

Device Control ist mehr als USB-Sperre

Der Betrieb externer Geräte an Unternehmens-Clients ist gefährlich. Einfach die Schnittstellen abzudrehen ist aber auch keine Antwort. Erst mit dem Einsatz von ausgereiften Device Control Lösungen wird es möglich, sich gegen die Gefahren abzusichern und gleichzeitig die Leistungsfähigkeit der Clients für die betriebliche Nutzung zu erhalten.



Fixe Arbeitsplatzrechner und mobile Clients haben eines gemeinsam – sie verfügen über eine Vielzahl von Schnittstellen, die den Anschluss externer Geräte ermöglichen. USB, Firewire, WLAN, Bluetooth, Infrarot sowie serielle und parallele Schnittstellen verbinden Computer mit

Externe Geräte sind sogar dann gefährlich, wenn sie von Marken Anbietern stammen. Wird ein infiziertes Gerät an einen Client angeschlossen, ist der Computer praktisch sofort befallen. Die physischen Schnittstellen jedes Clients sind also ein erhebliches Sicherheitsrisiko.

Memory-Sticks, Mobiltelefonen, Festplatten, MP3-Playern, Kameras und jeder anderen nur erdenklichen Peripherie. Diese grenzenlosen Möglichkeiten bringen aber ebenso grenzenlose Gefahren mit sich. Mit extern anschließbaren Speichermedien ist es sehr leicht, Daten aus dem Unternehmen zu bringen – eine Kundendatei oder andere sensible Informationen sind schnell auf einen USB-Stick kopiert. Darüber hinaus wird mit den Schnittstellen unerwünschter Schadsoftware Tür und Tor geöffnet. Wie die Beispiele im Bild zeigen, werden selbst mit Geräten von Markenherstellern immer wieder Trojaner oder Würmer eingeschleppt. Wenn der betroffene Client ins Unternehmens-

netzwerk eingebunden ist, muss in weiterer Folge sogar eine Verbreitung der Malware im ganzen Haus befürchtet werden.

Einladung zum Bacher Systems Breakfast 08. März 2007

Mehr über **Lösungen für echte Device Control** erfahren Sie auf dem nächsten Bacher Systems Breakfast am 8. März 2007 (9:30 bis 12:00) im Atelier Augarten. Die Teilnahme ist kostenlos, um rechtzeitige Anmeldung unter www.bacher.at/breakfast wird gebeten.

Echte Kontrolle ist möglich

Die logische Konsequenz aus diesen Umständen ist, dass eine einfache USB-Sperre so gut wie gar nichts nützt. Sie kann viel zu leicht umgangen werden und ist in ihrer Definition zu grob – denn manche externe Geräte müssen einfach betrieben werden können. Auch die mit Windows Vista neu gebotenen Funktionalitäten zur Gerätekontrolle sind für Unternehmensmaßstäbe nicht ausreichend. Das bedeutet, dass die Problematik



Newsletter 1/2007

Informationen für IT-Sicherheit und IT-Infrastruktur

nur mit ausgereiften Lösungen für Device Control in den Griff zu bekommen ist. Sie bieten eine umfassende Kontrolle aller Geräte nach dem White-List Prinzip und halten dabei gleichzeitig die volle Funktionalität der Clients aufrecht. Die Nutzung von externen Geräten wird damit gezielt steuer- und nachvollziehbar. Das Netzwerk wird vor dem Einschleusen von Schadsoftware geschützt und es wird verhindert, dass Daten unbemerkt auf externe Speichermedien kopiert werden können. Werden externe Datenträger eingesetzt, die von der Device Control explizit erlaubt sind, so werden die Daten einer Verschlüsselung unterzogen. Neben dem Nutzen, dass die Unternehmensdaten auf diese Weise wirkungsvoll abgesichert werden, haben echte Device Control Lösungen auch noch einen wichtigen Nebennutzen: Sie liefern einen Nachweis über die Datensicherheit, die mit den zunehmenden Compliance-Anforderungen verlangt wird.

