CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnost operacijskog sustava Windows 7

NCERT-PUBDOC-2009-12-286

Nacionalni CERT

u suradnji s

LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem Nacionalni CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom Nacionalnog CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

Nacionalni CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. UVOD 4

2. POVIJESNI RAZVOJ OPERACIJSKIH SUSTAVA WINDOWS 5

2.1. DOS JEZGRA 5

2.1.1. Windows 1.0 5

2.1.2. Windows 2.0 5

2.1.3. Windows 3.0 i Windows 3.1 6

2.1.4. Windows 95 6

2.1.5. Windows 98 6

2.1.6. Windows ME 7

2.2. NT JEZGRA 7

2.2.1. Windows NT 3.1 7

2.2.2. Windows NT 4.0 7

2.2.3. Windows 2000 7

2.2.4. Windows XP 7

2.2.5. Windows Vista 8

2.3. PREGLED SIGURNOSNIH NEDOSTATAKA PRIJAŠNJIH INAČICA 10

3. NOVOSTI U SUSTAVU WINDOWS 7 15

3.1. INSTALACIJA 15

3.2. POBOLJŠANE PERFORMANSE 15

3.3. PROMJENE U IZGLEDU SUČELJA 16

3.4. POBOLJŠANO UPRAVLJANJE NAPAJANJEM 17

3.5. WINDOWS DODIRNA TEHNOLOGIJA 17

3.6. WINDOWS MEDIA CENTAR 17

3.7. VIRTUALNI XP 17

4. SIGURNOST OPERACIJSKOG SUSTAVA WINDOWS 7 18

4.1. SIGURNOSNI ELEMENTI 18

4.1.1. Action Center 18

4.1.2. Vatrozid 20

4.1.3. BitLocker i BitLocker To Go 21

4.1.4. AppLocker, Microsoft Security Essentials 22

4.1.5. Osnovna grupa 22

4.1.6. Biometrija 23

4.2. PRONAĐENE RANJIVOSTI 23

4.2.1. Propust u protokolu za dijeljenje datoteka Server Message Block 23

4.2.2. Propust u User Account Control sigurnosnom mehanizmu 23

5. USPOREDBA S DRUGIM OPERACIJSKIM SUSTAVIMA 24

5.1. MAC OS X 10.6 – SNOW LEOPARD 24

5.2. UBUNTU 9.10 – KARMIC KOALA 25

6. ZAKLJUČAK 27

7. REFERENCE 28

1. Uvod

Samo dvije godine nakon izdavanja Windows Viste (2007.g.) , Microsoft je izdao novi operacijski sustav naziva Windows 7. Ispitivanje Windowsa 7 trajalo je više od godine dana, a Microsoft je vrlo ozbiljno uzimao u obzir sve kritike upućene prethodnoj inačici OS-a. Windows 7 je u odnosu na Vistu nešto brzi, zauzima manje memorije, stabilniji je i pokazuje bolje performanse. Kao što je to bila tendencija i u prijašnjim inačicama, na vrhu liste prioriteta opet se našlo povećanje sigurnosti. Velika pažnja posvećena je zaštiti jezgre operacijskog sustava, izdana je nova inačica Internet Explorera (IE8), sigurnosni centar unaprijeđen je u Action center koji nadgleda cijeli operacijski sustav uključujući i sigurnost te su unaprijeđeni brojni sigurnosni alati kao User Account Control, Windows Firewall i Windows Defender. Pomoću ovih unaprjeđenja broj potencijalnih vrsta napada koji se mogu izvesti na ovoj inačici smanjen je u odnosu na prijašnje inačice. Stoga, nije teško povjerovati riječima Microsofta da je Windows 7 trenutno najsigurnija inačica Windowsa na tržištu. Iako je Windows 7 tek nekoliko mjeseci na tržištu, kritika mu je vrlo naklona, a čini se i korisnici. Prema izvješću Microsofta, prodaja operacijskog sustava Windows 7 je u konstantnom porastu.

U dokumentu će biti opisan povijesni pregled operacijskih sustava Windows te sigurnost prijašnjih inačica. Zatim, popisani su i opisani noviteti koje Windows 7 donosi, s naglaskom na sigurnost. Na kraju je dana usporedba Windowsa 7 s druga dva operacijska sustava koja zauzimaju značajan udio tržišta: Mac 10.6 – Snow Leopard i Ubuntu 9.10 – Karmic Koala.

2. Povijesni razvoj operacijskih sustava Windows

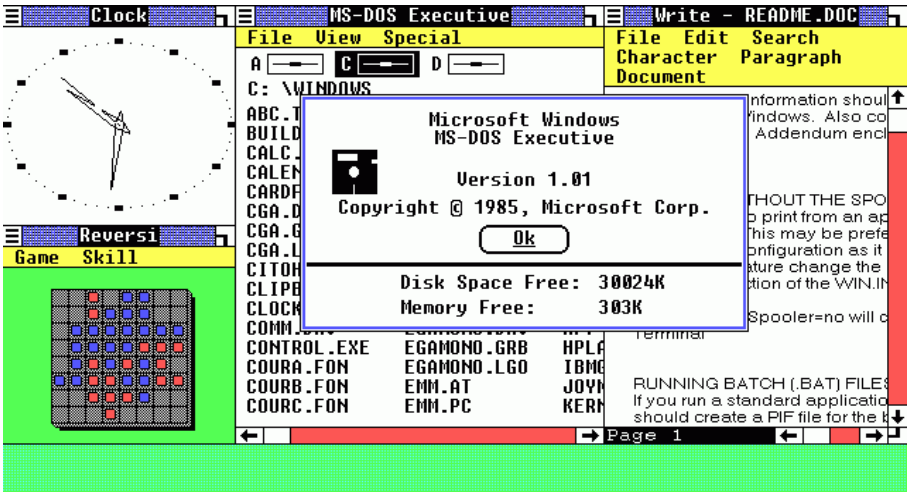
Davne 1983. godine Microsoft je najavio razvoj Windowsa kao grafičko korisničko sučelje (*eng. Graphical User Interface GUI*) za svoj operacijski sustav MS-DOS (*eng. Microsoft Disk Operating System*) kojeg je isporučivao na IBM PC računalima. S vremenom Windows, zbog svoje velike popularnosti, prerasta u operacijski sustav. Paralelno se razvijaju dvije osnovne grane koje koriste različite tehnologije:

- DOS jezgra i
- NT jezgra

2.1. DOS jezgra

2.1.1. Windows 1.0

Prva samostalna inačica sustava Windows, inačica 1.0, objavljena je 1985. godine. Izvorno se trebala zvati „Interface Manager", ali Rowland Hanson (voditelj marketinga u Microsoftu) je uspio uvjeriti vodstvo tvrtke kako će naziv Windows biti puno privlačniji potrošačima. Inačicom Windows 1.0 predstavljeno je novo programsko okruženje za razvoj i pokretanje aplikacija korištenjem ikona i pokazivača. Prije pojave Windowsa, korisnici osobnih računala radili su isključivo u linijsko naredbenom načinu rada (eng. command line). Proizvod je uključivao kalendar, uređivač teksta (Notepad), kalkulator, sat, upravljačku ploču (Control Panel) te alate za crtanje (Paint) i pisanje (Write) čija je zadaća bila pomagati korisniku u izvođenju dnevnih zadataka. Jedan od zanimljivih detalja ovog operacijskog sustava bili su prozori koji se nisu mogli preklapati, jedino su mogli biti posloženi jedan do drugog. Samo prozor koji prikazuje sistemske informacije (eng. dialog box) se mogao pojaviti „preko" ostalih prozora. Slika 1. prikazuje grafičko sučelje Windowsa 1.0. Inačica Windows 1.0 nije postigla veliku popularnost.



Slika 1: Grafičko sučelje Windows 1.0.

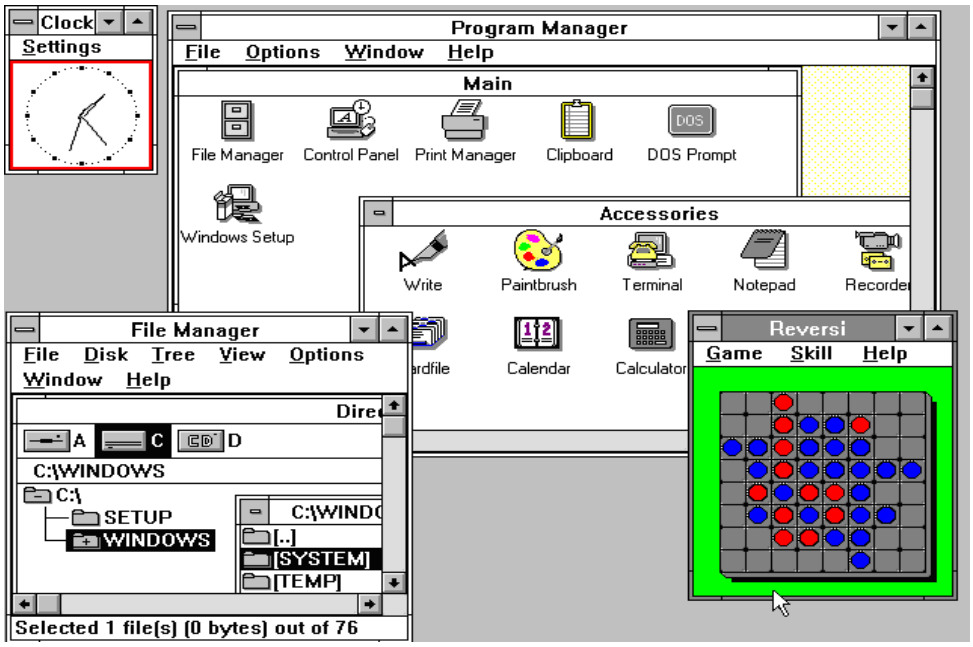
Izvor: Google

2.1.2. Windows 2.0

1987. godine predstavljen je Windows 2.0 kojeg je pokretao procesor Intel 286 s proširenom memorijom i boljom podrškom za grafiku. U ovoj inačici prvi puta se javlja napredni mehanizam kratica pomoću tipki tipkovnice, terminologija „Minimize" i „Maximize" (do tada su se koristili termini „Iconize" i „Zoom") te je omogućeno preklapanje prozora. Prve inačice Microsoft Word-a i Microsoft Excel-a počele su se upotrebljavati na Windows 2.0. Iako je Windows 2.0 bio popularniji od Windowsa 1.0 još uvijek nije bio masovno korišten. Stoga je većina proizvođača i dalje izrađivala DOS inačice svojih aplikacija.

2.1.3. Windows 3.0 i Windows 3.1

Inačicama Windows 3.0 (1990 g.) i Windows 3.1 (1992. g.) znatno se unaprijedilo korisničko sučelje te su se uvela brojna tehnička poboljšanja kako bi se što bolje iskoristile memorijske mogućnosti procesora Intel 286 i 386. Korisnicima je omogućeno korištenje miša kojim se moglo upravljati podacima jednom rukom bez pamćenja naredbi MS-DOS-a te pokretanje više aplikacija u isto vrijeme (*eng. multitasking*). Slika 2. prikazuje korisničko sučelje inačice Windows 3.0. 1991. godine objavljene su ekstenzije za multimediju koje su omogućavale podršku za CD-ROM i zvučnu karticu. 1993. godine predstavljena je inačica Windows for Workgroups 3.11 koja je donijela podršku za umrežavanje i kućno povezivanje računala u mreže. Ovom inačicom osobna računala postaju dio klijent-poslužitelj računalne evolucije u nastajanju. Instalacija za Windows 3.11 nalazila se na devet disketa, a ukupna veličina instalacije iznosila je manje od 13 MB.



Slika 2: Grafičko sučelje Windows 3.0

Izvor: Google

2.1.4. Windows 95

U narednim godinama slijede nove velike stvari iz Microsofta: 1995. godine na tržište dolazi Windows 95 koji je postigao veliku popularnost. Inačica Windows 95 imala je ugrađen TCP/IP protokol (*eng. Transmission Control Protocol/Internet Protocol*), PnP podršku (*eng. Plug i Play)* kojom se omogućavalo korištenje uređaja odmah nakon uključivanja i bez puno podešavanja, a omogućavala je mnoge multimedijalne funkcije te *dial-up* (način pristupanja Internetu pomoću modema i telefonske linije) spajanje na udaljeno računalo. Windows 95 objavljen je na disketama i CD mediju.

