www.All-About-Security.de

Veröffentlicht am: 03.12.2007

Institute der Universität Freiburg schützen USB Schnittstellen mit CoSoSys Endpoint Protector

Autor: mat

Mit Endpoint Protector können PC-Administratoren USB Schnittstellen von PCs kontrollieren. Delikte wie Missbrauch von IT Ausstattung, Datenklau und Wirtschaftsspionage durch mobile USB Datenspeicher werden durch Endpoint Protector zuverlässig verhindert.

CoSoSys, Anbieter für Endpoint Security Lösungen, gibt bekannt, dass die Wirtschaftswissenschaftlichen Institute der Albert-Ludwigs-Universität Freiburg auf den Schutz der USB Schnittstellen durch Endpoint Protector von CoSoSys vertraut.

Die Software wird in drei Räumen mit jeweils 20-60 Computerpool Rechnern der Wirtschaftswissenschaftlichen Institute an der Wirtschafts- und Verhalten-Wissenschaftlichen Fakultät eingesetzt. Die Computerpool Rechner haben High-Speed Internetanschluss und sind für Studenten als Arbeitsmittel zugänglich.

Endpoint Protector erlaubt es, Datentransfers über USB Schnittstellen zu tragbaren Datenspeichern wie USB Sticks, iPods, Digitalkameras etc. verlässlich zu unterbinden. Das „Whitelist-Verfahren" ermöglicht eine volle Kontrolle, im Bedarfsfall kann der Datentransfer gezielt erlaubt werden.

Studenten können nun keine Inhalte wie Musik oder Filme, die beispielsweise Copyright-Richtlinien unterliegen, über die Computerpool Rechner auf Ihre iPods, MP3/MP4 Spieler oder mobile Datenträger wie USB Sticks laden. Damit wird zusätzlich auch das unerlaubte Kopieren von Informationen auf tragbare Speichermedien verhindert, ein potentieller Virenbefall wird unterbunden, und die Mal- oder Spyware Infektion über die USB Schnittstelle ist nicht möglich.

Für den Administrator der Computerpool Rechner bietet das WEB Browser basierte Management und das „Whitelist-Verfahren" von Endpoint Protector entscheidende Vorteile:

- Eine Sicherheits-Richtlinie der Universität untersagt die freie Verwendung von USB Speichergeräten, wobei aber situationsbedingt auch eine Aufhebung der Sperrung möglich sein muss („Whitelist-Verfahren").
- Mit dem WEB basierten Management von Endpoint Protector kann der Administrator die Verwendung einzelner USB Speichergeräte ad hoc von jedem Rechner im Netz konfigurieren. Ebenso ist eine Vorkonfigurierung von Listen vertrauenswürdiger USB Speichergeräte, Benutzer, Benutzergruppen und PCs möglich.

Endpoint Protector (Client) ist kompatibel zu Desktoprechnern mit Windows Vista, Windows XP und Windows 2000.

Das zentrale Management (Server) kann auf Windows 2000, Windows 2003 und Linux (Debian) Plattformen installiert werden.

Gedruckt am: 09.12.2007