Comprehensive guide to Windows 7 security - Part 1

In this article we will introduce you some basic knowledge needed to secure Windows 7 properly, help you achieve basic security ...

In this article we will show you how to secure Windows 7 and introduce some of the lesser known security features that this operating system provides.

Windows 7 is Microsoft's latest desktop computer operating system, built on the strengths and weaknesses of its predecessors, Windows XP and Windows Vista. Every aspect of the operating system like, how to run services and how to load applications will make this operating system more secure than ever. All services are enhanced and there are more reliable security options available. However, the fundamental improvements to new systems and services, Windows 7 also provides better security functions, improved authentication and test features, and encryption capabilities. Remote connection and data, this operating system also has many improvements for protecting internal components, ensuring system safety such as Kernel Patch Protection, Service Hardening, Data Execution Prevention, Address Space Layout Randomization and Mandatory Integrity Levels.
It can be said that Windows 7 is designed to be safer. First, it was developed on the basis of Microsoft's Security Development Lifecycle (SDL). Secondly, it is designed to support the general standard requirements for

certification Evaluation Assurance Level (EAL) 4, to meet the information processing standards Federal Information Processing Standard (FIPS) # 140-2. When used as a standalone operating system, Windows 7 will protect individual users well. It has many useful security tools inside, but only when used with Windows Server 2008 (R2) and Active Directory, protection will be more effective. By raising the level of security from tools like Group Policy, users can control all aspects of desktop security. If used for personal or small office, the operating system still appears to be quite secure in preventing multiple attack methods and can be recovered quickly in case of a disaster, so although there will be more advantages if Windows 2008 is available, this is not necessary to get a high level of security for Windows 7.

However, even though it may be assumed that Windows 7 is itself a secure operating system, that doesn't mean that you rely solely on the default configuration but forget about making some adjustments to reinforce. his security capabilities. Be aware that you are the target of some form of malware or Internet attacks when your computer is used in public networks. Be aware that if the computer is used for public Internet access, your system and the network it connects to will be a good bait for attackers.

In this article, I will show you some basic knowledge needed to secure Windows 7 properly, help you achieve basic security, consider some advanced security configurations as well as go explore some of the lesser known security features in Windows to prevent and protect against possible attacks. Introducing a number of ways to ensure data security, perform backup and run quickly if you encounter some attacks or system malfunctions in a catastrophic way beyond your ability to handle. Then there are some security concepts, how to 'solidify' Windows 7, how to install and provide security for running applications, how to manage security on a Windows 7 system and prevent problems. threads caused by malware.

The article also introduces data protection, operating system backup and restore features, how to restore the operating system back to its previous operating state, some ways to protect data and system state. If disaster happens. We also introduced a number of strategies for quickly implementing those tasks. The topics covered in this article also include how to work safely while online, how to configure biometric controls for advanced access control, how and when to use them with Windows Server 2008 (and Active). How to Directory), how you can safely integrate options for control, management and testing. The goal of this article is to introduce you to the security features of Windows 7, the enhancements and their applications, and to provide you with the knowledge of planning, using the right features. This security feature. The concepts that we introduce will be broken down and organized by block method.

Note : If you work in a company or other professional environment, you should not make adjustments to your company's computer. Follow the published security plan (or policy), as well as the best practices, principles, and guidelines published in the organization. If you're not familiar with security topics and Microsoft products, read the product documentation before applying any changes to the system.

Basic security issues

Before diving into the details of Windows 7, I want to introduce you to some basic concepts about security and how to plan for its applications. You also need to know why testing to maintain security is so important and how to correctly check security services to find the problem. More importantly, we also need to know how to check and discover if we have to open the door for easy attacks. Security is not something you can plan arbitrarily and then quickly apply. It is a concept that must be applied to every technical aspect in deployment as well as in practice. It is also something that needs to be considered carefully before being deployed and then tested and managed after application. It is required that you conduct an analysis to make appropriate adjustments to the current security architecture, as well as discover potential attacks. Most need to be tested by a malicious program or an attacker to find access in this process; Then you can pioneer in protecting yourself if you see any attempts

and actions that are invasive. Take notes and then verify, you will find interesting information about what is querying your router login prompts, administrator account login attempts, .

Logs and warnings are very useful because, when something goes wrong, you can respond quickly and accurately by analyzing source IP addresses, or login attempts are caught by assessment. Responding to an attack with a detailed plan is called incident incident. Preparation will be the main key to the act of 'responding to the incident', so having a pioneering plan and a response plan is important to have before the disaster happens. The Disaster Recovery Plan (sometimes used in conjunction with the work continuation plan, BCP), will include a recovery strategy from incidents. Some IT units also have IT experts dedicated to responding to the case, this is the group that will take responsibility according to the plan set out to overcome and solve important issues that may cause a halt The system works significantly, or worse, data loss, network and system attacks, etc.

For home users and independent systems, you need to follow such a strategy but at a simplified level. Because you still need to protect everything, you need to react to the disaster, so a good plan created in advance for disaster recovery will do the right thing for you. A good example of such a simple plan would be, if your system is infected with malware (such as a Trojan), chances are you'll have to reinstall the operating system if all attempts are made. restore and fix failure. If this is the case, you need to assign the team members, detailed steps and pre-prepared disaster procedures to be able to respond correctly and a test process to ensure that everything is done right after recovery takes place. Being able to access, or have a copy of the installation files or any other program and application in hand now saves you time troubleshooting, and if set up correctly, it can show you the right direction you need to take.

Note : To help you plan and know more about security issues, you can search the checklists and plans in the referenced links section of this article.

Also review your plans on a regular basis, especially after a serious problem has occurred and have additional action items if needed. Once you have the right plan, you need to consider building on the platform with many functions and services.

Tip : Security needs to be reviewed and applied to which systems or services are used to mitigate the risks involved while working. And if security is applied in such a way as to prevent an attack or a disaster, what you have to spend will be much less expensive. Security, even at its most basic level, needs to be applied to keep personal data safe, but make sure that if you need to completely reinstall Windows from the rubble, you can still reuse their data and can access and use this data. Security cannot be ignored.

Consideration should also be given to implementing security in both conceptual and technical uses of the Defense in Depth security concept. Security needs to be considered and applied to all network systems, services, applications and devices, which need to keep your system up and running with the Internet. Published policies and plans have been developed to help users gain high productivity in using the systems, along with general understanding of the use of policies. Continuous maintenance will increase your investment. But to prevent vulnerabilities in security architecture, you must consider planning and applying security models that use the concept of 'Defense in Depth'. Figure 1 shows the 'Defense in Depth' application at the simplest level, you can add other classes, depending on how your family or corporate network is set up.

