des zufallsgenerierten Kennwortes durch den Computer und haben stets die Steigerung der Sicherheit als Ziel. Im Interesse des Benutzers soll damit die missbräuchliche Nutzung des Accounts durch Unbefugte unterbunden und vertrauliche Daten sowie Handlungsoptionen im Verantwortungsbereich des Anwenders geschüzt werden.

Die Vielzahl vorhandener Authentifizierungsdaten samt verschiedenstartiger Restriktionen und Verhaltensvorgaben überfordern jedoch all zu oft die Fähigkeiten, das Verständnis sowie die Einsicht der Anwender und verfehlen somit ihr Ziel, die Sicherheit des Authentifizierungsprozesses zu steigern. Die Missachtung menschlicher Einflussfaktoren als wesentliches Element in der Entwicklung und Gestaltung von Sicherheits- und Authentifizierungsmechanismen führt zu einer schlechten Benutzbarkeit und gibt den Nutzern Anreize zur Umgehung vorgegebener Sicherheitsmaßnahmen. Darunter leidet sowohl die Effektivität als auch die Sicherheit des Systems. Das entwickelte System erfüllt in der Folge einen geringeren Grad an Sicherheit, als dass es durch Einbeziehung von Kenntnissen und Ergebnissen verfügbarer Usability-Analysen erreichen könnte.

Die Einbeziehung von Ergebnissen aus dem Bereich der Human-Computer-Interface Forschung ist daher ein wichtiges Element im Software-Engeneering-Prozess. Ohne die Berücksichtigung menschlicher Verhaltensweisen und Umgang kann das Funktionieren der zu implementierenden Sicherheitsmechanismen nicht gewährleistet werden. Die HCI-Forschung gibt nicht nur Aufschluss über die Gründe des Fehlverhaltens und Scheiterns klassischer Authentifizierungsmechanismen, sondern zeigt Lösungsansätze auf, diese zu beheben und das System sowohl sicherer als auch anwendungsfreundlicher zu gestalten.

2 Authentifizierungsmechanismen

Um auf Computersysteme oder digitale Dienste zugreifen zu können, ist es in der Regel notwendig, sich erfolgreich zu authentifizieren. Dieser Prozess wird überlicherweise in zwei Vorgänge unterteilt. Im ersten Schritt, der Identifizierung, gibt der Nutzer an, wer er ist. Dies erfolgt überlicherweise durch Angabe eines eindeutigen Loginnamens, einer User-ID oder Emailadresse. Anschließend erfolgt die Verifikation seiner Angaben, in welcher der Anwender seine Identität nachweist. Bei der Authentifizierung kann zwischen drei Methoden unterschieden werden:

- ...what you know: Authentifizierung mittels Wissen
  Die wissensbasierte Authentifizierung erfodert ein spezielles Wissen des Benutzer, bspw. eine PIN, ein Passwort oder die korrekte Antwort auf eine vordefinierte Frage.

- ...what you have: Authentifizierung mittels Besitz
  Die besitzbasierte Authentifizierung setzt den persönlichen Besitz eines Objektes voraus. Dabei handelt es sich gewöhnlich um Schlüssel, digitale Zertifikate oder Zugangskarten, zunehmend in Form von Chip-Karten oder mit eingesetzter RFID-Technologie.

- ...who you are: Authentifizierung mittels dem Sein
  Mit Biometrische Merkmale, insbesondere mit Methoden zum Abgleich des Fingerabdrucks, der Stimme oder der Iris wird die Identität des Anwenders überprüft.

Auf einer Meta-Ebene dieser Klassifizierung lässt sich der Kontext als Methode zur Authentifizierung heranziehen. Mittels Umgebungsinformationen, wie bspw. die verwendete IP, die Nutzung lokaler oder nur für einen eingeschränkten Personenkreis zugänglicher Ressourcen oder aber durch die Unterscheidung verschiedener Sicherheitszonen und -level ergeben sich weitere Möglichkeiten zur Authentifizierung, ohne diese klar in die ergriffene Charakterisierung von Sicherheitsmechanismen einordnen zu können. So kann gemäß der Herkunft einer Anfrage die Entscheidung für den Zugriff auf sensible Daten oder die Ausführung von Methoden und Module getroffen werden. Insbesondere im Datenbankbereich oder bei der Kommunikation von Hardwaremodulen eines Gerätes kommen diese Authentifizierungsmechanismen vermehrt zum Einsatz, aber auch im alltäglichen Bereich, wo wir beim Betreten eines Büros nicht den Ausweis des unbekannten Personals verlangen, ehe wir unser Anliegen vortragen.

Trotz vieler alternativer Authentifizierungsmöglichkeiten gehört die Überprüfung der Identität anhand wissensbasierter Merkmale zu den gebräuchlichsten Methoden. Während die besitzbasierte Authentifizierung oftmals die kosten- und aufwandsintensive Erstellung von Magnet- oder Chipkarten voraussetzt, die kaputt oder verloren gehen bzw. sogar gestohlen werden können, stellen Passwörter die am einfachsten zu implementierende Authentifizierungsmethode dar. Im Gegensatz zur Verwendung biometrischer Verfahren müssen keine technischen Geräte beschafft und installiert

werden, treten in der Regel keine Erkennungsfehler auf oder kommt es gar zu fehlerhaften Zurückweisungen. Ebenso handelt es sich bei Passwörtern nicht um veränderliche bzw. alternde Merkmale, deren Erkennung im Laufe der Zeit beeinträchtigt werden kann.

Während sich die Authentifizierung in der Biometrie grundsätzlich mit statistischen Fragestellungen auseinandersetzen muss, liefert die Überprüfung eines Passwortes stets ein eindeutiges Ergebnis. So ist bei der Überprüfung biometrischer Merkmale stets ein Abgleich gespeicherter Daten mit neu zu erfassenden Merkmalspunkten erforderlich, welcher oft durch den Einsatz optischer Sensoren bewerkstelligt wird. Sowohl bei der Erfassung der Originaldaten als auch die bei der Authentifizierung zu überprüfenden Merkmale werden dabei von technischen Geräten mit unterschiedlichem Fehlerverhalten und unterschiedlicher Varianz bei der Mustererkennung bestimmt, so dass das Resultat stets ein relativer Vergleich unter Berücksichtigung von Wahrscheinlichkeitswerten ist. Nutzerausfallraten, Falschakzeptanz, -rückweisungs, -identifikations, -match und -non-match-Raten bilden im Gegensatz zur reinen Vergleichsoperation auf die Identität zweier Zeichenfolge im Bereich wissensbasierter Authentifizierung ein komplexes, statistisches Model, das unter schlechten Bedingungen durchaus auch falsche Ergebnisse liefert. Die Performanz biometrischer Systeme ist darüber hinaus personenabhängig und hat dabei ebenso mit Erkennungsschwierigkeiten umzugehen, wie es auch im menschlichen Bereich bei der Unterscheidung von Personen ohne markante Eingenschaften vorkommt.

Passwörter können daher dazu verwendet werden, Schwachstellen alternativer Authentifizierungsmechanismen zu kompensieren und kommen daher oft in Kombination mit besitzbasierten Methoden zum Einsatz. Sowohl die Folgen des Verlustes besitzbasierter Authentifizierungsmerkmale als auch die klassischen Probleme von Passwörtern, die Möglichkeit sie unbefugt weiterzugeben, können somit effektiv eingeschränkt werden. In Anwendungsbereichen, wo hingegen höchste Zuverlässigkeit gewährt werden muss, wie sie auf Grund defekter Magnetkarten oder Biometrie mit einer statistischen Fehleranfälligkeit nicht garantiert ist, sind Passwörter unabdingbar. Das grundlegende Problem wissensbasierter Systeme stellt dabei jedoch das Vergessen sowie die Qualität bzw. Güte von Passwörtern dar, was im Folgenden unter Beachtung der HCI-Forschung analysiert wird.

