SearchSecurity.de

CoSoSys Endpoint Protector 2008 schützt Daten auf USB-Sticks

Firmendaten durch erzwungene Verschlüsselung vor Missbrauch sicher

03.06.2008 | Redakteur: Peter Schmitz

Endpoint Protector 2008 schützt wertvolle Firmenddaten vor Datenverlust oder Diebstahl und bietet Nachverfolgbarkeit des Datentransfers und garantierte Datenverschlüsselung.

USB-Sticks und andere mobile Speichermedien sind trotz der mit ihnen verbundenen Sicherheitsrisiken aus dem Büroalltag nicht mehr wegzudenken. Das Tool Endpoint Protector 2008 von CoSoSys bietet hier mit Trusted Device Technologie und erzwungener Verschlüsselung zwei interessante Lösungsansätze.

Mobile Speichermedien sind in Unternehmen kaum mehr zu kontrollieren. Selbst wenn der Einsatz von USB-Sticks verboten ist, fassen iPods und Smartphones längst selbst Gigabyte an Daten. Brachialster Ausweg ist das unbrauchbar machen von USB-Ports mittels Heißklebepistole, oder – etwas weniger rustikal – das Deaktivieren des USB-Ports im Bios.

Weitaus eleganter sind aber Lösungen, die an den Firmen-PCs den Einsatz von USB-Sticks überwachen, beschränken und in manchen Bereichen sogar ganz verbieten können. Solche Endpoint Security Lösungen haben als Ziel, dass Unternehmen trotz des erlaubten Einsatzes von mobilen Datenspeichern ein Höchstmaß an Kontrolle über ihre wertvollen Daten behalten.

Endpoint Security durch Device-Kontrolle und Verschlüsselung

Die Endpoint-Security-Lösung Endpoint Protector 2008 von CoSoSys arbeitet hier zweigleisig. Zum einen kann das Unternehmen bestimmte PCs oder Benutzer bestimmen über die überhaupt nur Daten auf mobilen Speichermedien abgelegt werden dürfen. Dann ist außerdem noch eine Beschränkung auf bestimmte USB-Medien möglich. Damit wird anhand der einmaligen Device-ID nur einem ganz bestimmten USB-Stick erlaubt im Firmennetzwerk Daten aufzunehmen. Das CoSoSys-Tool überwacht und protokolliert außerdem den Datentransfer von Desktops auf autorisierte USB-Medien mittels File Tracing und File Shadowing.

Ergänzt wird diese Device-Kontrolle nun auch noch durch eine erzwungene Verschlüsselung. Dabei kann der Administrator mittels Policy festlegen, dass Daten auf ein Trusted Device ausschließlich verschlüsselt gespeichert werden dürfen. Kopiert nun ein Anwender Dateien auf einen vertrauenswürdigen UBS-Stick verschlüsselt die Software diese Daten automatisch mit einem 256 Bit AES Schlüssel.

Endpoint Protector 2008 steuert im Netzwerk alle Rechte mittels eines einfachen Policy Managers, der sich über ein Webinterfache bedienen läßt. Systeme die vom Netzwerk getrennt sind bleiben auch weiterhin nach der letzten aktiven Policy gesichert. Praktisch für Administratoren sind darüber hinaus auch die leistungsfähigen Reporting-Funktionen.

Der Server-Teil der Endpoint-Protector-2008-Lösung läuft auf Windows Server 2003 oder Linux-Systemen, Als Webserver und Datenbanken arbeitet das System mit Apache oder IIS und mit Microsoft-SQL- oder MySQL-Datenbanken zusammen. Client-seitig unterstützt das Tool Windows XP und Vista. Endpoint Protector 2008 kostet bei für 50 zu schützende Clients etwa 1600 Euro und bei 100 zu schützenden Clients etwa 2100 Euro.