Expert Reference Series of White Papers

Seven Security Myths of Windows 7

Seven Security Myths of Windows 7

Randy Muller, MCT, MCTS, MCSE, CEH, Global Knowledge Instructor

Introduction

Network security is everyone's concern, not just the security and network administrators'. This also applies to computer security. Many security breaches occur due to user ignorance of basic security principles, not malicious intent. Good security begins with understanding what you can do to keep your systems safe and implementing a layered approach. If you depend on one program or feature to secure your computer and keep it safe (think a castle wall), then when (not if, but when) that dependency is breached, you may have personal information stolen or even have your computer taken over. Network and computer security are like an onion – there are multiple layers.

1. Windows 7 is Windows 7 when it comes to security features

Not all versions of Windows 7 are created equal. This can be confusing to home users and small businesses that do not have an Active Directory domain. Many features that you have heard about when it comes to improved security are only found in the more expensive editions. In fact, only the Ultimate and Enterprise editions contain all of the security features. The Professional edition does have Group Policy controls and Encrypting File System (EFS), but does not include AppLocker or BitLocker. The Home Premium version does not even have the reduced security features found in the Professional Edition. In short, you will have to pay more if you want the more advanced security features, so be careful to purchase the edition of Windows 7 that meets your security requirements. There is not a "one-size-fits-all" version of Windows 7, and there definitely is not an a la carte edition.

2. Do you myth the UAC (User Account Control)?

This may also be seen as the Principle of Least Privilege. In this principle, users or processes must be able to access onlythe information and resources required for their specific roles. In this case, we are looking at applying the least-privileged user account (LUA). Many home users are also members of the local administrators group, giving them complete access to the system. In most corporate environments, this is not a safe security practice. Granting administrative access – even on a local computer – can lead to numerous security vulnerabilities. The User Account Control (UAC) component can limit changes being made to a computer that require administrator-level permission. The UAC will notify a user if a change is attempted and if the user is an administrator, than the user can click Yes to continue. If the user is not an administrator, than someone with an administrator account on the computer will have to enter their password for the user to continue. Relying solely on the UAC to provide security for changes to your system is an invitation to disaster – especially when UAC is turned off completely.

3. AppLocker, all you need to control software

Network administrators have Software Restriction Policies that can be implemented to control the behavior of software (what can or cannot run). AppLocker can extend the capabilities of Software Restriction policies. Now, an administrator can restrict or permit applications to run based on unique identities of files and to specify which users or groups can run these applications. With AppLocker, an administrator can control the type of applications that can run, which user or security group can run a program, create exceptions for programs, and even use PowerShell to control AppLocker. In short, AppLocker is a powerful utility for network administrators; it cannot replace a more comprehensive security model including a robust anti-virus program. Trojan programs can still be used to install malware on a system and users can be tricked into running other malware programs.

4. I can Bitlocker, can you?

BitLocker Drive Encryption is a feature available on Windows7 Enterprise and Windows 7 Ultimate (another myth-conception of Windows 7). BitLocker and BitLocker To Go provide another layer of security to limit the potential loss of data through the loss or theft of a computer. BitLocker To Go can be used to protect USB flash drives as well as external hard drives. Not all computers can use BitLocker or BitLocker To Go. To use BitLocker, the hard disk on the computer must have two partitions, the operating system and active system partition must be formatted with NTFS, and the BIOS must support Trusted Platform Module (TPM) 1.2, though there is an exception. If the computer does not have a TPM of 1.2 or higher, you can use a USB drive to store the encryption keys. While this is an excellent method to secure your data, BitLocker or BitLocker To Go should be used in conjunction with other security methods to control access to your data.

5. Where can you DirectAccess?

There is always a secure, remote connection for Windows 7 users. Well, sort of. You would need to configure DirectAccess to provide for a secure automatic remote connection. DirectAccess allows users of Windows 7 Enterprise and Ultimate editions to make remote direct connections to a Windows Server 2008 R2 (as well as Windows 8 Server and beyond) server without having to use a VPN connection. Currently, users must use a VPN connection in order to make a secure remote connection. Once you implement DirectAccess, it is a completely transparent for action for end users. When the computer connects to the Internet, DirectAccess automatically creates a secure connection to the corporate network without any action on the user's part, and it automatically routes requests to the internal network through that connection. This is a version issue of Windows 7. You must have either Ultimate or Enterprise editions of Windows 7. Not all security capabilities are present in all versions.

6. Security Myth–Adventures of Windows 7

While Windows has more security features than previous editions and is vastly more secure, it simply does not have everything a business or home user requires to keep data and systems safe. Windows 7 has BitLocker and Bitlocker To Go to secure your data, but key loggers and shoulder surfers can defeat this security measure. The Windows 7 firewall does provide defense from many network-based threats, but it simply cannot provide the capabilities of a full-fledged firewall program that can examine packets and detect host intrusion detections and protection. A home user might be able to manually maintain a few systems, but simply could not handle a corporate environment. A corporate security administrator will employ a network-based security program rather than manually configure firewalls. There are many security threats beyond the capabilities of Windows 7 to pro-

vide a safe environment. New bots, hackers, identity theft techniques, rootkits, spyware, Trojans, and worms that can defeat even the best natively secured system.

7. The XP Myth (XP Mode)

Windows XP Mode (XPM) is a separate download available from Microsoft whereby you can run programs that were designed for Windows XP on computers running Windows 7. One thing to keep in mind is that the Windows 7 edition must be Professional, Enterprise, or Ultimate. Windows XP Mode runs in a separate window on the Windows 7 desktop, much like a program, except it's a fully functional version of Windows XP, and that is the concern. It is a complete Windows XP environment that is not protected in any way by the Windows 7 security controls (all of the above features we talked about). That means you do not have UAC, AppLocker, or the Windows 7 firewall. When you install a program in Windows XP Mode, that program will appear in both the Windows XP Mode list of programs and in the Windows 7 list of programs, so you can open the program directly from Windows 7. That means all of the vaunted security you have implemented now can potentially be bypassed.

Windows 7 is a very secure and robust operating system. For home users, it can be secured fairly easily, but you will want to invest in a good anti-virus program and possibly a firewall program as well. The corporate user has the advantage of having a partnership with the IT department and their security team. Windows 7 clearly demonstrates that Microsoft has done a fantastic job of producing a secure operating system. Now we just have to wait for Windows 8 to see what new security features will be available.

Learn More

To learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge, check out the following Global Knowledge courses:

Defending Windows Networks

Administering and Maintaining Windows 7 (M50292)

Planning and Managing Windows 7 Desktop Deployments and Environments (M6294)

Configuring and Troubleshooting a Windows Server 2008 Network Infrastructure (M6421)

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

Randy Muller (MCT, MCTS, MCSE, CEH) is an instructor with Global Knowledge, specializes in teaching Microsoft Office 365, Exchange, Lync Server as well as Windows Server 2008.