2.1.5. Windows 98

1998 godine izlazi inačica Windows 98 kao nadogradnja na Windows 95. Windows 98 uključuje dodatnu zaštitu za važne datoteke na računalu, ugrađen je alat za automatsku izradu sigurnosne kopije registra (*eng. back up*), poboljšana je podrška za AGP (*eng. Advanced Graphics Port*), DirectX, DVD, USB te MMX standarde. Windows 98 bio je puno veći i sporiji od Windowsa 95 te je izvorna inačica imala dosta problema sa stabilnošću. Novi pomak donosi Windows 98 Second Edition (SE) kojim su ispravljeni neki nedostaci te je dodana nova aplikacija Microsoft Windows NetMeeting koja omogućuje povezivanje ljudi preko interneta.

2.1.6. Windows ME

Windows Millennium Edition (Windows ME) predstavljen je 2000. godine kao nadogradnja na Windows 95 i Windows 98. U inačici Windows ME prvi puta se spominje funkcija *System Restore* koja korisniku daje mogućnost povratka sustava u prijašnje stanje bez gubitka dokumenata ili zapisa. Sistemske datoteke su zaštićene i ne dozvoljava se njihova modifikacija nikome, čak ni administratoru. Windows ME uključuje podršku za UPnP (*eng. Universal Plug and Play*) te je uvedeno API (*eng. Application Programming Interface*) sučelje koje korisničkim aplikacijama omogućava pristup skupu funkcija ili programa drugih aplikacija i/ili operacijskog sustava. Iako su s Windows ME uvedene brojne promjene i poboljšanja, Microsoft je stalno bio na udaru kritike koja se žalila na nestabilnost izdane inačice.

2.2. NT jezgra

Windows NT (*eng. New Technology*) predstavlja granu operacijskih sustava temeljenih na korisnik-poslužitelj (*eng. Client-Server*) arhitekturi koja povezuje više manjih računala s poslužiteljem. Windows NT čine dva proizvoda: Microsoft NT radna stanica (eng. Microsoft NT Workstation) i Microsoft NT poslužitelj (eng. Microsoft NT Server). Osnovna ideja je razdvojiti radnu stanicu od poslužitelja tako da je za vrijeme korisnikova rada na računalu, veći dio vremena računalo (radna stanica) odvojena od poslužitelja. Radna postaja s vlastitom programskom potporom iz poslužitelja poziva podatke (datoteke) u svoju radnu memoriju, samostalno obrađuje podatke i po obradi vraća ih na poslužitelj gdje se čuvaju i na raspolaganju su svim korisnicima mreže. Windows NT dizajniran je kao višekorisnički, višeprocesorski sustav koji upravo zbog korištene arhitekture, NTFS datotečnog sustava, korištenih naredbi, činjenice da se radi o 32-bitnom višekorisničkom i višeprocesorskom sustavu jako podsjeća na Unix.

2.2.1. Windows NT 3.1

Windows NT 3.1 predstavljen je 1993. god. kao prvi 32-bitni operacijski sustav koji je uz NT tehnologiju donio i novi datotečni sustav, strukturu pomoću koje računala organiziraju podatke na tvrdom disku. Datotečni sustav NTFS (*eng. New Technology File System*) omogućuje bolje performanse i veću sigurnost podataka na tvrdom disku odnosno particijama ili jedinicama diska nego datotečni sustavi FAT/FAT32, korišteni u inačicama Windows sustava temeljenima na DOS jezgri. Korisničko sučelje vrlo je slično sučelju inačice Windows 3.1, ali je način rada znatno drugačiji.

2.2.2. Windows NT 4.0

Windows NT 4.0 izdan je 1996. godine. Korisničko sučelje je identično inačici Windows 95, no to su dva potpuno različita operacijska sustava različitih namjena. Windows NT 4.0 sadržavao je naprednu zaštitu, naprednu mrežnu podršku, cjelokupni 32-bitni Windows sustav raspoloživ kao radna stanica i poslužitelj te napredne korisničke administracije.

2.2.3. Windows 2000

2000. godine objavljen je Windows 2000 kojeg se ponekad zove i Windows NT 5.0. Windows 2000 sadrži preko 29 milijuna linija koda pisanih većinom u programskom jeziku C++. Od toga 8 milijuna je pisano za upravljačke programe (eng. driver). Windows 2000 je jedan od najvećih komercijalnih projekata ikada. Windows 2000 uz NTFS datotečni sustav koristi i EFS (*eng. Encrypted File Systems)* šifrirani datotečni sustav kojim se štite važni podaci. Aplikacija „Windows Installer“ prati aplikacije te prepoznaje i zamjenjuje komponente koje nedostaju.

2.2.4. Windows XP

Kao nadogradnja na Windowse 2000, samo godinu dana kasnije predstavljeni su Windowsi XP (*eng. Experienced*). Ispočetka je ova inačica imala malih problema u radu, ali izdavanjem skupnih zakrpa (eng. service pack) postala je standard za operacijske sustave. Iako je prošlo osam godina od njezinog izdavanja, danas još uvijek najveći broj korisnika koristi upravo tu inačicu Windowsa. Od noviteta potrebno je izdvojiti bolje kućno povezivanje računala, podršku za bežičnu mrežu, multimedijalne mogućnosti, bolji sustav pomoći (*eng.help center*) te podršku za nove vanjske uređaje. Korisničko sučelje je također znatno promijenjeno i

unaprijeđeno. Osim svih tih noviteta, XP će se sigurno pamtiti i po svojoj brzini i stabilnosti. Pojavljuje se dvije inačice: Home Edition za kućne i Professional Edition za poslovne korisnike. Osim što se izdavala kao 32-bitni sustav, prvi puta se na tržištu pojavljuje inačica Windowsa izdana kao 64-bitni operacijski sustav. Slika 3. prikazuje korisničko sučelje Windows XP-a.

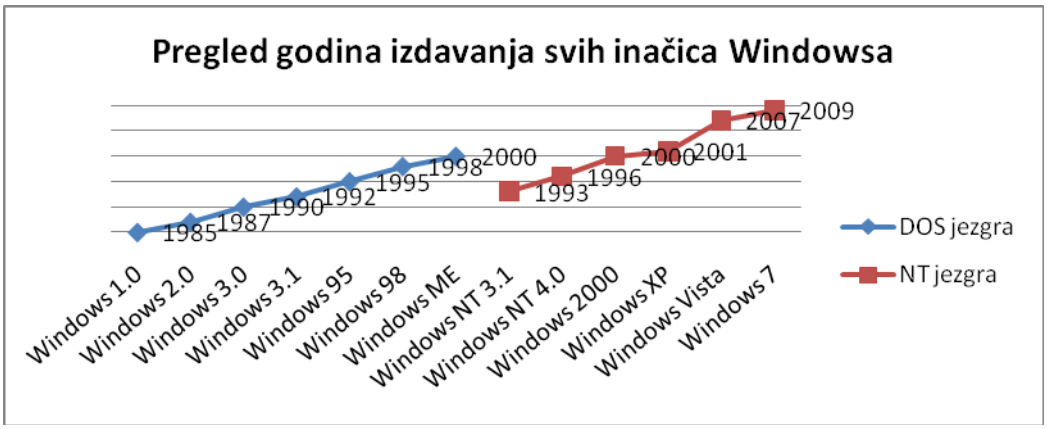
Slika 3. Prikaz korisničkog sučelja Windows XP-a

Izvor: Google

2.2.5. Windows Vista

Microsoft je Windows Vistu dugo nazivao kodnim imenom „Longhorn“. Iako je izrada Viste završena 2006. godine, na policama trgovina pojavila se tek 2007. Izrada Windows Viste odužila se na više od pet godina te je upravo to vrijeme postalo najduže razdoblje između izdavanja dvije inačice Windowsa. Originalni „Longhorn" koji je bio zasnovan na XP-ovom izvornom kodu je odbačen te se krenulo sasvim ispočetka u izgradnju novog operacijskog sustava. Windows Vista sadržava stotine novih značajki, unaprijeđeno je grafičko korisničko sučelje poznato pod nazivom Windows Aero, unaprijeđena je tražilica, pojavljuju se novi multimedijski alati kao Windows DVD Maker i potpuno redizajnirani mrežni, audio te grafički podsustavi. Windows Vista pokušava povećati razinu komunikacije između uređaja na kućnoj mreži koristeći *peer-to-peer* tehnologiju, te omogućuje lakšu razmjenu datoteka između računala i uređaja poput USB uređaja, printera te kamera. Vista uključuje inačicu 3.0 .NET Frameworka, koja programerima omogućuje lakšu izradu visokokvalitetnih aplikacija. Prilikom izrade Windows Viste, Microsoft je puno pažnje posvetio sigurnosti. Windows Vista je bila na stalnom udaru kritike uglavnom zbog ograničenja kopiranja zaštićenih digitalnih sadržaja te korisnosti novih značajki sustava kao što je kontrola korisničkih računa (UAC).

Kako bi se opisane inačice što bolje vremenski smjestile, graf 1 prikazuje pregled godina izdavanja svih inačica Windowsa.



Graf 1. Pregled godina izdavanja svih inačica Windowsa

Dok Tablica 1. prikazuje popis noviteta koje dolaze uz svaku inačicu Windowsa.

INAČICA	NOVOSTI
Windows 1.0	Proizvod je uključivao kalendar, uređivač teksta (Notepad), kalkulator, sat, upravljačku ploču (Control Panel) te alate za crtanje (Paint) i pisanje (Write)
Windows 2.0	Napredni mehanizam kratica pomoću tipki tipkovnice Terminologija „Minimize" i „Maximize" (do tada „Iconize" i „Zoom") Prve inačice Microsoft Word-a i Microsoft Excel-a
Windows 3.0 i Windows 3.1	Korisnicima je omogućeno korištenje miša kojim se moglo upravljati podacima jednom rukom bez pamćenja naredbi MS-DOS-a Pokretanje više aplikacija u isto vrijeme (*eng. multitasking*).
Windows 95	Ugrađen TCP/IP protokol (*eng. Transmission Control Protocol/Internet Protocol*) PnP podrška (*eng. Plug i Play)* kojom se omogućava korištenje uređaja odmah nakon uključivanja, bez puno podešavanja Multimedijalne funkcije *Dial-up* (način pristupanja internetu pomoću modema i telefonske linije) spajanje na udaljeno računalo.
Windows 98	Dodatna zaštita za važne datoteke na računalu Ugrađen alat za automatsku izradu sigurnosne kopije registra (*eng. back up*) Poboljšana podrška za AGP (*eng. Advanced Graphics Port*), DirectX, DVD, USB te MMX.
Windows ME	*System Restore* funkcija koja korisniku daje mogućnost povratka sustava u prijašnje stanje bez gubitka dokumenata ili zapisa Sistemske datoteke su zaštićene i ne dozvoljava se njihova modifikacija nikome, čak ni administatoru Podrška za UpnP (*eng. Universal Plug and Play*) API (*eng. Application Programming Interface*) sučelje koje korisničkim aplikacijama omogućava pristup skupu funkcija ili programa drugih aplikacija i/ili operacijskog sustava.
Windows NT 3.1	Prvi 32-bitni operacijski sustav Novi datotečni sustav NTFS (*eng. New Technology File System*)
Windows NT 4.0	Napredna zaštita Napredna mrežna podrška Cjelokupni 32-bitni Windows sustav raspoloživ kao radna stanica i

	poslužitelj
	Napredne korisničke administracije.
Windows 2000	Uz NTFS datotečni sustav koristi i EFS (*eng. Encrypted File Systems)* šifrirani datotečni sustav kojim se štite važni podatci
	Aplikacija „Windows Installer“ prati aplikacije te prepoznaje i zamjenjuje komponente koje nedostaju.
Windows Xp	Bolje kućno povezivanje računala
	Podrška za bežičnu mrežu
	Multimedijalne mogućnosti,
	Bolji sustav pomoći (*eng.help center*)
	Podrška za nove vanjske uređaje
	Promijenjeno i unaprijeđeno korisničko sučelje
	Prvi 64-bitni operacijski sustav
Windows Vista	Unaprijeđeno grafičko korisničko sučelje Windows Aero
	Unaprijeđena tražilica
	Novi multimedijski alati kao Windows DVD Maker
	Potpuno redizajnirani mrežni, audio te grafički podsustavi
	Peer-to-peer tehnologija
	Inačica 3.0 .NET Frameworka, koja programerima omogućuje lakšu izradu visokokvalitetnih aplikacija.