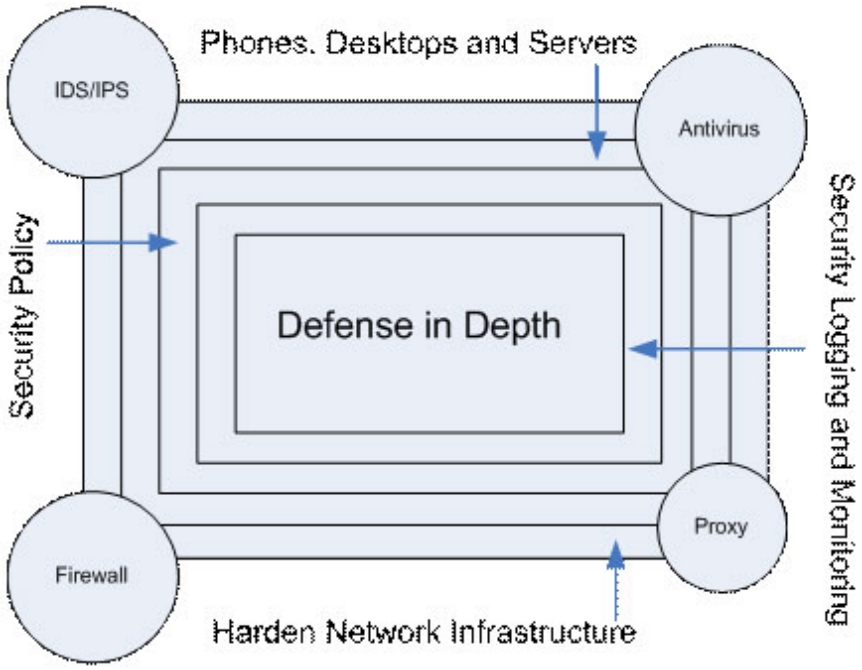


Figure 1: See how Defense in Depth is focused and deployed

Defense in Depth as you can see, can be customized to suit your needs. In this example, the security policy is to provide security and communication direction to users in the system and the network. In addition, it should be considered to solidify your systems, phones, desktops, services, applications, servers, routers, switches and PBXs, all, to ensure that all The entrances are well shielded. Obviously, there are still some forms of public Internet protection (such as firewalls) that need to be used during the usage process, but always have to extend this issue and add other items such as polling sets. , filtering, scanning to get more sophisticated support. In addition, you should also have a way to check and record all this information for purposes of reviewing and reviewing if necessary.

Windows 7 is designed to be integrated into any environment that conforms to a high level of security, such as the US government and the US military. When considering the basic security principles of Windows, you need to remember that any enterprise-level system must be certified at C2 security level from the gold book. Microsoft Windows also needs to follow the general standard certificate. For more information on these topics, you can find other articles and other information at the end of the reference links. Windows 7 is quite flexible, with many options that allow you to configure a system with complete functionality (minimum security), or a basic-level configuration, with only the operations you configure for permission to use (maximum security). With Windows 2008 and Windows 7, the security function will increase tenfold when used together properly.

Note : Remember that denying a problem (or a potential problem) is not an option. Previous problems can be used later, or omitted completely. Lazy just makes you spend a lot of time. Even so, obscure security is not confidential. Failure to follow a strict rule will only cause many problems later. A security deployment throughout home computers or within a business (both important) will prevent detection and attacks, providing multi-layer security to help the status quo. Your security is at a high level of security, but not all of them will be avoided. You need to know the basics of security, how to prepare ahead and how to cope with attacks if you want to be safe.

So far you have become familiar with some of the basic security concepts, let us take a look at what we have studied in the process of configuring Windows 7 security settings. The point of looking at how we gain knowledge begins with why we want to apply security, when to apply it, as well as the reasons for managing, testing and upgrading it, all What we need to do is dig more into those security concepts while configuring a basic Windows 7 system. This problem will be done quite easily if you know what you want to accomplish. If a new Windows user or someone who is very difficult to adapt to this new operating system (you probably missed Vista) then you will probably need to spend a lot of time learning the tools and Study them on online websites to get a deeper understanding. For example, you can find many online templates and checklists from Microsoft.com, which will give you the ability to step-by-step apply security issues on Windows systems. You can also find useful tools in the reference links at the end of this article.

Templates are not always the answer, sometimes it can cause unwanted consequences if not used properly (or properly configured), always observe the notes - even Releases download directly from Microsoft.com. Another important thing that you need to do is always read the documentation that comes with the template to be able to use it correctly. It must be emphasized that, without a basic platform for an operating system itself, or the basic principles that the operating system operates, you will not be able to maintain a high level of security in one. long time. Knowledge of the core operating system and its translations is also essential if you want to maintain a high level of security, even after properly configuring the security on your base system. Event Viewer logging is extremely useful, because you can configure the audit action (for example) and get detailed information about what's going on inside your systems. Most (but not all) of the records are intrinsically incomprehensible and interpret problems in the most basic terms or with a set of machine languages. You will need online to remove your problems, this is a way to make your work easier. And you'll see a lot of things I don't know and will find a lot of tools that I want to add to my kit for future deployments when tested carefully.

There is also a degree of flexibility when applying security, which allows you to achieve the goals and requirements of your business (such as Internet access) without having problems. What, while still maintaining the high level of security needed. A great example is the User Account Control (UAC) tool, which is a tool when adjusted, can provide a high level of security, or can be turned off completely. You will have to restart your system if you turn off UAC.

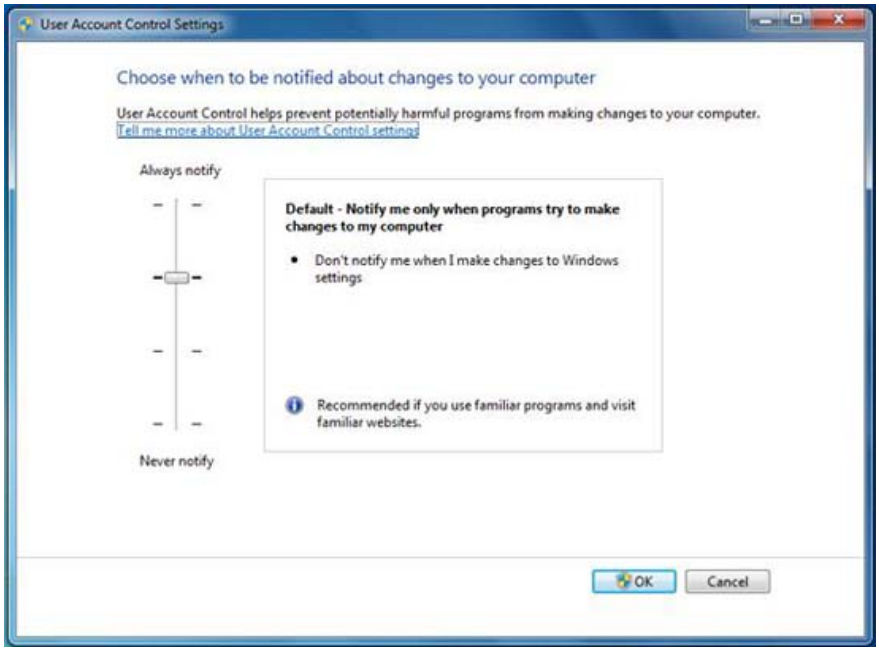


Figure 2: Adjusting the Level of Security by adjusting UAC settings

UAC is used to prevent programs and applications from making changes to your operating system. It works by restricting access within the operating system core, then providing detailed information to the user about the programs that are trying to install or interfere with the operating system configuration. This is a very useful tool, it gives you the opportunity to assess what programs are working and can interfere if that's what you don't want. UAC has been introduced since Windows Vista, but since Vista users cannot turn off this utility, it seems to be an annoyance for most. In Vista, UAC also annoys users because they can't seem to find a way to solve those problems. Windows developers also have a lot of trouble writing the code because of UAC limitations and some related but necessary issues. Now, with Windows 7, UAC can be turned off completely, which is an insecure level of security configuration, but it provides users with flexibility and an additional choice.

