

Re: Basic Windows Security Question

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2005-04/0027.html>

From: C. Francis Pineda (cfspineda_at_gmail.com)

Date: 04/05/05

Date: Mon, 4 Apr 2005 21:15:17 -0500

To: Andrew McIntosh <amcintosh@networkadvocates.com>

guys,

(on the usb)

last year, we had a seminar from a gfi partner on their new product that can control removable media (usb thumb drives/mp3, firewire, floppies, cd) via AD.

here's the link:

<http://www.gfi.com/lanpsc/>

features:

How it works

To control access, GFI LANguard P.S.C. installs a small footprint agent on the machine. This agent is only 1.2MB in size – the user will never know it is there. GFI LANguard P.S.C. includes a remote deployment tool, allowing you to deploy the agent to hundreds of machines with just a few clicks. After installation, the agent queries Active Directory when the user logs on and sets permissions to removable storage accordingly. If the user is not a member of a group that allows him/her access, then access to the device/CD/floppy is blocked.

Controls access to all types of USB sticks, SD cards (digital cameras) and more
USB sticks are one of the main threats as they are small, easily hidden and can store up to 1GB of data. GFI LANguard P.S.C. recognizes all USB sticks. In addition, it can control access to any device that can be mounted as a hard disk (whether accessed via USB, FireWire, etc.). For example, plugging a digital camera into a USB port gives users access to storage on an SD card; SD cards are available in several sizes including 512MB and over.

Controls access to CDs and floppies

You can centrally disable users from reading or writing data to/from a CD or floppy. This way, you can block normal users from bringing in data that could be harmful to your network, such as viruses, Trojans

SecurityFocus BASICS: Re: Basic Windows Security Question

and other malware. Although you can switch off CD and/or floppy access from the BIOS, in reality this solution is impractical: You would have to physically visit the machine to temporarily switch off protection and install software. In addition, advanced users can hack the BIOS.

Easily configure users who can have access via Active Directory
To grant a user access to any one or all three types of devices, simply make that user a member of pre-defined Active Directory groups for each of the three kinds of devices. You can also leverage the power of groups and make an entire department a member of the group. Other storage control software requires cumbersome per-machine administration, forcing you to make the changes on a per-machine basis and update the configuration on each machine before the settings can take effect. Configuration of GFI LANguard P.S.C. is effortless and leverages the power of Active Directory.

Includes remote deployment tool

The GFI LANguard P.S.C. remote deployment tool can deploy the agent network-wide in minutes. You can configure to deploy domain-wide, per computer or to a list of computers.

Centralized control facilitates temporary access

Because you can easily add/remove a user to a group in Active Directory, it is simple to grant temporary access to a removable media, floppy or CD. Temporary access may be occasionally required, but should not mean that you cannot control access the rest of the time.

On Mar 29, 2005 4:20 PM, Andrew McIntosh <amcintosh@networkadvocates.com> wrote:

> *Hello Everybody,*

>

> *I am curious to see the different suggestions for this scenario:*

>

> *Suppose you have a small company of less than 100 employees. One of the employees likes to bring his work home on occasion. He does so using a USB thumb drive. One day he catches a [virus, worm, Trojan, spyware, anything you can think of] at home and it winds up on his thumb drive, which he in turn brings to the company network.*

>

> *The company certainly should have anti-virus software in place, which would fix that problem. But what if he unknowingly loads a key logging program that could capture private customer information? What do you suggest? Here is what I could think of so far:*

>

> *Disable USB Port – That would solve the particular problem and create other problems. For instance, substitute the thumb drive with a floppy disk or CD. For obvious reasons you don't want to disable those as well.*

>

> *Restrict user permissions – That could potentially prevent a program from installing itself, but it would also cause the user some grief if they need to install programs themselves, or even do simple things like*

SecurityFocus BASICS: Re: Basic Windows Security Question

> *changing personal settings.*
>
> *Security Policy – Haven't looked into this yet, but maybe there is a way*
> *to prevent the use of thumb drives and other specific devices through*
> *security policy.*
>
> *What do you think?*
>
> *Thanks!*
>
> =====
> *amcintosh@ntad.com*
> =====
>
>

--

Cecil Francis S Pineda
Email: cfspineda@gmail.com

"There's a war out there, old friend. A world war. And it's not about who's got the most bullets. It's about who controls the information. What we see and hear, how we work, what we think... it's all about the information! The world isn't run by weapons anymore, or energy, or money. It's run by little ones and zeroes, little bits of data. It's all just electrons.
- Cosmo(Ben Kingsley), Sneakers 1992

Earn your MS in Information Security ONLINE
Organizations worldwide are in need of highly qualified information security professionals. Norwich University is fulfilling this demand with its MS in Information Security offered online. Recognized by the NSA as an academically excellent program, NU offers you the opportunity to earn your degree without disrupting your home or work life.
[http://www.msia.norwich.edu/secfocus en](http://www.msia.norwich.edu/secfocus_en)
