Technik

My Password is my Castle

Kay Behrman über Datensicherheit

Müssen Sie sich auch jeden Morgen mittels Passwort bei ihrem wichtigsten Arbeitsmittel zu erkennen geben? Ein Retina-Scan hat sich in Ihrem Büro noch nicht durchsetzen können, genauso wenig wie Smartcard, SecurID oder Fingerabdrucksensor? Nun gut, dann ist der technische Fortschritt noch nicht in letzter Konsequenz an Ihrem Arbeitsplatz angekommen, aber dafür dürfen Sie sich zur Mehrheit der Anwender zählen. Wenn Sie sich zudem durchschnittskonform verhalten, so hat Microsoft in einer Studie herausgefunden, dann haben Sie in Ihrer Karriere als Internetnutzer inzwischen 25 Zugänge auf Webseiten mit Passwort eingerichtet und haben dafür 6,5 verschiedene Passwörter verwendet. Mit anderen Worten: Im Schnitt verwenden Sie auf etwa vier verschiedenen Webseiten das gleiche Passwort.

Der Administrator von kochrezepte.de kann Ihre gmx-Email lesen, sofern Sie das gleiche Passwort nutzen. Die Mehrzahl der Web-Angebote speichert Username und Passwort nämlich lesbar im Klartext. Das zeigen auch die Fälle von gehackten Web-Servern, bei denen Anmeldungen mit Kennwort komplett öffentlich bekannt wurden. Immerhin kennen wir aus diesen Listen auch das beliebteste Passwort der Welt: „123456“. Keine kreative Höchstleistung, aber etwa vier von 1000 Anmeldern nutzen es. Eine ähnliche Statistik zur PIN von iPhones ergab übrigens, dass mit zehn Versuchen 15% aller iPhones geknackt werden können.

In Firmennetzwerken gibt es die üblichen Methoden, um die Kollegen zu einem komplexeren Passwort zu zwingen. Es reicht ein Häkchen in den Kennwortrichtlinien ihres Windows-Servers, dann muss Otto Normaluser Ziffern und Sonderzeichen im Passwort verwenden, eine Mindestlänge erreichen, und alle paar Tage sein Passwort erneuern. Bis zu 24 kann sich das normale Windows zudem merken, um Passwort-Recycling zu unterbinden.

Mit der Nutzung dieser Richtlinien beginnt oft eine Art Evolution. Der Schuss geht meist zunächst nach hinten los, denn der gequälte User kann sich „W2Gz$kö%hKv+“ nun mal schlecht merken. Oder, um aus einer ernsthaften wissenschaftlichen Studie zu diesem Thema zu zitieren: „Die Qualität und die Merkbarkeit eines Passworts verhalten sich umgekehrt proportional zueinander“. Deshalb finden sich dann häufig kleine gelbe Merkzettel am Monitor oder unter der Schreibtischunterlage. Die Firmenleitung reagiert darauf mit einem entsprechenden Verbot. Ab dieser Evolutionsstufe hat der Helpdesk viel damit zu tun, vergessene Passwörter zurück zu setzen. Ein Kölner Marktforschungsunternehmen will im Auftrag von Symantec herausgefunden haben, dass deutschlandweit jedes Jahr über sechs Milliarden Euro Schaden durch derartige Passwortverwaltung entsteht.

Manchmal spricht sich auch herum, dass ein Anruf beim Helpdesk „Hallo, hier Müller, können Sie bitte mein Passwort zurück setzen?“ reicht, um an die Daten von Herrn Müller zu kommen. Und überhaupt kann jedermann in YouTube mittels Suche nach „Passwort löschen“ sehen, wie man auch ohne Passwort in jedes Windows „reinkommt“. Die Firmendaten auf dem Server hat man dann noch nicht, dafür bedarf es eines Crack-Programms. Ein britischer IT-Journalist hat kürzlich demonstriert, dass er durch Nutzung des Rechenkerns auf der Grafikkarte seines PCs rund 3,3 Milliarden Passwörter pro Sekunde probieren kann. Jedes siebenstellige Passwort, auch mit Ziffern, Groß- und Kleinbuchstaben, ist innerhalb von 17 Minuten geknackt.

Es setzt sich die Erkenntnis durch, dass Passwörter alleine nicht mehr reichen. Deshalb landen viele Unternehmen letztlich bei Hardwarelösungen. Es gibt gute Lösungen, aber ein dominanter Standard hat sich noch nicht gebildet. Der Prozess von „Variation und Selektion“ läuft noch. Am Ende wird der PC morgens mehr von uns verlangen. So etwas wie Retina-Scan , Smartcard, SecurID oder Fingerabdruck.

Kay Behrmann ist selbständiger IT-Berater
www.vv.de