Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten des Bundes und der Länder

Orientierungshilfe

Datensicherheit bei USB-Geräten

Stand: 27. November 2003

1 Problem

Öffentliche Stellen können ihre Datenverarbeitung nicht nach Belieben organisieren, sondern müssen die Verwaltungs-(Verfahrens-)Vorschriften einhalten. Um dies sicherstellen zu können, dürfen ohne Wissen der Behördenleitung keine Daten verarbeitet werden. Dies gilt insbesondere für personenbezogene Daten, da deren Missbrauch zu Schäden für die Betroffenen führen kann. Deshalb schreiben einige Datenschutzgesetze explizit vor, dass Datenverarbeitungsverfahren einer Freigabe durch die Behördenleitung bedürfen (z. B. § 19 Landesdatenschutzgesetz Mecklenburg-Vorpommern).

Neben der verwendeten Software ist auch die Hardware förmlich freizugeben. Zu Recht wird häufig der Zugriff auf Laufwerke aller Art (CD-ROM, Disketten, Zip-Laufwerke etc.) unterbunden, da sie es ermöglichen, unkontrollierbare Datensammlungen anzulegen und nicht zugelassene und unerwünschte Software auszuführen. Schnittstellen für Modems und andere Datenübertragungsgeräte werden abgeschaltet, damit keine unerlaubten und unkontrollierbaren Seiteneingänge in das lokale Netz geschaffen werden können.

Seit einiger Zeit werden praktisch alle Personal Computer mit Buchsen für den Universal Serial Bus (USB) ausgestattet. Diese Schnittstellen dienen dem einfachen Anschluss verschiedener Hardwarekomponenten wie Disketten-, DVD oder CD-Rom-Laufwerken, Festspeicher-Medien oder Netzwerkhardware. Aufwändige Installationsprozeduren für Hard- und Software entfallen, da moderne Betriebssysteme die neu angeschlossenen Geräte sofort erkennen und einbinden. Dadurch sinkt die Hemmschwelle, nicht freigegebene oder auch private Technik zu nutzen. Die bisher eingerichteten Nutzungsbeschränkungen für CD- und Floppy-Laufwerke sind dann nicht mehr ausreichend wirksam. Es müssen folglich Mechanismen gefunden werden, mit denen der Zugriff auf den USB auf genau die zugelassenen Geräte beschränkt werden kann.

2 Einsatzszenarien und Bedrohungen

Die technische Entwicklung zeigt, dass der Trend zum sogenannten „legacy-free PC“ ohne die klassischen seriellen, parallelen und PS/2-Anschlüsse geht. Zumindest für Tastatur und Maus, aber auch für Arbeitsplatzdrucker wäre dann USB zwingend notwendig. Darüber hinaus sind zunehmend dienstliche PDAs in Gebrauch, deren Synchronisation mit stationären Geräten häufig über die USB-Schnittstelle stattfindet. Damit stehen ein Anschluss und ein Protokollstack zur Verfügung, die jedoch auch zum Anschluss nicht freigegebener Hardwarekomponenten genutzt werden können. Die Betriebssystemunterstützung ist in der Regel so ausgelegt, dass USB-Geräte nach dem Einstecken sofort betriebsbereit sind.

Sicherheitsrelevant ist insbesondere der Einsatz nicht zugelassener Netzwerkadapter, Modems oder ISDN-Adapter, da mit ihnen unerlaubte „Seiteneingänge“ in Netzen geschaffen werden, die die zentralen Sicherheitseinrichtungen unterlaufen. Auch über USB anschließbare Speichermedien bergen ein erhebliches Sicherheitsrisiko in sich. Das betrifft insbesondere so genannte memory sticks. Das sind handliche Geräte in der Größe eines Schlüsselanhängers mit einem nicht flüchtigem Speicher, dessen Größe ein Gigabyte übersteigen kann. Sie werden wie wechselbare Festplatten angesprochen und gestatten das Speichern von schutzwürdigen Daten, den Zugriff auf mitgebrachte private Daten sowie das Ausführen von unerlaubten und nicht freigegebenen Betriebssysteme und Programmen, mit denen auch Sicherheitsmechanismen unterlaufen werden können.