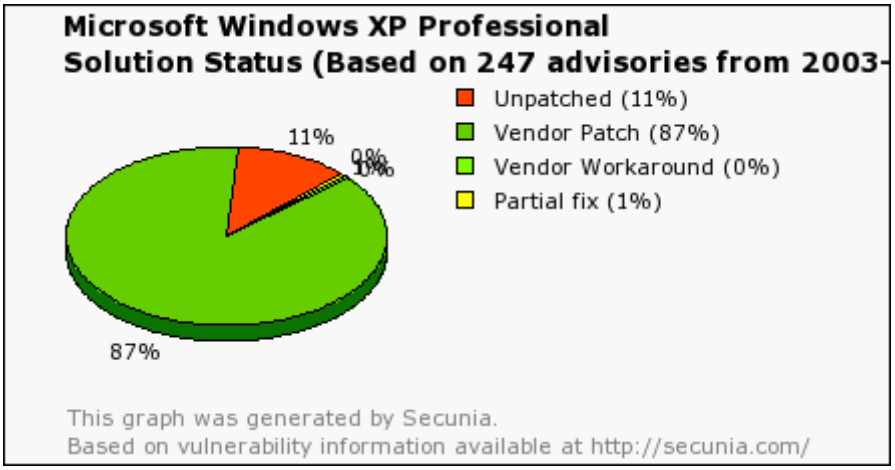
Tablica 1. Popis noviteta koji dolaze uz svaku inačicu

2.3. Pregled sigurnosnih nedostataka prijašnjih inačica

U današnje vrijeme, zbog sve većeg broja sigurnosnih prijetnji koje okružuju korisnika i konstantne povezanosti na Internet kod operacijskih sustava se rješavanje sigurnosnih problema smatra jednim od najvažnijih prioriteta. Napadi zlonamjernih korisnika mogu imati različite posljedice, od krađe povjerljivih podataka do umetanja zlonamjernih programa koji mogu dovesti do potpunog rušenja sustava. Windows, kao najzastupljeniji operacijski sustav, je najčešće na udaru zlonamjernih korisnika. Slijedi popis sustava u Windowsima koji su se pokazali najranjivijima prema istraživanju SANS (*eng. SysAdmin, Audit, Network, Security*) instituta:

- Internet Information Services (IIS)
- Microsoft SQL Server (MSSQL)
- Windows Authentication
- Internet Explorer (IE)
- Windows Remote Access Services
- Microsoft Data Access Components (MDAC)
- Windows Scripting Host (WSH)
- Microsoft Outlook Express
- Windows Peer to Peer File Sharing (P2P)
- Simple Network Management Protocol (SNMP)

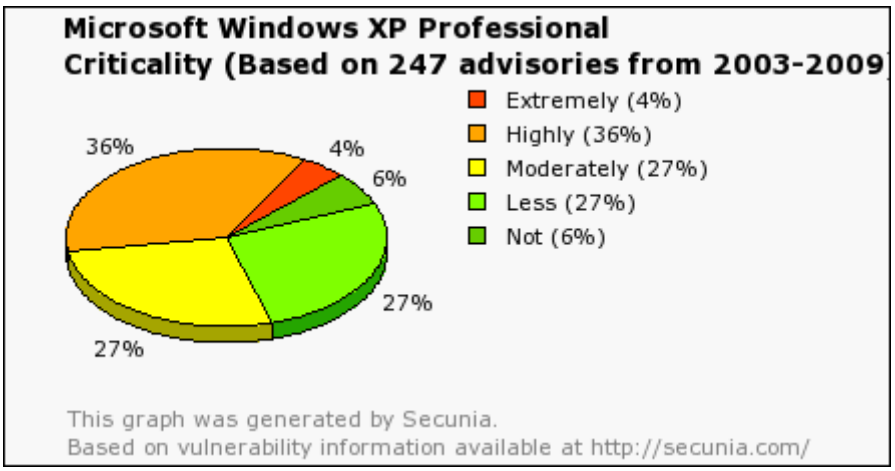
Kako bi dobili uvid koliko je napada bilo, koji su najčešći tipovi napada te koliko je sigurnosnih propusta uklonjeno slijede statistički podaci za operacijske sustave Windows XP i Windows Vista. Prikazani grafovi napravljeni su na temelju dugogodišnjeg istraživanja tvrtke Secunia. Prve tri slike prikazuju statističke podatke za operacijski sustav Windows XP. Na slici 4. može se uočiti ukupan broj otklonjenih, djelomično uklonjenih i neuklonjenih sigurnosnih propusta u razdoblju od 2003.-2009. godine. Nažalost veći broj propusta Microsoft još uvijek nije uklonio.



Slika 4: Podjela sigurnosnih propusta prema statusu

Izvor: Secunia

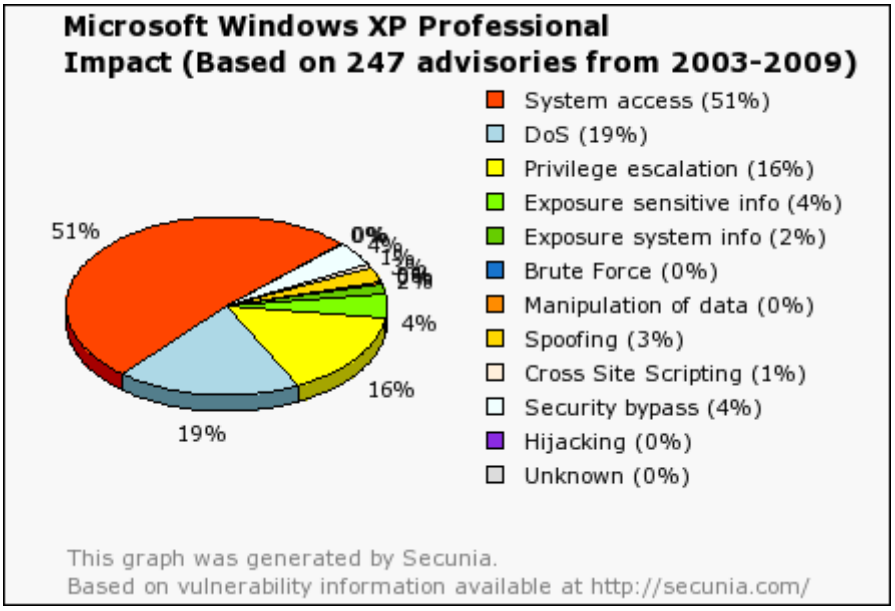
Sigurnosni propusti se mogu podijeliti u nekoliko grupa, ovisno o šteti koju mogu prouzročiti. Slika 5. prikazuje podjelu sigurnosnih propusta za Windows XP sustav u navedene grupe. Iz slike je vidljivo da je najveći broj propusta bio visoko opasan.



Slika 5: Podjela sigurnosnih propusta prema šteti koju uzrokuju

Izvor: Secunia

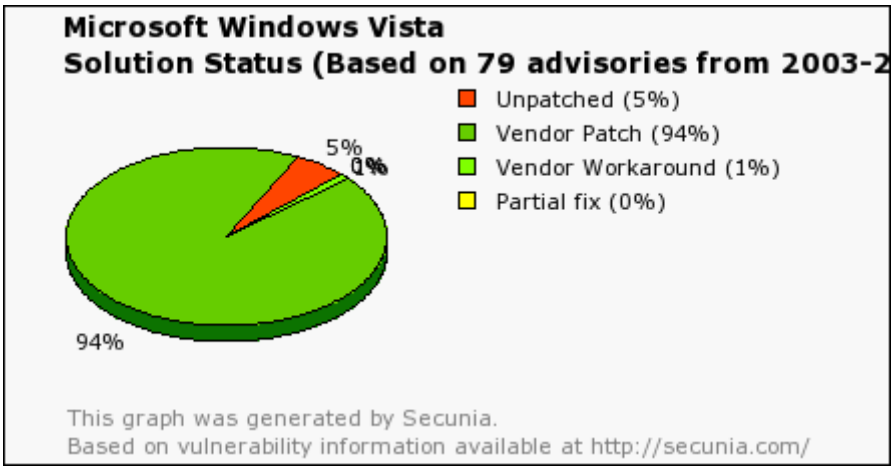
Posljednja slika, vezana za operacijski sustav Windows XP, opisuje koji tipovi napada su bili najzastupljeniji. Iz priložene slike vidi se da su najzastupljeniji tzv. "*System access"* napadi, nakon čega slijede DOS (*eng*. *Denial of Service*) napadi.



Slika 6: Najzastupljeniji tipovi napada

Izvor: Secunia

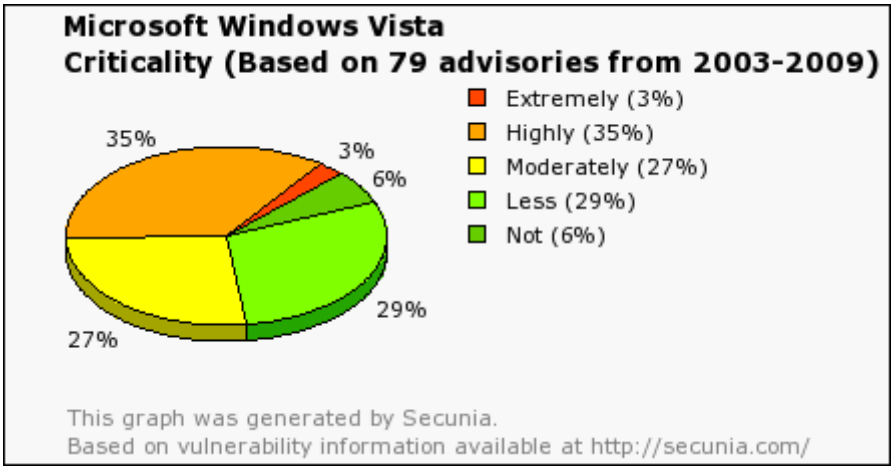
Nakon prikaza statističkih podataka za Windows XP, slijedi prikaz istih statističkih podataka za Windows Vistu. Iz slike 7. vidi se kako je broj sigurnosnih propusta koji nisu uklonjeni znatno smanjen u odnosu na Windows XP.



Slika 7: Podjela sigurnosnih propusta prema statusu

Izvor: Secunia

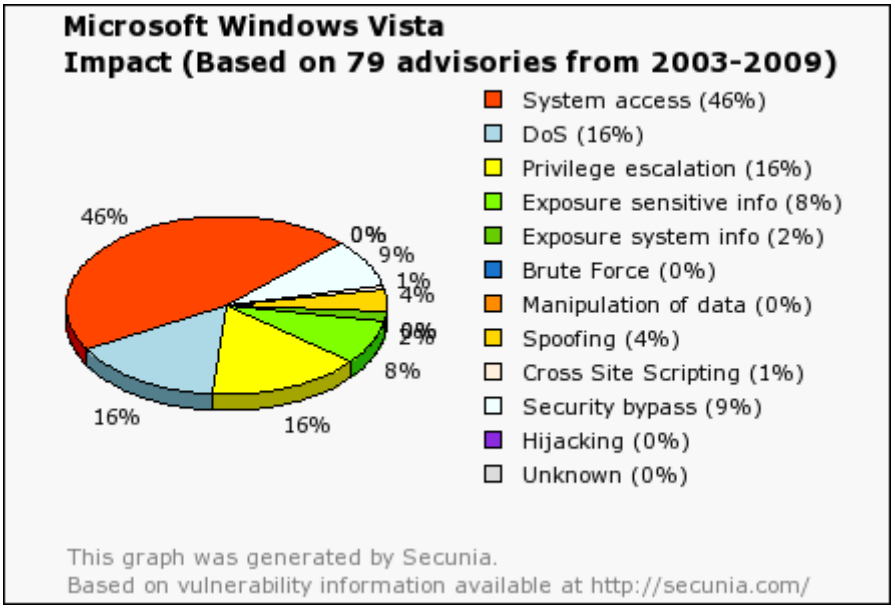
Slika 8. prikazuje podjelu sigurnosnih napada u nekoliko grupa. Ukoliko tu sliku usporedimo sa slikom 6. vidimo da je raspodjela sigurnosnih propusta u grupe u Windows Visti gotovo identična podjeli kod Windows XP-a.



