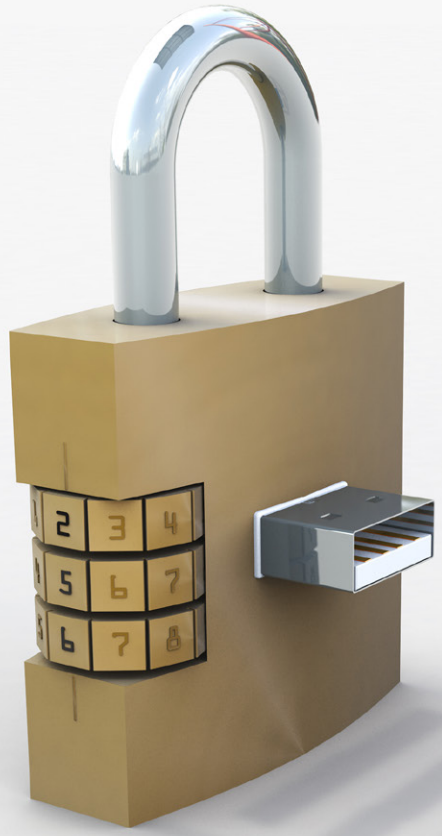
Umfassende Regulierung der Nutzung von
USB-Sticks und anderen mobilen Datenträgern



Inhaltsprüfung für gespeicherte Daten

Bewertung des Datenleck-Risikos

Zugriffssteuerung

Window Security.com READERS' CHOICE WINNER

SC MAGAZINE

OPSWAT. BRONZE CERTIFIED Device Access Control

Weitere Informationen und kostenlose Testversion:

gfisoftware.de/endpointsecurity

Microsoft Partner
Gold Application Development
Silver Midmarket Solution Provider

GFI EndPointSecurity™

Kontrolle von iPods, USB-Sticks und anderen mobilen Endgeräten

Umfassende Regulierung der Nutzung von USB-Sticks und anderen mobilen Datenträgern

Beliebte Mobilgeräte wie Smartphones, Multimedia-Player und sonstige Devices mit Netzwerkzugang kommen auch in Unternehmen zum Einsatz, ebenso wie USB-Sticks und andere tragbare Massenspeicher – und fördern Diebstahl und Verlust wichtiger geschäftlicher Daten. Ebenso hoch sind Sicherheitsrisiken und rechtliche Gefahren durch eingeschleppte Viren und Raubkopien.

Zum Schutz vor Angriffen von außen sind in den meisten Fällen Antiviren-Software, Firewalls und sonstige Sicherheitslösungen für E-Mail und Internet-Nutzung im Einsatz. Doch Bedrohungen lauern auch firmenintern: Vielfach wird übersehen, wie einfach Mitarbeiter mobile Datenträger an Netzwerkrechner anschließen können. Vertrauliche und unternehmenskritische Informationen sind binnen Minuten in großem Umfang kopiert – unbemerkt.

Ein komplettes Sperren aller USB-Schnittstellen ist jedoch keine praktikable Lösung, um Sicherheitsrisiken zu minimieren. GFI EndPointSecurity hilft Ihnen, die Verwendung mobiler Speichermedien gezielt zu überwachen und zu steuern, auch unter genauer Berücksichtigung von übertragenen Daten und Benutzern.

Funktionsweise

Zur Zugangskontrolle wird ein manipulationssicherer, für Anwender unsichtbarer Agent auf Benutzerrechnern im gesamten Netzwerk installiert – automatisch, schnell und einfach. Selbst Mitarbeiter mit Administrationsrechten können Einstellungen des Agenten nicht ändern.

Abwehr von Bedrohungen dank differenzierter Zugriffssteuerung

Legen Sie zentral fest, welche Benutzer keine portablen Speichermedien verwenden dürfen, um das Risiko von Datendiebstahl oder Virenbefall über tragbare Geräte zu minimieren. Autorisierten Mitarbeitern hingegen kann der Zugriff auf ausgewählte Speichergeräte gezielt gestattet werden. Die von erfahrenen Anwendern ohnehin leicht zu umgehende, aufwendige Deaktivierung von Schnittstellen per BIOS ist somit nicht erforderlich.

Zugriffsprotokollierung für portable Geräte im Netzwerk

Lassen Sie gerätespezifische Benutzerzugriffe im Ereignisprotokoll und in einer zentralen SQL-Server-Datenbank protokollieren. Auch auf portablen Speichermedien geöffnete Dateien werden genau erfasst.

Verschlüsselung tragbarer Speichermedien

Legen Sie fest, dass Daten nur verschlüsselt auf USB-Medien gespeichert werden dürfen. Ein spezielles Traveler-Tool gestattet es berechtigten Anwendern, auch außerhalb des Netzwerks auf entsprechend geschützte Dateien zuzugreifen.

Weitere Funktionen

- Richtlinien-Assistent für Regeln zur granularen Zugriffssteuerung
- Täglicher/wöchentlicher Überwachungsbericht
- Statusüberwachung und Warnungen in Echtzeit
- Umfassende Berichte zur Verwendung mobiler Speichermedien mit dem Zusatzmodul GFI ReportPack
- Unterstützung von Microsoft Windows 7 BitLocker To Go
- Individuell anpassbare Popup-Meldungen zu Gerätesperrungen für Benutzer
- Backend-Datenbank zur Protokollierung und Anzeige von Benutzeraktivitäten und Geräteverwendung
- Einrichtung von Computer-Gruppen für Abteilungen, Domänen u. Ä.
- Unterstützung Unicode-kompatibler Betriebssysteme

Gratis-Testversion herunterladen unter: **gfisoftware.de/endpointsecurity**

Die wichtigsten Vorteile auf einen Blick

Verwaltungsfreundliche Zugriffssteuerung für tragbare Speichermedien zur Verhinderung von Datenabfluss und -diebstahl

Datensicherheit bei Diebstahl oder Verlust von Wechselspeichern dank Verschlüsselung

Bewertung des Datenleck-Risikos durch tragbare Speichermedien für alle Endgeräte plus Empfehlung von Schutzmaßnahmen

Vollständige Verschlüsselung von Wechselmedien

Gerätesperrung nach Kategorie, Dateierweiterung, Schnittstelle oder sogar Seriennummer

Zeitlich begrenzbare Freigabe von Geräten oder Schnittstellen

Vollständige Übersicht zu allen Vorteilen: **www.gfisoftware.de/endpointsecurity**

Systemanforderungen

Microsoft Windows 2000 (SP4), XP, Vista, 7, 8, Windows Server 2008, 2012 (32- und 64-Bit-Versionen)

Microsoft Internet Explorer 5.5 oder höher

Microsoft .NET Framework 4.0

Port: TCP-Port 1116 (Standard)

Datenbank-Backend: Microsoft SQL Server 2000, 2005, 2008; falls nicht verfügbar:

automatischer Download von Microsoft SQL Server Express mit anschließender Installation und Konfigurierung

GFI®

www.gfisoftware.de

Kontaktdaten aller GFI-Niederlassungen weltweit:
www.gfisoftware.de/contact-us