Note : It is important to protect your system safely, not completely turn off UAC or if you turn it off for some reason, you need to turn it on immediately.

Install and 'solidify' Windows 7

It can be said that Windows 7 is a safe design. When deploying it, you should perform a fresh installation on a newly purchased computer, need to have the required hardware configuration and then 'solidify' it. Enabling the system is a process that increases the security level for a newly installed computer by configuring necessary security settings, removing unnecessary software and making adjustments. some advanced policy settings.

Note : You need to create a plan when selecting hardware for Windows 7, because if you want to use virtualization, or the Windows Trusted Platform Module (TPM) Management feature as well as other features such as BitLocker, you need to must buy the right hardware that it supports these features.

When your operating system is properly installed and basically configured, it is time to do the "solidify" process. Is it necessary to have a new Windows installation or can it "solidify" a system already in use? Technically, you can 'solidify' any system that is already installed and being used, but before you do it, you should do research, analyze, test and verify the levels. Current security is configured in use. Not "solidifying" something was compromised. You also do not know how security applications will affect the production system when used in the home or corporate environment. Some cloning systems set up to test will cost you a bit of time and resources, but this is worth doing because it can find out and avoid some problems that may appear with the device. Your design and deployment. You can do more damage than do it better if you don't know how changes in security settings or templates will affect services on the production system. For example, it is possible to apply security to a system and limit changes to the firewall's filtering features, remove functionality from a program that you have installed and used - it can use one certain ports are currently closed by the firewall and this will result in a connection error. This problem can cause undesirable effects if the application is used for business, necessary for production and may need a lot of time to search and fix. That's why it is simpler to install fresh Windows 7 operating system, then 'solidify' it quickly, you can verify that security will remain in place until deploy it. In addition, you can also make the process faster, especially if you are using a virtual machine (VM) or VHD file, these are things that give you many options to create multiple instances of the desktop to be able to manually virtual failover or restore quickly if there are no reserve options. Virtualization simplifies the installation process when creating asexual images for backup purposes, so you can restore your desktop easily and within a few minutes. We will introduce virtualization in the later part of this series. If automatic failover is enabled and configured, desktop users may not even notice a stop on the device at all if they are virtualized.

You can 'solidify' the system and then access your secure data through drives, databases and shared repositories - all done at high speeds, with options. Select failover not only makes it safe, but also separates the data you access. If you plan correctly, you can create a complete snapshot of the configured, safe, and updated Windows version, and when disaster strikes, you can restore the system quickly. Then, after restoring the basic operating system, you can re-mount the shared drive to access the data.

So when installing Windows, what steps do you need to take to 'solidify' it? And is there a certain order to choose? If there are some installation steps and 'solidify' they will be the basic installation order, removing some unused things, updating the system, applying basic security, then creating a backup to restore quickly when needed, see list below:

- **Step 1** - Install the basic operating system by selecting the options during the installation process to increase security, not selecting unnecessary services, options and programs.
- **Step 2** - Install the Administrator toolkit, security tools and necessary programs.
- **Step 3** - Remove unnecessary services, programs and software. Disable or remove unused user or group accounts.
- **Step 4** - Upgrade service packages, patches, as well as all installed programs.
- **Step 5** - Perform security audits (scans, samples, MBSA, .) to assess the current security level.
- **Step 6** - Run System Restore and create a restore point. Backup and restore application for disaster recovery.
- **Step 7** - Backup the operating system in some way to quickly recover it in case of a disaster.

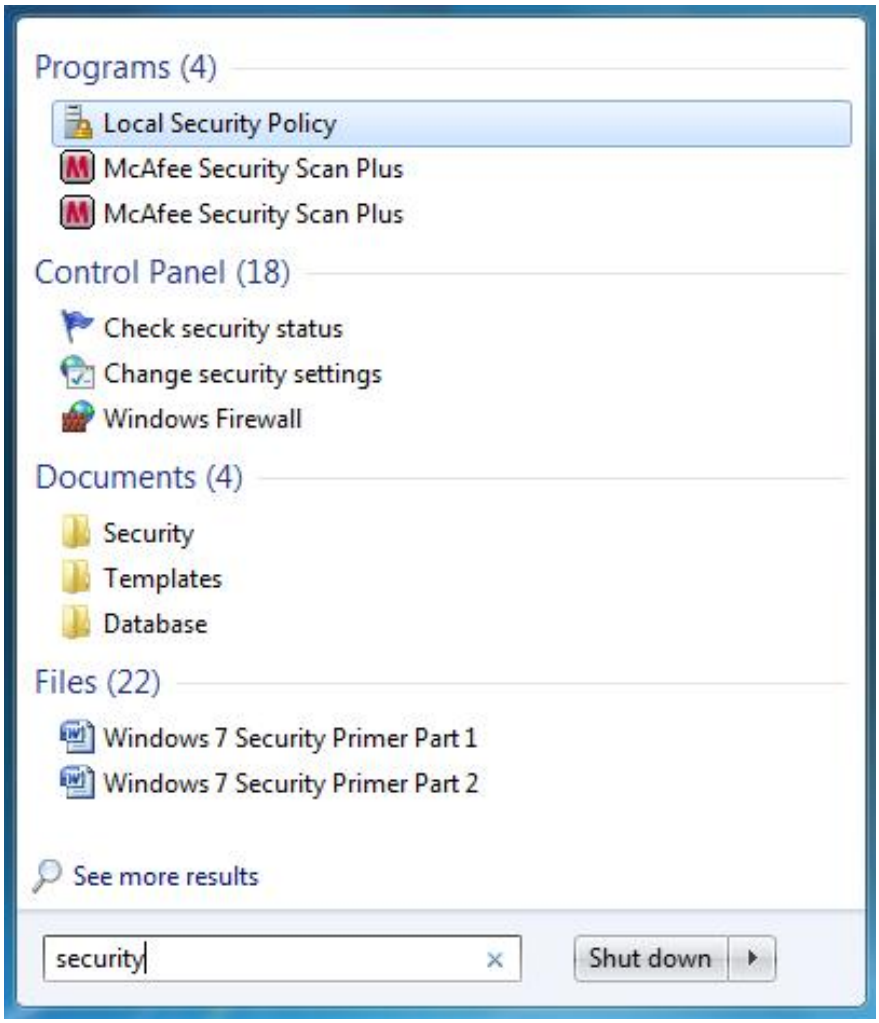
This is just a simple list. B?n có th? b? sung thêm m?t s? b??c và m? r?ng danh sách này h?n n?a. Rõ ràng nó không ph?i là m?t danh sách b?t bu?c, tuy nhiên danh sách này là m?t ?i?m kh?i ??u khá t?t khi áp d?ng b?o m?t vào Windows 7 sau khi ?ã cài ??t c? b?n. N?u hoàn t?t m?t cài ??t fresh cho Windows 7, b??c ti?p theo là g? b? ph?n m?m, d?ch v?, giao th?c và ch??ng trình mà b?n không mu?n hay không c?n ch?y nó. Công vi?c này có th? th?c hi?n d? dàng trong Control Panel.

