

iAdministrator

Das Magazin für professionelle System- und Netzwerkadministration

**Im Vergleichstest:
Vier Windows-Tools
zur Schnittstellenüberwachung
Kein Zugriff unter diesem Anschluss**

**Sonderdruck
für ProSoft**

Im Vergleichstest: Vier Windows-Tools zur Schnittstellenüberwachung

Kein Zugriff unter diesem Anschluss

von Jürgen Heyer



Quelle: Pixello.de

Zugriff verboten: Deviceblocker kontrollieren, wer wann wo Anschluss an die Clients im Netzwerk findet

Noch immer unterschätzen viele Firmen das interne Gefährdungspotenzial, wenn es um den Schutz ihrer Daten geht. Um dennoch nicht generell die Nutzung mobiler Speichermedien wie USB-Sticks zu unterbinden, bieten sich spezielle Deviceblocker-Tools an. Diese erlauben die Kontrolle darüber, welche Speichermedien oder Peripheriegeräte wann und wo angeschlossen werden dürfen. IT-Administrator hat in einem großen Vergleichstest vier der gängigen Deviceblocker unter die Lupe genommen. Die Kandidaten: Centennial DeviceWall, Centertools Drivelock, DeviceLock und Safend Protector / Utimaco Safeguard PortProtector. Überzeugen konnten letztlich alle, doch der feine Unterschied macht's.

Mehrere GByte große USB-Sticks mit Abmessungen kleiner als ein Finger, teilweise versteckt in Armbanduhren und anderen Gebrauchsgegenständen, sowie winzige Speicherkarten bieten vielfältige Möglichkeiten, Daten unkontrolliert in das Firmennetz einzuschleusen oder auch von dort abzuziehen. Das gleiche gilt prinzipiell für die vorhandenen Disketten-, CD- und DVD-Laufwerke, auch wenn USB-Sticks aufgrund ihrer Größe eher prädestiniert sind. Eine wenig praktikable Lösung ist es, alle entsprechenden Anschlüsse auszubauen oder etwa zu verkleben, gibt es doch immer wieder wichtige Gründe, bestimmte Geräte dediziert für einzelne Mitarbeiter zuzulassen.

Hilfreicher sind hier Tools zur Schnittstellenüberwachung, sogenannte Deviceblocker. IT-Administrator hat sich vier auf dem deutschen Markt verbreitete Deviceblocker angesehen: DeviceWall 4.62

CAE (Content Aware Edition) von Centennial Software, DriveLock 5.0 von Centertools, DeviceLock 6.2.1 vom gleichnamigen Hersteller und Protector 3.3 von Safend. Das fünfte Produkt, Utimaco Safeguard PortProtector, ist keine eigenständige Entwicklung, sondern entspricht der Software von Safend und wurde von Utimaco nur mit eigenem Branding versehen. Funktional ist es absolut identisch. Allerdings können wie zum Testzeitpunkt die Versionsstände etwas unterschiedlich sein. So liefert Utimaco zum Test noch die Version 3.2.

Safend Protector 3.3 / Utimaco Safeguard PortProtector

Die in Deutschland von Prosoft vertriebene Software "Protector" des Herstellers Safend hat auch Utimaco lizenziert und bietet es mit einem eigenen Branding unter dem Namen "Safeguard PortProtector" an. Zum Testzeit-

punkt war die von Prosoft gelieferte Version 3.3 etwas aktueller, als die von Utimaco angepasste Version 3.2. Im Weiteren beschreiben wir den Funktionsumfang der Version 3.3.

Als Installationsvoraussetzung ist beim Safend Protector der IIS gefordert, hinsichtlich einer Datenbank nutzt das Programm entweder eine eigene, die mit eingerichtet wird (MySQL), oder einen MS SQL-Server (SQL 2000 oder höher). Im Installationsverlauf können bei Bedarf die beiden benötigten Ports 443 zu den Clients und 4443 zur Konsole geändert werden, außerdem wird ein Password Encryption Key abgefragt. Die Installation der zentralen Serverkomponenten kann unter Windows XP oder auf einem Windows 2003 Server erfolgen. Breiter ist die Clientunterstützung, die auch Windows 2000 und Vista beinhaltet. Mit Version 3.3 ist eine Instal-

lation als Cluster möglich, damit sich mehrere Server die Aufgabe teilen können und auch der Ausfall eines Systems kompensiert werden kann.

