www.All-About-Security.de

Veröffentlicht am: 03.06.2008

CoSoSys schützt USB Datenspeicher mittels forcierter Verschlüsselung

Autor: kol

Endpoint Protector 2008 verhindert Datendiebstahl und Datenverlust in Unternehmen. Neues Sicherheitsmerkmal der Software für die Verwendung von tragbaren Datenspeichern wie USB Sticks ist die „erzwungene“ Verschlüsselung von Daten.

Durch die Verfügbarkeit von tragbaren Datenträgern und Lifestyle-Geräten wie externen Festplatten und MP3 Player vereinfacht sich die Art und Weise wie wir arbeiten, leben und Daten transportieren. Außer Frage stehen Produktivitätsgewinne durch die Benutzung von mobilen Datenträgern wie USB Sticks. Doch diese Geräte bergen ganz erhebliche Risiken bezüglich Datendiebstahl, Datenverlust bis hin zur Industriespionage.

Die Unternehmen selbst sehen ihre Innovationen, das Know-How und Vertrauliches als Ziel von Datendieben. Zusätzlich sind alle Organisationen von Seiten des Gesetzgebers verpflichtet, ihre Kundendaten vor jeder Art von Fremdzugriffen zu schützen.

Endpoint Protector 2008 von CoSoSys ermöglicht es Unternehmen, sich den Produktivitätszuwachs von tragbaren Speichermedien nützlich zu machen. Zusätzlich verhindert Endpoint Protector für das Unternehmen Risiken wie Datenverlust oder unautorisiertes Kopieren (Diebstahl) von Daten. Mit der Software definiert ein Unternehmen die für den Betrieb zugelassenen externen Datenträger. Diese können eindeutig Mitarbeitern und Computern zugeordnet werden. Der Datentransfer von autorisierten Geräten zwischen mobilem Datenspeicher und PC kann mit den Funktionen „File Tracing“ und „File Shadowing“ überwacht werden.

Mit der neuen Version von Endpoint Protector 2008 wird das so genannte TrustedDevice Konzept realisiert. In kurzen Worten: Alle Daten, die auf einen zuvor autorisierten tragbaren Datenspeicher (TrustedDevice) abgespeichert werden, sind „erzwungen“ mit einem 256bit AES Algorithmus verschlüsselt.

Ein Abspeichern von Daten aus dem Firmennetzwerk in unverschlüsseltem Zustand auf externe Datenspeicher ist damit unmöglich.

Das Risiko eines Datenverlustes im Falle eines verlorenen oder gestohlenen Datenspeichers (z.B. USB Stick) besteht nicht mehr. Die gespeicherten Informationen können von Dritten nicht gelesen werden.

Endpoint Protector 2008 ist ein wichtiger Bestandteil für Unternehmen, um sich gegen Datenverlust oder vorsätzlichen Datendiebstahl zu schützen. Die Lösung realisiert die nahtlose Nachverfolgung von Datentransfers von und zu tragbaren Datenspeichern und garantiert die Datenverschlüsselung auf eingesetzten USB Datenträgern.

Als Data Loss Prevention (DLP) Lösung kann Endpoint Protector 2008 Server auf Windows 2003 Servern und auch auf Linux Servern (z.B. Debian) betrieben werden. Die Software kann mit geringem Aufwand in eine bestehende Microsoft Umgebung eingebunden werden oder wahlweise separat und kostenneutral unter Linux betrieben werden.

Die Software schützt Client Systeme mit Windows XP und Vista.
Das WEB-basierte Cockpit zur Administration und zum Reporting besitzt einen intuitiv bedienbaren „Policy Builder“. Selbst die Verwaltung vieler Benutzer ist mit Hilfe einer Active Directory Synchronisation bequem realisierbar.

Gedruckt am: 03.06.2008