



Sicherheitsproblem USB-Geräte



Bildungszentrum des Hessischen Handels gGmbH
Westendstraße 70
60325 Frankfurt am Main
Beauftragter für Innovation und Technologietransfer im Handel
Herr Thomas Scherer
Tel.: 069 / 74742–222
Fax: 069 / 74742–300
Mail: bit@bzffm.de

1. Einleitung

Der Einsatz von mobilen Speichermedien ist mittlerweile in Unternehmen weit verbreitet und gehört zum Tagesgeschäft. Dies gilt für geschäftlich zur Verfügung gestellte Geräte ebenso wie für private Geräte.

Egal ob USB-Stick, MP3-Player, iPhone oder PDA, die verschiedenen Geräte lassen sich meist problemlos an vorhandenen PCs oder Laptops anschließen und installieren.

Meist wissen Unternehmen gar nicht in welchem Maße ihre Mitarbeiter private Datenträger im Unternehmen nutzen um z.B. dem Kollegen die letzten Urlaubsfotos zu zeigen oder Musikdateien auszutauschen.

Mittlerweile dienen USB-Geräte aber nicht nur als Datenspeicher, sondern werden auch für Anwendungen genutzt, die direkt vom USB-Gerät aus gestartet werden. Dass hierbei die Gefahr besteht das Firmennetzwerk mit Viren zu infizieren, bzw. die Kontrolle über den Datenaustausch zu verlieren wird von den meisten Unternehmen unterschätzt.

Des weiteren ändert sich durch den Anschluss eines neuen Gerätes auch die Konfiguration des jeweiligen Rechners, der somit nicht mehr den ggf. vorhandenen Vorgaben des Unternehmens entspricht.

Auch die Mitnahme von Dateien/Daten nach Hause zwecks Heimarbeit birgt nicht zu unterschätzende Sicherheitsrisiken. Eine Befragung der britischen Regierung ergab, dass zwei Drittel der Befragten schon einmal ein USB-Gerät verloren hatten. In über 50% der Fälle waren auf dem Speichermedium auch geschäftliche Daten vorhanden.

2. Viren

Der Schutz vor infizierten Dateien über E-Mail Programme ist in vielen Unternehmen selbstverständlich.

Der Schutz vor Infizierungen über mobile Datenträger durch Trojaner, Viren, Mal- und Spyware dagegen ist meist nicht vorhanden.

Hierbei kann eine Verbreitung von Viren, Trojanern usw. natürlich in beide Richtungen verlaufen; sowohl vom privaten PC über das USB-Gerät in das Firmennetzwerk, als auch auf umgekehrten Weg.

3. Datenklau

Da die Kapazität mobiler Speichermedien mittlerweile im Bereich von Gigabyte angekommen ist, ist deren Einsatz kaum noch beschränkt. Somit lassen sich nahezu alle Formen von Daten auf ihnen speichern. Die Art der Daten kann von Fotos, Kundendaten, Umsatzzahlen über Adressbücher und Dokumente bis hin zu vollständigen Datenbanken reichen.

Bei den Geschwindigkeiten heutiger Rechner und den Schnittstellen zu den USB-Geräten ist das Kopieren von Daten nur noch eine Sekundensache; und welches Unternehmen überprüft schon seine Mitarbeiter beim Verlassen des Arbeitsplatzes.

4. Maßnahmen

Als einfachste Maßnahme kann natürlich die Nutzung von USB-Geräten im Unternehmen generell verboten werden.

Je nach Unternehmensart ist dies aber keine praktikable Lösung, da auf den Gebrauch von USB-Geräten aus diversen Gründen nicht verzichtet werden kann.

Weiterhin kann man den Benutzern die Rechte entziehen neue Geräte auf ihren PCs zu installieren. Auch der Zugriff der Nutzer auf firmeninterne Daten lässt sich meist auf ein Minimum reduzieren.

Innerhalb des Unternehmens kann man z.B. verschiedene USB-Geräte definieren, die eingesetzt werden dürfen. Auf den PCs im Unternehmen wird eine Software installiert, die nur die Nutzung der definierten Geräte zulässt.

Hinsichtlich der Infizierung von Daten sollten PCs so eingestellt werden, dass auch angeschlossene USB-Geräte gescannt werden.

Vor dem Zugriff auf das USB-Gerät sollten diese manuell mit dem lokal installierten Virens scanner überprüft werden.

Das selbe Verfahren sollte auch angewendet werden bevor das USB-Gerät wieder entfernt und an einen anderen PC angeschlossen wird.

Quellen:

<http://www.cio.de>

<http://www.pcwelt.de>

<http://www.akademie.de>

**Haben wir Ihr Interesse geweckt?
Setzen Sie sich mit uns in Verbindung, wir beraten Sie gerne!**

Bildungszentrum des Hessischen Handels gGmbH
Westendstraße 70
60325 Frankfurt am Main

Beauftragter für Innovation und Technologietransfer im Handel
Herr Thomas Scherer
Tel.: 069 / 74742—222
Fax: 069 / 74742—300
Mail: bit@bzffm.de
Web: www.bzffm.de

Gefördert vom Bundesministerium für Wirtschaft und Technologie aufgrund eines
Beschlusses des Deutschen Bundestages sowie dem Hessischen Ministerium für
Wirtschaft, Verkehr und Landesentwicklung (HMWVL)



Hessisches
Ministerium für
Wirtschaft,
Verkehr und
Landesentwicklung