3 Konstruktion sicherer Passwörter

Studien von Cheswick and Bellovin [ChBe94] aus dem Jahr 1994 bescheinigen, dass schwache Passwörter die häufigste Ursache für das Eindringen in Computersysteme darstellte. Mit der zunehmenden Vernetzung und der standardmäßigen Anbindung an das Internet entstanden eine Vielzahl neuer Angriffsmöglichkeiten und wurden ständig neue Exploits eingesetzter Software entdeckt, die Methoden zur Umgehung der Authentifizierung finden und den Zugriff auf fremde Systeme ermöglichen. Dennoch existiert das klassische Problem unsicherer Passwörter weiterhin und ist nicht

zu vernachlässigen. So stellt die Vertraulichkeit der Daten ein elementares Schutzziel bei der Konstruktion sicherer Systeme dar. Um die Vertraulichkeit zu gewährleisten und sensible Daten vor Unbefugten zu bewahren, liegt die Aufmerksamkeit der Systementwickler in der Konstruktion sicherer Authentifizierungsmechanismen.

Um die bekannte Schwachstelle wissensbasierter Authentifizierungsmethoden - unsichere Passwörter - aufzugreifen, liegt der klassische Lösungsansatz oftmals in der Erstellung von Sicherheitsrichtlinien und -empfehlungen. Darin werden grundlegende Regeln zur Konstruktion sicherer Passwörter genannt und zu vermeidende Merkmale aufgeführt. Unvorsichtiges Verhalten der Nutzer soll inbesondere durch die Aufnahme der Regeln in Benutzerordnungen oder Arbeitsverträgen vorgebeugt werden. Ergänzt bzw. realisiert werden diese Sicherheitsrichtlinien durch die Einführung technischer Maßnahmen. Mit der technischen Implementierung soll sicher gestellt werden, dass Benutzer die grundlegenden Anforderungen erfüllen und ein bestimmter Grad an Sicherheit gewährleistet werden kann. Anwender werden duch reglementive Mechanismen zur Konstruktion sicherer Passwörter aufgefordert und durch die Prüfung auf Einhaltung qualitativer Mindestanforderungen unterstützt. Die technische Umsetzung reicht dabei von Mechanismen mit rein informativem Charakter über die Zurückweisung unsicherer Eingaben bis hin zur Vorgabe computergenerierter Passwörter. Anhand trivialer Merkmale wie der Länge der Zeichenfolge, das Prüfen auf das Vorhandensein von Sonderzeichen, Ziffern oder anderen Zeichentypen wird die Qualität des Passwortes gemessen und die Einhaltung von Sicherheitsrichtlinien überprüft.

Die maximale Sicherheit eines Passwortes wird dabei unter der größtmöglichen Ausschöpfung des zur Verfügung stehenden Zeichensatzes und der erlaubten Länge erreicht. Durch die zufällige Wahl aus dem gesamten Zeichensatz ohne Einschränkungen auf bevorzugte Teilmengen verfügbarer Zeichen, entsteht das größtmögliche Spektrum gleichwahrscheinlicher Passwörter. Leider handelt es sich hierbei um eine rein ideale Annahme, die selbst bei computergenerierten Passwörtern auf Grund der schwierigen Implementierung tatsächlicher Zufallszahlen nicht erreicht werden kann. Bleibt dem Nutzer die Wahl seines Passwortes selbst überlassen, so liegt die bestmögliche Sicherheit nicht zwangsläufig in der Verwendung zufallsgenerierter Kennwörter [Jian00]. Studien haben gezeigt, dass Passwörter basierend auf Abkürzungen einprägsamer Sätze, so genannter Passphrases, den gleichen Grad an Sicherheit gewährleisten. Da als Grundlage des Passwortes jeder beliebige Satz verwendet werden kann, in dem bereits genügend viel Sonderzeichen vorkommen können und Klein und Großschreibung in der Regel variieren, weist die Gestalt des erstellten Passwortes gleichermaßen zufälligen Charakter auf. Durch Häufigkeitsanalysen [Zepp06] im Hinblick auf die Sprachherkunft des gewählten Satzes kann im Gegensatz zu vollkommen zufällig gewählten Kennwörter die Menge der in Frage kommenden Passworte eingegrenzt werden. Der im Vergleich zu klassischen Kennworten erzielte Zuwachs an Sicherheit erfüllt in der Regel alle Anforderungen gängiger Sicherheitsrichtlinien.

In einer Vielzahl gängiger und ähnlichlautender Empfehlungen [Corp06] werden die grundlegenden Details zur Gestaltung sicherer Passwörter genannt. Eines der

wichtigsten Kriterien ist die Länge des Kennwortes: Je einfacher ein Passwort aufgebaut ist, desto länger sollte es im Allgemeinen sein. Zweiter wesentlicher Einflussfaktor ist die Verwendung möglichst vieler Zeichenklassen, wie Abbildung 1 verdeutlicht. So sollte das Passwort aus einer Kombination von Buchstaben, Ziffern und Sonderzeichen bestehen, während Buchstaben sowohl in Klein- als auch Großschreibweise auftreten sollten. Insbesondere die Verwendung von ASCII-Zeichen, die nicht auf der Tastatur abgebildet sind, führt zur wesentlichen Steigerung der Sicherheit des Passwortes, sofern sie als Eingabe zugelassen sind. Durch die Kombination verschiedener Zeichentypen wird die Basis der enstehenden Kombinationsmöglichkeiten erweitert und führt zu einer Erhöhung der möglichen Passwörter. Mit zunehmender Länge wird es Angreifern dabei erschwert, Kennwörter duch Ausprobieren aller in Frage kommender Kombinationen (Brute-Force-Angriff), indem erheblich mehr Rechenzeit erforderlich wird.

Abbildung 1: Erforderliche Rechenzeit zur Ermittlung von Kennwörtern - Verwendete Länge

Zu vermeiden sind hingegen in Wörterbücher aufgeführter Begriffe, Namen von Personen, Tieren und anderen Objekten sowie die Verwendung persönlicher Benutzerdaten. Auch Begriffe ausländischer oder fremdsprachiger Objekte sind keine geeigneten Bestandteile von Kennwörtern und mindern deren Sicherheit. Mit kostenlos verfügbaren Wörterbuch- und Namenslisten können derartig konstruierte Passwörter in angemesener Zeit automatisiert herausgefunden werden. Ein aktuelles Beispiel hierfür liefert die vor wenigen Tagen veröffentlichten Zugangsdaten ca. 100 000 Benutzer eines Internet-Flirtportals [?]. Eine Analyse der Passwortliste zeigte, dass ca. 2,5 Prozent der Passwörter mit '1234' begannen. Als auffällig stellte sich der starke Themenbezug der ermittelten Kennworte und die Verwendung von Markennamen, Sportvereinen und Jahreszahlen heraus. Das Anhängen von Ziffern oder Verändern einzelner Zeichen gleicht den durch die Verwendung von Namen eingetretenen Verlust an Sicherheit jedoch nicht aus. Redundanzen und mehrfach vorkommende Zeichen reduzieren gleichermaßen die Sicherheit wie Eingabemuster oder Eingabefolgen naheliegender Tasten. Passwort-Crack-Programme sind darauf eingerichtet, diese Kombinationen bevorzugt zu testen, da deren Verwendung dem Verhalten vieler Nutzer entspricht. Auch der Austausch ähnlichaussehender Symbole gehört zu den bekannten Maßnahmen und Verhaltensweisen der Anwender und führt daher ebenso wenig zu Steigerung der Passwortqalität. Warum die Wirkung dieser Ansätze nicht das erhoffte Ergebnis erreicht, zeigt sich bei der Analyse bekannter Programme zur Ermittlung eingesetzter Passwörter, wie LC5 oder 'John the Ripper' [Proj].