Ti?p ??n, b?n có th? vào Control Panel và thi?t l?p xem ai ???c phép s? d?ng máy tính trong User Accounts applet. ? ?ây b?n nên remove các tài kho?n không c?n thi?t, ho?c vô hi?u hóa nó. Rõ ràng, nên c?n th?n v?i ng??i dùng và nhóm ng??i dùng m?c ??nh, m?t s? tài kho?n ?ó s? ???c th?t ch?t v?i các d?ch v? ?ang ch?y, cách truy c ?p d? li?u c?a b?n và ,. B?n có th? vô hi?u hóa c?ng nh? remove tài kho?n m?t cách d? dàng. M?t k? thu?t khác ???c s? d?ng b?i h?u h?t các chuyên gia b?o m?t là ?? tài kho?n qu?n tr? viên n?i b? ? m?t n?i thích h?p và th?m ??nh nó cho các c? g?ng s? d?ng. M?t cách làm chung là không s? d?ng các tài kho?n m?c ??nh khi qu?n lý m?t m?ng Microsoft v?i s? l??ng l?n các h? th?ng và thi?t l?p các tài kho?n qu?n tr? viên m?i có th? ???c l?n v?t n?u c?n. B?ng cách th?m ??nh các tài kho?n m?c ??nh này và s? d?ng tài kho?n ???c t?o m?i v?i các ??c quy?n qu?n tr? viên có liên quan v?i nó, b?n s? t?ng ???c ?? b?o m?t lên g?p hai. M?t là b?n s? phát hi?n ra ai ?ó ?ang c? g? ng truy c?p vào máy tính c?a mình b?ng các tài kho?n m?c ??nh khi mà l? ra không ai ???c làm vi?c ?ó. N?u ??? c th?m ??nh, b?n có th? th?y các c? g?ng và th?i ?i?m chúng di?n ra. ?ng d?ng b?o m?t cho tài kho?n ???c bi?t ?? n nh? m?t *honeypot* và h?u d?ng trong vi?c tìm ki?m các c? g?ng gây ra b?i nh?ng ng??i dùng ?ang c? g?ng truy c?p vào h? th?ng c?a b?n. Hai, b?n có th? b? ???c m?t n?a ph??ng trình khi ai ?ó c? g?ng crack tài kho?n c?a b?n thông qua các ch?ng ch? c? b?n, ch?ng h?n nh? s? k?t h?p c?a username và password. N?u b?n l?y ?i các thông tin d? ?oán v? username, thì b?n ch? còn l?i m?t kh?u, th? có th? ???c c?u hình theo cách nào ?ó ?? không th? b? crack. N?u ?ã thi?t l?p các tài kho?n m?c ??nh nh? m?t honeypot thì b?n có th? t?o m?t m?t kh?u g?n nh? không th? crack và h?n ch? nó ?? không th? th?c hi?n th? gì n?u có b? th?a hi?p (h?n ch? ???c ?nh h??ng khi b? th?a hi? p). B?n nên thay ??i t?t c? m?t kh?u cho các tài kho?n m?c ??nh. S? d?ng m?t kh?u theo cách có th? làm cho m?t kh?u ???c kh?e nh?t ?? b?o m?t cho các tài kho?n và c?n th?m ??nh chúng . B?n c?ng nên c?u hình chính sách ?? ng??i dùng c?n thay ??i m?t kh?u qua m?t quá trình mà ? ?ó h? ch? ???c phép thay ??i nó n?u ch?n m?t kh?u m?i

m?nh và không d? b? hack. ?ây ch? là m?t m?o 'làm v?ng ch?c' mang l?i nhi?u l?i ích, ch?ng h?n nh? kh? n?ng phát hi?n các t?n công thông qua vi?c ghi chép và th?m ??nh.

M?o : Trong Windows Server 2008, b?n có th? cài ??t ch?c n?ng 'core' (lõi), m?t quá trình 'làm v?ng ch?c' ???c áp d?ng cho h? th?ng trong giai ?o?n cài ??t th?c s?. Khi cài ??t, máy ch? ch? ch?y v?i nh?ng ch?c n?ng t?i thi?u mà b?n c?n ??n, vì v?y s? gi?m ???c b? m?t t?n công. Windows 7 có th? ???c 'làm v?ng ch?c' nh?ng không có tùy ch?n cài ??t gi?ng nh? ? Windows Sever 2008. ?? 'làm v?ng ch?c' Windows 7, b?n c?n áp d?ng các chính sách, các template ho?c ph?i t? c?u hình các thi?t l?p b?o m?t c?n thi?t.

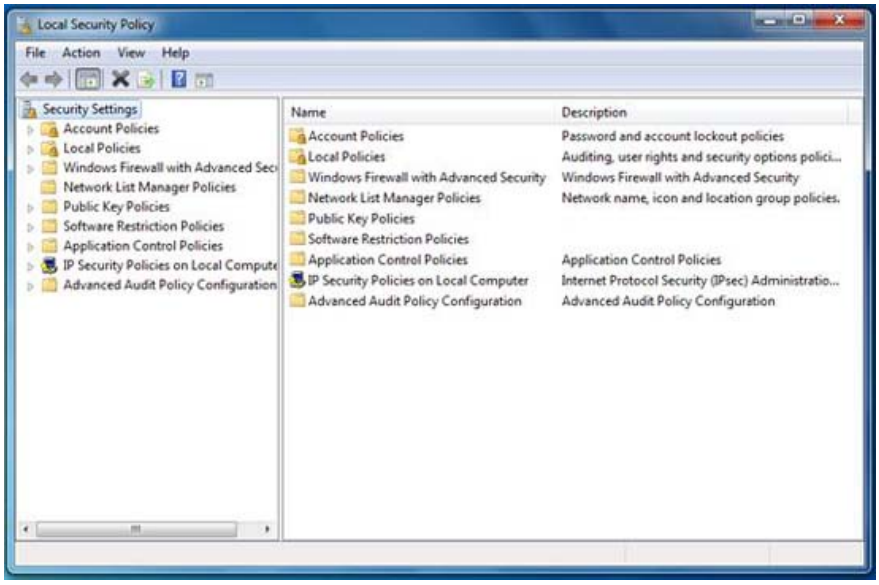
Nói là v?y nh?ng cách mà b?n b?t ??u ?? khóa ch?t và b?o m?t cho Windows 7 nh? th? nào? M?t cách d? dàng nh?t ?? b?t ??u quá trình 'làm v?ng ch?c' h? th?ng c?a b?n là s? d?ng menu Start ?? tìm ki?m b?t c? th? gì có liên quan ??n v?n ?? b?o m?t ???c l?u bên trong h? th?ng và ?ã ???c ?ánh ch? s?. ?? th?c hi?n ?i?u ?ó, hãy kích nút **Start** ?? m? Start menu. Sau ?ó ?ánh vào t? khóa ' **security'** trong tr??ng **Search Programs and Files** . Hình 3 bên d??i hi?n th? các tùy ch?n c?a Start menu d?a trên t? khóa tìm ki?m 'Security'.



