Schutz der Schnittstellen

# Keine Überraschungen durch den USB-Anschluss!

**Wie der neueste Bericht der Melde- und Analysestelle Informationssicherheit MELANI des Bundes zeigt (http://www.melani.admin.ch), bleibt Industriespionage ein aktuelles Thema. Die Schweiz gilt immer noch als sehr innovatives Land mit vielen technologisch hochstehenden Entwicklungen. Diese Informationen sind auch für ausländische Firmen von grossem Interesse. Die vergangenen beiden Artikel haben gezeigt, wie Hacker vorgehen, um in ein Netzwerk einzudringen. Diese Ausgabe beleuchtet, wie die Schnittstellen eines Computers geschützt werden können, damit nicht via CD/DVD-Brenner oder den allgegenwärtigen USB-Ports Daten das eigene Unternehmen verlassen.**

Autor: Andreas Wisler

**Jeder moderne PC verfügt über verschiedenste Schnittstellen:** CD/DVD ROM, oft gar ein entsprechender Brenner, Firewire und mehrere USB-Anschlüsse. Via diese Wege kann (schädliche) Software installiert werden, aber auch Daten können, oft unbemerkt, das eigene Unternehmen verlassen. Diesen Gefahren muss durch geeignete organisatorische oder technische Sicherheitsmassnahmen entgegengewirkt werden. Nachfolgend sind einige technische Möglichkeiten aufgeführt.

### Ausbau von Laufwerken

Der Ausbau von Laufwerken bietet zwar den sichersten Schutz, ist aber meist mit erheblichem Aufwand verbunden. Weiterhin ist zu berücksichtigen, dass der Ausbau unter Umständen die Administration und Wartung des IT-Systems behindert. Diese Lösung sollte in Betracht gezogen werden, wenn besondere Sicherheitsanforderungen bestehen.

### Verschluss von Laufwerken

Für einige Laufwerksarten und Schnittstellen gibt es abschliessbare Vorrichtungen, mit denen die unkontrollierte Nutzung verhindert werden kann. Bei der Beschaffung sollte sichergestellt werden, dass die Laufwerksschlösser für die vorhandenen Laufwerke geeignet sind und diese nicht beschädigen können. Ausserdem sollte darauf geachtet werden, dass die Schlösser herstellerseitig mit hinreichend vielen unterschiedlichen Schlüsseln angeboten werden.

Im BIOS (Basic Input Output System, "Grundsoftware", die das Betriebssystem mit der Hardware verbindet) können viele Schnittstellen deaktiviert werden. Somit ist kein Zugriff auf die angeschlossenen Geräte mehr möglich. Dies bedeutet aber auch, dass allenfalls Personen mit speziellen Erlaubnissen ebenfalls nicht mehr zugreifen können. Zudem muss sichergestellt sein, dass der Zugriff auf das BIOS mit einem sicheren Passwort geschützt wird.

Kontrolle der Schnittstellennutzung
Der Betrieb von externen Speichermedien wie USB-Memory-Sticks lässt sich nur sehr schwer verhindern, wenn die verwendete Schnittstelle auch für andere (erlaubte) Zugriffe genutzt wird. So werden beispielsweise Notebooks ausgeliefert, die zum Anschluss einer Maus nur die USB-Schnittstelle zur Verfügung stellen. Dadurch ist es in der Regel nicht sinnvoll, ein "USB-Schloss" zu verwenden oder die Schnittstelle durch andere mechanische Massnahmen zu deaktivieren.

Aus diesem Grund bieten verschiedene Software-Hersteller Produkte an, mit

## Zum Autor

**Andreas Wisler**
(Tel.: 052 320 91 20)
Dipl. Ing. FH, CISSP, ISO 27001 Lead Auditor, ist Geschäftsführer der GO OUT Production GmbH, welche sich mit ganzheitlichen und produktneutralen IT-Sicherheitsüberprüfungen und -beratungen auseinandersetzt. System Hardening rundet das Profil ab. Regelmässig veröffentlicht er einen informativen Newsletter zu aktuellen Sicherheitsthemen, der kostenlos und unverbindlich auf www.gosecurity.ch (INFONEWS) heruntergeladen werden kann. Für Blickpunkt:KMU beleuchtet er in jeder Ausgabe einen neuen Aspekt der IT-Sicherheit.


welchen sich diese Schnittstellen zentral steuern lassen. Mittels Regeln wird definiert, wer welche Berechtigungen hat. So kann beispielsweise einem Benutzer der DVD-Brenner zur Verfügung stehen, ein anderer Mitarbeiter darf nur DVDs lesen, aber nicht brennen, ein weiterer wiederum darf seinen Fotoapparat an dieser Schnittstelle verwenden. Den Ideen und Wünschen sind in der Regel keine Hindernisse gesetzt.

Auch Microsoft hat sich (endlich) dieses Problems angenommen. Mit dem DMI (Device Management and Installation) können Sie die Geräteinstallation auf den von Ihnen verwalteten Computern steuern. Sie können unter anderem festlegen, welche Geräte vom Benutzer installiert werden können und welche nicht. DMI ist Teil von Microsoft Windows Server 2008 und Windows Vista. Da Windows nur über eine bestimmte Software mit der Hardware kommunizieren kann, dem Gerätetreiber, können an einer zentralen Stelle Regeln definiert werden, was erlaubt und damit möglich ist. Zur Konfiguration stehen drei Möglichkeiten zur Verfügung:

- Verhindern der Installation aller Geräte
- Zulassen der Installation autorisierter Geräte
- Verhindern der Installation von verbotenen Geräten

Somit kann im Vorfeld eine Liste mit erlaubten Geräten erstellt werden und diese via Active Directory, der zentralen Schnittstelle von Microsoft, an Clients verteilt werden.

### Fazit

Dass die Steuerung und Vergabe von Zugriffsrechten auf die verschiedenen Schnittstellen ein brennendes Thema ist, zeigen die vielen Programme, die auf dem Markt verfügbar sind. Eine Suche im Internet bringt eine Vielzahl von Lösungen zutage. Bevor Sie sich jedoch für eine Lösung für Ihr Unternehmen entscheiden, sollten Sie sich überlegen, was es zu schützen gilt, wer Zugriff auf diese Daten haben darf und wer nicht sowie wie diese Daten transportiert werden dürfen. Erst danach können technische Massnahmen umgesetzt werden, um damit die Sicherheit in Ihrem Netzwerk zu erhöhen und unerlaubten Datendiebstahl zu verhindern. ◆