

DX-Union Device Management

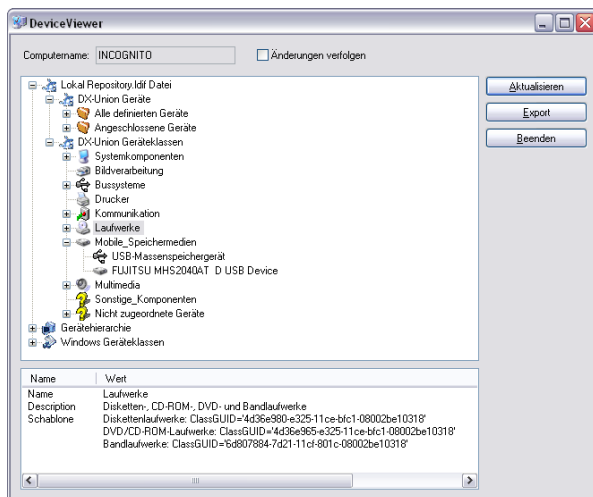


MANAGEMENT VON PLUG&PLAY-GERÄTEN MIT DX-UNION

Externe Geräte können dank der USB-Schnittstelle und den Möglichkeiten der Plug&Play-Integration einfach und unkompliziert an Windows-Systeme angeschlossen werden. Die für die Geräte benötigten Treiber sind in der Regel bereits im Windows-Medium enthalten, was mit einer Sicherheitslücke verbunden ist: unerwünschte Applikationen können in das System gelangen und unternehmenskritische Informationen können herausgeschleust werden.

Oftmals sind die Schäden, die durch Sicherheitslücken innerhalb einer Organisation entstehen, viel größer als die durch Außenstehende verursachten Schäden. Dabei ist sowohl das Einschleusen von arglistigen Programmen, so genannte Malware, als auch das Kopieren sensibler Daten festzustellen. Die dadurch entstehenden Produktivitäts- und Stabilitätsprobleme sind bei einer Beurteilung ebenfalls zu berücksichtigen.

Moderne Geräte wie USB-Sticks oder USB-Festplatten erlauben das Kopieren großer Datenmengen. Aus normalen Festplatten kann mit geringen finanziellen Mitteln (weniger als 20 Euro) eine USB-Festplatte gemacht werden. Damit stehen Datenvolumina von 64 MB bis 200 GB zur Verfügung.



PDA's und Digitalkameras lassen sich einfach an einem PC betreiben. Sie werden wie andere Speichermedien in das Betriebssystem eingebunden und können daher für das Kopieren von Daten verwendet werden.

Ein komplettes Sperren der USB-Schnittstelle unterbindet die Nutzung der Geräte und macht ein Kopieren unmöglich. Neuere Notebooks bieten oftmals

keine PS2-Anschlüsse mehr für Mäuse, so dass diese Form des Schutzes ausfällt. Auch bieten viele Druckermodelle nur noch USB-Anschlüsse.

Für Windows XP SP2 bietet sich ein eigener Schutz an: mit Hilfe bestimmter Registry-Einträge kann das Schreiben auf USB-Massenspeichergeräte unterbunden werden. Da ein Auslesen der Daten jedoch uneingeschränkt möglich bleibt, ist diese Lösung begrenzt.

Eine weitere Möglichkeit ist es, nur die für spezielle Geräte notwendigen Treiber zu installieren oder Plug&Play für bestimmte Geräteklassen abzustellen. Diese Möglichkeiten erfordern jedoch für jede Änderung ein aktives Eingreifen am PC.

Eine effektive und umfassende Lösung ist ein Administrations-Tool, das die gewünschten Sperrungen und Freigaben von zentraler Stelle aus durchführt.

Der DX-Union Device Inspector verhindert das unerwünschte Anschließen von Plug&Play-Hardware durch eine WhiteListe. Hierdurch sind alle durch den DX-Union Device Inspector überwachten Geräteklassen, wie z. B. Diskettenlaufwerke und Speichermedien, zuerst einmal gesperrt. Dieses Vorgehen erfordert kein kontinuierliches Nachpflegen beim Auftreten neuer Geräte, was wiederum schnell zu einer Sicherheitslücke werden kann. Eine Freigabe für ganze Geräteklassen oder spezielle Geräte kann durch den Administrator erfolgen. So kann z. B. eine spezielle Digitalkamera zugelassen werden, wohingegen Digitalkameras im Allgemeinen nicht zugelassen sind.

Freigaben können sogar benutzer- oder PC-spezifisch erfolgen. Geräteklassen oder spezielle Geräte werden dadurch nur für einzelne Benutzer oder an bestimmten PCs zur Verwendung frei geschaltet.

Für die lokalen Platten und mobile Speichermedien können sehr feine Rechte für die erlaubten Aktionen vergeben werden. Die Rechte zum Lesen, Schreiben, Ausführen, Löschen, Umbenennen und sogar zum Anzeigen von Dateien können in Abhängigkeit von Benutzer, PC und Applikation eingestellt werden. Damit ist eine Definition möglich, die beispielsweise einen Benutzer an einem bestimmten PC nur mit dem Notepad Textdateien zum Lesen öffnen lässt, er diese aber nicht schreiben, löschen oder umbenennen darf sowie keine exe-Dateien im Explorer angezeigt bekommt.

Die Konfigurationsdaten liegen in der DX-Union Datenhaltung und werden über die bekannte Administrationsoberfläche verwaltet. Damit ist ein Single Point of Administration gegeben.

Der DX-Union Device Inspector liest während des Boot-Vorgangs und nach der Anmeldung eines Benutzers die Konfigurationsdaten vom Server und legt diese in einem geschützten Bereich lokal ab. Damit sind der Device-Schutz und die Device-Freigabe auch dann gegeben, wenn sich der PC nicht im Netz befindet, da die lokale Kopie verwendet wird. Schließt ein Benutzer ein gesperrtes Gerät an, wird er ggf. über einen Hinweisdialog informiert, warum das Gerät gesperrt ist. Die Texte können dabei geräteklassen- oder gerätespezifisch sein.

Um neue Geräte frei zu schalten, sind diese an einen PC anzuschließen, wobei es sich sowohl um den lokalen PC des Administrators oder den PC eines Endanwenders handeln kann. Die Geräteinformationen können nach DX-Union importiert werden und stehen für die Freigabe zur Verfügung.

Informationen zu diesem und weiteren DX-Union Modulen finden Sie im Internet unter www.dx-union.de. ■

Kontakt

MATERNA GmbH
Information & Communications
Voßkuhle 37, 44141 Dortmund
Tel.: +49 231 5599-160, Fax -165
E-Mail: marketing@materna.de
www.materna.de

