HADMÉRNÖK

VII. Évfolyam 2. szám - 2012. június

Baráth Artur
magicman@mail.duf.hu

CRAFTS ON HOW TO USE MICROSOFT WINDOWS 7 IN A SECURE WAY FOR ABSOLUTE USERS

Absztrakt/Abstract

A Windows 7 használata nem kíván nagy kompetenciákat a felhasználóktól. Az viszont, hogy a használatból eredő problémák minimalizálhatóak legyenek, szükséges némi ismeret és rálátás részükről. Jelen cikkemben ehhez próbálok segítséget nyújtani, hisz nem várhatjuk el mindenkitől, hogy rendszergazdai szinten kezelje operációs rendszerét. A cikk elsősorban a biztonságos használatot hivatott segíteni, elsősorban az Absolut User-ek részére, akiknek szakterülete nem terjed ki a számítógép karbantartására és beállításaira, hanem egyszerűen csak használják azt. A biztonsági beállításokról, az alapszintű védekezési mechanizmusokról és praktikus tanácsokról olvashatnak a továbbiakban.

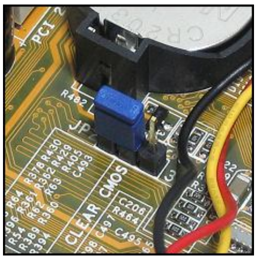
The use of Windows 7 does not require high competences from its users. So that the problems arisen from its use can be minimalized they need to have some ideas and an overview about it. In my present article I am trying to help about this as we can not expect everybody to handle its operational system at administrator level. This article is primarily supposed to help the secure use first of all for Absolute Users whose specialty does not include computer maintenance and computer settings, they are just simply using it. Hereunder you can read about security settings, minimum defense mechanism and some practical advice.

Kulcszsavak/Keywords: *Windows 7, biztonság, virusvédelem, tűzfal konfiguráció, hálózat-kezelés ~ Windows 7, secure, virus protection, firewall configuration, network-management*

1. BEFORE STARTING WINDOWS 7

Windows 7 is one of Microsoft's newest operating system which was developed for home and office use. It was announced first in 2007 but for its arrival we had to wait until the October of 2009. In contrast to the prior editions Windows 7 was not intended to be a revolutionary innovation but an improvement of Vista. Hereafter we are dealing with how to use securely this operation system by Absolute Users.

When we power on a computer a so named BIOS (Basic Input Output System) is being launched. Already at this stage we are allowed to reset a new password for the sake of protecting the computer. Naturally at this point the Windows is not running yet. This sort of security is good for protecting our operation system from unauthorized users and to prevent them doing harm for it. Naturally in spite of this people specialized for this can break it up. Its disadvantage practically is that if someone forgets the password only the deletion of CMOS (Complementary Metal-Oxide Semiconductor) can help about it. Usually on the motherboards there is a for this purpose constructed jumper with the label 'clear CMOS' which can help setting BIOS into original position. About the launching we will talk about the MBR, the boot menu and the F8 menu option. From a security point of view the boot menu is an interesting point as if it is not protected appropriately the booting source can be modified (instead of HDD USB or optical drive) and so someone can circumvent the entering system of Windows or access the full content of our HDD.



After our Windows 7 operation system launched it is key important whether we sign in as a system administrator or as a user. This is of great importance because system changes can be done only with system administrator privileges. In absence of this the system will not allow us making this kind of changes or rather using the system as a restricted user. An account name and a password of a system administrator will be always required. However our system administrator account is hidden and blocked for security reasons. To unlock our system we need to find the 'My computer' icon. We shall make a right click and choose the „Usage" option and then on the left side „Local users and user groups" within which we shall choose the user option. We shall make a double click on the system administrator folder and finally we shall deselect the option „the folder is blocked" and save the changes. This setting can be done also by using a command line. We launch the Run option and write in the CMD command which will pop up a command window. For activation we shall type „net user system administrator / active: yes". For deactivation we shall type the „net user system administrator /active: no" command. Its result is that by signing in our system administrator folder will appear. It is important to know that the before mentioned settings can be done exclusively by system administrator privileges.

