

Pressemitteilung, 21.06.2011 - 11:39 Uhr

## Überlegenheit SMS-basierter Authentifizierung gegenüber Security-Token



(PM) München, 21.06.2011 - Vor Kurzem räumte der Hersteller von Sicherheits-Hard- und Software RSA in einem offenen Brief an seine Kunden eine teilweise erfolgreiche Hacker-Attacke auf seine Server ein. Wie in einem Beitrag der Computerwoche vom 14.06.2011 geschildert wurde, sind die Folgen der Hacker-Angriffe gravierender als

bislang angenommen und offenbaren die Schwäche auf Token basierender Systeme für die Einwahl in geschützte IT-Bereiche. Dieses Thema mag für Privat-anwender von geringer Bedeutung sein, stellt aber ein ernstzunehmendes Sicherheitsrisiko für Unternehmen und öffentliche Einrichtungen dar. Hier werden oftmals lokale Authentifizierungstechniken benötigt, die über eine einfache Passwortabfrage hinausgehen und unberechtigten Personen den Zugriff auf vertrauliche Informationen verwehren. Da so genannte Einmal-Passwörter (OTP= One Time Password) bei Token bereits vor dem Login existieren, können Login-Daten und OTP „gephisht“ werden. Auf diese Weise gefährden sie den sicheren Zugang zu vertraulichen Bereichen. Gegen die Verwendung der inzwischen in die Jahre gekommenen Token-Technologie spricht auch die aufwändige und teure Verwaltung von Hardware-Token. Diese müssen am Authentication-Server angemeldet und den jeweiligen Nutzern zugeordnet werden. Nicht selten gehen die Token verloren und stellen dann bis zur Abmeldung automatisch eine Sicherheitslücke dar – oder sie werden, wie im aktuellen Fall, gehackt und müssen ausgetauscht werden. Dieses ist aufwändig und sehr teuer. Vergleichsweise sicher, schlank in der Verwaltung und dementsprechend preiswert sind SMS-basierte Authentifizierungslösungen zu bewerten. Dazu erläutert Markus Seyfried, CTO, Brainloop AG: „Wir bieten für den sicheren Zugriff auf unternehmenskritische Informationen eine so genannte Zwei-Faktor-Authentifizierung an. Dieses mehrstufige Login-Verfahren kombiniert die Verwendung eines Benutzernamens und eines Passworts mit einer kurzlebigen SMS-PIN, die im Echtzeitverfahren generiert und auf das Mobiltelefon des Nutzers gesendet wird. Dort gilt sie nur für eine Sitzung und verfällt nach einer festgelegten Zeit.“ Da Mobiltelefone für die Erreichbarkeit der Anwender von großer Bedeutung sind, fällt deren Verlust rasch auf. Eine Sperrung der SIM-Karte durch den Nutzer ist die logische Folge. Damit stellt dieses Endgerät eine hoch flexible und sichere Infrastruktur dar. Zur Übersicht der Sicherheitsfunktionalitäten der Brainloop AG siehe auch:

[www.brainloop.de/produkte/sicherheit.html](http://www.brainloop.de/produkte/sicherheit.html)

### ANLAGEN

▶ Pressemitteilung "Überlegenheit SMS-basierter Authentifizierung" (PDF, 571,08 KB)

### ANSPRECHPARTNER/KONTAKT

Brainloop AG  
 Frau Nicole Dietrich  
 Franziskanerstr. 14  
 81669 München  
 ☎ +49-89-4446990  
 ✉ [presse.brainloop@googlemail.com](mailto:presse.brainloop@googlemail.com)  
 🏠 [www.brainloop-ag-secure-dataroom.de](http://www.brainloop-ag-secure-dataroom.de)

### ÜBER ÜBER DIE BRAINLOOP AG

Die Brainloop AG mit Firmensitz in München und Boston ist der führende Anbieter von Document