Доцент д-р Сашо Гелев
Универзитет „Гоце Делчев„ Штип,
Електротехнички факултет;

Вон. проф. д-р Ристо Христов
Европски универзитет, Скопје
Факултет за информатика;

Ана Ивановска

БЕЗБЕДНОСТ ВО WINDOWS 7

Абстракт: Во секој оперативен систем на Windows па и во Windows 7 големо внимание се посветува на усовршување на безбедноста, подобрување на интерфејсот, пократки и поедноставени чекори за менаџирање на содржини и.т.н. Во овој труд ќе се задржиме на безбедноста која е применета во Windows 7 оперативниот систем со цел да се увидат добрите и лошите страни. Ќе го објасниме Windows 7 Action Center, Windows Firewall и Microsoft Security Essentials. Скоро секоја година компјутерските оперативни системи се обновуваат и надградуваат. Новите технологии, новите апликации носат нови закани, и принудени сме на нови механизми за заштита и одржување на оперативните системи.

Abstract: in every Windows operative system including Windows 7 significant attention is dedicated to improvement of security, advancement of the interface, shorter and simpler steps for managing of the contents and etc. In this paper we are going to hold on to the security that is implemented in Windows 7 operative system with an aim to understand its advantages and disadvantages. We are going to describe Windows 7 Action Center, Windows Firewall and Microsoft Security Essentials. Almost every year the computer operative systems are renewed and upgraded. The new technologies and new applications lead to new treats and we are forced to implement new mechanisms for protection and maintenance of the operative systems.

Клучни зборови: Windows 7 Action Center, Windows Firewall, Microsoft Security Essentials

1. Вовед

Windows оперативниот систем е производ на корпорацијата Microsoft. Се проценува дека Windows оперативниот систем е дојден до степен на доминација во светот на персоналните компјутери до околу 90% од светскиот пазар на оперативни системи.

По стапките како и Windows XP кој има повеќе верзии, Windows 7 доаѓа во шест верзии и тоа: **Windows 7 Starter**. **Windows 7 Home Basic, Windows 7**

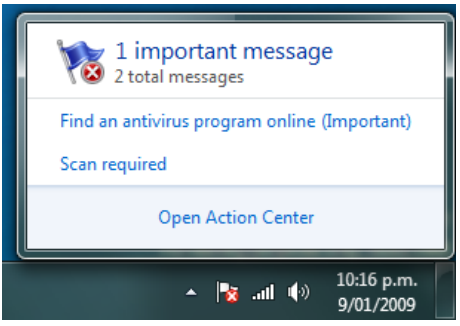
Home Premium, Windows 7 Professional, Windows 7 Enterprise и Windows 7 Ultimate

Основно заедничко за сите верзии на Windows 7 прави да програмата и програмирањето на драјверите на уредите се реализираат многу полесно бидејќи драјверите од уредите и софтверските програми треба да бидат создадени само еднаш, не двапати.

Во секој оперативен систем на Windows па и во Windows 7 големо внимание се посветува на усовршување на безбедноста. Овде ќе го објасниме Windows 7 Action Center, Windows Firewall и Microsoft Security Essentials кои покрај другото се грижат за безбедноста на компјутерскиот систем.

2. Windows 7 Action Center

Windows 7 Action Center е место каде што можете да најдете информации за одржување на системот, сигурносни информации и размена на компјутерски проблеми ако ги има. Мајкрософт го има реформирано XP и Vista Security Center во повеќе корисен и информативен Action Center. Action Center-от ги известува корисниците кога има некоја важна порака (апдејтирање, решавање на некој проблем, побарување на антивирусна програма, барање на бекап на одреден период, и.т.н.), така што корисниците ќе можат да превземат соодветни мерки.



Слика 1. Известување од Action Center.