Slika 8: Podjela sigurnosnih propusta prema šteti koju uzrokuju

Izvor: Secunia

Slika 9. prikazuje koji su tipovi napada bili najzastupljeniji. Ako se ova slika usporedi sa slikom 6. vidljivo je da je broj "*System access"* napada smanjen s 51% na 46% odnosno da je broj DOS napada smanjen s 19% na 16%.



Slika 9 : Najzastupljeniji tipovi napada

Izvor: Secunia

Microsoft je svjestan koliko je bitno stalno poboljšavati sigurnost operacijskih sustava. Svaki drugi utorak u mjesecu Microsoft izdaje niz sigurnosnih zakrpa za otkrivene propuste ili otkrivene napade. Zakrpe se izdaju za sve inačice Windowsa koje su još u uporabi kod većeg broja korisnika. Ukoliko se dogodi veći broj napada ili propusta Microsoft izdaje Service Pack-ove (SP) za pojedine inačice. Tu tradiciju je započeo s Windows XP-om za kojeg su izdana tri SP-a. SP1 donio je poboljšanu USB 2.0 podršku, što u praksi znači jednostavniju uporabu pisača ili nekog drugog USB uređaja, SP2 pamtimo po ugrađenom vatrozidu (eng. firewall), podršci za bežičnu komunikaciju te automatskoj nadogradnji (eng. Update), dok SP3 u velikoj mjeri doprinosi stabilnosti i sigurnosti Windows XP sustava.

Osim sigurnosnih zakrpa, Microsoft povećava sigurnost operacijskih sustava i razvojem tehnologija za zaštitu jezgre operacijskih sustava. U inačicama Windows Vista i Windows 7 koristi se nov način zaštite od iskorištavanja sigurnosnih propusta prekoračenjem kapaciteta međuspremnika. ASLR (eng. Address Space Layout Randomization) tehnologija omogućava

učitavanje ključnih sistemskih datoteka u različite memorijske lokacije svaki put kad se računalo pokrene, što otežava pokretanje automatiziranih napada te izvršavanje malicioznog koda. ASLR nije Microsoftova inovacija, jer sličnu tehnologiju već neko vrijeme koriste OpenBSD te Pax i Exec Shield za operacijske sustave Linux. Određeni napadi pokušavaju pozvati sistemske funkcije Windows-a, npr. funkciju socket() iz biblioteke "wsock32.dll" za otvaranje mrežnog priključka, a korištenjem ove tehnologije sistemske datoteke se nalaze na nepredviđenom mjestu čime se otežava posao napadaču.

3. Novosti u sustavu Windows 7

Windows 7 je radni naziv najnovijeg operacijskog sustava, nasljednika Viste. Na tržištu je dostupan od 22. listopada 2009. godine u 32-bitnoj i 64-bitnoj inačici. Prema riječima Microsofta, Windows 7 je dorađena i poboljšana inačica postojeće Viste. Ispitivanje novog operacijskog sustava trajalo je više od godine dana. Prvi puta u ispitivanju su pomagali i milijuni zainteresiranih korisnika koji su besplatno mogli skinuti probnu (eng. beta) inačicu na određeno vrijeme. Na taj način otklonjeni su mnogi problemi te nekompatibilnosti koje su mučile Vistu od samog izlaska.

3.1. Instalacija

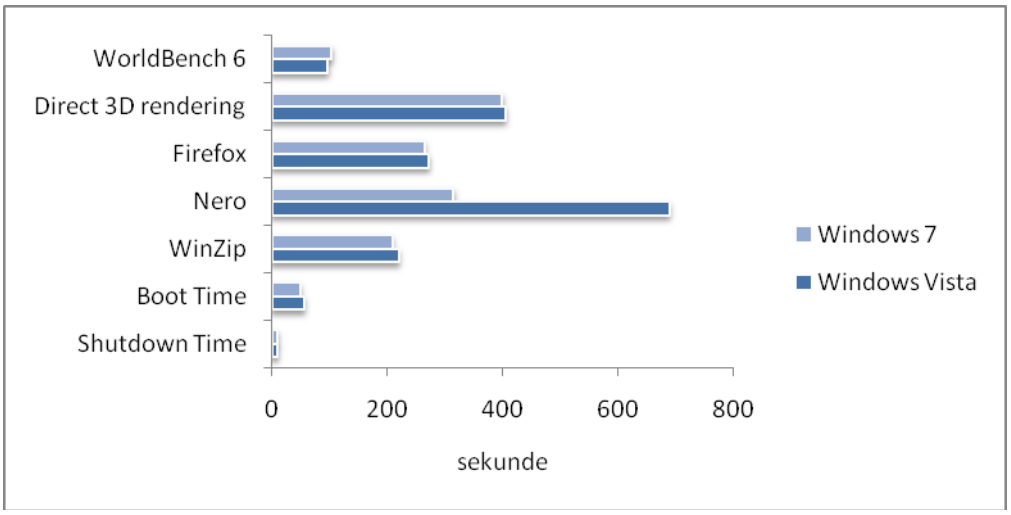
Instalacija Windowsa već je dugo prilično bezbolan i kratak proces. Windows 7 u tome nije iznimka, a sam proces instalacije kraći je no ikada. Inačica Windows 7 inteligentno prepoznaje stari operacijski sustav te zna automatski napraviti „dual-boot“ instalaciju koja omogućava pokretanje dva operacijska sustava na jednom računalu, ali ne u isto vrijeme. Prilikom podizanja računala korisnik sam odlučuje koji operacijski sustav želi koristiti. Microsoft je s Vistom uveo nešto drugačiji proces podizanja OS-a korištenjem BDC (*eng. Boot Configuration Data*) tehnologije. Time je Microsoft uveo nešto drugačiji način podizanja OS-a zamjenom datoteke boot.ini s BDC(*eng. Boot Configuration Data)* datotekom. Osim što pomoću nje možemo napraviti *dual boot* s ranijim inačicama Microsoftovih OS-a, BDC omogućava kombiniranje s *boot loaderima (*program koji služi za podizanje točno određenog operacijskog sustava*)* drugih OS-ova koji nisu Microsoftovi. Tako, primjerice, možemo iskoristiti kombinaciju Microsoftovog *boot loadera* i GRUB-a (*eng. Grand Unified Bootloader*) ili LILO-a (*eng. Linux Loader*) da bismo napraviti *dual boot* s Linuxom.

3.2. Poboljšane performanse

Microsoft je veliku pažnju posvetio poboljšanju performansi. Ključna poboljšanja:

- Windows 7 oblikovan je za brži ulazak u stanje mirovanja, brži izlazak iz njega i brže ponovno povezivanje s bežičnom mrežom.
- Sortiranje i grupiranje podataka znatno je ubrzano stoga korisnici puno brže dolaze do rezultata pretraživanja.
- Kada se prvi put priključi prijenosni izmjenjivi memorijski pogon ili neki drugi USB uređaj, Windows 7 osposobljava ga za rad u samo nekoliko sekundi. Ako je taj uređaj već korišten čekanje je još kraće.
- Za razliku od prethodnika, sustav Windows 7 napravljen je tako da sporedne servise, koji smanjuju brzinu, pokreće samo kada ih se treba. Npr. ukoliko se Bluetooth uređaj ne koristi, Windows 7 Bluetooth servis neće ga niti uključiti.

Kako bi dokazali da je Microsoft zaista poboljšao performanse Windows 7 u odnosu na Vistu, slijedi usporedba navedenih operacijskih sustava, prikazana na slici 10., koju je radio The PC World Test Center.



Slika 10: Usporedba performansi Windowsa 7 i Windows Viste

Testiranja su provođena korištenjem stolnih računala HP Pavilion a6710t s instaliranom 64-bitnom inačicom Windows Vista Ultimate odnosno Windows 7 Ultimate. Kao što je vidljivo sa slike, napredak u performansama inačice Windows 7 u odnosu na Windows Vistu postoji, ali on nije dramatičan kao što se to najavljivalo.

3.3. Promjene u izgledu sučelja

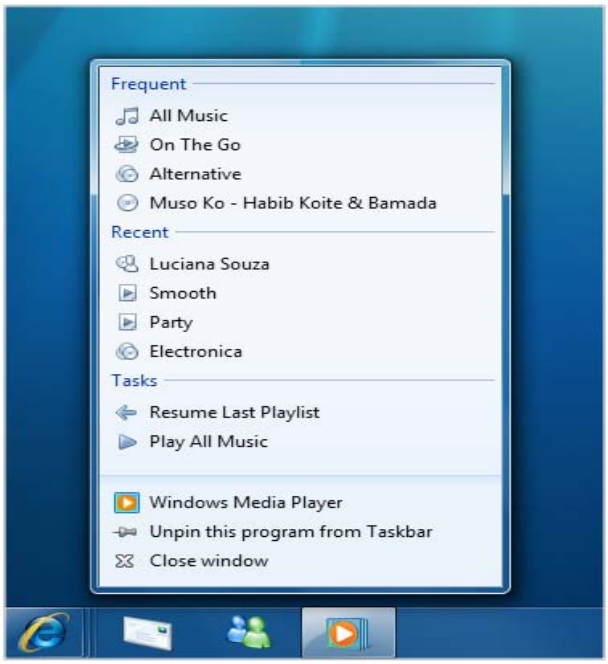
Inačica Windows 7 donijela je mnoge promjene u izgledu sučelja. Prva promjena može se uočit u alatnoj traci koja se u potpunosti razlikuje od one u Visti. Na alatnu traku može se pričvrstiti bilo koji program za kojeg želite da Vam uvijek bude dostupan jednim klikom. Svi programi prikazani su samo ikonom, bez teksta. Velikom broju korisnika nova alatna traka stvara probleme jer se sada na njoj nalaze pomiješane ikone aktivnih aplikacija s ikonama onih koje su samo ondje pričvršćene, a nisu pokrenute. Ikone su povećane radi lakšeg korištenja. Prelaskom miša preko ikona, pojavljuje se minijatura svakog prozora ili datoteke koja se otvara pomoću tog programa. Držanjem pokazivača miša iznad minijature, prikazuje se pregled tog prozora preko cijelog zaslona. Micanjem pokazivača miša s minijature, pregled nestaje. Slika 11. prikazuje alatnu traku.

Slika 11: Alatna traka Windowsa 7

Izvor: Google

Rad s prozorima na radnoj površini je pojednostavljen. U Visti je bio predstavljen Windows Aero (*eng. Authentic, Energetic, Reflective, Open*) koji je u novoj inačica operacijskog sustava još unaprijeđen. Aero 3D je mogućnost koja omogućuje trodimenzionalni prikaz otvorenih prozora, koji se mogu brzo listati. Aero Peek je nova mogućnost koja otvorene programe čini prozirnima, omogućujući tako pogled na radnu površinu, bez zatvaranja prozora. Aero Shake mogućnost se koristi za minimiziranje svih ostalih prozora, jednostavnim prodrmavanjem mišem željenog prozora. Mijenjanje veličine otvorenih prozora moguće je jednostavnim povlačenjem prema rubovima zaslona uz Aero Snap mogućnost.

Potpuno novu značajku sučelja Windows 7 čini *Jump List*. Radi se o funkcionalnosti koja omogućuje brzi pristup nedavno korištenim datotekama. Npr. desnim klikom miša na ikonu programa Word, prikazuju se nedavno korišteni Wordovi dokumenti. Na skočni popis moguće je pričvrstiti i vlastite datoteke kako bi nam uvijek bile pri ruci. Slika 12. prikazuje skočnu listu *Windows Media Playera*.



