

## Sicherheit

### Meldung

#### DLP unter Linux

CoSoSys hat die DLP-Lösung 'Endpoint Protector' erweitert. Das neue Modul 'Content Aware Protection' für Linux-Desktops prüft beim Datentransfer Inhalte, Semantiken und Dateiformate auf Rechnern mit Linux-Distributionen. Die Funktion soll so die Übermittlung von sensiblen Daten nach außen und damit Datenverluste durch interne Benutzer verhindern.

"Content Aware Protection" [1] für Linux-Desktops ergänzt die Gerätekontrolle für Linux, die die physischen Ports an den Endgeräten überwacht, und verhindert, dass Mitarbeiter Unternehmensdaten auf tragbare Speichermedien kopieren. Der Schutz vor Datenverlust und Datendiebstahl wird hierfür auf internet-basierte Schnittstellen ausgeweitet und der Transfer sensibler Informationen über Cloud- und Webdienste wie zum Beispiel Webmail, ownCloud oder Skype unterbunden.

Dafür werden die Dateien in Bewegung nach Dateitypen und vordefinierten Inhalten wie personenbezogene Daten und Kreditkarten-, Konto- oder Ausweisnummern gefiltert. Für die Prüfung auf unternehmensspezifische Inhalte lassen sich individuelle Wörterbücher mit Schlüsselbegriffen und Regulären Ausdrücken zur Analyse von Zeichenketten anlegen.

Endpoint Protector ist eine Client-Server-Lösung und als Hardware- oder virtuelle Appliance erhältlich. Sie stellt die Funktionen Device Control und Content Aware Protection zur Verfügung und unterstützt beide auf Windows XP bis Windows 10 (32 und 64 Bit), auf Mac OS X sowie auf den Linux-Distributionen Ubuntu, OpenSUSE, CentOS und RedHat. Die Unterstützung weiterer Distributionen ist laut Hersteller vorgesehen. Die Funktionalität für Linux wird mit der Server-Version 4.4.1.0 von Endpoint Protector ausgeliefert.

Weitere Infos:

[1] [www.endpointprotector.com/linux](http://www.endpointprotector.com/linux)

27.05.2016/dr