Die oftmals als Schikane wirkenden, grundlegenden Gestaltungsregeln finden ihre Begründung in den Methoden von Programmen zum Angreifen passwortgeschützter Systeme. Von diesen werden in erster Instanz Listen gängiger Benutzer- sowie Vornamen als auch fach- und sprachspezifische Wörterbücher eingesetzt, um häufig

verwendete Kennwört automatisiert zu testen. In einem weiteren Durchlauf werden diese Wörter permutiert, Ziffern und Sonderzeichen vorangestellt bzw. angehängt, Groß- und Kleinschreibung variiert und ähnlich aussehende Zeichen, wie @ und a, i und !, l und 1, o und 0, etc. substituiert. An Stelle von Wörterbüchern werden ebenso Abkürzungsverzeichnisse und Passphrase-Sammlungen verwendet, um übliche oder bekannte Zitate, Aphorismen und Sprüche als Basis von Passwörter herauszufinden. So mögen Passphrasen deutlich sicherer als gewöhnliche Passwörter sein und sich mit der Qualität zufallsgenerierter Kennwörter messen können, doch nur unter Vermeidung von Abkürzungen und Variationen bekannter Sätze wie 'an apple a day keeps the doctor away'. Passwörter nach diesem Schema sind daher nur bedingt eine sichere Alternative. In der letzten Instanz gehen die Programme dazu über, Brute-Force-Attacken auszuüben, in welchen jede erdenkliche Zeichenkombination getestet wird.

Der Zeitaufwand für die Methoden zum Auffinden schwacher Passwörter hängt dabei entscheidend von der Länge des Passwortes sowie dem verwendeten Zeichensatz ab. Gilt es bei einem fünfstelligen, kleingeschriebenem Wort 265 Möglichkeiten, also ca. 11,8 Millionen Kombinationen, auszuprobieren, so sind es bei einem achtstelligem, alphanumerischen Wort bereits 2,8 Billionen zu testende Zeichenfolgen. Trotz der imens groß wirkenden Zahlen sind diese Passwörter bereits mit der aktuellen Rechnerkapazität in wenigen Sekunden [Shaf00], im letzten Fall innerhalb weniger Monate, zu ermitteln. Dieses kleine Rechenexample sowie Abb. 1 und 2 demonstrieren die zunehmende Bedeutung langer und komplexer Passwörter. Studien von Robert Morris und Ken Thompson im Jahre 1979 über die Sicherheit von Passwörtern [Klei90] erkannten bereits früh diese Problematik und stellten fest, dass mehr als jedes sechste Passwort drei oder weniger Zeichen enthielt. Weitere Studien von Daniel Klein zur Verbesserung der Sicherheit von Kennwörtern ergaben 1990 dass ein Viertel aller Passwörter bereits mit einem kleinen Wörterbuch zu ermitteln sind. Dazu testete Klein fast vierzehn tausend Accounts mittels Wörterbüchern unterschiedlicher Thematik und ermittelte 24.2% der Kennwörter. Zugleich erstellte Klein anhand der gecrackten Passworte eine Statistik, in der er feststellte, dass ein Drittel aller Passwörter sechs Zeichen umfassen, die Hälfte sieben oder acht Zeichen lang sind.

Abbildung 2: Erforderliche Rechenzeit zur Ermittlung von Kennwörtern - Verwendete Länge

Bemühungen seitens Systementwickler gehen daher in die Richtung, diese üblichen und bekannten Mängel des wissensbasierten Authentifizierungsmechanismus durch technische Implementierungen und Überprüfungsroutinen zu beheben. Mit erzwungenen, regelmäßigen Änderungen des Passwortes soll Angreifern zudem die Möglichkeit genommen werden, Passwörter durch Brute-Force-Angriffe über längere Zeiträume hinweg auszuprobieren, indem die Gültigkeit auf wenige Wochen oder Monate begrenzt wird. Sofern die Benutzer des Systems nicht dazu übergehen, Va-

riationen ihrer alten Passwörter zu verwenden oder nur zwischen festgelegten Kennwortalternativen wechseln, erhält der Angreifer bei geeigneten Aktualisierungsintervallen trotz erfolgreicher Dechiffrierung nur ungültige Kennwörter. Die Zeitpunkte zur erforderlichen Kennwortänderungen müssen entsprechend kurz gewählt werden, so dass die Berechnungsdauer für die Durchführung genannter Attakierungsmöglichkeiten nicht zur Nutzung entdeckter Kombinationen ausreicht. Da diese wie gezeigt von der Komplexität und Qualität des Passwortes abhängt, steht die Wahl der Gültigkeitsdauer im engen Verhältnis geltender Sicherheitsrichtlinien.

Passwort-Histories verhindern das Risiko kompromitierter Passwörter, indem die erneute Nutzung bereits verwendeter Kennwörter unterbunden wird. So soll es Anwendern nicht möglich sein, das identische Kennwort im Zuge einer Änderung erneut zu verwenden. Die Länge der History muss dabei groß genug gewählt werden, um die Nutzer an der vorsätzlichen Umgehung dieses Mechanismuses zu hindern. Ist sie hingegen zu kurz eingestellt, so tendieren einige Anwender dazu, ihr Passwort entsprechend oft zu ändern, bis das bereits genutzte Passwort nicht mehr in der History aufgeführt und für die weitere Verwendung freigegeben wird. Intelligente Sicherheitssysteme fangen in diesem Zuge 'verwandte' bzw. ähnlich konstruierte Passwortkombinationen ab. So sollen Sequenzen wie 'geheim_Mai', 'geheim_April', ... abgefangen und zurückgewiesen werden, die im Falle eines kompromitierten Passwortes einfach zu erraten sind. Variationen von Passwörtern werden somit abgewiesen und zwingen zur tatsächlich Neukonstruktion der Kombinationen, wie es von den Sicherheitsrichtlinie beabsichtigt ist

Die Konstruktion sicherer Passwörter kann somit weitgehend auf die Einhaltung standardmäßiger Sicherheitsmerkmale reduziert und technisch leicht integriert werden. Das Grundschutzhandbuch des Bundesamt für Sicherheit in der Informationstechnik nennt dazu wesentliche Eigenschaften [Info]. Ebenso lässt sich mit den genannten Anforderungen ein Mass für die Sicherheit bzw. Qualtiät von Passwörter bestimmen, welche neben der Implementierung als regulative Mechanismen auch als Qualitätsanzeige mit rein informativen Charakter denkbar sind. Auf zahlreichen Registrierungsseiten des Internets sowie in lokalen Programmen finden sie bereits Anwendung und unterstützen die Eigenverantwortung des Nutzers.

4 Nutzerverhalten

4.1 Bedeutung in der Entwicklung sicherer Systeme

Mit den beschriebenen Mechanismen zur Gestaltung sicherer Passwörter werden dem Anwender restriktive Vorgaben aufgebürdet, die es ihm schwer machen, ein gutes Passwort zu erstellen. Während die meisten Regeln erläutern, was bei der Wahl des Passwortes zu berücksichtigen ist, bleibt das ẅieïn der Regel unerklärt. Der Nutzer muss sich daher mit der Menge technischer Einzelregelungen zurecht finden, ohne konkrete Methoden zur Konstruktion genannt zu bekommen. So kann es vorkommen, dass Vorschläge bzw. Angaben des Nutzers mehrmals zurückgewiesen werden,

da er die Vielzahl und das Zusammenwirken zu berücksichtigender Merkmale nicht mehr überschauen kann. Die Wahl des Passwortes resultiert damit oftmals in einer schlecht zu merkenden Zeichenfolge und wird kurzerhand vergessen. Dies geschieht insbesondere bei der Festlegung unveränderbarer Passwörter durch das System. Als Folge der schlechten Benutzbarkeit sicherer Passwörter, werden diese notiert und in zugänglichen Bereichen aufbewahrt. Damit werden die strikten Sicherheitsbemühungen durch das Verhalten der Benutzer unterwandert; die sinnvoll erachteten Maßnahmen zur technischen Umsetzung der sicheren Authentifizierung erzielen das entgegengesetzte Ziel und machen das System verwundbarer. Für Systemdesigner ist daher unerlässlich, das Verhalten der Nutzer in die Gestaltung sicherer Systeme mit einzubeziehen. Ohne die menschlichen Einflussfaktoren und Beweggründe zu analysieren und gebührend zu berücksichtigen, können die Folgen technischer Maßnahmen nur schwer abgeschätzt und prognostiziert werden. Zumal Angreifer passwortgeschützer Systeme die Bedeutung des Nutzerverhaltens bei der Entwicklung geeigneter Tools frühzeitig erkannt und aufgegriffen haben, entstehen durch das Ignorieren der menschlichen Komponente im Umgang mit dem vermeintlich sicheren System gravierende Mängel.

