

## HELPDESK

# Ein Weg zum sicheren Passwort

Jede Woche beantworten Sicherheitsexperten Leserfragen und geben Ratschläge, wie sich die Sicherheit in einem Unternehmen erhöhen lässt.

**Frage:** Unsere Security Policy verlangt, dass die Mitarbeiter sichere Passwörter wählen und ihr Passwort jeden Monat ändern. Wie geht das, ohne die Passwörter aufzuschreiben?

Problem: Nach wie vor ist die Kombination von User-ID und zugehörigem Passwort der meistverbreitete, weil kostengünstigste Authentifizierungsmechanismus. Bei Smartcard- oder Secure-Token-basierten Authentifizierungsmechanismen basiert die Sicherheit auf dem Credo: Wissen (der PIN beziehungsweise der angezeigte Wert) und Haben (die Hardware: Secure Token oder Smartcard). Es nützt einem Unberechtigten wenig, wenn er zwar die Hardware ergattern konnte, aber den zugehörigen Schlüssel nicht kennt oder vice versa. Nach ein paar misslungenen Anmeldeversuchen wird der User-Account und die Hardware gesperrt und damit unbrauchbar.

Bei rein auf User-ID und zugehörigem Passwort basierenden Mechanismen steht und fällt die Sicherheit mit der Qualität des Passworts und dem Umgang mit demselben. Wenn ein Unberechtigter mittels Social Engineering oder gezieltem Blick auf den Computer

oder unter die Tastatur das Passwort erlangen kann, steht dem erfolgreichen digitalen Identitätsdiebstahl nichts mehr im Wege. Ein Unberechtigter, der nur die User-ID kennt, wird versuchen, das Passwort zu erraten.

Anforderungen: Um es Unberechtigten nicht allzu einfach zu machen, sind so genannte «starke» Passwörter zu verwenden. Stark steht in diesem Fall für kaum erratbar und auch mit viel Rechenpower nicht innert weniger Jahre zu knacken. Somit sind

**«Eine praktikable Lösung bietet die Satzbildungsmethode: Dabei wird ein beliebiger Satz formuliert, und jeder Anfangsbuchstabe extrahiert.»**

starke Passwörter komplex: Verwendung von Gross- und Kleinschreibung, Buchstaben, Ziffern und Sonderzeichen. Ausserdem dürfen die Passwörter nicht aus dem direkten Umfeld der sie verwendenden Person stammen. Somit sind Namen (Frau, Freundin, Kinder, Lieblingsmannschaft) oder Nummern wie Telefon-, Auto-, oder Hausnummer tabu. Ein starkes Passwort für einen normalen User-Account sollte mindestens sechs, besser

aber acht bis zehn Zeichen lang sein. Administratoren-Accounts sollten mit mindestens zwölf Zeichen langen Passwörtern geschützt werden. Doch wie lassen sich solche Passwörter erfinden und merken, ohne sie aufzuschreiben – zumal Passwörter monatlich geändert werden sollten?

Lösung: Eine praktikable Lösung bietet die Satzbildungsmethode: Dabei wird ein beliebiger Satz formuliert und jeder Anfangsbuchstabe extrahiert. Somit wird beispielsweise aus dem Satz: «Am 5. September regnete es auch nur 1 mal!» das starke Passwort: «A5Srean1m!». Umlaute sollten aus praktischen Gründen vermieden werden, weil sie die User

vor ein Problem stellen könnten, falls sie ihr Passwort einmal an einem System mit fremdsprachigem Tastaturlayout eingeben müssen. Das Problem des regelmässigen Passwortwechsels kann elegant gelöst werden, indem bei jedem Wechsel beispielsweise eine inkrementierte Ziffer vor oder hinter das Passwort gesetzt wird. Dieser Trick kann nur angewendet werden, wenn einerseits kein technischer Mechanismus implementiert

wurde, welcher bei jedem Passwortwechsel sicherstellt, dass im neuen Passwort nur wenige Zeichen mit dem alten Passwort übereinstimmen. Andererseits muss das Passwort vom User absolut geheim gehalten werden. Ansonsten verkommt jeder Authentifizierungsmechanismus und das stärkste Passwort zur Farce.

Wer die Stärke eines Passworts testen möchte, kann dies auf der Website des Datenschutzbeauftragten des Kantons Zürich tun: <https://passwordcheck.datenschutz.ch/check.php> (ähnliches, nicht identisches Passwort eingeben). Das Beispielpasswort wurde als stark bewertet. Ein Unberechtigter würde bei 500 000 Versuchen pro Sekunde 21 435 Jahre benötigen, um das Passwort zu knacken. ■



**Der Autor**  
Christoph Baumgartner ist Senior Consultant bei der Sicherheitsberaterin Oneconsult, Thalwil, [www.oneconsult.com](http://www.oneconsult.com).

**Unsere Experten beantworten Ihre Fragen.** Schreiben Sie uns: [it-security@computerworld.ch](mailto:it-security@computerworld.ch)

Ein Archiv der Helpdeskartikel finden Sie im Internet: [www.computerworld.ch](http://www.computerworld.ch)