

Musterlösung
für Schulen in
Baden-Württemberg

Windows 200x

Sichere Kennwörter

Ulrich Hollritt
Stand 15.12.05 / 2. Fassung

Inhaltsverzeichnis

1. Was ist ein Kennwort?.....	3
1.1. Wieso ist das Kennwort im Netzwerk so wichtig?	3
1.2. Wie sieht ein sicheres Kennwort aus?	3
1.3. Zu beachten beim Erstellen eines sicheren Kennworts!	4
1.4. Umgang mit dem Kennwort.....	5
2. Administrator-Kennwörter im ML Netz	7
2.1. Unterschiede in den Kennwörtern	7
2.2. Quellen und Links	7

1. Was ist ein Kennwort?

Ein Kennwort oder auch Passwort ist ein allgemeines Mittel zur Authentisierung eines Benutzers innerhalb eines Systems.

Das Kennwort ist eine beliebige, in der Regel vom Nutzer selbst gewählte, alphanumerische Zeichenfolge.

Die Authentizität des Benutzers bleibt daher nur gewahrt, wenn er das Kennwort geheim hält. Hacker verwenden Programme, die automatisch und nach dem Zufallsprinzip tausende möglicher Kennwörter testen.

Sie erhöhen die Sicherheit Ihres PC's, indem Sie sichere Kennwörter verwenden, das Kennwort bedacht einsetzen und Ihre Benutzerkonten überwachen.

1.1. Wieso ist das Kennwort im Netzwerk so wichtig?

Kennen Schüler das Kennwort eines Lehrers, so haben sie Zugriff auf das Tauschverzeichnis der Lehrer, sowie auf die persönlichen Verzeichnisse aller Schüler.

Klassenarbeiten, Arbeitsblätter, Konferenzbeschlüsse und was sonst noch im Netzwerk abgelegt ist, kann nun kopiert, gelöscht oder heimlich verändert werden.

Schüler können damit auch die Einstellungen des Webfilters oder Druckersperren verändern.

Würden Sie einem Schüler den Schlüssel zu ihrem Arbeitszimmer geben und ihn dann unbeaufsichtigt „spielen“ lassen?

1.2. Wie sieht ein sicheres Kennwort aus?

Die Sicherheit eines Kennwortes hängt vor allem davon ab, dass dieses geheim bleibt. Andere Faktoren zum Schutz des Kennwortes sind z.B.:

Wie häufig kann das Kennwort zur Authentifizierung verwendet werden?

Die größte Sicherheit ist bei einmaliger Verwendung gegeben, dieser Fall ist aber in der Schule nicht relevant. Auch das Ändern in regelmäßigen Abständen (z.B. alle vier Wochen) lässt sich zwar durch das System vorgeben, wird aber im Umfeld Schule keinen Einsatz finden.

Wie leicht lässt sich das Kennwort von einem Angreifer erraten?

Da die meisten Kennwörter von menschlichen Benutzern eingegeben werden und vor allem diese es sich merken müssen, kommen häufig einfach zu ratende Kennwörter zum Einsatz, wie z.B. Name der Frau, Freundin, des Mannes, Freundes oder Haustieres.

Das Kennwort sollte möglichst lang sein.

Das System sollte einen möglichst großen Zeichensatz verwenden (Buchstaben, Zahlen und Sonderzeichen) mit dem das Kennwort gebildet wird.

Zudem sollte das System nach einer bestimmten Zahl von fehlerhaften Eingaben keine neuen Eingaben akzeptieren, bis eine bestimmte Zeit vergangen ist bzw. das System manuell wieder freigeschaltet wurde.

Leider verwenden unerfahrene User immer noch einfache Wörter wie Tiernamen, Vornamen der Kinder usw. Dies ist sehr gefährlich, da solche Kennwörter durch manuelles Raten sehr leicht herausgefunden werden.

Es gibt zahlreiche Crackprogramme für Kennwörter jeder Art im Internet. Einfache Wörter werden hierbei extrem schnell geknackt. Allerdings lässt sich dagegen auch nicht unbedingt Vorsorge treffen: gelingt es einem Hacker, an Ihre Passwortdaten heranzukommen (was nur mit Administratorrechten möglich ist), so ist das Knacken nur eine Frage des *wie lange* und nicht mehr des *ob*.

Wahrscheinlich wissen Sie bereits, dass es nicht ratsam ist, Kennwörter aus fortlaufenden Zahlen, wie etwa „12345678“, oder aus im Alphabet oder auf der Tastatur aufeinander folgenden Buchstaben, wie „lmnopqrs“ oder „qwertz“, zu erstellen. Und sicherlich wissen Sie auch, dass man seinen Anmeldenamen, den Namen des Ehepartners oder sein Geburtsdatum nicht als Kennwort verwenden sollte.

