

# »Doppelt gesichert ist einfach besser gesichert«

Passwort und Benutzername dienen vielfach als Zugangskontrolle. Doch ganz sicher ist dieses System nicht. Mit Zwei Wege-Authentifizierung allerdings schon.

**WIEN** – Sicherheit spielt über alle Bereiche der IT hinweg eine enorm wichtige Rolle. So ist etwa im Bereich des Content Management- und der Unternehmensportale die Strategie, Benutzername samt Passwort zu vergeben, weit verbreitet. Doch diese erweist sich zunehmend als Sicherheits-Trugschluss. Können Passwörter doch unter anderem mittels Keylogger-Software leicht ausspioniert werden.

Das Wiener Websoftware-Unternehmen Lemon42 setzt dem nun eine neue Strategie entgegen und stellt auf der ITnT 2006 seine neue Zwei Wege-Authentifizierung vor. »Unsere cms42-Software ist bei über 100 Kunden im Einsatz. Diese wickeln umfangreiche Geschäftsprozesse, wie Absatz- oder Supportprozesse, mittels unserer Technologie ab und nutzen diese im Mission Critical-Bereich. Wir haben uns da-

her der Aufgabe gestellt, den Zugriff in unsere Systeme bestmöglich zu sichern und uns für die Implementierung einer Zwei Wege-Authentifizierung entschieden«, erklärt Wolfgang Krainz, Geschäftsführer von Lemon42.

## ONE TIME-CODE VIA SMS

Die Zwei Wege-Authentifizierung sei ein neuartiges Verfahren, welches unerlaubte Nutzung und die Ausführung unerlaubter Tätigkeiten weitgehend verhindern soll. »Im Prinzip geht es hier um die Kombination von Wissen und Besitz: Der berechtigte User verfügt über einen Usernamen und ein Passwort, weiß also diese Daten.« Durch Phishing oder andere Verfahren könnte dieses Wissen allerdings an unberech-

tigte Dritte gelangen. »Ein physisches Objekt dagegen, welches ergänzend zur Authentifizierung dient, muss dem berechtigten User tatsächlich entwendet werden.« Üblicherweise würden solche physischen Authentifizierungs-Tools als Tokens bezeichnet. Die Zwei Wege-Authentifizierung geht also davon aus, dass durch die Kombination von Login und Passwort mit der Nutzung von Tokens, die wieder von physischen Geräten zur einmaligen Nutzung generiert werden, der Systemzugriff bestmöglich gesichert ist.

Lemon42 nutzt bei seinem Ansatz die SMS-Technologie: Nach der Abfrage und Prüfung von Usernamen und Passwort generiert das Produkt einen One Time-Code, der mittels SMS auf das in der Userverwaltung

dem jeweiligen User zugeordnete Mobiltelefon zugestellt wird. Dabei setzt das Unternehmen auf quantenphysikalische Zufallszahlen. Somit wird die reine Kenntnis von Benutzername und Passwort für einen potentiellen Angreifer wertlos. »Damit erreichen wir höchstmögliche Sicherheitsstandards bei der Authentifizierung: Unsere Kunden honorieren diese Entwicklungen sehr«, freut sich Krainz. Ergänzend zur Zwei Wege-Authentifizierung bietet Lemon42 auch weitere Security-Lösungen, die gegen Angriffe wie beispielsweise URL-Hacking, Code Injection oder auch Fiel Manipulation schützen. Die Lemon42-Technologie signiert hierbei den ausgelieferten HTML-Code. [tm] Lemon42, Stand A0334

**ZITAT.**  
»Wir investieren massiv in die Sicherheit unserer Technologie. Mit secure cms42 stellen wir eine echte Innovation im ECM- und WCM-Markt vor.«  
Wolfgang Krainz, Lemon42