

Medientyp:	Tageszeitung	Gedr. Auflage:	34652
Erscheinungsdatum:	11.08.2009	Verk. Auflage:	28655
Seite:	19	Verbr. Auflage:	32281
		Reichweite:	94042

Tipps für unknackbare Passwörter

COMPUTER Um sich vor Hackern zu schützen, sollten Nutzer ihre Verschlüsselung sehr sorgsam auswählen.

Von Till Wortmann

Düsseldorf. Passwörter gehören zum Computer-Alltag wie die Marmelade zum Brot. Aber Hand aufs Herz: Sind die Zeichenfolgen auch wirklich sicher? Tatsächlich gehen die meisten PC-Anwender mit ihren persönlichen Codes grob fahrlässig um. Zu diesem Schluss kommt eine Untersuchung der PC-Feuerwehr. Die Computer-Notfallhilfe aus Hamburg bietet unter <http://passwortcheck.pc-feuerwehr.de> ein kostenloses Tool an, mit dem jeder Anwender die Tauglichkeit seines Passwortes selbst prüfen kann. Erschreckende Bilanz: Nur gut 30 Prozent der PC-Besitzer benutzen ein wirklich sicheres Passwort. Bei rund 65 Prozent ist das Geheimwort hingegen völlig unbrauchbar. Darunter fallen Zauberwörter wie „Mausi“, „Liebling“ oder der eigene Vorname, die in der Beliebtheitskala der PC-Anwender weit oben rangieren.

Die Mehrfachnutzung der Codes ist besonders schlecht

Schlecht auch, wenn sich das Kennwort leicht erraten lässt: Wer Romeo als Login-Namen wählt, sollte nicht ausgerechnet Julia als Passwort benutzen. Ebenso fatal sieht es bei der Mehrfachnutzung der Zugangsdaten aus: Für den E-Mail-Zugang und – wo der

größte Schaden droht – fürs Onlinebanking – stets die gleichen Codes. Sogar im Büro treten haarsträubende Mängel auf – zu diesem Ergebnis kommt eine Untersuchung der Software-Firma Econet. Verlässt nämlich ein Mitarbeiter für längere Zeit seinen Schreibtisch bleiben dessen Zugänge oft nur scheinbar geschützt zurück. Den Bayern zufolge bewahren viele Mitarbeiter ihre Passwörter leicht auffindbar am Arbeitsplatz auf oder teilen sie sogar Kollegen mit. Ist ein Mitarbeiter nicht im Büro kann seine digitale Identität so missbraucht werden.

Höchste Zeit also, dass die PC-Besitzer ihren Kennwörtern mehr Aufmerksamkeit widmen. Denn natürlich kennen auch die Hacker die Liebe der PC-Besitzer für Kosennamen & Co. Dabei kann man sich einfach schützen: Ein Spitzen-Passwort besteht aus wenigstens acht Zeichen, zusammengesetzt aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen, zum Beispiel „uZ6&fG5t“. Der Nachteil: Es lässt sich schwer merken. Zum Glück nehmen Passwort-Manager dem PC-Besitzer die Denkarbeit ab. Sie entlasten das Gehirn, weil sich der PC-Besitzer die Zugangsdaten für Websites wie soziale Netzwerke, Webmail oder Online-Foren nicht mehr einprägen muss – ein Master-Passwort als Sesam-Öffner reicht. So verschlüsselt der kostenlose „Passwort Manager Free“ der Firma Steganos (www.steganos.de) die Daten im Tresor nach einem von Experten als unknackbar geltenden Verfahren mit 256 Bit. Nach Eingabe des Tresor-

Passworts lassen sich Kennwörter und Nutzernamen einfach in das jeweilige Online-Formular ziehen.

Einige Programme verschlüsseln sogar E-Mails

Wer es noch komfortabler liebt, wählt die „Privacy Suite 11“ vom gleichen Anbieter. Die Lösung enthält zusätzlich einen Daten-Safe und verschlüsselt sogar E-Mails. Der Empfänger kann die Post dann nur nach Eingabe eines Codes lesen. Mit rund 50 Euro ist das Produkt allerdings recht teuer. Ein weiterer empfehlenswerter Passwort-Manager verbirgt sich hinter dem kostenlosen „Keypass 2.08“ von Dominik Reichl in Metzingen (<http://keepass.info>). Wer sich die Plackerei per Passwort-Manager sparen will, kann sich natürlich auch selbst ein Ungetüm ausdenken – per Gedächtnisstütze geht es sogar leichter als man vermutet. So lässt sich selbst ein Weltklasse-Passwort wie „F-WSsSm10Fu9Mv“ kinderleicht einprägen, denn dahinter verbergen sich die Anfangsbuchstaben aus dem Satz „Frank-Walter Steinmeier stellt Schattenkabinett mit 10 Frauen und 9 Männern vor“.

