

BRAINLOOP AG: SMS SICHERER ALS SECURITY-TOKEN

BRAINLOOP AG INFORMIERT ÜBER DATENSICHERHEIT IM UNTERNEHMEN

München, 21. Juni 2011 - Vor Kurzem räumte das Sicherheitsunternehmen RSA eine teilweise erfolgreiche Hackerattacke 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 von Token-Systemen für die Einwahl in geschützte IT-Bereiche. Dieses Thema mag für Privatanwender von geringer Bedeutung sein, stellt aber ein ernstzunehmendes Sicherheitsrisiko für Unternehmen und öffentliche Einrichtungen dar, die Datensicherheit bzw. Datenschutz gewährleisten müssen. Für den Dokumentenschutz werden oftmals lokale Authentifizierungstechniken benötigt, die über eine einfache Passwortabfrage hinausgehen und unberechtigten Personen den Zugriff auf vertrauliche Informationen und Dokumente verwehren.

Die Nutzung von Tokens garantiert keine optimale Datensicherheit. Da so genannte Einmal-Passwörter (OTP= One Time Password) bei Tokens bereits vor dem Login existieren, können Login-Daten und OTP „gehisht“ werden. Auf diese Weise gefährden sie den sicheren Zugang zu vertraulichen Dokumenten und versagen dabei, diese effektiv zu schützen. 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. Diese Lösung in Sachen Datensicherheit und Dokumentschutz ist aufwendig und sehr teuer.

Vergleichsweise sicher, schlank in der Verwaltung und dementsprechend preiswert sind SMS-basierte Authentifizierungslösungen. Diese schaffen einen hohen Level von Datensicherheit im Unternehmen und sind den gängigen Token-Lösungen damit überlegen. Markus Seyfried, CTO Brainloop AG, erläutert die eigene Lösung für die Datensicherung im Unternehmen: „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, die hilft, für Dokumentensicherheit und zum Beispiel auch für den Schutz personenbezogener Daten zu sorgen.

Zur Übersicht der Lösungen der Brainloop AG im Bereich Datensicherheit, Dokumentensicherheit, Schutz von Bewerbungsunterlagen und Compliance siehe auch:
<http://www.brainloop.de/produkte/sicherheit.html>

ÜBER DIE BRAINLOOP AG

Die Brainloop AG mit Firmensitz in München und Boston ist der führende Anbieter von Document Compliance Management-Lösungen (DCM) für den hochsicheren Umgang mit vertraulichen Dokumenten. Die Lösungen ermöglichen die lückenlose Nachvollziehbarkeit aller Zugriffe und Änderungen eines Dokumentes und somit die Einhaltung aller Compliance-Auflagen. Zu den Kunden der Brainloop AG zählen u.a. Deutsche Post, Deutsche Telekom, Deutsche Bundesbank, ERGO, ESA (European Space Agency), Landesbank Berlin, Postbank AG, Sky, T-Systems und ThyssenKrupp sowie führende Anwaltskanzleien und Investmentbanken, die den Brainloop Datenraum als Online-Service nutzen.

Die DCM-Lösungen der Brainloop AG sind web-basiert. Dadurch wird die Bearbeitung und Verteilung streng vertraulicher Dokumente auch über Unternehmensgrenzen hinweg ermöglicht. Durch eine

hochsichere Verschlüsselung und eine Abschirmung aller Dokumente vor unbefugtem Zugriff interner und externer Angreifer wird die Zusammenarbeit in ein hochsicheres Umfeld verlagert. Durch vollständige Nachvollziehbarkeit und Protokollierung aller Zugriffe und Aktionen werden weitere Compliance-Voraussetzungen erfüllt. Angewandt werden die Lösungen u.a. in der Gremienkommunikation, in Personalabteilungen sowie beim Finanz- und Vertragsmanagement.

<http://www.brainloop.de>

PRESSEKONTAKT:

Brainloop AG
Franziskanerstr. 14, 81669 München
Tel.: +49 (89) 444 699 0, Fax: +49 (89) 444 699 99
E-Mail: presse@brainloop.de Internet: www.brainloop.de

Copyright © 2011, Brainloop AG. Alle Rechte vorbehalten. Alle Warenzeichen, die in diesem Dokument genannt werden, sind Eigentum Ihrer jeweiligen Besitzer.