4.2 Umgang mit Passwörtern in der Realität

Bleibt die Wahl des Passwortes dem Benutzer überlassen, so bescheinigen Studien von A. DeAlvare [DeAl90], dass Nutzer dazu tendieren, so wenig wie mögliche Zeichen zur Erstellung zu verwenden. Problematisch ist dies insbesondere auf Grund DeAlvares Feststellung, dass ein gewähltes Passwort nur widerwillig geändert wird, ehe es als kompromitiert nachgewiesen wurde [DeAl88]. Besonders Aufschreiben von Passwörtern stellt ein signifikantes Problem dar. Nach Umfragen von Anne Adams und Martina Sasse [AdSa99] macht eine große Mehrheit der Anwender von dieser Vorgehensweise Gebrauch, wobei es sich sowohl um gewöhnliche Anwender als auch Experten oder Teilnehmer von speziellen Sicherheitsschulungen handelt. Dabei erhielten Adams und Sasse Angaben, die ihnen erlaubten die Personengruppen weiter zu klassifizieren. Während einige Nutzer strikt alle verwendeten Passwörter notieren, konnten sie weitere Nutzergruppen differenzieren, die ihre Kennwörter nur für den anfänglichen Gebrauch niederschrieben bis sie auswendig erlernt wurden oder aber nur selten genutzte Passwörter notiert wurden. Teils werden dazu selbst ausgedachte Schemen zur Verschlüsselung angewendet, wie PINs beispielsweise als Telefonnummer im Adressbuch zu vermerken oder weitere zufällig gewählte Ziffern anzuhängen. Weitere Ergebnisse der Befragung zeigten, dass Anwender oftmals das selbe Passwort zur Authentifizierung verschiedener Systeme verwenden. Während die Befragten in bis zu 50 verschiedenen Situationen zur Eingabe von Passwörter aufgefordert werden, stehen diesen nur eines bis maximal sieben unterschiedliche Passwörter gegenüber, welche zudem in der Regel Variationen eines einzelnen Ausgangswortes darstellten.

Entgegen eindeutiger Empfehlungen von den Entwicklern sicherer Authentifizierungsmethoden verwenden Benutzer nach Adams und Sasses Erkenntnissen überwiegend Kennwörter mit einer persönlichen Bedeutung. Telefonnummern, Lieblingsfilme

und Namen aus dem Bekanntenkreis oder der Familie gehören zu den gebräuchlichsten Passwörtern. Die Missachtung der eindeutigen Regeln und Vorgaben zur Konstruktion sicherer Passwörter erfolgen nicht selten auch von Teilnehmern spezieller Sicherheitsseminare und werden trotz intensiver Aufklärung und Belehrung als unpraktikabel zurückgewiesen. Als durchschnittliches Passwort identifizierten Adams und Sasse die Wahl einer sechs Zeichen langen Buchstabenfolge gefolgt von zwei Ziffern. Einige ausländische Benutzer bedienen sich bei der Erstellung ihrer Passwörter vorzugsweise ihrer Muttersprache, die sie angesichts englischsprachiger Wörterbuchattacken als sicher betrachten.

Im Allgemeinen stellten Adams und Sasse fest, dass Anwender nur die notwendigsten Bemühungen aufbringen, die von Systemen durch die Verwendung sicherheitsrelevanter Einschränkungen vorausgesetzt werden. Erforderliche Änderungen des Passwortes auf Grund begrentzter Gültigkeit haben meist nur den Einsatz einer Variation alter Passwörter zur Folge und verhindern damit den beabsichtigten Effekt, das System durch neue Kennwörter sicherer zu gestalten. Gerade bei Systemen, die zur regelmäßigen Änderung des Passwortes zwingen, entwickeln Benutzer häufig ihre eigenen Strategien oder Schemata zur Erstellung 'verwandter' bzw. ähnlicher Passwörter. Das Anhängen von Ziffern für den aktuellen Monat oder die Version bzw. Nummer des Passwortes gehört zur gebräuchlichsten Vorgehensweise.

Das Erinnern an Kennwörter, deren Einsatz oder sogar Verlust betrachten alle Teilnehmer der Umfrage als sehr problematisch. Einhergehend äußern viele Anwender den Wunsch [AnLu97], die Sicherheit des Systems zu reduzieren. Dennoch spricht sich die Mehrzahl der Benutzer gegen die Verwendung alternativer Authentifizierungsmechanismen aus, die mit neuen und schwieriger zu umgehenden Problemen verbunden werden. Während sich der Verlust des Passwortes durch Notieren einschränken lässt und Bemühungen zum Erlangen neuer Anmeldedaten verhältnismäßig gering sind, befürchten die meisten Benutzer die Folgen des Verlusts von Authentifizierungskarten oder Unzuverlässigkeit biometrischer Systeme. Ebenso verhindern alternative Mechanismen meist, Benutzerkonten gemeinsam zu benutzen, was viele Anwender als eine übliche und gängige Maßnahme betrachten und entgegen gewöhnlicher Nutzerbedingungen ausüben. Mitarbeiter eines Unternehmens machen ihre Passwörter Kollegen daher unbedacht bekannt, unter dem Kontext einer gemeinsamen Arbeitsleistung, Teamarbeit und dem Austausch von Informationen und Ergebnissen. Eigene, geheime Passwörter werden deshalb als unpraktikabel und hinderlich bei der Zusammenarbeit an gemeinsamen Projekten betrachtet, die zusätzliche Hürden erstellen und die Effizienz der Arbeit mindern.

Das tatsächliche Verhalten der Nutzer resümiert, steht es daher im krassen Gegensatz zur Empfehlung sicherer Passwörter und Implementierungen von Authentifizierungsmechanismen. Aufgestellte Regeln sowie Überlegungen zur Steigerung der Sicherheit werden in der Praxis kaum befolgt und durch best-practice-Erfahrungswerte ersetzt. Damit wird oftmals das Ziel verfolgt, den workflow durch p̈raxisgerechtenËinsatz von Passwörtern zu optimieren - die sicherheitsrelevanten Anforderungen bleiben dadurch jedoch zurück. Doch nicht nur die Konstruktion

der Passwörter, sondern auch die bereitwillige Angabe vertraulicher Daten oder sogar des Passwortes selbst sind keine Seltenheit. So gelingt es bereits durch direktes Fragen, Zugangsdaten in Erfahrung zu bringen [MaWe01]. Moderne Methoden automatisieren diesen Prozess in Form von Pishing, indem Informationen nicht mehr gezielt erfragt werden, sondern der Erfolg durch die Vielzahl angeschriebener Nutzer entsteht. Auch diese Schwachstellen sind bei der Konstruktion sicherer Systeme zu berücksichtigen, um die Vertraulichkeit der Daten und das Funktionieren der Zugangsmöglichkeiten zu gewährleisten.

4.3 Ursachen unsicherer Verhaltensweisen

Der durchschnittliche Anwender muss sich heutzutage mit der Verwaltung einer Vielzahl von vertraulichen Accountdaten und -informationen beschäftigen. Im beruflichen sowie im privaten Bereich steigen die teils obligatorischen Möglichkeiten, Tätigkeiten mittels computergestützten Systemen zu erledigen. Trotz der beabsichtigten und oftmals einhergehenden Effizienzsteigerung durch das Tranferieren alltäglicher Prozesse in digitale und bequem vom privaten Arbeitsplatz nutzbarer Dienste, entsteht dem Nutzer zusätzlicher Aufwand durch den Umgang mit verschiedenen Authentifizierungsmechanismen. Durch die steigende Zahl an Authentifizierungsdaten und verschiedensten Bedingungen und Restriktionen bei der Wahl des Passwortes, wird die Fähigkeit des Anwenders überschritten, sich all diese unter Einhaltung von Sicherheitsvorschriften und -empfehlungen zu merken. Als Resultat werden Kennwörter sogar von Anwender mit entsprechender Schulung und Sicherheitstrainings sowie Sicherheitsexperten notiert, wie Studien von Adams und Sasse [AdSa99] zeigten.