Hình 3: Tìm và sau ?ó xem các tùy ch?n b?o m?t bên trong menu Start

? ?ây b?n có th? th?y các ch??ng trình, Control Panel applet (hay các action), tài li?u và file ?ã ???c ch?n và ???c t? ch?c theo cách d? xem và truy c?p. Local Security Policy (n?u ???c ch?n) là b? ch?nh s?a chính sách, cho

phép b?n xem và c?u hình các chính sách b?o m?t cho h? th?ng. Local Security Policy editor có th? th?y nh? trong hình 4. ? ?ây b?n có th? th?c hi?n m?t s? ?i?u ch?nh cho t?t c? các thi?t l?p d?a trên chính sách trên h? ?i?u hành c?a mình.

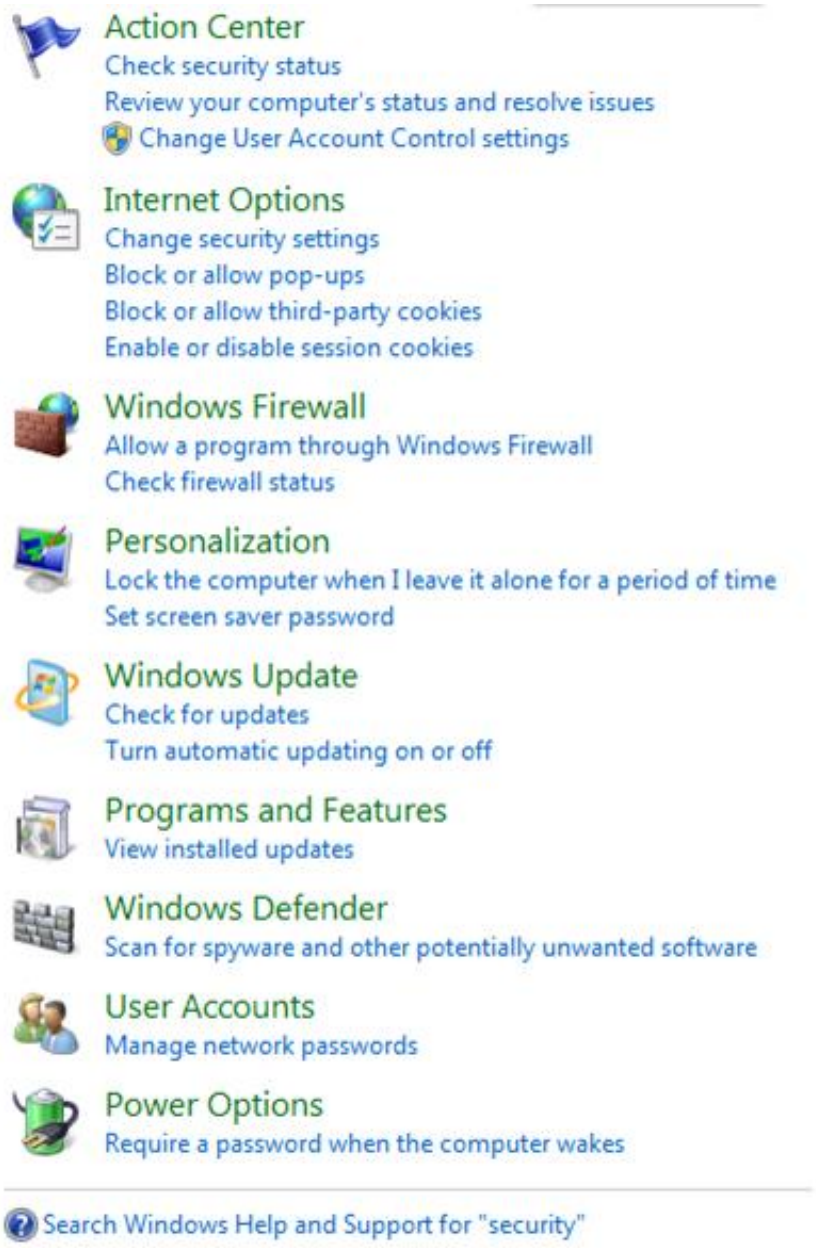


Hình 4: Xem và c?u hình b?o m?t v?i chính sách b?o m?t n?i b?

M?o – ?? có quy?n ?i?u khi?n toàn b? chính sách, b?n nên s? d?ng Windows 7 v?i các s?n ph?m Windows Server, ch?ng h?n nh? Windows Server 2008 R2. N?u th?c hi?n nh? v?y, b?n có th? s? d?ng Active Directory (AD) và Group Policy.

N?u mu?n thi?t l?p c?c b? hành ??ng th?m ??nh cho m?t s? ki?n nào ?ó (ch?ng h?n nh? s? ki?n ??ng nh?p và ?? ng xu?t), b?n có th? ch? ??nh hành ??ng ?ó trong c?a s? Local Security Policy (hình 4). Trong Control Panel, b?n có th? vào Administrative Tools applet ?? tìm Local Security Policy editor, ho?c tìm ki?m nó trong Start menu. Khi Windows 7 ???c s? d?ng v?i Active Directory, b?n có th? s? d?ng Group Policy, m?t d?ch v? m?nh cho phép b?n tùy ch?nh, qu?n lý và tri?n khai các thi?t l?p c?ng nh? s? ?u tiên trong tri?n khai ph?n m?m m?t cách d? dàng, tuy nhiên b?n c?n k?t n?i Windows 7 v?i mi?n tích c?c và qu?n lý nó ?úng cách.

N?u c?n c?u hình b?o m?t theo chính sách thì ?ây là cách làm ??n gi?n nh?t. Tuy nhiên ngoài ra b?n c?ng có th? th?y nhi?u công c? c?n thi?t cho vi?c c?u hình b?o m?t trong Control Panel ho?c trong MMC mà b?n thi?t k? và tri?n khai. Microsoft Security Center (Windows Vista, XP) ?ã ???c s? d?ng ?? t?p trung h?u h?t các ch?c n?ng b? o m?t tr??c ?ây. ?ây là th? ???c thay th? b?ng Action Center, và các hành ??ng b?o m?t hi?n d? tìm h?n nhi?u, ???c quan sát và ???c ch?n d?a trên s? cho phép c?a b?n. Cho ví d?, nh? th? hi?n trong Start menu (hình 3), hành ??ng 'Check security status' khi ???c ch?n s? t?o m?t danh sách các c?u hình b?o m?t mà Windows 7 khuy?n khích, ch?ng h?n nh? nâng c?p h? th?ng, hay m?t ch??ng trình nh? antivirus (AV). Khi ???c ch?n, b?n s? ???c g? i ??n Action Center ?? b?n bi?t thêm các v?n ?? c?n quan tâm.



Hình 5: C?u hình các hành ??ng b?o m?t và các tùy ch?n trong Control Panel

M?o : Hình 5 hi?n th? các hành ??ng có trong Control Panel mà b?n có th? l?a ch?n. N?u kích **Start** menu, ?ánh ' **security** ' và kích liên k?t Control Panel, b?n s? nh?n ???c m?t danh sách các hành ??ng và c?u hình b?o m?t, ? ây là danh sách b?n có th? tùy ch?nh ngay l?p t?c v?i các tùy ch?n d? tìm và d? truy c?p.

