SearchSecurity.de

Neues Modul für CoSoSys Endpoint Protector 4.1

Data Loss Prevention für die Cloud

21.05.12 | Redakteur: Stephan Augsten

Mit dem Endpoint Protector 4.1 lässt sich der Datenfluss in die Cloud kontrollieren.

Cloud-Speicher wie Dropbox, Google Drive, iCloud oder Microsoft Skydrive sind nützlich, bergen aber für Unternehmen das Risiko unerwünschten Datenabflusses. Ein neues DLP-Modul für den Endpoint Protector von CoSoSys soll diese Gefahr bannen.

Bei der Data Loss Prevention (DLP) haben die Anbieter bislang vornehmlich traditionelle Schnittstellen adressiert. Hierzu gehören beispielsweise Hardware-Schnittstellen wie USB-Ports und DVD-Laufwerke, Kommunikationskanäle wie E-Mail und Instant Messaging sowie Netzwerk-Verbindungen.

Doch mit dem Trend hin zu Cloud-Diensten steht die Datensicherheit vor ganz neuen Herausforderungen. Der DLP-Spezialist CoSoSys begegnet diesem Problem mit einer Vorabversion des Endpoint Protector Version 4.1. Die Gerätekontrolle wurde um ein neues „Content Aware Protection"-Modul erweitert.

Noch bevor eine Datei über das Netzwerk einen Windows-PC verlässt, wird Sie „on the fly" auf ihren Inhalt überprüft. Für einen Datentransfer müssen PC und/oder Benutzer über entsprechende Berechtigungen verfügen. Zentral lässt sich kontrollieren und bestimmen, wer vertrauliche Daten bewegt.

Endpoint Protector erkennt Datei-Inhalte und -Typen

CoSoSys stellt vor allem die unkomplizierte Bedienung des „Content Aware Protection"-Moduls heraus. So sei es mit nur wenigen Mausklicks möglich, Dateiinhalte mit internen Richtlinien abzugleichen, sie als sensibel zu markieren und Transfers zu protokollieren oder bei Bedarf zu stoppen. Regel und Filter lassen sich nicht nur auf

den Inhalt, sondern auch auf Datei-Typen anwenden.

In der Praxis ist es mithilfe des Regelwerks beispielsweise möglich, den Versand von Dokumenten via E-Mail oder Instant Messenger zu stoppen, wenn sie Kreditkartendaten, Sozialversicherungsnummern und bestimmte Schlüsselwörter enthalten. Content Aware Protection enttarnt jene Benutzer, die gegen die Richtlinien verstoßen.

Zu den unterstützten Cloud-Speichern gehören beispielsweise Google Drive, Dropbox, iCloud oder SugarSync. Der Endpoint Protector 4.1 mit dem Modul Content Aware Protection ist als Hardware oder virtuelle Appliance erhältlich. Auf der Webseite findet sich neben einer Liste der unterstützten Anwendungen (E-Mail-Clients, Instant Messenger, Browser etc.) auch eine kostenlose Testversion.