Regel-Vorlagen für Compliance

Beim Start der Management-Konsole ist eine Anmeldung erforderlich. Dabei kommen nicht zwingend die Credentials des angemeldeten Windows-Benutzers zum Einsatz. Die Konsole besitzt ein etwas gewöhnungsbedürftiges und schlichtes Outfit, da keinerlei Schaltflächen sichtbar sind, sondern die einzelnen Begriffe wie Hyperlinks bei Anwahl die Farbe wechseln. Recht übersichtlich ist die Aufteilung der Funktionen auf mehrere Registerblätter. Statt bei der Installation die Einstellungen für eine initiale Regel abzufragen (sollen standardmäßig einige oder alle Geräte gesperrt oder zugelassen werden?), sind hier insgesamt neun Standard-Policies angelegt, die sich dann als Basis für eigene Regeln anbieten. Dazu gehören Policies, die sich an den Vorgaben von HIPAA, PCI und SOX orientieren. Am besten dupliziert der Administrator die Regel, die seinem Ziel am meisten entspricht, führt dann seine individuellen Anpassungen durch und speichert das Resultat unter eigenem Namen.

Das Regelwerk unterscheidet beim Zugriff auf die Geräte nicht nur zwischen Erlauben, Verweigern und Lesezugriff, sondern gibt alternativ auch einen Verschlüsselungszwang vor, so dass beispielsweise beim Speichern von Dateien auf einem USB-Stick grundsätzlich verschlüsselt werden muss. Mit der Version 3.3 lässt sich nicht nur die Verschlüsselung auf USB-Flash-Laufwerken, Memory Sticks und SD-Karten erzwingen, sondern auch auf externen Festplatten und CD/DVD-Laufwerken. Das Programm unterteilt die Kontrollmöglichkeiten in fünf Gruppen. Dies sind Ports wie USB, FireWire, PCMCIA, Seriell, Parallel, WiFi, IrDA und Bluetooth, dann Geräte wie PDAs, Drucker, Telefone, Netzwerkkarten, Au-

*Anmerkung der Redaktion: Die deutsche Version ist inzwischen verfügbar.

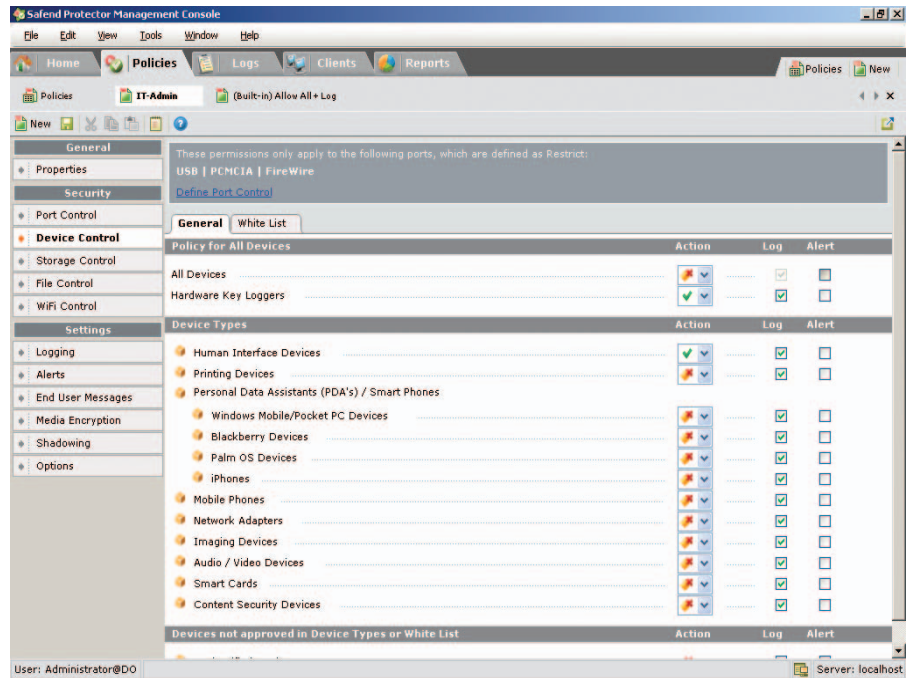


Bild 7: Safend Protector ermöglicht für jeden Gerätetypen nicht nur die Festlegung einer Sperr-Regel, sondern auch die Maßgabe, ob Ereignisse in die Log-Datei eingetragen werden oder einen Alarm auslösen sollen

dio- und Videogeräte, weiterhin Speichergeräte wie externe Festplatten und CD-/DVD-Laufwerke und zuletzt Datentypen sowie WiFi-Geräte.