Известувањата до корисниците доаѓаат во вид на балон порака. Пример за известување е прикажан на слика 1. Која и да било порака која од страна на Action Center-от ќе ве предупреди е важна за безбедноста и одржувањето на вашиот систем. Ако се случи да не ја забележите или ја игнорирате балон пораката, со проблемот можете да се справите подоцна со помош преку знаменцето кое се наоѓа во icon tray. Ако сите барања од Action Center-от се задоволени тогаш знаменцето изгледа како на слика 2. Кога не се обавени сите барања од Action Center-от знаменцето изгледа како на слика 3.

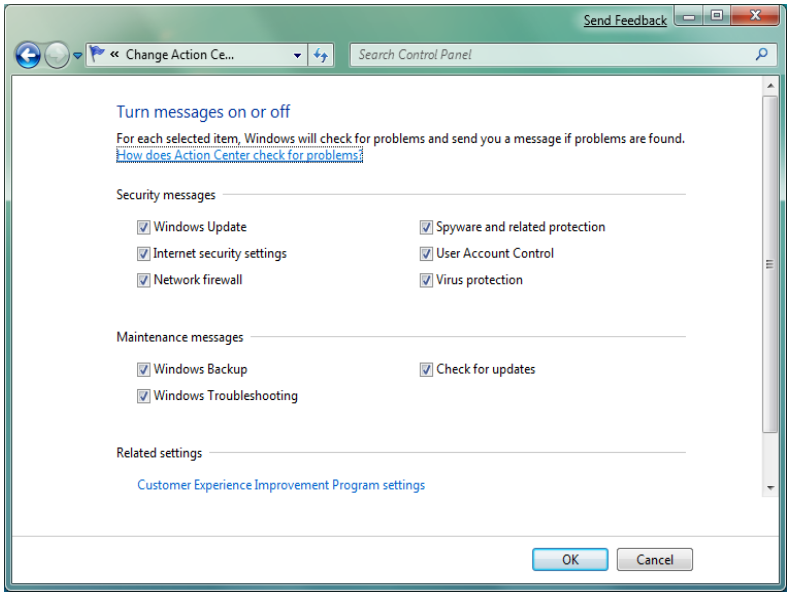
Слика 2. Знаменце без побарувања.

Слика 3. Знаменце со побарувања

Некои корисници пораките можат да ги чувствуваат како досадни и преферираат известувањата да бидат исклучени. Опции кои можете да ги користите за конфигурација на Action Center за добивање на известувања се прикажани на слика 4.

Action Center е составен од две подкатегории:

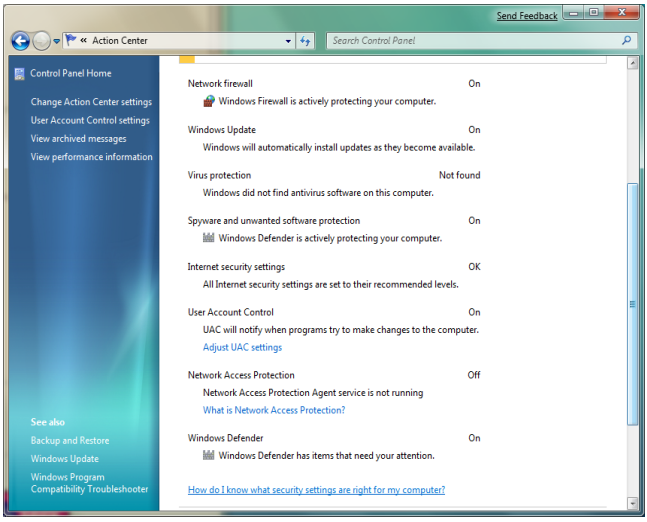
1. Безбедност- Security
2. Одржување- Maintenance (не е предмет на разгледување)



Слика 4. Конфигурација на Action Center за добивање на известувања.

2.1. Action Center–Security (Безбедност)

Во овој дел на корисниците им се претставуваат сите потребни информации за безбедноста, проблемите и можностите за решавање на проблеми. Изгледот на делот Security во Action Center-от е прикажан на слика 5.



