



[case study: sanctuary device control]

Ausgangslage

Nach einem Upgrade von Windows NT4 auf Windows XP bei einem unseren grösseren Kunden bestand das Problem, dass der Zugriff auf externe Medien und Datenspeicher nicht verwaltbar war. Durch Windows XP konnten unzählige externe Medien und Datenspeicher an den Computer angeschlossen werden. Die Gefahr des Missbrauchs ist damit dramatisch angestiegen.

Dieses Problem wurde so gehandhabt, dass sämtliche Computer ohne CD-Roms ausgeliefert wurden. Der Zugriff durch USB-Geräte wurde durch Deaktivierung des USB-Treibers unterbunden. Diese Lösung war jedoch sehr starr und zeitaufwendig. Deshalb wurde nach einer flexiblen und leicht zu verwaltenden Lösung gesucht.

Lösung

Nach der Evaluation von mehreren Software-Lösungen haben wir beim Kunden „Sanctuary Device Control“ von der Firma SecureWave installiert. Diese Software erfüllt sämtliche Bedürfnisse des Kunden.

Verwalten der Gerätekategorien

- Mit der Software „Sanctuary Device Control“ ist es möglich, den Zugriff auf die verschiedenen Wechselmedien flexibel und bedarfsgerecht zu verwalten und protokollieren zu können.
- Sämtliche Schnittstellen können in verschiedene Gerätekategorien verwaltet werden.
- Entfernbare externe USB-Geräte können einzeln verwaltet werden. (z.B. USB-Sticks, Multi Card Reader oder Digitalkameras.)
- Andere Schnittstellen für externe Geräte wie z.B. die parallele oder serielle Schnittstelle können als einzelne Anschlüsse freigegeben oder gesperrt werden.
- Der Zugriff auf die Medien kann einzeln verwaltet werden. Jede spezifische CD oder DVD kann für jeden einzelnen Benutzer individuell freigegeben werden.
- Der Zugriff kann entweder geräte- oder benutzerspezifisch geregelt werden. Wird benutzerspezifisch verwaltet, können die Gruppen und Benutzer des Active Directory verwendet werden.
- Bei Schnittstellen mit der Möglichkeit Daten zu speichern wird zwischen Lese- und Schreibzugriff unterschieden.



Verschlüsselung

USB Wechselmedien wie USB-Sticks können durch "Sanctuary Device Control" verschlüsselt und mit einem Passwort geschützt werden. Auf das Medium kann anschliessend nur noch zugegriffen werden, wenn man im Besitz des Schlüssels und des Passwortes ist. Es ist somit gewährleistet, dass verloren gegangene oder gestohlene Medien nicht missbraucht werden können.

Shadowing

Es kann überwacht und protokolliert werden, welche Dateien wann, wo und von wem auf externe Medien kopiert oder verschoben wurden. Diese Angaben werden in einer Datenbank gespeichert. Man hat die Möglichkeit nur die Aktion zu protokollieren oder gleich ein Duplikat von den betroffenen Daten in der Datenbank abzulegen.

Vorgänge über die parallele und serielle Schnittstelle wie Drucken oder Modemzugriff werden ebenfalls protokolliert.

Momentan können mit "Sanctuary Device Control" nur ausgehende Daten überprüft und protokolliert werden.

Der Hersteller begründet dies damit, dass die Gefahr durch eingehende Daten weniger in deren Inhalt als mehr durch den Befall mit Viren besteht. Diese Problematik wird meist bereits durch einen vorhandenen Virenschutz gelöst.

Verwaltung

Die Verwaltung und die Datenbank des Programms befinden sich auf einen Server in der überwachten Umgebung. Der Endbenutzer hat selber keine Möglichkeit das Programm anzupassen oder sogar auszuschalten. Ebenso kann er die protokollierten Vorgänge weder anschauen noch verändern.

Offline Funktionalität

Ist der Computer oder Laptop des Benutzers nicht mit der verwalteten Domäne verbunden, gelten die konfigurierten Zugriffsrechte weiterhin. Wurden dem Gerät noch keine Zugriffsrechte zugewiesen, gelten die Standardzugriffsrechte von „Sanctuary Device Control“. Das heisst, sämtliche konfigurierbaren Zugriffe sind gesperrt. Werden während dieser Zeit auf dem Server neue Einstellungen konfiguriert, so werden diese beim nächsten Anmeldevorgang synchronisiert. Dasselbe gilt auch für die Shadowing Funktion.

Die Überwachung ist weiterhin aktiv und wird zuerst lokal und verschlüsselt abgespeichert. Der Benutzer hat keinerlei Möglichkeiten die Daten zu löschen oder zu verändern.



Resultat

Durch den Einsatz von "Sanctuary Device Control" konnten die Bedürfnisse und Sicherheitsanforderungen des Kunden erfüllt werden. Er kann nun den Gebrauch der externen Schnittstellen durch den Endanwender von einer zentralen Stelle einfach und effizient konfigurieren und verwalten. Durch Shadowing hat er ausserdem die Möglichkeit den Datentransfer über die verschiedenen Schnittstellen nachzuvollziehen.

FITIT Informatik GmbH

Bernstrasse 67, Postfach
3122 Kehrsatz
Telefon:+41 (0)31 961 61 61
Telefax:+41 (0)31 961 34 45

www.fitit.ch
info@fitit.ch