Slika 12: Skočna lista Windows Media Playera

Izvor: Google

3.4. Poboljšano upravljanje napajanjem

Windows 7 donosi poboljšanja za uštedu energije s ciljem produljenja vijeka trajanja baterije. Npr. svjetlina zaslona će se automatski zatamniti ukoliko se računalo ne koristi neko vrijeme. Ostala poboljšanja obuhvaćaju korištenje manje energije za reprodukciju DVD medija (korisno na putovanjima) i bolju iskorištenost procesorske snage.

3.5. Windows dodirna tehnologija

Premda su odlični za obavljanje mnogih zadataka, tipkovnica i miš nisu uvijek najelegantniji alati. Sustav Windows 7 omogućuje korištenje zaslona osjetljivog na dodir. Dodirujući prstima zaslon moguće je kretati se, mijenjati veličinu prozora, reproducirati medijski sadržaj te pregledavati fotografije. Windows 7 uvodi i podršku za novu tehnologiju višestrukog dodira koja omogućuje upravljanje događajima na zaslonu s većim brojem prstiju . Primjerice, slika je moguće povećati primicanjem dva prsta te vratiti u prvobitno stanje razmicanjem dva prsta. Sliku na zaslonu moguće je zakrenuti rotiranjem jednog prsta oko drugog.

3.6. Windows Media Centar

S pojednostavnjenim korisničkim sučeljem i podrškom za nove vrste sadržaja i digitalnu televiziju, Windows Media Centar čini gledanje televizije, filmova i ostalih video sadržaja na računalu lakšim no ikada prije. Emisije iz rasporeda se može snimati i gledati putem kabelske veze i jednostavne USB TV kartice.

3.7. Virtualni XP

Windows XP Mode ili XPM (*eng. Windows XP Mode*) nova je mogućnost Windowsa 7 dostupna vlasnicima inačica Professional, Enterprise i Ultimate. Namijenjen je poslovnim korisnicima koji posjeduju programe pisane za Windowse XP, a imaju želje i mogućnosti za prelazak na Windows 7. XP Mode unutar virtualnog računala pokreće Windows XP. Valja imati na umu da je XP Mode

koncept, a virtualizacijski softver je Virtual PC, unutar kojega se izvodi Mode XP. Stoga računalo, točnije njegov procesor, mora sklopovski podržavati virtualizaciju. Virtual PC podržava samo 32-bitna virtualna računala te se pritom zahtijeva dodatnih 2 GB memorije.

4. Sigurnost operacijskog sustava Windows 7

Sigurnost operacijskog sustava Windows 7 u odnosu na Windows Vistu nije znatno promijenjena, već je samo unaprijeđena. Slijedi pregled sigurnosnih elemenata i otkrivenih propusta u novom operacijskom sustavu.

4.1. Sigurnosni elementi

Operacijski sustav Windows 7 dolazi s nekoliko različitih aplikacija namijenjenih održavanju sigurnosnih sustava. U nastavku su navedene značajnije aplikacije zajedno s kratkim opisom rada.

4.1.1. Action Center

Windows Security Center preimenovan je u akcijski centar (eng. Windows Action Center) koji sada korisnicima osim pregleda i mijenjanja postavki računalne sigurnosti služi i za redovito održavanje sustava. U sklopu akcijskog centra mogu se pronaći moduli za nadzor vatrozida (eng. Firewall), antivirusnog te antispyware programa, ali i upozorenja o novim nadogradnjama s Windows Update-a, poruke Windows Backupa ili popis problema s Windows Troubleshooting-a.

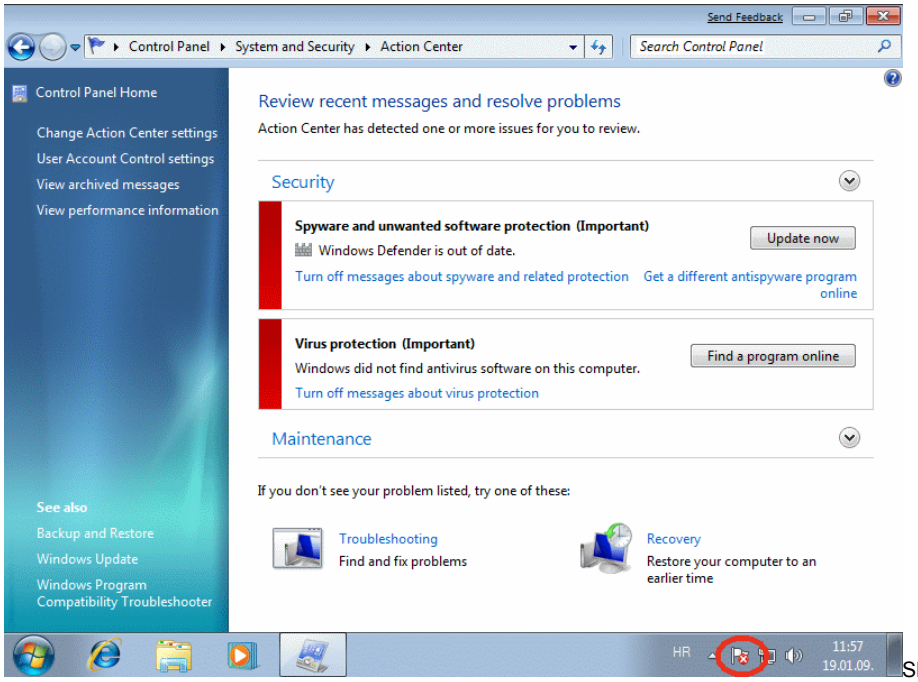
Sigurnosni elementi koje provjerava akcijski centar:

- **Vatrozid** – da li je instaliran i uključen,
- **Antivirusni program** – da li je instaliran, ima li najsvježije definicije zloćudnih programa te je li omogućen sigurnosni pregled korištenih aplikacija,
- **Anti-spyware** – je li instaliran, ima li najnovije definicije spyware programa te je li omogućen sigurnosni pregled korištenih aplikacija.

Alati za održavanje:

- **Windows Troubleshooting** – alat koji bilježi sve probleme sa sustavom te se povremeno spaja na Microsoftovu stranicu kako bi pronašao i predložio rješenja. Osim toga, iz njega je moguće pokrenuti i niz radnji za konfiguriranje sustava (poput konfiguracije mreže, podešavanja nekog uređaja i sl.),
- **System Restore** - alat koja osim vraćanja operacijskog sustava u neko od prethodno snimljenih stanja u novoj inačici OS-a omogućuje i reinstalaciju samog operacijskog sustava,
- **Windows Update** – obavještava o mogućim nadogradnjama sustava.

Kada se status nadzirane stavke promijeni (npr. antivirusni softver zastari), akcijski centar vas o tome obavještava porukom u području obavijesti na traci sa zadacima. Status stavke u akcijskom centru mijenja boju da bi uputio na ozbiljnost poruke te preporučio daljnje postupke. Slika 13. prikazuje postavke akcijskog centra.



Slika **Slika 13:** Akcijski centar – podešavanje postavki sigurnosti i održavanja

Izvor: Google

Osim prethodno navedenih alata, akcijski centar uključuje i Windows Defender te mehanizam za kontrolu korisničkih računa.

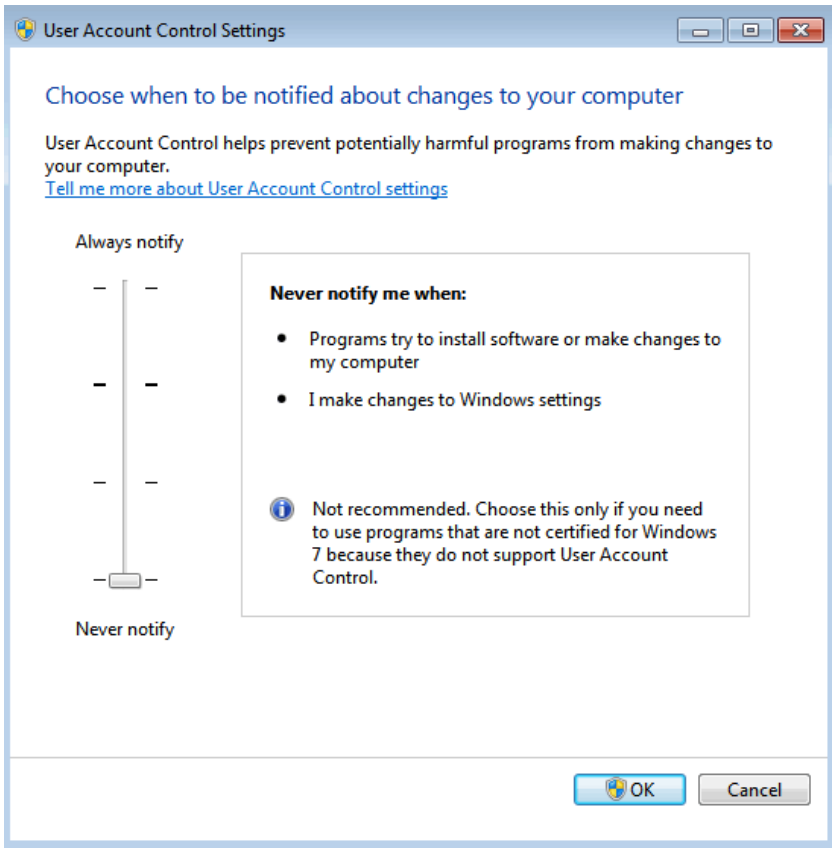
Windows Defender je alat razvijen s namjerom sprječavanja i izolacije programa koji skupljaju osobne podatke korisnika bez njihovog znanja (*eng. spyware*). Nakon sigurnosnog pregleda, ovisno o potencijalnoj opasnosti zlonamjernih programa, Windows Defender opisuje probleme s najvećim - visokim, srednjim te niskim rizikom i omogućuje korisniku da odluči hoće li nastaviti s korištenjem problematičnog programa. Iako Windows Defender nije značajnije promijenjen u odnosu na prijašnju inačicu, dodana je ipak jedna nova mogućnost. Mogućnost „Očisti sustav“ omogućuje uklanjanje sumnjivog programa na jednostavan način. Detalje o ovom alatu moguće je pronaći na službenim stranicama CERTa u dokumentu „*Sigurnost Windows Vista operacijskog sustava*“ (http://www.cert.hr/documents.php?id=286).

Kontrola korisničkih računa (*eng. User Account Control UAC*) je sigurnosna značajka koja pomaže u sprječavanju neovlaštenih promjena na računalu. Te promjene mogu inicirati zlonamjerni programi ili drugi korisnici. UAC dopušta promjene samo uz odobrenje administratora računala. Promjene koje ne odobri administrator neće se aktivirati i sustav će ostati nepromijenjen. UAC je najviše kritizirana funkcija u sustavu Windows Vista, koja je vrlo uporno obavještavala korisnike o svakom događaju, od pokretanja Windows Update-a do promjene rezolucije. Kod sustava Windows 7 puno je bolje podešena. Za razliku od sustava Windows Vista, gdje su bile samo dvije moguće postavke UAC-a (uključiti ili isključiti), u Windowsima 7 postoje četiri razine za izbor. Razlike među njima su sljedeće:

- **Uvijek obavijestiti** (*eng. Always notify*)– obavijest će se pojaviti svaki put kad neki program pokuša izvršiti promjene na računalu ili na postavkama Windows sustava koje zahtijevaju dozvolu administratora. To je postavka najvišeg stupnja razine.
- **Obavijesti me samo kada programi pokušavaju napraviti promjene na mojem računalu (***eng. Notify me only when* programs *try to make changes to my computer***)** - postavka kojom korisnici sami odlučuju kada žele primati obavijesti. Uvijek treba biti oprezan u pogledu programa kojima se dopušta pokretanje na računalu. Neki programi koji su obuhvaćeni u sklopu sustava Windows mogu primati naredbe ili podatke, a zlonamjerni program može to iskoristiti za instalaciju programa ili promjenu postavki na računalu.
- **Obavijesti kad neki program pokuša izvršiti promjene na računalu (ne zatamniti radnu površinu) (***eng. Notify me only when programs try to make changes to my computer (do not dim my desktop)***–** postavka koja se od prethodno navedene razlikuje

samo u činjenici da radna površina nije zatamnjena te stoga drugi programi mogu prekriti UAC dijaloški prozor.

