USB Flash Drive Security

(1) Convenience and Portability

USB thumb drives have become popular and affordable the last few years. They can go in your pocket or on a key ring. You might know them as flash drives, key drives or jump drives. Smaller thumb drives can hold anywhere from 8 megabytes (5 floppy disks) to 256 megabytes (177 floppy disks) of data!

Thumb drives plug into USB ports. That makes them useful on just about every computer sold these days. Newer operating systems (XP, Win2K, and some Linux distributions) automatically recognize and mount these USB drives, assigning the next-available drive letter. And usually you don't have to install any software to use one.

Older operating systems (e.g., Win9x) may require a driver to recognize the USB device. Falling prices are the major reason they've become so popular.

(2) Security Concerns

Thumb drives are also convenient because they're so small. But that happens to be their major weakness. They can be lost, stolen, or "borrowed" easily. Your photos, work and personal files could end up in someone else's pocket. They can also serve as a tremendous source of data leakage.

Attacks from peripheral devices usually require physical access to the host system, but janitors or contractors can easily exploit such access with a USB attack device. Thumb drives can be bootable, so they're also popular for diagnostic or repair work, but also very convenient for the bad guys.

Users often store the information they need, such as passwords or other sensitive information, on these USB flash devices. Because these devices are so small, they're an easy target for thieves, and they're also easier for users to lose or misplace. And that means that vital secrets can disappear before you know it.

(3) Known Vulnerabilities

Vulnerabilities in USB drivers for Windows could allow an attacker to take control of locked workstations using a specially programmed Universal Serial Bus device. The buffer-overflow vulnerabilities could enable an attacker to circumvent Windows security and gain administrative access to a user's machine.

This is just the latest example of a growing danger posed by peripheral devices that use USB (Universal Serial Bus), FireWire and wireless networking connections, which are often overlooked in the search for remotely exploitable security holes.

While it may be tempting to ban the use of these devices altogether, that really isn't necessary. These common devices are extremely useful, and it's perfectly fine to allow them on your network. But that doesn't mean you can neglect the inherent security concerns either. To better protect corporate data, take steps to add a layer of security to go with the information these handy devices can store.

(4) Security Controls

One of the best defenses for files on a thumb drive is encryption. Most manufacturers realize this and include encryption programs on their drives. Unfortunately, the best bargains are usually drives offering no security.

Use technology that can secure peripheral or "end point" devices.

Use technology that can block unauthorized peripheral devices, including insecure USB drives.

Provide users with encrypted, password-protected USB drives.

Purchase devices that include built-in security features. The additional cost is minimal when you compare it to the extra layer of security provided.

Before deploying these devices, make sure you update the organization’s security policy to address their use in the organization.

Consider maintaining a password database for the devices. Otherwise, if users forget their passwords, the cost of data recovery might not be equal to the corporate value of the data.

Consider using software that enables you to control access to removable media devices. This can be an effective security control.

Finally, be careful with your thumb drive. Treat it like luggage at an airport. Rarely let it leave your sight. It would hurt to lose one even if its information is safe.

Ty Cooper, CISSP, CSCP
Chief Information Security Officer (CISO)
Information Resources Management Division
U.S. Office of Government Ethics
1201 New York Avenue, NW, Suite 500
Washington DC 20005-3917
(202) 482-9300 x226
(202) 482-9237 (Fax)
ty.cooper@oge.gov

IT security is no accident. Be aware, be alert, and be safe in cyberspace.