4.3.1 menschlichen Fähigkeiten

Grund für dieses Verhalten stellen u.a. die erforderlichen, technischen Merkmale zur Gestaltung sicherer Passwörter dar, die den menschlichen Fähigkeiten und Verhaltensweisen entgegenstehen. Während sich der Nutzer schwer tut, sich an bedeutungslose Dinge zu erinnern, handelt es sich gerade dabei um eine sehr wichtige Eigenschaft für die Konstruktion von Passwörtern. Schließlich sollen diese eine möglichst zufällige Zusammenstellung von Zeichen darstellen und nicht in einem Wörterbuch zu finden sein. Des weiteren basiert die menschliche Erinnerungsfähigkeit auf sich wiederholende Dinge und Ereignisse. Passwörter sollen hingegen ohne Redundanzen und mehrfachkommende Zeichen konstruiert werden und sich mit einmaligem Charakter komplett von anderen Kennwörtern unterscheiden. Ferner müssen Passwörter in der Abfolge ihrer Zeichen ohne Anhaltspunkte korrekt wiedergegeben werden, während dem menschliche Gedächtnis die unstrukturierte Rekonstruktion leichter fällt.

Die Fähigkeit, sich an Passwörter zu erinnern hängt jedoch nicht unbedingt vom Leistungsvermögen des einzelnen Nutzers ab. Die Häufigkeit des Gebrauchs übt wesentlichen Einfluss auf das Erinnerungsvermögen des Passwortes aus. So wird bei häufigem Gebrauch das Eingeben des Passwortes zur Routine und führt dazu, dass der Benutzer sich oftmals gar nicht mehr bewusst an den genauen Inhalt erinnern

muss, sondern das Wort automatisch eingeben kann. Erzwungene Änderungen abgelaufener bzw. begrentzt gültiger Passwörter verhindern diesen Effekt jedoch. Während das Gedächtnis nicht auf Befehl alte Passwörter vergessen kann, müssen neue Kennwörter, meist umgehend oder zumindest kurzfristig ausgedacht und eingeprägt werden. Daher werden neue Passwörter oftmals aufgeschrieben oder entstehen durch Variieren bereits bestehender Wörter. Die Vielzahl von Passwörtern aber auch Variationen ähnlich konstruierter Zeichenfolgen verwirrt den Nutzer zusätzlich und führt damit erst recht zur geringeren Fähigkeit, sich Passwörter auswendig zu behalten [Wick92]. In der Folge werden einfachere Passwörter konstruiert, die sich sowohl vom Anwender besser einprägen lassen als auch von Angreifern leichter zu ermitteln sind.

4.3.2 Einsicht und Verständnis der Nutzer

Jedoch nicht nur die Fähigkeiten, sondern auch die Einsicht der Nutzer spielt eine entscheidende Rolle im Umgang mit Passwörtern. So befolgen Nutzer, trotz intensiver Bemühungen der Systemadministratoren mittels Schulungen, Aufklärung und Trainingsprogramme oder auch bloßer Empfehlungen und Regeln bewusst nicht die geforderten Merkmale. Teils fühlen sich die Teilnehmer dieser Seminare schlichtweg nicht von der Problematik betroffen Wahrnehmung der Sicherheit und haben sehen daher keinen Anlass, sich die tägliche Arbeit durch Verwendung komplexerer und schwerer zu merkenden Kennwörter zu erschweren. Andere Mitarbeiter betrachten ihre Rolle widerrum nicht als sicherheitsrelevant und gehen davon aus, dass ihre Passwörter keinen oder nur geringen Einfluss auch die Sicherheit des Gesamtsystems hat. So sind im Extremfall sogar unsichere Standardeingaben wie 'passwort', 'test' oder '123' vorzufinden, die trotz ihres offensichtlichen Mangels an Sicherheit in vielen Systemen von unaufgeklärten oder aber uneinsichtigen Nutzern verwendet werden.

Die Ursache liegt zudem in der meist zeitaufwendigen Wiederherstellung der Zugangsdaten, wozu der zuständige Systemadministrator kontaktiert und informiert werden muss. Dies ist oftmals nur innerhalb bestimmter Zeiten möglich und verursacht bei bürokratisch organisierten Unternehmen einen hohen Overhead, da sowohl die Arbeitszeit des Systemtechniker als auch der eigene Arbeitsausfall Folge der vergessenen Zeichenkette ist. Dies sowie der verbundene Prestigeverlust und Erklärungsnot des Anwenders, ist den Benutzern eine ausreichende Begründung für die Niederschrift ihrer Kennwörter.

Das Zusammenwirken von Authentifizierungsmethoden mit der praktischen Arbeitsweise der Mitarbeiter gibt weiteren Aufschluss über die Akzeptanz oder Ablehnung implementierter Maßnahmen. Die Organisation, insb. die Unterscheidung der Arbeitsweise, haben großen Einfluss auf den vorgeschriebenen Umgang mit Passwörter. So sind individuelle Passwörter ungeeignet für Teamarbeiten und werden oftmals mit Gruppenmitgliedern getauscht um den erforderlichen Informationsaustausch zu fördern. Die Sicherheitstechnischen Vorgaben werden hingegen als inkompatibel mit der zu erledigenden Arbeit betrachtet.

Während die Umsetzung der Sicherheitsregelungen im militärischen Bereich auf Grund der straffen Befehlsstruktur problemlos realisierbar ist, werden sie modernen Arbeitsweisen im Dienstleistungssektor nicht gerecht. Die Einführung von Richtlinien und Vorschriften müssen den Benutzern daher erläutert und begründet werden (need-to-know principle), um auf Akzeptanz zu stoßen. Ohne die Erklärung der möglichen Konsequenzen kompromitierter Passworte, fehlt den Nutzern andernfalls das Verständnis für den Mehraufwand durch die Verwaltung sicher Kennwörter.

4.3.3 Kenntnisstand & Kommunikation

Das aufgezeigte Unverständnis resultiert dabei aus mangelnder Kenntniss über die Erfordernis der aufgestellten Regeln. So identifizieren Adams, Sasse und Lunt in ihrer Studie [AnLu97] fehlende Kommunikation zwischen Systemadministration und Anwendern als Ursache unsicherer Verhaltensweise. Von den Entwicklern des Systems werden oftmals Bedürfnisse und Anforderungen der Benutzer übersehen oder ungenügend beachtet. Damit müssen sich Anwender ihren eigenen Weg finden, sich mit Authentifizierungsmechanismen auseinanderzusetzen und finden diese oftmals in der Umgehen von Sicherheitsrichtlinien.

Zwar wird den Nutzern üblicherweise die Wahl des eigenen Passwortes zugestanden und ihnen somit Verantwortung für die Sicherheit zugetragen, doch werden ihnen kaum Informationen über die Funktionsweise der Sicherheitsmechanismen vermittelt, was in einem fehlenden Basiswissen resultiert. Anwender absichtlich über die Sicherheitsmaßnahmen in Unkentniss zu lassen, um ihnen möglichst wenig Einblick und Angriffspotential zu gewähren, erzielt jedoch geringere Sicherheit. Die Ursache hierfür sehen Adams, Sasse und Lunt auch in der zentralen Organisation des Usermanagements, die Distanz zwischen Administratoren und Anwendern schafft und somit für geringen Kontakt verantwortlich ist.