Khi ? trong Action Center (ho?c n?u ?ang xem danh sách các hành ??ng), b?n có th? chuy?n xu?ng ph?n d??i danh sách và c?u hình nh?ng gì phù h?p v?i mình. ?ây là nh?ng gi?i thi?u v?n t?t v? các tùy ch?n có th? ???c c?u hình trong danh sách c?a Action Center:

- **Action Center** – Action Center thay th? cho Security Center. Action Center là n?i b?n có th? ch? ??nh các hành ??ng mà h? ?i?u hành có th? th?c hi?n. V?i s? cho phép c?a b?n, các hành ??ng có th? di?n ra. ? ?ây b ?n s? ???c thông báo r?ng ch?a th?c hi?n nâng c?p ph?n m?m Antivirus (ví d? nh? v?y). B?n có th? truy c? p vào thành ph?n trung tâm ?? th?c hi?n các hành ??ng có liên quan ??n b?o m?t c?n thi?t.
- **Internet Options** – Duy?t web v?i b?t c? hình th?c nào c?ng ??u m? c?a cho các r?i ro Internet. N?u s? d? ng máy ch? proxy, s? d?ng hành ??ng l?c và ki?m tra web, c?p nh?t các b?n vá l?i m?i nh?t cho h? ?i?u hành, b?n v?n có th? r?i vào tình hu?ng mà ? ?ó b?o m?t c?a b?n b? th?a hi?p. Bên trong Internet Options Control Panel applet, b?n có th? ch? ??nh các vùng an toàn, ch? cho phép các URL nào ?ó ???c phép truy c?p, tri?n khai các thi?t l?p b?o m?t nâng cao trong tab Advanced và,. B?n thân trình duy?t c?ng có tính n? ng l?c Phishing ?? ng?n ch?n các t?n công Phishing và các tùy ch?n c?u hình khác ch?ng h?n nh? InPrivate Browsing, tính n?ng ng?n ch?n vi?c l?u l?i các thông tin cá nhân c?a ban sau khi duy?t web, ??c bi?t h?u d ?ng khi s? d?ng m?t máy tính dùng chung.
- **Windows Firewall** – Gi?ng nh? b?t c? ph?n m?m nào ho?c t??ng l?a ph?n c?ng nào, Windows Firewall có th? làm ch?ch h??ng các t?n công c? b?n và có th? ???c c?u hình ? 'm?c tinh h?n' ??t m?c ki?m soát cao cho nh?ng gì vào ra kh?i h? th?ng máy tính c?a b?n khi k?t n?i v?i m?t m?ng public hay private. B?ng cách vào Control Panel và ch?n Windows Firewall, b?n có th? truy c?p ??n h?u h?t các thi?t l?p c?u hình c ?a t??ng l?a. Có th? kích liên k?t Advanced settings trong h?p tho?i ?? truy c?p Firewall with Advanced Settings và các tùy ch?n c?u hình. V?i Windows 7, b?n còn có th? tri?n khai nhi?u chính sách t??ng l?a ?? ng th?i và s? d?ng th? b?c mi?n m?i ?? c?u hình và qu?n lý t??ng l?a Windows d? dàng h?n.
- **Personalization** – Tùy ch?n Personalization là n?i b?n có th? thay ??i di?n m?o b? ngoài c?a Windows, tuy nhiên nó c?ng là n?i b?n c?u hình m?t kh?u screensaver n?u mu?n. N?u ch?y Windows 7 trong doanh nghi?p, ng??i dùng nên bi?t cách khóa các máy tr?m làm vi?c c?a h? b?t c? khi nào h? r?i bàn làm vi?c ho? c s? d?ng m?t thi?t l?p chính sách ?? th?c hi?n vi?c ?ó m?t cách t? ??ng sau m?t kho?ng th?i gian không ho ?t ??ng nào ?ó, m?c dù v?y n?u quên, b? b?o v? màn hình ?ã ???c c?u hình s? yêu c?u ??ng nh?p l?i có th? khá h?u d?ng. T?i nhà, ?ây s? là tuy?n phòng ch?ng n?u b?n r?i h? th?ng c?a mình và quên khóa nó.
- **Windows Update** – T?t c? các phát hành ph?n m?m ??u yêu c?u m?t s? m?c vá nh?t ??nh. B?n có th? chu ?n b?, test và phát tri?n ph?n m?m hoàn h?o nh?ng không th? tính toán h?t ???c m?i th?. C?ng v?y, các nâng c?p và phát hành m?i c?ng yêu c?u các nâng c?p cho h? ?i?u hành qua th?i gian t?n t?i c?a phiên b?n h? ?i?u hành hi?n hành. Do có nhi?u ti?n b? trong h? th?ng, nhi?u yêu c?u c?n thi?t cho các k? thu?t phát tri?n, nhi?u l? h?ng b?o m?t m?i ???c phát hi?n theo th?i gian, các nâng c?p driver cho hi?u su?t và ch?c n ?ng t?t h?n nên s? luôn có m?t nhu c?u cho Windows Update. Windows (và Microsoft) Update, ho?c các phiên b?n qu?n lý b?n vá c?a doanh nghi?p (WSUS,.) ???c s? d?ng ?? ki?m soát và tri?n khai các nâng c? p. Các công c? này ???c s? d?ng ?? ?i?u khi?n, theo dõi và ki?m tra các nâng c?p hi?n hành và t??ng lai c? n thi?t. C?u hình sao cho nó có th? th?c hi?n nhi?m v? này m?t cách t? ??ng, ho?c b?n ph?i có thói quen th ?c hi?n nó vì ?ây là m?t v?n ?? th?c s? quan tr?ng. N?u b?n không vá h? ?i?u hành c?a mình nh?ng gì khuy ?n khích (?ôi khi là yêu c?u), b?n có th? s? là ??i t??ng t?n công.
- **Programs and Features** – Ngoài vi?c ki?m tra và th?y nh?ng gì Windows Updates cài ??t, b?n c?ng c?n ki?m tra ?? xem nh?ng gì mình ?ã cài ??t vào h? th?ng c?a mình m?t cách th??ng xuyên, ??c bi?t n?u làm vi?c trên Internet ho?c download ph?n m?m t? các máy ch? web trên Internet. Cho ví d?, b?ng vi?c cài ??t m?t nâng c?p Java, n?u b?n không ??c các thông tin hi?n th? trên màn hình m?t cách c?n thân trong quá trình cài ??t, b?n có th? s? cài ??t c? toolbar trên h? th?ng c?a mình, th? s? ???c tích h?p vào trình duy?t web c?a b?n. Gi? ?ây, dù có ???c s? ki?m soát ch?t ch? h?n v? ?i?u ?ó, tuy nhiên v?n nên ki?m tra m?t cách ??nh k? ?? th?y nh?ng gì hi?n ???c cài ??t vào h? th?ng c?a mình.
- **Windows Defender** – Spyware là ph?n m?m ???c s? d?ng ch? y?u cho các m?c ?ích th??ng m?i trái phép, nó s? th?c hi?n nh?ng th? nh? phân ph?i m?t t?i tr?ng tr?c tuy?n, redirect trình duy?t c?a b?n ho?c g?i l?i các thông tin trên hành ??ng c?a b?n. M?c dù ph?n m?m Antivirus có m?t s? tùy ch?n ?? ch?ng l?i hành vi này nh?ng Windows Defender (ho?c các ?ng d?ng remove Spyware khác) có th? là m?t l?a ch?n ?? d?n d?