Слика 5. Security.

Ова е слично на Виста центарот за безбедност со речиси исти можности и сличен интерфејс, а со различен интерфејс од центарот за безбедност на Windows XP. Во Action Center-от безбедноста односно делот Security се состои од неколку подкатегории и тоа:

- Network Firewall-Во компјутерската технологија firewall е хардверска направа со претходно инсталиран софтвер кој што функционира во мрежни околини и служи да спречи различни видови на комуницирања во мрежите кој се забранети од полисите.
- Windows Update-Карактеристично за Windows Update е да не известува за најновите апдејти и баг фајлови за Windows 7 оперативниот систем и директно да ги преземаме од официјалната веб страната на Microsoft.
- Virus Protection-Virus Protection е дел кој се грижи да имаме антивирусен софтвер кој ќе се грижи против вирусите.
- Spyware and unwanted software protection-Во делот Spyware and unwanted software protection од самата инсталација на Windows 7 постои инсталиран софтвер наречен Windows Defender кој служи за заштита од малициозен софтвер, а може корисникот и сам да инсталира софтвер по свој избор.
- Internet security settings-Во овој дел се поставуваа сите интернет мерки за безбедност кои се сетираат по левели.
- User Account Control- UAC ќе не извести преку нотификација кога некоја програма ќе сака да изврши некоја измена на системот.
- Network Access Protection- NAP е мрежна платформа на администраторот која може да ни помогне во заштита на мрежите.

3. Windows Firewall

Во Windows 7, Мајкрософт ви нуди можност да управувате со Windows Firewall на неколку различни начини. Можете да управувате со основната функционалност на firewall-от со помош на Windows Firewall во Control Panel, и напредна функционалност на користење на заштитен Windows Firewall преку напредна безбедносна конзола (Advanced Security console).

Сегашната верзија на Windows Firewall во Windows 7 нуди добри карактеристики како што се:

- Филтрирање на IPv6 конекција (ви овозможува да го користите IPv6 протокол на безбеден начин.).
- Филтрирање на влезни и излезни пакети(Firewall правилата за влезни и излезни филтрирани пакети го сочинуваат мнозинството напредни конфигурации на вашиот firewall. Овие правила определуваат како протокот на мрежата за сообраќај се контролира преку вашиот компјутер. Вие управувате со протокот на влезен и излезен сообраќај во текот на овие правила.
- Напредно филтрирање на пакети (овозможува да креирате правила поврзани со повеќе IP адреси. Оваа опција ви дава поголема флексибилност во менаџирањето со конекциите за користење на извор или дестинација на IP адреса).
- IPSec интеграција(IPSec интеграција ви овозможува да управувате конекции со користење на енкрипција).
- Енкрипциско барање.
- Конзола за менаџирање (MMC) (Ова ви овозможува да управувате со различни типови на врски и правила преку еден интерфејс. Администраторите може лесно да управуваат со Windows Firewall врските и да ги здружуваат со поставките на Group Policy).

Заедно овие функции нудат големи подобрувања во текот на Windows Firewall кој беше прво воведен во Windows XP. Овие карактеристики исто така помагаат за олеснување на потребата да не го исклучите Windows Firewall, како што некогаш мораше од самиот почеток да го исклучите вашиот firewall.