Der Grund des Fehlverhaltens liegt damit nicht allein auf der Seite der Anwender [Patr02], sondern basiert auf unzureichender Schulung der Mitarbeiter, die oftmals auf die notwendigsten Sicherheitsmerkmale reduziert wird und hauptsächlich technische Details, kaum aber Ursachen, Konsequenzen und das Umfeld der Maßnahmen erläutert. Damit verfügen Mitarbeiter nicht über grundlegende Kenntnisse und können auch kein Verständnis für die auferlegten Einschränkungen entwickeln.

4.3.4 Wahrnehmung der Sicherheit

Einhergehend mangelnder Aufklärung und Schulung, ist vielen Benutzern nicht bewusst, dass Passwörter mittels Wörterbuchatacken erraten werden können und zeigen sich verwundert darüber, wie eine fremde Person auf den Namen des Haustieres oder das Geburtsdatum eines Verwandten kommen soll. Ebenso sehen viele Anwender, ohne speziell vermittelten Kentnissen, den Benutzernamen als eine andere Form des Passwortes, da dieses häufig als kryptischer String vergeben wird oder User-IDs verwendet werden.

Die Wahrnehmung der User über den Einsatz und ihr Mitwirken an der Sicherheit des Systems ist damit ein weiterer wichtiger und zu untersuchender Aspekt im Umfeld der Systemsicherheit. Viele Anwender fühlen sich von der Problematik nicht betroffen, da sie keine direkten Erfahrungen mit Bedrohungen und Schwachstellen in der Sicherheit des Systems gemacht haben. Ohne das Feedback der Systemverwaltung über eingetretene Vorfälle und der Auswirkung von Schwachstellen auf das System, bezeifeln viele Nutzer die Wichtigkeit der Maßnahmen und erstellen ihr eigenes Bild im Umgang mit Sicherheit. Der Gund liegt in der Tatsache, dass die Benutzer in der Regel nicht über versuchte oder sogar erfolgte Angriffe informiert werden und keine Kenntnisse über sicherheitsrelevante Vorgänge erhalten. Ohne eine solche klare Rückmeldungen und Mitteilungen gehen Nutzer von der bestehenden Sicherheit des Systems aus und fühlen sich nicht motiviert, ihr Verhalten zu ändern und halten die Verwendung unsicherer Passwörter weiterhin für ausreichend. Die Information über das Stattfinden von Angriffen und die Bedrohung durch bestehende Schwachstellen wirkt sich damit direkt auf das Verhalten der Benutzer aus.

Ebenso spielt die Bedeutung des zu schützenden Systems sowie die Wichtigkeit und Vertrauenswürdigkeit der Daten eine entscheidende Rolle in der Verhaltensweise der Anwender. So messen einige Benutzer dem System mindere Wichtigkeit zu und stufen die ergriffenen Sicherheitsanforderungen als übertriebene Maßnahme ein. Die zu schützenden Daten werden als unbedeutend betrachtet oder sind es den Benutzern oftmals nicht wert, die mit der Steigerung der Sicherheit verbundenen Bemühungen und Einschränkungen im täglichen Arbeiitsablauf dafür einzugehen [AnLu97] (Information sensitivity). Da sie die vom System verarbeiteten Informationen als unwichtig ansehen, verstehen sie nicht den Aufwand und die Sorge um die Absicherung dieser Daten.

Verstärkt wird dieses Verhalten wenn das zu grundeliegende Datenverarbeitungssystem nur über einen geringeren Sicherheitsgrad verfügt. Strauss und Corbin fanden in Studien 1990 heraus, dass Nutzer im geringen Sicherheitsstand des Systems geringe Vertrauenswürdigkeit der Daten interpretieren und sich daher nicht veranlasst sehen, ihr persönliches Passwort geheim zu halten. Das Verhalten der Administratoren kann dafür ebenso massgeblich sein, indem Benutzer bei der Hilfestellung durch Systemtechniker nach Passwörtern gefragt werden oder diese sogar nur mit deren Kenntnis erstellt und geändert werden können. Dadurch entsteht der Eindruck, vertrauenswürdigen oder verantwortungstragenden Mitarbeiter dass Passwort mitteilen zu dürfen und trägt zu einem unbedachteren Umgang mit Passwörtern bei. Teilweise betrachten die Anwender ihr Verhalten selbst als unsicher und folgern somit auf die Unsicherheit des gesamten Systems, was sie widerum demotiviert, ihr Passwort sicher zu gestalten [AnLu97].

Sind die Sicherheitsstandards in der subjektiven Perspektive der Anwender widerum zu hoch, führt dies ebenfalls zu fahrlässigem Umgang mit Sicherheitsmechanismen. Angesichts strikter Vorkehrungen halten die Nutzer den unbedachten Umgang mit Passwörtern zu Gunsten komfortablerer und effizienterer Arbeiten am System für vertretbar, da die greifenden Sicherheitsanstrengungen wohl schon für

die Absicherung des Systems sorgten. Sasse, Brostoff & Weirich erforschten weiterhin [MaWe01], dass manche Benutzergruppen sich zu wichtig für die Verwendung von Passwörtern oder anderer Formen kontextloser Authentifizierungsmechanismen halten. Geschäftsführende Personen oder leitende Angestellte verlangen häufig von Systemtechniker die automatische Abwicklung dieses Prozesses, delegieren diese Verfahren an ihr Sekretariat oder verzichten vollständig auf die Benutzung dieser als unwichtig betrachteten, zeitintensiven Vorgänge.

5 Verbesserung der Anwenderfreundlichkeit

Mit den vorgestellten Maßnahmen zur Konstruktion sicherer Passwörter ist es möglich die Güte der Kennworte sicherzustellen und ein Mindestmas an Sicherheit zu gewährleisten. Sie scheitern im praktischen Einsatz jedoch auf Grund ihrer geringen Anwenderfreundlichkeit, durch die sich Benutzer zur Umgehung der eingeführten Mechanismen gezwungen fühlen. Dafür stehen zahlreiche Indikatoren wie das Aufschreiben von Passwörtern, die Rücksetzungsquote und -anfragen bei Administratoren, die Anzahl fehlgeschlagener Anmeldeversuche oder die Verwendung von Abspeicherungsoptionen, Identitäts- und Passwortmanager. All diese Dinge weisen auf die schlechte Benutzbarkeit und Probleme im Umgang mit Passwörtern hin.

Dennoch verfolgen wir das Ziel, nicht den Authentifizierungsmechanismus zu wechseln, sondern den Umgang mit Passwörter leichter und benutzerfreundlicher zu gestalten. Dazu müssen die Mechanismen zur Erstellung sicherer Passwörter auf die Bedürfnisse der Benutzer eingehen und den Verhaltensweisen angepasst werden. So wird ein benutzbares Passwort dadurch erreicht, Methoden zur Erstellung merkbarer Passwörter einzuführen, Restriktionen auf ein notwendiges Minimum abzubauen und Anwender durch bessere Instruierung, die Gestaltung sicherer Passworte zu erleichtern. Passwörter sollten den Arbeitsbedingungen angepasst sein und die Authentifizierung - insbesondere mit verschiedenen Zugangsdaten - nur dann erfolgen, wenn sie auch tatsächlich notwendig ist.

Der wesentliche Ansatz bei der Konstruktion anwenderfreundlicher Passworte, liegt in der Schulung und Aufklärung der Anwender durch engeren Kontakt und verbesserter Kommunikation. Die Gestaltung sicherer als auch benutzbarer Authentifizierungsmechanismen setzt eine bessere Zusammenarbeit von Systembetreuer und Benutzer voraus. Nur so können Anwendern, Ratschläge eingehend erklärt und für mehr Verständnis gesorgt werden. Ein zentrales Anliegen ergibt sich aus dem Ziel, den Benutzern nicht nur Verantwortung für sicherheitsrelevante Vorgänge zu übertragen, sondern sie über die Auswirkungen ausführlich zu informieren. Das Bewusstsein für die Notwendigkeit als auch der Sinnhaftigkeit der Maßnahmen soll hergestellt werden, um ein positives Mitwirken der Anwender überhaupt zu ermöglichen.