- **Nikada obavijestiti** (*eng. Never notify*)- To je postavka najmanje razine sigurnosti. Kad se u UAC-u isključi primanje obavijesti, računalo se izlaže sigurnosnom riziku. Ako se u UAC-u isključi primanje obavijesti, treba biti oprezan s programima koji imaju dozvolu za pokretanje jer oni tada imaju isti pristup računalu kao i korisnici. To obuhvaća čitanje i izvođenje promjena na zaštićenim područjima sustava, osobnim podacima, spremljenim datotekama te svemu što je pohranjeno na računalu. Programi će također moći komunicirati i prenositi informacije putem bilo čega što je povezano s računalom, što uključuje i Internet. Detalje o ovom alatu moguće je pronaći na službenim stranicama CERT-a u dokumentu „*Sigurnost Windows Vista operacijskog sustava*“ (http://www.cert.hr/documents.php?id=286). Slika 14. prikazuje postavke UAC-a.



Slika 14: Postavke UAC-a

Izvor: Google

4.1.2. Vatrozid

Vatrozid (*eng. Firewall*) je programska ili sklopovska podrška koja provjerava informacije koje dolaze s interneta ili neke druge mreže, te ih zaustavlja ili im dopušta prolaz do operacijskog sustava korisnika ovisno o postavljenim sigurnosnim pravilima. U operacijskom sustavu Windows 7 vatrozid je proširen s još boljim sustavom podešavanja.

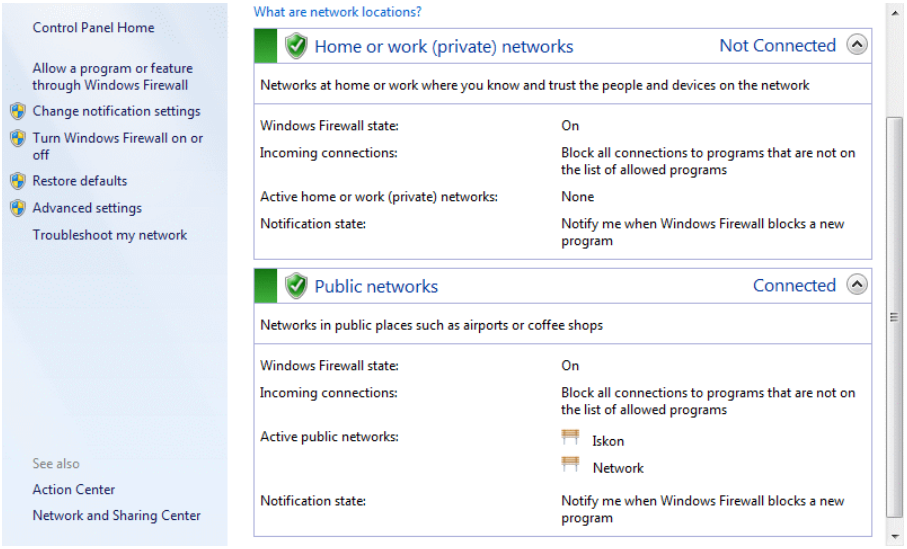
Novi sustav omogućuje precizno podešavanje zaštite i obavijesti za svaki mrežni profil (kuća, posao i javno mjesto) posebno. Prilikom spajanja na javnu mrežu , primjerice u knjižnici ili kafiću, poželjno je blokirati sve dolazne veze. To može ometati rad kod kuće ili na poslu. Bez obzira na odabranu razinu sigurnosti profila, moći ćete se s lakoćom prebacivati s jednog na drugi. U Windows 7 funkcije vatrozida razdvojene su u dva odvojena sustava nadzora - kućna i poslovna mreža te javna mreža.

Prilikom prvog povezivanja s mrežom, potrebno je odabrati mrežno mjesto. Tako se automatski postavljaju odgovarajuće vatrozidne postavke za vrstu mreže s kojom se povezuje. Ako se povezuje s mrežama na različitim mjestima (primjerice s mrežom kod

kuće, u obližnjem kafiću ili na radnom mjestu), zahvaljujući odabiru mrežnog mjesta računalo će uvijek biti postavljeno na odgovarajuću sigurnosnu razinu. Postoje četiri mrežna mjesta:

- Kućno ili radno mjesto (*eng. Home or Work (private) network*) – mrežno mjesto se odabire ukoliko su osobe i uređaji povezani s mrežom poznati i pouzdani. Značajka otkrivanja mreže je uključena te omogućuje korisniku da vidi druga računala i uređaje na mreži,
- Javno mjesto (*eng. Public network*) – mrežno mjesto koje se odabire na javnim mjestima. Namjena ovog mrežnog mjesta je učiniti korisnikovo računalo nevidljivo za ostala računala na mreži te ga zaštititi od zlonamjernih programa s Interneta,
- Mrežno mjesto Domena (*eng. Domain*) - koristi se za mreže s domenama, npr. one u korporacijama. Tom vrstom mrežnog mjesta upravlja mrežni administrator i ne može se birati ni mijenjati.

Odabirom javnog mjesta blokira se rad određenih programa i servisa da bi se računalo zaštitilo od neovlaštenog pristupa dok je povezano s mrežom na javnom mjestu. Ukoliko je računalo povezano s mrežom na javnom mjestu te je vatrozid uključen, neki programi i servisi tražit će da ih se deblokira (omogući im se da komuniciraju kroz vatrozid) da bi pravilno radili. Kad deblokiranja programa, vatrozid ga deblokira za svaku mrežu koja ima iste vrste mjesta kao i mreža s kojom je računalo trenutno povezano. Ako se, na primjer, korisnik poveže s mrežom u kafiću i odabere „Javno mjesto" kao vrstu mjesta, a zatim deblokira program za neposredno slanje poruka, taj će program biti deblokiran za sve mreže na mjestu „Javno mjesto". Korisnik jednostavnim stavljanjem kvačice ili njezinim micanjem odlučuje na kojem mrežnom mjestu želi dozvoliti ili onemogućiti pokretanje određenog programa. Mrežna mjesta nije moguće mijenjati niti dodavati. Slika 15. prikazuje postavke vatrozida u sustavu Windows 7.



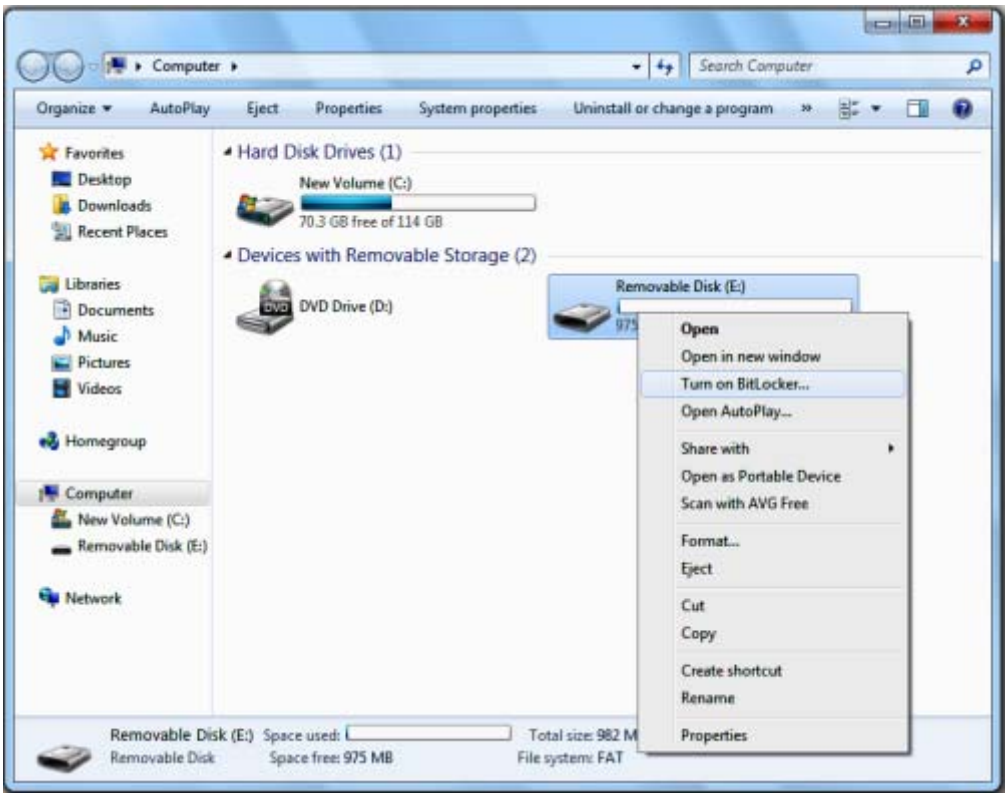
Slika 15: *Vatrozid*

4.1.3. BitLocker i BitLocker To Go

Bitlocker Drive Encryption je mehanizam koji omogućuje sigurnu enkripciju cijelog fizičkog diska računala. Za razliku od šifriranog datotečnog sustava (eng. Encrypting File System EFS), koji omogućuje šifriranje pojedinih datoteka, BitLocker šifrira cijeli disk. Kompletno kriptirani disk je u slučaju krađe u potpunosti zaštićen, dok se kod kriptiranja pojedinih datoteka i mapa lako može dogoditi da se zaboravi na privremene datoteke koji Windowsi pohranjuju u odgovarajuće mape koje najčešće tamo i ostaju. Podaci kriptirani Bitlockerom otključavaju se lozinkom, pametnom karticom ili se može postaviti pogon za automatsko otključavanje prijavom određenog korisnika na sustav. Iako sam mehanizam nije značajno promijenjen u odnosu na Vistu, dodana je jedna nova mogućnost - zaštita svih datoteka pohranjenih na eksternim memorijama za trajnu pohranu (vanjski tvrdi disk ili USB memorije). Bitlocker to go obavlja taj postupak, a nakon enkripcije, podaci spremljeni na

primjer na USB memoriji, postaju čitljivi samo nakon unosa lozinke. S obzirom da se USB memorija lako gubi, ovo je jednostavan i brz način zaštite podataka. Nažalost, mehanizam ima jedno veliko ograničenje, a to je da se podaci na USB memoriji mogu mijenjati, dodavati ili brisati samo na računalima s instaliranim sustavom Windows 7. Na Windowsima XP ili Visti dopušteno je samo čitanje podataka dok na ostalim operacijskim sustavima ovako zaštićena USB memorija nije uopće čitljiva. Otkrije li potencijalni sigurnosni rizik, BitLocker će zaključati pogon operacijskog sustava i zatražiti poseban BitLocker ključ oporavka da bi ga otključao. Vrlo je važno stvoriti ovaj ključ oporavka prilikom prvog uključivanja BitLockera jer u protivnom korisnik može trajno izgubiti pristup svojim datotekama.

Bitlocker se uključuje vrlo jednostavno iz sigurnosnog dijela Control Panela. Nakon pokretanja zahtjeva za uključivanjem Bitlockera potrebno je samo pratiti upute čarobnjaka. Slika 16. prikazuje enkripciju podataka spremljenih na USB memoriju pomoću BitLockera.



Slika 16: Enkripcija podataka spremljenih na USB memoriju pomoću Bitlockera

Izvor: Google

4.1.4. AppLocker, Microsoft Security Essentials

AppLocker je skup postavki iz Group Policy-a kojima se određuje koji korisnici smiju pokretati koje aplikacije na računalu ili mreži. Granulacija ide vrlo fino, ne samo do aplikacije nego i do inačice koja je dopuštena. Za razliku od nekih drugih mehanizama, AppLocker neće onemogućiti pokretanje zabranjenih aplikacija, nego će samo dozvoliti pokretanje aplikacija koje su na popisu dopuštenih (tj. sve što nije izričito dozvoljeno jest zabranjeno).

Inicijalno sustav Windows 7 ne uključuje niti jedan antivirusni program. Odmah po instalaciji, akcijski centar javlja da nije instaliran antivirusni program te savjetuje da ga korisnik instalira što prije. Microsoft već neko vrijeme izrađuje svoj antivirusni program - Microsoft Security Essentials koji bi se trebao dodatno naplaćivati. Za sada nije poznato kada se može očekivati izlazak komercijalne inačice.