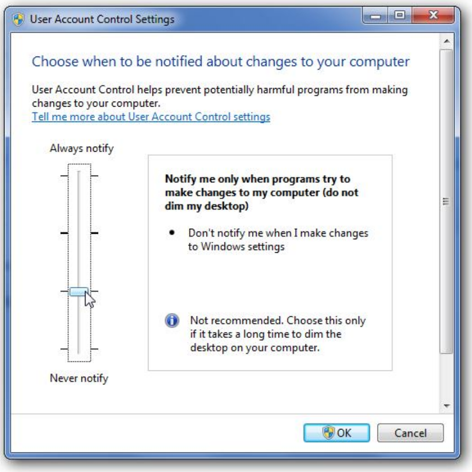
2. THE USER ACCESS CONTROL

The following security point, which everybody has met so far, who uses the Windows 7 operating system, is the so named „User Access Control" (UAC). This is a complex security module which prevents that undesired programs access our system. This setting option can be found under the Control panel / Action center / User access settings menu.

There are four setting options:

1. „Always ask for notification"
2. „Ask for notification only in case a program would like to modify any of the computer settings"

3. „Ask for notification only in case a program would like to modify any of the computer settings (the desktop will not darken in this case)”
4. „Never ask for notification”



User Account Control Settings

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Always notify

Notify me only when programs try to make changes to my computer (do not dim my desktop)

- Don't notify me when I make changes to Windows settings

Not recommended. Choose this only if it takes a long time to dim the desktop on your computer.

Never notify

The first option will always send a warning notification whether we would like to install a new program or would like to make some modifications on the Windows. It is recommended for those who are not aware of the weight and the consequences of the changes. (Absolute Users, Beginners)

The second option (default option) sends no notification only if I modify the Windows settings. This possibility is recommended for those who know how Windows 7 is operating, the consequences of the changes, but often experiment with installing and using of new or unknown programs.

The third option is as a matter of fact identic to the second option with the only difference that this option is recommended for those who have a lower-performance computer. For them the darkening of the screen means a serious waste of time. It is recommended also for those who are simply disturbed by this phenomenon.

The forth option is not recommended by the Windows except the case we would like to install such programs on the computer which are not authenticated for the reason they do not support the user account control.

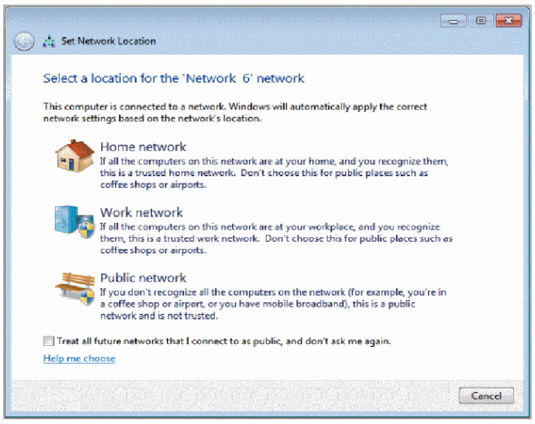
This security point has also its advantages and disadvantages. For example it warns the user when an undesired application is about to launch and make such modifications for which system administrator privileges would be necessary (Windows custom settings – implicitly at system level – can be modified only with system administrator privileges. This notification is valid in this case). It lowers the probability of a virus attack but is not able to make any selections. If a user downloads content from the internet and would like to install it it must be allowed to run as otherwise he/she will not be able to install it. In case one allows this unknown application to run it will not be blocked even if it contained any virus.

Summarized everything UAC is a useful and good advancement. It lowers efficiently the possibility of virus attacks. 80% of all users also apply it.

3. SET THE NETWORK LOCATION

The next protection line in Windows 7 is the *Set Network Locations*. This sort of protection meant a great leap forward regarding the system as by connecting to the network we can block some of the functions. Earlier in the XP series we used to get connected to the internet whether at home or at public location and surf on the net without even suspecting what danger was waiting for us. Here in turn there are three options for us if we would like to connect to the network. Our system makes a distinction among home, office and public network.