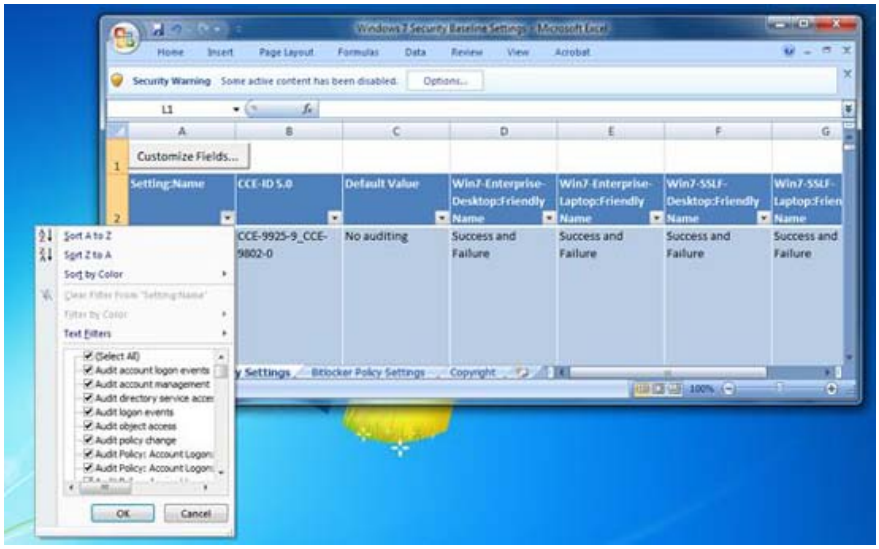
p ph?n còn l?i. Các Cookie m?c dù vô h?i theo b?n tính c?a nó, nh?ng ?ôi khi l?i b? thao túng v?i m?t vài lý do không ?úng. C?n ph?i b?o ??m nâng c?p Windows Defender th??ng xuyên v?i các file ??nh ngh?a m ?i và các nâng c?p c?n thi?t c?a nó ?? b?o ??m b?n có th? quét t?t c? Spyware m?i nh?t. SpyNet c?ng là m ?t c?ng ??ng mà Microsoft nói v? cách ng?n ch?n các m?i hi?m h?a gây ra b?i Spyware.

- **User Accounts** – Vi?c qu?n lý các tài kho?n ng??i dùng là c?t lõi c?a vi?c truy c?p an toàn máy tính c?ng nh? m?i th? ch?y bên trong nó. Cho ví d?, n?u t?o m?t tài kho?n ng??i dùng m?i và gán nó cho nhóm Administrators, b?n s? có quy?n truy c?p toàn b? vào h? th?ng máy tính. N?u c?u hình tài kho?n ?ó là ng?? i dùng chu?n thì các ?i?u kho?n mà ???c phép s? r?t h?n ch? và ng??i dùng ch? ???c phép th?c hi?n m?t s? th? c? th? nào ?ó. B?n c?ng có th? c?u hình m?t kh?u v?i chính sách m?t kh?u t?i thi?u ?? b?t bu?c ng??i dùng ph?i t?o m?t m?t kh?u khó b? crack. Khi Windows Server 2008 và Active Directory ???c tri?n khai, b?n có th? truy c?p m?t vào m?t mi?n nào ?ó mà khi truy c?p s? cho phép c?u hình các ?i?u kho?n NTFS 'tinh h?n' cho th? m?c và file c?ng nh? các ngu?n chia s? khác nh? máy in ch?ng h?n.
- **Power Options** – Power Options Control Panel applet là n?i b?n có th? c?u hình các hành vi m?c ??nh cho h? ?i?u hành khi không ???c c?m ngu?n tr?c ti?p, ?óng ho?c chuy?n sang ch? ?? 'ng?'. C?u hình b?o m?t ?? thi?t l?p là m?t m?t kh?u ???c yêu c?u khi máy tính th?c gi?c t? tr?ng thái ng?. B?t c? khi nào có th? truy c ?p, b?n c?ng c?n xem xét m?t cách k? l??ng.

V?y n?u c?n áp d?ng b?o m?t cho Windows 7, Start menu là m?t cách t?t ?? b?t ??u 'làm v?ng ch?c' m?t cách c? b?n h? th?ng c?a b?n, m? c?a cho các công c? có s?n. Có nhi?u tùy ch?n ? ?ây b?n có th? s? d?ng ?? 'làm v?ng ch ?c' h? th?ng Windows 7 c?a mình, ??c bi?t bên trong Control Panel. S? d?ng Start menu c?ng là cách d? dàng ?? giúp b?n có ???c tuy?n phòng v? cho h? th?ng c?a mình sau khi v?a cài ??t xong. M?t m?o mà b?n có th? th? là thi?t l?p m?t tuy?n phòng v? sau khi cài ??t ban ??u và c?u hình h? th?ng c?a mình, nhi?m v? s? yêu c?u b?n c?u hình t?t c? các tùy ch?n b?o m?t, ?ng d?ng c?ng nh? download các b?n vá l?i và nâng c?p, sau ?ó backup toàn b? h? th?ng v?i System Restore hay ti?n ích t?o ?nh h? th?ng. Gi? ?ây b?n s? có m?t snapshot cho h? th?ng c?a mình trong trang thái fresh ?? ?? phòng khi c?n thi?t có th? chuy?n ??i. Có th? t?o m?t ?i?m khôi ph?c, ?? có th? s? d?ng n?u h? th?ng b? th?a hi?p hay th?m h?a. Chúng tôi s? gi?i thi?u cho các b?n m?t s? tùy ch?n c?a System Restore trong ph?n khôi ph?c th?m h?a c?a lo?t bài này.

L?u ý : Start menu c?ng có th? cung c?p nhi?u thông tin v? tài li?u có liên quan ??n b?o m?t trên h? th?ng. ?ây là m?t ??a ch? h?u d?ng khi tìm ki?m tài li?u ch?ng h?n nh? m?t chính sách b?o m?t,.

B?n có th? 'làm v?ng ch?c' m?t cách nhanh chóng Windows b?ng cách download các công c? và tài li?u tr?c ti?p t? Microsoft. Cho ví d?, n?u mu?n c?u hình m?c b?o m?t c? b?n cho Windows 7, b?n có th? d? dàng download template b?o m?t c? b?n ?? s? d?ng, ch?y nó và có ???c h?u h?t các thi?t l?p b?o m?t ?ã ???c ?i?u ch?nh. Hình 6 cung c?p m?t Windows 7 Security Baseline Settings template v?i các entry ???c chia tab cho vi?c th?m ??nh tài kho?n ng??i dùng, BitLocker và . Tìm hi?u thêm trong ph?n các liên k?t tham chi?u ? cu?i bài ?? t?ng truy c?p vào nó.



