

## Das Bild ist der Schlüssel

### Viele Menschen können sich sichere Passwörter nicht einprägen. Darum sollen jetzt Bilder persönliche Daten sichern.

Bilder statt Zeichenkombinationen: So will die Kölner sfr Gesellschaft für Datenverarbeitung in Zukunft die Daten von Taschencomputern gegen unbefugten Zugriff sichern. Ihre Software **visual Key** soll klassische Passwörter überflüssig machen. Das Programm gibt es für die PDA-Betriebssysteme Windows CE und PocketPC 2002, eine Version für Palm-Geräte ist für das dritte Quartal geplant. In Arbeit ist auch eine Ausgabe für PCs mit Windows 2000 und Windows XP.

Nutzer können ein beliebiges Bild wählen. Per Mauszeiger werden markante Bildpunkte in beliebiger Reihenfolge angeklickt. Die Software ordnet, für die Anwender unsichtbar, diese Punkte in automatisch berechnete Koordinatensysteme ein. Position und Reihenfolge ergeben einen visuellen Schlüssel.

Beim Start zeigt der PDA die gewählte Grafik. Um Zugang zu den Daten zu erhalten, muss man die Bildpunkte in der gespeicherten Folge anklicken. Dabei legen Anwender selbst fest, mit welcher Genauigkeit sie die Punkte mit dem Mauszeiger treffen müssen - ob pixelgenau oder mit einer Unschärfe von bis zu 99 Pixeln. Je höher die Sicherheitsstufe, desto genauer muss man zielen.

Das Programm soll es einfacher machen, digitale Assistenten wirksam zu schützen. Viele Nutzer können sich keine komplizierten Passwörter merken und wählen nahe liegende Begriffe: den Namen der Frau, des Erstgeborenen oder des Haushundes. Hackprogramme entschlüsseln solche Passwörter in Sekundenschnelle, wie dies eine [Website der Hochschule für Technik in Rapperswil](#) demonstriert. Erst der Gebrauch von Sonderzeichen - Komma, Strichpunkt, Prozentzeichen - schafft sichere Passwörter. Doch die sind zu abstrakt fürs menschliche Gedächtnis.

Theoretisch ergeben sich bei der Wahl von zum Beispiel vier markanten Bildpunkten bereits viele Millionen möglicher Kombinationen, je nach gewählter Treffgenauigkeit. Dagegen bieten aus vier Ziffern bestehende Identifikationsnummern bloss 10 000 Kombinationen.

Viele Hackerprogramme prüfen mit schierer Rechenleistung alle möglichen Zeichenfolgen, bis sie das richtige Passwort gefunden haben. Gegen den visuellen Schlüssel sind sie so machtlos wie Key Logger, die heimlich Tastaturbefehle aufzeichnen: Es gibt bei **Visual Key** keine Tastatureingaben.