Allerdings stehen den oben genannten Risiken bei der Nutzung von USB-Peripherie auch Vorteile für die Datensicherheit gegenüber. So erscheint es durchaus sinnvoll, besonders vertrauliche Datenbestände auf memory sticks oder USB-Festplatten zu speichern. Den physischen Zugriff zu diesem Medium kann man auf einfache Weise einschränken, und so die Chancen eines potenziellen Angreifers vermindern. Dies wäre mit der Speicherung auf (größeren) Wechselmedien vergleichbar. Gegen unbefugte Zugriffe bei Verlust des Mediums bzw. des USB-Gerätes hilft die verschlüsselte Speicherung der Daten mit Produkten wie PGP-Disk oder Steganos unter Windows oder PPDD (Practical Privacy Device Driver) unter Linux.

Die genannten Aspekte verdeutlichen, dass USB-Controller in den PCs in naher Zukunft kaum noch abgeschaltet werden können. Somit kann der Zugriffsschutz folglich nur über die Konfiguration des USB-Protokollstacks oder über allgemeine Zugriffsschutzmechanismen des Betriebssystems realisiert werden.

3 Lösungsansätze

3.1 Windows

3.1.1 Setzen von ACLs; kommerzielle Produkte

Der eleganteste Weg, Geräte aller Art unter Windows 2000/XP zu kontrollieren, ist das Setzen von ACLs auf diese Geräte. (ACLs, access control lists, sind spezielle Zugriffsschutzdaten; sie werden beispielsweise Geräten und Dateien zugeordnet und vom Betriebssystem verwaltet.) Das ist auch die einzige Möglichkeit, um Schwierigkeiten im Multiuserbetrieb (z.B. auf einem Terminalserver) zu umgehen. ACLs sind bereits unter Windows NT sehr mächtig. Allerdings bietet Microsoft den vollständigen Zugriff auf ACL-Objekte nur Programmierern an (über Programmierschnittstellen, die *APIs*). Geeignete Konsolenprogramme oder Editoren stehen bislang nicht zur Verfügung. Leider sind sicherheitsrelevante API-Funktionen für Geräte im DDK (*Device Driver Kit*, Entwicklungssoftware für Gerätetreiber) nur spärlich dokumentiert. Dieser Weg scheidet für die meisten Anwender deshalb aus, weil sie nicht über die erforderlichen Kenntnisse in der Systemprogrammierung von Windows verfügen.

Zur Zugriffssteuerung für das USB-Subsystem bringt Windows ebenfalls standardmäßig keine Werkzeuge mit. Nach [1] ist eine entsprechende Lösung zwar geplant, jedoch bislang nicht realisiert.

SecureNT ist ein kommerzielles Tool, welches auf ACL-Basis den Zugriff auf USB-Geräte steuert (http://securewave.com/products/securent). SecureNT kann darüber hinaus auch den Zugriff auf weitere Geräte steuern, also auch auf PCMCIA-Geräte, Floppy, CD-ROMs, ZIP-Drives, memory cards usw. Mit dem Produkt Device-Lock kann der Zugriff auf USB-Geräte ebenfalls wirksam beschränkt werden.

3.1.2 Überwachen der Registry

Darüber hinaus kann nach [1] der Registrierungsschlüssel

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB

überwacht werden. Neu eingebundene USB-Geräte werden hier eingetragen. In [1] ist hierzu ein VBScript-Programm beschrieben, welches auch als Dienst eingerichtet werden kann. Es antwortet bei Erscheinen unzulässiger Gerätetypen mit einer konfigurierbaren Aktion. So kann es den Rechner herunterfahren oder den Systemadministrator informieren. Es scheint nämlich zumindest unter Windows 2000 und XP nicht möglich zu sein, die Schlüssel einfach automatisch zu löschen.

3.1.3 Überwachen der USB-Geräte mittels WBEM

Man kann den USB-Controller auch mittels eines Dienstes über die WBEM-Instanz *Win32_USBController* überwachen. (WBEM ist das Web Based Enterprise Management; die Implementation von Microsoft heißt Windows Management Instrumentation WMI) Taucht ein neues Gerät auf, überprüft der Dienst, ob der angemeldete Nutzer das Gerät nutzen darf. Dazu ist jeder bekannten USB-Device-ID eine Gruppe zugeordnet. Ist das USB-Gerät unbekannt oder ist der angemeldete Nutzer nicht Mitglied der jeweiligen USB-Zugriffsgruppe, wird das USB-Gerät gesperrt (via *SetupDiCallClassInstaller*-API). Meldet sich ein neuer Nutzer an, der seinerseits Mitglied der jeweiligen USB-Zugriffsgruppe ist, wird das USB-Gerät wieder freigegeben. Unter Umständen ist noch ein Reboot nötig. Das Verfahren funktioniert leider nicht auf Terminalservern, da es nicht multi-user-fähig ist. Diesen Dienst zu schreiben erfordert jedoch Kenntnisse in der Windows-Systemprogrammierung, in der Sprache C, eine entsprechende Entwicklungsumgebung und die Zeit, ein Programm von etwa 600 Zeilen C-Code zu erstellen und zu testen.