3.1. Конфигурирање на основен Windows Firewall

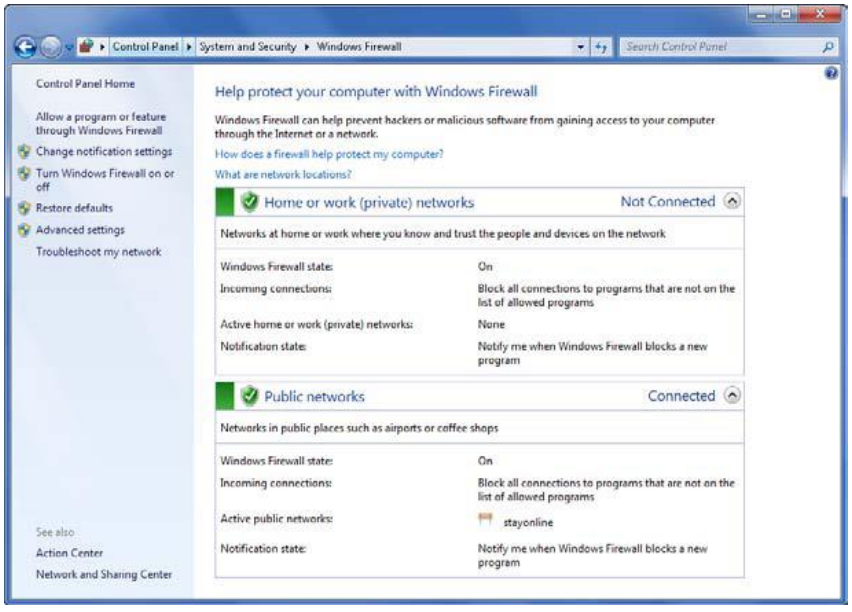
Основното суштинско значење за Windows Firewall е предвидување на безбедноста на вашиот компјутер. Со користењето на основниот firewall за заштита на вашиот компјутер, ќе се заштитите од многу видови на напади. Во Control Panel, можете да ја конфигурирате основната конфигурација на

firewall-от со кликнување на System and Security и потоа кликнете на Windows Firewall. Како што е прикажано на слика 6, главната страница на Windows Firewall дава преглед на конфигурација на firewall-от и статус. Овие информации се користат за да утврдите дали вашиот firewall е вклучен или не е вклучен, без разлика дали известувањата се прикажани кога програмот е блокиран и на кој тип на мрежа сте поврзани во моментот. Типот на мрежата ни открива тип на firewall профил кој моментално се применува. Постојат повеќе провили за конфигурирање на Windows Firewall и тоа:

- Домашна или работна (приватна) мрежа.
- Јавна мрежа.
- Domain мрежа.

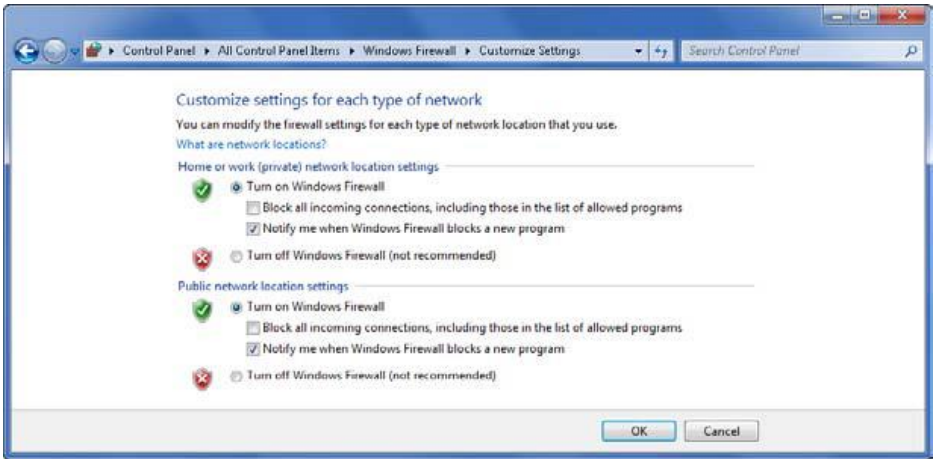
Во левиот панел постојат повеќе линкови за подесување на некои дополнителни опции и тоа:

- Дозволете програма или функција преку Windows Firewall.
- Промена на подесувањата за известување.
- Windows Firewall вклучете или исклучите.
- Враќање во стандардна форма (Restore defaults).
- Напредни поставувања.