Groß- und Kleinschreibung kommen hier abwechselnd zum Einsatz, sogar ein Sonderzeichen ist mit von der Partie – da haben die Passwort-Spione ein Leben lang dran zu grübeln.

SICHERHEITSMASSNAHMEN

REGEL 1 Verwenden Sie nicht zu lange ein und dasselbe Kennwort. Tauschen Sie vielmehr

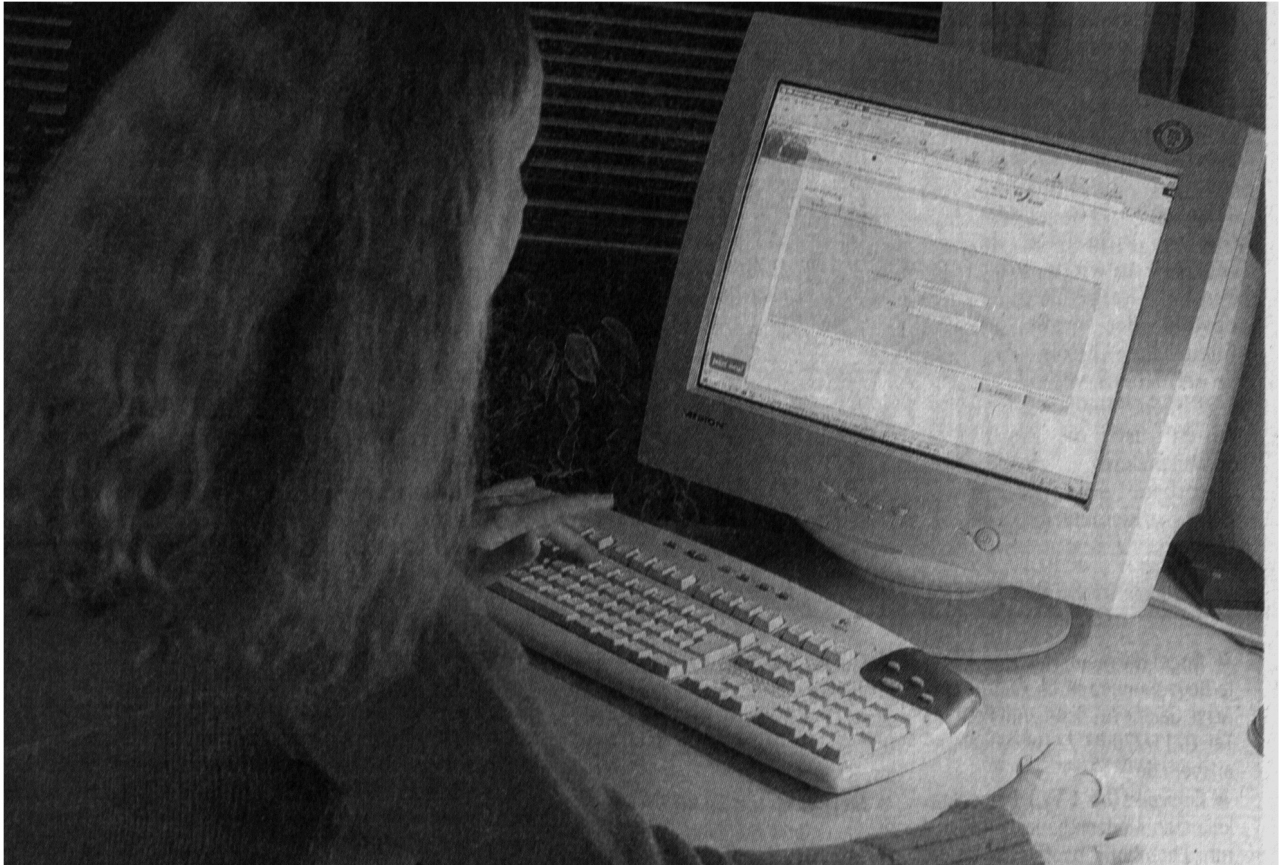
Ihre Passwörter regelmäßig aus.

REGEL 2 Speichern Sie Ihre Login-Daten niemals automatisch – ansonsten könnten fremde Personen, die auch auf Ihrem PC arbeiten, auf Ihre Konten zugreifen.

REGEL 3 Verraten Sie niemals Ihre Passwörter an scheinbar seriöse Firmen wie etwa Ihrer Hausbank – auch wenn diese Sie per E-Mail dazu auffordert – in der Regel steckt ein Betrüger dahinter.

REGEL 4 Am sichersten gelten Passwörter, die Sie vollständig nach dem Zufallsprinzip entwerfen.

REGEL 5 Versuchen Sie wenigstens ein paar der obigen Regeln zu beherzigen.



Kosenamen oder Eigennamen eignen sich nicht als Passwort.

Foto: Imago