

Intelligenter Datenschutz

Die Überwachung von Schnittstellen und Geräten, die an den Arbeitsplatz-PC angeschlossen werden, spielt eine zentrale Rolle beim Schutz der Daten vor Verlust und Diebstahl. **Jörg Lützenkirchen**

Untersuchungen zeigen, dass die meisten Datenverluste von den eigenen Mitarbeitern verursacht werden. Dabei ist weniger böse Absicht im Spiel, sondern in der Mehrzahl der Fälle Unachtsamkeit oder Fahrlässigkeit. Häufig sind mobile Datenträger involviert, Laptops, Mobiltelefone oder USB-Sticks, die verloren gehen oder gestohlen werden, wenn Mitarbeiter beispielsweise Daten zum Weiterarbeiten nach Hause mitnehmen. Bei Verlust oder Diebstahl kann nicht ausgeschlossen werden, dass die Daten in falsche Hände geraten – auf mehr als 40 Prozent der Datenträger sind die Daten nicht verschlüsselt. In den meisten Unternehmen ist jedoch ein Verschluss von Laufwerken nicht praktikabel. Dann sind als Bestandteil der Strategien im Zusammenhang mit Datenschutz und Datensicherheit Lösungen gefragt, die die Nutzung der Schnittstellen überwachen.

mensleitung, die EDV-Revision und die Mitarbeitervertretung beteiligt sein. Damit Kollisionen zwischen Konzept und Technik vermieden werden, ist in vielen Fällen die Unterstützung durch einen externen IT-Berater sinnvoll.

Lösungsbestandteile. Zu einer Lösung für die Überwachung der Gerätenutzung gehören in der Regel eine Datenbank als zentraler Speicherort für die Geräte-Listen, Berechtigungen und Logs sowie ein oder mehrere Anwendungsserver, über die die Kommunikation zwischen der Datenbank, den Clients und der Management-Konsole läuft. Dazu kommen Agenten auf den zu überwachenden Clients und Servern sowie eine Management-Konsole.

Die Standardrichtlinien für den Benutzerzugriff werden bei der Installation der Lösung in der Datenbank angelegt, ebenso werden alle Datenträger, die an den Clients angeschlossen sind und waren, nach Art, Modell und / oder ID erfasst und Richtlinien zugeordnet. Sicherheitshalber sollte der lokale Administrator keine Änderungen an den Sicherheitseinstellungen vornehmen können; auch der auf den Clients installierte Agent muss manipulationssicher sein: Ein Kernel-Mode-Treiber verhindert, dass der Client bei deaktiviertem Agent gestartet werden kann.

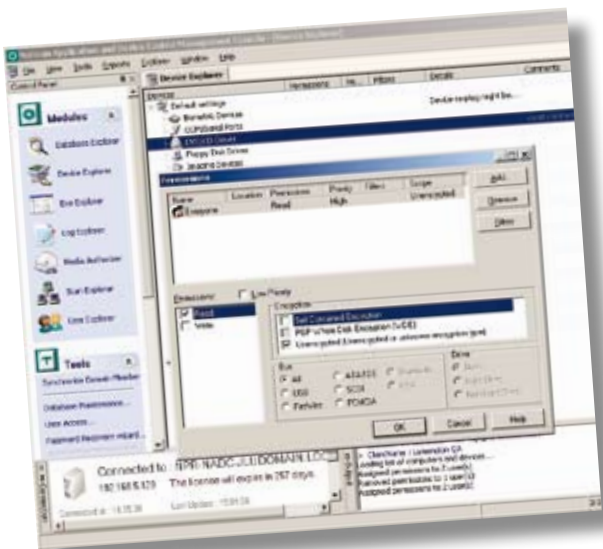
Wenn ein Nutzer also Informationen auf einen USB-Stick kopieren möchte, fragt der Agent am Anwendungsserver an, ob der Nutzer dazu berechtigt ist. Der Anwendungsserver reicht die Anfrage an die Datenbank weiter, die die Regelung an den Server übermittelt. Das Ergebnis wird dort entschlüsselt, zwischengespeichert und an den Agenten weitergereicht. Ist der Nutzer zur Datenübertragung berechtigt, werden die Daten bei der Übertragung verschlüsselt.



Der Autor
Jörg Lützenkirchen
ist Business Consultant bei
Norman Data Defense Systems

Konsolen-Funktionen. Über eine Management-Konsole sind Menüs für spezifische Administratoren-Arbeiten zugänglich. Die Gerätegruppen müssen sich verwalten lassen; Berechtigungen für Benutzer und Benutzergruppen müssen hinzugefügt und geändert werden können. Ebenso lassen sich beispielsweise die Datenmengen beschränken, die ein Nutzer täglich auf Wechseldatenträger oder Medien kopieren kann. Manche Nutzer benötigen eine zeitlich beschränkte Zugriffsmöglichkeit, auch für künftige Zugriffe zu festgelegten Zeiten. Über die Konsole werden auch die Regeln für die Erstellung von Schattenkopien erstellt und verwaltet und die Nutzungsberechtigung für verschlüsselte Datenträger erteilt.

Die Agenten auf den Clients protokollieren sämtliche anwenderseitigen Zugriffe auf Datenträger einschließlich der Zugriffsversuche nicht berechtigter Nutzer und stellen sie in der Konsole zur Auswertung bereit. Erfasst werden alle eingehenden und ausgehenden Aktivitäten mit Datenträgern sowie per Schattenkopie alle Dateien, die auf einen Datenträger kopiert wurden. Bei Verlust oder Diebstahl eines Datenträgers kann also nachvollzogen werden, welche Daten abhanden gekommen sind. Das ermöglicht eine frühzeitige und angemessene Reaktion auf den Vorfall. Die Administratoren-Aktivitäten werden ebenfalls protokolliert.



Norman Device Control: Rechte-Set für „Lesezugriff auf CD-DVD erlauben“

Zuerst das Konzept, dann die Technik. Grundlage für die Implementierung ist ein Konzept, das detailliert beschreibt, welcher Mitarbeiter welche Rechte für welche Medien benötigt. An der Konzepterstellung sollten neben den IT-Verantwortlichen auch die Unterneh-