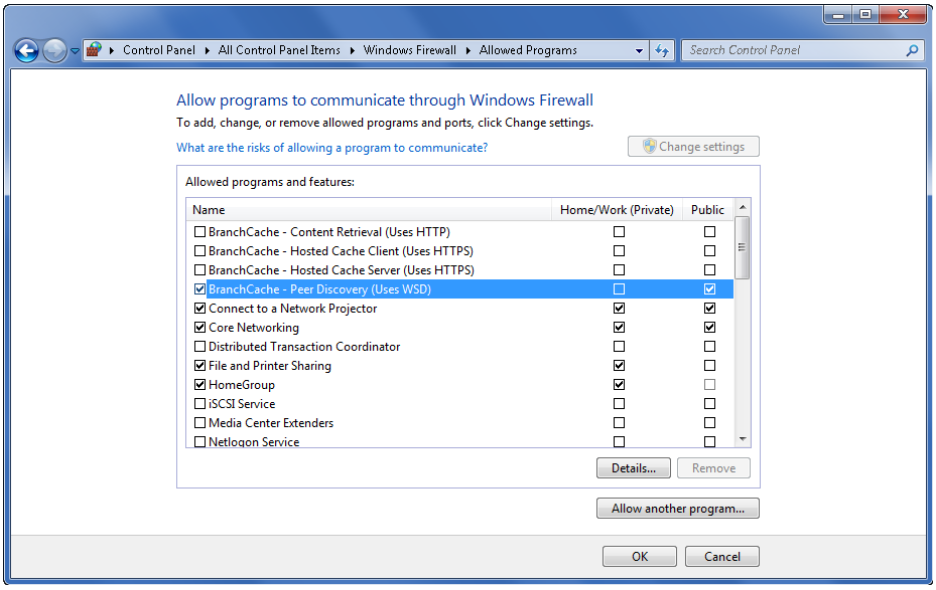
Слика 6. Преглед на статусот на Windows Firewall.

Со кликнување на "Change notification settings" или "Turn Windows Firewall on or off" се отвора Customize Settings страница. Можете да ги користите опциите во делот за персонализација на поставувањата на firewall-от да го вклучите или исклучите (слика 7) за секој профил посебно. За да го вклучите firewall-от кликнете на "Turn on Windows Firewall". Оваа опција овозможува firewall-от да ги блокира дојдовните конекции кои можат да имаат штетно влијание брз вашиот компјутер. За да го исклучите firewall-от кликнете на "Turn off Windows Firewall (не е препорачливо)". Оваа поставка служи за исклучување на firewall-от и го прави вашиот компјутер ранлив од несакани напади преку мрежата и интернет врските.



Слика 7. Вклучување или исклучување на firewall-от.

Кога сте конектирани на мрежа која е помалку сигурна, може да посакате да го вклучите вашиот firewall и да ги блокира сите дојдовдни конекции на вашиот компјутер. За да го направите тоа изберете "Turn on Windows Firewall" и кај опција “Block all incoming connections...” чекирајте го квадратчето. Оваа поставка ги игнорира сите подесувања во конфигурација на firewall-от и ја блокира секоја конекција со вашиот компјутер. Можете да ги исклучите известувањата со чекирање на квадратчето до "Notify me when Windows Firewall blocks a new program". Назад на Windows Firewall главната страница, кликнете "Allow a program or feature through Windows Firewall" се отвора листа со програми на кои имате чекирано дозвола. Оваа страница е прикажана на слика 8 и ви овозможува да контролирате како програмите ќе комуницираат со Windows Firewall-от. Многу компоненти на Windows често се користат за поврзување но има исклучоци наведени во програми или некој порт листи. По стандард (default), можете да го видите конфигурираните исклучоци но не може да правите измени. За да ги промените подесувањата, кликнете на “Change Settings”.



