



DISCUSSION WHITEPAPER

“Tackling the Removable Device Threat”

Jane is an office temp. She has been recruited by a rival firm to steal your company client list. During lunch the office is virtually deserted, so she plugs her 512Mb USB memory stick into the PC she is using and copies several folders and your client database from the local and network drives. She unplugs and pockets the memory stick and continues her work. The whole process takes less than 5 minutes, and nobody knows that she has stolen more than 300Mbytes of your corporate data.

This all too possible scenario illustrates a growing security concern. The fear is that people will use USB memory sticks, iPods, MP3 players, Smartphones, PDA's and the like to upload malware, steal data from corporate networks, and share stolen software, MP3 or AVI files.

Introduction

Most people now own some form of removable storage device. USB Memory stick, flash drive, smart phone, iPod, PDA, music player, digital camera - the list is nearly endless.

With no moving parts and permanent storage they are more reliable and rugged than CDs, and they typically offer up to 2Gb or more of storage space.

The benefits of these devices are obvious; fast, painless transfer of files between virtually any computer, and durable, portable data storage.

The Security Threat

These devices also present a huge potential security headache, that bypasses many of the security measures that organisations have put in place. Any individual with access to a computer within an organisation can quickly copy information and walk out of the front door undetected within minutes. As the devices generally connect to the USB (or firewire) port, Windows will happily install the device automatically *and* doesn't require the user to have any administrator rights.

Information copied to the device can be anything that can be accessed by the user of the computer; this could be the customer database, source code for unreleased software, expensive research or even the computer's own password file. Besides cleaners, temps, contractors and disgruntled employees looking to move to a competitor or leak information to others, access can also often be gained by outsiders using simple social engineering techniques.

To date most organisations have made it difficult for users to copy large amounts of data by restricting devices such as CD writers to IT staff. Additionally email monitoring and content filters prevent users emailing files and firewalls and monitoring software minimises the opportunities for transfer of information over the Internet.

None of these, however, prevent the copying of data to or from a memory stick.

In its report, "How to Tackle the Threat from Portable Storage Devices," Gartner suggested that organisations forbid attachment of privately owned portable storage devices to corporate PCs. The report also recommended that desktop PCs be carefully configured to remove or disable drivers needed to use such unauthorised devices.

This however, is easier said than done.

The Solution

So what can be done to protect from this threat?

The obvious solution would seem to be to disable USB support, thereby preventing the PC from installing the Flash Drive in the first place. This, however is not as easy as it might appear as USB / Firewire devices cannot be managed through Windows Group Policies – and what about legitimate USB keyboards and mice – how would they continue to function if all USB support were to be disabled?

The best technical solution is to install a dedicated third party product such as DeviceLock, which is designed from the ground up to control, and audit access to all aspects of the PC's removable device configuration, including USB ports, bluetooth, Wifi, Firewire, CD writers, floppies, tape drives and more.

More information on DeviceLock can be found at <http://www.pestscan.co.uk/devicelock>

A Computer Usage Policy is also essential. In addition to specifying the use of Internet and email, this should make explicit statements banning storage of organisation information on personal devices - and specifically Flash Drives. By making clear statements the common user defence of 'I didn't realise it meant that?' is negated. A total ban on Flash Drives could be added, but their size and portability means that they may still 'accidentally' be bought into the office. Good security awareness and training is also effective in ensuring users know about and understand the policy and the reasons for it.

A good Computer Usage Policy will also state that breach of the policy may lead to disciplinary action and potential dismissal, giving the organisation the authority to sack offenders.

To prevent unauthorised access users should be instructed to lock their PC when they leave it and use a password protected screensaver with a minimum timeout of 5 minutes or less should be used. This can also be enforced using Windows group policy.

Conclusion

Flash Drives are an example of an interesting and useful technical device that presents a new challenge to IT security. This is best tackled with a logical and practical approach to the problem that considers the real world and business issues and solves these through not only technical solutions, but using a mixed approach involving processes and people, common of many information security issues today.