3.1.4 Löschen der USB-Treiber; USB-Netzwerkgeräte

Zu guter Letzt kann man auch die Treiber aus dem System entfernen, die zur Verwaltung bestimmter USB-Geräte erforderlich sind. Windows kommuniziert beispielsweise über den Treiber *usbstor.sys* mit USB-Massenspeichern. Administratoren können diesen Treiber aus dem Windows-System-Verzeichnis und aus dem Driver Cache löschen, um den Zugriff auf USB-Sticks zu unterbinden.

Das Einbinden von USB-Netzwerkadaptern sowie USB-Modems erfordert unter Windows 2000/XP Administrationsrechte. Es genügt daher, darauf zu achten, dass diese Rechte gewöhnlichen Benutzern nicht zugeteilt werden.

3.2 Linux

Um unter Linux den unbefugten Gebrauch von USB-Speichergeräten einzuschränken, sollte explizit festgelegt werden, wer überhaupt bestimmte Geräte montieren darf. Dazu müssen die Zugriffsrechte auf die entsprechenden Gerätedateien gesetzt werden. In der Regel werden USB-Geräte wie SCSI-Geräte behandelt; memory sticks und USB-Festplatten werden also mit Namen wie */dev/sda*, */dev/sda1* etc. angesprochen. Es ist empfehlenswert, alle zugelassenen Benutzer in einer Gruppe zusammenzufassen und die entsprechende Gerätedatei dem Eigentümer *root* und dieser Gruppe zu übergeben (mittels *chown*, *chgrp*).

Das unbefugte Montieren von Datenträgern kann ferner dadurch verhindert werden, dass die dazu notwendigen Einträge in der */etc/fstab* gelöscht oder in einen Kommentar umgewandelt werden. Dann bleibt diese Aktion in jedem Falle dem Systemverwalter *root* vorbehalten.

Darüber hinaus besteht die Möglichkeit, die nicht benötigten Treiber im Verzeichnisbaum unter */lib/modules* zu löschen, darunter *usb-storage.o* . Ferner kann auch die Konfiguration des für die USB-Geräte-Verwaltung zuständigen Daemons hotplug so angepasst werden, dass bestimmte Treiber nicht geladen werden (in */etc/hotplug/blacklist* aufnehmen) oder dass genau die zulässigen Treiber geladen werden (in */etc/hotplug/usb.*map*).

USB-Netzwerkadapter und USB-Modems sind Benutzern unter Linux nicht zugänglich, wenn dies nicht ausdrücklich eingerichtet ist, da die Konfigurationstools wie *ifconfig* nur dem Systemverwalter Änderungen gestatten. Die Rechte an entsprechenden Geräte-Dateien verbieten gewöhnlichen Benutzern standardmäßig den Zugriff. Auch die Konfigurationsdateien, die die Netzwerkkonfiguration beim Booten des Systems steuern, können von normalen Benutzern üblicherweise nicht verändert werden, weil ihnen die Rechte dafür fehlen.

3.3 Booten von USB-Geräten

Damit die oben erwähnten Zugriffsschutzmechanismen der Betriebssysteme wirksam werden können, dürfen nur die freigegebenen Betriebssysteme oder System-Konfigurationen gestartet werden können. Es sollte daher sichergestellt sein, dass das Booten von herkömmlichen CDROM-/DVD-Laufwerken, Disketten-Laufwerken und vom Netzwerk (falls zutreffend) unterbunden wird. Dies ist bereits jetzt Stand der Technik (siehe [4]).

Es ist jedoch auch möglich, von USB-Geräten zu booten, wenn sowohl das PC-BIOS als auch das USB-Gerät dazu in der Lage sind. Einige aktuelle BIOS-Versionen gestatten das Booten von memory sticks, mitunter auch von USB-Disketten- und -CDROM-Laufwerken ([2], [3]).

Um das Starten von Betriebssystemen von USB-Geräten und anderen wechselbaren Medien zu verhindern, sollte im BIOS die Boot-Optionen angepasst werden. Das Booten von USB-Geräten und anderen wechselbaren Laufwerken sollte in dem entsprechenden BIOS-Menü abgeschaltet werden. Falls dies nicht möglich ist, sollten die Boot-Optionen so konfiguriert werden, dass USB-Geräte erst nach der System-Festplatte (oder nach dem Netzwerk, falls zutreffend) angesprochen werden.

