Becker & Partner GmbH	
Titel	**itdaily**
Datum	24.10.2013
Webseite	www.it-verlag.de

Sichere Passwortverwaltung per Mobilfunkkarte

Veröffentlicht am Donnerstag, 24. Oktober 2013 22:41

SIMcrypt nutzt erstmals die Verschlüsselungsmöglichkeiten von SIM-Karten für den zuverlässigen und zugleich praxistauglichen Schutz hochsensibler Passwörter.

Bei Daten oder Zugriffsrechten in IT-Anwendungen gehören starke Passwörter zu den wichtigsten Bausteinen für umfassende Sicherheit. Eine praxistaugliche, sichere und wirtschaftliche Lösung für das Speichern und Verwalten von Zugangsdaten bietet jetzt SIMcrypt von Becker & Partner. 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.

Als Speichermedium für die Zugangsdaten – oder auch für einfache Skripte wie Anmeldeskripte in Unternehmensnetzwerken – setzt Becker & Partner auf handelsübliche Mobilfunkkarten. „Der Speicherbereich der SIM-Karte – ursprünglich für Telefonbuch und SMS genutzt – wird vom Anwender per Mausklick neu formatiert. Die Daten werden dann PIN- und PUK-geschützt dort abgelegt.", erklärt Martin Becker, verantwortlich für die Entwicklung von SIMcrypt, das Prinzip des Systems. „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."

Sicherheitslücke Passwort geschlossen

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 Becker. Der Grund: Die Passwörter sind kaum zu behalten und sehr umständlich einzugeben. „Also wird auf zu kurze und naheliegende Passwörter ausgewichen", so der Geschäftsführer von Becker & Partner weiter. 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 löst jetzt die konzeptionelle Schwäche, dass schwer zu knackende Passwörter schwierig zu handhaben sind.

Für alle aktuellen Windows-Systeme

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 lediglich eine frei wählbare vier- bis achtstellige PIN eingegeben werden – entweder 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 übersichtlich 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 einfach per drag-and-drop in die jeweiligen Eingabefelder gezogen. Dabei bietet die Ende-zu-Ende-Verschlüsselung der verwendeten Inject-Methode größtmögliche Sicherheit. Die Zwischenablage – unumgänglich bei copy-and-paste – und der Tastaturspeicher bleiben außen vor. So können sie nicht von eingeschleusten Datenloggern ausspioniert werden.

www.simcrypt.de