Vorteilhaft ist, dass sich die diversen Meldungen für die Endanwender mit individuellen Texten belegen lassen. So kann das an sich englischsprachige Programm problemlos mit deutschen Fehlermeldungen versehen werden. Darüber hinaus will Safend noch im Laufe des Jahres eine deutsche Version veröffentlichen.*

Der Protector ermöglicht eine automatisierte Verteilung der Client-Agenten, setzt hierbei aber ebenso wie DriveLock auf eine Installation via Login-Skript oder mit Hilfe von Gruppenrichtlinien. Eine einfache, per Mausklick bedienbare Verteilerroutine wie bei DeviceWall und DeviceLock ist nicht implementiert. Etwas unglücklich ist auch, dass die Clientinstallation abschließend einen Neustart verlangt. Bezüglich der Kommunikationsfreudigkeit des Agenten kann der Administrator wählen, ob dieser in der Taskleiste als Icon sichtbar ist und mittels Meldungsblasen anzeigt, wenn sich die

Policies geändert haben oder wenn er ein Gerät blockiert hat. Der Agent kann aber genauso absolut schweigsam und unsichtbar im Hintergrund seine Arbeit verrichten. Mittels Deinstallations-Passwort lässt sich verhindern, dass ein Anwender den Agenten heimlich wieder entfernt, um die Schnittstellen wieder unkontrolliert nutzen zu können. Abgesehen davon würde ein fehlender Agent auch bei der nächsten manuellen Policy-Verteilung auffallen, wenn die Aktualisierung nicht klappt.

Gelungene Policy-Zuweisung und Schattenkopien

Sehr flexibel gestaltet sich die Policy-Zuweisung, wobei der Administrator zur Auswahl der Clients entweder nach Namen filtern oder im Active Directory browsen kann. Je nach Bedarf weist er direkt die Clients zu oder verknüpft eine Policy mit einer OU, einer Gruppe oder einem Benutzer. Damit lassen sich Policies nicht nur an Benutzer, sondern auch an Clients binden, was beispielsweise bei Kiosk-Systemen sinnvoll ist. Bei der Zuweisung ist es durchaus möglich, dass für einen Client mehrere Regeln wirksam sind. Im Hand-

buch ist an diversen Beispielen beschrieben, wie das Policy Merging funktioniert und wie sich die so entstehenden effektiven Regeln ermitteln lassen.

Wie bei den anderen Produkten auch lässt sich eine Zugriffssperre für eine gewisse Zeit aufheben. Hierzu wird ein Client-spezifisches Passwort generiert und an den Anwender übermittelt, damit dieser damit seinen Arbeitsplatz entsperren kann. Wird ein Client vom Netz genommen, greifen die Regeln weiterhin. Nicht vorhanden ist allerdings ein Scheduler, der eine zeitabhängige Steuerung erlaubt.

Ebenso wie DeviceLock und DriveLock unterstützt Safend Protector mit der Version 3.3 das so genannte File Shadowing, bei dem von allen Dateien, die zu und von einem Wechselmedium kopiert werden, ein Duplikat in einem Verzeichnis abgelegt wird. So lässt sich jederzeit kontrollieren, welche Dateien die Anwender bewegen, außerdem kann ein Administrator beispielsweise einen zusätzlichen Virenschanner einsetzen, der unabhängig von den Clients dieser Dateien nochmals auf Virenbefall prüft. Optional lässt sich Safend Protector auch mit dem Produkt Information Leakage Prevention (ILP) von Websense kombinieren. ILP prüft dann alle bewegten Dateien auf ihren Inhalt.

Zwei weitere besondere Features von Safend Protector sind die Zusammenarbeit mit OPSEC (Open Platform for Security) von Checkpoint und NAC von Cisco. Mittels OPSEC und NAC lässt sich der Safend-Client-Status (genutzte Version, letztes Policy-Update, Policy-ID, genutzter Server) ganz detailliert verifizieren und so verhindern, dass falsch konfigurierte Clients genutzt werden.

