Becker & Partner GmbH	
Titel	**Midrange Magazin**
Datum	27.01.2014
Webseite	www.midrangemagazin.de

Simcrypt verwaltet Passwörter mit SIM-Karten

[[27.01.14]] +++ Starke Passwörter sind das A und O bei Zugriffsrechten in IT-Umgebungen. Meist fordern Unternehmen von den Mitarbeitern, komplizierte Kombinationen von Ziffern, Buchstaben und Sonderzeichen zu verwenden – in der Praxis wird aber simplifiziert. Erleichterung schafft Becker & Partner mit Mobilfunkkarten als Speichermedium: Die Verwendung von Zugangsdaten geschieht einfach per Drag-and-Drop.

Simcrypt nutzt die Verschlüsselungsmöglichkeiten von SIM-Karten für den zuverlässigen und zugleich praxistauglichen Schutz hochsensibler Passwörter. Mit dem handlichen System aus SIM-Karte als Token, Kartenleser und Software-Tool lassen sich Passwörter verschlüsselt speichern, für nahezu beliebig viele Anwendungen verwalten und einfach per Drag-and-Drop verwenden. Auch die Erzeugung starker Passwörter oder Schlüssel ist möglich.
„Der Speicherbereich der ursprünglich für Telefonbuch und SMS genutzten SIM-Karte wird vom Anwender per Mausklick neu formatiert. Die Daten werden dann PIN- und PUK-geschützt dort abgelegt", erklärt Martin Becker, bei Becker & Partner verantwortlich für die Entwicklung von Simcrypt, das Prinzip. „SIM-Karten sind, anders als USB-Sticks oder andere Smartcards, ein bewährter definierter Standard. So können Anwender völlig sicher sein, dass es keine versteckte Hintertür gibt, über die Daten in falsche Hände geraten können."
Die Verantwortung für ein starkes Passwort wird in nahezu allen Unternehmen oder Organisationen an die Anwender delegiert. „In der Praxis sind diese durch lange und komplizierte Kombinationen von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen jedoch häufig überfordert", erläutert der Geschäftsführer von Becker & Partner. Der Grund: Die Passwörter sind kaum zu behalten und sehr umständlich einzugeben. „Also wird auf zu kurze und naheliegende Passwörter ausgewichen." Oft sind die Passwörter sogar als Haftnotiz am Bildschirm zu entdecken.
Genauso gravierend für die IT-Sicherheit in Unternehmen sind Passwörter in ungeschützten Text-Dateien oder wenn für unterschiedliche Anwendungen dasselbe Passwort genutzt wird. Für das Management ergibt sich daraus im Schadensfall ein erhebliches Verantwortungs- und Haftungsproblem.
Simcrpyt lässt sich komfortabel an jedem aktuellen Windows 32- oder 64-bit-System nutzen. Der SIM-Kartenleser wird per USB-Schnittstelle angeschlossen. Zur Anmeldung muss eine frei wählbare vier- bis achtstellige PIN eingegeben werden – per Tastatur oder Maus über eine Bildschirmtastatur. Wahlweise kann eine zusätzliche Absicherung mit einem Passwort eingerichtet werden.
Klickt der Anwender im Programmfenster auf eine der dargestellten Verwendungen, erfolgt im Hintergrund der zugehörige Programmaufruf automatisch. Sind etwa die Zugangsdaten für ein Online-Portal hinterlegt, startet der Webbrowser. Benutzername und Passwort werden dann per Drag-and-Drop in die jeweiligen Eingabefelder gezogen. Dabei bietet die Ende-zu-Ende-Verschlüsselung der verwendeten Inject-Methode größtmögliche Sicherheit. Die Zwischenablage und der Tastaturspeicher bleiben außen vor. So können sie nicht von eingeschleusten Datenloggern ausspioniert werden.
Hier geht's zu Becker & Partner