Anforderungen an Device Control

Der Nutzen von Device Control entfaltet sich aber nur dann, wenn die eingesetzten Produkte ganz bestimmte technische Anforderungen erfüllen. Viele halbherzige Lösungen machen es allzu leicht möglich, den gebotenen Schutz zu unterwandern und die Device Control zu umgehen. Hier exemplarisch drei der wichtigsten Anforderungen:

- **Verschlüsselte Client/Server-Kommunikation:** Die Kommunikation zwischen dem Administrations-Server der Lösung und den Clients muss unbedingt verschlüsselt und unabhängig von leicht angreifbaren Kommunikationskanälen (wie z.B. RPC) erfolgen. Damit wird sichergestellt, dass die Übertragungen gegen Veränderungen geschützt sind. Andernfalls könnte der Verkehr abgehört und verändert oder gefälscht werden. Auf diese Weise wäre es möglich, die Geräte-Anschlussrechte des Clients zu manipulieren und die Device Control zu umgehen.
- **Geschützte Software-Komponenten:** Nicht nur auf Grund der Geschwindigkeit sondern auch aus Sicherheitsgründen muss die Device Control Funktionalität auf dem Client im Kernel angesiedelt sein. Dem Benutzer wird es damit selbst mit Administrator-Rechten praktisch unmöglich gemacht, die Sicherheitssoftware zu umgehen. Auch im abgesicherten Modus ist so der volle Schutz gegeben.
- **On/Offline-spezifische Regeln:** Die vergebenen Geräterechte müssen nach On- und Offline-Betrieb unterschieden werden. So ist es beispielsweise für ein Notebook sinnvoll, außer Haus für den Internetzugang eine PCMCIA-Modemkarte einzusetzen. Wird das Notebook aber im Firmennetzwerk verwendet, darf der Aufbau einer solchen Verbindung nicht möglich sein – die Security-Policy des Unternehmens würde unterlaufen werden.

Diese und weitere zentrale Anforderungen an Device Control Lösungen werden nur von ganz wenigen Herstellern erfüllt. Die Bacher Systems Experten empfehlen nach eingehenden Evaluierungen das Sanctuary Device Control Produkt von SecureWave. Mehr über die Realisierung echter Device Control Lösungen erfahren Sie auf dem nächsten Bacher Systems Breakfast.

Trainings bei Bacher Systems

IT-Infrastruktur

Symantec Backup Exec 10d for Windows Server: Administration I
5.03. - 7.3.2007 / € 1.530,-

Symantec Backup Exec 10d for Windows Server: Administration II
8.3. - 9.3.2007 / € 1.020,-

Unix Grundlagen der Solaris 10 Betriebssystemumgebung
12.3. - 15.3.2007 / € 1.990,-

Sun Cluster 3.1 Verwaltung
12.3. - 16.3.2007 / € 3.890,-

Solaris 10 OE Systemadministration I
19.3. - 23.3.2007 / € 2.790,-
23.4. - 27.4.2007 / € 2.790,-

Solaris 10 OE Systemadministration II
26.3. - 30.3.2007 / € 2.790,-

Netzwerkadministration für Solaris 10 OE
16.4. - 20.4.2007 / € 2.790,-

IT-Sicherheit

Check Point Security Administration NGX I 1.1
19.3. - 20.3.2007 / € 1.350,-

Check Point Security Administration NGX II 1.1
21.3. - 23.3.2007 / € 1.990,-

**Package
NGX I+II
€ 2.900,-
statt € 3.340,-**

Alle Preise pro Person exkl. MwSt.
Firmenspezifische Kurse auf Anfrage.
Anmeldungen: training@bacher.at

Kursinfos: www.bacher.at/training

Änderungen vorbehalten

Bacher Systems EDV GmbH, 1100 Wien, Clemens-Holzmeister-Straße 4, Tel.: +43.1/60 126-0, Fax: +43.1/60 126-4, E-Mail: info@bacher.at