Ausgelagerter Gerätescanner

Im Unterschied zu den übrigen Testkandidaten hat Safend die Funktion zur Erkennung von angeschlossenen Geräten in ein eigenes Programm gepackt. Das

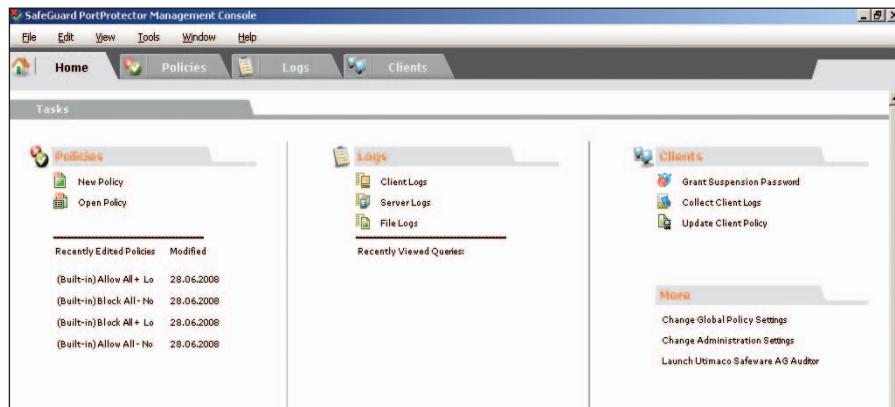


Bild 8: Mitunter gewöhnungsbedürftig ist die GUI von Safend Protector / Utimaco Safeguard PortProtector

Programm "Auditor" scannt auf Anforderung einen oder mehrere Clients, wobei die Systeme aus dem Active Directory ausgewählt oder als IP-Bereich angegeben werden können. Weiterhin lässt sich die Analyse auf bestimmte Schnittstellen wie USB, FireWire oder PCMCIA beschränken. Das Resultat wird in eine XML-Datei geschrieben. Um nun die Scandaten zur Erstellung einer individuellen Berechtigungsliste (Whitelist) zu verwenden, muss die XML-Datei im Hauptprogramm eingelesen werden, womit die erkannten Geräte in der zentralen Datenbank landen. In der Praxis erweist sich diese Vorgehensweise als etwas umständlich und langwierig.

Insgesamt präsentieren sich die Produkte Safend Protector beziehungsweise Utimaco Safeguard PortProtector als recht mächtig und dennoch einfach bedienbar. Zwar muss sich der Administrator an das etwas eigenwillige Design der Benutzeroberfläche gewöhnen, er wird aber recht schnell die ersten erfolgreichen Konfigurationen durchführen können. Etwas umständlich ist die Trennung des Auditing-Tools vom Hauptprogramm. Mit der Vista-Unterstützung ist das Programm auch für aktuelle Clients einsetzbar.

*Anmerkung der Redaktion: Da die deutsche Version zum Zeitpunkt des Tests noch nicht verfügbar war, wurde im Originaltext im Heft als Produkt-Nachteil die "englische Benutzeroberfläche" angegeben. Dies wurde nun aufgrund der inzwischen vorliegenden deutschen Benutzeroberfläche im Sonderdruck entfernt.

Produkt

Programm zur Kontrolle lokaler Client-Zugriffe auf CD-/DVD-Laufwerke, USB-Ports und WiFi-Verbindungen

Hersteller

Safend
www.safend.com, www.prosoft.de

Preis

Safend Protector ist bei Prosoft ab 25 Lizenzen für je 23 Euro erhältlich, Utimaco Safeguard PortProtector kostet bei 10 Lizenzen je 30 Euro, ab 100 Lizenzen je 24 Euro.

Vorteile

- > Eingängige Bedienung
- > Vorbereitete Policies
- > Rechte auf Benutzer, Gruppen, OUs und Computer anwendbar

Nachteile*

- > Keine zeitabhängigen Regeln
- > Ausgelagerter Gerätescanner

So urteilt IT-Administrator (max. 10 Punkte)

Installation 8

Funktionsumfang 8

Bedienung und Konfiguration 8

Active Directory-Integration 9

Betriebssystemunterstützung 8

Gesamtbewertung 8,2

Protector 3.3 / Safeguard PortProtector