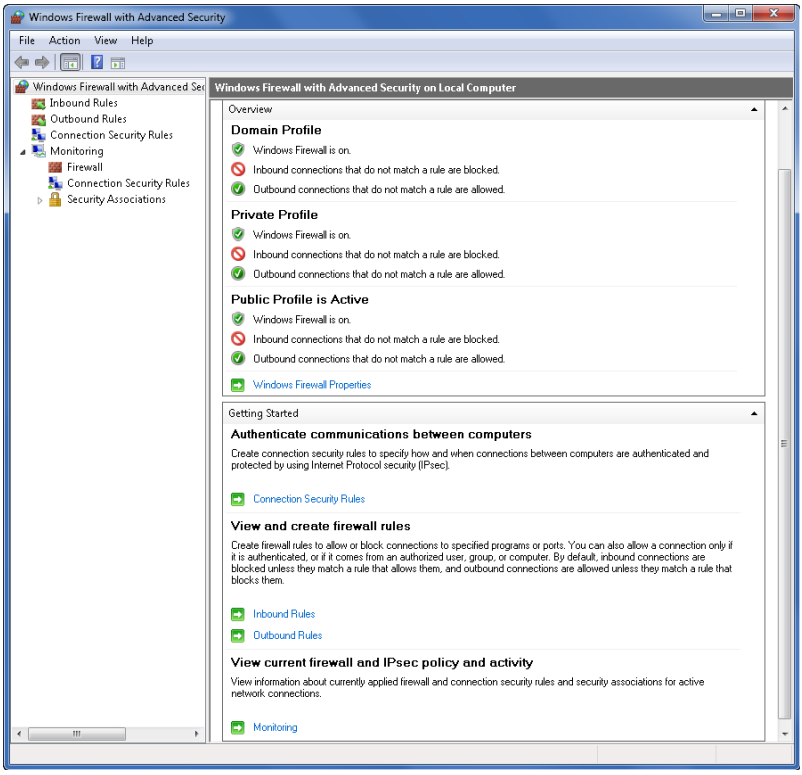
Слика 8. Конфигурација на исклучоци во firewall-от.

Може да се овозможи исклучок за програма со чекирање на квадратчето и потоа изборот на профили на кој треба да биде исклучокот. По стандард (default), квадратчето за чекирање е чекирано за активниот профил. За да го исклучите исклучок за профилот, отчекирајте го квадратчето кое се наоѓа во полето на профилот. За да го исклучите исклучокот целосно отчекирајте го квадратчето кое се наоѓа лево одма до името на програмата или отчекирајте ги сите исклучоците кои се наоѓаат во полето на секој профил. За да дознаете повеќе за исклучоците на Windows компонентите изберете еден исклучок за кој сте заентереситани и прво кликнете на него а потоа притиснете детали (Details). Со користење на "Allow another program" копчето можете да додадете нови програми во листата за исклучоци кои ќе ви даваат поголема контрола над безбедноста на вашите компјутерски параметри. Можете трајно да го отстраните секој исклучок со кликнување на исклучокот, а потоа притиснете отстрани (Remove). Со кликнување на “Restore defaults” ви се овозможува да ги избришете сите Windows Firewall подесувања кои пред тоа ги имате конфигурирано за сите ваши мрежни профили. Иако ова може да предизвика некои програми да престанат да работат, вашиот Windows Firewall ќе го ресетирате и ќе го доведете до неговата оригинална почетна конфигурација.

3.2. Конфигурирање на напреден Windows Firewall

Покрај основниот Windows Firewall, Windows 7 во себе вклучува Windows Firewall со напредно конфигурирање. За домашна употреба најверојатно нема да работите со напреден firewall, но за корисници кои имаат потреба и

знаат да подесуваат firewall со напредни подесувања ќе го користат. Прозорецот “Advanced Security” за конфигурирање е прикажан на слика 9.



Слика 9. Конфигурација на firewall-от со напредни поставувања.