Aber wussten Sie auch, dass man niemals ein Wort irgendeiner Sprache verwenden sollte, das in einem Wörterbuch zu finden ist? Ja, Hacker verwenden ausgeklügelte Tools, die im Handumdrehen Kennwörter anhand von Einträgen in Wörterbüchern verschiedener Sprachen erraten können, gängige Wörter sogar dann, wenn sie rückwärts buchstabiert sind.¹

Wenn Sie ein gängiges Wort als Kennwort verwenden, meinen Sie vielleicht, dass es sicher ist, wenn Sie einzelne Buchstaben davon durch Zahlen oder Symbole ersetzen, die den Buchstaben ähneln, z. B. M1cr0\$oft oder P@ssw0rt. Leider kennen auch Hacker diese Tricks.

1.3. Zu beachten beim Erstellen eines sicheren Kennworts!

Die Herausforderung besteht darin, ein Kennwort festzulegen, das Sie sich leicht merken können und das trotzdem von anderen Personen nicht leicht erraten werden kann.

Sie können sich natürlich eine völlig willkürliche Kombination aus Zahlen und Symbolen ausdenken, doch das ist nicht sehr praktisch. Wie sollen Sie sich so ein Kennwort merken? Gewiss, Sie können es aufschreiben und in Ihre oberste Schreibtischschublade legen, doch dann ist es bereits kein sicheres Kennwort mehr.

Ein „starkes“ Kennwort ist eines, das mindestens acht Zeichen umfasst, aus einer Kombination von Buchstaben, Zahlen und Symbolen besteht und für Sie leicht zu merken, für andere aber schwer zu erraten ist.

Die einfachste Art, ein starkes Kennwort zu erstellen, das Sie nicht aufzuschreiben brauchen, besteht darin, sich eine Passphrase auszudenken. Eine Passphrase ist ein Satz, den Sie sich merken können, z. B. „Mein Sohn Heinz ist drei Jahre jünger als meine Tochter Anna.“ Durch die Aneinanderreihung der Anfangsbuchstaben der einzelnen Wörter entsteht ein ziemlich starkes Kennwort. In diesem Beispiel wäre das Kennwort „mshidjjamta“. Sie können dieses

¹ Passwortknacker arbeiten oft in mehreren Stufen:

1. Alle trivialen Passwörtern und solche, die in einem Wörterbuch stehen
2. Kleinere Abwandlungen dieser Wörter
3. „Brute Force“ – alle Zeichenkombinationen werden durchprobiert. Auf einem normalen PC dauert das bei max. 8 Zeichen ca. eine Woche. „Echte“ Hacker verwenden aber im voraus berechnete Codes, da geht das viel schneller.

Kennwort aber noch stärker machen, indem Sie eine Kombination aus Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen, die wie Buchstaben aussehen, verwenden.² Aus demselben leicht zu merkenden Satz wird dann mit ein paar Tricks das Kennwort „M\$H1i3JamT@“.

Wenn Ihnen auch das zu schwer zu merken ist, probieren Sie es mit einer bekannten Redewendung wie „Wer anderen eine Grube gräbt, fällt selbst hinein“. Wenn Sie eine solche bekannte Wendung verwenden, sollten Sie allerdings auch mindestens ein Symbol in das Kennwort einfügen. Beispiel: w@1Gg_f\$h

Grundsätzlich sollte ein *Administratorkennwort* mindestens 13 Zeichen haben.

Es folgen einige allgemeine Richtlinien zum Erstellen sicherer Kennwörter:

Bilden Sie ihr Passwort aus mindestens 8 Zeichen.

Verwenden Sie **Groß-** und **Kleinbuchstaben** sowie **Ziffern** und **Sonderzeichen**.
Achtung: Bei der Eingabe des Kennworts wird zwischen Groß- und Kleinschreibung unterschieden

Verwenden Sie mindestens vier unterschiedliche Zeichen (wiederholen Sie nicht dieselben Zeichen).

1.4. Umgang mit dem Kennwort

Nur Kennwörter, die Sie geheim halten, können sichere Kennwörter sein. Geben Sie Kennwörter niemals an Kollegen weiter³. Schreiben Sie sie niemals auf, um sie dann auf Ihrem Schreibtisch oder im Computerraum liegen zu lassen. Schreiben Sie sie auch niemals in eine ungeschützte Datei auf Ihrem Computer. Kommt ein Schüler an das Kennwort eines Kollegen, so kann er auch auf Ihre Daten zugreifen.