Grundlegende Ansätze technikbasierter Art werden in einer Reihe konkreter Vorschläge und technischer Standards des amerikanischen 'Institute of Computer Sciences and Technology' beschrieben [Publ85]. Die aufgeführten Regeln wurden bereits 1985 entwickelt und werden in neueren Empfehlungen [Info] ebenso aufgegriffen.

Unter anderem werden Maßnahmen angeraten, um die Zuordnung erfolgter Prozesse einzelnen Nutzern zuordnen zu können. Das Teilen von Accounts mit anderen Personen, inbesondere die Einführung von Gruppenaccounts, soll vermieden werden, um die Verantwortung für die Verwendung des Accounts zu konkretisieren. Ferner sollen Nutzer nicht dazu motiviert werden, Passwörter anderen Mitarbeiter mitzuteilen und die Wichtigkeit der zu schützenden Daten damit hervorgehoben werden. Teamarbeit muss durch die Bereitsstellung entsprechender Mittel und Programme zum Austausch von Informationen und Unterstützung gemeinsamer und paraleller Vorgänge bewerkstelligt werden und dürfen nicht, wie in der Praxis gerne umgesetzt, über die Weitergabe von Zugangsdaten erfolgen. Der eigene Verantwortungsbereich soll klar erkennbar sein und von den Aktionen anderer Benutzer abgegrenzt werden, zur Schaffung eines höheren Sicherheitsbewusstseins.

Hilfestellungen bei der Konstruktion von Passwörtern bewirken die Anwenderfreundlichkeit zu erhöhen. Mit persönlichen Anweisungen und dem Vorführen guter sowie negativer Beispiele, kann dem Benutzer besser beigebracht werden, sichere und zugleich erinnerungsfreundliche Passwörter zu erstellen. Besonders geeignet ist in diesem Fall die Erläuterung von Passphrases. Mit Tools zur Messung der Güte des Passwortes kann der Benutzer die Sicherheit überprüfen und unterschiedliche Kombinationen testen und vergleichen. Zugleich sollten die Menge erforderlicher, verschiedener Passworte auf die minimale Zahl notwendiger Kennworte reduziert werden. Diese dürfen daher jedoch nicht zueinander in Beziehung stehen. Damit wird erreicht, dass anstelle vieler unsicherer Passwörter eine überschaubare Anzahl qualitativer Kennworte verwendet wird, was der Erinnerungsfähigkeit sowohl durch die geringere Anzahl als auch die Vermeidung irritierender Variationen behilflich ist.

Der Einsatz von Passwort-Knack-Programmen dient das Angreiferverhalten zu simulieren. Schwachstellen können damit erkannt und beseitigt werden und die Benutzer über unsichere Passwörter informiert werden, ehe dies potentiellen Angreifern möglich ist. Damit werden nicht nur negative Konstruktionsbeispiele aufgezeigt, sondern ebenso die Präsenz von Bedrohungen, die unmittelbar mit dem Verhalten des Nutzers in Verbindung steht. Dies führt zu einem empfindlicheren Bewusstsein im Umgang mit den aufgestellten Sicherheitsrichtlinien und zeigt den Anwendern, dass auch ihr Account betroffen ist und ihm Bedeutung für die Sicherheit des Gesamtsystems zugemessen wird. Informationen über erfolgte Angriffe oder Angriffsversuche machen den Anwendern deutlich, dass es sich nicht um eine fiktive Bedrohung handelt, sondern eine reele Gefahr für die Sicherheit des Systems besteht. Ebenso sollten die Folgen möglicher Angriffe dargestellt werden. Diese können unbemerkt verlaufen oder aber sogar mehrtägige System- und damit Arbeitsausfälle verursachen. Die imensen Kosten bereits kurzfristiger Ausfälle und des möglichen Wirtschaftsschadens verdeutlichen den Benutzern die ernsthafte Problematik.

Um die Vertrauenswürdigkeit der Daten hervorzuheben, wird die Klassifizierung von Dokumente nahegelegt. Vor der digitalen Verwaltung von Dokumenten und Verwendung von Rechnern zur zur Kommunikation erfüllten Stempel die Zumessung der Bedeutung einzelner Schriftstücke. Mit ergänzende Bemerkungen wie 'vertrau-

lich', 'nur für den internen Gebrauch', 'streng geheim' oder 'persönlich' kann die Bedeutung der Daten hervorgehoben werden. Dies impliziert klare Verhaltensregeln für den Umgang mit Informationen und zeigt dem Nutzer explizit die Bedeutung der Daten und Sicherheit des Systems zur Wahrung der Vertraulichkeit auf. Dieser Prozess kann durch die Einführung unterschiedlicher Sicherheitslevels verbessert werden, indem sich die Authentifizierung nach der Wichtigkeit der Daten richtet. So genügt in einem Unternehmen die kontextbasierte Authentifizierung für den Zugriff auf Dokumente des alltäglichen Geschäftsbetriebs, die durch das Betreten des jeweiligen Büros bereits erreicht wird. Die Überprüfung der Identität sollte erst dann notwendig sein, wenn der Benutzer Informationen abruft, die anderen Mitarbeitern nicht zugänglich sein sollen. Der Zusammenhang zwischen den Sicherheitsstufen und der Bedeutung der geschützten Informationen muss den Benutzern erklärt und offensichtlich dargelegt werden.

Unterstützt sollte die Authentifizierung auf dem jeweiligen Sicherheitslevel durch sogenannte Single-Sign-On Systeme werden. Mit der einmaligen Authentifizierung hat der Benutzer somit Zugriff auf alle Daten und Anwendungen einer Sicherheitsebene. Dem Benutzer bleibt während einer Session die mehrmalige Eingabe seiner Benutzerdaten erspart, welche die Arbeitsweise durch den Wegfall sich wiederholender Authentifizierung nicht beeinträchtigt, die Sicherheit des Systems jedoch dennoch gewährleistet. Erreicht kann dieses Ziel durch die Synchronisation und Verteilung der Passwörter im System werden. Von zentraler Stelle wird dem Anwender damit die Verwaltung seiner Kennwörter ermöglicht und die Zuordnung bzw. Verteilung auf ausgewählte Dienste unterschiedlicher Sicherheitslevels überschaubar dargestellt.

Der Benutzer muss sich damit nicht nur wenigere Passworte behalten, sondern erhält den Überblick über deren Einsatz. Das Raten, welches Passwort an welcher Stelle zu verwenden ist, wird zunehmend vermieden. Zwar kann dies auch durch individuell erstellbare Kennwórthinweise oder Anzeige des Kennwortschemas realisiert werden, gibt diese Informationen jedoch auch möglichen Angreifern des Systems preis. Durch die zentrale Verwaltung entfällt ebenso der Aufwand, Passwörter in jeder Anwendung einzeln erstellen oder ändern zu müssen. Der Umgang mit der Authentifizierung wird komfortabler gestaltet, zeitintensive Überprüfungen der Zugangsberechtigung werden vermieden.

Behilflich ist unter anderem auch die Kombination wissensbasierter Authentifizierungsmechanismen mit anderen Methoden zur Überprüfung der Indentität. Chip- oder Magnetkarten bzw. RFID-Transponder können mit dem Einsatz von Passwörtern zur Authentifizierung auf höheren Sicherheitsebenen verbunden werden. Auf niedrigeren Sicherheitsleveln ist es gegebenenfalls bereits ausreichend, nur die besitzbasierte Komponente als Zugangsberechtigung einzusetzen. Auch hier sollte jedoch darauf geachtet werden, den Benutzer nicht durch eine Vielzahl verschiedener Karten und unterschiedlichen Verwendungsarten zu verwirren, sondern diesen Prozess möglichst einheitlich zu gestalten und möglichst alle Funktionen in einem Objekt zu

integrieren.