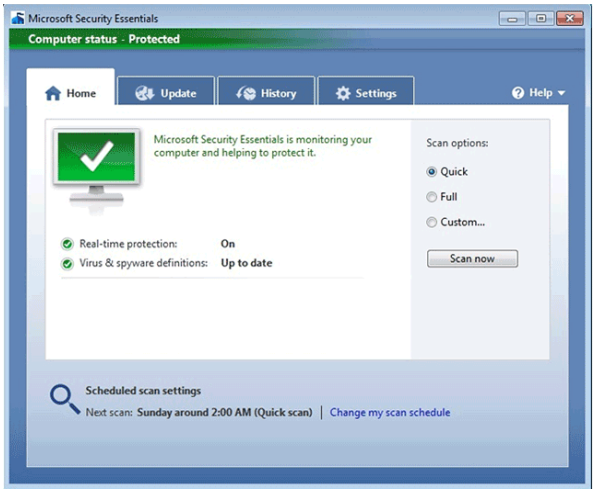
Windows Firewall со напредна безбедност одржува посебен firewall профил за секој тип на мрежа на која можете да се поврзете. За секој профил можете да управувате со поставки за firewall-профилот, влезни конекции, излезни конекции, известувања, unicast одговор, и логирање. Како што е прикажано во табела 3, стандардна конфигурација за сите поставувања е иста за секој профил.

Поставувања	**Домеин профил**	**Приватен профил**	**Јавен профил**
Firewall State	Вклучено	Вклучено	Вклучено
Влезни конекции	Блокирано	Блокирано	Блокирано
Излезни конекции	Овозможено	Овозможено	Овозможено

Известување	Да	Да	Да
Уникаст одговор	Да	Да	Да
Пријавување на отфрлени пакети	Не	Не	Не
Пријавување на успешна конекција	Не	Не	Не

Табела 1. Стандардна конфигурација за Windows Firewall профилите со напредна безбедност.

4. Microsoft Security Essentials



Слика 10. **Microsoft Security Essentials.**

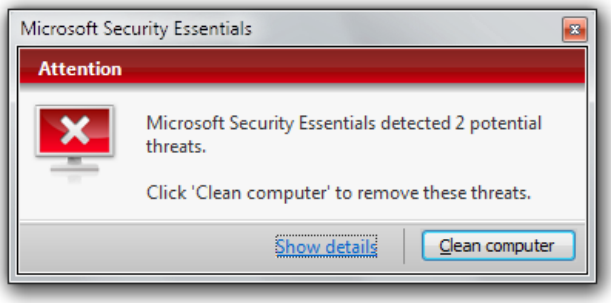
Microsoft Security Essentials (MSE) е бесплатен антивирусен софтвер основан од страна на Мајкрософт кој обезбедува заштита од вируси, spyware, rootkits и тројанци, а е изработен за Windows XP, Windows Vista (x86 и x64), како и за Windows 7 (x86 и x64).

MSE е дизајниран за сопствена безбедност на потрошувачите. Таа се базира на Forefront Client Security десктоп агент, но и нуди заштита од малициозен софтвер, детекција и отстранување со централизиран менаџмент на функции. Тоа вклучува некоја Anti-Malware алатка (наречена "Microsoft Malware Protection Engine", или кратенка MSMPENG), вирусни дефиниции од сите Microsoft други десктопи кои имаат опција за споделување, вклучувајќи Forefront Client Security, Windows Live OneCare, и Windows Defender

(исклучува антивирусни дефиниции кои се одвоени од антиспајвер дефинициите). Пред инсталацијата MSE прави проверка на валидноста на инсталираната копија на Windows-от. MSE не бара регистрација или лични информации. MSE ќе го исклучи Windows Defender, поради што предвидува заштита од малициозен софтвер кај кој не е ограничен на spyware и adware.

Ажурирањата на апдејтите се објавени три пати на ден на Microsoft Update.