4.1.5. Osnovna grupa

Osnovna grupa (*eng. HomeGroup*) ili kućno grupiranje je način za jednostavno umrežavanje kućnih računala. Preciznije, *HomeGroup* se ne koristi za umrežavanje, već za dijeljenje sadržaja i uređaja između računala. Stvaranje osnovnih grupa odvija se u dva koraka – prvo

se odabiru biblioteke (*eng. libraries*) i pisači koji se žele dijeliti s drugim članovima grupe, a nakon toga se upisuje lozinka koja će trebati ostalim članovima da bi pristupili navedenim sadržajima. Sav sadržaj iz dijeljenih datoteka vidljiv je svim članovima grupe koji ga mogu samo čitati, ali ne i brisati ili mijenjati. Osnova grupa je potpuno neovisna od klasičnog sustava dijeljenja datoteka u Windowsima. Zahvaljujući tome, u osnovnu grupu je moguće dodati i računala koja su već pridružena nekoj domeni. Ova funkcionalnost je jako korisna u situaciji kada se poslovni prijenosnik želi koristiti i kao jedno od računala kućne mreže (za razmjenu glazbe, filmove, fotografije i sl.). Jedno računalo može biti član samo jedne osnovne grupe, a sama grupa može se koristiti jedino s mrežnim profilom „*Home*“. Nažalost, i u ovom novitetu postoji nekoliko ograničenja. U izdanjima Windowsa 7 Starter i Home Basic moguće je samo pridružiti se nekoj postojećoj osnovnoj grupi, a nije ju moguće stvoriti. Ovaj mehanizam nije kompatibilan s prijašnjim inačicama, čak ni s Windows XP-om ili Vistom. U mrežama koje sačinjavaju računala sa više različitih operacijskih sustava Windows korisnik će biti prisiljen dijeliti datoteke između računala s različitim operacijskim sustavima na način korišten u prijašnjim inačicama (koji je znatno složeniji).

4.1.6. Biometrija

Biometrija (*eng. Windows Biometric Framework* WBF) je novi dodatak Windowsa 7 koji omogućava transparentno korištenje biometrijskih metoda autentifikacije korisnika. WBF trenutno podržava samo čitače otiska prsta. Program za korištenje čitača otiska prsta do sada je bio u nadležnosti proizvođača računala, no s dolaskom WBF-a Microsoft nudi jednostavno sučelje za podešavanje svih postavki, integrirano u Control Panel-u. Sve što dobavljač računala odnosno čitača otiska mora napraviti jest napisati upravljački program (eng. driver) kompatibilan s WBF-om. S korisničke strane, integracija u Control Panel znači jednostavnije korištenje. Dodatna prednost je i integracija s domenama – WBF omogućuje prijavu na domenu, što do sad nisu omogućavali svi proizvođači prijenosnika u svojim alatima. Također, dodavanje WBF-a u Windowse omogućit će i korištenje čitača otisaka prsta u ostalim aplikacijama. Npr. prijava na Internet bankarstvo ili kupnja proizvoda preko web dućana mogla bi biti olakšana korištenjem čitača otiska prsta.

4.2. Pronađene ranjivosti

Iako Microosft stalno napominje kako je Windows 7 njihov najsigurniji operacijski sustav, nekoliko mjeseci nakon izdavanja službene inačice već su se pojavili prvi propusti i zakrpe. Slijedi pregled nekih od njih.

4.2.1. Propust u protokolu za dijeljenje datoteka Server Message Block

Sigurnosni analitičar Laurent Gaffie iznio je podatke o propustu u sustavu Windows 7. Gaffie tvrdi da ranjivost može uzrokovati ulazak računala u beskonačnu petlju te time uskratiti pristup uslugama. Propust se nalazi u SMB (*eng. Server Message Block*) komponenti Windowsa 7. SMB je mrežni protokol u aplikacijskom sloju koji se koristi za raspodjelu mrežnih resursa na operacijskom sustavu Windows. Gaffie je napomenuo da se ranjivost može iskoristiti putem Internet Explorera te napadaču omogućava zaobilaženje zaštite vatrozidom. Propust pogađa Windows 7 i Windows Server 2008 R2. Microsoft je potvrdio otkriveni propust te naglasio kako se propust ne može iskoristiti za preuzimanje nadzora nad računalom, ali se može iskoristiti za izvršavanje napada uskraćivanjem usluga. U svojim sigurnosnim uputama Microsoft je objavio postavke vatrozida u Windowsima 7 koje pomažu u sprečavanju zlouporabe propusta, a kao dodatnu sigurnosnu mjeru, dok se ne izda odgovarajuća zakrpa savjetuje se blokiranje TCP portova 139 i 445.

4.2.2. Propust u User Account Control sigurnosnom mehanizmu

Propust koji se nalazi u sigurnosnom mehanizmu za kontrolu korisničkih računa (*eng. User Account Control* UAC) otkriven je još u beta inačici Windowsa 7. UAC se može podesiti na način da ne traži od korisnika odobrenje za pokretanje prethodno odobrenih aplikacija. Upravo je tu činjenicu moguće iskoristiti tako da se kombinacijom nekoliko unaprijed odobrenih aplikacija sustav navede da pokrene zlonamjerni kod s punim administratorskim pravima. Prema riječima Microsofta, ovaj propust je riješen u konačnoj inačici Windows 7.

5. Usporedba s drugim operacijskim sustavima

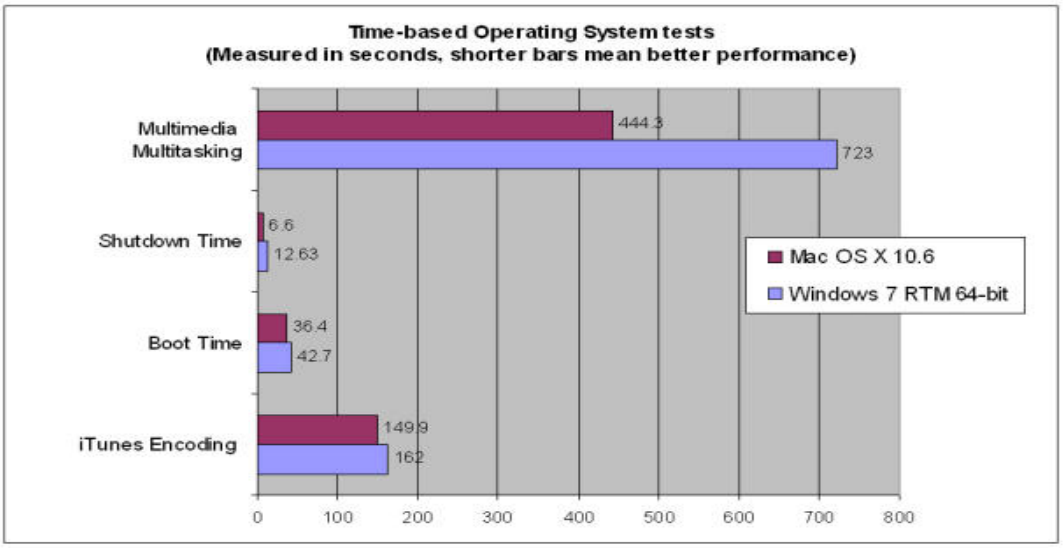
Nedavno su dva Microsoftova konkurentna objavili nove inačice svojih operacijskih sustava. Slijedi usporedba sustava Windows 7 sa Snow Leopardom i Karmic Koalom.

5.1. Mac OS X 10.6 – Snow Leopard

Mac OS X 10.6 – Snow Leopard ime je Apple-ovog novog operacijskog sustava koji se pojavio na tržištu 28. kolovoza 2009. godine. Snow Leopard je najavljen prije nešto više od godine dana te se otpočetka znalo da noviteta neće biti, nego da će težište biti stavljeno na razna poboljšanja i dotjerivanja već kvalitetnog i izuzetno stabilnog Leoparda. Tako je i bilo. Najveći se broj promjena, njih preko tri stotine, nalazi "ispod haube", a korisničko je sučelje gotovo nepromijenjeno u odnosu na prethodni Leopard. S obzirom da je Apple veliki konkurent Microsoftu, pogotovo u Americi, od njega se jako puno očekivalo. Odgovor na pitanje koji je operacijski sustav bolji, Snow Leopard ili Windows 7, dan je u sljedećoj usporedbi.

U testu je korišteno 15-inčno MacBook Pro računalo sljedeće konfiguracije: 2.5 GHz Intel Core 2 Duo, 4 GB RAM-a te 512MB GeForce 9600M GT grafičke kartice. Na tvrdom disku su instalirana dva operacijska sustava, Snow Leopard 10.6.1. te Windows 7. Kako bi Windows 7 mogli podići na Mac računalu potreban je Boot Camp. Boot Camp je Appleov softverski pomoćnik koji omogućuje instaliranje Windowsa na Mac računalima. Snow Leopard je izvorno *64*-bitni sustav sa svim aplikacijama izrađenim u *64* bita stoga je instalirana 64-bitna RTM (*eng. Released To Manufacturing)* inačica Windowsa 7 s izvornim pogonskim programima iz Boot Campa 3.0.

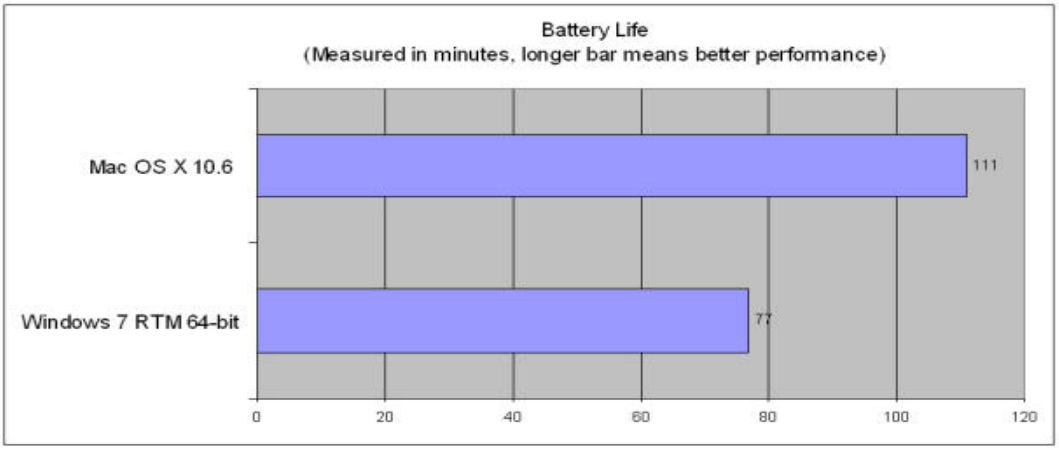
U testu se mjerilo vrijeme potrebno za određene operacije. Slika 17. pokazuje rezultate testiranja. Iz slike je vidljivo da je Snow Leopardu potrebno puno kraće vrijeme da podigne i ugasi sustav. U iTunes testu mjerilo se vrijeme potrebno da se 17 pjesama pretvori iz MP3 formata u AAC format u čemu je bio brži Snow Leopard. Zadnji test je nazvan Multimedia Multitasking. U njemu je bilo potrebno pretvoriti film iz MP4 formata u iPod fomat, dok su se u pozadini pretvarale pjesme. Taj test nije bio baš najpošteniji jer se za Windows koristio QuickTime 7, a za Snow Leoparda QuickTime X za kojeg Apple tvrdi da mu je poboljšao performanse u odnosu na prethodnu navedenu inačicu. Snow Leopard opet je bio brži.



Slika 17: Usporedba performansi Windowsa 7 i Snow Leoparda

Izvor: CNET

Slika 18. pokazuje vrijeme trajanja baterije. Iako se zna da je Microsoft unaprijedio sustav napajanja, na Mac računalu Windows 7 još uvijek brže troši bateriju.