Durch die zentrale Verwaltung und Bündelung der Funktionen kann dem einzelnen Benutzer ein individueller Systembetreuer und -berater zugewiesen werden. Anstatt sich in Abhängigkeit unterschiedlicher Funktionen mit einer Vielzahl anonym organisierter Abteilungen auseinandersetzen zu müssen, erhält der Anwender einen persönlichen Ansprechpartner, der ihm in jedem Einsatzgebiet unterstützt. Der Anwender ist somit nicht mehr auf sich alleine angewiesen, sondern bekommt einen kompetenten Helfer zur Seite gestellt, der für alle sicherheitsrelevanten Bereiche zuständig ist und zur Beratung und Betreuung zur Verfügung steht. Dem Nutzer wird der Authentifizierungsprozess damit nicht nur komfortabler und anwendungsfreundlicher im Sinne der bereitgestellten Dienstleistung gestaltet, zugleich wird durch die Aufsicht die Einhaltung der Sicherheitsbestimmungen gewährleistet, um sowohl die Benutzbarkeit als auch die Sicherheit des Vorgangs zu garantieren. In der Praxis scheitert dies jedoch leider oft auch aus Kosten- und Qualifikationsgründen. Der persönliche Support ist oft zu teuer. Die Betreuung erfolgt dann durch virtuelle Assistenten, Portale oder computergestützte Hotlines. Ist der Support jedoch nicht ausreichend oder die Sprechstunden nur unter Einschränkungen verfügbar, so ist die Gefahr aus Anwendersicht zu hoch, zentrale Passwörter zu verlieren und damit von mehreren Diensten temporär ausgeschlossen zu werden.

6 Zusammenfassung

Nachdem die Konstruktion sicherer Passworte ausführlich dargelegt und beschrieben wurde, wurde der Umgang mit Authentifizierungsmechanismen in der Realität und die Ursachen des Verhaltens der Anwender analysiert. Zahlreiche Studien und auch andere Anzeichen und Indikatoren verwiesen auf die schlechte Benutzbarkeit des wissensbasierten Authentifizierungsprozesses und führte zur geringeren Sicherheit des Systems. An konkreten Beispielen und Reaktionen der Nutzer wurde der Einfluss der menschlichen Komponente beim Entwurf sicherer Systeme und Authentifizierungsmechanismen aufgezeigt sowie die Bedeutung, Erkenntnisse aus der Human-Computer-Interface-Forschung darin zu integrieren. In einer Reihe von Empfehlungen und Lösungsansätzen wurde deren Einsatzmöglichkeiten vorgestellt, die sowohl sichere als auch umgänglichere Authentifizierungsprozesse ermöglichen.

Dabei ist allerdings zu berücksichtigen, dass der Einsatz jeder Methode zur benutzerfreundlicheren Gestaltung des Systems das grundlegende Problem für die Unsicherheit von Passwörtern - den begrenzten menschlichen Fähigkeiten, insbesondere die eingeschränkte Erinnerungsfähigkeit - nicht lösen kann. Die Anwendung von Ergebnissen aus der HCI-Forschung trägt jedoch dazu bei, die Defizite aktueller Methoden zur wissensbasierten Authentifizierung basierend auf der perfekten Erinnerung zu kompensieren und Systeme anwendungsfreundlicher zu gestalten. Insbesondere die Kombination mit alternativen Authentifizierungsmechanismen, wie die Verwendung von RFID-Chips oder Erkennungsmethoden der Biometrie, werden zunehmend

eingesetzt.

Elektronische Reisepässe, Zugangs- und Zeiterfassungssysteme, Bezahl- sowie Authentifizierungsfunktionen werden heute bereits vielerorts verwendet. Die Fehler und Schwächen dieser Methoden sind jedoch nicht zu vernachlässigen und werden auch weiterhin die Bedeutung und Erfordernis wissensbasierter Methoden notwendig machen. Auf die Bedürfnisse und den Einfluss der Benutzer aufmerksam gemacht, wird die Entwicklung in diesem Bereich ebenso herangetrieben und führt zu verbesserten Systemen und Anwendungen. Passwortverwaltungsprogramme, Identitätsmanager und die Entwicklung grafischer Passwortsysteme sind nur wenige Beispiele für die Reaktion auf vorhandene Defizite in diesem Bereich.

Dennoch bieten wissensbasierte Authentifizierungsmechanismen noch genügend Gelegenheit zur Innovation und Umsetzung erfolgter Erkenntnisse. So lange Angriffe auf passwortgeschützte Systeme durch menschliche Verhaltensweisen ermöglicht werden und Anzeichen wie das Notieren von Passwörtern bestehende Probleme anzeigen, werden Maßnahmen aus der HCI-Forschung noch nicht ausreichend realisiert und sind weitere Analysen erforderlich. Die Entwickler heutiger Systeme haben diesen Einfluss jedoch erkannt und beziehen die menschliche Komponente sowie Anforderungen der Anwender zur Gestaltung benutzerfreundlicher und sicherer Systeme in den Software-Engeneering-Prozess mit ein.

Literatur

[AdSa99] Adams, A.; Sasse, M. A.: “Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures”. In: , URL http://www.cs.ucl.ac.uk/staff/A.Sasse/p40-adams.pdf, 1999. 9, 11

[AnLu97] Anne Adams, M. A. S.; Lunt, P.: “Making Passwords Secure and Usable”. In: , URL http://www.sims.berkeley.edu/~rachna/security_usability.html, 1997. 10, 13, 14

[ChBe94] Cheswick, B.; Bellovin, S.: “Firewalls and Internet Security: Repelling the Wily Hacker”. In: , URL http://www.wilyhacker.com/, 1994. 4

[Corp06] Corporation, M.: “Schützen Sie Ihre persönlichen Daten mit sicheren Kennwörtern”. In: , URL http://www.microsoft.com/switzerland/athome/de/security/privacy/password.mspx, 2006. 5

[DeAl88] DeAlvare, A.: “A Framework for Password Selection”. In: , 1988. 9

[DeAl90] DeAlvare, A.: “How Crackers Crack Passwords OR What Passwords to Avoid”. In: , 1990. 9

[Info] für Sicherheit in der Informationstechnik, B.: “IT-Grundschutz-Katalog”. In: , URL http://www.bsi.bund.de/gshb/deutsch/m/m02011.htm. 8, 15

[Jian00] Jianxin Yan, R. A. A. G., Alan Blackwell: “The memorability and security of passwords - some empirical results”. In: , URL http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-500.pdf, 2000. 5

[Klei90] Klein, D.: “A survey of, and improvements to, password security”. In: , URL http://www.klein.com/dvk/publications/passwd.pdf, 1990. 7

[MaWe01] Martina Angela Sasse, S. B.; Weirich, D.: “Transformng the ’weakest link’: A human/computer interaction approach to usable and effective security”. In: , URL http://www.cs.ucl.ac.uk/staff/A.Sasse/ttw.pdf, 2001. 11, 15

[Patr02] Patrick, A. S.: “Human Factors of Security Systems. A Brief Review”. In: , URL http://www.andrewpatrick.ca/passwords/passwords.pdf, 2002. 13

[Proj] Project, O.: “John the Ripper password cracker”. In: , URL http://www.openwall.com/john/. 6

[Publ85] Publication, F. I. P. S.: “Password Usage”. In: , URL http://www.itl.nist.gov/fipspubs/fip112.htm, 1985. 15

[Shaf00] Shaffer, G.: “Cracking Password Techniques”. In: , URL http://geodsoft.com/howto/password/cracking_passwords.htm, 2000. 7

[Vu06] Vu, K.-P.: “Password Security is Her Game”. In: , URL http://www.csulb.edu/misc/inside/archives/v58n5/2.htm, 2006. 1

[Wick92] Wickens, C.: “Engineering Psychology and Human performance”. In: , 1992. 12

[Zepp06] Zeppmeisel, M.: “Einführung in die Grundlagen der Quantenkryptographie”. In: , URL http://www.cip.physik.uni-muenchen.de/~milq/quantenkryp/Quantenkryptographie.pdf, 2006. 5