Поп-ап известувањето се појавува кога малициозниот софтвер ќе биде пронајден (слика 11). Инсталацината на MSE е едноставна, брзото скенирање после инсталација е околу 10 минути, а целосно скенирање е околу 45 минути после инсталација на Windows 7.



Слика 11. Известување.

За време на скенирање MSE наоѓаат 89 проценти од примероците на малициозен софтвер, наоѓа 67 проценти од rootkits, а во меѓувреме при пронаоѓањето на малициозниот софтвер и блокира дел од него.

4.1. Безбедносни мерки

Обезбедување на вашиот компјутер: четири Essential чекори:

1. Вашиот firewall-от да е вклучен
2. Вашиот Windows секогаш да е апдејтиран навреме.
3. Користете антивирусна програма.
4. Користете антиспајвер програм. Windows Defender, која е вклучена со Windows 7 и служи добро за оваа функција.

Action центарот ги следи секоја од овие четири области со кои би постигнале подобра безбедност, а ако нешто недостасува Action центарот ќе ве извести. Покрај овие неколку Essential чекори важно е да научиме да избегнуваме инсталација на софтвер кај кој постои потенцијален ризик. Сепак не може со ништо да се спречи инсталирање на малициозен софтвер од страна на корисникот, само со исклучок на воздржаност.

5. ЗАКЛУЧОК

Кога за прв пат ќе се сретнете со оперативниот систем Windows 7 на прв поглед ќе ви изгледа сложен за работа. Windows 7 за разлика од Windows XP е многу подобар. Windows 7 е збогатениот интерфејс кој користи аеро теми. Апликациите и сервисите кои постојат во Windows XP, постојат и во Windows 7 само што тука се повеќе и се надоградени.

Windows 7 Action Centar во Windows 7 е поделен на две подкатегории: безбедност и одржување.

Firewall припаѓа во подкатегоријата на безбедност. Kaj Firewall-от во Windows 7 се подобрени повеќе особини со што се зголемува безбедноста. Во овој сервис може да конфигурираме заштитен sид со напредни поставувања, во кој се вклучуваат многу методи на заштита.

Апликација која е многу корисна и има улога да го заштитува системот од малициозен софтвер е Microsoft Security Essentials. MSE припаѓа во подкатегоријата на безбедност.

Денес во светот се користат многу уреди кои се поврзани на интернет па затоа и расте побарувањето на IP адреси, а со IPv6 протоколот се решава овој проблем. Иднината не можеме да ја предвидиме, бидејќи од ден на ден потребите на корисниците за IP адреси е се поголем. Ни преостанува само да чекаме и да се прилагодуваме на новото време што следи со новата технологија.

6. БИБЛИОГРАФИЈА

1. Авторизирани предавања по предметот Проектирање на компјутерски мрежи, доц. д-р Сашо Гелев, 2009/2010.
2. Сашо Гелев, Оперативни системи, ЕУРМ, Скопје 2010.
3. Greg Harvey , “Windows® 7 For Dummies® Quick Reference”, ISBN: 978-0-470-48961-1.
4. Ed Bott, Carl Siechert, and Craig Stinson, Windows 7 Inside Out (10-2009), Library of Congress Control Number: 2009932321.
5. Nancy Muir, “Windows 7 Just the Steps for Dummies (2009)”, ISBN: 978-0-470-49981-8.
6. Rich Robinson, “Windows 7 – The Pocket Guide v 1.0 2009”.
7. Paul Thurrott,Rafael Rivera, “Windows 7 Secrets”, ISBN: 978-0-470-50841-1.
8. William R. Stanek, Windows 7 The Definitive Guide (Oct.2009), ISBN: 978-0-596-80097-0.
9. Robert Cowart and Brian Knittel, “Microsoft Windows 7 In Depth”, First Printing: September 2009, ISBN-13: 978-0-7897-4199-8, ISBN-10: 0-7897-4199-7.