Slika 18: Prikaz trajanja baterije

Izvor: CNET

Na temelju ovih rezultata možemo zaključiti da Snow Leopard pokazuje bolje performanse od Windowsa 7. No kod takvih zaključaka treba biti vrlo oprezan i uzeti u obzir nekoliko stvari:

- Apple ne dopušta da njihov program bude ispitan na drugim računalima tako da sve operacijske sustave koje želimo usporediti s Apple-om moramo testirati na Apple-ovoj platformi.(tu je Apple u velikoj prednosti jer je njihov i programski i sklopovski dio što se naravno vidi i u boljim rezultatima koje Apple postiže u testiranjima),
- Apple je napisao Boot Camp 3.0 koji prilikom instalacije sam pronalazi i preuzima potrebne drivere za Windows

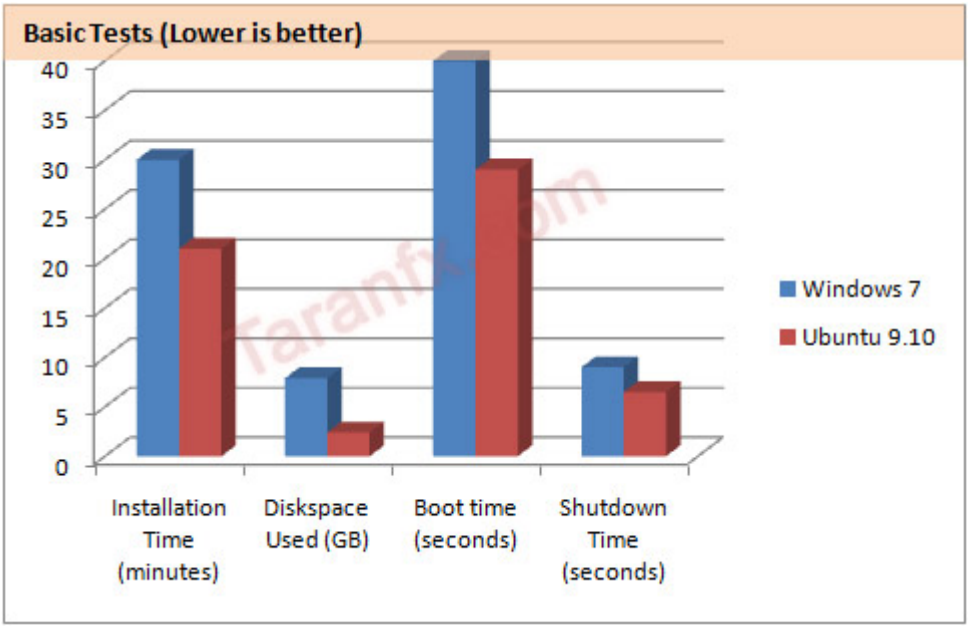
Zaključak je da je cijeli test rađen pod kontrolom Apple-a i da se bez testiranja Snow Leoparda na drugim računalima i platformama teško može zaključiti koliko je on zaista bolji (ili lošiji) od Windowsa 7.

Iako su Appleovi operacijski sustavi slovili kao izuzetno stabilni, čini se da su se i oni našli u problemima izdavanjem inačice Snow Leopard. Prva nadogradnja na novi operacijski sustav s oznakom 10.6.1 već je izdana. Skupom zakrpi Apple je riješio uočene probleme sa kompatibilnošću Sierra Wireless 3G modema te prikazom DVD sadržaja. Nažalost i dalje se otkrivaju novi propusti. Tako je otkriven i propust koji može dovesti do resetiranja (postavljanja na inicijalne – tvorničke vrijednosti) svih postavki na računalu, kao i brisanja svih podataka na tvrdom disku. Do njega dolazi kad se korisnik prijavi na račun kao gost (*eng. guest*), a nakon toga se ponovno prijavi, ali ovaj puta preko svog vlastitog računa. Jedini način kojim je moguće vratiti podatke jest ukoliko je prethodno napravljena sigurnosna kopija. Za sada se čini da se ovaj problem javlja samo kod korisnika koji su napravili samo nadogradnju sustava s Leoparda na Snow Leopard. Apple još nije izdao nadogradnju za rješenje ovog problema, niti je poznato kad će ono biti objavljeno.

5.2. Ubuntu 9.10 – Karmic Koala

Canonical je 29. listopada 2009. službeno predstavio konačnu inačicu jedne od najpopularnijih Linux distribucija. Novi Ubuntu oznake 9.10 nosi ime Karmic Koala, a donosi brojne novitete i poboljšanja. Vrlo često se nameće pitanje je li besplatni operacijski sustav jednako dobar kao i onaj za kojeg se mora izdvojiti pozamašna svota novca? Kako bi pokušali dati odgovor na to pitanje, usporedit će se svojstva oba operacijska sustava.

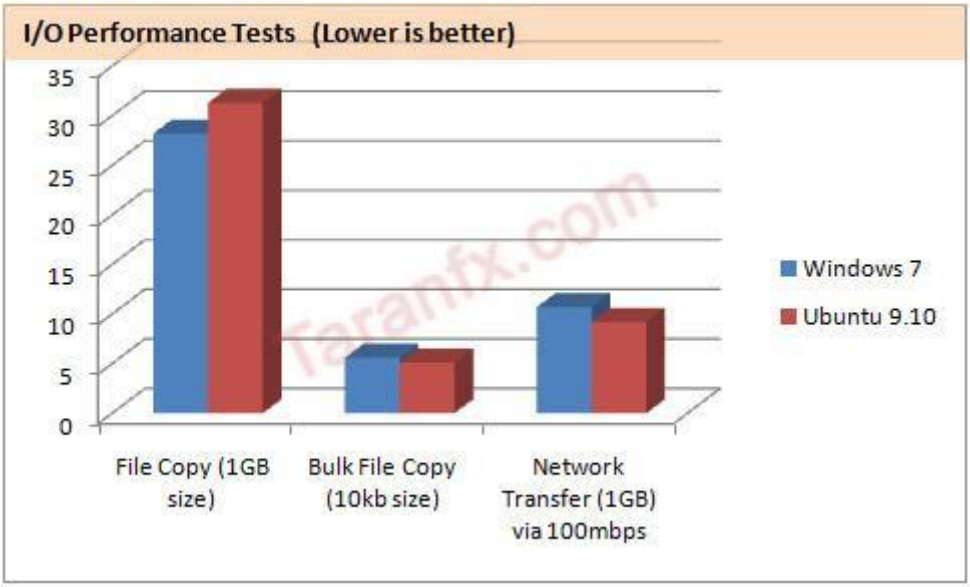
Test je rađen na računalu sljedeće konfiguracije: 2.53 GHz Intel Core 2 Duo, 4 GB RAM-a te 512 MB GeForce 230M GT grafičke kartice. Sljedeće slike prikazuju rezultate testiranja. Slika 19. prikazuje rezultate osnovnih testova poput vremena potrebnog za instalaciju, paljenje i gašenje sustava te zauzeće prostora diska (*eng. disk space*). Iz priložene slike vidljivo je da je u svim testovima Ubuntu 9.10 bio bolji.



Slika 19: Prikaz rezultata osnovnih testova

Izvor: http://www.taranfx.com/windows-7-vs-ubuntu

Slika 20. prikazuje rezultate testiranja performansi ulazno izlaznih jedinica. Prvi test obuhvaćao je mjerenje vremena potrebnog da se prebace podaci veličine 1 GB iz vanjske memorije na računalo. Drugi test mjerio je vrijeme potrebno za kopiranje skupine podataka, svakog veličine 10 kb. Zadnji test je mjerio vrijeme potrebno za prebacivanje podataka lokalnom mrežom brzinom 100Mbps. Windows 7 je bio brži samo u prvom testu dok je u preostala dva bio brži Ubuntu 9.10.



Slika 20: Prikaz rezultata testiranja performansi ulazno izlaznih jedinica

Izvor: http://www.taranfx.com/windows-7-vs-ubuntu

Iz priloženih rezultata vidi se da novi Ubuntu 9.10 pokazuje zavidne rezultate u usporedbi s Windowsima 7. Ubuntu je danas najpopularnija distribucija Linuxa, a iz ovih rezultata jasno je da će broj njezinih korisnika i dalje rasti.

Kako raste broj korisnika koji se s njime služe, tako raste i broj napada zlonamjernih korisnika. Da u tome nije iznimka ni Linux vidi se i iz činjenice da je nedavno otkrivena ranjivost u radu jezgre

operacijskog sustava. Jezgra je središnji dio operacijskog sustava i obavlja zadaće poput upravljanja memorijom, rukovanja sklopovljem i sl. Sigurnosna je ranjivost posljedica logičke pogreške u datoteci "drivers/net/skfp/skfddi.c". Zlonamjerni korisnik može iskoristiti ranjivost za zaobilaženje određenih sigurnosnih ograničenja. Svim se korisnicima ranjivog operacijskog sustava savjetuje nadogradnja jezgre na novije inačice, kod kojih je sigurnosna ranjivost uklonjena.

6. Zaključak

Dugo iščekivana inačica operacijskih sustava Windows nosi naziv Windows 7. Iako je tek nekoliko mjeseci na tržištu, prvi dojmovi i kritike izuzetno su pozitivni, a prodaja je u stalnom porastu. Ako je vjerovati podacima iz Microsofta, tržišni udio Windows 7 već sada je nadmašio udio koji je Vista postigla u više od pola godine.

Na temelju prethodno navedenih testova koje su provodili stručnjaci diljem svijeta može se zaključiti da je Microsoftova konkurencija svakim danom sve opasnija. Dva mjeseca prije lansiranja Windowsa 7, Microsoftov stari suparnik - Apple, predstavio je svoj poboljšani operacijski sustav (Snow Leopard). Umjesto novih dodataka, većina promjena odnosila se na bolju i lakšu uporabu. Za razliku od Microsofta, Apple proizvodi i softver i hardver, što olakšava rad i stabilnost sustava. Iako je Apple već dugo vrijeme standard za kvalitetu, previsoke cijene Macintosh računala sigurno neće još neko vrijeme ugroziti dominaciju Windowsa. S druge strane, najveći potencijalni izazov Microsoftu mogao bi se pojaviti iduće godine kada Google najavljuje izdavanje svog operacijskog sustava – Chrome OS. Sustav koji je rađen na istim temeljima kao i Linux trebao bi biti jeftin i jednostavan za uporabu te omogućiti pristup svim Google-ovim aplikacijama. Iako su kritičari jako skeptični prema ovom operacijskom sustavu treba ipak pričekati i vidjeti što je to Google pripremio.

Samo nekoliko mjeseci nakon izdavanja Windows 7, već se počelo šuškati da Microsoft radi na razvoju Windowsa koji bi mogli podržavati 128-bitnu arhitekturu. S obzirom da je za razvoj potreban i odgovarajući hardver, Microsoft se nada da bi uz suradnju s Intelom, AMD-om, HP-om i IBM-om moglo doći do realiziranja navedene arhitekture. Windows 8 mogući je naziv sljedećih Windowsa koji bi trebali donijeti značajnije promjene u odnosu na dosadašnje sustave. Spominju se novi algoritmi i API funkcije za hibernaciju, podrška za klastere (skup usko povezanih računala koja rade zajedno tako da se mogu gledati kao jedno računalo), kvalitetnija podrška za SSD-ove te još mnoštvo ostalih tehnologija. Sve ove informacije nisu još službeno potvrđene, a datum izlaska novih Windowsa očekuje se tijekom 2012. godine.

7. Reference

[1] Microsoft Windows, http://en.wikipedia.org/wiki/Microsoft_Windows, prosinac 2009.

[2] History of Microsoft Windows
http://en.wikipedia.org/wiki/History_of_Microsoft_Windows, prosinac 2009.

[3] Novosti u sustavu Windows 7
http://www.microsoft.com/croatia/windows/windows-7/whats-new.aspx, prosinac 2009.

[4] Windows 7 Performance Tests,
http://www.pcworld.com/article/172509/windows_7_performance_tests.html, prosinac 2009.

[5] Propust u Windowsima 7
http://www.bug.hr/vijesti/propust-windowsima-7/99403.aspx, prosinac 2009.

[6] Microsoft popravio Windows 7 UAC
http://www.sigurnost.info/vijesti/43-itzatita/560-microsoft-popravio-windows-7-uac-, prosinac 2009.

[7] Performance showdown: Windows 7 vs. Snow Leopard
http://reviews.cnet.com/8301-31012_7-10319612-10355804.html, prosinac 2009.

[8] Windows 7 vs Ubuntu 9.10, http://www.taranfx.com/blog/windows-7-vs-ubuntu, prosinac 2009.

[9] Windows 8 u 128 bita, http://www.bug.hr/vijesti/windows-8-128-bita/98923.aspx, prosinac 2009.