Although the under mentioned settings are identified with a location they are not dependent on them. It depends on the network how the connection is qualified. I would like to mention as an example that a home network can also be public if the computer is connected directly to the ISP link. The office Wi-Fi network is also qualified public by default.



Set Network Location

Select a location for the 'Network 6' network

This computer is connected to a network. Windows will automatically apply the correct network settings based on the network's location.

Home network
If all the computers on this network are at your home, and you recognize them, this is a trusted home network. Don't choose this for public places such as coffee shops or airports.

Work network
If all the computers on this network are at your workplace, and you recognize them, this is a trusted work network. Don't choose this for public places such as coffee shops or airports.

Public network
If you don't recognize all the computers on the network (for example, you're in a coffee shop or airport, or you have mobile broadband), this is a public network and is not trusted.

☐ Treat all future networks that I connect to as public, and don't ask me again.

Help me choose

- *Home network* is recommended for those people who stay at home, have incidentally more computers connected to the same network and who send files from one computer to another or maybe play a network game. In this case the so named Network detection function is turned on.
- *Office network* is recommended for those who use their computers at work, are connected to the network and are able to recognize the available networks. The network detection function is on also in this case but it is not possible now to create a home group account or to get connected to it.
- Finally the *Public network* which is worth to be used in public places (for example at cafes, restaurants) or by mobile-based internet connection. By this we can eliminate that an unauthorized person can connect to our computer as this function was developed in a way that our computer can not be visible for the others. The network detection function is off.

When the user selects the appropriate settings it may happen that she/he will not be able to get connected to another computer. It looks to be simple but in order to set a correct and effective security we need to go a bit deeper inside the settings. After we opened the network and sharing center and chose certainly the most appropriate option we shall search the advanced sharing settings. In this menu we can precisely customize our network settings. We can turn on/off the network detection function, can set whether to share our printer through the network and can share our public folder. This is useful because then everybody knows where to store or from where to copy some data. In further we can customize the media processes and provide our shared contents with a code in order unauthorized people can not access them. The experience shows that who knows a bit more about how these systems work will not choose the default settings of the Windows, but will create new ones, which is much more effective as it is set by oneself. Yet in this case we are talking about an Advanced User (AU) of whom we are going to dissert in the following articles.

4. WINDOWS 7 DEFAULT FIREWALL

Windows firewall: this is a software which monitors the network traffic and determines whether to block or to allow that data flow on the computer based on the default firewall size settings.

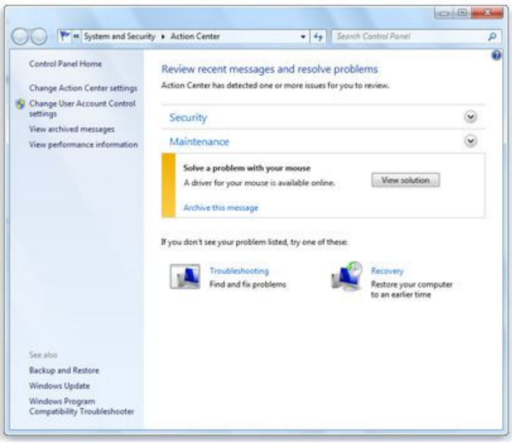
Three types of settings can be done on the firewall general page:

- On: This is the default setting. When the firewall is on most programs are not able to communicate through the firewall. In case we unblock this option we can add the given program to the exception page list. The disadvantage of this function can be the following: if we would like to share a network drive or install a printer it can occur that before we have to modify the firewall settings.
- Blocking connections: This setting blocks all incoming connection attempts towards our computer. This is to protect our computer at the highest possible level for example when we connect to a public network on a train or when a virus is spreading on the internet. By using this setting our firewall will not send any notifications when it blocks certain programs and will not consider even those softwares which are listed on the exception page list. It is important to know that this setting excludes the possibility to operate features on our computer, by the nature of this setting configuration, but this is again the territory of AU-s.
- Off: This option is worth to be used when also another firewall is running on the computer. By turning off the Windows firewall our computer can be endangered by unauthorized people and harmful softwares.