Hình 6: C?u hình b?o m?t c? b?n t? các Template c?a Microsoft

L?u ý tùy ch?n 'Security Warning' ? phía trên toolbar (ribbon) c?a Microsoft Office Excel 2007, ?ây là tùy ch?n ng?n ch?n b?n s? d?ng template b?ng cách vô hi?u hóa Macro cho t?i khi b?n chú tâm ??n Security Warning (xem trong hình 6). ? ?ây, Security Macros ?ã b? vô hi?u hóa và ???c yêu c?u cho ?ng d?ng c?a template này. ? ây là m?t ví d? hoàn ho?n cho b?o m?t và s? linh ho?t. ?? có ???c s? linh ho?t trong ví d? này, b?n c?n t?t b? ho? c h?n ch? m?c b?o m?t ???c áp d?ng cho nó. Ch?n th? công tùy ch?n này ?? ch?y, ho?c vô hi?u hóa s? b?o v?, ch ?y Macro sau ?ó nâng m?c b?o m?t m?t l?n n?a ?? gi? b?o m?t ?úng cách s? có ???c cài ??t m?u.

H? th?ng c?a b?n ?ã s?n sàng và b?n ?ã c?u hình m?t s? tính n?ng b?o m?t c? b?n, lúc này b?n nên xem xét cách qu?n lý nó, c?ng nh? ki?m trra s? xâm nh?p, malware và các v?n ?? khác ???c phát hi?n th?y trong các b?n ghi s? ki?n.

L?u ý : B?n nên l?u ý r?ng Windows 7 có m?t tùy ch?n mang tên XP-mode, ?ây là tùy ch?n ???c s? d?ng cho vi? c gi?i quy?t các v?n ?? liên quan ??n s? t??ng thích ?ng d?ng cho các ?ng d?ng XP c?. Nh? nh?ng gì chúng ta ?ã th?o lu?n v? ch? ?? ?o hóa bên trên, khi xem xét vi?c s? d?ng ch? ?? XP-mode, b?n hi?n ?ang cài ??t Virtual PC trên Windows 7 và ch?y m?t instance c?a XP trên Virtual PC. N?u s? d?ng XP-mode, hãy b?o ??m làm v?ng ch? c b?t c? VM nào ?ang ch?y trên các máy ?o theo cách mà b?n làm v?i h? ?i?u hành c? b?n. Các hành ??ng g?m có b?o v? AV, chính sách khóa, gói d?ch v?, nâng c?p ph?n m?m,. B?n có th? cung c?p m?c b?o m?t qua ?o hóa nh?ng m?c b?o m?t ?ó là không hoàn t?t, vì v?y b?n v?n c?n ??n m?t s? b??c 'làm v?ng ch?c', th?m chí n?u ?o hóa ???c s? d?ng.

Conclude

H? th?ng Windows 7 gia ?ình có th? ???c khóa ch?n và qu?n lý m?t cách d? dàng. B?n có th? c?u hình nó m?t cách an toàn ?? ???c truy c?p trên Internet t? m?t v? trí t? xa. Windows 7 có th? ???c trang b? m?t lá ch?n n?u b? n th?c s? mu?n 'làm v?ng ch?c' ?? khóa ch?n hoàn toàn các ?i?m có th? xâm ph?m. Tuy nhiên nó có th? v?n tr? thành ??i t??ng t?n công và ch?c ch?n s? là v?y n?u b?n s? d?ng máy tính trên Internet, m?t ví d? nh? v?y. Do ?ó chúng ta c?n l?p k? ho?ch cho nh?ng kh? n?ng có th? x?y ra và làm v?ng ch?c Windows 7 theo ?ó.

Khi xem xét ??n vi?c s? d?ng Windows 7, trong tình hình các t?n công và khai thác ngày nay, các tùy ch?n b?o m?t và s? linh ho?t là ?u tiên hành ??u cho vi?c t?o quy?t ??nh. Windows 7 r?t an toàn nh?ng không ph?i an toàn

100%. B?n c?n ph?i bi?t áp d?ng ki?n th?c, các công c? khác và các c?u hình nâng cao ?? b?o m?t m?i khía c?nh c?a nó và sau ?ó nâng c?p và ki?m tra chúng m?t cách th??ng xuyên. ?ây là m?t công vi?c r?t quan tr?ng và ?áng giá n?u b?n mu?n tránh t?n công. Thêm vào ?ó Windows 7 c?ng có nhi?u c?i ti?n v? b?o m?t và có th? ???c c?u hình ?? khôi ph?c nhanh chóng.

Các nguyên lý b?o m?t c? b?n ch?ng h?n nh? Defense in Depth ph?i ???c áp d?ng k?t h?p v?i nh?ng h??ng d?n b ?o m?t và các hành ??ng t?t nh?t ?? không ch? áp d?ng cho vi?c b?o v? mà nó còn là nhi?u l?p che ??y toàn b? ki ?n trúc và mã ch??ng trình.

Trong ph?n này chúng ta m?i ch? ??ng ch?m ??n b? m?t trong ph?n này, có r?t nhi?u ki?n th?c khác mà chúng ta c?n ph?i nghiên c?u thêm, tuy nhiên hy v?ng nh?ng thông tin này s? giúp ích cho b?n. ?? tìm hi?u thêm, b?n có th? ??c các liên k?t tham chi?u bên d??i, ?ây là các thông tin chi ti?t v? các công c? mi?n phí, các template và h ??ng d?n. Và không quên theo dõi ?ón ??c ph?n 2 và 3 s? ???c chúng tôi phát hành t?i ?ây.

Các liên k?t tham chi?u

- Windows 7 Security Features
- Windows 7 Security Enhancements
- target=_blankWindows 7 Security TechNet Blog
- target=_blankWindows 7 Security Checklist
- Ten Things IT Professionals Should Know About Windows 7
- Microsoft Malicious Software Removal Tool and Safety Assessment Scan
- Windows 7 System Requirements
- Virtual PC and XP-Mode
- Windows 7 Compatibility Center
- Windows Performance and Hardware Compatibility
- AppLocker
- Download and Install Microsoft Security Essentials for Windows 7
- BitLocker Drive Encryption Step-by-Step Guide for Windows 7
- Windows Trusted Platform Module Management Step-by-Step Guide
- Microsoft Security Compliance Management Toolkit
- Windows Server 2008 Security Compliance Management Toolkit
- Enterprise Security Management with Forefront
- Network Access Protection (NAP)
- Cisco Network Admission Control (NAC)
- Introduction to DNSSEC
- DNSSEC Components and Terminology
- The Trustworthy Computing Security Development Lifecycle (SDL)
- Common Criteria Certification: Microsoft Windows Platform Products
- Responding to IT Security Incidents (Incident Response Planning)
- An Introduction to Kernel Patch Protection
- Data Execution Prevention
- Windows Integrity Mechanism Design
- Understanding and Working in Protected Mode Internet Explorer
- Strategies for Managing Malware Risks
- Security Risk Management Guide and Toolkit
- Security Monitoring and Attack Detection
- Windows 7 and Windows Server 2008 R2: Controlling Communication with the Internet

- Leverage Windows 7 Security in Business Environments
- Windows 7 Security in the Enterprise
- Request for Comments (RFC) Search