BIOS-Einstellungen sind in jedem Fall gegen Änderungen durch Unbefugte zu sichern. Dazu muss der Passwortschutz für das BIOS-Setup aktiviert werden.

Bootfähige USB-Netzwerk-Adapter sind bislang nicht bekannt.

3.4 Grenzen beim Zugriffsschutz

Das USB-Subsystem arbeitet - ähnlich wie die PCMCIA-Karten - mit zwei Kennzeichen, die den Typ eines Gerätes eindeutig beschreiben, der Vendor ID und der Product ID. Damit ist aber keine Identifikation des einzelnen Exemplars möglich. Das Script aus [1] sowie der Linux-USB-Manager werten im Wesentlichen die genannten Kennungen aus. Der US-Standard gestattet zwar die Implementation von Seriennummern, jedoch wird diese Möglichkeit nicht von allen Herstellern genutzt. Die Seriennummern von Datenträgern, die in verschiedenen Dateisystemen vorgesehen sind, sind demgegenüber leicht fälschbar. Man braucht lediglich bestimmte Bytes im Dateisystem zu verändern.

Eine Einschränkung auf explizit zugelassene Geräte ist somit – ähnlich wie bei anderen Datenträgern – nicht möglich. Dies gilt für alle Betriebssysteme.

4 Ergebnis

Nach derzeitigem Kenntnisstand bedroht der unkontrollierte Einsatz von USB-Massenspeichern Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten. Neben den

kleinen und leichten memory sticks betrifft dies auch transportable Festplatten, MP3-Player, Digital-Kameras, CD-, Floppy- oder Karten-Laufwerke. Neben CD-[R|RW|ROM]s oder Floppies mit fest eingebauten Laufwerken stehen somit mobile Laufwerke zur Verfügung, mit denen Sicherheitsbestimmungen unterlaufen werden können.

Mit den Bordwerkzeugen von Windows kann der Zugriff auf USB-Geräte nicht auf einfache Weise verhindert werden. Mit moderatem zusätzlichem Aufwand kann die Installation nicht zugelassener Gerätetypen jedoch erkannt und blockiert werden. Dazu ist der Einsatz entsprechender Skripte oder kommerzieller Produkte erforderlich. Microsoft arbeitet an einer einfacheren Lösung.

Unter Linux ist es ebenfalls mit geringem bis moderatem Aufwand möglich, den Zugriff auf ausdrücklich benannte Geräteklassen oder -typen zu beschränken. Die dazu nötigen Schritte lassen sich aus der Dokumentation zum USB-Subsystem ableiten. Wer auf welche Geräte zugreifen darf, wird über die Zugriffsrechte auf die entsprechenden Gerätedateien festgelegt.

Um die Zugriffsschutzmechanismen der Betriebssysteme ausnutzen zu können, muss darüber hinaus das Booten von USB-Geräten im BIOS abgeschaltet werden, wie dies schon von CDROM-, DVD- und Diskettenlaufwerken her bekannt ist. Damit diese Einstellungen wirksam bleiben, muss auch der BIOS-Passwortschutz aktiviert werden.

Prinzipbedingt können USB-Geräte nur anhand ihrer Vendor-ID und Product-ID identifiziert werden. Eine feinere Granularität ist nicht erreichbar, da Geräte-Seriennummern oft nicht implementiert sind und da sich Datenträger-Kennzeichen auf dem Speichermedium selbst leicht fälschen lassen.

5 Literatur

[1] Hohmann, R.: USB-Wächter – Digitaler Keuschheitsgürtel aus VBScript für die USB-Schnittstelle. In: c't Magazin für Computertechnik 08/2003, S. 190ff., Heinz Heise Verlag, Hannover

[2] Ilmberger, A., Baasch, K.: Daten aus der Hosentasche. In: Chip 10/2003, S. 77ff., Vogel Burda Communications, München

[3] Schmidt, J., Vahldiek, A.: Hols vom Stöckchen – Notfallsystem vom USB-Stick booten. In c't Magazin für Computertechnik 13/2003, S. 208ff., Heinz Heise Verlag, Hannover

[4] Bundesamt für Sicherheit in der Informationstechnik (Hg.): IT-Grundschutzhandbuch – Abschnitt M 4.84 Nutzung der BIOS-Sicherheitsmechanismen. Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2002.