Hier ein paar allgemeine Tipps zum sicheren Umgang mit Kennwörtern:

Halten Sie Ihre Kennwörter geheim.

Ändern Sie Ihr Kennwort mindestens alle sechs Monate.

Besprechen Sie mit Ihren Kollegen/Schülern gleich zu Beginn wie ein gutes Kennwort aussieht. Erinnern Sie die Kollegen/Schüler daran, wie wichtig der sichere Umgang mit dem eigenen Kennwort ist (Bsp. Pin beim Handy, Haustürschlüssel).

² Auch hier gilt wieder: gegen ein professionelles Tool bieten diese Maßnahmen keinen Schutz. Gegen manuelles Erraten hingegen ist der Schutz fast perfekt.

³ Wollen Sie administrative Aufgaben an einen Kollegen delegieren, so richten Sie ihm ein eigenes Konto mit Administratortorberechtigungen ein.

Weisen Sie Ihre Kolleginnen und Kollegen auf die Gefahren unsicherer Kennwörter und die verbotene Weitergabe von Kennwörtern hin.

Für Kennwörter „im alltäglichen Gebrauch“ gelten die folgenden Hinweise:

Auch wenn Sie bereits wissen, dass ein Kennwort nicht an Freunde verraten oder aufgeschrieben gehört, sollten Sie es nicht einmal leichtfertig an eine Website übermitteln. Eine neue Hackermethode zur Entlockung fremder Kennwörter ist das so genannte Phishing. Hierzu werden Millionen gefälschter E-Mails versendet, die anscheinend von einer namhaften Website wie eBay, Amazon oder Ihrer Bank stammen. Die E-Mails wirken so offiziell, dass viele Benutzer bedenkenlos der Aufforderung nachkommen, ihren Benutzernamen und ihr Kennwort zu nennen.

Microsoft, eBay, Amazon, PayPal oder ein anderes seriöses Unternehmen wird Sie niemals dazu auffordern, Ihr Kennwort per E-Mail zu versenden. Wenn Sie eine Aufforderung zur Übermittlung eines Kennworts, einer PIN-Nummer oder anderer vertraulicher Daten per E-Mail erhalten, verständigen Sie das (echte) Unternehmen umgehend telefonisch oder über dessen Website

Am sichersten ist es, für jede Website oder Anmeldeaufforderung ein eigenes Kennwort zu erstellen. Dies ist jedoch fast so unpraktisch wie das Auswendiglernen einer langen Folge willkürlich gewählter Zeichen. Einfacher ist es, sich eine kleine Anzahl wirklich starker Kennwörter auszudenken und diese da zu verwenden, wo es entscheidend auf Sicherheit ankommt, beispielsweise für Ihre Bank, Ihren Online-Broker oder Ihre Direktversicherung. Für alle übrigen Zwecke können Sie dann eine kleine Gruppe leichter zu merkender Kennwörter erstellen.

Und denken Sie dran:

Ein starkes Kennwort ist eines, das Sie jeweils nach einigen Monaten wieder ändern.

2. Administrator-Kennwörter im ML Netz

2.1. Unterschiede in den Kennwörtern

Im Netzwerk der Musterlösung gibt es zwei Administratoren. Den lokalen Administrator an den Clients und den Domänenadministrator im Netzwerk.

Da die Clients mit RIS oder RIPREP installiert wurden, wird für den lokalen Administrator zunächst dasselbe Kennwort verwendet wie für den Administrator im Netzwerk.

Aus Sicherheitsgründen sollte sich das Passwort des lokalen Administrators an den Clients von dem des Domänenadministrators unterscheiden. Auch sollte man beide von Zeit zu Zeit ändern.

Das lokale Administratorkennwort ergibt sich aus dem Eintrag in der ristndrd.sif – Datei auf dem Server im Verzeichnis

RIS\Setup\German\Images\winXP.pro\i386\

im Abschnitt [GuiUnattended]

Dieses sollten Sie in ein sicheres Kennwort ändern.

Sie können auch nachträglich mit einem Startskript zentral das lokale Administratorpasswort an jedem Client ändern.

Das Skript und die Anleitung finden Sie auf dem Lehrerfortbildungsserver im Bereich der Windows Musterlösung unter Praxistipps – Startskripte – Lokales Adminpasswort setzen.

<http://lehrerfortbildung-bw.de/netz/muster/win2000/material/tipps/startup/lokalespasswort/index.html>

2.2. Quellen und Links

<http://www.microsoft.com/switzerland/athome/de/security/privacy/password.msp>

<http://de.wikipedia.org/wiki/Kennwort>