Summarizing all the above Microsoft developed its Windows firewall concerning all the possibilities. However it can happen that it blocks a tool that we would like to use. A (general) user will not know how to add a certain application or tool to the exception list and so will block the firewall. On the other hand the operating system will be right away unprotected this way. It is also doubtful whether an user can recognize that he/she was actually blocked by the firewall because our firewall will not send him/her any notification like „Yes, I blocked him/her.” For this reason it is worth to read after this before making any modifications about the settings.

6. OTHER SUPPORTERS

Action center: this is an application which collects the alerts coming from the main maintenance and security features of the Windows. If our Windows would like to warn us about something for example error reporting, Defender feature, user account control, than the action center link will appear on the taskbar. By clicking on that icon proposed warnings and solutions will be displayed.



Review recent messages and resolve problems

Action Center has detected one or more issues for you to review.

Solve a problem with your mouse

A driver for your mouse is available online.

If you don't see your problem listed, try one of these:

Troubleshooting: Find and fix problems

Recovery: Restore your computer to an earlier time

The action center draws up a list of the important messages about security and maintenance settings. Its red color elements marketed important mean high importance problems which need to be handled in short time for example if our virus killer expired. Handling of the yellow color elements is to be considered.

To open the action center we shall click on the start button, then on the control panel command and after this on the element ’Check the computer status’ on the system and security page.

If you move your mouse on the action center icon located on the right side of the taskbar at the notification part of you will see whether new messages arrived or not. To see further details about security or maintenance attributes for example please click on this icon. To deal with problems please click on the appropriate message. If you would like to see the full message please open the message center.

Backup and restore. In the Windows 7 system there is an advanced ’Backup and restore’ feature which makes a copy of our set personal files in order we can always be prepared for the worst. Windows is able to follow any kind of scheduling which can be set as per our own request. The copies can be stored on another drive (Microsoft does not recommend to use its own drive) or rather on a DVD disk. By using its Professional or Ultimate editions backups can be created even on the network. Its usage is very simple as by creating them a wizard will appear and ask about all variations. The backup and restore can be found at Start then Control panel then after on the System and security page at the Backup and restore command. It is advisable to set some schedules by the task scheduler and save what is necessary.

Updating the Windows 7 system (Windows update). Installing the updates is maybe one of the most important things. Windows Update downloads the newest updates through the internet from the Microsoft webpage in order our protection lines (the main part of the updates are to ensure secure operation) are always up-to-date. In the Windows 7 system Windows update is already part of the action center. Updating is important for two things. First case: the first published series contains some errors and the updates correct these errors. Second case: In case of a system attack as not only Microsoft is developing its softwares. Simultaneously hackers are working for the purpose to break up its system and steal very important data but by updating our Windows continuously we can feel ourselves more secure. There is one very important thing to know though. Microsoft supports its editions only till a certain date of time. In this case it means that for Windows 7 the newest updates are ensured to be available until January 2015, not later. This is negative from the point of view that users need to buy a newer version so as to feel secure again. What is to be considered is that after making an update the computer might have to be restarted in order updates can be finalized. After updating at first restart it can happen that updates are configured for long time by the Windows but this is normal.

As summary Windows 7 has become a very reliable system, it is very user friendly, lots of its setting options are simplified which makes this system easily configurable even for an absolute user (naturally to a given level). In terms of compatibility it is advanced (comparing it to the XP for example) and is relatively stable. It has some errors though by the way, but it is worth to be used even with these together and if someone knows a bit more about it then can avoid them. In my next publication I am going to dissert also about these.

References

[1] Gál Tamás (2010.): Microsoft Windows Server 2008 R2 A kihívás állandó

[2] Joan Peppernau - Joyce Cox (2009.): Windows 7 lépésről lépésre

[3] Bártfai Barnabás (2009.): Windows 7 Zsebkönyv

[4] Wikipedia

All pictures are adding the author