Speichermedien

Sticks des Grauens

Während vor ein paar Jahren noch Disketten das vorherrschende Datenaustauschmedium waren, haben sie heute fast vollständig an Bedeutung verloren. Denn so genannte USB-Sticks haben ihre Aufgabe komplett übernommen. Sie sind kleiner, robuster und haben bis zum Tausendfachen an Speicherkapazität. Doch gerade diese Vorteile machen sie zum Schrecken jedes DSB , da sie den heimlichen Transport großer Datenmengen erleichtern.

Nach Anlaufschwierigkeiten hat sich die USB-Schnittstelle auf breiter Front durchgesetzt. Hierzu haben auch ganz wesentlich die praktischen USB-Sticks beigetragen. Dabei handelt es sich um elektronische Speicherbausteine, die mittels eines USB-Steckers direkt an den USB-Port eines Computers angeschlossen werden können.

Datenübertragung und Speicher

Die Datenübertragung zwischen dem Rechner und einem USB-Gerät erfolgt mit 1,5 MBit/s (Low Speed), 12 MBit/s (Full Speed) oder 480 MBit/s (High Speed, ab USB Version 2.0). Die Speichergröße der USB-Sticks geht von 16 MB – schon im Kostenbereich von Werbegeschenken – bis zu 2 GB. Da unter anderem Lebensmitteldiscounter USB-Sticks vertreiben, sind sie auch im Privatbereich weit verbreitet.

Beliebt sind auch die Geräte zum Lesen von Speicherkarten (Compact Flash, SD-Karte, Memory-Stick usw.), wie sie z.B. in Digitalkameras verwendet werden. Viele aktuelle MP3-Player können wie USB-Sticks direkt in den Rechner gesteckt werden. Auf ihnen können nicht nur Musikstücke, sondern auch beliebige andere Dateien gespeichert werden.

Regeln Sie die Nutzung von USB-Sticks schriftlich!

Eine recht einfache Methode ist die organisatorische Regelung des Umgangs mit USB-Sticks. Regeln Sie die folgenden Punkte in einer Nutzerordnung bzw. Betriebsvereinbarung:

- Die Nutzung privater USB-Sticks ist verboten.
- Werden auf dienstlichen USB-Sticks personenbezogene oder andere vertrauliche Daten gespeichert, so muss der USB-Stick am Arbeitsplatz verbleiben und weggeschlossen werden, wenn er nicht in Gebrauch ist.
- Werden auf dienstlichen USB-Stick personenbezogene oder andere vertrauliche Daten transportiert, so sind die gespeicherten Daten zu verschlüsseln.
- Für die Einhaltung der Regeln ist der Mitarbeiter verantwortlich, dem der Stick zur dienstlichen Nutzung überlassen wurde.

Diese Regeln werden dem Mitarbeiter mit Übergabe des USB-Sticks schriftlich ausgehändigt.

„Getarnte“ USB-Sticks erschweren die Kontrolle erheblich

Die Industrie baut mittlerweile USB-Sticks mehr oder weniger gut getarnt in Gebrauchsgegenstände wie Armbanduhren, Stifte und sogar Taschenmesser ein. Diese „getarnten“ USB-Sticks machen es dem Werkschutz selbst bei Taschenkontrollen nicht leicht, sie als Speichermedium zu erkennen.

Setzen Sie spezielle Software-Tools ein, die den Zugriff kontrollieren

Nachdem Microsoft keine offizielle Möglichkeit zum Deaktivieren von USB-Speichermedien zur Verfügung stellt, ist dies ein guter Markt für Drittanbieter. Es gibt eine Reihe kommerzieller Lösungen, mit denen Sie den Zugriff auf USB-Speichermedien kontrollieren können. Diese Lösungen erlauben in der Regel auch weitergehende Kontrolle, indem sie Floppies, CD-ROMs und Schnittstellen blockieren können.

Drei verschiedene USB-Sticks. Bei der Uhr ist links vom Zifferblatt das ins Armband integrierte helle Anschlusskabel erkennbar.

Kontrollieren Sie den Zugriff durch restriktive Rechtevergabe

Diverse Anleitungen, die Rechte auf den USB-Speichermedientreiber so zu setzen, dass er nicht mehr installiert werden kann, funktionieren nur, wenn der Treiber nicht schon installiert ist – also nur direkt nach der Erstinstallation – und wenn der Nutzer keine lokalen Administratorrechte hat (vgl. z.B. Axel Vahldiek, Stick-Stopp: USB-Speichermedien unter Windows XP blockieren, c't 12/04, Seite 206).

Die Speicherkapazität steigt, und damit auch das Sicherheitsrisiko

Derzeit sind Festplatten in externen Gehäusen mit USB und/oder Firewire schwer im Kommen. Dabei geht es um Speicherkapazitäten von 20–80 GB bei 2,5-Zoll-Festplatten und ca. 200 GB bei 5,25-Zoll-Platten. Sie sind kaum größer als eine Zigarettenschachtel. Auch wenn diese Geräte etwas voluminöser und damit nicht ganz so leicht zu verbergen sind wie USB-Sticks, stellen sie aufgrund der enormen Speicherkapazität ein Sicherheitsrisiko dar.

Prof. Dr. Rainer W. Gerling

Rainer W. Gerling ist Datenschutzbeauftragter der Max-Planck-Gesellschaft und Honorarprofessor für IT-Sicherheit an der FH München.